Oracle Fusion Cloud Customer Experience

Securing Sales and Fusion Service

Oracle Fusion Cloud Customer Experience
Securing Sales and Fusion Service

F77857-04

Author: Carmen Myrick, Shannon Connaire, Dinesh Venugopal, Sekhar Pappu, Jiri Weiss

Contents

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

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.

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 About This Guide

Audience and Scope

This guide provides you with the concepts and procedures you need to implement and administer security.

You perform some of the tasks described in this guide only when you're implementing the sales applications. But most tasks can be performed at any time and as new requirements emerge. Use the guide to learn more about topics such as these:

- How role-based access control is implemented in the sales applications.
- How users gain visibility to object data.
- 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 set up, manage, and use the Security Console and the Sales and Service Access Management work areas.
- How to create security artifacts, such as security policies and roles.

During implementation, you perform security-related tasks from a functional area task list. Once the implementation is complete, you can perform most security-related tasks on the Security Console or the Sales and Service Access Management work area. Any exceptions are identified in relevant topics. For example, you create users in the Manage Users work area, not on the Security Console.

Related Guides

Refer to the following guides for additional information about implementing and administering Oracle Fusion Cloud Sales and Fusion Service.

Title	Description
Oracle Fusion Cloud Sales Automation: Implementing Sales	Explains how to implement a sales force automation solution using features of both Digital Sales (Next Gen Sales) and CX Sales. See the Implementation Reference guide for additional setups.
Oracle Fusion Cloud Sales Automation: Implementation Reference	Implementation reference guide for Oracle Sales.
Oracle Fusion Service: Implementing Service Center with the Classic User Experience	Describes how to set up service components and features of Oracle Fusion Service.
Oracle Fusion Service: Implementing Service Center with the Redwood User Experience	Describes implementing Service Center with the Redwood User Experience.

Title	Description
Oracle Fusion Cloud Applications: Configuring Applications Using Application Composer	Describes how to use Application Composer to configure and extend Oracle Applications Cloud.
Oracle Fusion Cloud Applications: Configuring and Extending Applications	Describes how to use runtime tools such as Page Composer or flexfields to configure and extend Oracle Applications Cloud.
Oracle Fusion Cloud Customer Experience: Understanding Import and Export Management for Sales and Fusion Service	Describes how to import legacy and other data into Oracle CX Sales and Fusion Service using Import and Export Management, and export data out of these applications.
Oracle Fusion Cloud Customer Experience: Security Reference for Sales and Fusion Service	Provides a reference to roles, role hierarchies, privileges, and policies as delivered for the Sales and Fusion Service offerings.
Oracle Fusion Cloud Customer Experience: Creating and Administering Analytics for Sales and Fusion Service	Explains how to create, edit, and embed analytics in Sales and Fusion Service applications.
Oracle Fusion Cloud Customer Experience: Subject Areas for Transactional Business Intelligence in Sales and Fusion Service	Provides descriptions, business questions, and security roles for the subject areas in Sales and Fusion Service.
Oracle Fusion Cloud Customer Experience: Implementing Customer Data Management	Describes tasks to configure and set up Oracle CX Customer Data Management capabilities, such as, duplicate identification, duplicate resolution, address verification, and data enrichment.
Oracle Fusion Cloud Sales Automation: Security Reference for Incentive Compensation	Provides a reference of roles, role hierarchies, privileges, and policies as delivered for Incentive Compensation.
Oracle Fusion Cloud Sales Automation: Implementing Incentive Compensation	Describes how to configure and set up Incentive Compensation.
Oracle Fusion Cloud Customer Experience: Understanding Scheduled Processes	Describes the scheduled processes for Oracle Fusion Cloud Sales and Oracle Fusion Service and contains guidance on how to use them.

Related Topics

- Oracle Help Center

2 Authentication

Authentication and Identity Management

Read this topic for a quick overview of the authentication and identity management services provided by Oracle for Cloud Applications.

Standard Authentication for Cloud Applications

Authentication, the process of verifying that a user is who they claim to be, is applied to all users, automated agents, or Web services that access an Oracle Cloud application. User credentials are checked at login and access is then granted or denied. In the standard method of authentication in Oracle Cloud environments, authentication providers validate user and application access based on a user name-password combination. Authentication providers also make user identity information available to other Cloud components when needed.

Identity Store

The Oracle Cloud authentication providers access the LDAP identity store, which is a logical repository of enterprise user identity data. Your LDAP directory stores definitions of LDAP user accounts.

In general, changes you make to user accounts are automatically synchronized between your sales application and your LDAP directory server. But you must also run processes on a daily basis to manage information exchange between your application and your LDAP directory server. For information, see the chapter about setting up application security.

Single Sign-On Authentication

You can opt to use single sign-on as your user authentication solution. Single sign-on enables users to sign in to a system using one set of credentials to access multiple applications.

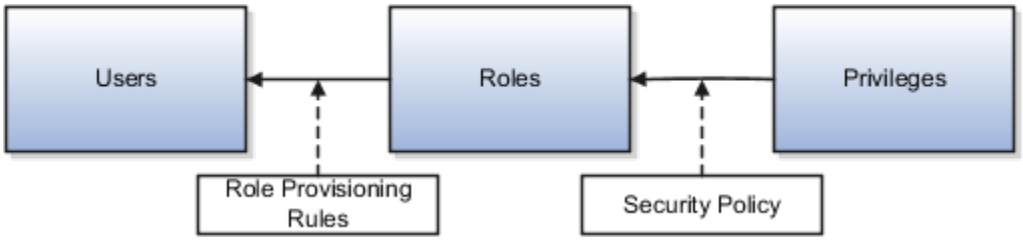
You can set up Oracle Applications Cloud to operate as your single sign-on service provider. Doing so provides users with single sign-on access to applications and systems located across your enterprise network. Single sign-on also applies to signing out of the enterprise network. When users sign out form one application, they're automatically signed out from all applications on the network. For information on configuring single sign-on, see the chapter Single Sign-On.

3 Introduction to Role-Based Security for Sales and Service

Overview of Role-Based Access Control

When you receive your Oracle Cloud application, access to its functionality and data is secured using a role-based access control security model. In a role-based access control security model, you provide users with roles which are assigned access privileges to protected resources.

This diagram shows the relationship between users, roles, and privileges.



In the sales application, users gain access to application data and functions when you assign them these types of roles:

- Job roles, which provide users with the permissions they need to perform tasks that are specific to a job, such as a sales representative
- Abstract roles, which provide users with the permissions to complete tasks that are common to all users

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. For example, a user might be assigned the Sales Manager role, the Sales Analyst role, and the Employee role. In this case, the user has this access:

- As an employee, the user can access employee functions and data.
- As a sales manager, the user can access sales manager functions and data.
- As a sales analyst, the user can access sales analysis functions and data.

When the user signs in to the application and is successfully authenticated, a user session is established and all the roles assigned to the user are loaded into the session repository. The application 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.

Related Topics

- Role Provisioning

Predefined Sales and Service Roles

Oracle provides many predefined job and abstract roles as part of the security reference implementation for the sales and service applications. The security reference implementation is a predefined set of security definitions that you can use as-is.

Sales Roles

The following are some of the predefined job roles for sales users:

- Channel Account Manager
- Channel Operations Manager
- Channel Sales Manager
- Customer Contract Administrator
- Customer Data Steward
- Customer Relationship Management Application Administrator
- Data Steward Manager
- Enterprise Contract Administrator
- Enterprise Contract Manager
- Incentive Compensation Manager
- Incentive Compensation Plan Administrator
- Incentive Compensation Analyst
- Inside Sales Manager
- Inside Sales Representative
- Marketing Manager
- Marketing Operations Manager
- Marketing VP
- Master Data Management Application Administrator
- Partner Administrator
- Partner Sales Manager
- Partner Sales Representative
- Sales Administrator
- Sales Analyst
- Sales Catalog Administrator
- Sales Lead Qualifier
- Sales Manager
- Sales Representative
- Sales VP
- Supplier Contract Administrator

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

- Employee
- Resource

Note: Be extremely cautious when assigning predefined roles as-is. See *Guidance for Assigning Predefined Roles* and "Advisory Note on Subscription Impact" in the *Security Reference for Common Features* guide.

If you're using the Incentive Compensation functionality, you can also assign the following abstract roles to users:

- Incentive Compensation Participant
- Incentive Compensation Participant Manager

Service Roles

A number of job roles and duty roles are predefined in the Service offering. These are the predefined job roles specific to this product area:

- Chat Agent
- Customer Service Manager
- Customer Service Representative
- Knowledge Analyst
- Knowledge Manager
- Field Service Technician
- Internal Help Desk Administrator
- Internal Help Desk Agent
- Internal Help Desk Manager
- Case Manager
- Case Worker

Guidance for Assigning Predefined Roles

As a security administrator, you have access to the predefined roles and privileges that are readily available for assignment. However, you must assess the user's need before assigning those roles as is with the complete set of privileges.

When you assign predefined roles and privileges as is, you're entrusting users with full access to all data and functionality. Such unrestricted access without really determining the business need might pose a security concern. Also, the assigned privileges might account for subscription consumption irrespective of whether you purchased the cloud service or not. A detailed list of all the predefined roles that impact subscription is available for reference. See the spreadsheet *Predefined Roles with Subscription Impact*.

If you are aware of a requirement or recommendation to assign specific predefined roles as is, it's fine to do so. For example, only while setting up an application, you may need to assign the predefined Application Implementation Consultant role as is. Once the setup is complete, you can unassign it. Otherwise, the recommended process is to always

make a copy of the predefined role, remove the privileges you don't need, and assign only the required privileges. That way, you will hit the subscription usage in a controlled way, based on your business need.

> **Note:** Updates to Fusion Applications might also include changes to certain predefined roles. Check the release readiness documents for your product area to know if there are any updates to the predefined roles that are in use. If you find changes that are relevant, incorporate the same changes to your custom role. This will remain an ongoing maintenance activity for the custom roles.

Related Topics

- Compare Roles
- Role Copying or Editing
- Create Roles in the Security Console

Options for Reviewing Predefined Roles

There are a number of ways in which you can access information about predefined roles. This information can help you to identify which users need each role and whether to make any changes before provisioning roles.

Security Console

On the Security Console, you can:

- Review the role hierarchy of any job, abstract, or duty role.
- Extract the role hierarchy to a spreadsheet.
- Identify the function security privileges and data security policies granted to a role.
- Compare roles to identify differences.

> **Tip:** The role codes of all predefined roles have the prefix ORA_.

Reports

You can run the User and Role Access Audit Report to produce an XML-format report of the function security privileges and data security policies for a specified role, all roles, a specified user, or all users.

Security Reference Manuals

The following manuals describe the security reference implementation for Oracle CX Sales and Fusion Service users:

- The Oracle Applications Cloud Security Reference for Common Features includes descriptions of all predefined security data that's common to Oracle Fusion Applications.
- The Security Reference for CX Sales and Fusion Service includes descriptions of all predefined security data for Oracle CX Sales and Fusion Service.
- The Security Reference for Incentive Compensation includes descriptions of all predefined security data for Incentive Compensation.

These manuals contain a section for each predefined job and abstract role. For each role, you can review:

- Duty roles
- Role hierarchy
- Function security privileges
- Data security policies

You can access the security reference manuals on https://docs.oracle.com/.

Sales and Service Access Management Work Area

You can review the visibility provided by a job role to object data in the Sales and Service Access Management work area. You can display a read-only view of all the data security policies provided by a selected role for a selected object.

Roles for Workflow Administration Access

Predefined roles provide access to workflow administration functionality. Users with the workflow roles can perform tasks such as setting up approval rules and managing submitted approval tasks.

This table identifies the predefined Oracle Business Process Management (BPM) role for sales workflow administration access, and the predefined job roles that inherit it. It also shows the BPM role that provides workflow administration access for all product families. You can assign a predefined BPM role to a custom job role, if required.

Product Family	Role Name and Code	Inherited by Job Role
Sales	BPM Workflow Customer Relationship Management Administrator BPMWorkflowCRMAdmin	Corporate Marketing Manager Customer Relationship Management Application Administrator Marketing Analyst Marketing Manager Marketing Operations Manager Marketing VP Sales Lead Qualifier
All	BPM Workflow All Domains Administrator Role BPMWorkflowAllDomainsAdmin	This role isn't assigned to any predefined job role, but you can add it to custom job roles.

Role Types

The different types of roles provided with your sales application work together to provide users with permissions to application resources. These types of roles are provided:

- 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. Sales Representative and Sales Manager are examples of predefined job roles. You can also create job roles.

Job roles provide users with the permissions they need to carry out tasks specific to their jobs. For example, providing a user with the Sales Manager job role permits the user to manage salespeople within the organization, follow up on leads, generate revenue within a territory, build a pipeline, manage territory forecasts, and assist salespeople in closing deals. You can assign job roles directly to users.

Abstract Roles

Abstract roles represent a user's functions in the enterprise that are independent of the job they do. These are examples of the abstract roles used in the sales application:

- Employee
- Resource

Abstract roles let users to perform tasks that are common to all employees and resources. For example, users who are employees must be provisioned with the Employee abstract role, so they can update their employee profiles and pictures. You must also provision users with the Resource abstract role, so they can be assigned as a sales resource to work on leads, opportunities, and other sales tasks. You can assign abstract roles directly to users. You can also create abstract roles.

Duty Roles

Job and abstract roles permit users to carry out actions because 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.

For example, the Sales Manager job role inherits the Sales Lead Follow Up duty and the Sales Forecasting Management duty. The Sales Lead Follow Up duty makes it possible for managers to work with leads. The Sales Forecasting Management duty lets managers work with sales forecasts. Job roles and abstract roles can inherit duty roles either directly or indirectly.

You can create duty roles and can include predefined and custom duty roles in custom job and abstract roles. You don't assign duty roles directly to users.

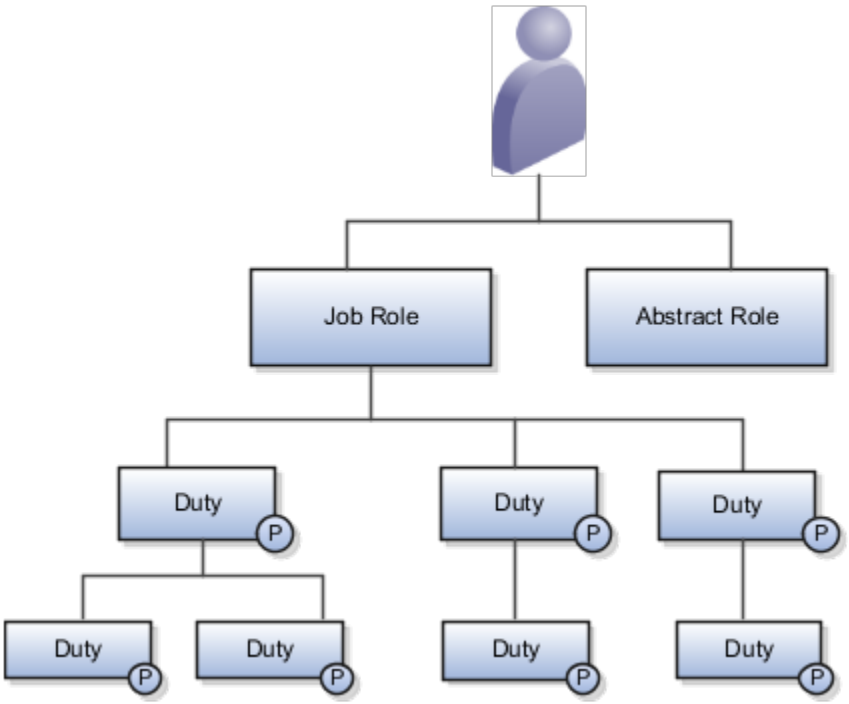
Related Topics

- Duty Role Components

Role Hierarchies and Role Inheritance

Each role is a hierarchy of other roles that are linked to each other in a parent-child relationship. As this hierarchy chart shows, 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.

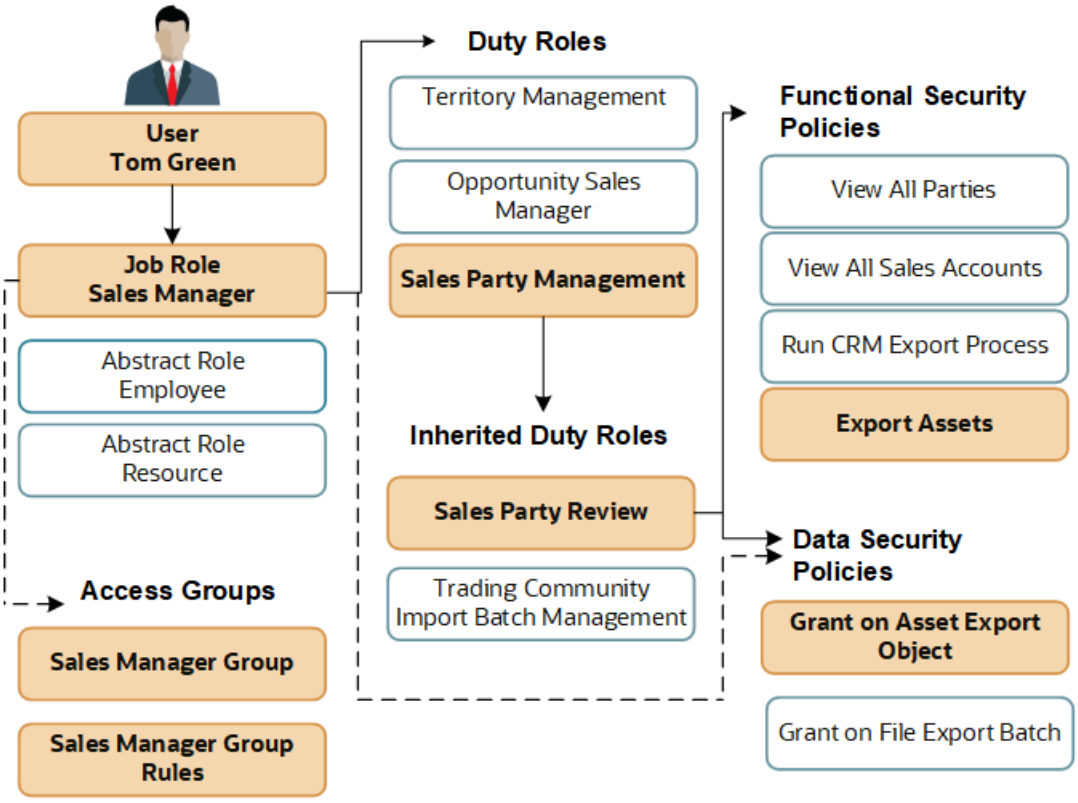


Role hierarchies allow privileges to be grouped to represent a feature set, which simplifies feature management. Role hierarchies also provide privilege granularity and facilitate role reuse. For example, each role hierarchy beneath the job role represents a feature that's available through the job role 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.

Role Inheritance Example

This example shows how roles and privileges are inherited for a user, Tom Green, assigned the Sales Manager job role. The chart shows a few of the duty roles that Tom inherits.



As an employee sales manager, Tom Green is provisioned with the roles required to do the job: the Sales Manager job role, and the Employee and Resource abstract roles. Roles are inherited as follows:

- The Sales Manager job role inherits duty roles including the Sales Party Management duty role and the Opportunity Sales Manager duty role.
- Duty roles inherit other duty roles. For example, the Sales Party Management duty inherits the Sales Party Review duty and the Trading Community Import Batch Management duty, as well as many privileges.
- The duty roles can be associated with functional security policies and data security policies. For example, the inherited Sales Party Review duty includes security policies that specify which application pages sales managers can access to export assets.
- Data security policies are also assigned to the Sales Manager job role directly.
- When the sales manager Tom Green is provisioned with the Sales Manager job role, he's also automatically enrolled into a system access group, the Sales Manager Group, which is assigned rules that provide the same access to data as the data security policies assigned to the Sales Manager job role.

  If you were provisioned with the sales application for the first time in release 22B or later, your database resources are secured using system access groups and rules by default. Using access groups and rules is also the recommended way of configuring data security. For additional information about access groups, see the topic *Data Privileges and Access Groups*.

Duty Role Components

If you want to configure the predefined security model by creating your own duty roles, then it's important to understand how duty roles are constructed.

A typical duty role consists of two components: data security policies, and function security privileges. Duty roles can also inherit other duty roles.

Function Security Policies

Function security policies permit a user who's assigned a duty role to access different user interface elements, Web services, tasks flows, and other functions. For example, a sales manager who has the Delete Opportunity functional policy can view and click the Delete button. Removing that policy removes the button from view. A function security policy is composed of:

- A duty role name. The name of the duty where the policy applies, for example, Opportunity Sales Manager.
- A functional privilege that specifies the application features that are being secured, for example, Delete Opportunity.

Some user interfaces aren't subject to data security so some function security privileges don't have an equivalent data security policy.

In the security reference manuals, functional privileges are listed in the Privileges section.

Data Security Policies

Data security policies specify the 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 role name. The name of the role the data security policy is granted to. The role can be a duty role, a job role or an abstract role. For example, the Opportunity Sales Manager duty role.
- The business object that's being accessed, for example, opportunity. The data security policy identifies the object by its table name, for example, MOO_OPTY for opportunity.
- A data privilege that defines the actions permitted on the data. For example, View Opportunity.
- The condition that must be met for access to the business object to be granted. For example, sales managers can view opportunities provided they're in the management chain or are members of the sales team for the opportunity.

  If the View All condition is specified, the role provides access to all data of the relevant type.

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 Cloud 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 Cloud applications.

Data Privileges and Access Groups

If you started using the sales application for the first time in release 22B or later, your database resources are secured through system access groups and rules and not through data security policies.

When you assign job roles to users, users are automatically assigned membership of an associated system access group, and receive all the data permissions provided by the access group object sharing rules. The access group object sharing rules specify the access groups that can perform a specified action on an object, and the conditions under which the action can be carried out.

An access group rule is composed of:

- The business object that's being accessed, for example, opportunity.
- An access level that defines the actions permitted on the data. For example, Read or Update access.
- The condition that must be met for access to the business object to be granted. For example, sales managers can view opportunities provided they're in the management chain or are members of the sales team for the opportunity.
- The name of the access group the object sharing rule is assigned to. A rule can be assigned to many access groups.

For additional information about access groups, see the Access Groups chapter and the Configure and Troubleshoot Data Security chapter in this guide.

Guidelines for Configuring Security

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

For example, the predefined Sales Representative job role includes sales forecasting privileges. If sales managers do sales forecasting in your organization, not the sales representatives, then you can create a sales representative role without those privileges.

During implementation, you evaluate the predefined roles and decide whether changes are needed. If changes are required, then you can either create a role from scratch or copy an existing role. 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_. For example, the role code of the Sales Representative application job role is ORA_ZBS_SALES_REPRESENTATIVE_JOB.

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 can create your own job roles. Add duty roles to custom job roles, as appropriate.

Predefined Roles with Different Privileges

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

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.

The typical implementation doesn't use custom duty roles.

Related Topics

- Options for Reviewing Predefined Roles

Oracle Cloud Applications Security Console

The Security Console is an easy-to-use administrative work area where you perform most security-management tasks.

Security Console Tasks

You can do these tasks on the Security Console:

- Review role hierarchies and role analytics.
- Create and manage custom job, abstract, and duty roles.
- Review the roles assigned to users.

  > **Note:** You use the Manage Users work area, not the Security Console, to create users and to provision users with roles.

- Compare roles.
- Simulate the Navigator for a user or role.
- Manage the default format of user names and the enterprise password policy.
- Manage notifications for user-lifecycle events, such as password expiration.
- Manage PGP and X.509 certificates for data encryption and decryption.

  > **Note:** Oracle Sales and Fusion Service don't use certificate functionality.

- Set up federation, and synchronize user and role information between Oracle Applications Security and Microsoft Active Directory, if appropriate.

Security Console Access

You must have the IT Security Manager job role to use the Security Console. You open the Security Console by clicking the **Security Console** link under the **Tools** heading in the Navigator. These tasks, performed in the Setup and Maintenance work area, also open the Security Console:

- Manage Job Roles
- Manage Duties
- Manage Data Security Policies

4 Data Sharing Mechanisms and Object Visibility

Data Sharing Mechanisms

Review the information in this chapter to learn how users gain visibility to various objects used in the sales and service applications.

The conditions specified in access group rules or data security policies control visibility to record-level data associated with a schema object, such as an opportunity. Conditions can use the following components as mechanisms for sharing data, provided that the sharing mechanism is applicable for the object:

- Team
- Partner team
- Territory
- Resource hierarchy
- Business unit

For example, for the Opportunity object, data can be shared through team membership, through the resource hierarchy, or through territory membership.

How Sales Users Gain Access to Sales Information

The security reference implementation provided by Oracle determines who can access opportunity information in your sales organization. While basic information on accounts and contacts is available to all salespeople, your access to sales data is restricted by your position in the resource hierarchy, membership in the sales team, and ownership.

Whether or not you can access a particular opportunity or a lead depends on your membership in the resource and territory hierarchies. Here's how you gain access to opportunities. Lead access follows the same pattern. You can access an opportunity if:

- You create the opportunity.
- You're on the opportunity sales team.
- The opportunity owner or sales team member is your direct or indirect report in the resource hierarchy.
- You're the owner or are a member of the territory assigned to the opportunity.
- You're the owner or member of a parent territory of the territory assigned to the opportunity.
- You're assigned to a territory for the account associated with the opportunity.
- You're assigned to a territory that's a parent of the territory for the account associated with the opportunity.

Salespeople can see all opportunities related to their accounts but access differs between territory members and opportunity members:

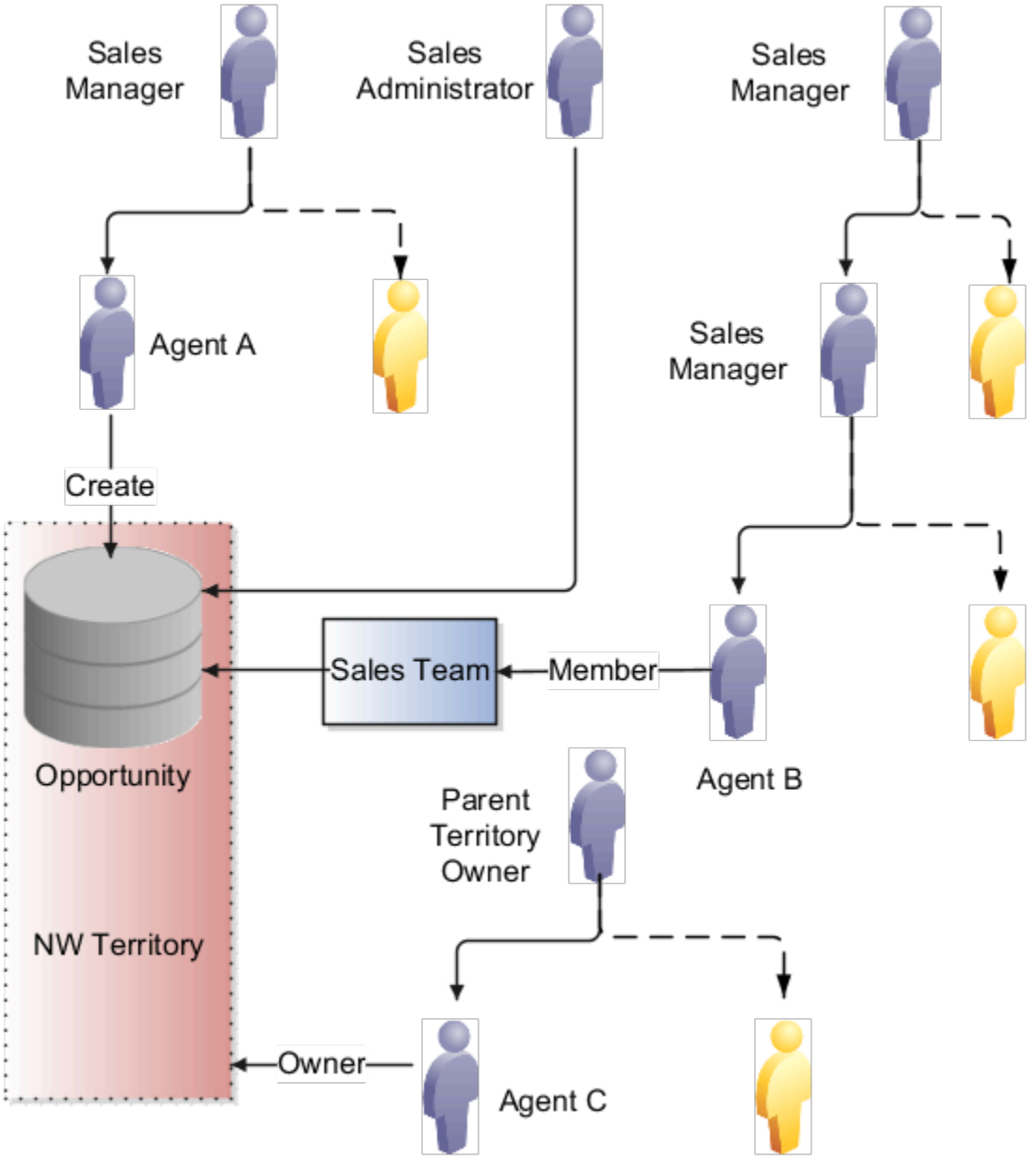
- An opportunity owner gets full access to the opportunity, which includes the ability to edit as well as add and remove team members.
- Owners and members of territories or parent territories assigned to the opportunity account get read-only access to the opportunity and aren't added to the opportunity sales team.
- Owners and members of territories assigned to the opportunity product lines are added as a distinct list of territories to the opportunity sales team. Owners and members of these territories get full access to the opportunity. Depending on a profile option, either only the owner or all the members of the territory are added as resources to the opportunity sales team. Regardless of the access level for these members as a resource on the opportunity team, they always have full access.

  Owners and members of parent territories of the territory assigned to the opportunity aren't added to the opportunity sales team but they always get full access.

The following diagram illustrates some of the different ways that you can gain access to an opportunity:

- Named agents in the diagram (A, B, and C) can access the opportunity.
- Unnamed agents (highlighted in yellow) can't access the opportunity.
- Sales managers can access the opportunity because a salesperson in their management chain has access.
- Owners of parent territories can access the opportunity through the sales territory hierarchy.

This diagram shows who in a sales hierarchy can access an opportunity.



- Agent A can access the opportunity because she created it. When you create an opportunity, you're the initial owner.
- Agent B can access the opportunity because he's on the sales team.
- Sales managers who are higher up in the management chain can also see the opportunity because access is provided through the resource hierarchy. The managers of Agent A and Agent B can access the opportunity information, but agent A and Agent B's colleagues can't.
- Agent C can access the opportunity because he's the owner of the NW territory. The owner of the parent territory can also access the opportunity.
- Sales administrators can access the opportunity.

Note: Access using accounts isn't shown in this diagram.

Special Access

Some access isn't affected by the management hierarchy and membership in sales teams or territories. This special access includes:

- Administrators: Users assigned the Sales Administrator job role get full access to opportunities and other objects. This access is based on their privileges, regardless of where the administrators are in the management hierarchy. Administrators don't have to be on the sales team or members of territories.
- Deal Protection: Salespeople assigned to an opportunity retain the sales credit on an opportunity even if they're moved to another opportunity.

How Sales Users Gain Access to Digital Sales Objects

Three objects are specific to Digital Sales: the Sales Contests object, the Sales Goals object, and the Sales KPI object. Sales users with access to the Digital Sales UIs gain access to these object records through a number of access paths. Review the following sections to learn who can create and view sales contests, sales goals and sales KPIs.

How Users Gain Access to Sales Contests

You can access data about a sales contest if you're the owner of the contest, are a participant in the contest, or if you're in the management hierarchy of the owner or a participant. All users who have access to a contest can view data for all contest participants. Specifically, you can access a sales contest if:

- You create the contest. If you create a contest, you're the contest owner.

  Sales Managers, Sales VPs, and the Sales Administrators can create contests. Sales Managers and Sales VPs can only add participants from their own downward hierarchy to the contest. Sales Administrators can add any users as participants.
- You're a participant in the contest.

  Users added to a contest can view contest data for themselves and for all other participants in the contest.
- The contest owner or participant is your direct or indirect report in the resource hierarchy.

  You can view contest details for your reports.
- The user who owns the contest can edit or delete the contest.
- Sales administrators can view all contests and can edit and delete any contest.

Once a contest is running, the contest owner, all participants, and the management hierarchy of the participants receive access to view the contest. Everyone who gets access to the contest can see the same information. So, for example, contest participants can see each other's scores on a given KPI, along with statistics such as the daily average score of each participant.

How Users Gain Access to Sales Goals

Whether or not you can access data about a particular sales goal depends on your membership in the resource hierarchy and whether or not you're a goal participant. In general, you can access goal data for yourself and for your direct and indirect reports. Specifically, you can access a goal if:

- You create the goal.

  The user who creates the goal can view the goal and can edit and delete the goal.

  Sales Managers, Sales VPs, and the Sales Administrator can create goals. When creating a goal, Sales Managers and Sales VPs can only add users from their own downward resource hierarchy as participants of the goal. Sales Administrators can add any users as goal participants.
- You're a participant of the goal.

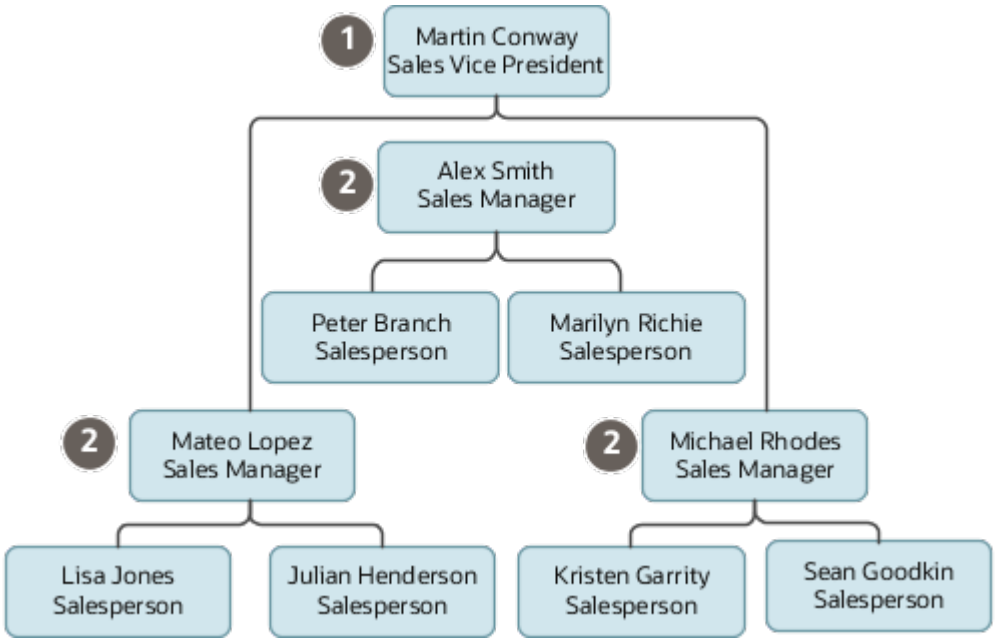
  Each participant can see only their own goal target and progress.
- The goal owner or participant is your direct or indirect report in the resource hierarchy.

  Members of the management hierarchy of a goal participant can view goal data and edit targets for goal participants in their own downward resource hierarchy.

  For example, the following figure shows an example sales hierarchy consisting of a sales VP who has three sales managers reporting to him. Each of the sales managers has a team consisting of two direct reports. If Martin

Conway, the sales VP, sets a goal for all the sales people in his organization, then each member of the hierarchy has access to goal performance data according to their own position in the hierarchy as follows:

a. (Callout 1) Martin Conway can see goal performance data for each of the three sales teams and for each participant in each team.
b. (Callout 2) Each sales manager can see goal performance data for their direct reports. So Alex Smith can see goal data for Peter and Marilyn but not for any of the salespeople on Michael or Mateo's teams.
c. Each individual salesperson can see their own goal performance data but can't see goal data for anyone else.



- Sales administrators can access all goals and all goal participants, and can edit and delete any goal.

How Users Gain Access to Sales KPIs

Oracle provides a number of predefined key performance indicators (KPIs) that sales managers can use for creating goals and contests but you can also create your own KPIs. All users can view KPIs but only sales administrators can create and manage KPIs. You can access sales KPI data as follows:

- All users can view the predefined sales KPIs.

  Sales Managers, Sales Representatives, Sales VPs, and Sales Administrators can view the predefined sales KPIs.
- Only sales administrators can create custom KPIs.

  Sales Managers, Sales Representatives, and Sales VPs can view all active, custom sales KPIs.
- Sales administrators can update, delete, and change the status of custom KPIs. Sales administrators can also change the status of predefined KPIs and can copy predefined KPIs.

Multiple Business Units and Data Access for Sales Objects

The way that you implement multiple business unit functionality in your enterprise can affect your users access to object transactional data.

A business unit (BU) is a unit of an enterprise that performs one or more business functions, such as sales or marketing. A business unit primarily provides a means of separating or sharing setup data and controlling transactional data access within an enterprise. By default, an enterprise structure is created as a single business unit to which all users belong but you can create additional business units if you need to.

Users are associated with a business unit through their resource organization membership. Resource organizations are mapped to one or more business units. When you create a sales user and assign the user to a resource organization, the user gains access to each business unit that's mapped to the resource organization. For example, users can access relevant transactional data associated with their primary business unit, but might also have access to relevant transactional data in other business units through their resource organization.

> **Note:** When you create a user in the sales application, you specify a business unit for the user. But only the BUs associated with the user's resource organization are relevant in determining the business units a user can access. If a business unit isn't specified for a resource organization, the default business unit is used.

Within the sales application, these business objects support the use of multiple business units:

- Contracts
- Leads
- Opportunities
- Resource Organizations
- Territories

When you create an object that supports multiple business units, such as an opportunity, you specify the business unit to associate with the object.

Object Access in a Single Business Unit Environment (Default)

In this type of implementation, all users can access master data, such as product or account information, by default. Users also have access to transactional data for objects such as opportunities, contracts or leads:

- Sales administrators can access transactional data for all objects.
- Sales users gain access to transactional data for an object through one of these methods:
    - They have been granted full access to the object
    - Through territory or team membership
    - Through the resource management hierarchy

  Full access to an object is provided through data security policies that include a condition of All Values. This table provides information about other methods of object access.

Type of Object Access	Description
Territory membership	You gain access to an object if: o You're the owner or member of the territory that's assigned to the object. o You're the owner or member of an ancestor territory of the territory assigned to the object. o Your direct or indirect report in the resource hierarchy is the owner or a member of the territory assigned to the object. o Your direct or indirect report in the resource hierarchy is the owner or member of an ancestor territory of the territory assigned to the object.
Team membership	You gain access to an object if: o You're a member of the sales team assigned to the object. o Your direct or indirect report in the resource hierarchy is a member of the sales team assigned to the object . o You're a member of the partner team assigned to the object.

Object Access in a Multiple Business Unit Environment

In a multiple business unit environment, access to objects and data is influenced by the business unit the user belongs to. In this type of implementation, access to transactional data for objects, such as opportunities or leads, is determined in these ways:

- Sales administrators can access transactional data for all objects that are associated with the business unit or units to which the administrators are assigned.
- Sales users access to transactional data for an object is the same in multiple business unit environments and single business unit environments. So sales users can access object data across business unit boundaries provided that they have valid access to the object by means of territory or team membership, through the resource hierarchy, or by being granted full access to the object.

  But business unit assignment can indirectly affect a user's access to object transactional data. In a multiple business unit environment, business units are available as territory dimensions and can be included as part of the territory coverage definition for the assignment of transactions. A sales user gains access to object data through territory membership. If business unit is specified as a territory dimension, then the user's access to data is limited to objects which, when they were created, were assigned to the same business unit that's assigned to the user's territory team.

For additional information about using multiple business units, see the Oracle Fusion Cloud Sales Automation: Implementation Reference guide.

Related Topics

- Overview of Sales Resources and Multiple Business Units
- Associate Resource Organizations with Multiple Business Units

Configure Data Access in a Multiple Business Unit Environment

This topic provides an example of how you might configure the data access provided by a role in a sales environment where multiple business units are defined.

You can configure the default data security settings for your sales users by creating a custom version of the role users are assigned. Depending on whether you're using access groups or data security policies, you can then edit the custom role, or system access group generated for the custom role, to provide the access to object data you need.

The conditions specified in access group rules or data security policies can use a number of components as mechanisms for sharing data. So one important consideration to keep in mind when configuring users access to data is that users might have access to object records through more than one access path. For example, a user assigned a role that grants access to opportunities based on team and territory can access the opportunity through both access paths independently. If you want to limit this access, you have to remove or modify the access group rules or data security policies that provide access using either path.

For example, in a multiple business unit environment, users from different business units might be assigned to an account team. In this scenario, you might want sales representative on the account team to be able to view only opportunities they created, but not opportunities created by their team members. Here are the steps to use.

Use these steps to restrict users access to opportunities using access groups and rules.

1. Sign in to the sales application as a user who has the IT Security Manager job role.
2. Create a copy of the Sales Representative job role in the Security Console, for example Sales Representative Custom, and assign the role to at least one user.

   A custom access group, Sales Representative Custom Group, is created for the custom role but isn't associated with any predefined access group rules.

   > **Note:** System access groups are generated only for job roles that have at least one user associated to them.

3. Navigate to the Sales and Service Access Management work area **Navigator** > **Tools** > **Sales and Service Access Management**.

   The Access Groups page is displayed listing any existing active access groups.
4. Search for and select the Sales Representative Custom Group generated for the custom role you created in step 2.
5. On the Edit Access Group: Overview page, click the Object Rules tab, then select **Opportunity** from the **Object** drop-down list.
6. Click **Add Rule**.
7. Select the **Opportunity Owner** rule, click **Apply**, then click **Done**.

   This rule provides group members with access to opportunities they own. As you don't want group members to have access to opportunities through access paths other than opportunity ownership, such as through account team membership or territory membership, there's no need to assign any other rules to the group.
8. Click **Save and Close**.
9. On the Edit Access Group: Object Sharing Rules page, in the **Access Level** field select the access level for the rule you've just added, then make sure the **Enable** check box is selected to enable the rule.
10. Click **Save and Close** to save the changes you made to the access group.

11. Provision the Sales Representative Custom job role instead of the Sales Representative job role to relevant users.

    Users provisioned with the Sales Representative Custom job role are automatically added as members of the Sales Representative Custom Group access group and receive access to only those opportunities they own.

Use these steps to use to restrict users access to opportunities using data security policies.

1. Create a copy of the Sales Representative job role in the Security Console, for example Sales Representative Custom.
2. Edit the new Sales Representative Custom role.
3. Navigate to the Edit Role: Data Security Policies page of the Security Console.
4. Remove any policies defined for the opportunity object that contain conditions that provide opportunity access through access paths other than opportunity ownership, such as through account team membership or territory membership.

    - Team membership. To remove users access to opportunities created by their account team members or members of the territory associated with the account, remove all policies with this condition:

      ```
      Access the opportunity for table MOO_OPTY where you are member or in management chain of
      opportunity account team, account territory team or upward territory hierarchy
      ```

    - Territory membership. Remove users access to opportunities they can access through opportunity territory membership.

      Users might have access to opportunities through their membership of the territory associated with the opportunity. For example, user A might be an account team member and also a member of a territory (for example, the NW territory) that isn't assigned to the account. If a second user B, who is not an account team member, creates an opportunity for the account, and the opportunity is assigned to the NW territory, user A gains access to the opportunity record through territory membership. To remove this access, remove all policies that contain this condition:

      ```
      Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity
       territory team or a territory resource with a descendant territory in the opportunity territory
       team
      ```

5. Save the custom role you created and provision this role to users instead of the Sales Representative job role.

    Users assigned this role only have access to opportunities on the account that they created themselves.

For additional information about access groups, see the Access Groups chapter. For additional information about configuring data security, see the chapter Configure and Troubleshoot Data Security.

Related Topics

- Copy Job or Abstract Roles
- Overview of Access Groups
- Overview of Data Security Configuration

Data Sharing and Visibility in Incentive Compensation

The conditions specified in data security policies control visibility to record-level data associated with a schema object, such as an incentive compensation plan and a paysheet.

Conditions can use these components as mechanisms for sharing data, provided that the sharing mechanism is applicable for the object:

- Business unit
- Analyst assignment
- Person security profile

Business Unit

For incentive compensation administrators, the basis for data sharing is the business unit they have access to. Incentive compensation administrators are users assigned to these job roles:

- Incentive Compensation Manager
- Incentive Compensation Plan Administrator
- Incentive Compensation Analyst

Analyst Assignment

You have the option to further limit data access for users assigned to the Incentive Compensation Analyst role. You can limit the analyst access to the business unit or to participants who are directly assigned to the analyst. In the Setup and Maintenance work area, use the following:

- Offering: Sales
- Functional Area: Incentives
- Task: Manage Parameters

For example, analyst Amy is directly assigned to the participants Jack and Ravi. Analyst Ryan is assigned to the participants Juan and Mary. When the Manage Parameter setting indicates analyst security is by participant, Amy can't manage participant data for Juan and Mary because she isn't the assigned analyst. This functionality applies to data within the Participant Snapshot and Payments work areas.

You can assign analysts to participants when the participants are imported, using the Participant Assignments, Manage Analyst Assignments task, and using the Participant Snapshot, Participant Details task.

Person Security Profile

The predefined person security profile types can be assigned to abstract roles, such as the employee, line manager, and contingent worker roles. You can also assign the security profile to the Incentive Compensation Participant and Incentive Compensation Participant Manager abstract roles. The person security profile, view own record option provides visibility to the participant's own data. The person security profile, view manager hierarchy option provides the participant manager with visibility to participant data for the subordinates in their management hierarchy.

Data Sharing and Visibility in Service

A service application user's access to service requests is determined by the set of access group rules or data security policies associated with all the roles the user is provisioned with.

The predefined roles in the service application don't provide for service request visibility based on business unit or queue. But you can configure either queue or BU-based visibility to service requests for specific roles. Users assigned these roles can see only the service requests assigned to the business unit or queue where they're a resource member.

For more information about restricting service request visibility by business unit or by queue, see the Fusion Service: Implementing Service Center with the Classic User Experience guide.

Related Topics

- How You Set Up Visibility Based on Queue
- How You Set Up Visibility Based on BU

5 Set Up Applications Security

Overview of Applications Security Setup Tasks

If you're assigned the IT Security Manager job role, then during implementation you can prepare the application security environment by performing the tasks described in this chapter. These are some of the security setup tasks:

- Manage Applications Security Preferences

  This task opens the Administration tab of the Security Console. Select the appropriate tab of the Security Console to set enterprise-wide preferences that affect users, roles, and notifications to application users.
- Import Users and Roles into Application Security

  This task runs a process that initializes and maintains the Oracle Fusion Applications Security tables.
- Run User and Roles Synchronization Process

  This task runs a process that copies data from the LDAP directory to Oracle Fusion Applications Security tables.
- Verify your data security setup

  If you were provisioned with the sales and service application for the first time in release 22B or later, verify your data security setup in the Sales and Service Access Management work area.

Many of the security setup tasks can be run from the Users and Security functional area of the Sales offering in the Setup and Maintenance work area.

Related Topics

- Application Security Preferences
- Import Users and Roles into Applications Security
- Synchronize User and Role Information
- Verify Your Data Security Setup

Import Users and Roles into Applications Security

Before you can use the Security Console to implement security, you must initialize the Oracle Fusion Applications Security tables with existing user and role information. To do this, perform the Import Users and Roles into Application Security task.

Run the Import User and Role Application Security Data Process

Sign in as a setup user and follow these steps:

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales

- Functional Area: Users and Security
- Task: Import Users and Roles into Application Security

2. On the Import Users and Roles into Application Security page, click **Submit**.

This action starts the Import User and Role Application Security Data process. Once the process completes, you can use the Security Console.

Note: Oracle recommends that you schedule this process to run daily.

Related Topics

- Schedule the Import User and Role Application Security Data Process
- How do I update existing setup data?

Synchronize User and Role Information

Run the Retrieve Latest LDAP Changes process once during implementation to initialize the Oracle Fusion Applications tables.

User accounts for Oracle Fusion Applications users are maintained in your Lightweight Directory Access Protocol (LDAP) directory. The LDAP directory also stores information about the roles provisioned to users. During implementation, any existing information about users and their roles must be copied from the LDAP directory to the Oracle Fusion Applications tables. After that, the data is synchronized automatically. To copy this user and role information, use the task Run User and Roles Synchronization Process. This task calls the Retrieve Latest LDAP Changes process.

Run the Retrieve Latest LDAP Changes Process

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Run User and Roles Synchronization Process
2. On the process submission page for the Retrieve Latest LDAP Changes process, click **Submit**.
3. Click **OK** to close the confirmation message.

Related Topics

- How do I update existing setup data?

Application Security Preferences

There are a number of options on the Security Console that you can use to control the default behavior of functionality such as working with roles or certificates.

Some of these options can be overridden, but it's a good idea to set these options during implementation, before you start to create application users or configure your security environment.

To configure the security preferences, the initial user, or a setup user with the IT Security Manager job role, performs the task Manage Applications Security Preferences. This task opens the Administration tab of the Security Console from where you can set these default values and preferences:

- On the General subtab of the Security Console Administration tab, you can set these values:
  - Specify for how long certificates remain valid by default.

    Note: The sales and service applications don't use certificate functionality.
  - 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 can set these values:
  - 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 User Categories tab of the Security Console, you can set these values:
  - Create user categories and add users to a category.
  - Specify the default format of user names for the user category.
  - Manage the password policy for a user category.
  - Manage the notification of user and password events to users in a selected user category.
  - Create notification templates for a user category.

You can also configure security preferences by navigating directly to the Security Console (**Navigator** > **Tools** > **Security Console**). For detailed information about configuring default functionality for user names, roles and notifications, see the topics in the remainder of this chapter. For information about configuring the password policy for a user category, see the chapter Manage Passwords.

Options on the Security Console also allow you to implement location-based access, to configure a bridge between Oracle Applications Cloud and Microsoft Active Directory, and to set up single sign-on authentication. For information on these configuration tasks, see the relevant chapters in the guide.

Set the Default User Name Format

During implementation, you specify the default format of user names for users in the default user category. The default format is used to automatically generate a user name for a user if you don't specify one when creating the user.

This topic describes how to specify the default format of user names and the formats that are available.

Specify the Format of User Names

1. In the Setup and Maintenance work area, go to:

- Offering: Sales
- Functional Area: Users and Security
- Task: Manage Applications Security Preferences

The Administration page of the Security Console opens.

> **Tip:** You can navigate directly to the Security Console at any time by clicking **Security Console** from the Navigator.

2. Click the **User Categories** tab, then click the name of the default user category to open it.
3. Click **Edit** on the Details subtab.
4. In the **User Name Generation Rule** field, select one of the available user name formats.

   This table describes the available user name formats.

Format Name	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 user'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 user's last name prefixed with the initial of the user's first name. For example, the user name for John Smith is jsmith.
Person or party number	The person or party number generated by the application is the user name. For example, if John Smith's party number is 100000000178803, then the user name is 100000000178803. Because user names generated from party or person numbers can be difficult to remember you might prefer not to select this option.

5. Enable or disable the option **Generate system user name when generation rule fails**. This option controls whether a system user name is generated if the user name rule fails. For example, a user name rule will fail

if the default user name format is party number or email but these values aren't available when the user is created.

- If the option is enabled, a system user name is generated by applying these options in the following order until a unique user name is defined:
  i. Email
  ii. FirstName.LastName
  iii. If only the last name is available, then a random character is prefixed to the last name.
- If the option is disabled, then an error is raised if the user name can't be generated in the selected format.

6. Click **Save and Close**. Any changes take effect immediately.

Edit User Names

When creating users on the Create User page, you can enter user names in any format to override the default user names. You can also edit user names for individual users on the Edit User page.

Related Topics

- How do I update existing setup data?

Role Preferences

Select default role preferences for the enterprise during implementation. To set role preferences, you perform the Manage Applications Security Preferences task, which opens the General subtab of the Security Console Administration tab. From there, click the Roles subtab to display the Role Preferences page.

Copied-Role Names

It's best practice when creating roles to copy predefined roles and edit the copied versions of the 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 Role Preferences page. These are the default values:

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

For example, if you copy the Channel Account Manager job role (ORA_ZPM_CHANNEL_ACCOUNT_MANAGER_JOB), then the default name and code of the copied role are:

- Channel Account Manager Custom
- ZPM_CHANNEL_ACCOUNT_MANAGER_JOB_CUSTOM

You can supply prefix values and change the suffix values on the Role Preferences page as required. If you change these values, click **Save** and 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. If you want to display role hierarchies in graphical format by default instead, deselect the **Enable default table view** option on the Role Preferences page.

When role hierarchies appear on the Roles tab, the number of nodes can be very high. You can limit the number of nodes by setting the **Graph Node Limit** option on the Role Preferences page. When you display a role hierarchy with more nodes than the specified limit, gray arrows indicate additional nodes. You can set such a node as the focus node to see the rest of its hierarchy.

Overview of User Categories

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

Typical scenarios in which you might want to group users are:

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

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

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

Segregate Users into Categories

Create user categories and add existing users to them. All existing users are automatically assigned to the Default user category unless otherwise specified. You can 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 the Oracle Applications Cloud Sign In page. You can specify only one URL per user category.

Set User Preferences

Select the default format of the User Name, the value that identifies a user when signed in. It is generated automatically in the format you select. For additional information, see the topic Set the Default User Name Format.

Define the Password Policy

Determine the password policy for a user category. For example, specify the number of days a password remains valid or select a password format. For additional information, see the topic Password Policy.

Enable and Disable Notifications

You can enable and disable the email notifications sent to users when specific events occur. For additional information, see the topic Enable Notifications.

Related Topics

- Set the Default User Name Format
- Password Policy
- Enable Notifications
- REST API for Common Features in Oracle Applications Cloud

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 Notifications

Notifications are enabled by default, but you can disable them if required.

You can also enable or disable notifications separately for each user category. If users belonging to a specific category don't want to receive any notification, you can disable notifications for all life-cycle events. Alternatively, if users want to receive notifications only for some events, you can selectively enable the functionality for those events.

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

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

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

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

Related Topics

- Create Notification Templates
- How can I enable or disable notifications for users?

User Name and Password Notifications

Users in all user categories are notified automatically of changes to their user accounts and passwords by default. These notifications are based on notification templates.

During implementation, identify the notifications that you plan to use for each user category and disable any that aren't needed. Many templates are predefined, but you can also create templates for a user category.

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.

Notification Template	Description
Password Expiry Warning Template	Warns the user that a password is expiring soon and provides instructions for resetting the password.
Password Expiration Template	Notifies the user that a password has expired and provides instructions for resetting the password.
Forgot User Name Template	Sends the user name to a user who requested the reminder.
Password Generated Template	Notifies the user that a password has been generated automatically or manually changed, and provides instructions for resetting the password.
Password Reset Template	Sends a reset-password link to a user who requested a new password. Users can request new passwords by selecting the **Forgot Password** link on the application Sign In page, or by selecting the **Password** option on the Preferences page. To navigate to the Preferences

Notification Template	Description
	page, click your user image or name in the global header to open the **Settings and Actions** menu, then select the **Set Preferences** option.
Password Reset Confirmation Template	Notifies the user when a password has been reset.
New Account Template	Notifies a user when a user account is created and provides a reset-password link.
New Account Manager Template	Notifies the user's manager when a user account is created.

When you create a user category, it's associated automatically with the predefined notification templates, which are all enabled.

You can't edit the predefined templates but you can create new templates and disable the predefined versions. Each predefined event can be associated with only one enabled notification template at a time.

> **Note:** If you're using the sales application with Oracle Fusion Cloud Human Resources, additional notification templates are available that you can use to redirect user name and password notifications to a user's manager, if the user doesn't have a work email. For additional information, see the *Securing HCM* guide.

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 - 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

Token	Meaning	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
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.

Notifications for Users Based on Status

Security Console sends notifications to users for important events that occur in the application. However, some notifications aren't sent to users if they're inactive or have been locked out of the application.

Here's the list of notifications that are either sent or not sent to users based on their status:

Template Name	Event Name	When is the notification sent?	Sent to Inactive Users?	Sent to Locked Users?
ORA Expiring External IDP Signing Certificate	Expiring External IDP Signing Certificate	When an external identity provider certificate is about to expire	No	Yes

Template Name	Event Name	When is the notification sent?	Sent to Inactive Users?	Sent to Locked Users?
ORA Expiring Service Provider Encryption Certificate	Expiring service provider encryption certificate	When a service provider encryption certificate is about to expire	No	Yes
ORA Expiring Service Provider Signing Certificate	Expiring service provider signing certificate	When a service provider signing certificate is about to expire	No	Yes
ORA Forgot User Name	Forgot user name	When a forgot user name request is processed	No	Yes
ORA Password Expiration	Password expired	When a password has expired	No	No
ORA Password Expiry Warning	Password expiry warning	When a password expiry warning is sent	No	No
ORA Password Reset Confirmation Manager	Password reset confirmation - manager	When a password is changed and the manager must be notified	No	Yes
ORA Password Reset Confirmation	Password reset confirmation	When a password is changed	No	Yes
ORA Password Reset Manager	Password reset - manager	When a password is reset and the manager must be notified	No	Yes
ORA Password Reset	Password reset	When a password reset request is processed	No	Yes
ORA Administration Activity Request Template	Administration activity request	When an administrator initiates an administration activity	Yes	Yes
ORA Location Based Access Disabled Confirmation	Administration activity location-based access disabled confirmation	When an administrator disables location-based access through an administration activity request	Yes	Yes
ORA New Account Manager	New account created - manager	When a new account request is processed and the manager must be notified	Yes	Yes
ORA New Account	New user created	When a new account request is processed	Yes	Yes

Template Name	Event Name	When is the notification sent?	Sent to Inactive Users?	Sent to Locked Users?
ORA Password Generated	Password generated	When a password is issued	Yes	Yes
ORA Single Sign-On Disabled Confirmation	Administration activity single sign-on disabled confirmation	When an administrator disables single sign-on through an administration activity request	Yes	Yes

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 Run the Send Pending LDAP Requests Process

It's best practice 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 e-mails.

  If you include work e-mails when you create person records, then the process sends those e-mails 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.

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.

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

Related Topics

- Avoid Having Too Many Processes Run at the Same 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 Send Pending LDAP Requests 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**.

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

Related Topics

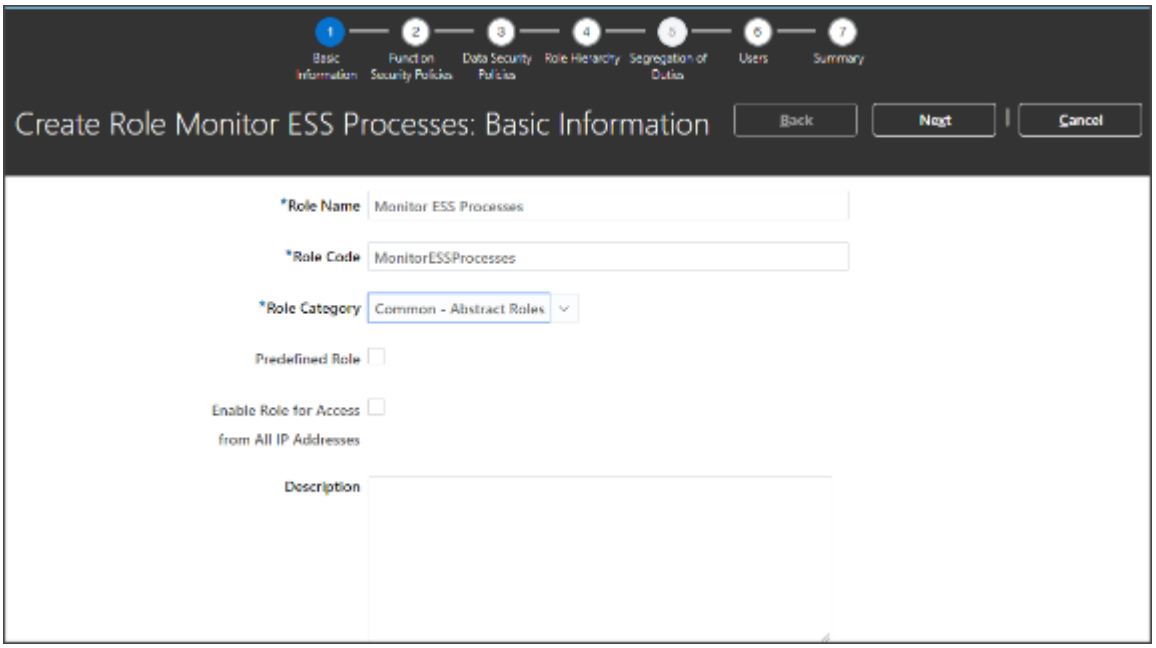
- Why You Run the Send Pending LDAP Requests Process
- Avoid Having Too Many Processes Run at the Same Time

Give Users the Permission to View All Scheduled Processes

Your application setup requires you to run numerous scheduled processes and ensure they complete successfully. By default, users can only see the scheduled processes they themselves submit. By creating a custom role in the Security Console and assigning all of the setup users to it, you ensure that everyone can see what processes are running and their status, no matter who submitted them. This setup applies to both CX Sales and Digital Sales.

1. Open the **Security Console**.
2. Click the **Roles** tab.
3. On the Roles tab, click **Create Role**.

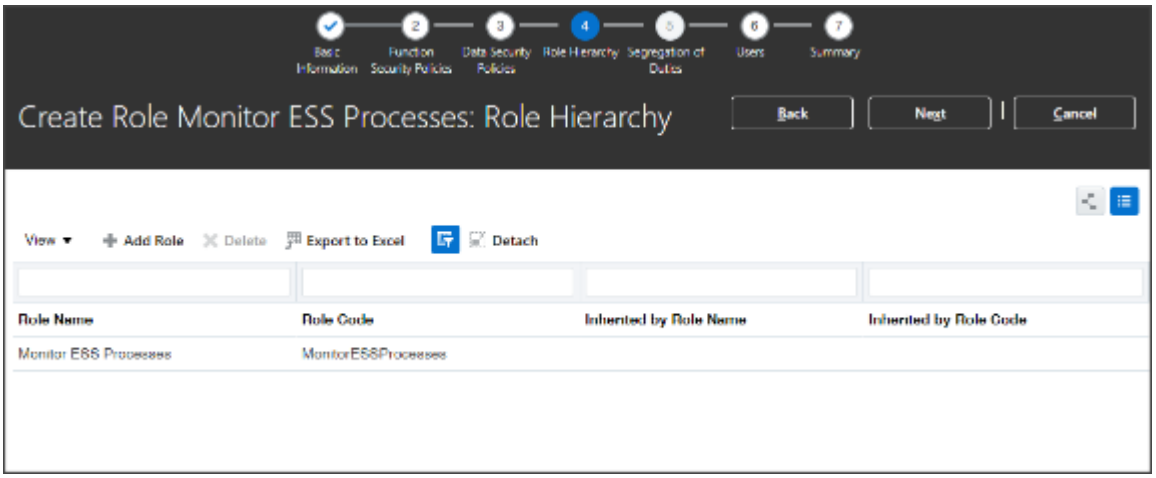
   The Create Role page displays a series of steps you can click directly or reach using the **Next** button.



4. In the Create Role: Basic Information step, make the following entries:

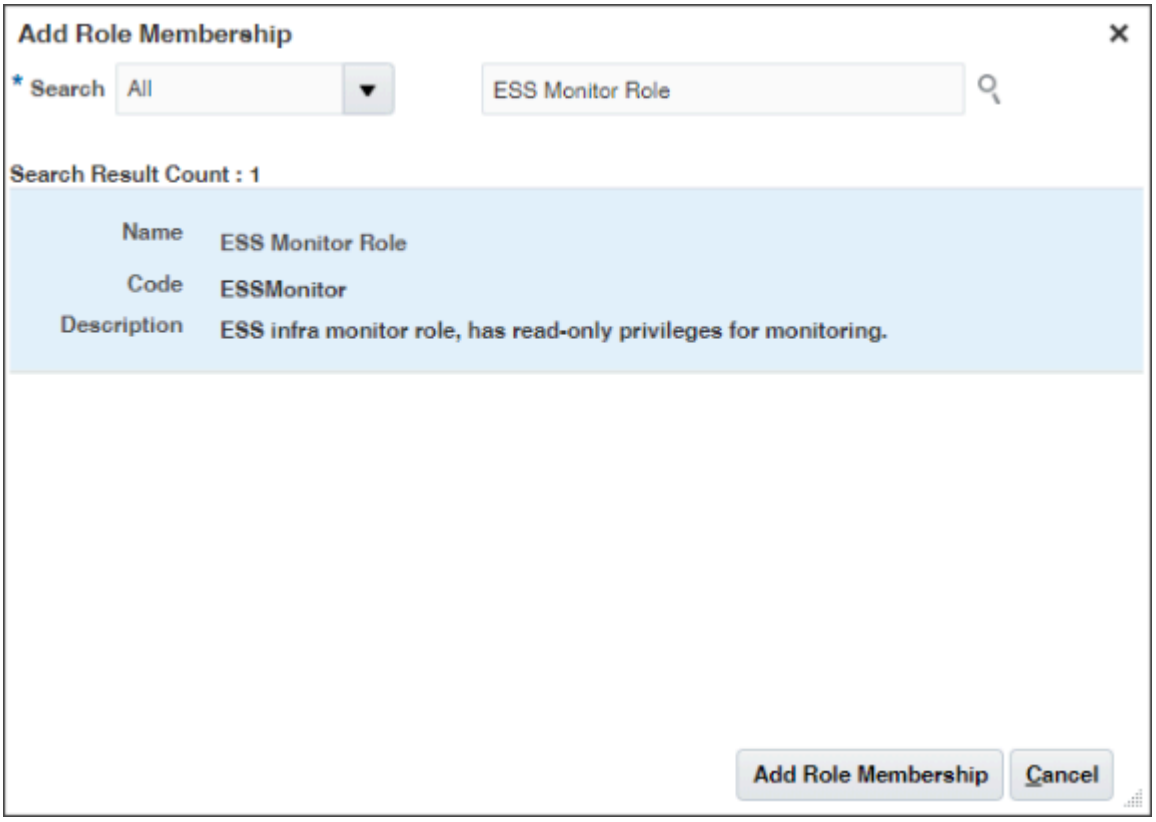
Field	Suggested Entry
Role Name	Monitor ESS Processes
Role Code	MonitorESSProcesses
Role Category	Common -Abstract Roles

5. Click the **Role Hierarchy** step.



6. Click **Add Role**.

7. In the Add Role Membership window, search for **ESS Monitor Role** and click **Add Role Membership**.



8. Click **Cancel** to close the Add Role Membership window.
9. Click the **Users** step.
10. Click **Add User** and add all of the setup users by searching for each by name and clicking **Add User to Role**.
11. Click **Cancel** when you are done.

    The Users step should list all of the users you added.
12. Click **Next** to get to the **Summary and Impact Report** step.
13. Click **Save and Close**.

    The users you added to the role can now monitor all of the scheduled processes in the **Schedule Processes** work area.

Verify Your Data Security Setup

If you're using the sales and service application for the first time in release 22B or later, verify your data security setup before provisioning users with job roles.

Starting with release 22B, users receive access to sales data through access groups and their associated rules. When you assign job roles to users, they are automatically assigned membership of an associated system access group and receive all the data permissions provided by the access group object sharing rules.

When your environment was provisioned, a process was automatically run to publish and activate all the access group object sharing rules. To make sure that your new environment is ready to use, verify that the publish process completed successfully. If it didn't, you'll need to re-run the publish process. Here are the steps to use.

> **Note:** If you set up your security environment before release 22B, you don't have to perform the steps in this procedure. Your users receive data access through data security policies, or through a combination of data security policies and access group rules if you've configured one or more access groups or object sharing rules.

1. Sign in to the sales application as a user who has the IT Security Manager job role. The initial user provided by Oracle has this job role.
2. Select **Navigator** > **Tools** > **Sales and Service Access Management**.

   The Configure Groups tab on the Sales and Service Access Management page is selected and displays the Access Groups page.
3. On the Access Groups page, click the Monitor tab.

   The Monitor page is displayed. From here, you can view all of the scheduled processes that are run to implement access group functionality.
4. Click the Publish Rules subtab and check the value of the **Status of Last Automatic Publish Process** field.
5. If the field has a value of **Succeeded**, there's nothing further to do.

   If the field has any other value, for example, **Error** or **Warning**, then run the publish process again using the steps in the topic Run the Publish Process to Setup Data Security.

Related Topics

- Overview of Access Groups

Run the Publish Process to Setup Data Security

Publish and activate access group object sharing rules in your new sales application environment using the steps in this procedure.

> **Note:** You only need to perform the steps described in this topic if the automatically generated publish process that ran when your environment was provisioned didn't complete successfully.

1. Navigate to the Scheduled Processes work area (**Navigator** > **Tools** > **Scheduled Processes**).
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 **Perform Assignment Data Publish, Refresh, and Synchronization** process, then click **OK**.
4. In the Basic Options section of the Process Details dialog box, enter these values:
   - In the **Application** field, select **Object Sharing**.
   - In the **Owner Module** field, enter **PREDEFINED_RULE_PUBLISH**.
   - Select the **Publish** check box.
5. Click **Submit**.
6. On the Overview page, click the Refresh icon to verify that the publish job completed successfully.

   Once the process completes, you can view the log files for the process or get more details about the status by selecting your process in the Search Results table and reviewing the information in the Process Details or Status Details tabs.

6 Location Based Access

Overview

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 for 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 (both Oracle and non-Oracle) 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

How many IP Addresses can I enter in the IP Address Allowlist text box?

Ensure that the number of characters of the IP Address list that you enter in the IP Addresses Allowlist text box doesn't exceed 10000 characters.

If you want to include more IP addresses beyond the 10000 characters limit, then you must enable the profile option ASE_EXTEND_LOCATION_BASED_ACCESS_CONTROL_IP_STORAGE.

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

If your organization has a huge network of computers, then you can import a .csv file containing the list of IP addresses. If the number of characters in the file doesn't exceed 10000 characters, the import is successful. If the number of characters exceed the limit, the import completes with a warning.

Do these steps:

1. In the Setup and Maintenance work area, select **All Tasks** from the **Show** drop-down list in the Initial Users section.
2. Click **Actions** for the task **Manage Applications Security Preferences**.
3. Click **Import from CSV File**, **Create New**.
4. Click **Browse** to select the file.

5. Click **Submit**.

   If the number of characters doesn't exceed 10000, the file is imported successfully. Else, the import completes with a warning.

7 Single Sign-On (SSO)

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.

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

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.

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.

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

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

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

- When an administrator requests access to the Administration Activity page to disable single sign-on
- When the single sign-on functionality is disabled
- When the external identity provider's signing certificate is about to expire
- When the service provider's signing certificate is about to expire
- When the service provider's encryption certificate is about to expire

Note: Notifications are sent to users who are assigned the **Manage SSO** privilege,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.

8 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.

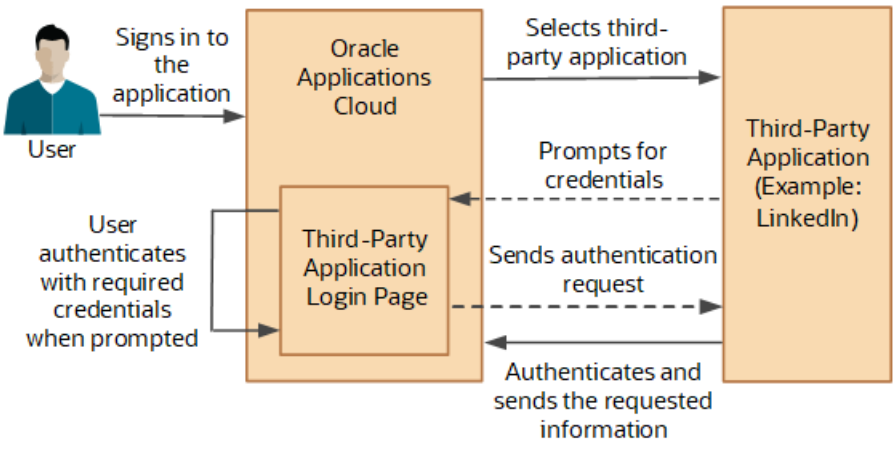
To understand the OAuth authorization protocol, let's take the example of a LinkedIn user who wants to access profile information from LinkedIn and display it in Oracle Applications Cloud. When Oracle Applications Cloud prompts for LinkedIn credentials, the user authenticates and provides the required 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

Enable OAuth Three-Legged Authentication for Creating External Client Application

While creating an external client application using the Security Console, only the JWT custom claims authentication type is available in the Select Client Type list on the External Client Application Details page.

To display the OAuth three-legged authentication type for selection, you must enable it using a profile option.

Here are the steps:

1. In the Setup and Maintenance work area, go to the **Manage Administrator Profile Values** task.

2. Search for the **ORA_ASE_ENABLE_OAUTH_THREE_LEGGED_SETUP** profile option code
3. In the Profile Values section, click the **Profile Values** list for the Site profile level and select Yes.
4. Click **Save and Close**.

The OAuth three-legged authentication type is enabled now. Enabling the profile option displays the OAuth three-legged authentication type in the Select Client Type list on the External Client Application Details page.

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.

9 Export and Import of Security Setup Data

Overview of Security Data Import and Export

Oracle provides a number of tools that let you easily move your security setup data between environments. Depending on the type of security data you want to move, different options are available as shown in the table.

Data to Move	Tools to Use	Where to Get More Details
Security Console setup data Custom roles, role hierarchies, and functional security policies	CSV file export and import options in the Setup and Maintenance work area	Review the topics in this chapter.
Functional security policies for custom objects Predefined and custom data security policies for predefined and custom objects	Configuration Set Migration (CSM)	See the chapter about moving and troubleshooting configurations in the guide Configuring and Extending Applications.
Access groups objects (access groups, group members, group membership rules, and object sharing rules)	Standard export and import management functionality	Review the section Import and Export Access Groups, Members, and Rules in the Access Groups chapter of this guide.

Related Topics

- Overview of Importing and Exporting Access Group Objects
- Tools for Moving and Troubleshooting Configurations

Export and Import of Security Console Data

You can move the Security Console setup data from one environment to another using the CSV file 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. You can now quickly replicate the same setup in another environment by exporting the setup data and then importing it into the other environment.

Export and Import the Data

Before you begin, learn how to export and import business object data using CSV files by following the instructions in the Manage Setup Using CSV File Packages chapter of the Using Functional Setup Manager guide.

To select your Security Console preference data for export or import, use the Manage Applications Security Preferences task in the Users and Security functional area of the Sales offering. Here are the steps to use:

1. Select **Navigator** > **My Enterprise** > **Setup and Maintenance**.
2. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Application Security Preferences
3. In the Tasks table, select **Columns** > **View** > **Actions** to make the applicable task actions visible.
4. From the corresponding **Actions** menu, select **Export to CSV File** or **Import from CSV file** as required.

What Gets Exported and Imported

The Security Console setup data consists of 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 the Security Console), nothing gets included in the export or 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, Role Hierarchies, and Role-to-Privilege Assignments

You can migrate your custom roles, role hierarchies, and privilege-to-role assignments from one environment to another by exporting and importing the business objects in the Users and Security functional area of the Sales offering.

Export and Import the Data

Before you begin, learn how to export and import business object data using CSV files by following the instructions in the Setup Data Export and Import chapter of the Using Functional Setup Manager guide.

To select your custom roles, role hierarchies and privilege-to-role assignments for export or import, use the Manage Job Roles task in the Users and Security functional area of the Sales offering. Here are the steps to use:

1. Select **Navigator** > **My Enterprise** > **Setup and Maintenance**.
2. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Job Roles
3. In the Tasks table, select **Columns** > **View** > **Actions** to make the applicable task actions visible.
4. From the corresponding **Actions** menu, select **Export to CSV File** or **Import from CSV file** as required.

What Gets Exported and Imported

When you migrate job roles, the following business objects are exported in the configuration package generated from the Users and Security functional area within the Sales offering.

- Functional Security Custom Roles

- Functional Security Custom Role Hierarchy
- Functional Security Custom Role Privilege Membership

Let's closely examine each business object to know what it contains.

Business Object	Information Included in Export and Import
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 irrespective of the IP address from where it's signed in. **Note:** The scope is limited to User Assignable roles only.
Functional Security Custom Role Hierarchy	The role hierarchy includes the following details: • Parent Role • Member Role • Add or Remove Role Membership
Functional Security Custom Role Privilege Membership	The role privilege membership includes the following details: • Parent Role • Member Privilege • Add or Remove Privilege Membership

What's Not Included

Data security policies that have been manually created from the security console. Access groups, rules, and memberships aren't exported or imported.

Related Topics

- Overview of Importing and Exporting Access Group Objects
- Overview of Setup Data Export and Import
- Overview of Migration
- Contents of the Migration Set

10 Sales Users and Role Provisioning

Types of Sales Users

After you have signed up with your Oracle cloud service, you receive the user name and password for one initial user. This topic describes the privileges assigned to the initial user and to each of the different types of sales user that the initial user can create.

> **Note:** The user types outlined are suggestions. The privileges granted to any user are entirely dependent on the assigned job and abstract roles so, for example, you can create a sales user who's also a setup user if you want.

Initial Users

As an initial user, you can perform many security tasks including creating other users. But you can't perform all the implementation tasks without assigning yourself additional privileges. For example, as an initial user you can submit scheduled processes but can't monitor their status.

These are the roles assigned to the initial user:

- 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.

Setup Users

You can create setup users and provision them with the same job roles as the initial user so that they can help to perform the setup tasks. Setup tasks include managing security, enterprise setup, and creating other users, including other users with the same privileges.

In order that setup users can perform all implementation tasks, then in addition to assigning them the same roles as the initial user, you must also provision them with these roles:

- Sales Analyst job role
  Makes it possible to create Sales Predictor rules.
- Sales Administrator job role
  Permits the setup user to perform the same tasks as a sales administrator, such as set up and administer sales territories and processes.
- Employee abstract role

Provides the ability to run and monitor background processes.

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

Sales Administrators

Sales administrators, like other sales application users, are created as resources and are provisioned with job and abstract roles on the basis of the resource role they're assigned. You must create at least one sales administrator user.

Sales administrators are provisioned with the Sales Administrator job role, which includes permissions to manage the import of data from legacy systems, to configure the application according to business needs, and to set up and administer the sales territories and sales processes.

Sales administrator users can view sales transactional data and reports but can't configure sales application security or perform tasks related to an enterprise setup. Sales administrator users are provisioned with these roles:

- Sales Administrator job role
- Resource abstract role
- Employee abstract role

To create sales administrators, follow the procedure outlined in the topic Creating Application Users.

Sales Application Users

You create sales application users as resources. As resources, application users can be assigned work and appear in your sales organization directory.

Sales users are provisioned with job and abstract roles according to the resource role they're assigned. The provisioned job roles don't permit sales users to perform implementation tasks, but they can perform a functional setup within the application, depending on their role. Provision sales application users with these roles:

- The job roles that they require to perform their job
- The Resource abstract role
- The Employee or the Contingent Worker abstract role, depending on the employee type of the user

Sales Restricted Users

To do their jobs effectively, users must be able to view all the data that's relevant to their role. In some cases, however, users don't require the ability to create, update, or delete that data. You can create sales application users who have extensive privileges to view sales data, but limited privileges to change data, by provisioning users with these roles:

- Sales Restricted User job role
- Resource abstract role
- Employee abstract role

Users assigned the Sales Restricted User job role can:

- View accounts, contacts, leads and opportunities.

- Create and modify reports and analytics.
- Update, create and manage service requests.
- Create, update and delete notes, tasks and activities for the Activity object.
- Edit forecasts.
- Access content in Sales Lightbox.

Assigning the Sales Restricted User job role to the following types of users provides these users with the visibility into sales data that they require, without assigning them excess privileges.

- Back office users can view reports, edit forecasts, and view activities.
- Service representatives can view customer information and can see leads and opportunities.
- Seasonal or administrative users can view leads and opportunities.

The Essential User license provides a user with a read-only subscription to Oracle CX Sales and Fusion Service. You must provision the Sales Restricted User job role to users who are assigned an Essential User license.

> **Note:** Some users may require read-only access to application data but don't need any data update privileges. For example, an auditor who reviews application data for regulatory reasons but isn't authorized to change anything. You can assign read-only access to individual users using the Read Only Mode (FND_READ_ONLY_MODE) profile option. For information on how to configure this access for a user, see the topic Provide Read-Only Access for Individual Users.

Related Topics

- How do I create sales restricted users?
- Give Users the Permission to View All Scheduled Processes
- Provide Read-Only Access for Individual Users
- How do I create application users?
- Create Setup Users

Methods of Creating Sales Users

You can create setup and sales application users in either of these ways:

- Create users individually in the Manage Users work area.
  You can navigate to this work area using the Navigator menu from any application page.
  Use this method to create setup users, and to create individual sales application users.
- Import users using the Import Management functionality or using the Quick Import Excel macros which you can download from My Oracle Support.
  Import users if you have a large number of users to create. To import users, you must understand how user attributes are represented in the application and how to map the source attributes to the attributes required by the application. You can't import setup users because the import process requires you to import sales resources. For additional information about importing users, see the following information at http://docs.oracle.com/:

- The chapter about importing users in the guide Implementing Sales
- The chapter about importing employee resources in the guide Understanding Import and Export Management for Sales and Fusion Service

Note: Don't use the Security Console for creating individual users. You must create sales users as resources who are part of the sales resource hierarchy and you can't create sales resources in the Security Console. Use the Security Console to perform the user management tasks, such as resetting user passwords and updating user email addresses, described in this guide.

Related Topics

- How do I create application users?

Tasks You Accomplish by Creating Users

When you create users, a number of other tasks are automatically performed. For example, users are sent emails with their user names and initial passwords, and the organization chart for your sales 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, sales administrators, or sales application users. These tasks are performed whether the user is created in the UI or through file import.

Task Accomplished	Comments
Notifies a user when a user account is created and provides sign-in details.	You can prevent emails 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 HCM Cloud, 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, the application 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.

Task Accomplished	Comments
Create resources that can be assigned sales work such as leads, opportunities, and tasks.	Setup users aren't resources in your application and so can't be assigned to sales teams or view reports.
Create the resource reporting hierarchy used for reporting, forecasting, and work assignments.	When you create a resource, you specify a manager for that resource and build a resource reporting hierarchy.
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 sales organization directory.
Create a hierarchy of resource organizations.	Each resource is assigned to a resource organization, and the application builds a hierarchy of these organizations based on the resource reporting hierarchy. Setup users aren't resources and so aren't assigned to resource organizations.

Resource Reporting Hierarchy

You build a resource reporting hierarchy when you create sales application users by specifying the manager of each user you create, except for the user at the top of the resource hierarchy, for example, the CEO. If you're creating users in the user interface, then you must start by creating the user at the top of the hierarchy and work your way down. If you're importing users, then the order doesn't matter provided that all of your users are in the same file.

The resource reporting hierarchy doesn't have to mirror the formal reporting hierarchy, which is captured separately in the Oracle HCM Cloud application if it has been implemented. In Oracle CX Sales and Fusion Service, you can have only one resource reporting hierarchy reporting to one person.

Resource Organizations and the Resource Organization Hierarchy

You must assign each manager that you create as a user with his or her own resource organization. All direct reports who are individual contributors inherit their manager's organization. The application automatically builds a resource organization hierarchy, using the resource reporting structure. The resource organizations remain even if managers leave. You can reassign the resource organizations to their replacements.

In CX Sales and Fusion Service, resource organizations serve a limited purpose. The name of each resource organization appears in the application's Resource Directory, which users can access to obtain information about their coworkers, and in social media interactions. However, resource organizations aren't used in application security or for work assignments. You assign work to individuals rather than their organizations.

You access the Resource Directory from the **Navigator** menu. The resource organization names appear under each person's title. The resource organization names don't have to reflect the names of departments. Departments are tracked along with employee records in the Oracle HCM Cloud application if it has been implemented.

Related Topics

- How do I create application users?

Role Provisioning

This topic describes how role provisioning is implemented in the sales application.

About Provisioning Roles to Users

Sales 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. You can provision both custom and standard job roles using role provisioning rules. 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

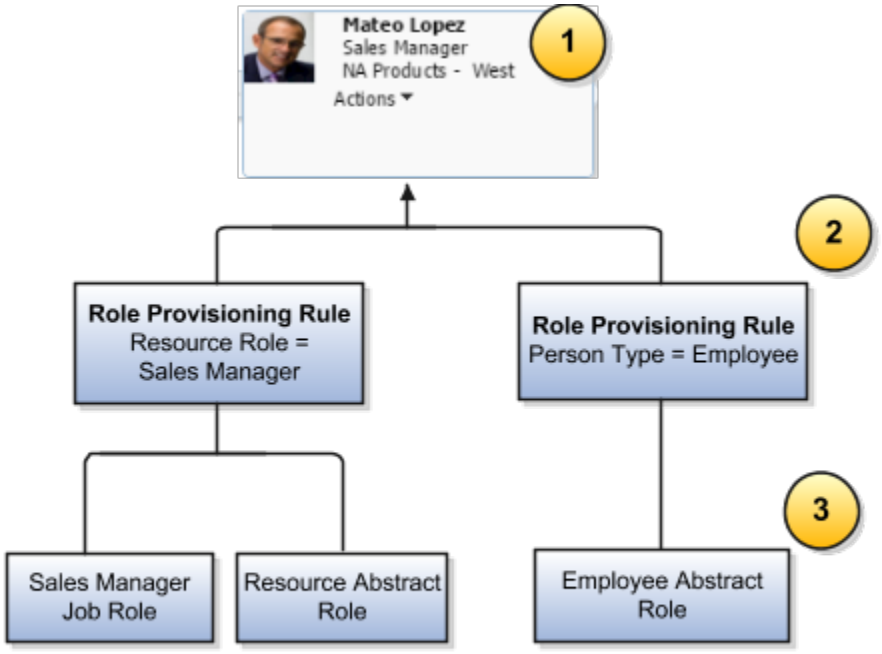
The provisioning rules use resource roles as the condition for provisioning job and abstract roles to sales users. Each provisioning rule can use one resource role and you assign a resource role to each sales user you create.

> **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.

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 or using the Sales User Quick Import Excel macro.

The following figure provides an example of how role provisioning rules work. When you create the Sales Manager user, you assign that user the Sales Manager resource role provided by Oracle (callout 1), which is the user's title in the organization. You also create the user as an employee person type. The role provisioning rules use the resource role and person type values as conditions. When you create a user as an employee with the sales manager resource role, then the conditions are true and the rules automatically assign the

user with the Sales Manager job role and the Resource abstract role, and with the Employee abstract role.



Sales Resource Roles Provided by Oracle

Oracle provides you with the following standard sales organization resource roles and the appropriate job roles for each:

- Channel Account Manager
- Channel Operations Manager
- Channel Sales Manager
- Chief Executive Officer
- Contract Administrator
- Contract Manager
- Customer Data Steward
- CX Inside Sales Manager
- CX Inside Sales Representative
- Data Steward Manager
- Partner Administrator
- Partner Sales Manager
- Partner Salesperson
- Sales Administrator
- Sales Lead Qualifier
- Sales Manager
- Salesperson
- Sales Restricted User

- Sales Setup User
- Sales Vice President

Sales Role-Provisioning Rules Provided by Oracle

Oracle provides role provisioning rules for provisioning most of the standard sales job roles to users. Oracle also provides rules to assign the Employee abstract role to all active users who are created as employees, and the Contingent Worker abstract role to active non-employee users who are created as contingent workers.

The role provisioning rules Oracle provides are created automatically when you set up your company information using the Create Company Information quick setup task. You perform this step after enabling your Sales or Service offering. If you set up the company information in a different way, perhaps because you're implementing a number of cloud services at the same time, then you must create the provisioning rules yourself using the steps outlined in the topic Create Rules to Automatically Provision Job Roles to Sales Users. For information about setting up your company information, see the Implementing Sales guide.

The following table lists the role provisioning rules provided by Oracle, the condition that triggers the provisioning, and the job and abstract roles the rule provisions. With the exception of the partner provisioning rules, each rule uses two rule conditions to provision the relevant roles to a user:

- Resource Role or Person Type

  The Resource Role or Person Type condition specifies the job and abstract roles assigned to users.
- HR Assignment Status

  The HR Assignment Status condition ensures that the provisioned job roles are automatically removed if the user is terminated.

  The HR Assignment Status condition isn't applicable to partner users who are created as external sales users. As a result, the partner provisioning rules specify only one condition, Resource Role.

The Requestable, Self-Requestable, and Autoprovision options are enabled for each role assigned by the provisioning rules.

Provisioning Rule Name	Condition	Job or Abstract Roles Provisioned
Channel Account Manager	HR Assignment Status is Active Resource Role is Channel Account Manager	Channel Account Manager Resource
Channel Sales Manager	HR Assignment Status is Active Resource Role is Channel Sales Manager	Channel Sales Manager Resource
Channel Operations Manager	HR Assignment Status is Active Resource Role is Channel Operations Manager	Channel Operations Manager Resource
Chief Executive Officer	HR Assignment Status is Active Resource Role is Chief Executive Officer	Sales VP Resource

Provisioning Rule Name	Condition	Job or Abstract Roles Provisioned
Contract Administrator	HR Assignment Status is Active Resource Role is Contract Administrator	Contract Administrator Resource
Contract Manager	HR Assignment Status is Active Resource Role is Contract Manager	Contract Manager Resource
Customer Data Steward	HR Assignment Status is Active Resource Role is Customer Data Steward	Customer Data Steward Resource
Data Steward Manager	HR Assignment Status is Active Resource Role is Data Steward Manager	Data Steward Manager Resource
Inside Sales Manager	HR Assignment Status is Active Resource Role is CX Inside Sales Manager	Inside Sales Manager Resource
Inside Sales Representative	HR Assignment Status is Active Resource Role is CX Inside Sales Representative	Inside Sales Representative Resource
Partner Administrator	Resource Role is Partner Administrator	Partner Administrator
Partner Sales Manager	Resource Role is Partner Sales Manager	Partner Sales Manager
Partner Sales Representative	Resource Role is Partner Salesperson	Partner Sales Representative
Sales Administrator	HR Assignment Status is Active Resource Role is Sales Administrator	Sales Administrator Resource
Sales Lead Qualifier	HR Assignment Status is Active Resource Role is Sales Lead Qualifier	Sales Lead Qualifier Resource
Sales Manager	HR Assignment Status is Active Resource Role is Sales Manager	Sales Manager Resource
Sales Representative	HR Assignment Status is Active Resource Role is Salesperson	Sales Representative Resource
Sales Restricted User	HR Assignment Status is Active Resource Role is Sales Restricted User	Sales Restricted User Resource

Provisioning Rule Name	Condition	Job or Abstract Roles Provisioned
Sales Setup User	HR Assignment Status is Active Resource Role is Sales Setup User	Application Implementation Consultant IT Security Manager Application Diagnostics Administrator Sales Administrator Sales Analyst
Sales Vice President	HR Assignment Status is Active Resource Role is Sales Vice President	Sales VP Resource
Contingent Worker	HR Assignment Status is Active System Person Type is Contingent Worker	Contingent Worker
Employee	HR Assignment Status is Active System Person Type is Employee	Employee

Resource Roles and Provisioning Rules for Digital Sales Access

When you assign these four resource roles to resources, the role provisioning-rules created automatically by the Setup Assistant provide access to the Digital Sales UIs.

- CX Inside Sales Representative
- CX Inside Sales Manager
- Sales VP
- Sales Administrator

The job roles provisioned by the Sales VP and Sales Administrator provisioning rules provide access to the CX Sales UIs as well as the Digital Sales UIs. Before creating users, edit the Inside Sales Manager and Inside Sales Representative provisioning rules so that they also provide access to the CX Sales UIs. For information on how to do this, see the topic Modify the Provisioning Rules for Digital Sales.

Resource Roles and Provisioning Rules for Service

Oracle provides resource roles for the Service offering which are used to provision the standard service job roles. Oracle also provides the role provisioning rules for these resource roles so that service users are automatically assigned the job and abstract roles they need.

These are the service role provisioning rules provided by Oracle, the condition that triggers the provisioning, and the job and abstract roles each rule provisions.

Provisioning Rule Name	Condition	Job or Abstract Roles Provisioned
Service Vice President	HR Assignment is Active Resource Role is Service Vice President	Customer Service Manager Resource
Service Administrator	HR Assignment is Active Resource Role is Service Administrator	Customer Relationship Management Application Administrator Resource
Service Manager	HR Assignment is Active Resource Role is Service Manager	Customer Service Manager Resource
Service Representative	HR Assignment is Active Resource Role is Service Representative	Customer Service Representative Resource

Note: If you didn't use the Create Company Information quick setup task to set up your company information, then the predefined role provisioning rules aren't created; you must create the provisioning rules yourself. For information about creating provisioning rules, see the topic Create Rules to Automatically Provision Job Roles to Sales Users.

Related Topics

- Modify the Provisioning Rules for Digital Sales
- Create Rules to Automatically Provision Job Roles to Sales Users

Steps for Setting Up Role Provisioning

Before you create sales users, there are some role provisioning setup tasks you might have to perform, 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. Resource role and job role names are the same except for the Salesperson resource role, which provisions the Sales Representative job role, and the Chief Executive Officer resource role, which provisions the Sales Vice President job role. Review the predefined resource roles provided with the application 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 are creating users with job roles that aren't provided by Oracle, or your organization uses different job titles. For example, you must create a Digital Marketing Manager resource role if you want to include the Digital Marketing Manager 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 example, if one of the sales managers in the organization is also in charge of maintaining territories and sales processes, then you create a new resource role that you can provision with both the Sales Manager and the Sales Administrator job roles.

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

Create Additional Role Provisioning Rules

Predefined role provisioning rules are created automatically when you set up your company information using the Create Company Information quick setup task. A role provisioning rule is provided for the standard resource roles included with the application but you must create provisioning rules for any additional resource roles you create.

When you're creating provisioning rules for users who are sales 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 provisioning rules, see the topic Create Rules to Automatically Provision Job Roles to Sales Users.

> **Note:** If you didn't use the Create Company Information quick setup task to set up your company information, then the predefined role provisioning rules aren't created; you have to create the provisioning rules yourself. For information about the predefined provisioning rules, see the topic Role Provisioning. For information about setting up your company information, see the Implementing Sales guide.

Modify Predefined Provisioning Rules

You might have to edit the predefined role provisioning rules in these circumstances:

- If you create custom roles based on the predefined roles, you'll also need to edit the predefined provisioning rules for those roles.

  For example, it's recommended that you use a custom version of the Employee abstract role to avoid unnecessary licensing charges. This means that you'll also need to edit the predefined rule that provisions the Employee role so it provisions the custom role instead. For additional information, see the topic How to Configure the Employee Abstract Role for Sales Users.
- If a predefined provisioning rule doesn't provision all the roles you want to assign to users.

  For example, the Inside Sales Representative and Inside Sales Manager provisioning rules provision users with the roles they need to use the Digital Sales UIs but not with the roles they need to access the CX Sales UIs. Edit these provisioning rules so that they provide users with access to both UIs. For information, see the topic Modify the Provisioning Rules for Digital Sales.

Related Topics

- Role Provisioning
- How to Configure the Employee Abstract Role for Sales Users
- Modify the Provisioning Rules for Digital Sales
- Create Rules to Automatically Provision Job Roles to Sales Users

11 Get Ready to Create Sales Users

What You Must Do Before Creating Sales Users

This topic describes the preliminary tasks you need to do before you start creating sales users.

When you create sales users, either in the UI or by importing them from a file, you not only provision the permissions the sales users need to do their jobs, but you also build the organization chart for your sales organization. This means that you must set up any additional role provisioning rules you require, as well as the elements that the application uses to create the organization chart in the Resource Directory, such as the root of the organization chart, and the names of the roles the resources play in the organization.

You're getting ready to create two types of sales users:

- Sales team members without any sales application administration duties. These include salespeople, sales managers, and sales vice presidents.
- At least one sales administrator user who will set up and administer the sales territories and sales processes.

Setup Overview

Before creating sales users, make sure that you have completed the following tasks:

1. Create any additional resource roles you need.

   You must assign a resource role, a name describing the role each resource plays in the organization, to each sales user you create. The resource roles display underneath user names in the resource directory and elsewhere in the UI. You also use the resource roles as conditions in your provisioning rules.

   For information about creating resource roles, see the topic Create Additional Resource Roles.
2. Create a resource organization for each of the manager users you create, including the top manager in your hierarchy.

   You can use the Manage Internal Resource Organizations task to create each resource organization. For details, see the topic Create a Resource Organization. Alternatively, you can create each resource organization as you create each manager user in the UI or when you import the user. Individual contributors who aren't managers inherit the organization assigned to their managers.

   As you create users, the application creates an organization hierarchy that you can use to browse through the sales organization's resource directory.
3. You can explicitly designate the resource organization you create for the top manager in your organization as the top of your organization tree by using the Manage Resource Organization Hierarchies task. For details, see the topic Designate an Organization as the Top of the Sales Hierarchy.

   If you don't 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.
4. Decide what job roles you want to assign to your users and determine whether or not you need to create any custom roles. For example, it's recommended that you provision sales users with a custom version of the Employee abstract role. For information, see the topic How to Configure the Employee Abstract Role for Sales Users.

Remember that you aren't restricted to assigning one job role to a user. For example, you might want to provision the sales manager in charge of determining sales territories and sales processes with the Sales Administrator job role in addition to the Sales Manager job role. Assigning both job roles allows this resource to perform the required sales setups.

You must create at least one user with the Sales Administrator job role to perform these setups.

5. If you created additional resource roles, then create the provisioning rules to automatically provision the appropriate job roles and abstract roles to users who are assigned those resource roles. You must create a provisioning rule for every resource role you use.

   For information about creating provisioning rules, see the topic Create Rules to Automatically Provision Job Roles to Sales Users.
6. Enable duplicate checking for the email addresses you enter while creating users in the UI.
7. When you create users, the application sends emails with the sign-in credentials to the new users unless you disable notifications. You can configure this behavior as described in the topic User-Name and Password Notifications.

How Setup Assistant Gets You Ready to Create Sales Users

If you used Setup Assistant to help you complete the initial implementation of the Sales offering, then some of the tasks described in the previous section are already completed for you. Here are some of the things Setup Assistant does:

- Creates the role-provisioning rules for the standard resource roles provided by Oracle.
- Creates additional resource roles. All you do is enter their names.
- Creates the role-provisioning rules to provision the job and abstract roles you specify for those additional resource roles.
- Creates the user at the top of the resource organization, and the name of the resource organization, if you enter these values.
- Prevents you from accidentally entering duplicate email addresses for users by setting the system profile option Enable Validation of User Work Email.

For information about the Setup Assistant, see the Implementing Sales guide.

Create a Resource Organization

Create a resource organization for every manager in your sales 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 you're creating manager users in the UI or when you import 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

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales

- Functional Area: Users and Security
- Task: Manage Internal Resource Organizations

2. On the Manage Internal Resource Organizations page, click the **Create** icon.

   The Create Organization: Select Creation Method page is displayed.
3. Select **Option 2: Create New Organization**, then click **Next**.
4. Enter the name of the resource organization in the **Name** field, for example, **Vision Corp**. This name is shown in the resource directory.

   Here are a few things to keep in mind when naming resource organizations:

   - Each resource organization name 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.
5. In the Organization Usages region, click the **Add** icon and select **Sales Organization**.
6. Click **Finish**.

   If you need to change the name of a resource organization at a later date, you can do so using the Manage Internal Resource Organizations task. For details, see the FAQ in this chapter: How can I change the name of the top resource organization and other resource organizations?

Related Topics

- How can I change the name of the top resource organization and other resource organizations?
- How do I update existing setup data?

Designate an Organization as the Top of the Sales Hierarchy

After you create the resource organization for the top person in the sales organization hierarchy, for example, the CEO, you can designate that resource organization as the top organization in the sales hierarchy.

If you don't explicitly designate 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 Sales Hierarchy

Here are the steps to designate a resource organization as the top of the sales hierarchy:

1. In the Setup and Maintenance work area, go to the following:

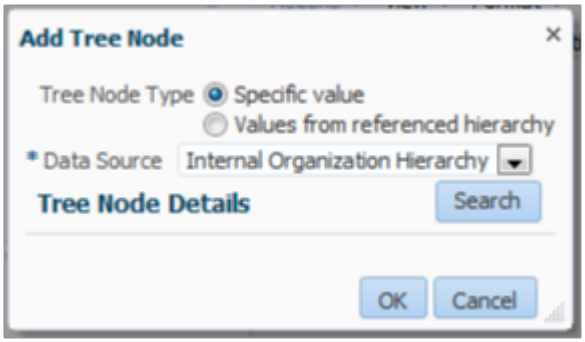
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage Resource Organization Hierarchies

2. On the Manage Resource Organization Hierarchies page, click **Search**.
3. 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.
4. From the **Action** menu, select **Edit This Hierarchy Version**.

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

   The Add Tree Node window appears.



6. Click **Search**.

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

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

Related Topics

- How do I update existing setup data?

Prevent Entry of Duplicate User Email Addresses

You can prevent the entry of duplicate email addresses when creating or editing users on the Create User or Edit User pages by enabling email validation.

When validation is enabled, a warning message is displayed listing the owner of the email address if you enter a duplicate value. Having this warning gives you the opportunity to enter a unique email before saving the user's record. Email validation on the Create User and Edit User pages is disabled by default. Follow the steps in this topic to enable validation.

Note: User import includes its own separate duplicate checking which is enabled by default.

Set the Profile Option

To enable email validation, you set the profile option PER_MANAGE_USERS_EMAIL_VALIDATION.

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Sales Foundation
    - Task: Manage Administrator Profile Values
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 email validation is enabled, it applies to the Create User and Edit User pages. It doesn't apply to user accounts that you manage on the Security Console.

Create Additional Resource Roles

Use these steps to review the resource roles provided by Oracle and to create any additional resource roles you need.

Remember that the resource role is only a title. So, if you create a resource role, you must also create the provisioning rule to go with it.

Create a Resource Role

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Resource Roles
2. On the Manage Resource Roles page, review the existing resource roles by clicking **Search** without entering any search criteria.
   All the available resource roles are listed. Roles that are predefined by Oracle are labeled **System**.
3. To create a new resource role, click **Create**.
   The Create Role page appears.
4. In the **Role Name** field, enter the name of the resource role as you want it to appear in the application UI, for example, `Digital Sales Manager`.
5. In the **Role Code** field, enter a unique internal name in capital letters. No spaces are permitted but you can use the underscore character instead. For example, enter `DIGITAL_SALES_MANAGER`. If you're importing users from a file then you must include this code in your file rather than the name.
6. If the resource role belongs to a manager, select the **Manager** option. If the resource role belongs to an individual contributor, select the **Member** option.
7. From the **Role Type** list, select **Sales** to classify the role that you're creating.
8. Click **Save and Close**.

Related Topics

- How do I update existing setup data?

Create Rules to Automatically Provision Job Roles to Sales Users

Before you create sales users, review the predefined role provisioning rules used to automatically assign job and abstract roles to users, and create any additional rules you need.

For example, you might want to create a new resource role and rule to provision a custom job role you've created.

Oracle provides a role provisioning rule for each of the standard resource roles included with the application but you have to create role provisioning rules for any new resource roles you create. The provisioning rules use the resource role that you assign to each sales user as the trigger condition for provisioning job roles.

For all internal sales users, including sales 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. Don't add the Resource abstract role for partner roles.

> **Note:** The role provisioning rules Oracle provides are created automatically when you set up your company information using the Create Company Information quick setup task. If you didn't use the Create Company Information quick setup task, then you must create all of these role-provisioning rules manually. For information about the predefined provisioning rules, see the topic Role Provisioning. For information about setting up your company information, see the Implementing Sales guide.

Use these steps to review existing provisioning rules, and to create new rules:

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
2. On the Manage Role Mappings page, if you want to review existing 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.
    b. Click **Search**.

       If a role provisioning rule exists for the resource role (either a predefined rule or a rule you created), it's 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.
3. To create a new provisioning rule, on the Manage Role Mappings page, click **Create**.

   The Create Role Mapping page appears.

4. In the **Mapping Name** field, enter a name that identifies the mapping. For example, if you're creating a rule to provision a resource role you created called Digital Sales Manager, enter `Digital Sales Manager` for the mapping name too.
5. In the Conditions region, enter these conditions:

Field	Entry
Resource Role	Select the resource role you want to provision. For example, select **Digital Sales Manager**.
HR Assignment Status	Select **Active**. This additional condition ensures that the provisioned roles are automatically removed if the user is terminated in Global Human Resources.

6. In the Associated Roles region, click **Add** to add the job roles you want to provision.

   For the Digital Sales Manager, for example, you might add the **Sales Manager** job role.

   For internal sales users, add the **Resource** abstract role. Don't add this role for partner roles.
7. Select one or more of the role-provisioning options shown in the table for each role you've added.

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 are users who satisfy the rule conditions.

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

8. Click **Save and Close**.
9. Run the scheduled process Autoprovision Roles for All Users after creating or editing role mappings. This process compares all current user role assignments with all current role mappings and creates appropriate autoprovisioning requests.

Related Topics

- Role Provisioning
- Role Provisioning Options
- Role Autoprovisioning
- How do I update existing setup data?

How to Configure the Employee Abstract Role for Sales Users

The Employee abstract role is assigned to all sales users who are employees but many of the privileges it provides aren't required if you've implemented only CX Sales.

Although these privileges aren't used, they can incur licensing charges. For this reason, Oracle recommends that you create a custom version of the Employee role that doesn't include these unnecessary privileges and provision the custom role to your sales users. This task involves these steps.

- Copy the predefined Employee role to create a custom version of the role.

  See the topic: *Create a Custom Employee Role for Sales Users*.
- Edit the custom employee role to remove unnecessary privileges.

  See the topic: *How do I remove unneeded privileges from my custom employee abstract role?*.
- Edit the predefined Employee provisioning rule so that it assigns the custom employee role instead of the predefined Employee role to all users created as employees.

  Test the changes you've made to the rule and then implement it for all your users. See the topic: *Provision the Custom Employee Role to Users*.

Create a Custom Employee Role for Sales Users

Create a custom employee abstract role that contains only the privileges sales users require using these steps.

1. Sign in to the sales application as a user who has the IT Security Manager job role.
2. Navigate to the Security Console (**Navigator** > **Tools** > **Security Console**).
3. On the Roles tab, search for and select the Employee abstract role (ORA_PER_EMPLOYEE_ABSTRACT).
4. In the search results, select **Copy Role** from the **Actions** menu of the Employee role.
5. In the Copy Options dialog box, select the **Copy top role and inherited roles** option, then click **Copy Role**.

   > **Note:** When you select the **Copy top role and inherited roles** option, you copy not only the role you've selected, but also all of the roles in its hierarchy. When inherited duty roles are copied, you can edit them without affecting other roles in the source role hierarchy.

6. On the Copy Role: Basic Information page, review and edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

   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, but you can overwrite these values for the role that you're copying. For example, you might want to name the role **Employee Custom Sales**. Any roles inherited by the copied role are unaffected by any name changes that you make here.

7. Click **Next**.
8. Click the Summary train stop.
9. On the Summary page, click **Submit and Close**, then click **OK** to close the confirmation message.

10. Review the progress of your role copy operation on the Role Copy Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

How do I remove unneeded privileges from my custom employee abstract role?

By default, some privileges are assigned to the Employee abstract role that aren't used by Sales users. You can delete these privileges from the custom employee role you previously created.

To delete privileges that are assigned directly to the custom employee role, edit the custom employee role you created. If a privilege is inherited from a duty in the custom employee role hierarchy, you've to edit the custom duty role to remove the privilege.

1. On the Roles tab of the Security Console, search for and select the custom employee role you've just created, for example, **Employee Custom Sales**.
2. In the search results, select the **Edit Role** option from the **Actions** menu of the Employee Custom Sales role.
3. Click **Next**.

   On the Edit Role: Function Security Policies page, all the privileges assigned directly to the Employee Custom Sales role are listed.
4. To display the privileges the custom employee role inherits from duty roles in its hierarchy, scroll to the end of the page, then click **Load Inherited Policies**.

   All the privileges the custom employee role has are now listed:
   - If the **Inherited from Role** column is blank for a privilege, the privilege is assigned directly to the employee custom role and can be deleted on this page.
   - If the **Inherited from Role** column isn't blank, you have to edit the custom duty role listed to delete a privilege from it.
5. Delete the privileges that are assigned directly to the Employee Custom Sales role that aren't required for sales users.
   a. Delete the following privileges by selecting each privilege in turn, then clicking **Delete**.
      - Manage Reputation Scores (HWR_REPUTATION_EE_PRIV)
      - Manage Social Roles (HWR_SOCIAL_ROLES_EE_PRIV)

   b. Click **Yes** in the Warning dialog box to confirm the deletion.

   c. Click the Summary train stop.

   d. On the Edit Role: Summary page, verify both privileges you deleted are listed as Removed in the Function Security Policies row, click **Save and Close**, then click **OK**.
6. Now delete the excess privileges that are inherited by the Employee Custom Sales role from duty roles in its hierarchy.
   a. On the Roles tab of the Security Console, edit each duty role shown in the table and remove the privilege listed.

   > **Note:** The default prefix and suffix for copied roles is specified on the Roles subtab of the Security Console Administration tab. By default, the role-name suffix is Custom but this might differ in your environment.

Privilege to Remove	Custom Duty Role to Edit
Manage Expense Report	Expense Entry Custom

Privilege to Remove	Custom Duty Role to Edit
Create Performance Document by Worker	Performance Management Worker Custom
Provide Performance Evaluation Feedback	Performance Management Worker Custom
View Performance Information on Worker Dashboard	Performance Management Worker Custom
Access Time Work Area	Time and Labor Worker Custom
Manage Requisition	Requisition Self Service User Custom
Access Learning Common Components	Access Learning Common Components Custom

   b. Once you've deleted each privilege, review your changes to the custom duty role on the Edit Role Summary page and save them.

7. Finally, edit the Employee Custom Sales role on the Security Console.

   Navigate to the Function Security Policies page and verify that all the excess privileges, both those assigned directly to the role and those inherited from other roles in the hierarchy, have been removed.

Provision the Custom Employee Role to Users

Modify the predefined provisioning rule for the Employee abstract role so that it assigns users the custom employee role you created instead of the predefined Employee role. Test your configuration for an individual user, then apply the change to all users.

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage HCM Role Provisioning Rules
2. On the Role Mappings page, enter **Employee** in the **Mapping Name** field, then click **Search**.
3. In the Search Results area, click the **Employee** mapping.
4. On the Edit Role Mapping: Employee page, make the following change in the Associated Roles region:
   a. Select the Employee row, then click the Remove icon to remove the predefined Employee role.
   b. Click the Add Row icon to add a new row.
   c. In the **Role Name** field, search for your custom employee abstract role, for example, **Employee Custom Sales**, then add the role.
   d. Select the **Autoprovision** option for the role.
   e. Click **Save and Close**, then click **OK**.
5. Click **Done** on the Role Mappings page.

6. Test that the role provisioning rule updates are working correctly for a single employee user:
    a. Open the Search Person page (**Navigator** > **My Team** > **Users and Roles**).
    b. Search for and select a user who was created as an employee person type.

       The Edit User page for the user opens.
    c. In the Roles region, click **Autoprovision Roles**. Any roles for which the user qualifies automatically appear in the Role Requests table with the status **Add Requested**. Your custom employee role, Employee Custom Sales, should be listed.

       > **Note:** If the Employee role was initially provisioned to a user manually rather than through automatic role provisioning, the change to the provisioning rule won't remove the original Employee role from the user.

    d. Click **Save and Close**.
7. Now navigate to the Scheduled Processes work area (**Navigator** > **Tools** > **Scheduled Processes**) and run the **Autoprovision Roles for All Users** process.

   This process compares all current user role assignments with all current role mappings and creates appropriate autoprovisioning requests. The process can take some time to complete depending on the number of users impacted.

Modify the Provisioning Rules for Digital Sales

Modify the predefined role-provisioning rules for the Inside Sales Representative and Inside Sales Manager job roles to give sales users all the permissions they need to do their work in both Digital Sales and CX Sales UIs.

Users who want to work in both the Digital Sales UIs and the CX Sales UIs must have two job roles: one to provide access to Digital Sales (Inside Sales Manager or Inside Sales Representative), and one to provide access to CX Sales (Sales Manager or Sales Representative).
The predefined Inside Sales Manager and Inside Sales Representative role provisioning rules only provision the Digital Sales job roles, but you can edit the rules so that they also provision the CX Sales roles. Here's what you have to do.

1. Sign in as a setup user or the initial user you received when you signed up with Oracle.
2. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
3. On the Role Mappings page, search for the role mapping for the CX Inside Sales Manager resource role:
    a. In the Search region, click the **Resource Role** list.
    b. Search for and select the `cx Inside Sales Manager` resource role.
    c. Click **Search**.

       The Search Results display the mappings for the CX Inside Sales Manager resource role.
4. Click the mapping name and make the following edits:
    a. On the Edit Role mapping page, in the Associated Roles region, click **Add Row** (the plus sign icon).
    b. In the new row, search for and add the **Sales Manager** job role.
    c. Select the **Autoprovision** option for the role.
    d. Click **Save and Close**.

5. Repeat step 3 for the CX Inside Sales Representative resource role.
6. Repeat step 4 to add the Sales Representative job role to the provisioning rule for the CX Inside Sales Representative resource role.
7. When you are finished, click **Done**.

Results:

Any users assigned the CX Inside Sales Manager or CX Inside Sales Representative resource roles are now automatically provisioned with both job roles they need.

Define Rules for Incentive Compensation Abstract Roles

You can define rules to assign the Incentive Compensation Participant and Incentive Compensation Participant Manager abstract roles to salespeople. You can either create new provisioning rules or modify the existing rules. In this procedure, you modify the existing rule.

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
2. In the Manage Role Mappings page search area, select the **Salesperson** resource role and click **Search**.
3. You see two Sales Representative mapping names, and you modify both. Click one of them.
4. In the Conditions region, you see the resource role is Salesperson.
5. In the Associated Roles region, the associated roles include Resource and Sales Representative. If these are also correct for your participant role, then click **Add**.
6. Search for and select the **Incentive Compensation Participant** abstract role.
7. Click **OK**.
8. Select whether you want to autoprovision the roles or have them be requested.
9. Save.

To map the Incentive Compensation Participant Manager role:

1. Search for **Sales Manager** in the Resource Role field.
2. Choose the Sales Manager role. It has the Sales Manager and Resource associated roles.
3. Click **Add**.
4. Search for and select the **Incentive Compensation Participant Manager** abstract role.
5. Click **OK**.
6. Save and close.

Role Provisioning Options

Job and abstract roles are assigned to users by defining a relationship, called a mapping or provisioning rule, between the role and some conditions. Users who satisfy the rule conditions are eligible to acquire the roles specified in the rule.

Predefined provisioning rules are provided with the application but you can also create new rules using the Manage HCM Role Provisioning Rules task in the Setup and Maintenance work area. This topic describes role mapping options for automatic and manual role provisioning.

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

Automatic Provisioning of Roles to Users

Role provisioning occurs automatically if:

- The user meets the conditions defined in the rule.
- You select the **Autoprovision** option for the role specified in the rule.

For example, to create a role provisioning rule that automatically provisions the Resource abstract role and the Sales Manager job role to users assigned a resource role, Digital Sales Manager, that you previously created, perform these steps:

1. Specify these conditions for the rule.

Field	Value
Resource Role	Digital Sales Manager
HR Assignment Status	Active

2. Specify the **Resource** abstract role and the **Sales Manager** job role for the provisioning rule, and select the **Autoprovision** option for each.

Users who match the conditions acquire the roles automatically when you either create or update the resource role or HR assignment status values for a user. 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 sales managers or administrators, can provision roles manually to other users if:

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

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

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

For example, to create a role provisioning rule to assign roles to each active employee who has been assigned a resource role, Sales Operations Manager, that you previously created, perform these steps.

1. Specify these conditions for the rule.

Field	Value
Resource Role	Sales Operations Manager

Field	Value
HR Assignment Status	Active

2. Specify these roles for the rule.

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

In this example, when you assign the Sales Operations Manager resource role to a user, the user:

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

Users keep manually provisioned roles until the user is terminated or the role is deprovisioned manually.

Role-Provisioning Rule Names

Use unique names for your provisioning rules and devise a naming scheme that shows the scope of each role mapping. For example, a provisioning rule named CEO Autoprovisioned Roles could include all roles provisioned automatically to resources assigned the CEO resource role.

Related Topics

- Role Autoprovisioning

Role Autoprovisioning

Autoprovisioning is the automatic allocation or removal of job or abstract roles to users. It occurs for individual users when you create or update the resource role assigned to a user or the user's HR assignment status.

You can also apply autoprovisioning explicitly for the enterprise using the Autoprovision Roles for All Users scheduled process. This topic explains the effects of applying autoprovisioning for the enterprise.

Roles That Autoprovisioning Affects

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

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

The Autoprovision Roles for All Users Scheduled Process

The **Autoprovision Roles for All Users** process compares the roles assigned to a user with all current role mappings.

- Users who satisfy 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.

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

It's a good idea to run **Autoprovision Roles for All Users** after creating or editing role mappings. You may also have to run it after importing new users to provision roles to the new users. 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 **Autoprovision Roles for All Users** can run at a time.

Autoprovisioning for Individual Users

You can apply autoprovisioning for individual users on the Create User or Edit User page by clicking **Autoprovision Roles** in the Roles region of the page.

Related Topics

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

Provision Roles for Testing

What's Required for Testing Configurations in the Sandbox

If you're creating configurations for a specific job role or creating your own custom objects, then you must be provisioned with additional job roles to view and test those configurations in the sandbox.

Enable the testing of both types of configurations using the steps described in this section.

What's Required for Role-Specific Configurations

If you're creating configurations for a specific job role in either Application Composer or Page Composer, then you must assign yourself that same job role to be able to test the configurations in the sandbox. For example, if you're creating your own page layout for the Sales Manager job role, then you must have the Sales Manager job role to view and test the layout. If you later create a different layout for salespeople, then you must deprovision the Sales Manager job role and provision yourself with the Sales Representative job role instead.

What's Required for the Objects You Create

If you're creating your own objects, then you must assign yourself the Custom Objects Administration (ORA_CRM_EXTN_ROLE) role. The application automatically generates this object role the first time you create an object in the application. Unless users have this role, they can't view or test the objects they create.

Setup Overview

1. While signed in as a setup user or the initial user you received when you signed up with Oracle, edit the role-provisioning rule for sales administrators and add the required job roles. Here is a summary of the steps:
    a. In the Setup and Maintenance work area, use the following:
        - Offering: Sales
        - Functional Area: Users and Security
        - Task: Manage HCM Role Provisioning Rules
    b. Search for all role-provisioning rules containing the Sales Administrator job role.
    c. For each rule, you add the job roles required for testing. Selecting the **Self-requestable** option makes it possible for individual users to assign themselves each job role when needed.
    d. If you're creating custom objects, then you must also add the Custom Objects Administration role. You must select both the **Self-requestable** and the **Autoprovision** option for this role. This object role is required for all objects you create, so you want to provision it automatically for future to sales administrators.
2. Sales administrators, who are resources with the Sales Administrator job role, navigate to the Resource Directory and assign themselves the job roles they need. Setup users, who are not resources, can edit their own user records in the Manage Users work area and assign themselves the roles there.

    For details on how resources can assign themselves job roles in the Resource Directory, see the Assign Yourself an Additional Job Role topic.

Related Topics

- Assign Yourself Additional Job Roles Required for Testing
- Enable Sales Administrators to Test Configurations in the Sandbox
- Enter Setup Data Using Assigned Tasks

Enable Sales Administrators to Test Configurations in the Sandbox

Modify the security role-provisioning rules to make it possible for administrators to assign themselves the job roles they need for testing custom configurations in the sandbox.

For viewing and testing the custom objects they create, administrators must have the Custom Objects Administration (ORA_CRM_EXTN_ROLE) role. To test job role-specific configurations, they must have the same job role. In this example, we are looking at sales administrators.

Modify the Provisioning Rule for Sales Administrators

1. Sign in as a setup user or the initial user you received when you signed up with Oracle.
2. In the Setup and Maintenance work area, use the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
3. On the Manage Role Mappings page, search for the role mapping for sales administrators:
    a. In the Search region, click the **Role Name** list and select the **Search** link.
    b. In the Search and Select window, enter `Sales Administrator` in the **Role Name** field and click **Search**.
    c. Select the role name and click **OK**.
    d. Click **Search**.
4. On the Manage Role Mapping page, click **Search**.

    The Search Results display the mappings with the Sales Administrator job role.
5. Click the mapping name of each mapping and make the following edits:
    a. In the Associated Roles region, click **Add Row** (the plus sign icon) and add the job roles required for testing.
    b. For each job role, select the **Requestable** and the **Self-requestable** options and deselect **Autoprovision**. You don't want the job roles assigned to the sales administrators automatically.
    c. If you're creating your own objects, then you must also add the Custom Objects Administration role. The application automatically generates this object role the first time you create an object. For this job role select all of the options: **Requestable**, **Self-requestable**, and **Autoprovision**. All users creating their own objects must have this role.
    d. Click **Save and Close**.
6. When you have added the job roles to all the provisioning rules, click **Done**.

Related Topics

- Assign Yourself Additional Job Roles Required for Testing
- Enter Setup Data Using Assigned Tasks

Assign Yourself Additional Job Roles Required for Testing

Administrators can use the procedure in this topic to assign themselves the roles they need to test role-specific modifications in the sandbox.

For example, if you're a sales administrator testing UI modifications for sales managers, you must assign yourself the Sales Manager job role. If you're creating your own custom objects, you must assign yourself the Custom Objects Administration role, if this role isn't already assigned to you. The Custom Objects Administration role is required for testing your objects in the sandbox.

> **Note:** You can only assign yourself job roles that are made self-requestable in the role-provisioning rules created by a setup user. A setup user has the privileges to create other users and manage application security.

1. Navigate to the **Resource Directory**.
2. Select **View Resource Details** from the **Actions** menu in your record.
3. On the Resource page, click the Roles tab.
4. Click **Add Role**.
5. In the Add Role window, search for the role you want to use for testing by name or partial name, select it, and click **OK**.

   For testing objects you created, you must add the Custom Objects Administration role.

   > **Note:** Available roles include only those that were set up as self-requestable during provisioning rule setup.

   The application returns you to the Resource page and displays the requested role in the Roles Requests region.
6. You can remove a role you no longer need for testing by selecting it and clicking **Remove**.
7. Click **Save and Close**.

   The new role becomes available for your use in a few minutes, pending the completion of a background process. The role displays in the Current Roles region the next time you navigate to this page.

FAQs for Preparing for Application Users

What happens when I autoprovision roles for a user?

The role-provisioning process reviews the user's assignments against all current role mappings. The following changes are made to the user's roles:

- The user acquires any role he or she qualifies for but doesn't have
- The user loses any role he or she no longer qualifies for

It's a good idea to autoprovision roles to individual users on the Edit User page when there are new or changed role mappings. Otherwise, no automatic updating of roles occurs until you next update the user's assignments.

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.

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.

How can I change the name of the top resource organization and other resource organizations?

You can change the name of the top resource organization or any other resource organization by editing the name using the Manage Internal Resource Organizations task.

1. In Setup and Maintenance, go to the **Manage Internal Resource Organizations** task:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Internal Resource Organizations
2. You can search for the organization by name, or select **Sales** as the **Usage** for your search.
3. Edit the organization name and save your changes.

12 Create Sales Users

User Setup Options

There are a number of different options you can use to control default functionality when users are created in the application. Review the user setup options described here and make any configuration changes you want before you start creating users.

User Name and Password Notifications

By default, users automatically receive an email notification containing their sign-in details when their user account is created. Oracle provides sample notifications but you can edit the text of the email notifications, create your own notifications, or suppress email notifications altogether.

Password Policy

During implementation, you set the password policy for the enterprise. For example, you can configure how complex passwords must be, when they expire, and when a user is notified that a password is about to expire. By default, the application requires passwords with eight letters and one number but you may want stronger passwords.

Default User Name Format

You can select the default format used to generate user names for users in cases where a user name isn't specified. Unless you specify otherwise, the default format is email address.

You can review user setup options by navigating to the Administration tab of the Security Console. For detailed information about configuring each of these options, see the chapter Setting Up Applications Security.

Related Topics

- Set the Default User Name Format
- Password Policy
- User Name and Password Notifications

How do I create application users?

You must create sales users as resources who are part of the sales resource hierarchy. You can create sales users either in the Manage Users task UI or by resource import, but you can't create resources in the Security Console.

This topic describes how to create individual sales users in the Manage Users task UI. If you have a large number of sales users to create, then importing users is useful. For additional information, see the chapter about importing sales users in the Implementing Sales guide or the chapter about importing resource data in the guide Understanding Import and Export Management for Sales and Fusion Service.

Before creating application users, make sure you have completed these tasks:

- 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's 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 directly under the top of the hierarchy and working your way down.

Steps to Create an Application User

Here's how to create sales users in the UI. The procedure is slightly different for managers and individual contributors:

- You must assign each manager with his or her own resource organization. You can create the resource organization while creating the manager.
- Individual contributors automatically inherit their managers' resource organization.

The application determines who's a manager from the resource role you assign to the user.

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

   The Create User page opens.
3. In the Personal Details region, enter the user's name and a unique email address. The application sends user notifications to this email address by default unless you disable notifications in the Security Console.

   > **Note:** After you create the user, if you want to change the email address you can do so on the Users tab of the Security Console or using file import. You can't change email addresses on the Edit User page of the Manage Users work area.

4. The application prefills today's date in the **Hire Date** field and uses that date as the start date for the resource.

   If you're planning to use quotas, then you must make sure that the hire date is a date before the start of the first quota period. For example, if you're allocating monthly quotas for fiscal year July 01, 2015 to June 30, 2016, then you must enter a hire date of 7-1-2015 or earlier. You can't change the hire date after you create the user.
5. In the User Details region, you can either create a new account or link an existing, standalone user account to the new person record you're creating.
   - When creating Sales users, create a new account. To create a new account, select the **Enter user name** option and then enter a user name. If you leave the User Name field blank, then the user name is generated automatically using the enterprise default format. Unless you specify otherwise, email address is the default user name format.
   - Alternatively, if you want to link the new person record you're creating to an existing standalone user account, select the **Link user account** option, then search for and select the user account in the **Link User Account** dialog box.
6. In the User Notification Preferences region, select the **Send user name and password** option if you want a notification to be sent to the user when you save the user record and the user account is created. The notification includes a URL users can use to reset their password and sign in.

The **Send user name and password** option is enabled only if notifications are enabled on the Security Console and an appropriate notification template exists. For example, if the predefined notification template **New Account Template** is enabled, then a notification is sent to the new user when you select the **Send user name and password** option.

If you deselect the **Send user name and password** option, a notification isn't sent when the account is created but you can choose to send the email later by running the Send User Name and Password E-Mail Notifications process. The process sends notifications to any users for whom you haven't so far requested an email. An appropriate notification template must be enabled at that time. Alternatively, you can use the Security Console to reset the password and send the notification.

7. In the Employment Information region, enter the values shown in the following table.

Field	Entry
Person Type	Select Employee.
Legal Employer	Select the legal employer Oracle created using the information you provided when you signed up with the cloud service.
Business Unit	Select the business unit for the user. Oracle creates an initial business unit using the information you provided when you signed up.

You don't have to complete the remaining fields in the Employment Information region.

8. In the Resource Information region, enter the following values.

Field	Entry
Resource Role	Select the role the user plays in the resource organization.
Reporting Manager	Select the user's manager. If you're creating the top user in your hierarchy, such as the CEO, you can leave this field blank.
Organization	If the user you're creating is a manager, and if you already created a resource organization for this manager, then select the appropriate resource organization. If you haven't created a resource organization for the manager, then you can create one by clicking the **Create** link from the end of the **Organization** list. The **Create Organization** dialog box is displayed allowing you to enter a new organization name. If the user you're creating isn't a manager, then the resource organization is automatically copied from the manager.

9. In the Roles region, click **Autoprovision Roles**.

   Any roles for which the user qualifies automatically appear in the Role Requests table with the status **Add Requested**.

   The application provisions roles according to the provisioning rules specified for the selected resource role. Each sales user must have both the Employee and the Resource abstract roles in addition to the job roles they require.
10. You can also provision a role manually to the user if required by clicking **Add Role**. The **Add Role** dialog box opens.
11. Search for and select the role. The role is added to the Role Requests table with the status **Add Requested**.

    > **Note:** Roles that you can provision to others must appear in a role mapping for which you satisfy the role-mapping conditions and where the **Requestable** option is selected for the role.

12. Click **Save and Close**.

    The application creates the user. If you selected the **Send user name and password** option, the application also sends the user the email with the URL the user can use to sign in to the application for the first time.
13. Click **Done**.

Related Topics

- Types of Sales Users
- Create a Resource Organization

How do I create sales restricted users?

You can create sales application users who have extensive privileges to view sales data, but limited privileges to create, update, or delete that data, by assigning users the Sales Restricted User job role.

For example, you might want to assign the Sales Restricted User job role to accounting or legal users, to seasonal or administrative users, or to users who are assigned an Essential User license. The Essential User license provides a user with a read-only subscription to the cloud service.

Use these steps to create a sales restricted user.

1. Create the user who's to have restricted access to the application.

   For information about this task, see the topic, *How do I create application users?*.
2. When creating the user, specify these values.

Field	Value
Person Type	Employee
Resource Role	Sales Restricted User

3. In the Roles region, click **Autoprovision Roles**.

   The user is automatically assigned the following roles:

   - Sales Restricted User job role
   - Resource abstract role
   - Employee abstract role

     A predefined rule automatically assigns the Employee abstract role to all active users who are created as employees.

Configure Administrators to Access Incentive Compensation

Use this procedure to create administrators who have access to the Incentive Compensation application.

1. Create provisioning rules that create a mapping between attributes of your person and the security role to be automatically assigned. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage HCM Role Provisioning Rules
2. On the Manage Role Mappings page, enter a name for your mapping.
3. There isn't a resource role that qualifies as an Incentive Compensation Administrator, so typically mappings use job roles. In the Conditions region, select a job role that was configured in Human Capital Management. For example, Incentive Compensation Analyst. Add any other conditions you want to use to select individuals to be assigned roles.
4. In the Associated Roles region, click **Add Row**.
5. Search for and select the role you want to assign to people who match your mapping conditions. These are the available Incentive Compensation roles:
   - Incentive Compensation Analyst
   - Incentive Compensation Plan Administrator
   - Incentive Compensation Manager
6. Save and close.
7. After users are assigned to an Incentive Compensation security role, they also need access to Incentive Compensation business units. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Incentives
   - Task: Manage Business Unit Data Access for Users
8. In the Manage Data Access for Users page, click **Create**.
9. Select a user name and role.
10. The security context must be Business Unit.

11. Select the name of the business unit in the Security Context Value field.
12. Save and close.
13. Create data access records for each role and business unit combination for this user.

13 Manage Passwords

Overview of Managing Passwords

There are a number of password management tasks you may have to perform either when you're setting up your application or on an on-going basis. Here are some examples.

Task	Where to Get More Details
Define the password policy for a user category if you don't want to implement the default policy.	See the topics Password Policy and Configure a Custom Password Policy in this chapter. For general information about user categories, see the Set Up Applications Security chapter in this guide.
Configure the email notifications sent to users when password-related events occur, such as when a user's password expires.	For information about configuring email notifications, see the Set Up Applications Security chapter in this guide.
Reset passwords for users.	See the topic Reset Passwords for Other Users in this chapter.
Enable users who are locked out of the application to sign in again.	See the topic View Locked Users and Unlock Users in this chapter.
Review password changes for your users.	To review password changes for your users in a specified period, run the User Password Changes Audit Report which is described in the User and Role Reports chapter in this guide.

Note: All users can request new passwords for themselves by selecting the Forgot Password link on the application Sign In page, or by selecting the **Password** option on the Preferences page. To navigate to the Preferences page, click your user image or name in the global header to open the **Settings and Actions** menu, then select the **Set Preferences** option.

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. • 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	Simple

Password-Policy Option	Description	Default Value
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

Password Expiry Report

The Password Expiry Report sends the password expiration warning and password expired notifications. You must schedule this report to run daily to help users know when their passwords have to be reset.

If the password expiration date set for users is in the past and if the users haven't reset the password, then this report automatically resets the password and notifies them about the change. Similarly, if the password expiration warning date set for users is in the future, then this report sends a warning notification to the users that their password is about to expire.

Here are the steps to schedule a password expiry report:

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. In the Schedule Process dialog box, search for and select the **Password Expiry Report** process.
3. Click **OK**.
4. In the Process Details dialog box, click **Advanced**.
5. On the Schedule tab, set **Run** to **Using a schedule**.
6. Select a **Frequency** value. For example, select **Daily**.

7. Select a start date and time.
8. Click **Submit**.

Configure a Custom Password Policy

Single Sign-On (SSO) configuration enforces users to use complex passwords. But, some users might want to use simpler passwords that don't enforce the use of minimum number of digits or characters. Using Security Console, you can create a custom password policy for such users.

Since password policies are linked with user categories, you can define a custom password policy for a specific user category. The policy automatically applies all users in that user category. However, there are a few conditions for creating a custom password policy. Users who use an SSO password can't use a custom password because their organization sets the SSO password policy. You can't create a custom password policy using the default Simple, Complex, and Very Complex password complexity options. You must use the Custom option and set values based on your security requirements.

1. On the Security Console, click **User Categories**.
2. Select a user category for which you want to create a custom password policy.
3. Click **Password Policy** > **Edit**.
4. Select **Custom** in the **Password Complexity** drop-down list.
5. Enter the values for all the password parameters as required.
6. Click **Save and Close**.

If you add existing users to the selected user category, then the custom password policy is enforced when they reset their password. If you want to create more custom passwords, then you must create user categories for each custom password.

Reset Passwords for Other Users

Use the Security Console to reset passwords for other users. Only setup users, and other users with the IT Security Manager job role, can access the Security Console.

> **Note:** All users can reset their own passwords by clicking their user name or image in the global header and then selecting the **Set Preferences** link in the **Settings and Actions** menu. They can also reset their passwords by using **Forgot Password** on the sign-in page.

1. Navigate to the Security Console **Navigator** > **Tools** > **Security Console**.
2. In the Security Console, click the **Users** tab.
3. On the User Accounts page, search for the user using one of these values:
    - First or last name, but not both
    - User name
4. From the **Action** menu for the user, select **Reset Password**.

   The Reset Password window is displayed showing the password strength policy.

5. If you want the application to send an email to users with a link that they can use to create their own passwords, then select the **Automatically generate password** option.
6. Use these steps to reset the password yourself:
    a. Select the **Manually change the password** option.
    b. Enter the new password twice.

    > **Note:** The option to reset a password manually is only available if you select the option **Administrator can manually reset password** on the Password Policy subtab of the User Categories page on the Security Console.

7. Click **Reset Password**.

Related Topics

- How do I update existing setup data?

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

Unlock Users

1. On the Security Console, click **Users**.
2. From the **Search** drop-down list, select **Locked Users** and click the search icon.

All the locked users are displayed.

3. Click the display name of a user to view the details.
4. Click **Edit**.
5. In the Account Information section, deselect **Locked**.
6. Click **Save and Close**.
7. Click **Done**.

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

14 User Management

Overview of Managing 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 on-going basis. Here are examples of some of the tasks you might have to do:

- Assigning different resource roles to users when they change jobs within the organization or are promoted
- 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 user management tasks using the sales application UI. But you can also use file import functionality to perform user management tasks such as:

- Making changes to employee resource information, for example, name or email address
- Enabling or disabling user accounts
- Making promotion, demotion, or transfer updates for an employee resource

For additional information, see the chapter about importing resource data in the guide Understanding Import and Export Management for Sales and Fusion Service at http://docs.oracle.com.

Change a User's Email Address

To change sales users' email addresses, use the same import process that you used to create them. You can also use REST services. This setup applies to both CX Sales and Digital Sales.

You can also use these steps to change email addresses on the Users tab in the Security Console work area. However, this method is not always foolproof:

1. Open the Security Console by clicking the **Security Console** link under the **Tools** heading in the Navigator.
2. Click the **Users** tab.
3. Search for the user using one of the following:
    - First or last name, but not both
    - User name
4. Click the user name link.
5. On the User Account Details window, click **Edit**.
6. In the Edit User Account window, edit the email address.

    > **Note:** Don't edit any of the other information available on the Edit User Account page. Use the Manage Users task instead.

7. Click **Save and Close**.

Related Topics

- What's the Security Console?

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.

Change User Names

User names are automatically generated in the enterprise default format when you create a new user if you don't manually specify a user name. The default format is the user's email address, but you can change this value.

For example, you might choose to use first name.last name as the default format. You can also manually override an individual user's existing user name, if necessary.

CAUTION: Although you can change the user name of an existing user, changing it isn't a good idea. Changing the user name requires extra setup for Oracle BI Answers. Oracle BI Answers, the embedded reporting tool for building and modifying reports, creates a separate GUID from the user name when you create a user. If you change the user name, then you must update the BI Answers GUID by running the Rename Accounts Self-Service utility. You can download the utility from My Oracle Support article Oracle Fusion BI: Self-Service Forget Accounts and Rename Accounts Tools (Doc ID 2635720.1). If you used the user name in any script, then you must update that script as well.

To change an existing user name, sign in to the application as a setup user, then perform 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 name you want to change.

The Edit User page for the user opens.
3. In the User Details region, enter the new user name in the **User Name** field.
   You can enter the user name in any format you choose.
4. Click **Save and Close**.
   The updated name is sent automatically to your LDAP directory server.
   The user's password and roles remain the same.

When you change an existing user name on the Edit User page, the user doesn't receive an automatic notification of the change. So it's a good idea to send details of the updated user name directly to the user.

How do I change user resource roles when job assignments change?

If an employee takes on a different role within the company, for example, if the employee is promoted, then you must update the resource role assigned to the employee. Changing the resource role assigned to an employee involves these steps:

- Assigning the user a new resource role that corresponds to the new assignment, for example, Sales Manager.
- Setting an end date for the old resource role, for example, Salesperson.

If the employee's new role also involves a change in the user's resource organization, for example, if the user is promoted to a management role from a non-management role, you must also change the user's organization membership.

You can make changes to role assignments using either the resource import management functionality or using the Sales UI. Although importing changes takes care of many tasks that you have to perform manually in the UI, if you're updating resource role information for an individual user, then using the UI can be more efficient.

These steps describe how to update role information in the UI for a user who's promoted from a sales representative role to a sales manager role.

1. Sign in to the application as the sales administrator or as a setup user.
2. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.
3. Search for and select the user who's being promoted. The Edit User page for the user opens.
4. In the Resource Information region, do the following:
   a. In the **Resource Role** field, add the new resource role for the user, for example, **Sales Manager**.
   b. In the **Reporting Manager** field, update the user's manager.
   c. In the **Organization** field, specify the user's resource organization.
      You must create a resource organization for every manager in your Sales organization. If you haven't created a resource organization for the new manager, then you can create one by clicking the **Create** link from the end of the Organization list. The **Create Organization** dialog box is displayed allowing you to enter a new organization name.
   d. To automatically provision any roles provided by the new resource role you just assigned the user, click the **Autoprovision Roles** button in the Resource Information section.
   e. Click **Save and Close**.
5. Set an end date for the user's old resource role using these steps:

a. Form the Navigator menu, select **Directory** > **Resource Directory**.
b. In the Tasks area of the Resource Directory page, select **View Resources**.
c. On the View Resources page, search for and select the user.

   The Resource page for the user opens.

   Note that the user is assigned the new resource organization you previously created.
d. Click the Roles tab, and in the Roles list, select the current role assigned to the user, for example, Salesperson, 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.
e. Click **Save and Close**.

Note: When you promote a user from one management position to another, for example, from a Sales Manager role to a Sales VP role, then the resource hierarchy is maintained provided that the promoted user's resource organization doesn't change. So any users who reported to the Sales Manager continue to report to the same individual when that individual is promoted to the Sales VP role. If the promoted user's resource organization does change upon the promotion, the user's reports must be reassigned to a new manager.

For information about changing role assignments using the resource import management functionality, see the topic about importing resource data in the Understanding Import and Export Management for Sales and Fusion Service guide.

Related Topics

- How do I import resource data?
- Make an Employee a Sales Resource

Terminate User Accounts

This topic describes how you can terminate a user account when an employee leaves your company. You can't delete a sales user account using the Security Console. But when an employee leaves your company, you can suspend the user account by completing these steps.

1. Do either one of these 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 CX Sales and Fusion Service. If your company also uses Oracle HCM Cloud, then a different process applies.

Note: When you deactivate a user account, the user record isn't deleted from the application. You can still view a deactivated user's record in the Manage Users work area.

Inactivating a User Account

When an employee leaves your company, 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.

These are the steps to inactivate a user account.

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.
2. On the Search Person page, search for and select the user whose account you want to inactivate. The Edit User page for the user opens.
3. In the User Details section, in the **Active** field, select **Inactive**.
4. Click **Save and Close**.

Removing 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. Navigate to the Search Person page as described in the previous task.
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.

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

These are the steps to set the end date for a user.

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Sales
   - Functional Area: Users and Security
   - Task: Manage Resources
2. On the Manage Resources page, search for and select the resource you want to edit. The Resource page for the individual opens.
3. With the Organization tab selected, select the **Edit** option from the **Actions** menu.

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

When the end date you specify for a resource arrives, this is what happens:

- The terminated employee is no longer available in the application so can no longer be newly associated with any Sales objects, such as sales account, territory, lead, and opportunity. The user's association with Sales objects made before the end date aren't automatically removed but you can remove them manually.
- Resource roles for the individual are deprovisioned.
- If the terminated individual had any reports, they're reassigned to his or her manager.

Related Topics

- How do I update existing setup data?

Impersonation and Proxy Users

Privileges Required by Proxy Users

You can use the impersonation functionality in the sales application to 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 sign in to the Partner Portal as a partner user to resolve a query relating to the UI pages or data.

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, that is, the Impersonate User privilege. The following job roles are assigned the Impersonate User privilege by default; therefore, users assigned these job roles can act as proxies for other users:

- 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 copied custom 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.

Related Topics

- Configure Impersonation Auditing
- Copy Job or Abstract Roles
- Impersonate a Partner User

Configure Impersonation Auditing

The impersonation functionality 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.

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 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 the sales application, including information about the objects that can be enabled for auditing, see the sales Implementation Reference 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. In the Setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Sales Foundation
    - Task: Manage Administrator Profile Values
2. On the Manage Administrator Profile Values page, in the Search: Profile Option section, enter **Audit Impersonation Transaction Enabled** in the **Profile Display Name** field.
3. Click **Search**.
4. In the Search Results list, select **FND_AUDIT_IMPERSONATION_TRANSACTIONS**.
5. In the FND_AUDIT_IMPERSONATION_TRANSACTIONS: Profile Values section, select the Site Profile level and set the value of the **Profile Value** field to either **Yes** or **No**.
6. Click **Save and Close**.

Related Topics

- Privileges Required by Proxy Users
- How do I update existing setup data?

Provide Read-Only Access for Individual Users

Some users may need read-only access to Oracle CX Sales and Fusion Service applications. For example:

- A service representative must replicate a user's transaction without saving any changes.
- An auditor reviews application data for regulatory reasons but isn't authorized to change anything.

Read-only access is controlled by the Read Only Mode (FND_READ_ONLY_MODE) profile option. This topic describes how to set Read Only Mode to all Oracle CX applications for specific users.

Set the Read Only Mode Profile Option

To enable read-only mode for a user:

1. In the Setup and Maintenance work area, use the **Manage Administrator Profile Values** task.
2. In the Search section of the Manage Administrator Profile Values page, enter **FND_READ_ONLY_MODE** in the **Profile Option Code** field and click **Search**.
3. In the FND_READ_ONLY_MODE: Profile Values section of the page, click the **New** icon.
4. In the new row of the profile values table:
    a. Set **Profile Level** to **User**.
    b. In the **User Name** field, search for and select the user.
    c. Set **Profile Value** to **Enabled** to activate read-only access for the selected user.
5. Click **Save and Close**.

When the user next signs in, a page banner reminds the user that read-only mode is in effect. The user can edit values in the application but can't update or save any changes they make.

FAQs for Managing Users

How are the records of a terminated employee reassigned?

After you terminate an employee in the application, the assignment process automatically excludes the terminated user when it runs again. But you must manually handle other reassignments, for example, replacing the terminated user with another user on the territory team.

For specific types of records, such as lead records or opportunity records, you can also use the Mass Transfer tool to transfer records from a terminated resource to another resource.

Related Topics

- Transfer Records Between Users
- About Transferring Records Between Users

Can I reactivate a terminated employee record?

Yes. Once you specify an end date for a resource, you can't reverse it in the application. But the former employee's record remains in the application so you can again identify that person as a resource if the person is rehired.

After identifying the person, you must assign roles and an organization again.

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.

15 User and Role Reports

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

Report Type	File Suffix	File Format	File Contents
			roles. The data security policies file is generated only when **Data Security Policies** is selected. **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 may 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.

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".

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 History Report

This topic describes the User History report, which extracts and formats the history of a specified user account. Oracle Support might 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, 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 HCM Person User Information report, which authorized users can run in the HCM Reports and Analytics work area. Information is provided in this report for sales resources who are also defined as users in HCM.

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

16 Review and Analyze Roles on the Security Console

Overview of Reviewing Roles

This chapter describes how you can use the Security Console to review and analyze role information. You perform these tasks from the Roles and Analytics tabs of the Security Console.

You can perform these tasks from the Roles tab:

- Visualize role hierarchies and role assignments to users.
- Review Navigator menus available to roles or users, identifying roles that grant access to Navigator items and the privileges required for that access.
- Compare roles.
- Copy roles, create roles, and edit custom job, abstract, and duty roles.

  For information about copying roles and creating roles, see the chapter Creating Job, Abstract, and Duty Roles.

From the Analytics tab, you can perform these tasks:

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

> **Note:** You can also use the Security Dashboard to get an overview of the security roles and how they're provisioned in your environment. For information, see the topic describing the Security Dashboard in this chapter.

Graphical and Tabular Role Visualizations

You can review role hierarchy information using either a tabular or graphical view on the Roles tab of the Security Console. This topic describes how to use each of these views.

> **Note:** The view you see by default depends on the setting of the **Enable default table view** option on the Administration tab.

Role hierarchies stretch from users at the top of the hierarchy to privileges at the bottom. In both graphical and tabular views, you can set the direction of the displayed hierarchy.

- To show from the selected user, role, or privilege up the hierarchy, set **Expand Toward** to **Users**.
- To show from the selected user, role, or privilege down the hierarchy, set **Expand Toward** to **Roles**.

The Tabular View

If the tabular view doesn't appear when you select a security artifact on the Roles tab, then you can click the **View as Table** icon. In the tabular view, you can:

- Review the complete role hierarchy for a selected user or role. The table shows roles inherited both directly and indirectly.
- Search for a security artifact by entering a search term in the column search field and pressing **Enter**.
- Set the contents of the table as follows:
  - If **Expand Toward** is set to **Privileges**, then you can set **Show** to either **Privileges** or **Roles**.
  - If **Expand Toward** is set to **Users**, then you can set **Show** to either **Roles** or **Users**.

  The resulting contents of the table depend on the start point. For example, if you select a privilege, **Expand Toward** is set to **Privileges**, and **Show** is set to **Roles**, then the table is empty.
- Export the displayed details to a Microsoft Excel spreadsheet.

The Graphical View

If the graphical view doesn't appear when you select a security artifact on the Roles tab, then you can click the **Show Graph** icon. In the graphical view, users, privileges, and the various types of roles are represented by nodes and differentiated by both color and labels. These values are defined in the **Legend**. You can:

- Review roles inherited directly by the selected role or user. To see roles and privileges inherited indirectly, select a directly inherited role, right-click, and select either **Expand** or **Expand All**. Select **Collapse** or **Collapse All** to reverse the action. Alternatively, double-click a node to expand or collapse it.
- Use the **Set as Focus** action to make any selected node the center of the visualization.
- Use the Overview icon to manipulate the visualization. For example, clicking a node in the Overview moves the node to the center of the visualization. You can also use drag and drop.
- Hover on a legend entry to highlight the corresponding nodes in the visualization. Click a legend entry to add or remove corresponding nodes in the visualization.

In the Control Panel, you can:

- Switch the layout between radial and layered representations.
- Click the **Search** icon and enter a search term to find a security artifact among currently displayed nodes.
- Zoom in and out using either the **Zoom in** and **Zoom out** icons or the mouse wheel.
- Magnify areas of the visualization by clicking the **Magnify** icon and dragging it to the area of interest. Click the icon again to switch it off.
- Click the **Zoom to Fit** icon to center the image and fill the display area.

Review Role Hierarchies

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

To review a role's hierarchy:

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 is displayed.
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. To view the privileges inherited by the role, set the **Show** field 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.
4. Click **Export to Excel** to export the current table data to Microsoft Excel.

Simulate Navigator Menus

You can simulate the Navigator for both users and roles. This feature can help you to identify how access is provided to specific work areas and tasks. You can then use this information when creating roles, for example.

Simulate the Navigator for a Role

Follow these steps:

1. On the Roles tab of the Security Console, search for the role, which can be of any type.
2. In the search results, select **Simulate Navigator** in the **Actions** menu for the role. The Simulate Navigator page opens. Icons may appear against Navigator entries. In particular:
   - The **Lock** icon indicates that the role can't access the entry.
   - The **Warning** icon indicates that the entry may not appear in the Navigator as the result of configuration, for example.

   Entries without either of these icons are available to the role.

> **Tip:** To view just the entries that the role can access, set **Show** to **Access granted**.

View Roles That Grant Access to a Navigator Entry

For any entry in the Navigator, regardless of whether it's available to the role, you can identify the roles that grant access. Follow these steps:

1. Click the entry.
2. Select **View Roles That Grant Access**.
3. In the Roles That Grant Access dialog box, review the list of roles. The roles can be of all types. After reviewing this list, you can decide how to enable this access, if appropriate. For example, you may decide to provision an abstract role to a user or add a duty to a custom role.
4. Click **OK** to close the Roles That Grant Access dialog box.

View Privileges Required for Menu

For any entry in the Navigator, regardless of whether it's available to the role, you can identify the privileges that grant access to:

- The Navigator entry
- Tasks in the associated work area

Follow these steps:

1. Click the entry.
2. Select **View Privileges Required for Menu**.
3. In the View Privileges for Work Area Access dialog box, review the list of privileges that grant access to:
    - The Navigator menu item.
    - Task panel entries in the associated work area. In the **Access Granted** column of this table, you can see whether the selected role can access these tasks.

    You can use this information when creating roles, for example. You can identify how to both add and remove access to specific tasks and work areas.
4. Click **OK** to close the View Privileges for Work Area Access dialog box.
5. Click **Close** to close the Simulate Navigator page.

Simulate the Navigator for a User

Search for the user on the Roles tab of the Security Console and select **Simulate Navigator** in the **Actions** menu for the user. Follow the instructions for simulating the Navigator for a role.

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.

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.

Compare Users

You can compare users to identify their access permissions and assign the missing permissions as required. This comparison includes both direct and inherited roles. From the results, you can find out if there are any discrepancies in roles.

Only administrators with the View User Account (ASE_VIEW_USER_ACCOUNT_PRIV) privilege can compare users. On the User Accounts page, you can compare users in two different ways:

- Use the Compare Users button.

- Search for a user and then click Compare Users from the Actions menu of that user.

Follow these steps:

1. On the Security Console, click **Users**.
2. Click **Compare Users**.
3. Search for and select both users one after another.
4. Click **Compare**. All the details of both the users are displayed.

In the comparison results, you can do the following actions:

- Click one of the **Show** options to view the corresponding details in the results.
- Click the Query By Example icon to enter the name of a specific role that you want to see from the search results.

You can then use the Export to Excel option to export the filtered search results.

Copy Roles from One User to Another

If the user you're creating must have the same set of roles that an existing user has, you can consider copying the required roles instead of manually assigning them.

Adding roles manually to replicate an existing user is a time-taking task. Instead, use the Copy User option in Security Console to create the user with all the roles assigned, at one go.

There are two ways in which you can copy the roles from an existing user to another user:

- Use the Copy User option in the Actions menu of the selected user on the User Accounts page. You can copy the user category and assigned roles of the selected user. Additionally, you can copy the Enable Administration Access for Sign In-Sign Out Audit REST API setting if the Enable access to Advanced User Management Settings profile option is enabled.
- Use the Add Role button on the Add User Account page.

If you have more than 20 roles to copy, then the application runs an asynchronous process in the background. You must wait for the asynchronous process to complete before you can edit, delete, copy, or compare roles on the target user. You can view the status of up to 25 recently run asynchronous processes at any time using the User-to-User Role Membership Transfer Status tab on the Administration page.

Note: You can search for an asynchronous process based on the user name or status.

Using the Copy User Option

1. On the Security Console, click **Users**.
2. On the User Accounts page, search for the user from which you want to copy the roles.
3. From the **Action** menu of that user, click **Copy User**. On the Add User Account page, the user category and assigned roles of the selected user appear. The Enable Administration Access for Sign In-Sign Out Audit REST API setting is selected if this setting is enabled for the source user.
4. Enter the details of the user and click **Save and Close**.

Using the Add Role Button

1. On the Security Console, click **Users**.
2. On the User Accounts page, click **Add User Account**.
3. On the Add User Account page, select a user category and enter the details of the user.

4. Click **Add Role**.
5. Select **Users** from the **Search** drop-down list and search for the user from which you want to copy the roles.
6. Select the user and click **Add Role Membership from User**. A confirmation message appears.
7. Click **OK** and click **Done**.
8. Click **Save and Close**.

Related Topics

- Role Copying or Editing

Analytics for Roles

You can review statistics about the roles that exist in your Oracle Cloud instance.

On the Analytics page, click the Roles tab. Then view these analyses:

- Role Categories. Each role belongs to a category that defines some common purpose. Typically, a category contains a type of role configured for an application, for example, "Financials - Duty Roles."

  For each category, a Roles Category grid displays the number of:

  - Roles
  - Role memberships (roles belonging to other roles within the category)
  - Security policies created for those roles

  In addition, a Roles by Category pie chart compares the number of roles in each category with those in other categories.
- Roles in Category. Click a category in the Role Categories grid to list roles belonging to that category. For each role, the Roles in Category grid also shows the number of:
  - Role memberships
  - Security policies
  - Users assigned to the role
- Individual role statistics. Click the name of a role in the Roles in Category grid to list the security policies and users associated with the role. The page also presents collapsible diagrams of hierarchies to which the role belongs.

  Click Export to export data from this page to a spreadsheet.

Analytics for 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.

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.

17 Create and Edit Job, Abstract, and Duty Roles

Overview of Security Configuration

This chapter describes some of the ways in which you can configure the predefined sales security model.

The Oracle implementation of role-based access control is designed to handle a wide range of security requirements in different environments. As a result, most companies can use the standard security settings without modification. If necessary, though, you can configure the default settings to meet specific business requirements. Before making any changes to the security reference implementation, make sure you follow these steps:

- Clearly define the change that's required and review the proposed changes with Oracle Support.
- Make sure you understand the interrelationships of the various security components and the effect of the proposed change on user access.
- Document any changes you make.

This chapter describes how you can create your own roles and role hierarchies. For information about configuring data security, see the chapter Configure and Troubleshoot Data Security.

For additional information about changing the standard security settings, go to the Security Resource Center, which is available at 1609084.1 (Document ID) on My Oracle Support. The Security Resource Center provides templates you can use to track the changes you make to standard settings. For information about the privileges or other security artifacts provided for new or updated functionality in each release, and the procedures to add these privileges to custom roles, see the Upgrade Guide for Oracle Sales Cloud Application Security article (Document ID 1989500.1) on My Oracle Support.

Related Topics

- Overview of Data Security Configuration

Guidelines for Copying Roles

Copying predefined roles and editing the copies is the recommended approach to creating 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 custom 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 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; 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.

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 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.

Copying Roles and Access Groups

When you copy a job role, a custom job role is created that includes the same duty roles and the same function and data security policies as the original role. A system access group is also generated for the custom job role, but it isn't assigned any object sharing rules.

To provide your users with data access using the access group generated for the custom role, you must either add rules to the group manually, or copy the rules from the access group generated for the source role you copied, then edit the rules as required. For additional information, see the topics Overview of Managing System Access Groups and Copy Object Sharing Rules from One Access Group to Another in the Access Groups chapter.

Report and Analytics Roles

You can't copy roles that are used to secure sales analytics and reports. Therefore you can't copy any of the following types of roles:

- Transaction Analysis Duty roles
- Business Intelligence roles
- Any role with a role code prefix of OBIA, for example, OBIA_ANALYSIS_GENERIC_DUTY

You can however, add any of these roles to custom job roles that you create. When you create a custom job role, either from scratch or by copying an existing job role and editing it, make sure that the role is assigned the BI Consumer role

and BI Author role if the custom role is to provide access to analyses and reports. The BI Consumer role provides view-only access to analyses and reports; the BI Author role provides access to create and edit analyses and reports.

Related Topics

- Role Preferences
- Overview of Managing System Access Groups
- Copy Object Sharing Rules from One Access Group to Another

Copy Job or Abstract Roles

You can copy any job role or abstract role and use it as the basis for a custom role. Copying roles is more efficient than creating them from scratch, especially if your changes are minor.

This topic explains how to copy a role to create a new role. You must have the IT Security Manager job role to perform this task.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact license usage. Before you proceed, see the topic Guidance for Assigning Predefined Roles.

Copy a Role

To copy a job or abstract role:

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:** 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 here.

7. Click the **Summary and Impact Report** train stop.
8. Click **Submit and Close**, then **OK** to close the confirmation message.
9. Review the progress of your copy on the Role Copy Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

Related Topics

- Guidelines for Copying Roles
- Guidance for Assigning Predefined Roles

Edit Job or Abstract Roles

You can create a role by copying a predefined job role or abstract role and then editing the copy. This topic describes how to edit a role on the Security Console.

You must have the IT Security Manager job role to perform this task.

Edit the Role

To edit a job or abstract role:

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: Function Security Policies page, any function security privileges granted directly to the copied role appear on the Privileges tab. Click **Load Inherited Policies** to populate the table with privileges that the role inherits. To view details of the code resources that a privilege secures, select the privilege in the Details section of the page.

You can add or delete existing privileges from copied roles but can't create new functional security policies. To delete a privilege that's added directly to the copied role, select the privilege and click the Delete icon. You can't delete inherited privileges.

To add a privilege to the copied 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 role to your custom role. 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.

   All the privileges you selected are listed on the Edit Role: Function Security Policies page.
7. Click **Next**.

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 Privileges

On the Edit Role: Data Security Policies page, any data security policies granted to the copied role appear. You can add or remove policies from the copied role, or edit the existing policies. For information about creating, editing, and adding data security policies to a role, see the topic Edit Data Security Policies on the Security Console.

Click **Next** to continue to the next page.

Add and Remove Inherited Roles

The Edit Role: Role Hierarchy page shows the copied role and its inherited duty roles. The hierarchy is in tabular format by default but you can switch to graphical mode. 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.

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**.

Assign the Role to Users

On the Edit Role: Users page you can assign the copied role to a user.

To remove user access to a role:

1. Select the user in the table.
2. Click the **Delete** icon.
3. Click **OK** to close the confirmation message.

To add user access to a role:

1. Click the **Add User** button.
2. In the **Add User** dialog box, search for and select a user or role (job or abstract role).
3. If you select a role, then click **Add Selected Users** to add all the users assigned the role to your custom role. If you select a single user, then click **Add User to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional users.
6. Close the **Add User** dialog box.

   The Edit Role: User page shows the updated role membership.
7. Click **Next**.

Review the Role

On the Edit Role: Summary and Impact Report page, review the summary of changes. Then do the following:

1. Click **Back** to make corrections.

2. When you have completed any corrections required, click **Save and Close** to save the role.
3. Click **OK** to close the confirmation message.

The role is available immediately.

Related Topics

- Copy Job or Abstract Roles
- Edit Data Security Policies on the Security Console

Create Job and Abstract Roles

If the predefined job or abstract roles aren't suitable, or you need a role with few privileges, then you can create a role from scratch. This topic explains how to create a job role or abstract role.

To perform this task, you must have the IT Security Manager job role.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact license usage. Before you proceed, see the topic Guidance for Assigning Predefined Roles.

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 **Digital Sales Manager**.
3. Enter a unique **Role Code**. For example, enter DIGITAL_SALES_MGR_JOB.

   Abstract roles have the suffix **_ABSTRACT**, and job roles have the suffix **_JOB**.
4. In the **Role Category** field, select the appropriate role category, for example, **CRM - Job Roles**.
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, 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 duty roles to your role. You're less likely to grant function security privileges directly to the role. If you're not granting function security privileges, then click **Next**. Otherwise, to grant function security privileges to the role:

1. On 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.

   You can either add an individual privilege or copy all the privileges that belong to an existing role.
3. If you select a role, then click **Add Selected Privileges** to add all the function security privileges assigned to the selected role to your custom role. 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.

   All the privileges you added are listed on the Create Role: Functional Security Policies page. You can:

   - Click on a privilege to view details of the code resource that it secures.
   - Delete any privilege by selecting the privilege and clicking the Delete icon.
7. Click **Next**.

Note: You can add existing privileges to the new role but can't create new functional security policies.

Add Data Security Policies

On the Create Role: Data Security Policies page, you can assign data security policies to your role. For information about creating and adding data security policies to a role, see the topic Edit Data Security Policies on the Security Console.

Click **Next** to continue to the next page.

Build the Role Hierarchy

The Create Role: Role Hierarchy page shows the hierarchy of your custom role in tabular format by default. You can add one or more job, abstract, and duty roles to the new role. Typically, when creating a job or abstract role you add duty roles. 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. Close the **Add Role Membership** dialog box.

   The Create Role: Role Hierarchy page shows the updated role hierarchy.
7. Click **Next**.

Assign the Role to Users

On the Create Role: Users page, you can assign the job or abstract role you're creating to selected users.

To assign the role to a user:

1. Click **Add User**.
2. In the **Add User** dialog box, search for and select a user or role.
3. If you select a role, then click **Add Selected Users** to add all the users assigned the role to the role you're creating. If you select a single user, then click **Add User to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 to add additional users.
6. Close the **Add User** dialog box.

   The Create Role: Users page shows the updated role membership.
7. Click **Next**.

Review the Role

On the Create Role: Summary and Impact Report page, review the summary of the changes. Click **Back** to make any 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 on the Security Console.

> **Tip:** Search for the job or abstract role on the Security Console and review its visualization. Edit the role to make any corrections.

Related Topics

- Guidance for Assigning Predefined Roles
- Edit Data Security Policies on the Security Console

Copy and Edit Duty Roles

The recommended way of creating a new duty role is to copy an existing role, then edit the copied role as needed. This topic explains how to do both tasks.

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

Copy a Duty Role

To copy a duty role:

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 is displayed in tabular format by default. 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.
   - If you select **Copy top role**, then only the selected role is copied. The copied role inherits the same role instances as the source role.
   - If you select **Copy top role and inherited roles**, then a copy is made of every role in the role hierarchy provided that a copy of the role with the same name doesn't already exist.
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 **Role Code** values are assigned the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. The prefix **ORA_** is also removed from the role code. You can overwrite the default prefix and suffix for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make here.

7. Click the **Summary and Impact Report** train stop.
8. Click **Submit and Close**, then **OK** to close the confirmation message.
9. Review the progress of your copy on the Role Copy Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

Edit the Copied Duty Role

To edit the copied role, perform the following 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: Function Security Policies page, any functional security privileges granted directly to the copied role appear on the Privileges tab. Click **Load Inherited Policies** to populate the table with privileges that the role inherits. To view details of the code resources that a privilege secures, select the privilege in the Details section of the page.

You can add or delete existing privileges from copied duty roles but can't create new functional security policies. To delete a privilege that's added directly to the copied role, select the privilege and click the **Delete** icon. You can't delete inherited privileges.

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 Privilege** to grant all function security privileges from the role to your custom role. 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.

   All the privileges you selected are listed on the Edit Role: Function Security Policies page.
7. Click **Next**.

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

On the Edit Role: Data Security Policies page, any data security policies granted to the copied role appear. You can edit or remove policies from the copied role, or create a new policy for the role. For information about creating, editing, and adding data security policies to a role, see the topic Edit Data Security Policies on the Security Console.

Click **Next** to continue to the next page.

Add and Remove Inherited Roles

The Edit Role: Role Hierarchy page shows the copied duty role and any duty roles that it inherits. The hierarchy is displayed 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**.

View Users Assigned the Role

On the Edit Role: Users page, click **Next**. You can't provision duty roles directly to users.

Review the Role

On the Edit Role: Summary and Impact Report page, review the summary of changes. Click **Back** to make corrections. Otherwise:

1. Click **Save and Close** to save the role.
2. Click **OK** to close the confirmation message.

The role is available immediately.

Related Topics

- Guidelines for Copying Roles
- Edit Data Security Policies on the Security Console

Create a Custom Role with Limited Access

To delegate some of the IT security management tasks to a helpdesk member within your company without assigning the IT Security Manager role, create a custom role with specific privileges.

These privileges are exclusively meant for controlling user management access. You can assign these privileges directly to a custom role.

Users without the IT Security Manager role who are assigned custom roles with these privileges have limited access to the Security Console. These users can only lock or unlock other users, reset their password, or view user details. They can't create users or edit user details.

The following table lists the privileges and the associated access controls. It also includes details of pages where the user does the task:

Table with Privileges, Access Control Details, and Pages Where User Does the Task

Privilege Name and Code	Access Control Details	Page Where You Do this Task
Lock and Unlock User Account (ASE_LOCK_UNLOCK_USER_PRIV)	Lock or unlock a user account	User Accounts
Update Password for User Account (ASE_UPDATE_PASSWORD_FOR_USER_PRIV)	Reset the password for a user account	User Accounts and User Account Details
View User Account (ASE_VIEW_USER_ACCOUNT_PRIV)	View the details of a user account	User Account Details

Related Topics

- View Locked Users and Unlock Users
- Reset Passwords

18 Configure and Troubleshoot Data Security

Overview of Data Security Configuration

Learn some of the ways you can configure and troubleshoot data security for sales and service users by reviewing the information in this chapter.

How sales database resources are secured in your environment depends on when you were provisioned with the sales and service application:

- If you started using the sales application before release 22B, then the database resources of your enterprise are secured using data security policies, which are assigned to job roles. Data security policies specify the roles that can perform a specified action on an object and the conditions under which the action can be carried out.

  > **Note:** If you've configured one or more access groups or object sharing rules, your users receive data access through a combination of data security policies and access group rules.

- If you're using the sales application for the first time in release 22B or later, your database resources are secured using system access groups and rules. When you assign job roles to users, they're automatically assigned membership of an associated system access group, and receive all the data permissions provided by the access group object sharing rules. These rules specify the access groups that can perform a specified action on an object, and the conditions under which the action can be carried out.

The conditions specified in both data security policies and access group rules control visibility to record-level data associated with a business object, such as an opportunity. Conditions can use a number of components, such as team or territory access, as mechanisms for sharing data. The scope of visibility varies by object, and multiple visibility levels are supported by an object for a role.

Regardless of whether your environment was provisioned with data security policies or system access groups rules, it's recommended that you use custom access groups to supplement the data access your users receive through their job role assignments.

The following table shows your options for reviewing, configuring, and troubleshooting data security.

Work Area	What You Can Do	When to Use
Access Groups	From the Access Groups page you can configure data security by creating custom access groups, adding members to these groups, and defining rules to specify the access that group members should have to object data.	It's recommended that you use access groups and rules to configure data security. Access groups are easy to create and manage, and are processed more efficiently than data security policies. **Note:** If you're using the sales application for the first time in release 22B or later, you have to use access groups to configure user access to object data.
Sales and Service Access Management	From the Sales and Service Access Management work area you can review and configure the data access provided by data security policies assigned to job roles. You can	Use this work area to get an overview of a user's access to data, to troubleshoot user access issues, and to review the data security policies assigned to job roles.

Work Area	What You Can Do	When to Use
	also review all a user's access to object data, whether from data security policies or access group rules.	
Security Console	From the Security Console, you can review and configure the access provided by the data security policies assigned to a role. You can also create database resources, and define custom conditions for a resource.	It's recommended that you use access groups and rules to configure data security when possible. But you can optionally use the Security Console to define database resources and custom conditions. You can also edit data security policies when creating, copying or editing roles on the Roles tab of the Security Console.

Note: Data security changes made in any of the work areas described in the table are immediately available in all work areas.

Review this chapter for information about how to use the Sales and Service Access Management work area to configure data security, or for information about managing database resources and editing data security policies on the Security Console. For information about configuring access using access groups, see the Access Groups chapter in this guide.

Sales and Service Access Management Work Area

As an IT Security administrator, you must be able to easily view the data a predefined role can access and to easily configure access to data for a user group using custom roles. Administrators must also be able to troubleshoot access issues for users.

You can perform all of these tasks using the Sales and Service Access Management work area, which provides simple interfaces where you can do these tasks:

- Create and manage access groups to provide sales resources with additional visibility to sales object data.

  See the Access Groups chapter for information about using access groups.
- Troubleshoot access issues for users:
  - Review all a user's access to object data, whether from data security policies or access groups
  - Identify the cause of any issues the user is experiencing in accessing specific records
- Review and configure the data access provided by roles:
  - View data access by object for a predefined Oracle CX role or for a custom role
  - Configure data security to add or remove a custom role's access to object data
  - End-date policies and configure advanced data permissions
  - Extend access to additional objects for custom roles

Note: You can view policies for custom objects in the Sales and Service Access Management work area but you can only configure security for custom objects in Application Composer.

Access to the Sales and Service Access Management Work Area

The Manage Sales and Service Access privilege (ZCA_MANAGE_SALES_AND_SERVICE_ACCESS_PRIV) grants access to all the functionality in the Sales and Service Access Management work area. This privilege is assigned by default to the IT Security Manager and the Customer Relationship Management Application Administrator job roles.

Users assigned the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV) can access the Sales and Service Access Management work area to create and manage access groups. By default, the Sales Administrator job role and the IT Security Manager job role have this privilege.

If necessary, you can provide access to all the work area, or to the Access Groups region of the work area, by granting the Manage Sales and Service Access functional privilege or the Manage Group Access functional privilege to a custom job role.

Review and Configure Data Access for Roles

Review a Role's Access to Object Data

You can review the visibility provided by job roles to object data by selecting the Manage Data Policies tab on the Sales and Service Access Management page. The Manage Data Policies page displays a read-only view of all the data security policies provided by a predefined or custom role for an object.

You can use this information to query existing policies so you can answer questions such as these:

- What's the most appropriate role to apply to a set of users?
- What's the most suitable role to copy when you need to extend the access provided by existing predefined roles?
- Why can't users access specific data?

By default, active policies are displayed for a role and object but you can also review inactive policies.

Here's how to review data access for a selected role and object:

1. Sign in to the application as a user who has either the IT Security Manager or Customer Relationship Management Application Administrator job role.
2. Select **Navigator** > **Tools** > **Sales and Service Access Management**.

   > **Tip:** You can also access the Sales and Service Access Management page from the Setup and Maintenance work area by selecting the Manage Sales and Service Access task in the Users and Security functional area of the Sales offering.

3. On the Sales and Service Access Management page, click the Manage Data Policies tab.

   The Manage Data Policies page contains two areas: the Active Policies table, which lists each data policy for the selected object and role combination, and the Advanced Permissions table, which shows more detail about any advanced permissions available for a policy selected in the Access Policies table.

4. Select a role in the **Role** field.

   You can select either a custom or a predefined role. To search for a role:

   a. In the **Role** field drop-down list, click **Search**, then enter the role name in the **Role** field of the Role dialog box.
   b. Click **Search** again. From the search results, select the role you want, then click **OK**. Note that in the search results predefined roles are identified by a **Yes** in the Predefined role column.

5. Select an object in the **Object** field.

   The **Object** field lists all the sales and service objects the role can access.

   > **Note:** Select the Trading Community Party object to view access policies for both accounts and contacts.

6. Click **Find Policies**.

   The Active Policies table now lists all the active data security policies relating to the object you selected for the role you selected. You can view more or less information for the policies in the table by selecting the **Columns** option in the **View** menu.

   This information is shown for each active policy in the Access Policies table.

Field	Value
Condition	Lists the condition that must exist for this data policy to take effect. For example, if you selected the Sales Representative role and the Opportunity object, the condition might state that this policy applies when the user assigned the Sales Representative role is an opportunity sales team member with edit or full access.
Permissions	Shows the access provided by the policy. For example, if the **Read**, **Update**, and **Delete** check boxes are selected, then this policy provides a user with read, update, and delete access to the object when the conditions specified in the policy are met, for example, when the user is an opportunity sales team member with edit or full access. The **Advanced** field indicates the number of advanced permissions defined for the policy. Not all objects or policies have advanced permissions.
Start Date	Indicates the date when the policy was activated.
End Date	Indicates the date when the policy is deactivated.
Role Code Role Name	Lists the role name and code of the role the policy is associated with. In most cases, the policy relates to the top-level job role you selected in the **Role** column, but in some cases, the policy is provided by an inherited duty role. A policy can even be provided by both the top-level role and by an inherited role.
Custom Condition	Indicates whether the condition specified in the policy is a predefined condition provided by Oracle or is a custom condition that you created previously.

Field	Value

7. You can limit the policies that are shown for the role and object by clicking the **Query By Example** filter icon and entering filter text. You can filter by condition, role name, or role code.

   For example, currently the standard Sales Representative job role provides data visibility to all accounts and contacts. To view the conditions that are providing this full access, use these steps:

   a. Select **Sales Representative** in the Role field, **Trading Community Party** in the **Object** field, and click **Find Policies**.
   b. Click the **Query By Example** filter icon, and enter the text **All records** in the query field above the Condition column.

   The page is refreshed and displays two policies that provide all record access. Notice that one policy is provided by the Sales Representative role and the other by an inherited role, Contract View Access Across All Contracts. If you wanted to create a version of the Sales Representative role that had more restricted access to accounts and contacts, you would have to create custom copies of both roles and remove the All records policies from each.

   To remove the filter, click the **Clear All** icon in the query row.
8. To view the advanced permissions defined for a selected policy in the Access Policies table, scroll to the Advanced Permissions table.

   Advanced permissions provide a finer-grained method of controlling what the user can do. For example, a policy might provide update access to an opportunity but the advanced permission for the policy might allow you to restrict that update access to specific attributes.

   For each advanced permission, the Advanced Permissions table shows the type of access provided, for example, Read access, and the action it relates to, for example, View Opportunity.
9. If you want to view the inactive policies for a selected role and object on the Manage Data Policies page, select the **Inactive policies** check box.

   Inactive policies are policies that you set an end-date for and the end-date has passed. The number of inactive policies for the role and object is shown in parentheses beside the **Inactive policies** check box. For example, the number **1** indicates that there is only one inactive policy for the role-object combination.

How do I edit the data access permissions for a custom role and an object?

You can update existing and future-dated policies for a custom role and object, and grant access to new subsets of data for the role, using the Active Policies edit page of the Sales and Service Access Management work area.

For example, you can:

- Add or remove all access to individual policies
- Configure read, update, and delete permissions for a specific policy
- End-date policies to inactivate them
- Configure advanced permissions for policies

Follow these steps to edit the permissions to object data for a custom role.

1. Sign in to the application as a user who has either the IT Security Manager or Customer Relationship Management Application Administrator job role.
2. Select **Navigator** > **Tools** > **Sales and Service Access Management**.
3. On the Sales and Service Access Management page, click the Manage Data Policies tab.
4. Search for or select a role in the **Role** field.

   You can't edit policies on predefined roles, so search for and select a custom role. For example, if you copied the predefined Salesperson role to create a custom version of the role, you could select it.
5. Select an object in the **Object** field, for example, select the **Sales Lead** object.

   > **Note:** Select the Trading Community Party object to view access policies for both accounts and contacts.
6. Click **Find Policies**.
7. Click the **Edit** icon and the Active Policies edit page for the selected role and object is displayed.

   The Access Policies table shows all available policies for the selected role and object by default but you can use the **Show Conditions** filter to display only policies that are granted or only policies that aren't granted.
8. Configure the access provided to the selected object for the selected custom role by selecting or deselecting the **Read**, **Update**, or **Delete** check boxes for a policy.

   For example, if you're editing policies for a custom Salesperson role and the Sales Lead object, you can perform data configuration tasks such as:

   - Restrict the ability to delete leads to lead owners by finding any policies that provide lead access to team members and deselecting the **Delete** check box for these policies.
   - Allow sales representatives to view retired leads by finding the policy that grants this access, then clicking the **Read** check box.
9. You can remove all access granted by a policy. For example, if your company doesn't use territory access, you can remove territory access to lead data using one of the following methods:

   - Review the Condition column to find the policies that grant territory access, then deselect the **Read**, **Update** and **Delete** check boxes for each of these policies.
   - End-date the policies so that they're no longer active by selecting a date that has passed in the **End Date** field, for example, select yesterday's date.

   > **Note:** To reactivate a policy that's deactivated, reassign the appropriate read, update, and delete permissions to the relevant criteria and specify a start date for the policy.
10. If a policy has an advanced permission associated with it, then you can edit the advanced permission to specify more granular levels of access to the object.

    For example, a policy might provide full access to lead data for a resource in the territory assigned to the sales lead. You can restrict this access by selecting the policy, then scrolling to the Advanced Permissions table for the policy. You can remove update access to the lead data but retain read access by deselecting the **Update** check boxes.

    > **Note:** You can update the advanced permissions for a policy only if the related permission in the parent row in the Access Policies table is checked. For example, if the read permission in the parent row of a policy isn't selected, none of the read permission options in the Advanced Permissions table can be edited.

11. Click **Save and Close**.

    Your changes are saved and the Manage Data Policies page is displayed where you can review your changes. If you've end-dated a policy, note that the number in parentheses beside the **Inactive policies** check box is incremented.

Considerations When Editing Inherited Roles

This topic describes some of the things to keep in mind when you edit inherited roles on the Active Policies page of the Sales and Service Access Management work area.

To add or remove a job role's access to object data, you have to know which policies provide the access. A job role can be assigned a policy in these ways:

- It can be assigned a policy directly
- It can inherit a policy indirectly from an inherited role
- It can receive the same policy from more than one role

The information on the Active Policies page lets you view all policies a job role is assigned, from all sources, for the selected object. For each policy in the Access Policies table, the **Role Name** field lists the role that the policy is associated with; this is either the top-level job role you selected on the Sales and Service Management page, or a duty role that the top-level role inherits.

You can't edit policies that are inherited from predefined duty roles because predefined roles can't be edited. But you can edit policies that are inherited from custom duty roles. If you edit a policy provided by an inherited custom duty role, keep in mind that if the custom duty role is also inherited, directly or indirectly, by other roles then the change you make to the policy also impacts these other roles.

To make sure that you don't inadvertently change the access provided by roles other than the top-level job role you're editing, a warning message alerts you if a policy change you're making impacts other roles. The message lists the names of all roles impacted by your edit, and prompts you to confirm whether or not you want to continue to make the change. Select one of these options:

- Click **Yes** to continue to apply the access change to the inherited custom role in either of these situations:
    - You want to make the access change to all the roles listed in the warning message.
    - You don't want to make the access change to all the roles listed in the warning message, but you do want to apply the access change to the job role you're editing now.

      In this situation, make a note of the roles listed in the message before clicking **Yes**. At a later time, you can directly update each role listed in the message to restore the access it provides to its original setting. This process can be time consuming if there are a number of roles affected by the edit of the inherited duty role so it's a good idea to avoid this situation if possible. For example, if you removed a privilege from the custom inherited role, you will have to manually add the privilege back to each job role listed in the message, or to the job role associated with each duty role listed in the message.

- Click **No** if you decide not to apply the access change to the inherited custom role. Instead, use these steps to implement the access change for the top-level job role only:
  a. Modify the role hierarchy of the top-level job role by removing the inherited custom role.
  b. Do one of the following:
     - Make a copy of the inherited custom duty role you removed using the **Copy top role** option, assign the copied duty role to the top-level job role, then edit the duty role as required.
     - Directly assign the job role with the access provided by the removed inherited duty role that you want to retain.

Edit Inactive Policies

If you specified an end date for a policy, then once the end date is passed, the policy is inactive. You can't edit inactive policies for custom roles but you can delete them.

To delete an inactive policy:

1. On the Sales and Service Access Management page, click the Manage Data Policies tab.
2. Select a custom role in the **Role** field and an object in the **Object** field.
3. Click the **Inactive policies** check box.
4. Click **Find Policies**.

   All inactive policies are displayed in the Inactive Policies table.
5. Click the **Edit** icon.
6. On the Inactive Policies page, select a policy and click the **Delete** icon.
7. Click **Yes** when a warning is displayed.
8. Click **Save and Close** to return to the main page.

   The deleted policy is no longer included in the Inactive Policies table and the number in parentheses beside the Inactive policies check box is reduced.

Note: You can reactivate a policy that's deactivated by reassigning the appropriate read, update, and delete permissions to the relevant criteria and specifying a start date for the policy on the Active Policies edit page.

Extend Access to Additional Objects for a Custom Role

You can provide custom roles with visibility to object data they can't currently access by creating new data security policies on those roles for the relevant object.

For example, if you want to provide sales managers with access to subscription account data for a specific initiative, then you have to create access to the relevant subscription account object for a custom version of the Sales Manager job role, because the Sales Manager job role doesn't provide access to this data by default.

To create access to a new object for a custom role:

1. On the Sales and Service Access Management page, click the Manage Data Policies tab.
2. Click the **Create** button.
3. On the Create Policies page, search for the custom role whose access you want to extend in the **Role** field.

4. Select the object you want to provide access to in the **Object** field.

   For example, select the object for subscription accounts, **Subscription Account**. The only objects available for selection are objects where data security policies are not already defined for the custom role.
5. Click **Find Policies**.

   All the data security policies defined for the selected object are displayed in the Access Policies table. There are no permissions selected in the Permissions columns because data access to the object hasn't previously been configured for the custom role you selected.
6. Locate the condition that provides the data access you want to implement for the object.

   For example, if you want to provide the custom sales manager role with read access to all subscription account records, use these steps:

   a. Locate the condition that provides the required access. In this example, locate the condition: **Access the subscription account for table ATC_SUBSCR_ACCOUNTS for all subscription accounts**.
   b. Click the **Read** check box for this condition.
   c. Specify a **Start Date** of today and an appropriate **End Date**.
7. Click **Save and Close**.

   On the Manage Data Policies page, the new policies you added are now listed in the Active Policies table for the role and object.

   > **Note:** You can view data security for custom objects using the Sales and Service Access Management work area, but you can only edit security policies for custom objects using Application Composer.

Review and Troubleshoot Data Access Issues for Users

Overview of the Data Access Explorer

You can use the access explorer functionality in the Sales and Service Access Management work area to quickly troubleshoot data access issues reported by your users. These are some examples of the typical access issues you might have to investigate:

- You create a custom sales representative role that removes access to all accounts but users assigned the custom role still have all account access. Which data access conditions or access group rules are providing the access?
- A sales manager can't see opportunities assigned to her reports. Which data access condition or access group rule must she be assigned to get access?

To identify the cause of a user access issue, you must be able to see all the access a user currently has to object data, whether from data security policies or access group rules, and all the policies or rules that provide access to the relevant object or record. You can view both types of information on the Explore UI. You can:

- Review all the access policies granted to a user for an object, and all the roles that provide the access.
- Review all the access group rules granted to a user for an object, and all the access groups that provide the access.
- Discover which data security policies and rules are affecting a user's ability to view a specific object record.

With this information, you can identify why a user can or can't view a specific record or records, and then grant or revoke the appropriate data access.

> **Note:** The Explore UI shows the data access users receive through the Oracle CX job and duty roles they're assigned. It doesn't show users access to object records provided by non-CX roles, such as Oracle HCM roles, that they might also be provisioned with.

Access Group Rules and the Access Groups Enablement Data Security Policies

On the Explore UI, you can view a user's access to data from both access group rules and data security policies. This topic describes the interaction between access group rules and the policies provided by the Access Groups Enablement duty role.

To receive access to object records through access groups, the following conditions must be met:

- Users must be assigned the relevant active rules through their access group membership.
- Users must be assigned the appropriate data security policies provided by the Access Groups Enablement duty role.

  These data security policies are required for users to get the access to object data provided through access groups, but they don't provide access to object data themselves.

Users are automatically assigned the Access Groups Enablement duty role through the predefined or custom job roles they're assigned, or through the Resource abstract role. In general, for each object supported for access groups, the Access Groups Enablement duty provides users with data security policies for each access level supported by the object; usually read, update, delete, and full access.

When reviewing information on the Explore UI, keep in mind that although users are assigned the Access Groups Enablement data security policies, they only receive the relevant data access if they're also assigned a corresponding active rule that provides the same access.

Review a User's Access to Object Data

You can view all the access group rules and data security policies that currently affect the visibility a user has to an object, and the names of all the access groups and roles (Oracle CX roles or custom roles) that provide each rule or policy, using the access explorer.

Being able to identify all the access paths through which a user gains access to object records is essential when you want to remove a user's access to a set of data. Here's how to review all the policies and rules assigned to a user:

1. On the Sales and Service Access Management page, click **Explore Access**.
2. On the Explore page, select the name of the user whose access you're investigating in the **User Name** field.
3. Select an object from the **Object** field, for example, select the **Opportunity** object.

   Don't enter a value in the **Public Unique Identifier** field. You only enter a value in this field if you want to investigate a user's access to a specific record.
4. Click **Explore**.

The Access Groups and Data Security Policies tables are displayed showing all the active rules and policies that are granted to the user, providing you with an overall view of the user's access to data for the selected object. In each table, you can display more or less data for each rule or policy by selecting options from the **View** drop-down list for the table.

> **Note:** The Provides Record Access column in each table indicates if a policy provides access to the record specified in the **Public Unique Identifier** field. Because you haven't entered a value for this field, the Provides Record Access column is empty and the **Provides Record Access** drop-down list, which lets you filter values for the Provides Record Access column, is inactive.

- By default, the following information is displayed in the Access Groups table for each active rule the user is assigned through their access group membership.

Field	Description
Status	The status of the rule. By default, active rules are displayed. A rule is active and provides the user with object access if the following conditions are met: - The rule is active - The rule is enabled for an access group the user is a member of - The access group is active
Rule Name	The name of the rule that provides object access. Provided you have the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV), you can review or edit the rule by drilling down on the rule name link. The access group Object Sharing Rules page is displayed allowing you to edit the rule in the context of an access group. See the Access Groups chapter for additional information.
Permissions (Read, Update, Delete)	The object permissions provided by the rule.
Group Name and Number	The name and number of the access group that provides the rule. Provided you have the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV), you can review or edit the group by drilling down on the group name link. The access group Edit Access Group page is displayed allowing you to edit the group in the context of an access group. See the Access Groups chapter for additional information.

- Data Security Policies and Advanced Permissions tables.

  By default, the following information is displayed in the Data Security Policies table for each active policy the user is assigned, either directly or indirectly. The advanced permissions defined for a selected policy in the Data Security Policies table are shown in the Advanced Permissions table.

Field	Description
Status	The status of the policy. By default, active policies are displayed.

Field	Description
Condition	The condition that must be satisfied for the data security policy to take effect.
Permissions (Read, Update, Delete, Advanced)	The access provided by the policy.
Start Date End Date	Indicates the policy activation start and end dates.
Role Name Role Code	The name and code of the role that provides the policy. If the user inherits the policy from more than one role, click the link beside the role name to see a list of all roles.
Custom Condition	Indicates whether the condition is a predefined condition or a custom condition that you created.

5. Once you have reviewed all the active policies or rules assigned to the user, you can select options from the **Show Access** drop-down list (Access Groups table) or the **Show Conditions** drop-down list (Data Security Policies table) to view rules and policies available for the object that the user isn't assigned or isn't receiving access from.

   For example, a user might be assigned a rule through group membership, but if the group isn't active, the user doesn't receive the access provided by the rule. Using these options can help you identify both gaps in a user's data access, and access a user doesn't require.

   This table shows the options available.

Filter Option	Description (Data Security Policies Table)	Description (Access Groups Table)
All	Display all policies defined for the object, including policies that are granted to the user and policies that aren't granted.	Display all rules that are defined for the object, including rules that are granted to the user and rules that aren't granted.
Granted and active	Display all active policies for the object that are granted to the user. This is the default value.	Display all active rules the user is assigned.
Granted and inactive	Display all inactive policies defined for the object that are granted to the user.	Display any rule that the user is assigned where the rule is inactive, where the group associated with the rule is inactive, or where the rule isn't enabled for the group.
Granted and future dated	Display all inactive policies defined for the object that are granted to the user which	Not applicable to rules.

Filter Option	Description (Data Security Policies Table)	Description (Access Groups Table)
	are set to become active at some date in the future.	
Not granted	Display all policies defined for the object that aren't currently granted to the user.	Display any rule that provides object access that isn't granted to the user through access group membership.

How do I troubleshoot user access issues?

Troubleshoot data access issues for users using the access explorer.

On the Explore page, you can view all the access group rules and data security policies that affect a user's ability to view an object record and see whether or not each rule or policy has been granted to the user. You can use this information to find answers to questions such as these:

- What access policy do I have to grant to give the user access to a specific record?
- Which granted rule do I have to remove from the user so that the user can no longer access a record?

> **Note:** The Explore UI shows the data access users receive through the Oracle CX roles they're assigned. It doesn't show users access to object records provided by non-CX roles, such as Oracle HCM roles, that they might also be provisioned with.

To discover why there are issues with a user's access to a specific object record, you need to know:

- The user name of the user.
- The name of the object.
- The Public Unique Identifier (PUID) of the record.

  For information on how to find the PUID of a record, see the topic Display Public Unique Identifiers for Object Records.

  > **Note:** Some objects don't support PUIDs. You can't investigate a user's access to a specific record for these objects.

Use these steps to review all the rules and policies that affect a user's access to a specific object record.

1. On the Sales and Service Access Management page, click **Explore Access**.
2. On the Explore page, select the name of a user in the **User Name** field.
3. Select an object in the **Object** field.
4. Enter the PUID of the relevant record in the **Public Unique Identifier** field.

   The **Public Unique Identifier** field is unavailable if the object doesn't support public unique identifiers.

5. Click the **Explore** button.

   By default, all the rules and data security polices defined for the object that grant access to the record are listed in the Access Groups table and the Data Security Policies table respectively. Review the information in the **Status** column of each table to see which of these rules and policies the user is granted.

   > **Tip:** You can display additional data for each rule or policy by selecting options from the **View** menu of each table.

6. Select the information you're interested in viewing in each table.

   You can display different views of the user's access to the object record by changing the selections in the filters available for each table.

   For example, if a user can't access the record, it might be because the user isn't granted access to the record, or because the user is granted access but the relevant rule or policy is inactive, or because the relevant data security policy is future dated. Select these filter options to figure out the cause of the issue.

Rules or Policies to View	Filter Options to Select
All the rules or policies that provide record access that the user isn't assigned	○ **Not granted** option from the **Show Access** list (Access Groups table) or the **Show Conditions** list (Data Security Policies table) ○ **Yes** option from the **Provides Record Access** list
All the inactive rules or policies assigned to the user that provide record access	○ **Granted and inactive** option from the **Show Access** list or the **Show Conditions** list ○ **Yes** option from the **Provides Record Access** list
All the future dated policies assigned to the user that provide record access	○ **Granted and future dated** option from the **Show Conditions** list ○ **Yes** option from the **Provides Record Access** list

7. In the Access Groups table, you can review the following information for each rule.

Field	Description
Status	This field can have one of these values: ○ **Active**. The rule is granted to the user, the rule is active, and the rule is enabled for an active access group. ○ **Inactive**. The rule is granted to the user but the rule is inactive, the access group the rule is associated with is inactive, or the rule to group association is disabled. ○ **Not granted**. The user isn't granted the rule.
Provides Record Access	This field indicates if a rule grants access to the record specified in the **Public Unique Identifier** field. A check mark indicates that the rule provides record access; if the field is empty, the rule doesn't provide access to the record.

Field	Description
	In the Access Groups table, this field can also be set to **Not Applicable**. This value is displayed for inactive custom rules. You must activate custom rules to see whether or not they provide record access.
Rule Name and Group Name	For rules that are granted to the user, these fields show the name of the rule and the name of the access group through which the user is assigned the rule. For rules that aren't granted to the user, only the rule name is shown. **Tip:** You can click the **Rule Name** or **Group Name** fields to drill down to the edit rule or edit group pages on the Access Groups UI if you have the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV). This is useful if, for example, you want to investigate why a rule is inactive, or if you want to change the activation status of a rule. See the Access Groups chapter for information about editing access groups and rules.
Permissions	For rules that are granted to the user, you can review the type of access provided by the rule.

8. In the Data Security Policies table, you can review the following information for each policy.

Field	Description
Status	This field can have one of these values: - **Active**. The policy is active and is granted to the user. - **Inactive**. The policy is granted to the user but is inactive. - **Future dated**. The policy is granted to the user but the policy **Start Date** is set to a date in the future so the policy isn't yet active. - **Not granted**. The user isn't granted the policy.
Provides Record Access	This field indicates if a policy grants access to the record specified in the **Public Unique Identifier** field. A check mark indicates that the rule provides record access; if the field is empty, the rule doesn't provide access to the record.
Role	The name of the role or roles that provide the policy. The role name is displayed only for policies that are granted to the user.
Permissions	For policies that are granted to the user, you can review the type of access provided by the policy.

Field	Description

You can use the information from the **Status** and **Provides Record Access** fields to figure out what you have to do to provide a user with record access or to remove record access. But you can't edit data security policies on the Explore page.

For example, you might find that a policy that provides a sales manager with access to their subordinates opportunity records is future dated. In this case, note the name of the role providing the policy and edit the role on the Manage Data Policies page or on the Security Console to change the **Start Date** of the policy to the current date.

Display Public Unique Identifiers for Object Records

The sales application generates a unique number (ID) for each business object record when the record is created. As an administrator, you can configure this ID to make it more user-friendly and readable. This user-friendly value is called the public unique ID (PUID).

Note: Not all objects support public unique IDs.

The PUID values for object records aren't displayed on the UI by default. To make these values visible, add the PUID field of the object to the object page using Application Composer. To do this, you require read-only access to all of the object records and access to Application Composer.

The following are the steps to add the **Opportunity Number** field to the Opportunities page. The **Opportunity Number** field displays the PUID value of opportunity records. Follow a similar process for any other objects whose PUID values you want to make available on the UI.

1. Activate a sandbox.

   See the topic Create and Activate Sandboxes for more information.
2. Select **Navigator** > **Configuration** > **Application Composer**.
3. On the Application Composer Overview page, navigate to the standard object whose PUID values you want to expose.

   For example, expand **Opportunity**
4. Select the **Pages** node.
5. Select the Application Pages tab.

   You can use the links on the tab to navigate to the object's configuration pages, where you can modify the pages that are available for the selected object. You can show or hide fields, rearrange fields, and add your own fields.
6. The **Opportunity Number** field shows the PUID value for an opportunity record. To make this field available on the UI, in the Landing Page Layouts region, select Standard Layout, then select **Duplicate** from the **Actions** menu.
7. Enter a name for the new layout, then click **Save and Edit**.
8. Locate the Fuse Opportunity Overview Table area and click the **Edit** icon.
9. In the Available Fields list, locate the **Opportunity Number** field and move it to the Selected Fields list.
10. Click **Save and Close**.

11. Test the changes by navigating to the Opportunities page as a user with access to the opportunities pages, for example, a salesperson.
12. Search for an opportunity, and verify that the PUID value is showing for the opportunity.
13. Publish the sandbox.
14. Navigate to the **Sales** > **Opportunities** page and search for an opportunity record. The PUID of the opportunity is displayed.

For information on exposing attributes and working with sandboxes, see the Configuring Applications Using Application Composer guide. For information on public unique IDs, see the sales Implementation Reference guide.

PUID Fields for Objects

This table shows the field that must be exposed in Application Composer to make the PUID values for the object's records visible on the UI.

Object Name in Application Composer	PUID Field to Expose
Account	Registry ID
Activity	Activity Number
Asset	Asset Number
Business Plans	Number
Campaigns	Campaign Number
Contact	Registry ID
Deal Registration	Registration Number
Deal Registration: Deal Products	DealProdNumber
Deal Registration: Deal Resources	DealResourceNumber
MDF Budget	Code
MDF Claim	Code
MDF Claim Settlement	Code
MDF Request	Code
Objective	Number
Opportunity	Opportunity Number

Object Name in Application Composer	PUID Field to Expose
Partner	Partner Number
Partner Programs	Program Number
Program Enrollments	Enrollment Number
Sales Lead	Lead Number
Sales Orders	Quote or Order Number
Sales Territory	Territory Number
Sales Territory Proposal	Proposal Number
Service Request	Reference Number
Subscription	Subscription Number
Work Order	Reference Number

Related Topics

- Configuring Applications Using Application Composer
- Implementation Reference
- Create and Activate Sandboxes

Why can't my ERP users access Sales and Service data?

Oracle's ERP roles don't give the same access as Sales and Service roles. Analyze your user's needs and give the appropriate roles to the Sales or Service user.

See the related topics for more information.

Related Topics

- Review a User's Access to Object Data
- How do I troubleshoot user access issues?
- Types of Sales Users

Edit Data Security Policies on the Security Console

This topic describes how to edit data security policies when creating, copying or editing roles on the Roles tab of the Security Console.

> **Note:** You can also use the Sales and Service Access Management work area to review and edit the data security policies assigned to job roles.

Edit Data Security Policies for Roles

To create a role, it's recommended that you copy a predefined role rather than create a role from scratch. In this case, your role automatically has the data security policies of the copied role. You can edit or remove the copied data security policies if necessary.

To edit or remove a data security policy for a copied role:

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**.

   The Edit Role: Basic Information page is displayed.
3. Click the Data Security Policies train stop.
4. On the Edit Role: Data Security Policies page, locate the policy then click the down arrow at the end of the policy row to show the actions menu.
5. Select one of the options listed:
   - To remove the policy, select the **Remove Data Security Policy** option.

     The policy is removed from the role.
   - To edit the policy, do the following:
     i. Select the **Edit Data Security Policy** option.

        The Edit Data Security Policy dialog box is displayed.
     ii. Change the values as required, for example, you can change the start date, the data set, or the action specified for the policy.
     iii. Click **OK** to save your changes, and close the confirmation message.

Create Data Security Policies for Roles

You're unlikely to create data security policies unless you create roles from scratch. However, you can do so if required. Here are the steps to use.

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, role code, and role category.

   For additional information about creating roles, see the topic Create Job and Abstract Roles.
3. Click **Next**, then click **Next** again.
4. On the Create Role: Data Security Policies page, click **Create Data Security Policy**.

5. The Create Data Security Policy dialog box is displayed. A **Start Date** value is automatically assigned to the policy but can be changed.
6. In the **Policy Name** field, enter a policy name.

   The names of predefined data security policies begin with the words **Grant on**.
7. Search for and select the database resource for which you're defining the policy, for example, search for a table name.
8. In the **Data Set** field, select the subset of the data made available by the database resource the policy applies to.

   The following table describes the values you can choose for the Data Set field.

Value	Description
Select by key	Use to limit the data set to a single record in the data resource. If you select this option, you must specify the primary key value that identifies the record in the database resource.
Select by instance set	Use to limit the data set to a subset of the data in the data resource. If you select this option, you must select a condition that defines a subset of the data. Conditions vary by resource. If the predefined conditions available for a resource aren't appropriate, you can create custom conditions using access groups and rules. For information about access groups, see the Access Groups chapter. If you need additional help, contact Oracle Support.
All values	Use to include all data from the data resource in the data set.

9. Complete the remaining fields, which depend on the selected combination of database resource and data set values.
10. In the **Actions** field, select the actions to which this data security policy applies.
11. Click **OK** to save the data security policy.

    You can view the new policy on the Data Security Policies page by scrolling to the end of the list of policies.

Related Topics

- Overview of Data Security Configuration
- Create Job and Abstract Roles

Manage Database Resources

Data security policies secure your database resources. You can configure database resources if you want to define and secure a new database resource, or if the predefined data security conditions for a database resource don't meet your needs.

Using the Manage Database Resources and Policies page of the Security Console, you can:

- Define a new database resource
- Create data security policies to secure a new database resource

- Create database resource conditions for a database resource

To perform the tasks in this topic, you must have the IT Security Manager job role.

Note: It's recommended that you use custom access groups to configure your users access to data whenever possible. Access groups provide better performance than custom data security policies and are easier to manage. Use the procedures in this topic to configure data security only if your requirements can't be achieved using access groups. For additional information about access groups, see the Access Groups chapter.

Define Database Resources

A database resource is a database table or view that corresponds to a business object. When you create a custom business object that you want to secure, you must define its associated database table or view as a database resource. To define a table or view as a database resource, you must:

- Specify the primary key column of the database resource
- Filter columns of the database resource to exclude columns from being included in the row instance sets that can be made available to users through data security policies
- Identify conditions and actions for the database resource to determine what portions of the resource you can secure with data security policies and the operations that can be performed on the data

The following procedure describes each of these tasks.

To define a new database resource:

1. On the Security Console Administration tab, select the General subtab, then click **Manage Database Resources**.

   The Manage Database Resources and Policies page is displayed.
2. In the Search Results region, click the Create icon.

   The Create Database Resource page is displayed. The General Information subtab is selected by default.
3. Enter the values for the new database resource.

   The following table describes the field values to specify for the new database resource.

Field	Value
Object Name	The name of the custom business object you want to define as a database resource.
Display Name	The display name of the business object.
Data Object	Select the data resource (table or view) that the custom business object represents. When you select a value for the **Data Object** field, the Primary Key Columns and Filter Column Details areas are displayed.
Module	Select the user module associated with the resource.

4. Click the **Function Security Enabled** check box if functional security policies have been defined for the business object.
5. In the Primary Key Columns area, click the Create icon.
6. In the **Primary Key** field, select the primary key column of the database table or view that the business object represents.
7. In the Filter Column Details area, select columns you want to exclude from the row instance sets defined by data security policies. The data from filtered columns isn't accessible by users. To select a column as a data filter, move it from the Available Columns list to the Selected Columns list.
8. Click the Condition subtab to create conditions for the new database resource, then click the Create icon.

   The **Create Database Resource Condition** dialog box is displayed. Conditions specify the rows of the database resource that can be secured by data security policies.
9. Create resource conditions as described in the procedure Creating Conditions for a Database Resource later in this topic.
10. Click the Action subtab.

    You define actions on the database resource to specify the operations data security policies can secure on a business object. For example, you can specify whether a user might have read, update, or delete access by naming actions for each of these and granting them in a data security policy to a particular role. An action must correspond with an operation that the business object implements.
11. Click the Add Row icon.
12. Enter a value in the **Name** and **Display Name** fields. The action name you enter must match an operation name defined for the corresponding business object. Actions act on the row instance sets specified by the database resource conditions that you define in a data security policy, that is, conditions determine the row instance set available to a user for a given action.

    You can specify more than one action.
13. Click **Submit**.
14. When the confirmation dialog box is displayed confirming that the database resource was created, click **OK**.

Create Conditions for a Database Resource

Database resource conditions define what portions of a database resource can be secured by data security policies. You can't edit the predefined conditions provided by Oracle but you can create new conditions for a predefined database resource or for a database resource you've created.

A condition is a group of row instances that are determined by a simple XML filter or an SQL predicate (WHERE clause) that queries the attributes of the resource itself. You can define a condition to specify multiple row instance sets using an SQL WHERE clause with parameters. You don't need to define a condition for single row instance conditions (single value) or for all row instance conditions (all values). Both the single-value case and the all-values case can be easily defined when you create the data security policy.

> **CAUTION:** It's recommended that you avoid creating custom SQL predicates because they can have a negative impact on application performance. If you do use custom SQL predicates, you are responsible for creating and maintaining them yourself.

To create conditions for a database resource:

1. On the General subtab of the Security Console Administration tab, click Manage Database Resources.

   The Manage Database Resources and Policies page is displayed.

2. Search for the database resource whose conditions you want to edit.
3. In the Search Results list, select the appropriate database resource, then click the Edit icon.

   The Edit Data Security page is displayed.
4. Select the Condition subtab to define a new condition for the resource.

   Any existing conditions defined for the database resource are displayed. You can't delete or edit any predefined conditions.
5. Click the Create icon.

   The **Create Database Resource Condition** dialog box is displayed.
6. Enter a name and display name for the condition.
7. For the **Condition Type**, select one of the following:
   - Select **Filter** if you want to use the attribute picker to define a simple condition. If you select the filter condition type, you also must specify the following values:
     - For the **Match** option, select the **All** option if you want the filter conditions to include AND clauses or select the **Any** option if you want the filter conditions to include OR clauses.
     - In the Conditions area, click the Add icon.
     - Define the filter values.

       The following table describes the filter values for each field.

Field	Value
Column Name	Select the column for which you're defining the filter.
Tree Operators	Select this option if the operator you want to use in the filter is a tree operator.
Operator	Choose the operator for the selected column filter.
Value	Enter a value as the test for the operator. If you specified the Tree Operators option, click the Search icon. The **Select Tree Node** dialog box is displayed allowing you to choose the operator value.

     - Click **Save**.
   - Select SQL Predicate if you know the attribute names of your condition and you want to use an SQL predicate consisting of a query on the table or view named by the database resource. Enter the SQL values in the **SQL Predicate** field.
8. Click **Save** to save the new condition.

Create a Data Security Policy for a Database Resource

When you register a new business object as a database resource, users will initially be prevented from initiating the operations of the business object or from accessing the data of the resource. You define data security policies to make the data of a custom business object available to the users of the application.

Before you create a data security policy, make sure that the following tasks have been completed:

- Identify the business object that you want to secure and register its associated database table or view as a database resource.
- Identify and define any conditions that you want to make available for the database resource.
- Identify and register the actions that you want to secure for this database resource.

To create a policy for a database resource:

1. On the General subtab of the Security Console Administration tab, click Manage Database Resources.

   The Manage Database Resources and Policies page is displayed.
2. Search for the database resource that you want to secure by defining a policy.
3. In the Search Results list, select the database resource, then scroll down to the Policies Details area.

   All the policies defined for the database resource are displayed.
4. You can select an existing policy for editing by selecting the policy then clicking the Edit icon. In this case, however, click the Create icon to create a new policy.

   The **Create Policy** dialog box is displayed with the General subtab selected.
5. Specify the following information for the new policy:
   - In the **Name** field, enter a name for the policy.
   - In the **Start Date** field, enter the date on which the policy is to become active.

   The **Module** field is pre-filled with the name of the module associated with the database resource for which you're creating the policy but you can change this value.
6. Click the Role subtab, then click the Add icon to select the roles that are to be assigned the new policy.

   The **Select and Add: Roles** dialog box is displayed.
7. Select the roles to be assigned the new policy as follows:
   - In the **Role Name** field, enter the name of the role.
   - In the **Application** field, enter the application stripe of the role, for example, CRM, HCM, or FSCM, then click **Search**.
   - Select a role from the list of roles displayed, then click **Apply** to associate the role with the new policy.
   - Select any additional roles from the list and, when you have finished adding roles, click **OK**.

   All users assigned the roles you select are provided with access to the data defined in the policy.
8. Click the Rule subtab to define a rule to specify the rows of the database resource to which the policy applies.
9. Select one of the following values in the **Row Set** field:
   - To secure a specific row, select **Single Value**, then search for and select the row you want to secure in the **Row** field.
   - To secure all rows in the resource, select All Values.
   - To secure a subset of the data in the data resource select Multiple Values, then search for and select the condition that defines the subset of the data to be secured in the **Condition** field.
10. Click the Action subtab, then move actions from the Available Actions list to the Selected Actions list to specify the actions, applicable to the data secured on the database resource, which you want to grant to the role.
11. Click **Save and Close**.

19 Access Groups

Overview of Access Groups

Use access groups to provide sales resources with additional access to sales object data. Access groups are an alternative way of granting data permissions to users, and they use a different access path to that provided by the predefined data security policies.

An access group uses the access control list model. You create an access group, assign users to the access group and all group members are given access to standard or custom object data. You define object sharing rules which provide users with access to the specific records of an object. These rules specify the type of access to an object to be provided and the conditions under which the access is provided. For example, users might be granted access to:

- All opportunities with a status of Open
- All accounts where country is set to UK

You can also define the type of data access provided, for example, Full access or Read access.

A user can be assigned to one or more access groups and will have the access assigned to each group. So if Lisa Jones is assigned to Access Group A, which provides access to opportunities, and Access Group B, which provides access to Accounts, she receives the access provided by both groups. You can also use one access group to assign access to multiple objects.

Objects That Support Access Groups

You can create access groups to provide data access to these objects:

- Account
- Activity
- Activity Assignee
- Asset
- Business Plan (includes Sales Objective)
- Campaign
- Category
- Contact
- Contests
- Conversation
- Conversation Message
- Custom objects
- Deal Registration
- Duplicate Identification Batch
- Duplicate Resolution Request
- Forecast Territory Details

- Goals
- Goal Participants
- Household
- HR Help Desk Request
- Internal Service Request
- KPI
- MDF Budget
- MDF Claim
- MDF Request
- Message
- Note
- Opportunity
- Partner
- Price Book Header
- Product
- Product Group
- Program Enrollments
- Quote and Order
- Resource
- Sales Lead
- Sales Quota Plan
- Sales Resource Quota
- Sales Territory
- Sales Territory Proposal
- Service Request
- Work Order

Note: When you provide users with access to the records of a top-level object using access groups, users automatically receive the same access to the records of any child objects.

Access Group Privileges

Users assigned the Manage Group Access privilege (ZCA_MANAGE_GROUP_ACCESS_PRIV) can create and manage access groups. By default, the Sales Administrator job role and the IT Security Manager job role have this privilege.

Users must be assigned a duty role, the Access Groups Enablement role, to get the access provided through access groups. By default, users assigned any of these roles have this privilege:

- Resource abstract role
- Any of the predefined sales and service job roles
- Any custom job roles that you create

CAUTION: Don't make any changes to the predefined data security policies assigned to the Access Groups Enablement duty role. Changing or deleting these data security policies prevents the access groups functionality from working correctly.

Types of Access Groups

There are two types of access groups: Custom (the ones you create) and System (the ones Oracle provides).

- Custom access groups

  Custom access groups are groups you create to provide users with access to data according to the needs of your business. You can add members to these groups, define rules to specify the access that group members should have to object data, and edit or delete the groups as required.
- System access groups

  These are access groups Oracle creates for you. A separate group is created for each of the predefined job roles in your environment and for the Resource abstract role. Predefined object sharing rules associated with each group provide the same access to data as is provided by the predefined job roles. The predefined rules are active and enabled for each group by default.

  A system access group is also created for each of the custom job roles in your environment, but these system groups aren't associated with predefined rules. You can manually add predefined or custom rules to these system groups as required.

  You can't edit, create, or delete system access groups. You also can't add members to or delete members from these groups. Users are automatically added to or removed from system groups according to the job roles that they're assigned.

On the Access Groups UI, the Type field indicates whether a group is a system group or a custom group. Custom groups are displayed by default. You can choose the type of group you want to view from the List drop-down list.

How Access Groups Work with Other Security Mechanisms

You use access groups to supplement the data access users receive through their job roles and other security mechanisms.

When you configure users' visibility to data using access groups, keep in mind that if you want only the access path provided by the group membership to take effect, you might also have to remove the access granted to group members by custom or predefined data security policies. If you don't remove these other access paths, users will have the data visibility granted both by the access group and by existing data security policies they're assigned through record ownership or team membership, or through territory management setup.

Example of How Access Groups Interact with Other Security Mechanisms

The following example illustrates how the different security mechanisms work together.

Let's say Lisa Jones, who's assigned the Sales Representative job role, requires access to all opportunities in Germany for a specific project. Currently, Lisa can only access a subset of German opportunities through her team and territory membership. Lisa's manager, Mateo Lopez, doesn't need access to the additional opportunities in Germany.

To provide Lisa with the additional access that she needs:

1. Create an access group and add Lisa Jones as a member of the group. Don't add Mateo Lopez to the group.
2. Create an object sharing rule for the access group that includes a condition similar to the following:
   Access all opportunities where country = Germany

Lisa can now access all opportunities in Germany. Which opportunities can Mateo now access? Mateo Lopez isn't a member of the access group, and access groups don't provide access through the resource hierarchy by default, so Mateo can't access the additional opportunities in Germany through Lisa's access group membership.

Lisa's manager can only access opportunities through the resource or territory hierarchy where Lisa is on the sales team, the account team, or the territory associated with the opportunity.

- If Lisa isn't on the team or territory of the opportunities that she gets access to through her access group membership (all opportunities in Germany), then Mateo still can't access those opportunities.
- If Lisa is on the team or territory of some of the opportunities in Germany, then both Mateo and Lisa have access to that subset of opportunities through the standard security mechanisms, regardless of Lisa's access group membership.

Access Groups and Functional Privileges

You can use access groups to give users additional permissions at the data security level. You can't use access groups to provide functional security access privileges. Consider the example of a user assigned a job role which provides the functional privilege to view leads, but not the functional privilege to delete them. If you assign the user to an access group that specifies rules that provide delete lead and view lead data access, the user will be able to view leads but without the delete functional privilege, they still won't be able to delete leads.

Considerations in Deciding When to Use Access Groups

You can extend a user's visibility to sales object data in a number of ways:

- By creating custom data security policies, assigning the custom policies to custom roles, and then assigning the custom roles to users.
- By using Territory Management to set up territories and to assign users to territories, then using Assignment Manager to assign territories to object records.
- By creating access groups and assigning users to the access group.

So which factors should you consider when deciding which option to choose? This topic provides you with some guidelines.

Custom Data Security Policies

In situations where you can use either access groups or custom data security policies to provide users with data permissions, use access groups for these reasons:

- Access groups provide better performance than custom data security policies.

- You can search for records assigned to users through their access group membership in Workspace. Records assigned to users through custom data security policies can't be searched in Workspace.
- Access groups are easier to manage.

Access Groups

Access groups work together with the existing access mechanisms to allow you to provide access to users based on parameters that aren't provided by the standard access framework, such as the user's context (country or sales region, for example), the user's resource organization or business unit, or some other attribute.

You can also use access groups to assign access based on custom attributes. For example, you can assign all users in a specific business unit to a group and then grant that group read permissions to opportunities.

Territory Management

You can use Territory Management to manage users' visibility to data. However, Territory Management isn't a security access mechanism. It's a way of assigning sales representatives to sales territories to enable optimal sales coverage. Territory Management is used to configure access primarily to facilitate the selling process by defining boundaries using hierarchical attributes, such as products, geographies, industry, and so on.

Use territory management functionality to extend visibility to data in these scenarios:

- If you want to use forecasting or quota management functionality.
- If the territory hierarchy and territory-based reporting and roll-ups are different to the reporting resource hierarchy.
- If you want to provide users with access based on hierarchical attributes and named accounts.

If you want to provide users with access using a standard mechanism, such as territory or management hierarchy, then use Territory Management. Otherwise, use access groups.

> **Note:** After you've implemented Territory Management, you can optionally use access groups to manage your territories. You can define custom rules for the Sales Territory or Sales Territory Proposal objects and assign them to custom access groups to specify who can manage the territory or territory proposal. For example, you can create rules for country-specific administrator access groups that allow the group members to view all territories in their country but not edit or delete the territories.

Overview of the Access Groups UI

You create and manage access groups and object sharing rules using the Access Groups UI in the Sales and Service Access Management work area.

The Access Groups UI includes 3 tabs: the Access Groups tab, the Object Rules tab, and the Monitor tab.

- Access Groups tab

  Displays the main Access Groups page. From here, you can review all the existing custom or system access groups, you can create custom access groups, review or add group members, and review or enable the rules assigned to a group. You can also add new rules to a group.
- Object Rules tab

Displays the main Object Sharing Rules page. From here, you can review all the rules defined for a selected object, you can create or delete object sharing rules and access extension rules, and you can assign rules to access groups.

- Monitor tab
  Displays the Monitor page which provides an overall view of all the scheduled processes that are run for access groups. You can check the status of active processes, start or cancel processes, or update the schedule for a process from the Monitor page. Having all the access group processes grouped on a single page makes it easier to monitor them and take action when needed.

You can manage your groups and rules on an on-going basis using either the Access Groups page or the Object Sharing Rules page, depending on whether you want to work with access groups from an access group context or an object sharing rules context.

For example, reviewing rule information from a rules context is useful if you decide to delete an object sharing rule you previously created and want to first check the rule isn't assigned to active groups. Similarly, reviewing rule information from a group context is useful if, for example, you want to review all the predefined rules assigned to a specific system group.

Create and Manage Custom Access Groups

Create a Custom Access Group

This topic guides you through the main steps in the process of creating an access group and providing group members with access to object data.

It describes these tasks:

1. Create an access group.
2. Create object sharing rules to give group members access to object data.
3. Add members to the group.

More detailed information about each task is available in other topics in the chapter.

> **Note:** You must be assigned the IT Security Manager job role or the Sales Administrator job role to create and manage access groups.

Step 1. Create an Access Group

Once you have identified a group of resource users that require additional access to object data, create an access group for those users.

1. Sign in to the application as the sales administrator or as a setup user.
2. In the Setup and Maintenance work area, go to the following:
   a. Offering: Sales
   b. Functional Area: Users and Security
   c. Task: Manage Sales and Service Access

   Alternatively, click **Navigator** > **Tools** > **Sales and Service Access Management**.

If you you have the Sales Administrator job role, the Access Groups page in the Sales and Service Access Management work area is displayed. If you have the IT Security Manager job role, the Sales and Service Access Management main page is displayed with the Configure Groups tab selected to display the Access Groups page.

The Access groups page lists any existing, active access groups. You can view all access groups (active and inactive) by selecting **All Groups** from the **List** drop-down list. You can also search for an existing group on this page.

3. Click **Create** to display the Create Access Group page.
4. Enter the values shown in the following table:

Field	Value
Name	Enter a name for your group. For example, if you're creating a group to give sales support users access to all open opportunities, you might name the group **Opportunity_Open**.
Description	Enter a description for your group (optional). For example, **Access to open opportunities**.
Active	Select a status for the new group. By default, the status for new groups is inactive. Click the **Active** check box to activate the group.

5. Click **Save and Continue** to save your new group.

   The Edit Access Group: Overview page is displayed for the group. From here, you can edit the access group details or delete the access group.

Step 2. Create Object Sharing Rules for the Group

Next, create object sharing rules to grant group members access to object records.

1. On the Edit Access Group: Overview page select the **Object Rules** tab.
2. To create a new rule, click **Create Rule**.
3. On the Create Object Sharing Rule page, select the object you're creating the rule for from the **Object** drop-down list. For example, select **Opportunity**.
4. Enter a **Name** for your new rule, for example, **Opportunity_Open**. You can optionally enter a rule **Description**.
5. In the **Access Level** field, select the type of object access you want to give group members, either **Read**, **Update**, **Delete** or **Full** access.
6. Make sure that the **Active** check box for the rule is checked.
7. In the Conditions area, specify the rule conditions.

   For example, you might specify that group members have access to opportunity records that have a **Status** attribute equal to **Open**.
8. Select **Save and Publish** from the **Actions** menu to publish the rule so it's available for assignment processing.
9. When the status indicator shows the publish process has completed, select **Save and Close** from the **Actions** menu, then select **Save and Close** to return to the main Access Groups page.
10. If this is the first custom rule you've created, you must also publish the new rule on the Object Sharing Rules page. To do this, select the Object Rules tab, then select **Publish Rules** from the **Actions** menu.

    For any subsequent rules you create, this step isn't required. You only have to publish the rule once as described in step 8.

11. Now run the Perform Object Sharing Rule Assignment Processing scheduled process to ensure that the object sharing rules for each object are assigned properly.

For detailed information about creating object sharing rules, see *Manage Object Sharing Rules for Access Groups* in this chapter.

Step 3. Add Members to the Group

Finally, add resources to your new, custom access group. You can add users to the group in a number of ways: manually add users on the UI, create group membership rules to automatically add users, or use the standard import and export functionality to add users.

Here are the steps to create group membership rules to add users to your group.

1. On the Edit Access Group: Overview page, click the **Member Rules** tab.
2. Click **Create Rule**.
3. On the Create Group Membership Rule page, enter a **Name** for the rule, for example, **Sales_Support_Resources**.
4. Optionally, enter a rule **Description**.
5. Select the rule conditions. The conditions determine which resources are added or removed as members of the group.

   For example, you might specify that all resources that have an **Organization** attribute equal to **Sales Support** are added to the group.
6. Select **Save and Publish** form the **Actions** menu to publish the rule, then click **Save and Close** from the **Actions** menu.
7. On the Edit Access Group: Overview page, click **Save and Close** to save the group details.

   On the Access Groups page, check that your new group is included in the list of groups.
8. Now run the Run Access Group Membership Rules scheduled process to ensure that the access group membership rules are assigned and resources are added to the group.

   The Run Access Group Membership Rules scheduled process automatically runs every hour to update access groups with changes to the group membership. But, you can also run the process at any time from the Access Groups main page by selecting the **Update Groups and Members** option from the **Actions** menu.

   Once the rules you created for your new access group are processed, all the users in the Sales Support organization will have access to all open opportunities.

   For more detailed information about the different methods of adding users to custom access groups see *Add Members to Custom Access Groups* in this chapter.

For an example of how to assign access to sales objects to groups of users on the basis of the users' home country, see *Assign Group Access By Country*.

Edit Access Groups

After you create a custom access group, you can edit the group details. For example, you might want to activate a group, add new object sharing rules for the group, or add or remove group members.

You can also edit system access groups to configure the rules assigned to the group.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. Select the access group whose details you want to edit from the groups listed.

Custom access groups are displayed by default, so if you want to edit a system access group, you first have to select **System Groups - Role** from the **List** drop-down list. You can also choose to list all access groups or just active groups.

Details relating to the group and its members are listed on the Edit Access Group: Overview subtab.

3. What you can do depends on whether you're editing a custom or a system group.
    - System groups

      For system groups, you can review the group details and members on the overview subtab, but you can't change any of the information and you can't delete the group. System groups are predefined by Oracle and are automatically created and updated to reflect the job roles and user-job role assignments in your environment.
    - Custom groups

      Here's what you can do from the overview page for custom groups:

        - Change the group name or description.
        - Activate or inactivate a group.

          If you inactivate a group, group members lose any data access provided by the group.
        - Add group members by clicking **Add Members**.
        - Remove all group members who were added to the group manually by clicking **Remove Members**, or delete individual members from the group by clicking the **Remove** icon in the member row.

          > **Note:** Members who were added through group membership rules can't be removed.

        - Delete the group by selecting **Delete Group** from the **Actions** menu.

          For information about deleting groups, see *Delete a Custom Access Group*.

4. Click the **Object Rules** subtab to view any predefined or custom object sharing rules defined for the group.

   You can make these changes for both system and custom access groups:

   - Enable or disable a predefined or custom rule for the access group by selecting or deselecting the **Enable** check box.
   - Remove a custom rule or a predefined rule you added to the access group. Click the rule and on the Edit Object Sharing Rule page, select **Delete** from the **Actions** menu.

     The rule is deleted for the group you're editing, but not for any other groups that the rule is associated with.
   - Add a preexisting rule to the access group. Click **Add Rule**, and then, in the search dialog box, search for and select the rule you want to add.
   - Create a new rule for the access group. Click **Create Rule**, and then define the new rule in the Create Object Sharing Rule page.
   - Change the access level provided by the rule for this group by selecting a new value from the rule's **Access Level** drop-down list.

   > **Note:** If you're editing a system access group, a **Lock** icon is displayed for any predefined rules that are associated with the group as part of the default security configuration. For these rules, you can't change the access level for the group and you can't remove the rule from the group. The only change you can make is to enable or disable the rule for the group.

   For information on object sharing rules, see *Create Custom Object Sharing Rules*.
5. Click the **Member Rules** subtab to view any group membership rules defined for the access group.

   > **Note:** You can't add members to system groups using group membership rules, so the Member Rules subtab isn't available for system groups.

   You can edit an existing rule from the Member Rules subtab by clicking the rule name link, or you can create a new rule by clicking **Create Rule**.

   If you select an existing rule to edit, the Access Group: Edit Group Membership Rule page appears, where you can edit or delete any of the rule details. For information on group membership rules, see *Create Membership Rules for Custom Access Groups*.
6. When you're finished editing the group details, click **Save and Close**.

   Changes you make to object sharing rules or group membership rules are processed when the Object Sharing Rule Assignment Process or the Access Group Membership Rules Process is next run.

Delete a Custom Access Group

You can delete a custom access group if you have the Delete Access Group privilege.

By default, users assigned the IT Security Manager job role have this privilege. Sales Administrators aren't provided with the Delete Access Group privilege.

> **CAUTION:** Once you delete a group and its members, you can't reactivate it. The users who were assigned to the group still exist, but they're no longer associated with the group, and group members lose any data access provided by the group.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. Select the access group you want to delete from the groups listed.

   On the Edit Access Group: Group_Name page, select **Delete Group** from the **Actions** menu.
3. In the confirmation dialog, click **Yes** to confirm your choice.

   The group is deleted and is no longer available on the Access Groups page.

Add Members to Custom Access Groups

Options for Assigning Members to Custom Access Groups

You can assign users to a custom access group when you create the group or you can add members later. You can't assign users to system access groups. You can add members to a custom access group in these ways:

- Manually add members to a group on the Edit Access Group: Overview page. This option is useful if you only need to add a few users to a group on an ad-hoc basis.
- Create access group membership rules. Users who meet the conditions specified in the rule are automatically added to a group. Using group membership rules, you can add a large number of users to a group at once and simplify the process of maintaining the group's membership in the future. Users are added or removed from the group automatically depending on whether or not they meet the rule conditions.
- Assign users to groups using the standard import and export functionality. If you have large numbers of users to assign to one or more access groups on a one-off basis, you can import users and groups.

You can assign a user to one or more access groups and the user will have the data access permissions assigned to each group.

Member Types

Access group members are categorized into member types according to how they're added to an access group:

- Manual members

  Users who are added to the group manually, either through the UI or through file import
- Rule members

  Users who are added to the group through rule processing

You can delete access group members on the Edit Access Group: Overview page if they were added to the group manually. Group members added through rule processing can't be manually removed from a group; they're only removed from a group if they no longer meet the rule conditions.

If a user is added to an access group more than once, manually and through group membership rule processing, the user is listed twice on the Edit Access Group: Overview page. You can delete the manual entry for the user but the user remains a group member provided they still satisfy the access group membership rule conditions.

For information about creating access group membership rules, see *Create Access Group Membership Rules*. For information about importing access groups and members, start with *Overview of Importing and Exporting Access Group Objects*.

Add Members to Custom Access Groups Using the UI

You can manually add resource users to a custom access group at any time using the Access Groups UI.

1. Navigate to the Access Groups page (**Navigator** > **Tools** > **Sales and Service Access Management**).
2. On the Access Groups page, select the group you want to add members to.
3. On the Edit Access Group: Overview page, click **Add Members**.
   The Add: Group Members page is displayed.
4. Search for the user you want to add using one of the search fields.
   For example, in the **First Name** field, enter the first 3 characters of a user's first name and click **Search**. Or in the **Role** field, select a resource role to view all users assigned that role.
   If you create a custom field for the Resource object, for example, Country, you can use Application Composer to expose the field so that it's available as a drop-down list on the Add: Group Members UI. You can then search for resources using this field. In this example, you can search for users by country.
5. In the Search Results area, select each of the users you want to add to the group and click **Apply**.

   > **Note:** You can only assign users to access groups who are assigned the Resource abstract role (ORA_HZ_RESOURCE_ABSTRACT).

6. Search for and select any additional members you want to add to the group and, when you're finished adding members, click **OK**.
7. Verify that all the members you added to the group are listed in the Group Members area of the Edit Access Group: Overview page.
8. If you want to remove a member, click the **Remove** icon in the member row. To remove all members of the group who were added manually, click **Remove All Members**.
9. Click **Save and Close** to save the group membership details.

How do I create membership rules for custom access groups?

You can add resource users to a custom access group by defining one or more group membership rules. Each rule consists of conditions that determine which resources are added as members of the group.

Any users who satisfy the conditions are automatically added to the access group. Group members who no longer meet the conditions are automatically removed from the group. You can't manually remove group members added through group membership rule processing.

Here's how you can create a group membership rule to add members to your access group:

1. On the Access Group page, select the group you're creating the membership rule for.
2. On the Edit Access Group: Overview page, select the **Member Rules** tab, then click **Create Rule**.
3. On the Access Group: Create Group Membership Rule page, enter a **Name** for the group membership rule and a **Description** if required.
4. In the Conditions section, specify the rule conditions.
   Each rule consists of one or more conditions that are evaluated individually. You can choose whether the rule action applies if any conditions are met, or only if all conditions are met, by selecting the appropriate value from the **Rule Applies If** list.
5. Enter a rule condition by clicking the **Add** icon and enter the values shown in the following table:

Field	Description
Object	Select either the **Resources** object or the **Resources Hierarchy** object. Only resource users can be added to an access group, so you can only select one of these objects.
Attribute	Select an attribute from the list. Both custom and standard attributes defined for the object you selected are listed. Support for a number of resource object attributes will be discontinued in future releases. So to prevent issues in the future: o Avoid using these attributes: User Account Status, Company, Phone, Job Title, Manager First Name, Manager Last Name, Organizations, Teams, Usages o Use custom attributes that are based on database columns only. Avoid using custom attributes, such as attributes based on the Formula field, that aren't based on database columns. Support for attributes that aren't based on database columns will be deprecated in future releases.
Operator	Select the operator for your condition. For example, **Equals** or **Is blank**. **Tip:** If an attribute can have multiple values, such as the Roles or Teams attributes, use the Contains operator instead of the Equals operator to make sure that the condition adds all the intended resources to the group. For example, if you create a rule, Roles Equals Salesperson, then users who are assigned only the Salesperson role are added to the group. If you create a rule, Roles Contains Salesperson, then users assigned the Salesperson role and any other role are also added to the group.
Value	Enter a value for the attribute, if relevant. If you're entering more than one value, separate each value with a comma.

Enter as many conditions as needed to suit your specific requirements. For example, if you want to add all resources who are sales representatives based in the Sales Support organization to your group, create two conditions with values similar to these and choose the **All conditions met** value from the **Rule Applies If** drop-down list.

This table lists example values for the fields in a rule condition:

Field	Condition 1	Condition 2
Object	Resources	Resources
Attribute	Job Title	Organization

Field	Condition 1	Condition 2
Operator	Equals	Equals
Value	Sales Representative	Sales Support

6. From the **Actions** menu, select **Save and Publish** to ensure that your changes get included in the assignment processing.
7. Click **Save and Close**.
8. Start the Run Access Group Membership Rules scheduled process to ensure that the access group membership rules are assigned.

   The Run Access Group Membership Rules scheduled process automatically runs every hour to update access groups with changes to the group membership. But you can also run the process at any time from the Access Groups main page by selecting the **Update Groups and Members** option from the **Actions** menu. For example, if you edit a rule, it's a good idea to run the process straight away.

   When the process completes, navigate to the Edit Access Group: Overview page where you can see that all the resources who meet the rule conditions are added to the group. Notice that the Member Type field is set to `Rule` for all the new members.

You can edit a group membership rule at any time by selecting the rule from the Edit Access Group: Group Membership Rules page. You can also delete or inactivate the rule. If you delete or inactivate a rule, any users added to the group through the rule are removed when the Run Access Group Membership Rules scheduled process is next run.

For information about running scheduled processes, see the Understanding Scheduled Processes guide.

Related Topics

- Understanding Scheduled Processes

Manage System Access Groups

Overview of System Access Groups

System access groups and rules provide users with access to object data on the basis of the job and abstract roles that users are assigned.

If you're using the sales application for the first time in Update 22B or later, system access groups and their associated object sharing rules are used to manage users' access to data by default. If you were provisioned with Oracle Sales or Fusion Service before Update 22B, it's recommended that you use system groups and rules instead of data security policies to manage data access.

Oracle creates two types of system access groups for you:

- Groups for predefined roles. An access group is generated for each of the predefined sales and service job roles in your environment and for the Resource and Authenticated User abstract roles.
  Predefined object sharing rules are assigned to each group. The rules provide group members with the access to the data that they require. These predefined rules are active by default.
- Groups for custom roles. An access group is generated for each of the custom job roles in your environment. The access groups generated for custom roles aren't associated with object sharing rules. You must manually add predefined or custom rules to these groups. You can also copy rules from another access group, such as the access group generated for the source role you copied, to provide group members with access to data.

On the UI, you can distinguish between the two types of system access groups as follows:

- **ORA_ prefix**: The numbers assigned to system access groups generated for predefined job roles or for the Resource and Authenticated User abstract roles start with the ORA_ prefix. The numbers assigned to access groups generated for your custom job roles don't include the ORA_ prefix.
- The **Predefined** check box is checked for system access groups generated for the predefined job roles and for the Resource and Authenticated User abstract roles. This check box isn't checked for groups that are generated for your custom job roles.

System Access Group Members

Any user you assign to a predefined or custom job role is automatically included as a member of the associated system access group. All authenticated users, including users who aren't resources, are also automatically added to the All Users system access group. You can use the All Users system access group to provide all authenticated users of your application with access to object records.

> **Note:** System access groups are generated only for job roles that have at least one user associated to them. If no users are assigned a specific job role, a system access group isn't generated for the role.

The Refresh Access Control Data process automatically runs every hour to update system groups with changes to the custom job roles and user-job role assignments in your environment. But you can also run the process at any time from the Access Groups main page by selecting the **Update Groups and Members** option from the **Actions** menu.

What Changes Can You Make to System Groups?

You can add additional predefined or custom object sharing rules to system groups.

However, you can't create new system groups or delete existing system groups. You also can't add or delete members of system groups, either manually, through group membership rules, or through import and export functionality. Users are automatically added to, or removed from, system access groups according to the job roles they're assigned.

System Groups and Predefined Rules

Each system access group for a predefined job role is associated with predefined object sharing rules that provide group members with the access to data required for their job roles.

The association between system groups and predefined rules is part of the default security configuration and can't be changed. If you're using the sales application for the first time in Update 22B or later, this association is enabled by default and your users automatically receive data access through their membership of access groups.

If you were provisioned with the sales application before Update 22B, your users receive data access through the data security policies assigned to their job roles, or through a combination of data security policies and access group rules, if you've configured one or more access groups or object sharing rules. If you want to replace data security policies with access group rules as the method used to provide your users with data access, you must migrate your data security policies to use access groups.

For information on migrating your data security policies to access group rules, start with *Migration Overview*.

> **Note:** System groups created for custom job roles, and the All Users system group that includes all authenticated users of the application, aren't associated with any object sharing rules. You add the rules you want to assign to these groups manually.

Objects Supported for Predefined Rules

Predefined rules aren't currently available for all sales objects. You can now use predefined rules to provide access to data for these objects:

- Account
- Asset
- Activity
- Activity Assignee
- Business Plan
- Campaign
- Contact
- Contests
- Custom objects
- Deal Registration
- Duplicate Identification Batch
- Duplicate Resolution Request
- Forecast Territory Details
- Goals
- Goal Participants
- Household
- HR Help Desk Request
- Internal Service Request
- KPI
- MDF Budget
- MDF Claim
- MDF Request
- Note
- Opportunity
- Partner

- Price Book
- Product
- Product Group
- Program Enrollment
- Quota Plan
- Quote and Order
- Resource
- Resource Quota
- Sales Lead
- Sales Territory
- Sales Territory Proposal
- Service Request

Related Topics

- System Groups and Predefined Rules for Custom Objects

Manage Object Sharing Rules for Access Groups

Overview of Object Sharing Rules

Object sharing rules provide access groups with access to an object's records. There are three types of object sharing rules:

- Object sharing rules

  Standard object sharing rules specify the type of object access to be provided, the conditions under which the access is provided, and the access groups to share the rule with.

- Hybrid object sharing rules

  A hybrid rule is an object sharing rule that combines a predefined rule condition with one or more custom rule conditions. Use hybrid rules to restrict the access provided by a predefined condition.

  You can enable or disable the creation of hybrid rules using a profile option. For information, see *Enable Hybrid Object Sharing Rules*.

- Access extension rules

  These rules extend the object sharing rules defined for one object to a related object. You can use both predefined and custom object relationships in an access extension rule.

For information about creating and editing each type of rule, see the relevant topics in this chapter.

There are also two categories of object sharing rules:

- Custom rules you create to configure data access for members of access groups. You can create these types of rules:

- Standard object sharing rules
- Hybrid object sharing rules
- Access extension rules

You must manually assign these rules to relevant access groups, and the rules are active by default.

- Predefined rules created by Oracle. These can be either standard object sharing rules or access extension rules.
  One or more predefined rules are assigned to each system access group that's generated for a predefined job role. These rules provide the same access to data for supported objects as the job role provides.
  On the Object Sharing Rules page, the Predefined column is checked if a rule is predefined. If the predefined rule is assigned to a system access group as part of the default security configuration, it also has a Lock icon to indicate that you can't change the association between the rule and the group, or the level of access provided by the rule to the group.
  For additional information, see *System Groups and Predefined Rules*.

Comparison of the Predefined and Custom Object Sharing Rules

There are a few differences between the object sharing rules you create and the predefined rules that Oracle provides. There are also differences in what you can do when a predefined rule is associated with a system group as part of the default security configuration and when it isn't. Some of the similarities and differences between the object sharing rules you create and the predefined rules are outlined in this table:

Custom Rules	Predefined Rules	Predefined Rules Associated to a System Group
You can create, edit, and delete the rule.	Oracle creates the rule. You can edit the rule.	You can only enable or disable the rule for the group.
Rule is active by default.	Rule is active by default.	Rule is active by default.
You can create one or more conditions for the rule.	Rule has one predefined condition which you can't change.	Rule has one predefined condition which you can't change.
You can't create rule conditions that provide either of these types of access: • Access to all of an object's records • Field-level access to object records, such as access to Personally Identifiable Information (PII) for the Contact object	Predefined rules with conditions that provide global and field-level access to object data are provided.	Predefined rules with conditions that provide global and field-level access to object data are available.
You can assign the rule to system access groups and custom access groups.	You can assign the rule to system access groups and custom access groups. **Note:** Predefined rules that provide global or field-level access to object data are an exception. You can't assign these rules to custom access groups.	NA

Custom Rules	Predefined Rules	Predefined Rules Associated to a System Group
You can change the access level provided by the rule for different custom or system groups.	You can change the access level provided by the rule for a custom access group. If a rule is predefined but doesn't have the Lock icon, you can also change the access level provided by the rule to a system group.	Can't change the access level provided by a predefined rule for a system access group.

Related Topics

- Create Custom Object Sharing Rules
- Create Access Extension Rules
- Combine Predefined and Custom Conditions in a Rule
- System Groups and Predefined Rules
- Enable Hybrid Object Sharing Rules

Object Sharing Rules Configuration Options

Overview of Rules Configuration Options

Before you begin to create custom object sharing rules, it's a good idea to review and configure the default options that determine how rules are processed and the types of rules you can use.

You can configure options that determine:

- Whether real-time or near real-time processing of object records is enabled
- Whether or not the object sharing rules assignment process is scheduled to run automatically, and how frequently the process runs
- Whether or not you can create hybrid object sharing rules; these are rules that include a predefined rule condition and one or more custom rule conditions

Review the topics in this section for additional information.

How do I configure real-time and near real-time access for access group object records?

Using profile options, you can implement real-time and near real-time processing for objects secured using access groups.

These options let you:

- Enable real-time processing of object records secured using access groups, so that when new object records are created, the records are immediately accessible on the UI to the creator of the object record.

  Real-time processing is supported for all access group objects.
- Enable near real-time processing for objects, so that when object records are created or updated, the new records are accessible in near real-time to all users who have the privileges to view them.

  Near real-time processing is supported for these objects:

- Account
- Activity
- Campaign
- Contact
- Custom objects
- Deal Registration
- HR Help Desk Request
- Internal Service Request
- MDF Budget
- MDF Claim
- MDF Request
- Lead
- Opportunity
- Partner
- Program Enrollments
- Service Request

The real-time processing options are enabled by default. However, to enable near real-time processing of object records, there are some extra steps for you to perform.

Configure Real-Time Processing of Object Records

Two profile options control the real-time processing of object records that are secured using access groups:

- Real-Time Transaction Tracking Enabled (ORA_ZCA_TRANSACTION_TRACKING_ENABLED)
- Real-Time Transaction Tracking for Access Groups Enabled (ORA_ZCA_ACCESS_GROUPS_TRACKING_ENABLED)

Both of these profile options are enabled by default at the site level so that real-time processing is enabled for all users. In general, you won't need to change the default values for these profile options, but you can disable real-time processing for all users at the site level, or for individual users at the user level, if necessary.

For example, you might want to disable real-time processing for a specific user who needs to import bulk data into the application. In cases like this, disable both profile options for the user using these steps:

1. From **Setup and Maintenance**, navigate to the **Manage Administrator Profile Values** task.
2. Search for the profile option name, for example, Real-Time Transaction Tracking Enabled.
3. In the Profile Values section, select **New** from the **Actions** menu.
4. In the Profile Level field, select **User**.
5. In the User Name field, search for and select a user, then click **OK**.
6. In the Profile Value field, select **No**.
7. Click **Save and Close**.
8. Repeat steps 2 - 7 for the Real-Time Transaction Tracking for Access Groups Enabled profile option.

Configure Near Real-Time Processing of Object Records

You can access records that are secured using access groups in near real-time, for objects that support near real-time processing. New object records are immediately available on the UI, without needing to run the Perform Object Sharing Rule Assignment Processing scheduled process, in these circumstances:

- When a new object record is created, when a user is added to or removed from the team associated with an object, or when the owner of an object record is changed
- When an object record is updated, when a user gets access to an object record through a hybrid rule, or when an access extension rule provides a user with access to an object related to the supported object

Note: Near real-time processing isn't supported for object records that are created or updated because of territory assignment processing. To see these types of changes on the UI, you must run the Perform Object Sharing Rule Assignment Processing process.

To implement near real-time processing for supported objects, both of these profile options need to be enabled:

- Near Real-Time Transaction Tracking for Access Groups Enabled (ORA_ZCA_ACCESS_GROUPS_NEAR_REAL-TIME_TRACKING_ENABLED)

  This option is enabled at the site level by default.
- Common CRM Signals Active (ORA_ZCA_ENABLE_SIGNALS).

  This option is disabled by default.

Enable the Common CRM Signals option to implement near real-time access for object records:

1. From **Setup and Maintenance**, navigate to the **Manage Administrator Profile Values** task.
2. Search for the profile option name, Common CRM Signals Active.
3. In the Profile Values section, select the **Site** profile level, then change the default value of the Profile Value field to Yes.
4. Click **Save and Close.**

Scheduling Options for Object Sharing Rules Assignment Processing

You can configure whether or not object sharing rules processing occurs automatically, and how often the process runs, using profile options.

After you create or edit an access group rule, or add a rule to an access group, you must publish the rule to make it available for assignment processing. Once an active rule is published, the *Perform Object Sharing Rules Assignment process* automatically assigns group members with the object access specified by the rule.

By default, the process is dynamically scheduled to run at regular intervals for any object that has an active rule associated with it. How frequently the process runs varies depending on whether or not near real-time processing is

enabled for an object. You can disable dynamic scheduling, or change how frequently the process runs, using these profile options:

- **Dynamic Scheduling of Scheduled Process Jobs Enabled**
  Controls whether or not dynamic scheduling of object sharing rules processing is enabled.

  > **Note:** If you disable dynamic scheduling, you must manually submit the Perform Object Sharing Rule Assignment process, or create your own schedule for running the process, to make sure access group members receive the access they need. In addition, any jobs that are already scheduled aren't canceled automatically. You have to cancel the scheduled jobs manually.

- **Frequency of Scheduled Process Jobs if Near Real-Time Processing Enabled**
  If dynamic scheduling is enabled, this option specifies how often the Perform Object Sharing Rule Assignment process runs when near real-time processing is enabled. The default value is 6 hours.
- **Frequency of Scheduled Process Jobs if Near Real-Time Processing Disabled**
  If dynamic scheduling is enabled, this option specifies how often the Perform Object Sharing Rule Assignment process runs when near real-time processing is disabled. The default value is 1 hour.
  If you require immediate access to new records and objects, you can manually submit the Perform Object Sharing Rule Assignment process to run immediately. You can also create your own processing schedule to replace or supplement the default schedule. For information, see the topic *Perform Object Sharing Rules Assignment Process*.

Related Topics

- How do I run the Perform Object Sharing Rule Assignment Process?

Configure Dynamic Scheduling of the Object Sharing Rule Assignment Process

The Perform Object Sharing Rule Assignment process is automatically scheduled to run at specified intervals by default. You can change how frequently the process runs to best suit your business needs. You can also disable automatic scheduling if required.

1. To change how frequently the Object Sharing Rules Assignment process runs, use these steps.
   a. Navigate to the Setup and Maintenance work area.
   b. Open the tasks search page and search for the task **Manage Administrator Profile Values**.
   c. On the Manage Administrator Profile Values page, do one of the following:
      - If near real-time processing of objects is enabled in your implementation, search for the profile option **Frequency of Scheduled Process Jobs if Near Real-Time Processing Enabled** (ORA_MOW_ESSJOB_FREQUENCY_WITHNRT).
      - If near real-time processing of objects isn't enabled in your implementation, search for the profile option **Frequency of Scheduled Process Jobs if Near Real-Time Processing Disabled** (ORA_MOW_ESSJOB_FREQUENCY_WITHOUTNRT).
   d. Change the value in the **Profile Value** field as required. The default values are **6** hours if near real-time processing is implemented, or **1** hour if it isn't.
   e. Click **Save and Close**.
2. To disable dynamic scheduling of the Object Sharing Rules Assignment process, use these steps.
   a. Navigate to the Setup and Maintenance work area.
   b. Open the task search page and search for the task **Manage Administrator Profile Values**.

c. On the Manage Administrator Profile Values page, search for the profile option **Dynamic Scheduling of Scheduled Process Jobs Enabled** (ORA_MOW_ENABLE_ESSJOB_DYNAMIC_SCHEDULING).
d. Change the default value of the **Profile Value** field from **Yes** to **No**.
e. Click **Save and Close**.

Enable Hybrid Object Sharing Rules

You can configure whether or not users can create hybrid object sharing rules for access groups.

A hybrid rule is a rule that includes a predefined rule condition with one or more custom rule conditions. Combining custom conditions with a selected predefined condition in a hybrid rule lets you refine the access that's provided by the predefined condition.

To enable hybrid rules, change the value of the profile option System and Custom Rule Conditions Combination Supported (ORA_MOW_SUPPORT_SEEDED_CONDITION) using these steps.

1. Navigate to the Setup and Maintenance work area.
2. Open the tasks search page and search for the task **Manage Administrator Profile Values**.
3. On the Manage Administrator Profile Values page, search for the profile option **System and Custom Rule Conditions Combination Supported**.
4. In the Profile Values section, select **Yes** in the **Profile Value** field.
5. Click **Save and Close**.

   For information on creating a hybrid object sharing rule, see the topic *Combine Predefined and Custom Conditions in a Rule*.

Create Custom Object Sharing Rules

Once you have created an access group you can create rules to provide the group with access to an object's records.

To create a custom object sharing rule, you specify the type of object access to be provided, the conditions under which the access is provided, and the groups to share the rule with. You then publish the rule to Assignment Manager. Finally, the Perform Object Sharing Rule Assignment Processing task runs to enable the resources in the associated access group to have access to the object records.

This topic describes how to create object sharing rules from an object context. But you can also create a rule in the context of a group when editing the group. For additional information see the topic Create a Custom Access Group.

Here are the steps to create an object sharing rule.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. On the Access Groups page, select the **Object Rules** tab.

   The Object Sharing Rules page is displayed. From here, you can modify an existing rule or create a new rule to share with an access group.
3. To make sure that any custom attributes or objects created in Application Composer that are enabled for access groups are available on this UI, select the **Synchronize Custom Objects and Fields** option from the **Actions** menu.

   For more information about using custom objects with access groups, see the topic Enable Access Group Security for Custom Objects.
4. Select the object you want to provide access to from the **Object** list. For example, select **Opportunity**.

For a list of objects supported with access groups, see the topic Overview of Access Groups.

5. To create a new object sharing rule, click **Create** in the Rules section.

   The Rules section lists any object sharing rules you previously created for this object and any predefined rules for the object.
6. On the Create Rule page, enter a **Name** and **Description** for the new rule.
7. New rules are set to **Active** by default. Deselect the **Active** check box if you don't want to activate the rule just yet.
8. In the Conditions section, specify the rule conditions.

   Note: The maximum number of conditions you can define for an object sharing rule is 500.
9. You can optionally select a predefined condition to use with the custom conditions you're about to create from the **Predefined Condition** list.

   The **Predefined Condition** list is only available if this functionality is enabled in your environment. For additional information on this functionality, see the topic Combine Predefined and Custom Conditions in a Rule.
10. Each condition in a rule is evaluated individually. You can choose whether the rule action applies if any custom conditions are met or only if all custom conditions are met by choosing the appropriate value from the **Rule Applies If** list.
11. Enter your first condition. For example, if you want to give group members read access to all opportunities associated with their home country, create a rule with values similar to these:

Field	Value
Object	Opportunity
Attribute	Country (this is a custom field for the Opportunity object)
Operator	Equals
Value	UK

Here are some considerations to keep in mind when selecting the attributes to use in rule conditions.

- By default, not all of the standard attributes for an object are displayed on the Access Groups Create Rule or Edit Rule UIs. To make additional standard attributes available for an object, follow the steps in the topic Enable Additional Attributes for Access Group Object Sharing Rules.
- Support for the object attributes listed in this table will be discontinued in future releases. When creating conditions, it's a good idea to avoid using these attributes.

Object	Attribute
Resource	Phone

Object	Attribute
Activity	Account, Asset, Business Plan, Campaign, MDF Claim, Deal Registration, Delegated By, MDF Request, Lead, Opportunity, Enrollment Number, Partner, Program, Sales Objective, Service Request
Asset	Asset Owner, Product
Account	Type, Favorite, Organization Type
Opportunity	Business Unit, Win Probability (RcmndWinProb)
Deals	Account Country
Product	Eligible for Service

- Use custom attributes that are based on database columns only. Avoid using custom attributes, such as attributes based on the Formula field, that aren't based on database columns. Support for attributes that aren't based on database columns will be deprecated in future releases.

12. Enter any additional conditions required to specify the access level you want the rule to provide.
13. Next, in the Action: Assign Access Group section, click **Select and Add** from the **Actions** menu.
14. Search for and select the access group you want to share this rule with, then click **Apply** and then **Done**.

    You can assign a rule to multiple access groups.
15. In the **Access Level** field, select the type of object access you want to give group members.

Access Level	Access Provided
Read	Read-only access If you're creating a rule for the Sales Quota Plan object, only the Read access level is supported.
Update	Read and update access
Delete	Read and delete access
Full	Read, update and delete access

16. Select **Save and Close** from the **Actions** menu.
17. On the Object Sharing Rules page, publish the new rule to ensure that your changes get included in the assignment processing by selecting **Publish Rules** from the **Actions** menu.
18. When the status indicator shows the publish process has completed, click **Close.**

The Perform Object Sharing Rule Assignment Processing process automatically runs at scheduled intervals to assign the object rules for the relevant access groups. You can also run the process manually at any time. For information, see the topic Run the Perform Object Sharing Rule Assignment Process.

> **Tip:** You might want to run the object sharing rule assignment process for an individual record (for each type of object) and confirm the access group rule processing is correct before processing all records for an object.

Rule Publishing

After creating a custom rule, you must publish the rule to make it available for assignment processing. You can publish a new rule in two ways:

- If you create the rule from the main Object Sharing Rules page (object context), you publish the rule by selecting the **Publish Rules** option from the **Actions** menu on the Object Sharing Rules page. Publishing rules this way published rules for all objects (global rule publish).
- If you create the rule in the context of a group when editing the group, then you can publish the individual rule by selecting **Save and Publish** from the **Actions** menu of the Create Object Sharing Rule page (single rule publish).

Related Topics

- Enable Additional Attributes for Access Group Object Sharing Rules
- Enable Access Group Security for Custom Objects
- How do I run the Perform Object Sharing Rule Assignment Process?

Combine Predefined and Custom Conditions in a Rule

You can create hybrid object sharing rules, that is, rules that combine a predefined condition with one or more custom conditions, if this feature is enabled in your environment.

Once enabled, a **Predefined Condition** list becomes available in the Conditions section of the Create Rule page where you can select a predefined condition. Combining custom conditions with a selected predefined condition in a hybrid rule lets you refine the access that's provided by the predefined condition.

For example, there is a predefined condition that provides all users who are on the opportunity team with access to the opportunity. If you want to restrict this access so team members have access to the opportunity only if it has a status of **Open**, then you can do so using these steps.

1. Create an object sharing rule for the Opportunity object.
2. In the Conditions section, select this condition from the **Predefined Condition** list:

   ```
   Opportunities where the access group member is on the opportunity team
   ```
3. Select a value from the **Rule Applies If** list to choose whether the custom conditions you're about to create are applied when any of the custom conditions are met, or only when all the custom conditions are met.

   The default value is **All Conditions Met**.

4. Create a rule with values similar to these.

Field	Value
Object	Opportunity
Attribute	Status
Operator	Equals
Value	Open

5. In the Action: Assign Access Group section, select the access group you want to share this rule with and the type of access to give group members.
6. Select **Save and Close** from the **Actions** menu to save the rule.
7. On the Object Sharing Rules page, publish the new rule by selecting **Publish Rules** from the **Actions** menu.
8. When the status indicator shows the publish process has completed, click **Close**.

When the Perform Object Sharing Rule Assignment Processing process next runs, any changes you've made to object record access are applied.

All users on an opportunity sales team can now view the opportunity provided it has a status of open.

For information about enabling hybrid object sharing rules, see the topic Enable Hybrid Object Sharing Rules.

Considerations When Using Predefined Conditions in a Rule

Here are some considerations to keep in mind when creating an object sharing rule that uses a predefined condition.

- You can select only one predefined condition for the rule.
- You have to define at least one custom condition for the rule.
- Once you have created and saved a rule containing a predefined condition, you can't change the predefined condition selected for the rule.
- If you create rules containing a predefined condition, then disable the profile option that lets you use predefined conditions in a rule, this is what happens:
    - On the Create Rule page, the **Predefined Condition** list is no longer available.
    - When you edit an existing hybrid rule, the predefined condition is visible in the **Predefined Condition** field on the Edit Rule page but you can't change the predefined condition.
    - If an existing hybrid rule is assigned to an access group, group members continue to receive the data access provided by the rule.

Related Topics

- Enable Hybrid Object Sharing Rules

Edit Object Sharing Rules

You can edit the predefined or custom object sharing rules at any time. For example, you might want to assign a rule to additional access groups, or change the level of access a rule provides to a specific group.

Depending on what you want to do, you can choose to edit the object sharing rules from either of these locations:

- The Edit Access Group: Object Rules subtab (group context)

  You can review and edit all the object sharing rules assigned to a specific access group, either by you or by Oracle, when editing an access group. Reviewing rule information from a group context is useful if you want to see what access group members have to data for different objects, or if you want to review all the predefined rules assigned to a system group. For additional information, see the topic Edit Access Groups in this chapter.
- The Object Rules tab on the Access Groups page (object context)

  You can review or edit all the predefined and custom object sharing rules and access extension rules that have been created for a specific object on the Object Sharing Rules page. If you want to delete a custom rule, or edit an access extension rule, you can only do so from this page.

Follow these steps to edit rules from an object context.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. On the Access Groups page, select the Object Rules tab.
3. On the Object Sharing Rules page, select the object you want to review from the **Object** list.

   All the rules and access extension rules defined for the object are listed.
4. Search for and select the rule whose details you want to edit.

   Details relating to the rule are displayed on the Edit Rule UI.
5. The changes you can make to a rule vary depending on whether you're editing a predefined rule or a rule you created yourself. But to use either type of rule, the rule must be active. To activate a rule, or inactivate a rule you no longer require, select or deselect the **Active** check box.
6. If you're editing a custom object sharing rule you created, you can delete the rule by selecting **Delete** from the **Actions** menu.

   Provided the rule isn't assigned to any access groups, the rule is deleted. You can't delete predefined rules.
7. Editing rule conditions:
   - If you're editing a predefined rule, you can't change the condition defined for the rule, delete the condition or add new conditions.
   - If you're editing a rule you created, you can create new conditions, or edit or delete the existing conditions in the Conditions area. For information on defining rule conditions, see the topic Create Custom Object Sharing Rules.
8. Editing access groups:

   The access groups the rule is assigned to are listed in the Action: Assign Access Group area. You can make these changes for both predefined and custom object sharing rules:
   - Enable or disable the rule for a specific access group by selecting or deselecting the **Enable** check box.
   - Remove an access group from the list by selecting the group and then selecting the **Delete** option from the **Actions** menu.

- Change the access level provided by the rule for a specific group by changing the value in the **Access Level** drop-down list.
- Assign the rule to additional custom or system access groups by performing these steps:
  - Select the **Select and Add** option from the **Actions** menu.
  - In the Select and Add: Access Group dialog box, search for and then select the custom or system access group you want to assign the rule to, then click **Apply**.
  - Add any other groups and, when you have completed your selections, click **Done**.

> **Note:** For a predefined rule for which Oracle has created the rule-system group association, a **Lock** icon indicates that this association is part of the default security configuration. In these cases, you can't edit the rule to change the access level for the group and you can't remove the rule from the group. The only change you can make is to enable or disable the rule for the group.

9. When you complete all your editing changes, click **Save and Close** from the Edit Rule page **Actions** menu.
10. On the Object Sharing Rules page, select the **Publish Rules** option from the **Actions** menu to apply the changes you made.
    When the Perform Object Sharing Rule Assignment Processing process next runs, any changes you've made to object record access are applied. If you want to apply the changes immediately, you can run the process manually using the steps outlined in the topic Run the Perform Object Sharing Rule Assignment Process.

Related Topics

- How do I run the Perform Object Sharing Rule Assignment Process?

Overview of Access Extension Rules

Access extension rules extend the access defined for an object in an object sharing rule to a related object.

For example, if you have secured access to an object such as Account using an object sharing rule, you can extend the access defined in the rule for the Account object to a related object, such as Activity, by creating an access extension rule. All members of an access group who can access account data will then have access to activity data for the account.

Supported Objects

Access extension rules functionality isn't currently supported for all the objects that are enabled for access groups. You can create an access extension rule only for these objects.

- Activity
- Activity Assignee
- Asset
- Business Plan
- Contact
- Conversation Message
- Custom objects
- Deal Registration
- Goal Participant
- HR Help Desk Request

- Internal Service Request
- MDF Budget
- MDF Claim
- MDF Request
- Message
- Note
- Opportunity
- Program Enrollments
- Quote and Order
- Sales Lead
- Service Request

You can define as many access extension rules as required for each object.

Predefined Access Extension Rules

As part of the default security configuration, Oracle provides predefined access extension rules, which are associated with specific system groups. You can activate or inactivate the predefined access extension rules, but you can't change the association between the rules and the system groups. You also can't associate the predefined access extension rules with other custom or system access groups.

For example, if you assign a predefined rule to a custom access group, and that rule is extended in a predefined access extension rule, the access provided to the related object by the access extension rule isn't applied to the custom group.

If you want a custom access group to have the same access to a related object that a predefined access extension rule provides, you have to create a custom access extension rule.

Considerations When Creating Access Extension Rules

Before creating an access extension rule for an object, review the following considerations.

- You can't link access extension rules.

  Each access extension rule provides access to records for only one object and can't be extended to provide access to records for a second object.

  For example, if you create an access extension rule to provide group members with access to activity data for accounts they can access (Rule 1), you can't create another rule to grant access to opportunities on the basis of the activities they can access through Rule 1. In this scenario, you have to create two new access extension rules for the Opportunity object:
  - A rule to provide opportunity access based on the group members access to activities
  - A rule to provide opportunity access based on the group members access to accounts
- When you define a relationship between two objects in Application Composer, you can optionally specify data filter criteria for both the source and target objects. The filter criteria control which records are available for association at runtime with a record from the other object in the relationship.

  Access Extension rules don't support filters, so if you create an access extension rule for related objects with filters, be aware that the filter isn't applied. For additional information about object relationships, see the Configuring Applications Using Application Composer guide.

- You can't extend the access of rules that provide global access to an object's data to related objects.

Related Topics

- Configuring Applications Using Application Composer

Create Access Extension Rules

Create access extension rules to extend the access defined for an object in a custom or predefined object sharing rule to a related object. Members of access groups assigned the object sharing rule will then receive access to the records of the related object, with the access level you choose in the access extension rule.

For example, to extend the access defined for the Account object to the related object, Activity, so that all users who can access account data have access to activity data for the account, use steps similar to the following.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. On the Access Groups page, click the Object Rules tab.
3. Select the **Synchronize Custom Objects and Fields** option from the **Actions** menu to make sure that custom attributes or objects that are enabled for access groups are available on the UI.
4. Select the object you're creating the extension rule for in the **Object** drop-down list. For example, select the **Activity** object.

   Any existing object sharing rules or access extension rules defined for the object are displayed.
5. In the Access Extension Rules area, click **Create**.
6. On the Create Access Extension Rule page, specify these values.

Field	Description
Name	Enter a unique name for the rule. It's a good idea to use a meaningful name that identifies the purpose of the rule. For example, if you're creating a rule to extend the access defined for an account to its related activities, you might name the rule something like ActivityToAccount.
Description	Enter additional details about the rule if required.
Active	Rules are active by default. Deselect the **Active** check box if you're not yet ready to apply the rule.

7. From the **Related Object** list, select the object whose access you want to extend. For example, select **Account**.

   All the object sharing rules defined for the related object you selected are listed in the rules table.

> **Note:** Only objects related to the object you're creating the rule for are listed in the **Related Object** list. For standard objects, the relationship between objects is predefined by Oracle. For example, if you're creating the rule for the Activity object, then the default related objects include Account, Contact, Sales Lead and Opportunity. But if you used Application Composer to define a custom relationship between two standard objects, between a custom object and a standard object, or between two custom objects, then additional objects are also available to select.

8. From the **Relationship** list, select the relationship that applies to the two objects in the access extension rule. For this example, select the **Account to Activity (Standard)** relationship.

   More than one predefined or custom relationship can be defined between the two objects in an access extension rule. For example, if you're creating the rule for the Quote and Order object and the related object is the Account object, then these two predefined relationships are listed in the **Relationship** field and you can select whichever is relevant:

   - Account to Quote and Order Account (Standard)
   - Account to Quote and Order's Opportunity Account (Standard)

   Object relationship names that include (Standard) at the end of the name are predefined by Oracle. See the section Object Relationship Naming Conventions at the end of this topic for additional information about naming conventions for standard relationships.
9. Select one of these options depending on whether you want to extend the access provided by all rules or by selected rules to the related object.

Option	Description
Extend all access defined for related object	Select this option if you want to extend the access provided by all the rules to all the groups assigned the rule. Any access group members assigned access to the related object by any of the rules listed is assigned the same access to the object you're creating the extension rule for. You can't change the level of access provided by the rules.
Select rules to extend access defined for related object	Select this option if you want to extend the access of only the rules you select to only the groups you select. When you select this option, the **Read**, **Update** and **Delete** access level check boxes for each rule in the rules table are deselected. - To apply a rule to your selected object, click one or more of the check boxes for the rule. For example, click the **Update** check box for a rule to specify that anyone who can access the related object (for example, Account) can update data for the object you're creating the rule for (for example, Activity). There's a separate row for each rule-group combination so you can choose to extend the access provided by a rule only to a specific access group or to a number of groups. - If you don't want to apply a rule, don't select the access level check boxes for the rule.

10. Click **Clear** at any time to deselect all the **Read**, **Update**, and **Delete** selections you made.
11. Click **Save and Close** to save your changes.
12. Publish the new rule on the Object Sharing Rules page by selecting the **Publish Rules** option from the **Actions** menu.
13. The access extension rule is assigned when the Perform Object Sharing Rule Assignment Processing process next runs.

Object Relationship Naming Conventions

The object relationship names listed in the **Relationship** field on the Create Access Extension Rule page include (Standard) at the end of the name if they're predefined by Oracle.

Standard relationship names distinguish between contacts in a business-to-business (B2B) or business-to-consumer (B2C) sales environment. In a B2B environment, the customer is a business or corporation (an account) and a contact refers to an individual who's associated with the account. In a B2C environment, the customer is an individual and a contact refers to the individual consumer. To reflect these differences the relationship names use the term Contact to refer to an individual associated with an account, and the term Contact of Type Account Consumer to refer to an individual consumer.

For example, if you create an access extension rule for the Opportunity object and the related object is the Contact object, then two predefined relationships are listed in the **Relationship** field:

- Contact to Opportunity (Standard)
  This relationship applies to a B2B environment. A specific individual is associated as a contact on the opportunity. The access extension rule lets users who can access a contact (individual) access the opportunities associated with the individual.
- Contact of Type Account (Consumer) to Opportunity Account (Standard)
  This relationship applies to a B2C environment. A specific consumer is associated as an account on the opportunity. The access extension rule lets users who can access a contact (consumer) access the opportunities associated with this consumer.

Enable Additional Attributes for Access Group Object Sharing Rules

Use the Manage Object Sharing Assignment Objects task to add additional attributes and make them available for your selected rules when you create or edit a standard object sharing rule.

You create object sharing rules to associate with access groups and if the attribute value that you want isn't available from the rule conditions drop-down list, you can enable the attributes you want from here.

Once you set up the rules with the conditions that records must meet, then resources from your access groups get assigned to the object when they match the rule conditions.

> **Note:** This procedure isn't needed for any custom objects. It's needed only if you want to expose additional attributes for one of your standard objects. Custom objects and attributes created in Application Composer are synchronized and available when you select the **Synchronize Custom Objects and Fields** menu item from the **Actions** menu on the Object Sharing Rules page.

Here's an example of the steps to enable an Opportunity object rule attribute for your access group.

1. Navigate to the **Setup and Maintenance** area, and search for the **Manage Object Sharing Assignment Objects** task.
2. On the Manage Object Sharing Assignment Objects page, select the **Opportunity** work object.
3. In the **Opportunity: Details** section, select the **Attributes** tab.
   The attributes defined for the selected Opportunity object are displayed.
4. Click the attribute that you want to add to an Opportunity record rule that you want to share.
   For example, if you want to provide the access group called High_Tech_Oppti_Members with access to the all opportunities for the GreenServer account based on the Asset ID, then enable the attribute **Asset ID** to include in your combination of attributes for the sharing rule.

5. Click **Save and Close**.

Once the additional attributes are enabled, you can create rules using the custom attributes from the Object Sharing Rules page.

Copy Object Sharing Rules from One Access Group to Another

You can copy the object sharing rules assigned to one access group to another group.

Predefined and custom rules, and access extension rules, are all copied. You can copy rules from system or custom access groups to access groups you create, or to system access groups generated for custom job roles. You can't copy rules to a system access group that's generated for a predefined job role.

Use the copy rules feature to simplify the process of creating custom access groups and implementing access groups generated for custom job roles. Instead of having to assign rules individually to these groups, you can copy the rules from an existing group that provides similar access to data as your custom group requires, and then enable and publish only the copied rules relevant for your group.

Use these steps to copy rules form one access group to another.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. Select the access group whose rules you want to copy from the groups listed.

   Custom access groups are displayed by default so if you want to copy rules from a system access group, you first have to select **System Groups - Role** from the **List** drop-down list. Details relating to the group and its members are shown on the Edit Access Group: Overview subtab.
3. Select the Object Rules subtab if you want to review the rules assigned to the group before copying them.
4. From the **Actions** menu, select the **Copy Rules** option. The Copy Object Sharing Rules dialog is displayed.

   > **Note:** The **Copy Rules** option doesn't copy the access group membership rules defined for an access group.
5. Select the group you want to copy the rules to from the **Copy to Group** drop-down list.

   You can only select valid groups to copy the rules to, that is, custom access groups you created, or system access groups generated for custom job roles.
6. Click **Save**.

   The rules are copied to your selected group provided that no existing rules are currently being published. If there's already a publish process running, wait until it completes and then try to copy the rules again.
7. Click **Save and Close** on the Edit Access Group: Overview subtab.
8. To verify that the rules have been copied successfully, on the Access Groups page, select the access group you've just copied the rules to.
9. On the Edit Access Group: Overview page for the group, click the Object Rules subtab.
10. Review the new rules assigned to the group, then click the **Enable** check box for all the rules you want to enable for the group.

    If you want, you can change the access level assigned by each of the copied rules to your group.

    > **Note:** If you copy a rule to a group that's already assigned the rule, then the access level specified for the copied rule overwrites the access level in the existing rule if these differ.
11. Click **Save and Close** to save your changes.

12. To publish the new rules you've copied and enabled for your group, select the Object Sharing Rules tab on the Access Groups page, then select **Publish Rules** from the **Actions** menu.

Related Topics

- Edit Object Sharing Rules

Access Group Scheduled Processes

Overview of the Access Group Scheduled Processes

You can review and manage all of the scheduled processes required for access group processing using the Monitor tab on the main Access Groups page.

Access group processes publish and assign object sharing rules, make custom objects and attributes available for use in access group rules, and ensure that groups are created and assigned members appropriately.

Most of these processes are scheduled to automatically run at specified intervals or are run when you select a relevant option on the access group UIs. But you can also run these processes at any time from the Monitor tab on the Access Groups page.

The Monitor page includes a subtab for each of the access group processes. From each of these subtabs, you can review and manage the relevant process. This table describes the access group processes, what task each performs, and how the task is initiated.

Process	Description	Initiated
Update Groups and Members This process starts these subprocesses: • Run Access Group Membership Rules • Refresh Access Control Data • Add Access Groups Enablement Duty to Custom Roles	After you create access group membership rules, the Run Access Group Membership Rules process adds users who match the rule conditions to the correct access groups. After you create custom job roles, or add users to job roles, the Refresh Access Control Data process and the Add Access Groups Enablement Duty to Custom Roles process update system groups with changes to custom job roles and to user-job role assignments.	All of these processes are run when you select the **Update Groups and Members** option from the **Actions** menu on the Access Groups main page. This process is also scheduled to run automatically every hour.
Perform Object Sharing Rule Assignment	Once an active rule is published, this process assigns group members with the object access specified by the rule.	By default, the process is dynamically scheduled to run at regular intervals. If you disable dynamic scheduling of the process, you must either create your own schedule, or run the process manually from the Monitor tab.
Synchronize Custom Objects and Fields	If you create custom attributes or objects in Application Composer and enable them for access groups, this process synchronizes the custom attributes or objects and makes them available in the Object Sharing Rules UI.	This process is run when you select the **Synchronize Custom Objects and Fields** option from the **Actions** menu on the Object Rules tab of the Access Groups page. This process isn't scheduled to run automatically.

Process	Description	Initiated
Publish Rules Runs the Perform Assignment Data Publish, Refresh, and Synchronization process.	After you create or edit an object sharing rule or a group membership rule for an access group, this process makes the object sharing rules effective and eligible for the subsequent object assignment process stage.	This process runs when you select the **Publish Rules** option from the **Actions** menu on the Object Rules tab of the Access Groups page. This option publishes rules for all objects. This process is also scheduled to run automatically at regular intervals. This process runs when you're initially provisioned with your sales application. It activates and publishes predefined access groups and rules so they're immediately available.

Manage the Access Group Scheduled Processes

The Monitor subtab on the Access Groups UI gives you a single location to monitor or manage all the scheduled processes for access groups.

You can run or cancel a process, view or update the schedule for a process, and monitor the status of an active process – all from the Monitor page. This page lets you easily manage access group processes and lets you quickly identify failed processes that might be causing issues with data access.

Here's how to review and manage scheduled processes on the Monitor page:

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. On the Access Groups page, select the **Monitor** tab.

   Each tab shows details for one of the access group scheduled processes.
3. Select the subtab for the process you want to review or manage.

   The table on the process page lists information about submitted processes that are currently running, that have completed, or that are scheduled to run in the future. Up to a maximum of 1,000 processes are listed, with the most recently submitted processes displayed first.

   If a process starts other processes, view information for these subprocesses by clicking the Expand icon in the process **Request Id** field.
4. Review the information in the process table to check the status of each job and to identify any issues that require intervention, such as jobs that finish with a status of **Error** or **Warning**.

   You can search for specific records or specific types of records in the table using the filters. Use the search **Request ID** field to search for a process with a specific identifier or add filters to search by other fields. For example, if you want to identify processes that didn't complete successfully, select the **Job Status** option from the search **Add** menu,

select the **Equals** operator, specify a value of **Error**, then click **Search**. Only processes with a status of **Error** will be listed in the table.

You can also perform these tasks from each process page:

- *Start an Access Group Process*
- *Cancel an Access Group Process*
- *How do I run the Perform Object Sharing Rule Assignment Process?*
- *Reschedule the Perform Object Sharing Rule Assignment Process*

  The **Schedule** option is available only on the Perform Object Sharing Rules Assignment page.

Start an Access Group Process

Here's how to run an access group scheduled process from the access groups Monitor page.

1. On the Access Groups page, select the Monitor tab.
2. On the monitor page, select the appropriate subtab depending on which process you want to start.
3. On the process page, click **Start Process**.

   If you are starting the Perform Object Sharing Rules process, a dialog box is displayed where you can select parameters for the process before submitting it. For details on starting this process, see the topic Run the Perform Object Sharing Rule Assignment Process.
4. After you submit a scheduled process, track its progress in the table by reviewing the value of the **Job Status** field for the job.

   Once you start a process, the **Status** field is generally set to **Running** but it can be set to other values. For example, if the process is scheduled for a future date it will have a status of **Wait**. Or if a process initiates other processes, then the status of the primary process changes to **Paused** when the secondary processes are running.

   For additional information on process status values, see the Understanding Scheduled Processes guide.
5. If you don't see the new process listed in the table, click the Last Refreshed icon. You can also search for the process using the **Request ID** filter or a filter you've selected from the search **Add** drop-down list.
6. When the process completes, the value of the **Job Status** field is updated.

   > **Note:** If you are running the Publish process, the **Status of Last Automatic Publish Process** field also shows the status of the last automatically run publish job.

   If the process doesn't complete successfully, for example, if it completes with a **Job Status** of **Error** or **Warning**, you can either re-run the job or investigate the cause of any issue by accessing the process log file using these steps:
   a. Note the process ID in the **Request Id** field.
   b. Navigate to the Scheduled Processes work area (**Navigator** > **Tools** > **Scheduled Processes**).
   c. In the Search Results section of the Overview page, search for the process ID you noted in step a.
   d. In the Search Results table, select the process, then review the log file information in the Process Details tabs.

Related Topics

- How do I run the Perform Object Sharing Rule Assignment Process?

How do I run the Perform Object Sharing Rule Assignment Process?

The Perform Object Sharing Rule Assignment scheduled process assigns access group object sharing rules to objects each time you add an access group and share the rules.

You schedule and run this process from the access groups Monitor page.

By default, the process runs automatically at scheduled intervals to make sure you've the required access to all object data for your selected access groups. But you can submit the process manually if, for example, you want immediate access to new records and objects.

> **Note:** If you disable automatic scheduling of the process, you must either create your own schedule for the process, or run the process manually. You can do both tasks from the Perform Object Sharing Rules Assignment subtab on the Monitor page. For more information about automatic scheduling, see the topic, *Scheduling Options for Object Sharing Rules Assignment Processing*.

Steps to Run the Process

1. On the Access Groups page, select the Monitor tab.
2. On the Perform Object Sharing Rules Assignment subtab, click **Start Process**.
3. On the Schedule Process page, enter these values in the Basic Options region.

Field	Entry
Work Object	Select the work object you want from the drop-down list.
Record Selection	You can run the assignment process for all records or for a subset of records by selecting the appropriate option from the **Record Selection** list. o The first time you schedule the job, select the **All records** option. After that, avoid processing delays by selecting the **All records** option only when it's essential. For example, when you activate and enable rules for a new object. **Tip:** You might want to run the object sharing rule assignment process for an individual record (for each type of object) and confirm the access group rule processing is correct before processing all records for an object. o In general, schedule the process to run for a subset of records using one of these options. - **Records Since Last Run** - **Records updated in last 'X' days** - **Records updated in last 'X' hours** - **Records updated between dates** - **Single record** It's recommended that you select the **Records Since Last Run** option in most cases. This option runs the job for only those records that were updated since the last time

Field	Entry
	the process was run for the object, or for records that failed or were missed during the previous run of the job. If the job has never been previously run for the object, then all records are processed. Using this option reduces job processing time and ensures that changes to object rules are processed for all relevant records. Here are some examples of how you can use the other options: - If you've scheduled the job to run every hour, select **Records updated in last 1 hours**. - If you've scheduled the job to run every 4 hours, select **Records updated in last 4 hours**. - If you've scheduled the job to run daily, then select **Records updated in last 1 days**.
Diagnostic Mode	Run the process in diagnostic mode to troubleshoot any issues with access group rules processing. When you run the process in this mode, access group rule changes aren't committed. Instead an output log is generated with details of the rules processing. You can use these details to troubleshoot any issues with access group rules assignment. For example, the log helps you understand why certain rules weren't applied as expected.

4. The first time you run the process click **Submit** to run it immediately.

   Alternatively, if you've disabled dynamic scheduling and want to create your own schedule for the process, or if you want to create an additional schedule to supplement the default schedule, use these steps:

   a. Click **Advanced**.
   b. In the Advanced Options region, click the Schedule tab.
   c. Select the **Using a schedule** option.
   d. Select how often you want to run the process in the **Frequency** field.
   e. Enter start and end dates for the process.
   f. Click **Submit**.

   Depending on your settings, your process runs immediately or at the intervals you specified. You can monitor its progress in the process table on the Perform Object Sharing Rule Assignment page.

Cancel an Access Group Process

Here's how to cancel an access group process from the access groups monitor page.

1. On the Access Groups page, select the Monitor tab.
2. On the monitor page, select the appropriate subtab according to the process you want to cancel.
3. In the process table, select the relevant process and click **Cancel Process**.
   You can cancel processes that have a status of **Running**, **Wait** or **Paused**.
4. Click the Last Refreshed icon to verify that the process completed and that the job was canceled.

Reschedule the Perform Object Sharing Rule Assignment Process

If you submitted the Perform Object Sharing Rules Assignment process to run on a schedule, for example, once a day, you can edit the schedule for the process even if some of the scheduled runs have already completed.

1. On the Access Groups page, select the Monitor tab.
2. On the Perform Object Sharing Rule Assignment subtab, select the process you want to reschedule from the process table. You can only reschedule processes that have a **Job Status** of **Wait**.
3. Click **Schedule Process**.
4. On the Edit Schedule page, you can make these changes:
    - Add a new time to the existing schedule.
      Click **Add Time** and then enter a new custom time for the schedule.
    - Change how often the process runs.
      Click **Change Frequency** and select a new frequency. You can optionally choose to enter an end date for the process. If you change the frequency, any custom times you previously added are lost.
5. When you've completed any changes, click **OK**.

   When you change the schedule for a process, the initial process job is canceled and a new job is created with the new schedule.

Related Topics

- Scheduling Options for Object Sharing Rules Assignment Processing
- Understanding Scheduled Processes

Assign Group Access By Country

If you want to provide a group of users with access to data on the basis of the users' context, such as their business units, countries, or regions, then access groups are the best way of providing such access.

This topic gives an example of the high-level steps to follow to assign access to sales objects (for example, accounts, contacts, opportunities, partners, and leads) to groups of resource users on the basis of the users' home countries. You can use a similar process to assign a group with data access using some other attribute, such as resource organization.

To provide users with access to sales records on the basis of their country:

1. Create a custom attribute, Country, for each sales object and make the attribute available as a custom field on the sales object UI.
   When creating or editing an object record, such as an opportunity, the user can then select the country associated with the record from the custom Country field on the UI.
2. Create a custom attribute, Country, for the Resource object to represent a user's country and make the attribute available as a custom field on the Resource object UI.
   When creating users, you can then select the country the user is associated with from the Country field on the UI.

3. On the Access Groups page of the Sales and Service Access Management work area, create an access group for each country and add existing resources to each country group. As new users join your organization, make sure you add them to a country group.

   You can add members to each country-based access group manually on the Access Groups UI. Or, use these steps to add members to access groups using the export and import functionality:

   a. Use the resource export functionality to generate a list of sales resources and filter the generated export file based on the Country field.
   b. Import country groups and members:

      - For each country-based access group, create an import file with values similar to those shown in this table:

        Sample Values for Countries in Import File

ACCESS_GROUP_NUMBER	NAME	DESCRIPTION	ACTIVE_FLAG
3788493471	GERMAN REGION	Access group for users in Germany	Y
3788493472	UK	Access group for users in UK	Y
3788493473	FRANCE	Access group for users in France	Y

      - To add members to each access group, create an import file of resources with values similar to those shown in this table:

        Sample Values for Resources in Import File

ACCESS GROUP NUMBER	GROUP_NAME	PARTY_NUMBER	RESOURCE_EMAIL_ADDRESS	PARTY_NAME
3788493471	GERMAN REGION	2793920203	tom.jones@example.co	Tom Jones
3788493471	GERMAN REGION	2793920204	lisa.jones@example.co	Lisa Jones
3788493471	GERMAN REGION	2793920205	matt.hooper@example	Matt Hooper
3788493471	GERMAN REGION	2793920206	jane.smith@example.c	Jane Smith

4. On the Access Groups page, click the **Object Rules** tab.

5. To make the Country attribute visible and available for selection on the Object Sharing Rules page, select the **Synchronize Custom Objects and Fields** item from the **Actions** menu.
6. When the value of the Last Synchronized field indicates that the synchronize process is finished, select the sales object that you want to assign by country. For example, select **Opportunity**.
7. Create an individual rule for each country by clicking **Create** in the Custom Rules region.

    a. In the Conditions region of the Create Rule page, in the **Attribute** field, select the **Country** attribute as the value used to assign object records.
    b. In the Action: Assign Access Group region, assign the rule to the relevant country-based access group and select the level of object access to be provided. For example, select **Read** or **Update** access.
    c. Click **Save and Close** from the **Actions** menu to save the rule.

    The Object Sharing Rules page is displayed.
8. When you have created an object sharing rule for each country, on the Object Sharing Rules page select **Publish Rules** from the **Actions** menu to publish all new and changed rules for the object.
9. When the Perform Object Sharing Rule Assignment Processing process next runs, any changes you've made to object record access are applied. If you want to apply the changes immediately, you can run the process manually using the steps outlined in the topic Run the Perform Object Sharing Rule Assignment Process.

    It's a good idea to run the object sharing rule assignment process for an individual record (for each type of object) and confirm the access group rule processing is correct before processing all records for an object.

For additional information about creating custom attributes and making them visible on a UI, see the *Configuring Applications Using Application Composer* guide. For additional information about importing and exporting data, see the *Understanding Import and Export Management for Sales and Fusion Service* guide.

Related Topics

- How do I run the Perform Object Sharing Rule Assignment Process?
- Configuring Applications Using Application Composer
- Understanding Import and Export Management for Sales and Fusion Service

Use Access Groups to Secure Product, Product Group, and Price Book Data

You can use access groups to provide different levels of access to sales catalog data (product, product group, and price book data) for different groups of users in your enterprise.

The Product, Product Group, and Price Book objects were previously unsecured so all users had unrestricted access to sales catalog data. Predefined access group rules still provide all users with unrestricted access to this data, but you can now remove or configure this access using these steps:

1. Remove users global access to sales catalog data in either of these ways:

    - Disable the association between the predefined rules and the All Users system group.

      The All Users system group includes all authenticated users in your environment.
    - Deactivate the predefined rules that provide access to all data.

2. Create custom access groups for different groups of users and specify the object access you want to assign to each group. For example, you might want most users to have Read access to all product, product group, or price book data but restrict Update and Delete privileges to administrators.

Here are the steps to secure the Product, Product Group, or Price Book objects using access groups.

Edit the Global Access Rules for Sales Catalog Data

To use access groups to secure product, product group, or price book data, first edit the predefined rule defined for each object that provides all authenticated users with global access. Here are the steps to edit the predefined rule for the Product object to remove all users access to product data.

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. On the Access Groups page, select the Object Rules tab.
3. Select the **Product** object from the **Object** list.

   All the rules defined for the object are listed in the Rules section.
4. Select the **All Products** system rule. Notice that the **Active** column is checked.

   Details relating to the rule are displayed on the Edit Rule UI.
5. Disable the rule for all users by deselecting the **Enable** check box for the **All Users Group** in the Action: Assign Access Group region of the page.

   Alternatively, if you don't want to assign global access to product data for any group of users, you can deactivate the rule by deselecting the **Active** check box for the rule.
6. Select **Save and Close** from the **Actions** menu.
7. On the Object Sharing Rules page, select **Publish Rules** from the **Actions** menu. Keep refreshing the screen, using the circular arrow next to the **Rules Last Published** field, until you confirm the rule deactivation has been published. You can also drill into the All Products rule to confirm the **Published Status** field indicates **Published**.
8. Click **Close**.
9. When the Perform Object Sharing Rule Assignment Processing process next runs, any changes you've made to object record access are applied.

To edit the predefined rules that provide global access to Product Group or Price Book object data, use the same process as outlined above, substituting the appropriate rule names:

- For the Product Group object, the predefined rule to edit is All Product Groups.
- For the Price Book object, the predefined rule to edit is All Price Book Headers.

Create Access Groups for Sales Catalog Data

You can now create access groups in the usual way and specify different levels of access to Product, Product Group, and Price Book object data for each group. Here's an example of the high-level steps to follow to configure access for products.

1. Identify the different access levels to product data you want to configure for users and create an access group for each.

   For example, you might create two groups: one group for specific administrators who are to have full access to product data, and one group for all other users who will have only Read access to product data.

2. Assign resources to each group.

   You can assign users to a group manually on the UI, or by defining group membership rules, or by importing the users from a file.
3. For each group, create object sharing rules for the Product object, specifying the type of access to object data group members should have:
   - For the general users access group, create a custom rule for the Product object that provides Read access and assign it to the group.
   - For the administrator users access group, create a custom rule for the Product object that provides Full access and assign it to the group.
4. Publish the rules.

   When the Perform Object Sharing Rule Assignment Processing process next runs, the access defined in the object sharing rules is applied to group members.

> **Note:** An alternative method of assigning full access to product data for the administration users is to create a custom job role and assign the custom role to the administration users. After the Refresh Access Control Data Process runs, a corresponding system access group is generated for the custom role that contains all the users assigned the custom role. Assign the predefined All Products system rule to the generated system group.

To create custom access groups for access to product group or price book data, follow the same process.

Sales Catalog All Access Duty Role

The Sales Catalog All Access (ORA_QSC_ SALES_ CATALOG_ ALL_ACCESS_DUTY) duty role provides all APPID users with global access to sales catalog data. You can't edit the data security policies provided by this duty role, but you can assign the role to other custom roles to provide users with global access to Sales Catalog data instead of creating an access group for these users.

Related Topics

- Create Custom Object Sharing Rules
- Create a Custom Access Group

Custom Objects and Access Group Security

Enable Access Group Security for Custom Objects

You can use access groups to provide resources with access to custom object data. To do this, you must first enable access group security for each custom object.

To enable access group security for custom objects, complete these steps:

1. Navigate to Application Composer and confirm that you're in an active sandbox.
2. Navigate to the Security node of the custom object that you want to enable access group security for.

3. On the Define Policies page, select the **Enable Access Group Security** check box.

   CAUTION: You can't disable access group security once enabled, but you can disable specific groups or rules on the Access Groups page in the Sales and Service Access Management work area.

4. Next, enable that custom object for access group object sharing rules. To do this, navigate to the Access Groups page in the Sales and Service Access Management work area.
5. Click the Object Rules tab.
6. On the Object Sharing Rules page, select the **Synchronize Custom Objects and Fields** item from the **Actions** menu. The custom object and its attributes are now available when defining object sharing rules for access groups.
7. In Application Composer, set functional security for required roles.
   Navigate to the custom object's Security node, and configure functional security in the Roles section of the Define Policies page. This step isn't related to access group security (data security), but it's a required step so that the right roles can see the custom object's user interface pages (functional security).

After you enable access group security for a custom object, you work with it just like a standard object. Create your object sharing rules for access groups, and all group members are given access to that custom object's data according to the rules.

Tip: When configuring data security, you can optionally configure owner security instead of access group security. With owner security, for example, you can provide create and read access to all users, update access to the record's owner and owner management chain, and delete access to only the owner. You configure owner security in the Roles section of the Define Policies page. If you configure both owner and access group security, then your users will see data from both their owner management chain as well as from access groups that they're members of.

Related Topics

- Create Custom Object Sharing Rules

Enable Team-Based Access to Custom Objects

You can provide resources with access to custom object data, where access is based on the resource's membership in a team, also known as team-based access group security. With this type of security, team members as well as their management hierarchy can access custom object records.

To enable team-based security for custom objects, complete these steps in Application Composer:

1. Create a relationship between your custom object and the Resource object.
   In Application Composer, create a many-to-many relationship between your custom object and the Resource object, where your custom object is the source object.
2. Create a subtab so that your users can add resources to custom object records at runtime.
   Add a Team subtab to the custom object details page layout, where the Team subtab is based on the intersection object created from your many-to-many relationship.
3. Configure security so that the team member on the custom object record as well as his management hierarchy have access to the record.
   To do this, set security for both the intersection object as well as the custom object.
   For the intersection object:

a. Navigate to the Security node for the intersection object.
b. On the Define Policies page, select each role that needs access and, for each column (Read, Update, Delete), select **All**.

For the custom object:

a. Navigate to the Security node for the custom object.
b. On the Define Policies page, select the Enable Access Group Security check box.
c. Select the Configure Team for Access Group Security check box and select the many-to-many relationship that you just created.

4. Configure functional security for the required roles.

   This step isn't related to access group security (data security), but it's a required step so that the right roles can access the custom object's user interface pages at the appropriate level (functional security).

   a. Navigate to the Security node for the custom object.
   b. On the Define Policies page, select each role that needs access and, for each column (Read, Update, Delete), select the access level for reading, updating, and deleting records: **Functional Read**, **Functional Delete**, or **Functional Update**.
5. Publish your sandbox.

Finally, enable your custom object for access group object sharing rules. You do the next set of steps in the Sales and Service Access Management work area.

1. Navigate to Access Groups in the Sales and Service Access Management work area.
2. On the Object Sharing Rules page, select the **Synchronize Custom Objects and Fields** item from the **Actions** menu.

   After you sync, your custom object displays in the Object list.
3. Select your custom object from the Object list to configure object sharing rules.

   In the Rules region, the (Custom Object) Team and (Custom Object) Team Hierarchy predefined rules display, in addition to the rules for (Custom Object) Owner and (Custom Object) Owner Hierarchy.
4. Click each rule to assign a custom access group and access level.

   Note that access groups are automatically created based on roles created using the Security Console.

   For more information, see the Access Groups chapter in the Oracle Fusion Cloud Customer Experience Securing Sales and Fusion Service guide:
5. On the Access Groups Monitor page, optionally schedule and run the Perform Object Sharing Rule Assignment process to assign access group object sharing rules to your custom object.

   By default, the process runs automatically at scheduled intervals to make sure you have the required access to all object data for your selected access groups. But you can submit the process manually if, for example, you want immediate access to new records and objects.

Related Topics

- Overview of Access Groups
- Overview of the Access Groups UI
- Edit Object Sharing Rules
- How do I run the Perform Object Sharing Rule Assignment Process?

System Groups and Predefined Rules for Custom Objects

After you create a new custom object in Application Composer and enable it for access group security, you have to synchronize the object to make it available for access groups and rules processing. Use these steps to synchronize the custom object:

1. Navigate to the Access Groups page in the Sales and Service Access Management work area.
2. Click the Object Rules tab.
3. On the Object Sharing Rules page, select the **Synchronize Custom Objects and Fields** option from the **Actions** menu.

Once the custom object is successfully synchronized, a system access group, Custom Objects Administration Group, is created that corresponds to the Custom Objects Administration job role. Predefined object sharing rules are generated for the new custom object and are assigned to the Custom Objects Administration Group system group.

The predefined rules provide the same access to the custom object data as the Custom Objects Administration job role provides, so rules are generated that provide access using these access paths:

- Custom_Object Owner
- Custom_Object Owner Hierarchy
- All Custom_Objects

If you also enabled the custom object for team access group security, two additional predefined rules are created for you:

- Custom_Object Team
- Custom_Object Team Hierarchy

The predefined rules are inactive by default. You can choose whether or not to activate each of the rules generated for the custom object, and whether or not to enable the association between the Custom Objects Administration Group and the generated rules. For additional information on activating and enabling object sharing rules, see the Manage System Access Groups section in this chapter.

Import and Export Access Groups, Members, and Rules

Overview of Importing and Exporting Access Group Objects

Speed up your work with access groups objects using Import and Export Management.

Here are some points to keep in mind when exporting and importing access group data:

- You can import and export access groups and access group members.

  If you have large numbers of users to add to one or more access groups – or whose assignments you want to change – use import and export management. For example, if there are thousands of sales representatives in your organization and you want to assign them to an access group, you could search for all users who are assigned the Sales Representative role and export this list of users to a CSV file. You could then edit the file to specify the name of the access group the users are to be assigned to, then import the updated CSV file.

- You can import and export access group membership rules, predefined and custom object sharing rules, hybrid rules, and access extension rules.
- You can't import access group relationship data for access extension rules.

  Use this functionality to move rules data from one environment to another, or to make large-scale updates to your custom rules at a time.

Note: You can't import system groups or add members to system groups using the import functionality.

For additional information about importing and exporting data, see the topics in this section and the guide *Understanding Import and Export Management for Sales and Fusion Service* on Oracle Help Center.

Import Management with Access Groups

When you import business objects to use with access groups, for objects that have child objects, you can either import both parent and child objects together, or import them separately.

Examples of objects that have child objects are opportunities and accounts. Whether you import the parent and child objects at the same or separately depends on your business needs and the volume of records you're importing.

Low-Volume Import Use Case

For **low-volume imports** you can import objects as a single object or as hierarchical records (for example, parent-child records) and you – as the importer – get immediate access to the records, without needing to run the *Perform Object Sharing Rules Assignment process*.

Note: Only the user performing the import gets immediate access to the records in the UI. Other users still must wait until the Perform Object Sharing Rules Assignment process runs to see the records in the UI.

To use this method where you get immediate access to the records, the Real-Time Transaction Tracking Enabled (ZCA_TRANSACTION_TRACKING_ENABLED) profile option must be set to Yes at site level (which it is by default). See *About Setting the Profile Option* in this topic for more information.

High-Volume Import Use Case

For **high-volume imports**, you import parent and child objects separately. To get access to the records in the UI, you need to run the Perform Object Sharing Rules Assignment process.

With this approach, you:

- Import the parent objects so that the parent records exist before you import the child object records.
- Run the *Perform Object Sharing Rules Assignment process* to make sure the parent records are correctly assigned and available.
- Import the child objects.

About Setting the Profile Option

To set the profile option, navigate to the **Manage Administrator Profile Values** task in Setup and Maintenance and search for the profile option, Real-Time Transaction Tracking Enabled (ZCA_TRANSACTION_TRACKING_ENABLED).

You can set the profile option at site level or at user level. By default, the site value is Yes. This means that any user who imports single-object records or hierarchial records (in low-volume import only) gets immediate access to those imported records and there's no need to run the Perform Object Sharing Rules process. Other users still must wait until the Perform Object Sharing Rules Assignment process runs.

Also see *Profile Option Settings and Need to Run the Process*.

Profile Option Settings and Need to Run the Process

Depending on how the profile option, Real-Time Transaction Tracking Enabled, is set at site or user level, you may or may not need to run the Perform Object Sharing Rules Assignment process.

This table describes some possible combinations of profile option settings and whether or not you need to run the Perform Object Sharing Rules process:

Profile Option Settings and the Need to Run the Process

Profile Option Setting at Site Level	Profile Option Setting at User Level	Run Perform Object Sharing Process Before Importing Child Records?
Y	N	Yes
N	N	Yes
Y	No record present	Not required
N	No record present	Yes
Y	Y	Not required
N	Y	Not required

Access Group Objects Import

Using the Import and Export Management, you can import access group data for these objects:

- Access groups and access group members
- Access group rules, access group rule conditions, and access group rule candidates
- Access extension rules and access extension rule details
  You can't import access group relationship data for access extension rules.

When you're importing data for a particular object, make sure that any prerequisite objects already exist in the application. For example, if you're importing group members for a group, then the group must already exist in the application. Or if you're importing rules and rule conditions, then import the rules before importing the conditions for the rules.

Each import file has a limit of 50,000 records. Unless you're importing records into a new environment, it's a good idea to import only records that you want to create, update, or delete.

To import data for an access group object:

1. Map the source data you want to import to target object attributes in your sales application. This way, the import process knows where to insert each of the information bits.

2. Create a CSV file containing your source data that's mapped to the target object attributes in your application.
3. Create the import activity.
4. Review the import results.

See the remaining topics in this section for information about performing these steps for each type of access group object.

Import Access Group Rules

There are two types of access group rules: object sharing rules that provide users with access to object records, and access group membership rules which add and remove users as access group members. You can import both types of rules.

You can use import management to create, update, or delete access group membership rules and custom object sharing rules, but you can only make limited updates to the predefined object sharing rules. Here are the changes you can make to the predefined rules during import:

- You can activate or inactivate a predefined rule and enable or disable a predefined group for a predefined rule.
- You can add a predefined or custom access group to a predefined rule or remove groups you added previously.
- You can change the access levels for groups you add to a predefined rule.

There are three access group rule objects: Access Group Rule, Access Group Rule Condition, and Access Group Rule Candidate. To import data for each object, create a separate CSV file containing the data you want to import. You must import rules first, and then any rule conditions and rule candidates you want to assign to the rule.

Before you begin, you need to understand how your source data maps to the target object attributes in your application. You also must identify the target object attributes your CSV import file to include.

Review Required Attributes and Validations for Access Group Rule Objects

The tables in this section list the attributes that are required when importing rules, rule conditions, and rule candidates. Some attributes are required to uniquely identify the object record, some are conditionally required depending on whether you want to create, update, or delete an object record, and some are optional. Make sure that you provide valid values for these attributes so that they pass import validations built into the application.

This table lists the required attributes for importing access group rule data:

Attribute	Description	Import Validations	Creating a Rule	Updating an Existing Rule	Deleting an Existing Rule
RuleName	Display name of the rule.	Not applicable.	Required	Optional	Optional
Object	The name of the object the rule is created for.	A valid object must exist.	Required	Optional	Optional
RuleNumber	The number of the rule. If you don't provide the rule number, it's automatically generated.	Not applicable.	Optional	Required	Required

Attribute	Description	Import Validations	Creating a Rule	Updating an Existing Rule	Deleting an Existing Rule
RuleID	The internal number assigned to the rule.	Not applicable.	Don't provide.	Don't provide.	Don't provide.
Active	A value to indicate whether or not the rule is active. A value of Y indicates the rule is active by default.	Not applicable.	Optional.	Optional	Optional
PredefinedFlag	A value that indicates whether the rule is a predefined or custom rule. The default value is N.	Not applicable.	Don't provide.	Don't provide.	Don't provide.
Description	The rule description.	Not applicable.	Optional	Optional	Optional
MatchingType	The matching type for the rule conditions. Valid values are OR or AND. The default value is AND.	Not applicable.	Optional.	Optional	Optional
ConditionCode	The condition code for predefined hybrid rules.	Not applicable.	Optional	Optional	Optional
ConditionName	The condition name for predefined hybrid rules.	Not applicable.	Optional	Optional	Optional

This table lists the required attributes for importing access group rule candidate data.

Attribute	Description	Import Validations	Creating a Rule Candidate	Updating an Existing Rule Candidate	Deleting an Existing Rule Candidate
AccessGroupNumber	The number of the access group associated with a rule.	A valid access group number must exist.	Required	Required	Required
RuleNumber	The number of the rule the access group is associated with.	A valid rule number must exist.	Required	Required	Required
RuleCandidateNumber	An internal number automatically generated.	Not applicable.	Don't provide.	Don't provide.	Don't provide.

Attribute	Description	Import Validations	Creating a Rule Candidate	Updating an Existing Rule Candidate	Deleting an Existing Rule Candidate
RuleCandidateId	An internal identifier automatically generated.	Not applicable.	Don't provide.	Don't provide.	Don't provide.
AccessLevel	The access level assigned to the access group associated with the rule. The default value is Read.	Valid values are Read, Delete, Update, Full.	Optional	Optional	Optional
EnableFlag	A value that indicates whether or not the access group is enabled for the rule.	Valid values are N or Y.	Optional	Optional	Optional

This table lists the required attributes for importing access group rule condition data.

Attribute	Description	Import Validations	Creating a Rule Condition	Updating an Existing Rule Condition	Deleting an Existing Rule Condition
RuleConditionId	The rule condition identifier.	If a value isn't specified for new rule conditions, it's automatically generated. For update and delete operations, this attribute is required.	Optional	Required	Required
Object	The object the rule condition is created for.	A valid object must exist.	Required	Required	Required
ObjectAttributeCode	The attribute the rule condition is created for.	A valid attribute code must exist for the selected object.	Required	Required	Required
Operator	The operator defined for the attribute. The operators IN and NOT IN aren't supported when updating rule conditions. Instead, delete the existing condition record and create a new one.	A valid operator for the attribute and object combination must be specified.	Required	Required	Required
RuleNumber	The number of the rule the condition is defined for.	A valid rule number must exist.	Required	Required	Required

Attribute	Description	Import Validations	Creating a Rule Condition	Updating an Existing Rule Condition	Deleting an Existing Rule Condition
RuleConditionNumber	The number of the rule condition.	This value is automatically generated if not specified for create condition operations.	Optional	Required	Required
ObjectAttributeName	The display name of the object attribute in the rule condition. If a value is specified for the ObjectAttributeCode attribute, this value is optional.	A valid attribute name must be specified.	Optional	Optional	Optional
Value	The value specified for the condition, if applicable.	If the value is selected from a predefined list of values, the value must be valid.	Optional	Optional	Optional

Create the Source CSV File

You include the data that you want to import into your application in a source CSV file. Create a separate CSV file for the access group rules, rule conditions, or rule candidates you want to import. You can use the templates available in the Import Objects UI page to create the source CSV file. To download a template:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**.
2. Select either the **Access Group Rule**, the **Access Group Rule Candidate**, or **Access Group Rule Condition** object in the Import Object Details table and click **Download**.

   You can now edit the downloaded file and provide valid values for the required attributes.

Create the Import Activity

Once you have the CSV file ready, create an import activity to import the rule information:

CAUTION: Make sure custom objects and attributes are synchronized before running the import.

1. Navigate to the Manage Imports page (**Navigator** > **Tools** > **Import Management** > **Import Queue**).
2. Click **Create Import Activity**.
3. In the Enter Import Options page, provide values for these fields:

Field	Description
Name	The name you want to assign to the import.

Field	Description
Object	From the **Object** drop-down list, select **Access Group Rule**, or **Access Group Rule Condition** or **Access Group Rule Candidate** depending on the object records you're importing. Import access group rules first, then import the conditions defined for the rule or the rule candidates, if applicable.
File Name	Select the CSV file you previously created for the rule import data.

4. If you're importing records for the Access Group Rule object, you can also import records for the child objects, Access Group Rule Candidate or Access Group Rule Condition, at the same time using these steps:
    a. Click the **Import Object Hierarchy** link. Now you can see the object hierarchy for Access Group Rule.
    b. Select the **Enabled** check box for the child objects you want to import.
    c. Select the CSV file for each of these child objects.
5. Click **Next**.
6. On the Map Fields page, you'll see that the source and target attributes are automatically mapped. Review and edit the mappings if required.
7. Check the file for unmapped columns or data format issues by clicking **Validate Data**. Click **Next**.
8. On the Review and Submit page, review the import details and then click **Submit** when you're ready.

Review the Import Results

Use the Manage Imports page to check whether your import succeeded. The Manage Imports page shows the status of all active, completed, and unsuccessful imports.

1. Navigate to the Manage Imports page: **Navigator** > **Import Management** > **Import Queues**.
    a. Click the **All Imports** infotile and search for the import activity that you created earlier.
    b. Check the Status column for the import activity. The import is successful if the status displays as Completed. You can drill down on the import activity to go to the Import Status page, which provides the status details of the import activity.
2. After the import process completes successfully, navigate to the Object Sharing Rules page: **Navigator** > **Sales and Service Access Management** > **Access Groups** > **Object Sharing Rules**.
3. Publish the rule changes by selecting **Publish Rules** from the **Actions** menu.
4. Run the Perform Object Sharing Rule Assignment Processing scheduled process to ensure that the access group sharing rules for each object are assigned properly.
5. Verify the changes to your access group rules and their associated conditions and candidates on the Object Sharing Rules page.

Import Access Groups and Group Members

You can import access groups and group members into your sales environment, instead of creating them manually in the UI.

To import access groups and group members, create two import CSV files, one for each of these objects:

- Access groups

- Access group members

Import the access groups first, then the group members.

Note: You can't import system groups or add members to system groups using the import functionality. If you export a system access group and then import the group data, the group is created as a custom group.

Before you begin, you need to understand how your source data maps to the target object attributes in your application. You also must identify the target object attributes your CSV import file.

Review Required Attributes for Access Group and Access Group Member Objects

The tables in this section list the attributes you need to specify when importing access groups and members. Some attributes are required to uniquely identify the object record and some are optional. Make sure that you provide valid values for these attributes so that they pass import validations built into the application.

This table lists the attributes for importing access groups:

Attribute	Description
Name	The name of the access group. This is a required attribute and the name you specify must be unique. If you enter the name of an existing group, the record isn't imported.
AccessGroupNumber	The number of the access group. This is an optional attribute. If you don't specify a number, it's assigned automatically.
Description	The access group description. This is an optional attribute.
Active	A value to indicate whether or not the access group is active. This is an optional attribute.

This table lists the required attributes for importing access group members.

Attribute	Description
PartyNumber	This is the resource registry ID of an existing user in the application. You can find this value for a user on the Add: Group Members page in the Sales and Service Access Management work area. This attribute is required.
AccessGroupNumber	The number of the group you want to assign the user to. This number must match the number of one of the groups you previously imported. This attribute is required.

Create the Source CSV File

You include the data that you want to import into your application in a source CSV file. Create a separate CSV file for the Access Groups or Access Group Members data you want to import. You can use the templates available in the Import Objects UI page to create the source CSV file. To download a template:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**.
2. Select either the **Access Groups** or **Access Group Members** object in the Import Object Details table and click **Download**.

   You can now edit the downloaded file and provide valid values for the required attributes.

Create the Import Activity

Once you have the CSV file ready, create an import activity to import the access group information:

1. Navigate to the Manage Imports page: **Tools** > **Import Management** > **Import Queue**, and then click **Create Import Activity**.
2. In the Enter Import Options page, provide values for these fields:

Field	Description
Name	The name you want to assign to the import.
Object	From the **Object** drop-down list, select **Access Groups** or **Access Group Members** depending on the object data you're importing. Import access groups before you import access group members.
File Name	Select the CSV file you previously created for the import data.

3. If you're importing records for the Access Groups object, you can also import records for the child object, Access Group Members, at the same time using these steps:
   a. Click the **Import Object Hierarchy** link. Now you can see the object hierarchy for Access Groups.
   b. Select the **Enabled** check box for the Access Group Members child object.
   c. Select the CSV file for the Access Group Members child object.
4. Click **Next**.
5. On the Map Fields page, you'll see that the source and target attributes are automatically mapped. Review and edit the mappings if required.
6. Check the file for unmapped columns or data format issues by clicking **Validate Data**. Click **Next**.
7. On the Review and Submit page, review the import details and then click **Submit** when you're ready.

Review the Import Results

Use the Manage Imports page to check whether your import succeeded. The Manage Imports page shows the status of all active, completed, and unsuccessful imports.

1. Navigate to the Manage Imports page: **Navigator** > **Import Management** > **Import Queues**.

a. Click the **All Imports** infotile and search for the import activity that you created earlier.
b. Check the Status column for the import activity. The import is successful if the status displays as Completed. You can drill down on the import activity to go to the Import Status page, which provides the status details of the import activity.

2. After the import process completes successfully, navigate to the Access Groups page in the Sales and Service Access Management work area: **Navigator** > **Sales and Service Access Management** > **Access Groups**.
3. Verify that you can see the access groups you imported and that they're assigned the correct members.

   Notice that imported users are listed in the Member Type column as Manual users. This is because they weren't added to the group through group membership rule processing.

Import Access Extension Rules and Rule Details

You can use import management to create, update or delete custom access extension rules. When importing predefined access extension rules, the only updates you can make are to activate or inactivate the rule.

You can import access extension rule data for these objects:

- Access Group Extension Rule
- Access Extension Rule Detail

Import access extension rules before you import rule details. To import data for each object, create a separate CSV file containing the data you want to import.

Before You Start

Before you import access extension rules and rule details, make sure that the access group relationships used in the rules already exist in your target environment. If they don't, the import rules process fails for any rules that are based on those relationships.

You can't use the standard import framework to import access group relationship data. So, to create the relationships in your target environment, you must first perform a configuration migration between your source and target environments. For information, see the topic, *Migrate Access Group Rules Setup Data*, in this guide.

Review Required Attributes and Validations for Access Extension Rule Objects

Before you begin the import, you need to understand how your source data maps to the target object attributes in your application. You also must identify the target object attributes your CSV import file.

The tables in this section list the attributes that are required when importing access extension rules and rule details. Some attributes are required to uniquely identify the object record, some are conditionally required depending on whether you want to create, update, or delete an object record, and some are optional. Make sure that you provide valid values for these attributes so that they pass import validations built into the application.

This table lists the required attributes for importing access extension rules:

Attribute	Description	Import Validations	Creating a Rule	Updating an Existing Rule	Deleting an Existing Rule
Name	The name of the access extension rule.	Not applicable.	Required	Optional	Optional

Attribute	Description	Import Validations	Creating a Rule	Updating an Existing Rule	Deleting an Existing Rule
RelationshipName	The name of the relationship between the objects specified in the rule.	To identify the relationship name, export the Access Group Relationship object from the source environment. To export, navigate to Tools > Export Management > Create Export Activity.	Required	Optional	Optional
RelationshipTypeCode	Specifies whether the relationship is predefined by Oracle (Standard) or custom (Custom).	Not applicable.	Required	Optional	Optional
RelationshipId	The identifier of the access group relationship.	Not applicable.	Optional	Optional	Optional
RelationshipDisplayNar	The display name of the relationship.	Not applicable.	Optional	Optional	Optional
SourceObjectCode	The code of the source object used in the relationship.	Not applicable.	Optional	Optional	Optional
TargetObjectCode	The code of the target object used in the relationship.	Not applicable.	Optional	Optional	Optional
SourceObjectName	The name of the source object used in the access group relationship.	Not applicable.	Optional	Optional	Optional
TargetObjectName	The name of the target object used in the access group relationship.	Not applicable.	Optional	Optional	Optional
AccExtRuleNumber	The alternate key identifier for the access extension rule. It is a unique system generated sequence number.	Not applicable.	Optional	Required	Required
ExtendAllRulesFlag	Indicates the method used to identify which rules from the source object should be extended to the target object.	Not applicable.	Required	Optional	Optional

This table lists the required attributes for importing access extension rule details:

Attribute	Description	Import Validations	Creating Rule Details	Updating Existing Rule Details	Deleting Existing Rule Details
SrcObjectRuleNumber	The alternate key identifier of the rule on the source object.	Not applicable.	Required	Required	Required
AccessGroupNumber	The alternate key identifier of the access group associated to the rule on the source object.	Not applicable.	Required	Required	Required
ReadAccessPermissionI	Indicates whether read access is granted.	Not applicable.	Optional	Optional	Optional
AccExtRuleNumber	The number of the access extension rule.	Not applicable.	Required	Required	Required
AccExtRuleDetailId	The identifier of the access extension rule details.	Not applicable.	Optional	Optional	Optional
DeleteAccessPermissio	Indicates whether delete access is granted.	Not applicable.	Optional	Optional	Optional
SrcObjectRuleGuid	The unique identifier of the rule on the source object.	Not applicable.	Optional	Optional	Optional
UpdateAccessPermissic	Indicates whether update access is granted.	Not applicable.	Optional	Optional	Optional

Create the Source CSV File

You include the data that you want to import into your application in a source CSV file. Create a separate CSV file for the access extension rules and access extension rule details you want to import. You can use the templates available in the Import Objects UI page to create the source CSV file. To download a template:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**.
2. Select either the **Access Group Extension Rule** or **Access Group Extension Rule Detail** object in the Import Object Details table and click **Download**.

   You can now edit the downloaded file and provide valid values for the required attributes.

Create the Import Activity

Once you have the CSV file ready, create an import activity to import the rule information.

CAUTION: Make sure custom objects and attributes are synchronized before running the import.

1. Navigate to the Manage Imports page (**Navigator** > **Tools** > **Import Management** > **Import Queue**).
2. Click **Create Import Activity**.

3. In the Enter Import Options page, provide values for these fields:

Field	Description
Name	The name you want to assign to the import.
Object	From the **Object** drop-down list, select **Access Group Extension Rule** or **Access Extension Rule Detail** depending on the object records you're importing.
File Name	Select the CSV file you previously created for the rule import data. Import access extension rules before you import access extension rule details.
Import Mode	In the Advanced Options area, in the **Import Mode** field, select whether you want to update and create records, only create records, or delete records.

4. Click **Next**.
5. On the Map Fields page, you'll see that the source and target attributes are automatically mapped. Review and edit the mappings if required.
6. Check the file for unmapped columns or data format issues by clicking **Validate Data**. Click **Next**.
7. On the Review and Submit page, review the import details and then click **Submit** when you're ready.

Review the Import Results

Use the Manage Imports page to check whether your import succeeded. The Manage Imports page shows the status of all active, completed, and unsuccessful imports.

1. Navigate to the Manage Imports page: **Navigator** > **Import Management** > **Import Queues**.
    a. Click the **All Imports** infotile and search for the import activity that you created earlier.
    b. Check the Status column for the import activity. The import is successful if the status displays as Completed. You can drill down on the import activity to go to the Import Status page, which provides the status details of the import activity.
2. After the import process completes successfully, navigate to the Object Sharing Rules page: **Navigator** > **Sales and Service Access Management** > **Access Groups** > **Object Sharing Rules**.
3. Publish the rule changes by selecting **Publish Rules** from the **Actions** menu.
4. The Perform Object Sharing Rule Assignment Processing scheduled process automatically runs at scheduled intervals. When the process is finished, verify the changes to your access group extension rules on the Object Sharing Rules page.

Related Topics

- Migrate Access Group Rules Setup Data

Export Access Groups, Members, and Rules

Using Import and Export Management, you can export access group objects from your sales environment into CSV files. The access group objects you can export include:

- Access groups
- Access group members
- Access group rules (group membership rules and predefined and custom object sharing rules)
  Each access group rule can have multiple rule conditions and can be assigned to multiple access groups (rule candidates). You can also choose to export only rule conditions or only rule candidates.
- Access group extension rules
- Access group extension rule details
- Access group relationships

For each object you export, you can select the data attributes you want to download for data analysis. You can also use filters to specify the range of access groups, members, or rules to export. For example, you can use filters to export access group rules for a specific object, such as the Account object. Ensure that any custom objects or attributes are synchronized before you export your access group rules.

CAUTION: Ensure that any custom objects or attributes are synchronized before you export your access group rules.

Here's how to export access group object details to a CSV file.

1. Navigate to **Tools** > **Export Management**.
2. On the Manage Exports page, click **Create Export Activity**.
3. On the Create Export Activity: Enter Export Options page, select a name for the export job in the **Name** field.
4. From the **Object** drop-down list, select one of the access group objects:
   - Access Groups
   - Access Group Members
   - Access Group Rule
   - Access Group Rule Candidate
   - Access Group Rule Condition
   - Access Group Extension Rule
   - Access Group Extension Rule Detail
   - Access Group Relationship

   You can export child objects at the same time as the parent object or you can export child objects individually. For example, Access Group Rule Candidate and Access Group Rule Condition are child objects of Access Group Rule, so you can export all three objects at the same time by selecting the Access Group Rule object.
   Similarly, Access Group Extension Rule Detail is a child object of Access Group Extension Rule so you can export both of these objects at the same time by selecting the Access Group Extension Rule object.
   The **File Name** field is automatically filled with a file name to reflect the object type you selected. For example, if you selected Access Group Rule as the object to export, a file name similar to

AccessGroupRule20200731_1307.zip is generated for you. If you select Access Group Rule Candidate, then a file name such as **AccessGroupRuleCandidate20200731_1310.zip** is automatically entered.

5. In the Advanced Options region, select **Language Independent Header** to ensure that column headers display correctly in the exported CSV file, then click **Next**.
6. On the Create Export Activity: Map Fields page, you can select the fields to export.

   Alternatively, you can select an existing mapping from the **Export Mapping** drop-down list which shows the maps that were used in earlier export jobs.
7. In the Export Objects area, select the child objects, if any, that you want to export by selecting the **Enabled** check box.
8. In the Attributes area, select the attributes you want to export for the selected object or objects by double-clicking the attribute in the **Available Fields** list or manually moving the attribute from the **Available Fields** list to the **Selected Fields** list.

   For example, for the Access Group object, you might select these fields: **Number**, **Name**, **Description**, **Active**.
9. You must provide a filter criterion for at least the top-level object. To filter the records to export using conditions, in the Export Objects area, click the **Filter Name** icon to display the **Filter Name** dialog box.
10. To create the filter:

    a. On the **Fields** tab select the attribute you want to use to filter the access group data that's exported and click the **Insert** button.
    b. In the Script Edit window, provide the filter conditions for the selected attribute using the available operators such as **AND**, **OR**, **=**, and **!=**.
    c. After creating the filter criteria script, click **Validate Script**.

    Here are some examples of filter criteria you might define for different access group objects.

Access Group Export Object	Filter Condition	Filter Script
Access Group Rule	Export all access group rules including object sharing rules and group membership rules.	`ObjectName != 'Null'`

Access Group Rule	Export group membership rules only.
	
	Export object sharing rules only.
		`ObjectName = 'Resources'`
		
		`ObjectName != 'Resources'`

Access Group Rule	Export access group rules for the Account object.	`ObjectName = 'Account'`
Access Groups	Export data for a specific access group.	`GroupName='France_Admin_Group'`
Access Groups and Access Group Members	Export all access groups with a specific member.	`EmailAddress='email_address'`

11. If the script validates successfully, click **Save and Close** to save the filter, then click **Next**.

12. On the Create Export Activity: Review and Submit page, review the export activity configuration, then click **Submit** to activate the export activity.
13. On the Manage Exports page, review the export job and when it completes, click the file link in the **Exported Data File** column to download the exported file. Verify that the file contains all the information you wanted to export.

Related Topics

- How You Monitor Export Activity

Migrate Access Group Rules Setup Data

You can migrate object sharing rules setup data from one environment to another using Import and Export Management.

If you export and import rules setup data using this option, make sure that any access groups and group members that exist in the source environment are created in the target environment before you import the object sharing rules. Otherwise, the rules aren't assigned correctly.

Perform the migration steps in this sequence:

1. (Optional) Perform a configuration set migration to move any configurations you have made in the source environment, such as creating custom objects or attributes, or creating custom relationships between objects, to the target environment.

   For information on this step, see the chapter about migration in the *Configuring and Extending Applications* guide.
2. Synchronize all custom objects and attributes you migrated in the previous step using the Manage Object Sharing Assignment Objects task in the Setup and Maintenance work area:

   a. Sign in as a setup user and navigate to the Setup and Maintenance work area.

   b. Select the Sales offering, then search for and select the Manage Object Sharing Assignment Objects task.
   c. From the **Actions** menu, select **Export to CSV File**.
   d. Once the rules are exported, download and extract the CSV file.
   e. In the target environment, import the CSV file you just extracted by selecting the Manage Object Sharing Assignment Objects task in the Setup and Maintenance work area.
   f. From the **Actions** menu, select **Import from CSV File**.

      You don't have to run the **Synchronize Custom Objects and Fields** option on the Object Sharing Rules page in the target environment after the import process completes.
3. Export and then import access groups and group members from your source environment to your target environment using the standard export and import framework.
4. Export and then import object sharing rules, including access extension rules, from your source environment to your target environment using the standard export and import framework.

   See the import and export topics in this chapter for information on importing and exporting access group objects.
5. After the import process completes successfully, navigate to the Object Sharing Rules page: **Navigator** > **Sales and Service Access Management** > **Access Groups** > **Object Rules**.

6. Publish the rule changes by selecting **Publish Rules** from the **Actions** menu.

   The Perform Object Sharing Rule Assignment Processing process automatically runs at scheduled intervals. When the process is finished, verify that the object sharing rules and group membership rules are displaying correctly in your environment.

For detailed information on importing and exporting setup data, see the topic, Export and Import CSV File Packages*Export and Import CSV File Packages*. For an example of importing and exporting Assignment Manager objects, see the topic, *Example of Uploading Assignment Objects and Rules Setup Data to a CSV File*.

20 Data Security Policy to Access Group Rule Migration

Migration Overview

You can use the predefined object sharing rules available with access groups to give users the same access to object data that the predefined data security policies provide.

If you want to replace data security policies with access group rules as the method used to provide your users with access to object data, this chapter provides all the information you need. It includes:

- The steps to follow to migrate from data security policies to access group rules.
- Tables for each object that list the predefined rule or rules that correspond to each of the data security policies defined for the object. Use these tables to identify:
  - The data security policies you need to deactivate
  - The corresponding predefined rules you need to enable

Note: If you're using the sales application for the first time in release 22B or later, your database resources are secured using system access groups and rules by default. You don't need to perform the steps described in this chapter.

Migrate from Data Security Policies to Access Group Rules

You can provide users with access to sales and service data using data security policies, access group rules, or a combination of both.

If you started using the sales application before release 22B, the predefined job roles and any custom job roles you create provide users with data access using data security policies. But you can supplement or refine the access each type of role provides using either data security policies or access groups rules.

You can also configure custom job roles so that the data access they provide is achieved using only, or primarily, access group rules. For example, you might decide that you want users assigned a custom sales representative job role to access object records using access group rules. To do this, you deactivate the data security policies assigned to the custom job role, then assign access group rules that provide the same access to the system access group generated for the custom role.

Note: Data security policies for the predefined job roles are locked and can't be deactivated.

There are five steps in the process of migrating a custom role to provide data access primarily through access group rules:

1. *Identify the Data Security Policies to Deactivate*
2. *Identify the Access Group Rules that Correspond to Data Security Policies*
3. *Add Rules to the Access Group Generated for the Custom Role*
4. *Deactivate Data Security Policies*
5. *Verify User Access to Data*

> **Tip:** It's a good idea to devise a few use-cases you can use to compare users data access before and after the migration process. That way, you can identify any gaps and avoid potential user access issues.

Identify the Data Security Policies to Deactivate

The first step in the process of migrating a custom job role to use access group rule data access is to identify the data security policies assigned to the custom role, then determine which policies you can deactivate and replace with access group rules.

1. Sign in to the application as a user with the IT Security Manager job role and select **Navigator** > **Tools** > **Sales and Service Access Management.**
2. Click the Manage Data Policies tab on the Sales and Service Access Management page.
3. On the Manage Data Policies page, select the custom role you want to migrate in the **Role** field.

   For this example, let's say the role is called **Sales Representative Custom**.
4. Select an object in the **Object** field. For example, select the **Opportunity** object to view the opportunity data security policies assigned to the role.
5. Click **Find Policies**.

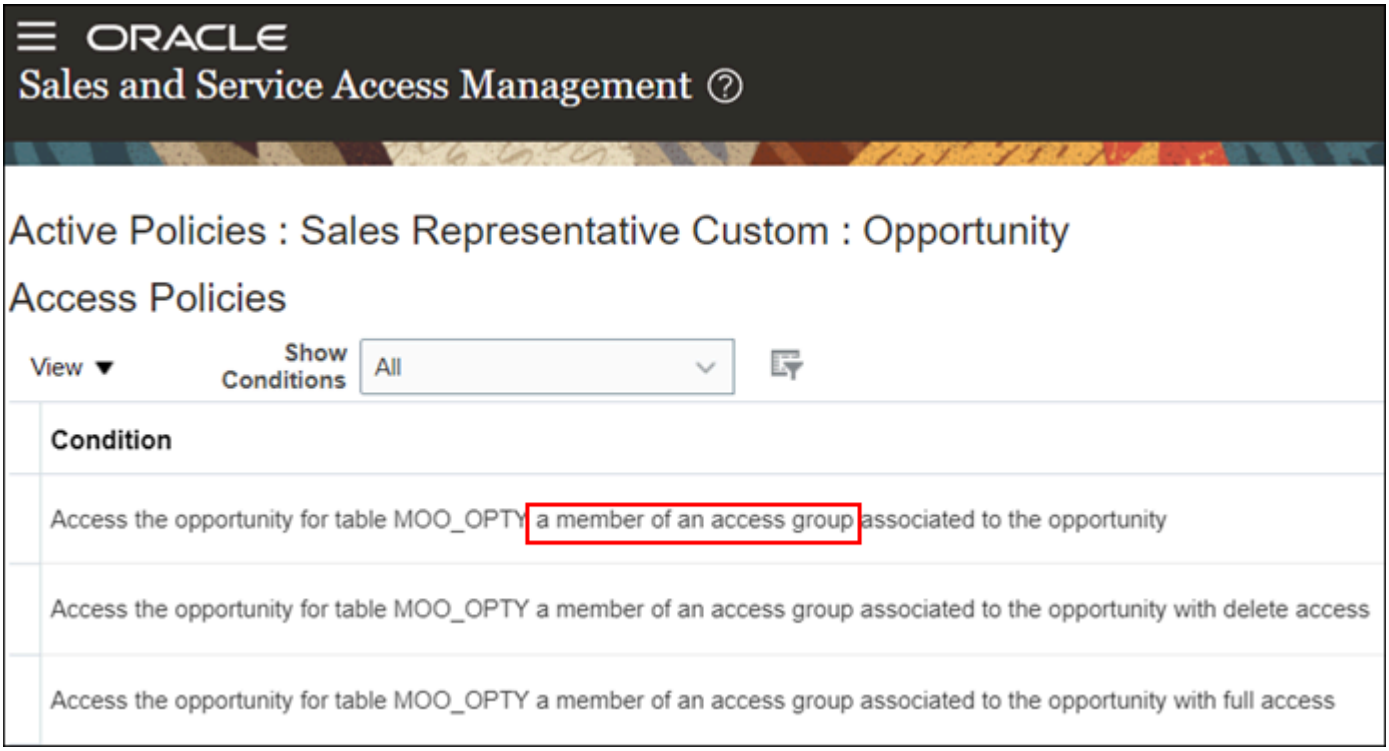
   The Active Policies table lists all the active data security policies for the opportunity object that are assigned to the Sales Representative Custom job role.
6. Click the Edit icon.

   The Active Policies edit page for the selected role and object is displayed.
7. Review the policies listed and identify active data security policies that are unlocked and can be edited.

   Some policies might be locked and can't be deactivated. For example, you can't deactivate policies that are inherited from predefined duty roles because predefined roles can't be edited. The permissions for these policies are grayed out.

8. Identify data security policies that are eligible for deactivation.

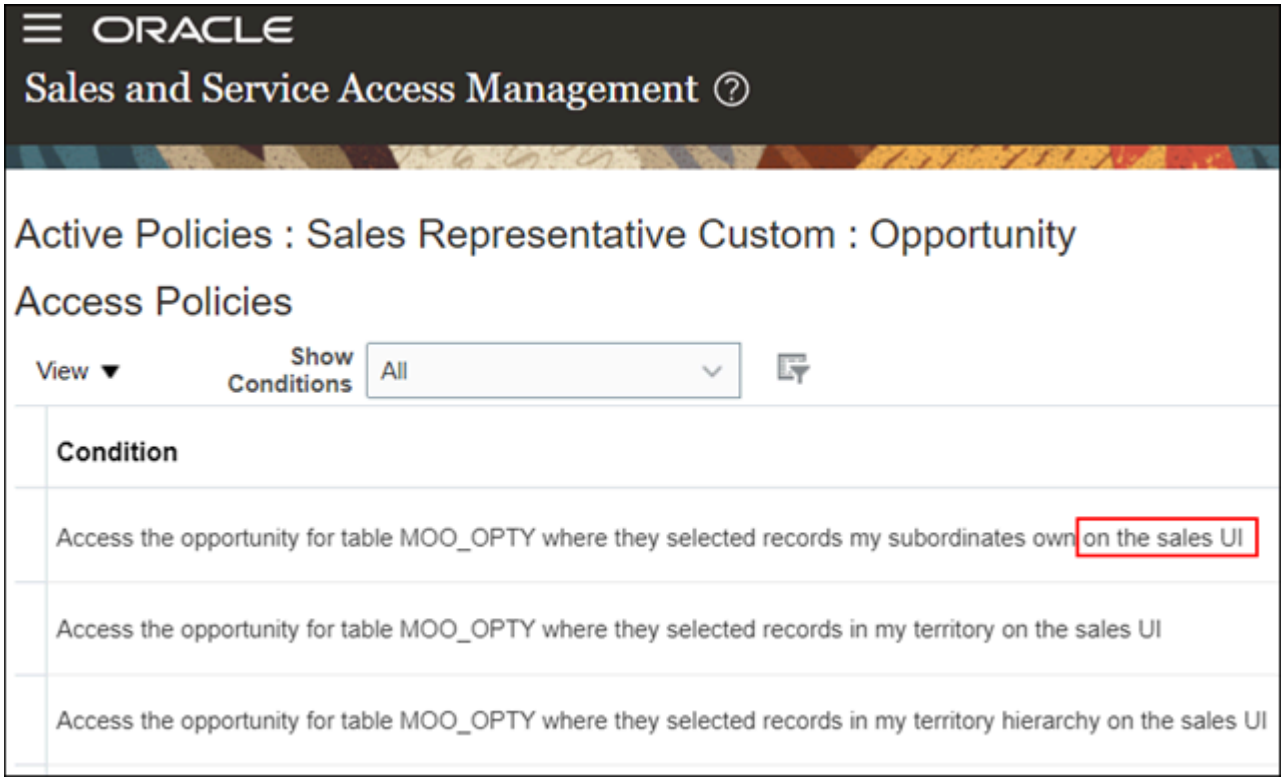
   Don't edit any policy where the Condition name of the policy includes a reference to 'access group'. These policies, shown in the screenshot, are required for users to get access to object data through access groups and must remain associated with the custom role.



9. Check if all of the active, unlocked policies that are eligible for deactivation are required:
    a. Make a note of each of the required policies and, for each policy, note the current permission levels selected.

       You'll need to activate corresponding access group rules that provide the same access levels as these policies.
    b. Make a note of each policy that isn't required. You can deactivate these policies without having to activate a corresponding access group rule.

       You can deactivate any policies that grant access based on sales UI privileges. These policies are redundant. The Condition name of these privileges contains a reference to 'sales UI' as shown in the screenshot.



10. Repeat steps 3-8 for each object associated with the Sales Representative Custom role that you want to migrate to using access group rule data access. You can migrate a custom role to use access group rules for all objects, or just for specific objects.

Results:

At the end of the process, for your custom role and object, you should have identified and noted:

- All the data security policies to be deactivated
- All the policies marked for deactivation for which you have to assign a corresponding access group rule
- The access levels you need to set for each rule you assign

Identify the Access Group Rules that Correspond to Data Security Policies

To replace data security policies with access group rules as a way of providing data access for a custom job role, identify the rule or rules that provide the same data access as each policy you're going to deactivate for the role. This chapter includes a table for each object that supports access groups. Each table lists the access group rules that correspond to each of the data security policies defined for the object.

1. Review the relevant table for the object you want to migrate and make a note of the object sharing rule that provides the same access as each policy you intend to deactivate.
2. Repeat step 1 for each object that you're switching to use access group rules data access.

   For example, to see how each data security policy defined for the Opportunity object maps to access group rules defined for that object, review the *Opportunity Object Mapping* table. Then repeat the process for Leads, Accounts, Contacts, and so on as required.

   A data security policy can map to more than one access group rule. When you deactivate a policy, make sure you enable all the rules the policy maps to for the relevant access group. For example, the Opportunity Object Mapping table includes these rows:

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Opportunity	MOOOPTYZBS9	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy	Opportunity	Account Territory Team	AccountPR9	Accounts where the access group member is a member of the territory associated with the account	ACCOUNTTERRITORY
Opportunity	MOOOPTYZBS9	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward	Opportunity	Account Territory Team Hierarchy	AccountPR10	Accounts where the access group member is a member of the territory that is an ancestor of the territory associated with the account	ACCOUNTTERRITORYHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		territory hierarchy					

In this case, one data security policy (shown in column 3) provides data access based on territory team and territory-team hierarchy membership. But two access group rules, Account Territory Team and Account Territory Team Hierarchy (shown in column 5), must be assigned to provide the same access.

Add Rules to the Access Group Generated for the Custom Role

Once you've identified the access group rule or rules that correspond to each policy you intend to deactivate for a custom job role, you then assign the rules to the system access group generated for the custom role when the role was created. This way, you don't lose your existing access paths to object data.

When you create a custom job role, a system access group is generated for the role but it isn't assigned any access group rules. You can add the rules you identified in the previous step to your custom access group manually but it's generally easier to copy the object sharing rules from another access group that provides similar access, then edit the rules as required.

For example, when you created the Sales Representative Custom job role, a system group, Sales Representative Custom Group, was generated. You can copy the object sharing rules from the group generated for the predefined Sales Representative job role (Sales Representative Group), then edit the rules as required for the Sales Representative Custom Group. Here are the steps to use.

1. Navigate to the Sales and Service Access Management work area.
2. On the Access Groups page, select **System Groups-Role** from the **List** menu.
3. Select the access group whose rules you want to copy. For this example, select **Sales Representative Group**.
4. On the Edit Access Group: Overview page, select the **Copy Rules** option from the **Actions** menu. The Copy Object Sharing Rules dialog is displayed.
5. From the Copy to Group drop-down list, select the group you want to copy the rules to. In this example, select the **Sales Representative Custom Group**.
6. Click **Save**. The rules are copied to your selected group.
7. Click **Save and Close** on the Edit Access Group: Overview subtab.
8. Once the rules are copied, on the Access Groups page, select the access group you've just copied the rules to, in this case, the **Sales Representative Custom Group**.
9. On the Edit Access Group: Overview page, click the Object Rules subtab.
10. Review the new rules assigned to the group against the list of rules you noted in the previous step (Identify the Access Group Rules that Correspond to Data Security Policies).
11. Delete any rules that aren't required by your access group by clicking the Delete icon for the rule.
12. Add any additional rules needed by clicking **Add Rule**, then selecting the rules to add.

13. For rules that are required:
    a. Verify that the access levels defined for the rule are correct.

       The access levels for a rule should be the same as those defined for the corresponding data security policy. Change the access levels as needed.

    b. Click the **Enable** check box for each rule you want to enable for the group.
    c. Activate any rule that's inactive by clicking the rule name link.

       On the Edit Object Sharing Rule page, click the **Active** check box to activate the rule, then click **Save and Close**.

14. On the Object Sharing Rules page, click **Save and Close** to save your changes.
15. Publish the new rules you copied and enabled for your custom access group by navigating to the Access Groups page, selecting the Object Rules tab, then selecting **Publish Rules** from the **Actions** menu.

Related Topics

- Identify the Access Group Rules that Correspond to Data Security Policies

Deactivate Data Security Policies

Once you've added the required access group rules to your custom access group, in this case, the Sales Representative Custom group, deactivate the policies you identified as candidates for deactivation in the step Identify the Data Security Policies to Deactivate.

You can deactivate a policy by removing all the permissions assigned to the policy. Alternatively, you can enter an end-date for the policy and specify a date in the past using these steps.

1. Navigate to the Sales and Service Access Management work area.
2. Click the Manage Data Policies tab.
3. Search for the custom job role, for example, **Sales Representative Custom**, in the **Role** field.
4. Select an object, for example **Opportunity**, in the **Object** field, then click **Find Policies**.
5. Click the Edit icon for the Active Policies table.

   The Active Policies edit page for the selected role and object is displayed.

6. In the Active Policies table, for each policy you want to deactivate for the object, select a date that has passed in the policy's **End Date** field. For example, select yesterday's date.
7. Repeat steps 3-5 for all the other objects assigned to the role that you want migrate to using access group rules data access.
8. Click **Save and Close**.

Related Topics

- Identify the Data Security Policies to Deactivate

Verify User Access to Data

Verify that the migration process didn't impact users access to object data.

Test users' access to each type of object data that you migrated to access group rules. Make sure that users assigned your custom role have the same access to data after the migration as they did before the migration.

Account Object Mapping

For each of the data security policies available for the Account object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZBS1(	Access the sales party for table HZ_PARTIES where they are the account owner	Account	Account Owner	AccountPR1	Accounts where the access group member is the account owner	ACCOUNTOWNER
Trading Community Party	HZPARTIESZBS1(	Access the sales party for table HZ_PARTIES where they are in the management chain of the account owner	Account	Account Owner Hierarchy	AccountPR2	Accounts where the access group member is in the management chain of the account owner	ACCOUNTOWNERHIER
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES where user is in the sales account team	Account	Account Team	AccountPR3	Accounts where the access group member is on the account team	ACCOUNTTEAM
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the sales account team with edit access	Account	Account Team with Edit Access	AccountPR5	Accounts where the access group member is on the account team with edit access	ACCOUNTTEAMWITHEDIT

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the sales account team with full access	Account	Account Team with Full Access	AccountPR7	Accounts where the access group member is on the account team with full access	ACCOUNTTEAMWITHFULL
Trading Community Party	HZPARTIESZCM3	Access the sales party for table HZ_PARTIES where user is in the management chain of a resource who is on the sales account team	Account	Account Team Hierarchy	AccountPR4	Accounts where the access group member is in the management chain of a resource who is on the account team	ACCOUNTTEAMHIER
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the management chain of a resource who is on the sales account team with edit access	Account	Account Team Hierarchy with Edit Access	AccountPR6	Accounts where the access group member is in the management chain of a resource who is on the account team with edit access	ACCOUNTTEAMHIERWITH
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the management chain of a resource who is on the sales account team with full access	Account	Account Team Hierarchy with Full Access	AccountPR8	Accounts where the access group member is in the management chain of a resource who is on the account team with full access	ACCOUNTTEAMHIERWITH
Trading Community Party	HZPARTIESZCM3	Access the sales party for table HZ_PARTIES where user is a member of the territory associated with the sales account	Account	Account Territory Team	AccountPR9	Accounts where the access group member is a member of the territory associated with the account	ACCOUNTTERRITORY

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is a member of the territory that is an ancestor of the territory associated with the sales account	Account	Account Territory Team Hierarchy	AccountPR10	Accounts where the access group member is a member of the territory that is an ancestor of the territory associated with the account	ACCOUNTTERRITORYHIER
Trading Community Party	HZPARTIESZCM5	Access the sales party for table HZ_PARTIES where user is the owner of the territory associated with the sales account	Account	Account Territory Owner	AccountPR11	Accounts where the access group member is the owner of the territory associated with the account	ACCOUNTTERRITORYOWN
Trading Community Party	HZPARTIESZCM5	Access the sales party for table HZ_PARTIES where user is the owner of the territory that is an ancestor of the territory associated with the sales account	Account	Account Territory Owner Hierarchy	AccountPR12	Accounts where the access group member is the owner of the territory that is an ancestor of the territory associated with the account	ACCOUNTTERRITORYOWN
Trading Community Party	HZPARTIESZCM8	Access the sales party for table HZ_PARTIES for all sales parties in the enterprise	Account	All Parties	AccountPR13	Access all parties	GLOBAL_ ACCOUNT
Trading Community Party	HZPARTIESHZ54	Access the trading community party for table HZ_PARTIES all accounts in the enterprise	Account	All Accounts	AccountPR14	Access all accounts	ALLACCOUNTS
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES for all prospects in the enterprise	Account	All Prospects	AccountPR15	Access all prospects	ALLPROSPECTS

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES for all customers in the enterprise	Account	All Customers	AccountPR16	Access all customers	ALLCUSTOMERS

Activity Object Mapping

For each of the data security policies available for the Activity object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ACTIVITIES where they are only an owner of an activity	ACTIVITY	Activity Owner	ActivityPR1	Activities where the access group member is the activity owner	ACTIVITYOWNER
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ACTIVITIES where they are only a delegator of an activity	ACTIVITY	Activity Delegator	ActivityPR2	Activities where the access group member is a delegator	ACTIVITYDELEGATOR
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ACTIVITIES where they are in the management chain of an owner only of an activity	ACTIVITY	Activity Owner Hierarchy	ActivityPR3	Activities where the access group member is in the management chain of the activity owner	ACTIVITYOWNERHIER
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ACTIVITIES	ACTIVITY	Activity Delegator Hierarchy	ActivityPR4	Activities where the access group member is in the	ACTIVITYDELEGATORHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		where they are in the management chain of a delegator only of an activity				management chain of a delegator on the activity	
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are only a resource of an activity	ACTIVITY	Activity Resource	ActivityPR5	Activities where the access group member is an activity resource	ACTIVITYRESOURCE
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are in the management chain of a resource only of an activity	ACTIVITY	Activity Resource Hierarchy	ActivityPR11	Activities where the access group member is in the management chain of a resource on the activity	ACTIVITYTASKRESOURCEH
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES for all template activities in the enterprise.	ACTIVITY	All Activity Templates	ActivityPR6	Access to all activity templates	ALLACTIVITYTEMPLATES
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or an owner or a delegator of a call report activity.	ACTIVITY	Activity Task Resource	ActivityPR7	Tasks where the access group member is a resource on the task	ACTIVITYTASKRESOURCE
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are	ACTIVITY	Activity Task Delegator	ActivityPR8	Tasks where the access group member is a delegator on the task	ACTIVITYTASKDELEGATOR

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		either a resource or a delegator of a task or an owner or a delegator of an appointment or an owner or a delegator of a call report activity.					
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ACTIVITIES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or an owner or a delegator of a call report activity.	ACTIVITY	Activity Appointment and Call Report Owner	ActivityPR9	Call reports and appointments where the access group member is the owner	ACTIVITYAPPTANDCROWN
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ACTIVITIES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or an owner or a delegator of a call report activity.	ACTIVITY	Activity Appointment and Call Report Delegator	ActivityPR10	Call reports and appointments where the access group member is the delegator	ACTIVITYAPPTANDCRDELE
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ACTIVITIES where they are either the owner or a delegator of an activity.	ACTIVITY	Activity Delegator	ActivityPR2	Tasks where the access group member is a delegator on the task	ACTIVITYDELEGATOR
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ACTIVITIES	ACTIVITY	Activity Owner	ActivityPR1	Activities where the access group member	ACTIVITYOWNER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		where they are either the owner or a delegator of an activity.				is the activity owner	
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are in the management chain of an activity resource.	ACTIVITY	Activity Resource Hierarchy	ActivityPR11	Activities where the access group member is in the management chain of a resource on the activity	ACTIVITYRESOURCEHIER
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are in the management chain for a task activity or they are an owner for an appointment activity.	ACTIVITY	Activity Appointment and Call Report Owner	ActivityPR9	Call reports and appointments where the access group member is the owner	ACTIVITYAPPTANDCROWN
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are in the management chain for a task activity or they are an owner for an appointment activity.	ACTIVITY	Activity Task Resource Hierarchy	ActivityPR12	Tasks where the access group member is the management chain of a resource on the activity	ACTIVITYTASKRESOURCEH
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES for all activities in the enterprise	ACTIVITY	Activity Resource	ActivityPR5	Activities where the access group member is an activity resource	ACTIVITYRESOURCE
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES for all activities in the enterprise	ACTIVITY	All Nonprivate Activities	ActivityPR13	Access to all nonprivate activities	ALLNONPRIVATEACTIVITIE

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are a member of the partner territory	ACTIVITY	Activity Partner Territory	ActivityPR15	Activities where the access group member is a partner on the territory for the activity	ACTIVITYPARTNERTERRIT
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are a member of the partner territory	ACTIVITY	Activity Partner Territory Hierarchy	ActivityPR16	Activities where the access group member is in the partner territory hierarchy for the activity	ACTIVITYPARTNERTERRIT
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where partner users are resources in the activity	ACTIVITY	Activity Nonprivate Partner Company	ActivityPR17	Activities where the access group member is in the partner company on the activity	ACTIVITYNONPRIVATEPAR
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where partner users are resources in the activity	ACTIVITY	All Nonprivate Activities for Child Partner Companies	ActivityPR18	Activities where the access group member is a member of an ancestor partner company related to the activity	ACTIVITYNONPRIVATEPAR
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are only a delegator of an activity	ACTIVITY	Activity Delegator	ActivityPR2	Activities where the access group member is a delegator	ACTIVITYDELEGATOR
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are only a delegator of an activity	ACTIVITY	Activity Resource	ActivityPR5	Activities where the access group member is an activity resource	ACTIVITYRESOURCE
ACTIVITY	ZMMACTYACTIV	Access the activity for table	ACTIVITY	Activity Delegator	ActivityPR2	Activities where the access	ACTIVITYDELEGATOR

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		ZMM_ACTY_ ACTIVITIES where they are a participant on the activity.				group member is a delegator	
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are a participant on the activity.	ACTIVITY	Activity Resource	ActivityPR5	Activities where the access group member is an activity resource	ACTIVITYRESOURCE
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or a call report activity.	ACTIVITY	Activity Appointment and Call Report Owner	ActivityPR9	Call reports and appointments where the access group member is the owner	ACTIVITYAPPTANDCROWN
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or a call report activity.	ACTIVITY	Activity Appointment and Call Report Delegator	ActivityPR10	Call reports and appointments where the access group member is the delegator	ACTIVITYAPPTANDCRDELE
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or a call report activity.	ACTIVITY	Activity Task Resource	ActivityPR7	Tasks where the access group member is a resource on the task	ACTIVITYTASKRESOURCE

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or a call report activity.	ACTIVITY	Activity Task Delegator	ActivityPR8	Tasks where the access group member is a delegator on the task	ACTIVITYTASKDELEGATOR
ACTIVITY	ZMMACTYACTIV	Access the activity for table ZMM_ACTY_ ACTIVITIES where they are in the management chain of the activity owner	ACTIVITY	Activity Owner Hierarchy	ActivityPR3	Activities where the access group member is in the management chain of the activity owner	ACTIVITYOWNERHIER

Activity Assignee Object Mapping

For each of the data security policies available for the Activity Assignee object, this topic shows the access extension rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either a resource or a delegator of an activity	Activity Assignee	Delegator of Related Activity	ActivityAssignee/	Predefined rule for delegator of related activity.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are	Activity Assignee	Resource of Related Activity	ActivityAssignee/	Predefined rule for resource of related activity.	ActivityToActivityAssignee

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		either a resource or a delegator of an activity					
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or an owner or a delegator of a call report activity	Activity Assignee	Resource of Related Task	ActivityAssignee/	Predefined rule for resource of related task.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or an owner or a delegator of a call report activity	Activity Assignee	Delegator of Related Task	ActivityAssignee/	Predefined rule for delegator of related task.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or an owner or a delegator of a call report activity	Activity Assignee	Owner or Delegator of Related Appointment	ActivityAssignee/	Predefined rule for owner or delegator of related appointment.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES	Activity Assignee	Owner or Delegator of Related Call Report	ActivityAssignee/	Predefined rule for owner or delegator	ActivityToActivityAssignee

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or an owner or a delegator of a call report activity				of related call report.	
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either the owner or a delegator of an activity	Activity Assignee	Delegator of Related Activity	ActivityAssignee/	Predefined rule for delegator of related activity.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either the owner or a delegator of an activity	Activity Assignee	Owner of Related Activity	ActivityAssignee/	Predefined rule for owner of related activity.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are in the management chain of an activity resource	Activity Assignee	Resource Hierarchy of Related Activity	ActivityAssignee/	Predefined rule for resource hierarchy of related activity.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are in the management chain for a task activity or they are an owner for an appointment activity	Activity Assignee	Resource Hierarchy of Related Task	ActivityAssignee/	Predefined rule for resource hierarchy of related task.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table	Activity Assignee	Owner or Delegator	ActivityAssignee/	Predefined rule for owner	ActivityToActivityAssignee

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		ZMM_ACTY_ASSIGNEES where they are in the management chain for a task activity or they are an owner for an appointment activity		of Related Appointment		or delegator of related appointment.	
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ASSIGNEES where they are in the management chain of the activity owner	Activity Assignee	Owner Hierarchy of Related Activity	ActivityAssignee/	Predefined rule for owner hierarchy of related activity.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ASSIGNEES for all activities in the enterprise	Activity Assignee	Resource of Related Activity	ActivityAssignee/	Predefined rule for resource of related activity.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ASSIGNEES for all activities in the enterprise	Activity Assignee	Assignees of Nonprivate Activities	ActivityAssignee/	Predefined rule for assignees of all non-private activities.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity resource for table ZMM_ACTY_ASSIGNEES where they are a resource for an activity	Activity Assignee	Delegator of Related Activity	ActivityAssignee/	Predefined rule for delegator of related activity.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity resource for table ZMM_ACTY_ASSIGNEES where they are a resource for an activity	Activity Assignee	Resource of Related Activity	ActivityAssignee/	Predefined rule for resource of related activity.	ActivityToActivityAssignee

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or a call report activity	Activity Assignee	Resource of Related Task	ActivityAssignee/	Predefined rule for resource of related task.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or a call report activity	Activity Assignee	Delegator of Related Task	ActivityAssignee/	Predefined rule for delegator of related task.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where they are either a resource or a delegator of a task or an owner or a delegator of an appointment or a call report activity	Activity Assignee	Owner or Delegator of Related Appointment	ActivityAssignee/	Predefined rule for owner or delegator of related appointment.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where partner users are resources in the activity	Activity Assignee	Owner or Delegator of Related Call Report	ActivityAssignee/	Predefined rule for owner or delegator of related call report.	ActivityToActivityAssignee
ACTIVITYASSIGN	ZMMACTYASSIG	Access the activity for table ZMM_ACTY_ ASSIGNEES where partner	Activity Assignee	Partner Resource of Related Activity	ActivityAssignee/	Predefined rule for partner resource of related activity.	ActivityToActivityAssignee

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		users are resources in the activity					

Asset Object Mapping

For each of the data security policies available for the Asset object, this topic shows the access extension rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a sales party team member of the asset owner party	Asset	Assets of Related Asset Owner Account Team	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Team.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a sales party team member of the asset owner party with edit access	Asset	Assets of Related Asset Owner Account Team with Edit Access	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Team with Edit Access.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a sales party team member of the asset owner party with full access	Asset	Assets of Related Asset Owner Account Team with Full Access	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Team with Full Access.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is in the	Asset	Assets of Related Asset Owner Account Team Hierarchy	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Team Hierarchy.	AccountToAssets

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		management chain of a resource who is a sales party team member of the asset owner party					
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ ASSET where user is in the management chain of a resource who is a sales party team member of the asset owner party with edit access	Asset	Assets of Related Asset Owner Account Team Hierarchy with Edit Access	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Team Hierarchy with Edit Access.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ ASSET where user is in the management chain of a resource who is a sales party team member of the asset owner party with full access	Asset	Assets of Related Asset Owner Account Team Hierarchy with Full Access	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Team Hierarchy with Full Access.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ ASSET where user is owner of the territory associated with the asset owner party	Asset	Assets of Related Asset Owner Account Territory Owner	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Territory Owner.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a owner of the territory that is an ancestor of the territory associated with	Asset	Assets of Related Asset Owner Account Territory Owner Hierarchy	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Territory Owner Hierarchy.	AccountToAssets

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		the asset owner party					
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a member of the territory associated with the asset owner party	Asset	Assets of Related Asset Owner Account Territory Team	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Territory Team.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a member of the territory that is an ancestor of the territory associated with the asset owner party	Asset	Assets of Related Asset Owner Account Territory Team Hierarchy	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Territory Team Hierarchy.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET all assets in the enterprise where asset owner party is a customer	Asset	Assets of Related All Asset Owner Account Customers	AccountAssetRul	Predefined rule for assets of Related All Asset Owner Account Customers.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET all assets in the enterprise where asset owner party is a prospect	Asset	Assets of Related All Asset Owner Account Prospects	AccountAssetRul	Predefined rule for assets of Related All Asset Owner Account Prospects.	AccountToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a sales party team member of the asset owner party	Asset	Assets of Related Asset Owner Contact Team	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Team.	ContactToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table	Asset	Assets of Related Asset	ContactAssetRule	Predefined rule for assets of	ContactToAssets

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		ZCA_ASSET where user is a sales party team member of the asset owner party with edit access		Owner Contact Team with Edit Access		Related Asset Owner Contact Team with Edit Access.	
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a sales party team member of the asset owner party with full access	Asset	Assets of Related Asset Owner Contact Team with Full Access	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Team with Full Access.	ContactToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ ASSET where user is in the management chain of a resource who is a sales party team member of the asset owner party	Asset	Assets of Related Asset Owner Contact Team Hierarchy	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Team Hierarchy.	ContactToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ ASSET where user is in the management chain of a resource who is a sales party team member of the asset owner party with edit access	Asset	Assets of Related Asset Owner Contact Team Hierarchy with Edit Access	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Team Hierarchy with Edit Access.	ContactToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ ASSET where user is in the management chain of a resource who is a sales party team member of the asset owner	Asset	Assets of Related Asset Owner Contact Team Hierarchy with Full Access	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Team Hierarchy with Full Access.	ContactToAssets

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		party with full access					
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ ASSET where user is owner of the territory associated with the asset owner party	Asset	Assets of Related Asset Owner Contact Territory Owner	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Territory Owner.	ContactToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a owner of the territory that is an ancestor of the territory associated with the asset owner party	Asset	Assets of Related Asset Owner Contact Territory Owner Hierarchy	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Territory Owner Hierarchy.	ContactToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a member of the territory associated with the asset owner party	Asset	Assets of Related Asset Owner Contact Territory Team	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Territory Team.	ContactToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET where user is a member of the territory that is an ancestor of the territory associated with the asset owner party	Asset	Assets of Related Asset Owner Contact Territory Team Hierarchy	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Territory Team Hierarchy.	ContactToAssets
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET all assets in the enterprise where asset owner party is a customer	Asset	Assets of Related All Asset Owner Contact Customers	ContactAssetRule	Predefined rule for assets of Related All Asset Owner Contact Customers.	ContactToAssets

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
Asset	ZCAASSETZCM2	Access the CRM Asset for table ZCA_ASSET all assets in the enterprise where asset owner party is a prospect	Asset	Assets of Related All Asset Owner Contact Prospects	ContactAssetRule	Predefined rule for assets of Related All Asset Owner Contact Prospects.	ContactToAssets

Business Plan Object Mapping

For each of the data security policies available for the Business Plan object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Business Plan	NA	NA	Business Plan	All Business Plans	BusinessPlanPR1	Access all business plans	GLOBAL_ BusinessPlan
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_ BP_BUSINESS_ PLANS where user is member of business plan team	Business Plan	Business Plan Team	BusinessPlanPR2	Business plans where the access group member is a resource on the business plan team	BPTEAM
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_ BP_BUSINESS_ PLANS where user is member of business plan team, with access level of edit or full	Business Plan	Business Plan Team with Edit or Full Access	BusinessPlanPR3	Business plans where the access group member is a resource on the business plan team with edit or full access	BPTEAMEDITORFULL
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_ BP_BUSINESS_	Business Plan	Draft Business Plan Team with Edit or Full Access	BusinessPlanPR4	Business plans where the access group member is a	BPDRAFTTEAMEDITORFUL

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		PLANS where user is member of business plan team, with access level of edit or full, and business plan status is draft or in revision				resource on the business plan team with edit or full access and business plan status is draft or in revision	
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where user is member of business plan team, with access level of full, and business plan status is draft or in revision	Business Plan	Draft Business Plan Team with Full Access	BusinessPlanPR5	Business plans where the access group member is a resource on the business plan team with full access and business plan status is draft or in revision	BPDRAFTTEAMFULL
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where their subordinate is member of business plan team	Business Plan	Business Plan Team Member in Resource Hierarchy	BusinessPlanPR6	Business plans where the access group member is in the management chain of a resource on the business plan team	BPTEAMRESHIER
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where their subordinate is member of business plan team, with access level of edit or full	Business Plan	Business Plan Team Member with Edit or Full Access in Resource Hierarchy	BusinessPlanPR7	Business plans where the access group member is in the management chain of a resource on the business plan team with edit or full access	BPTEAMEDITORFULLRESH
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where their subordinate is member of	Business Plan	Draft Business Plan Team Member with Edit or Full Access in Resource Hierarchy	BusinessPlanPR8	Business plans where the access group member is in the management chain of a resource on the	BPDRAFTTEAMEDITORFUL

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		business plan team, with access level of edit or full, and business plan status is draft or in revision				business plan team with edit or full access and business plan status is draft or in revision	
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where their subordinate is member of business plan team, with access level of full, and business plan status is draft or in revision	Business Plan	Draft Business Plan Team Member with Full Access in Resource Hierarchy	BusinessPlanPR9	Business plans where the access group member is in the management chain of a resource on the business plan team with full access and business plan status is draft or in revision	BPDRAFTTEAMFULLRESH
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where the business plan class is partner and user is member of business plan team	Business Plan	Partner Business Plan Team	BusinessPlanPR1	Business plans where the access group member is a resource on the business plan team and business plan class is partner	BPPARTNERBPTEAM
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where the business plan class is partner, user is member of business plan team, with access level of edit or full, and status is submitted to partner	Business Plan	Partner Business Plan Team with Edit or Full Access	BusinessPlanPR1	Business plans where the access group member is a resource on the business plan team with edit or full access and business plan class is partner and business plan status is submitted to partner	BPARTNERSUBMITBPTEAM
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_	Business Plan	Business Plans for Partner Resources	BusinessPlanPR1	Business plans where the access group	BPFORPARTNERRES

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		BP_BUSINESS_PLANS where the business plan class is partner and user is a contact of partner account				member is a member of the partner company related to the business plan and the business plan class is partner	
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where the business plan class is partner and user is a contact of partner account and status is submitted to partner	Business Plan	Submitted for Partner Business Plans for Partner Resources	BusinessPlanPR1	Business plans where the access group member is a member of the partner company related to the business plan and the business plan class is partner and status is submitted to partner	BPSUBMITFORPARTNERRE
Business Plan	ZCABPBUSINESS	Access the sales business plan for table ZCA_BP_BUSINESS_PLANS where the sales business plan class is partner	Business Plan	Partner Business Plans	BusinessPlanPR1	Business plans where class is partner	BPPARTNER

Campaign Object Mapping

For the data security policy available for the Campaign object, this topic shows the access group rule that provides equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Campaigns	NA	Access all marketing integration campaigns	Campaigns	All Campaigns	CampaignPR1	Access all campaigns	GLOBAL_CAMPAIGN

Contact Object Mapping

For each of the data security policies available for the Contact object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZBS1(	Access the sales party for table HZ_PARTIES where they are the account owner	Contact	Contact Owner	ContactPR1	Contacts where the access group member is the contact owner	CONTACTOWNER
Trading Community Party	HZPARTIESZBS1(	Access the sales party for table HZ_PARTIES where they are in the management chain of the account owner	Contact	Contact Owner Hierarchy	ContactPR2	Contacts where the access group member is in the management chain of the contact owner	CONTACTOWNERHIER
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES where user is in the sales account team	Contact	Contact Team	ContactPR3	Contacts where the access group member is on the contact team	CONTACTTEAM
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the sales account team with edit access	Contact	Contact Team with Edit Access	ContactPR5	Contacts where the access group member is on the contact team with edit access	CONTACTTEAMWITHEDIT
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the sales account team with full access	Contact	Contact Team with Full Access	ContactPR7	Contacts where the access group member is on the contact team with full access	CONTACTTEAMWITHFULL
Trading Community Party	HZPARTIESZCM3	Access the sales party for table HZ_PARTIES where	Contact	Contact Team Hierarchy	ContactPR4	Contacts where the access group member is in the	CONTACTTEAMHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		user is in the management chain of a resource who is on the sales contact team				management chain of a resource who is on the contact team	
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the management chain of a resource who is on the sales account team with edit access	Contact	Contact Team Hierarchy with Edit Access	ContactPR6	Contacts where the access group member is in the management chain of a resource who is on the contact team with edit access	CONTACTTEAMHIERWITHI
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the management chain of a resource who is on the sales account team with full access	Contact	Contact Team Hierarchy with Full Access	ContactPR8	Contacts where the access group member is on the contact team with full access	CONTACTTEAMHIERWITHI
Trading Community Party	HZPARTIESZCM3	Access the sales party for table HZ_PARTIES where user is a member of the territory associated with the sales contact	Contact	Contact Territory Team	ContactPR9	Contacts where the access group member is a member of the territory associated with the contact	CONTACTTERRITORY
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is a member of the territory that is an ancestor of the territory associated with the sales account	Contact	Contact Territory Team Hierarchy	ContactPR10	Contacts where the access group member is a member of the territory that is an ancestor of the territory associated with the contact	CONTACTTERRITORYHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZCM5	Access the sales party for table HZ_PARTIES where user is the owner of the territory associated with the sales account	Contact	Contact Territory Owner	ContactPR11	Contacts where the access group member is the owner of the territory associated with the contact	CONTACTTERRITORYOWN
Trading Community Party	HZPARTIESZCM5	Access the sales party for table HZ_PARTIES where user is the owner of the territory that is an ancestor of the territory associated with the sales account	Contact	Contact Territory Owner Hierarchy	ContactPR12	Contacts where the access group member is the owner of the territory that is an ancestor of the territory associated with the contact	CONTACTTERRITORYOWN
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES for all standalone contacts in the enterprise	Contact	All Standalone Contacts	ContactPR13	Access all standalone contacts	ALLSTANDALONECONTAC
Trading Community Party	HZPARTIESHZ54	Access the trading community party for table HZ_PARTIES all contacts in the enterprise	Contact	All Contacts	ContactPR14	Access all contacts	ALLCONTACTS
Trading Community Party	HZPARTIESHZ41	Access the trading community person for table HZ_PARTIES for all trading community persons in the enterprise except contacts created by partners	Contact	Internal Contacts	ContactPR15	Access internal contacts	INTERNALCONTACTS
Trading Community Party	HZPARTIESHZ19	Access the trading community person for table HZ_PARTIES for	Contact	Person Social Security Number	ContactPR16	Access person social security number	SOCIAL

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		all people in the enterprise					
Trading Community Party	HZCITIZENSHIPZ	Access the trading community citizenship for table HZ_CITIZENSHIP for all people in the enterprise	Contact	Person Citizenship Number	ContactPR17	Access person citizenship number	CITIZENSHIP
Trading Community Party	HZPARTYSITESZ	Access the trading community person address for table HZ_PARTY_SITES for personal addresses	Contact	Person Address	ContactPR18	Access person address	ADDRESS
Trading Community Party	HZCONTACTPOI	Access the trading community person phone for table HZ_CONTACT_POINTS for personal phone numbers	Contact	Person Mobile Phone Number	ContactPR19	Access person mobile phone number	MOBILE
Trading Community Party	HZCONTACTPOI	Access the trading community person e-mail for table HZ_CONTACT_P(for personal e-mail	Contact	Person Home Phone and Personal Email	ContactPR20	Access person home phone and personal email	EMAILPHONE
Trading Community Party	HZADDTNLPART	Access the trading community person additional identifier for table HZ_ADDTNL_PARTY_IDS for all identifiers in the enterprise	Contact	Person Additional Identifier	ContactPR21	Access person additional identifier	ADDITIONAL

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES for all prospects in the enterprise	Contact	All Prospects	ContactPR22	Access all prospects	ALLCONTACTSPROSPECTS
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES for all customers in the enterprise	Contact	All Customers	ContactPR23	Access all customers	ALLCONTACTSCUSTOMER

Contest Object Mapping

For each of the data security policies available for the Contest object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Contest	NA	NA	Contest	All Contests	ContestPR1	Access all contests	GLOBAL_ CONTEST
Contest	ZCACONTESTSZ	Access the sales contests for table ZCA_ CONTESTS where user is owner or creator of contest	Contest	Contest Owner	ContestPR2	Contests where the access group member is the owner of the contest	CONTESTOWNER
Contest	ZCACONTESTSZ	Access the sales contests for table ZCA_ CONTESTS where user is owner or creator of contest	Contest	Contest Creator	ContestPR3	Contests where the access group member is the creator of the contest	CONTESTCREATOR
Contest	ZCACONTESTSZ	Access the sales contests for table ZCA_ CONTESTS where user is	Contest	Contest Resource	ContestPR4	Contests where the access group member is a contest	CONTESTRESOURCE

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		participant or observer of contest				participant or observer	
Contest	ZCACONTESTSZ	Access the sales contests for table ZCA_CONTESTS where their subordinate is a participant or observer of contest	Contest	Contest Resource Hierarchy	ContestPR5	Contests where the access group member is in the management chain of a contest participant or observer	CONTESTRESHIER

Deal Registration Object Mapping

For each of the data security policies available for the Deal Registration object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS for all deal registrations in the enterprise	Deal Registration	All Deal Registrations	DealRegistration	Access all deal registrations	GLOBAL_DEALREGISTRATION
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS for all deal registrations in the enterprise and deal status is Draft, Return or Withdrawn	Deal Registration	All Deal Registrations that are in Draft or Returned or Withdrawn status	DealRegistration	Access all Deal Registrations where deal is in draft or returned or withdrawn status	DEALREGISTRATIONOPEN
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for	Deal Registration	All Deal Registrations that are in Draft	DealRegistration	Access all Deal Registrations where deal is in	DEALREGISTRATIONOPEN

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		table MKL_DM_DEALS for all deal registrations in the enterprise and deal status is Draft, Return or Withdrawn and deal is created by internal resource		or Returned or Withdrawn status		draft or returned or withdrawn status	
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS for all deal registrations in the enterprise and deal status is Pending Approval	NA	NA	NA	NA	NA
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS for all deal registrations in the enterprise and deal status is Pending Approval or Approved	NA	NA	NA	NA	NA
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS where they are a resource on the deal team with view, edit or full access	Deal Registration	Deal Registration Team	DealRegistrationF	Deal Registrations where the access group member is a resource on the deal registration team	DEALREGISTRATIONTEAM
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS where they are a resource on the	Deal Registration	Deal Registration Team with Edit or Full Access	DealRegistrationF	Deal Registrations where the access group member is a resource on the deal registration	DEALREGISTRATIONTEAM

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		deal team with view, edit or full access				team with edit or full access	
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS where they are a resource on the deal team with edit or full access and deal status is Draft, Return or Withdrawn	Deal Registration	Deal Registration Team with Edit or Full Access	DealRegistration	Deal Registrations where the access group member is a resource on the deal registration team with edit or full access	DEALREGISTRATIONTEAM
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS where they are a resource on the deal team with full access and deal status is Draft, Return or Withdrawn and deal is created by internal resource	Deal Registration	Deal Registration Team with Edit or Full Access	DealRegistration	Deal Registrations where the access group member is a resource on the deal registration team with edit or full access	DEALREGISTRATIONTEAM
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS where they are a resource on the deal team with full access and deal status is Pending Approval	Deal Registration	Deal Registration Team with Edit or Full Access	DealRegistration	Deal Registrations where the access group member is a resource on the deal registration team with edit or full access	DEALREGISTRATIONTEAM
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS where they are a resource on the deal team with edit	Deal Registration	Deal Registration Team with Edit or Full Access	DealRegistration	Deal Registrations where the access group member is a resource on the deal registration team with edit or full access	DEALREGISTRATIONTEAM

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		or full access and deal status is Pending Approval or Approved					
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS where they are in the partner organization and deal status is Draft, Return or Withdrawn	Deal Registration	All Deal Registrations for Partner Company	DealRegistrationF	Deal registrations where the access group member is a member of the partner company related to the deal registration	DEALREGISTRATIONFORPA
Deal Registration Summary	MKLDMDEALSM	Access the deal registration summary for table MKL_DM_DEALS where they are in the partner organization	Deal Registration	All Deal Registrations for Partner Company	DealRegistrationF	Deal registrations where the access group member is a member of the partner company related to the deal registration	DEALREGISTRATIONFORPA
NA	NA	NA	Deal Registration	Deal Registration Owner	DealRegistrationF	Deal Registrations where the access group member is the deal registration owner	DEALREGISTRATIONOWNE
NA	NA	NA	Deal Registration	All Deal Registrations for Child Partner Companies	DealRegistrationF	Deal registrations where the access group member is a member of an ancestor partner company related to the deal registration	DEALREGISTRATIONFORPA

Duplicate Identification Batch Object Mapping

For each of the data security policies available for the Duplicate Identification Batch object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Duplicate Identification Batch	ZCHDATAMGMTI	Access the trading community duplicate identification batch for table ZCH_DATA_MGMT_BATCHES_B for self	Duplicate Identification Batch	Duplicate Identification Batch Assignee	DuplicateIdentific	Duplicate identification batches where the access group member is the assignee	DUPIDENTIFICATIONASSIG
Duplicate Identification Batch	ZCHDATAMGMTI	Access the trading community duplicate identification batch for table ZCH_DATA_MGMT_BATCHES_B for all duplicate identification batches in the enterprise	Duplicate Identification Batch	All Duplicate Identification Batches	DuplicateIdentific	Access all duplicate identification batches	GLOBAL_DUPLICATEIDENTIFICATIO

Duplicate Resolution Request Object Mapping

For each of the data security policies available for the Duplicate Resolution Request object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Duplicate Resolution Request	ZCHDEDUPHEAD	Access the trading community duplicate resolution request for table ZCH_DEDUP_HEADERS_B for self	Duplicate Resolution Request	Resolution Request Assignee	ResolutionReque	Duplicate resolution requests where the access group member is the assignee	RESOLUTIONREQUESTASS
Duplicate Resolution Request	ZCHDEDUPHEAD	Access the trading community duplicate resolution request for table ZCH_DEDUP_HEADERS_B for all duplicate resolution requests in the enterprise	Duplicate Resolution Request	All Resolution Requests	ResolutionReque	Access all duplicate resolution requests	GLOBAL_RESOLUTIONREQUEST

Forecast Territory Details Object Mapping

For each of the data security policies available for the Forecast Territory Details object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Forecast Participant	ZSFFCSTPARTICI	Access the sales forecast participant for table ZSF_FCST_PARTICIPANT for the territory hierarchy that they own or delegated to currently	Forecast Territory Details	Territory Forecast Delegate	TerritoryForecast	Territory Forecast where the access group member is a delegate of the territory	FCSTDELEGATE
Forecast Participant	ZSFFCSTPARTICI	Access the sales forecast participant	Forecast Territory Details	Territory Forecast	TerritoryForecast	Territory Forecast where the access	FCSTDELEGATEHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		for table ZSF_FCST_ PARTICIPANT for the territory hierarchy that they own or delegated to currently		Delegate Hierarchy		group member is the delegate of a parent territory in the territory hierarchy	
Forecast Participant	ZSFFCSTPARTICI	Access the sales forecast participant for table ZSF_FCST_ PARTICIPANT for the territory hierarchy that they own or delegated to currently	Forecast Territory Details	Territory Forecast Owner	TerritoryForecast	Territory Forecast where the access group member is the territory owner	FCSTOWNER
Forecast Participant	ZSFFCSTPARTICI	Access the sales forecast participant for table ZSF_FCST_ PARTICIPANT for the territory hierarchy that they own or delegated to currently	Forecast Territory Details	Territory Forecast Owner Hierarchy	TerritoryForecast	Territory Forecast where the access group member is the owner of a parent territory in the territory hierarchy	FCSTOWNERHIER
Forecast Participant	ZSFFCSTPARTICI	Access the sales forecast participant for table ZSF_FCST_ PARTICIPANT for the territory hierarchy that they owned previously for the active forecast	Forecast Territory Details	Territory Forecast Old Owner	TerritoryForecast	Territory Forecast where the access group member is the previous owner	FCSTPREVOWNER
NA	NA	NA	Forecast Territory Details	All Territory Forecasts	TerritoryForecast	Access all Territory Forecasts	GLOBAL_ TERRITORYFORECAST

Goal Object Mapping

For each of the data security policies available for the Goal object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Goal	NA	NA	Goal	All Goals	GoalPR1	Access all goals	GLOBAL_GOAL
Goal	ZCAGOALSZBS1(	Access the sales goals for table ZCA_GOALS where user is owner or creator of goal	Goal	Goal Owner	GoalPR2	Goals where the access group member is the owner of the goal	GOALOWNER
Goal	ZCAGOALSZBS1(	Access the sales goals for table ZCA_GOALS where user is owner or creator of goal	Goal	Goal Creator	GoalPR3	Goals where the access group member is the creator of the goal	GOALCREATOR
Goal	ZCAGOALSZBS1(	Access the sales goals for table ZCA_GOALS where user is participant of goal	Goal	Goal Resource	GoalPR4	Goals where the access group member is a goal participant	GOALRESOURCE
Goal	ZCAGOALSZBS1(	Access the sales goals for table ZCA_GOALS where their subordinate is a participant of goal	Goal	Goal Resource Hierarchy	GoalPR5	Goals where the access group member is in the management chain of a goal participant	GOALRESHIER

Goal Participant Object Mapping

For each of the data security policies available for the Goal Participant object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Goal Participant	NA	NA	Goal Participant	All Goal Participants	GoalParticipantPI	Access all goal participants	GLOBAL_ GOALPARTICIPANT
Goal Participant	ZCAGOALPARTIC	Access the sales goal participants for table ZCA_GOAL_ PARTICIPANTS where user is owner or creator of goal	Goal Participant	Goal Participant Owner	GoalParticipantPI	Goal participants where the access group member is the owner of the goal	GOALPARTICIPANTOWNER
Goal Participant	ZCAGOALPARTIC	Access the sales goal participants for table ZCA_GOAL_ PARTICIPANTS where user is owner or creator of goal	Goal Participant	Goal Participant Creator	GoalParticipantPI	Goal participants where the access group member is the creator of the goal	GOALPARTICIPANTCREATC
Goal Participant	ZCAGOALPARTIC	Access the sales goal participants for table ZCA_GOAL_ PARTICIPANTS where user is participant of goal	Goal Participant	Goal Participant	GoalParticipantPI	Goal participants where the access group member is the goal participant	GOALPARTICIPANT
Goal Participant	ZCAGOALPARTIC	Access the sales goal participants for table ZCA_GOAL_ PARTICIPANTS where their subordinate is a participant of goal	Goal Participant	Goal Participant Resource Hierarchy	GoalParticipantPI	Goal participants where the access group member is in the management chain of the goal participant	GOALPARTICIPANTRESHIE

Household Object Mapping

For each of the data security policies available for the Household object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZBS1(	Access the sales party for table HZ_PARTIES where they are the account owner	Household	Household Owner	HouseholdPR1	Households where the access group member is the households owner	HOUSEHOLDOWNER
Trading Community Party	HZPARTIESZBS1(	Access the sales party for table HZ_PARTIES where they are in the management chain of the account owner	Household	Household Owner Hierarchy	HouseholdPR2	Households where the access group member is in the management chain of the households owner	HOUSEHOLDOWNERHIER
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES where user is in the sales account team	Household	Household Team	HouseholdPR3	Households where the access group member is on the households team	HOUSEHOLDTEAM
Trading Community Party	HZPARTIESZCM3	Access the sales party for table HZ_PARTIES where user is in the management chain of a resource who is on the sales account team	Household	Household Team Hierarchy	HouseholdPR4	Households where the access group member is in the management chain of a resource who is on the households team	HOUSEHOLDTEAMHIER
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the sales account team with edit access	Household	Household Team with Edit Access	HouseholdPR5	Households where the access group member is on the households team with edit access	HOUSEHOLDTEAMWITHED
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the management chain of a resource who is on the sales account team with edit access	Household	Household Team Hierarchy with Edit Access	HouseholdPR6	Households where the access group member is in the management chain of a resource who is on the households	HOUSEHOLDTEAMHIERWI

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
						team with edit access	
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the sales account team with full access	Household	Household Team with Full Access	HouseholdPR7	Households where the access group member is on the households team with full access	HOUSEHOLDTEAMWITHFU
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is in the management chain of a resource who is on the sales account team with full access	Household	Household Team Hierarchy with Full Access	HouseholdPR8	Households where the access group member is in the management chain of a resource who is on the households team with full access	HOUSEHOLDTEAMHIERWI
Trading Community Party	HZPARTIESZCM3	Access the sales party for table HZ_PARTIES where user is a member of the territory associated with the sales contact	Household	Household Territory Team	HouseholdPR9	Households where the access group member is a member of the territory associated with the household	HOUSEHOLDTERRITORY
Trading Community Party	HZPARTIESZCM4	Access the sales party for table HZ_PARTIES where user is a member of the territory that is an ancestor of the territory associated with the sales account	Household	Household Territory Team Hierarchy	HouseholdPR10	Households where the access group member is a member of the territory that is an ancestor of the territory associated with the household	HOUSEHOLDTERRITORYH
Trading Community Party	HZPARTIESZCM5	Access the sales party for table HZ_PARTIES where user is the owner of the territory associated with the sales account	Household	Household Territory Owner	HouseholdPR11	Households where the access group member is the owner of the territory associated with the household	HOUSEHOLDTERRITORYO

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESZCM5	Access the sales party for table HZ_PARTIES where user is the owner of the territory that is an ancestor of the territory associated with the sales account	Household	Household Territory Owner Hierarchy	HouseholdPR12	Households where the access group member is the owner of the territory that is an ancestor of the territory associated with the household	HOUSEHOLDTERRITORYO
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES for all prospects in the enterprise	Household	Household of Type Prospects	HouseholdPR13	Access all households which are sales prospects	ALLHOUSEHOLDPROSPEC
Trading Community Party	HZPARTIESZCM1	Access the sales party for table HZ_PARTIES for all customers in the enterprise	Household	Household of Type Customers	HouseholdPR14	Access all households which are sales customers	ALLHOUSEHOLDCUSTOMI
Trading Community Party	HZPARTIESHZ54	Access the trading community party for table HZ_PARTIES all accounts in the enterprise	Household	All Households	HouseholdPR15	Access all households	ALLHOUSEHOLDS

KPI Object Mapping

For each of the data security policies available for the KPI object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
KPI	ZCAKPIZBS1000	Access the sales KPI for table ZCA_KPI	KPI	All KPIs	KpiPR1	Access all KPIs	GLOBAL_KPI

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
KPI	ZCAKPIZBS1000(	Access the sales KPI for table ZCA_KPI where user is the creator of KPI	KPI	KPI Creator	KpiPR2	KPIs where the access group member is the creator of the KPI	KPICREATOR

Lead Object Mapping

For each of the data security policies available for the Lead object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a resource in the lead sales team	Lead	Lead Team	LeadPR4	Leads where the access group member is on the lead team	LEADTEAM
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a resource in the territory assigned to the sales lead	Lead	Lead Territory Team	LeadPR8	Leads where the access group member is a member of a territory associated with the lead	LEADTERR
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are an administrator of the resource organization in the primary assignment of the owner	Lead	Lead Owner Organization Administrator	LeadPR2	Leads where the access group member is the administrator of the resource organization of the lead owner	LEADOWNERORGADMIN

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are the owner of the sales lead	Lead	Lead Owner	LeadPR1	Leads where the access group member is the lead owner	LEADOWNER
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a resource in the lead sales team with full access	Lead	Lead Team with Full Access	LeadPR5	Leads where the access group member is on the lead team with full access	LEADTEAMWITHFULL
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS for all sales leads in the enterprise	Lead	All Leads	LeadPR12	Access all leads	GLOBAL_LEAD
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS for all retired, qualified, unqualified leads in the enterprise	Lead	All Leads	LeadPR12	Access all leads	GLOBAL_LEAD
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a territory resource in the sales lead territory team or a territory resource with a descendant territory in the sales lead territory team	Lead	Lead Territory Team	LeadPR8	Leads where the access group member is a member of a territory associated with the lead	LEADTERRITORY
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_	Lead	Lead Territory Team Hierarchy	LeadPR9	Leads where the access group member is a	LEADTERRITORYHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		LM_LEADS where they are a territory resource in the sales lead territory team or a territory resource with a descendant territory in the sales lead territory team				member of a territory that is an ancestor of a territory associated with the lead	
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS for all retired leads in the enterprise	Lead	All Nonconverted Leads	LeadPR10	Access all nonconverted leads	ALLNONCONVERTEDLEAD
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS for all partner leads in the enterprise	Lead	All Partner Leads	LeadPR11	Access all partner leads	ALLPARTNERLEADS
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a manager in the management hierarchy of a resource in the lead sales team with full access	Lead	Lead Team Hierarchy with Full Access	LeadPR7	Leads where the access group member is in the management chain of a resource who is on the lead team with full access	LEADTEAMHIERWITHFULL
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a manager in the management hierarchy of the owner of the sales lead	Lead	Lead Owner Hierarchy	LeadPR3	Leads where the access group member is in the management chain of the lead owner	LEADOWNERHIER
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a	Lead	Lead Team Hierarchy	LeadPR6	Leads where the access group member is in the management	LEADTEAMHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		manager in the management hierarchy of a resource in the lead sales team				chain of a resource who is on the lead team	
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are in the management hierarchy of the owner of the lead	Lead	Lead Team Hierarchy	LeadPR6	Leads where the access group member is in the management chain of a resource who is on the lead team	LEADTEAMHIER
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a member of the lead sales account team or in the management chain of an lead sales account team member	Lead	Account Team	AccountPR3	Accounts where the access group member is on the account team	ACCOUNTTEAM
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a member of the lead sales account team or in the management chain of an lead sales account team member	Lead	Account Team Hierarchy	AccountPR4	Accounts where the access group member is in the management chain of a resource who is on the account team	ACCOUNTTEAMHIER
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a territory resource in the lead sales account territory team or a territory resource with	Lead	Account Territory	AccountPR9	Accounts where the access group member is a member of the territory associated with the account	ACCOUNTTERRITORY

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		a descendant territory in the lead sales account territory team					
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are a territory resource in the lead sales account territory team or a territory resource with a descendant territory in the lead sales account territory team	Lead	Account Territory Hierarchy	AccountPR10	Accounts where the access group member is a member of the territory that is an ancestor of the territory associated with the account	ACCOUNTTERRITORYHIER
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS for all sales leads in the business units that they are authorized within	Lead	Business Unit Leads	LeadPR13	Leads in the business units that the access group member is associated with	BULEADS
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales account team, account territory team or upward territory hierarchy	Lead	Account Team	AccountPR3	Accounts where the access group member is on the account team	ACCOUNTTEAM
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead	Lead	Account Team Hierarchy	AccountPR4	Accounts where the access group member is in the management chain of a resource who is	ACCOUNTTEAMHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		sales account team, account territory team or upward territory hierarchy				on the account team	
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales account team, account territory team or upward territory hierarchy	Lead	Account Territory	AccountPR9	Accounts where the access group member is a member of the territory associated with the account	ACCOUNTTERRITORY
Sales Lead	MKLLMLEADSMI	Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales account team, account territory team or upward territory hierarchy	Lead	Account Territory Hierarchy	AccountPR10	Accounts where the access group member is a member of the territory that is an ancestor of the territory associated with the account	ACCOUNTTERRITORYHIER
Sales Lead	MKLLMLEADSZE	Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales team, member of territory team or upward territory hierarchy	Lead	Lead Team	LeadPR4	Leads where the access group member is on the lead team	LEADTEAM
Sales Lead	MKLLMLEADSZE	Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead	Lead	Lead Team Hierarchy	LeadPR6	Leads where the access group member is in the management chain of a resource who	LEADTEAMHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		sales team, member of territory team or upward territory hierarchy				is on the lead team	
Sales Lead	MKLLMLEADSZE	Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales team, member of territory team or upward territory hierarchy	Lead	Lead Territory Team	LeadPR8	Leads where the access group member is a member of a territory associated with the lead	LEADTERRITORY
Sales Lead	MKLLMLEADSZE	Access the sales lead for table MKL_LM_LEADS where they are member or in management chain of lead sales team, member of territory team or upward territory hierarchy	Lead	Lead Territory Team Hierarchy	LeadPR9	Leads where the access group member is a member of a territory that is an ancestor of a territory associated with the lead	LEADTERRITORYHIER

Advanced permissions are defined for some of the Lead data security policies. Advanced permissions let you refine the access provided by a data security policy. This table shows how the advanced permissions available with Lead data security policies map to predefined access group rules.

Data Security Policy Business Object	Data Security Policy Advanced Permission Name	Access Group Object	Predefined Rule Name	Access Level
Sales Lead	View Sales Lead	Lead	Any predefined rule	Read, Update, Delete, Full
Sales Lead	Update Sales Lead	Lead	Any predefined rule	Update, Full
Sales Lead	Delete Sales Lead	Lead	Any predefined rule	Delete, Full
Sales Lead	Convert Sales Lead	Lead	Any predefined rule	Full

MDF Budget Object Mapping

For each of the data security policies available for the MDF Budget object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MDF Budget	NA	All Values	MDF Budget	All MDF Budgets	MDFBudgetPR1	Access all MDF budgets	GLOBAL_ MDFBUDGETS
MDF Budget	MKTBDTBUDGET	Access the MDF budget for table MKT_ BDT_BUDGETS_ B for all MDF budgets in the enterprise, and the MDF budget is in draft status	MDF Budget	All MDF Budgets with Status-Based Access Level	MDFBudgetPR2	Access all MDF budgets where access level is status based	ALLMDFBUDGETS
MDF Budget	MKTBDTBUDGET	Access the MDF budget for table MKT_BDT_ BUDGETS_B where they are an MDF budget team member	MDF Budget	MDF Budget Team	MDFBudgetPR3	MDF budgets where the access group member is a resource on the MDF budget team	MDFBUDGETTEAM
MDF Budget	MKTBDTBUDGET	Access the MDF budget for table MKT_BDT_ BUDGETS_B where they are an MDF budget team member with edit or full access	MDF Budget	MDF Budget Team with Edit or Full Access	MDFBudgetPR4	MDF budgets where the access group member is a resource on the MDF budget team with edit or full access	MDFBUDGETTEAMEDITOR
MDF Budget	MKTBDTBUDGET	Access the MDF budget for table MKT_BDT_ BUDGETS_B where they are an MDF budget team member, or in the management chain of an MDF budget team member	MDF Budget	MDF Budget Team Hierarchy	MDFBudgetPR5	MDF budgets where the access group member is in the management chain of a resource who is on the MDF budget team	MDFBUDGETTEAMHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MDF Budget	MKTBDTBUDGET	Access the MDF budget for table MKT_BDT_BUDGETS_B where they are an MDF budget team member with edit or full access, or in the management chain of a resource on the MDF budget team member with edit or full access	MDF Budget	MDF Budget Team Hierarchy with Edit or Full Access	MDFBudgetPR6	MDF budgets where the access group member is a resource on the MDF budget team with edit or full access or is in the management chain of a resource who is on the MDF budget team with edit or full access	MDFBUDGETTEAMHIERED

MDF Claim Object Mapping

For each of the data security policies available for the MDF Claim object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MDF Claim	NA	All Values	MDF Claim	All MDF Claims	MDFClaimsPR1	Access all MDF claims	GLOBAL_MDFCLAIMS
MDF Claim	NA	NA	MDF Claim	All MDF Claims for Child Partner Companies	MDFClaimsPR10	MDF claims where the access group member is a member of an ancestor partner company related to the MDF claim	MDFCLAIMPARTHIER
MDF Claim	MKTBDTCLAIMS	Access the MDF claim for table MKT_BDT_CLAIMS where they are a resource on the MDF claim team	MDF Claim	MDF Claim Team	MDFClaimsPR2	MDF claims where the access group member is a resource on the MDF claim team	MDFCLAIMTEAM

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MDF Claim	MKTBDTCLAIMS'	Access the MDF claim for table MKT_BDT_CLAIMS where they are a resource on the MDF claim team with edit or full access, and the MDF claim status is draft or returned or failed or withdrawn	MDF Claim	MDF Claim Team with Edit Access	MDFClaimsPR3	MDF claims where the access group member is a resource on the MDF claim team with edit access	MDFCLAIMTEAMEDIT
MDF Claim	MKTBDTCLAIMS' MKTBDTCLAIMS'	Access the MDF claim for table MKT_BDT_CLAIMS where they are a resource on the MDF claim team with edit or full access, and the MDF claim status is draft or returned or failed or withdrawn Access the MDF claim for table MKT_BDT_CLAIMS where they are a resource on the MDF claim team with edit or full access, and the MDF claim status is draft	MDF Claim	MDF Claim Team with Full Access	MDFClaimsPR4	MDF claims where the access group member is a resource on the MDF claim team with full access	MDFCLAIMTEAMFULL
MDF Claim	MKTBDTCLAIMS'	Access the MDF claim for table MKT_BDT_CLAIMS where they are a resource on the MDF claim team, or they are in the management chain of a resource on the MDF claim team	MDF Claim	MDF Claim Team Hierarchy	MDFClaimsPR5	MDF claims where the access group member is in the management chain of a resource who is on the MDF claim team	MDFCLAIMTEAMHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MDF Claim	MKTBDTCLAIMS'	Access the MDF claim for table MKT_BDT_CLAIMS where they are a resource on the MDF claim team with edit or full access, or in the management chain of a resource on the MDF claim team with edit or full access, and the MDF claim status is draft or returned or failed or withdrawn	MDF Claim	MDF Claim Team Hierarchy with Edit Access	MDFClaimsPR6	MDF claims where the access group member is a resource on the MDF claim team with edit access or is in the management chain of a resource who is on the MDF claim team with edit access	MDFCLAIMTEAMHIEREDIT
MDF Claim	MKTBDTCLAIMS'	Access the MDF claim for table MKT_BDT_CLAIMS where they are a resource on the MDF claim team with edit or full access, or in the management chain of a resource on the MDF claim team with edit or full access, and the MDF claim status is draft	MDF Claim	MDF Claim Team Hierarchy with Full Access	MDFClaimsPR7	MDF claims where the access group member is a resource on the MDF claim team with full access or is in the management chain of a resource who is on the MDF claim team with full access	MDFCLAIMTEAMHIERFULL
MDF Claim	MKTBDTCLAIMS' MKTBDTCLAIMS' MKTBDTCLAIMS'	Access the MDF claim for table MKT_BDT_CLAIMS for all MDF claims in the enterprise, and the MDF claim status is draft or returned or failed or withdrawn Access the MDF claim for table MKT_BDT_CLAIMS for all	MDF Claim	All MDF Claims with Status-Based Access Level	MDFClaimsPR8	Access all MDF claims where access level is status based	ALLMDFCLAIMS

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		MDF claims in the enterprise, and the MDF Claim status is draft Access the MDF claim for table MKT_BDT_CLAIMS for all MDF claims in the enterprise, and the MDF claim status is draft or returned or failed or withdrawn, and the MDF claim is created by an internal resource					
MDF Claim	MKTBDTCLAIMS MKTBDTCLAIMS MKTBDTCLAIMS	Access the MDF claim for table MKT_BDT_CLAIMS for all MDF claims in the partner organization, and the MDF claim status is draft Access the MDF claim for table MKT_BDT_CLAIMS for all MDF claims in the partner organization, and the MDF claim status is draft or returned or failed or withdrawn Access the MDF claim for table MKT_BDT_CLAIMS for all MDF claims in the partner organization	MDF Claim	All MDF Claims for Partner Company	MDFClaimsPR9	MDF claims where the access group member is a member of the partner company related to the MDF claim	MDFCLAIMPARTCOMP

MDF Request Object Mapping

For each of the data security policies available for the MDF Request object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MDF Request	MKTBDTFUNDRE MKTBDTFUNDRE MKTBDTFUNDRE	Access the MDF request for table MKT_BDT_FUND_REQUESTS for all MDF requests in the enterprise, and the MDF request status is draft or returned or failed or withdrawn Access the MDF request for table MKT_BDT_FUND_REQUESTS for all MDF requests in the enterprise, and the MDF request status is draft Access the MDF request for table MKT_BDT_FUND_REQUESTS for all MDF requests in the enterprise, and the MDF request status is draft or returned or failed or withdrawn, and the MDF request is created by an internal resource	MDF Request	All MDF Requests with Status-Based Access Level	MDFRequestsPR	Access all MDF requests where access level is status based	ALLMDFREQUESTS
MDF Request	NA	NA	MDF Request	All MDF Requests for Child Partner Companies	MDFRequestsPR	MDF requests where the access group member is a	MDFREQUESTPARTHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
						member of an ancestor partner company related to the MDF request	
MDF Request	MKTBDTFUNDRE	Access the MDF request for table MKT_BDT_FUND_REQUESTS where they are a resource on the MDF request team	MDF Request	MDF Request Team	MDFRequestsPR	MDF requests where the access group member is a resource on the MDF request team	MDFREQUESTTEAM
MDF Request	MKTBDTFUNDRE	Access the MDF request for table MKT_BDT_FUND_REQUESTS where they are a resource on the MDF request team with edit or full access, and the MDF request status is draft or returned or failed or withdrawn	MDF Request	MDF Request Team with Edit Access	MDFRequestsPR	MDF requests where the access group member is a resource on the MDF request team with edit access	MDFREQUESTTEAMEDIT
MDF Request	MKTBDTFUNDRE	Access the MDF request for table MKT_BDT_FUND_REQUESTS where they are a resource on the MDF request team, or they are in the management chain of a resource on the MDF request team	MDF Request	MDF Request Team Hierarchy	MDFRequestsPR	MDF requests where the access group member is in the management chain of a resource on the MDF request team	MDFREQUESTTEAMHIER
MDF Request	MKTBDTFUNDRE	Access the MDF request for table MKT_BDT_FUND_REQUESTS where they are a resource on the MDF	MDF Request	MDF Request Team Hierarchy with Edit Access	MDFRequestsPR	MDF requests where the access group member is in the management chain of a resource on the	MDFREQUESTTEAMHIERE

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		request team with edit or full access, or in the management chain of a resource on the MDF request team with edit or full access, and the MDF request status is draft or returned or failed or withdrawn				MDF request team with edit access	
MDF Request	MKTBDTFUNDRE MKTBDTFUNDRE	Access the MDF request for table MKT_BDT_FUND_REQUESTS where they are a resource on the MDF request team with edit or full access, and the MDF request status is draft or returned or failed or withdrawn Access the MDF request for table MKT_BDT_FUND_REQUESTS where they are a resource on the MDF request team with edit or full access, and the MDF request status is draft	MDF Request	MDF Request Team with Full Access	MDFRequestsPR	MDF requests where the access group member is a resource on the MDF request team with full access	MDFREQUESTTEAMFULL
MDF Request	MKTBDTFUNDRE MKTBDTFUNDRE	Access the MDF request for table MKT_BDT_FUND_REQUESTS where they are a resource on the MDF request team with edit or full access, or in the management chain of a	MDF Request	MDF Request Team Hierarchy with Full Access	MDFRequestsPR	MDF requests where the access group member is in the management chain of a resource on the MDF request team with full access	MDFREQUESTTEAMHIERF

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		resource on the MDF request team with edit or full access, and the MDF request status is draft or returned or failed or withdrawn Access the MDF request for table MKT_BDT_FUND_REQUESTS where they are a resource on the MDF request team with edit or full access, or in the management chain of a resource on the MDF request team with edit or full access, and the MDF request status is draft					
MDF Request	NA	All Values	MDF Request	All MDF Requests	MDFRequestsPR	Access all MDF requests	GLOBAL_MDFREQUESTS
MDF Request	MKTBDTFUNDRE MKTBDTFUNDRE MKTBDTFUNDRE	Access the MDF request for table MKT_BDT_FUND_REQUESTS for all MDF requests in the partner organization Access the MDF request for table MKT_BDT_FUND_REQUESTS for all MDF requests in the partner organization, and the MDF request status is draft or returned or failed or withdrawn	MDF Request	All MDF Requests for Partner Company	MDFRequestsPR	MDF requests where the access group member is a member of the partner company related to the MDF request	MDFREQUESTPARTCOMP

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		Access the MDF request for table MKT_BDT_FUND_REQUESTS for all MDF requests in the partner organization, and the MDF request status is draft					

Note Object Mapping

For each of the data security policies available for the Note object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
NOTE	ZMM_NOTES_AUTHOR	Notes Instance set for Author	Note	Note Author	NotePR1	Note author	NOTEAUTHOR
NOTE	ZMM_NOTES_AUTHOR_PRIVATE	Private Notes Instance set for Author	Note	Note Author	NotePR1	Note author	NOTEAUTHOR
NOTE	ZMM_NOTES_CMPTR_USER_IS_AUTHOR	Access the competitor note for table ZMM_NOTES where they are the author of the note	Note	Note Author	NotePR1	Note author	NOTEAUTHOR
NOTE	ZMM_NOTES_OPTY_USER_IS_AUTHOR	Access the opportunity note for table ZMM_NOTES where they are the author of the note	Note	Note Author	NotePR1	Note author	NOTEAUTHOR

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
NOTE	ZMM_NOTES_REF_USER_IS_AUTHOR	Access the reference customer note for table ZMM_NOTES where they are the author of the note	Note	Note Author	NotePR1	Note author	NOTEAUTHOR
NOTE	ZMM_NOTES_MANAGE_REF_ALL	Access the competitor note for table ZMM_NOTES for all notes that are not private	Note	All Nonprivate Notes	NotePR2	All nonprivate notes visible to internal users	ALLNONPRIVATENOTE
NOTE	ZMM_NOTES_INTERNAL	Internal Notes Instance set	Note	All Nonprivate Notes	NotePR2	All nonprivate notes visible to internal users	ALLNONPRIVATENOTE
NOTE	ZMM_NOTES_ADMIN_SALES_ADMIN	Access the opportunity note for table ZMM_NOTES for all notes that are not private	Note	All Nonprivate Notes	NotePR2	All nonprivate notes visible to internal users	ALLNONPRIVATENOTE
NOTE	ZMM_NOTES_EXTERNAL	External Notes Instance set	Note	All External Notes	NotePR3	All external notes visible to channel and partner users	ALLEXTERNALNOTE
NOTE	ZMM_NOTES_OPTY_EXT	Access the opportunity note for table ZMM_NOTES for all external opportunity notes in the enterprise	Note	All External Notes	NotePR3	All external notes visible to channel and partner users	ALLEXTERNALNOTE
NOTE	ZMMNOTESZMM	Access the deal registration note for table ZMM_NOTES where they are the author of the note or notes that are not private created by their organization or external notes created by	Note	All Notes Created by Partner Company	NotePR4	Notes created by partner company	ALLNONPVTMYPARTNERC

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		the deploying company or external notes created by partner where they belong to the deploying company					
NOTE	ZMM_NOTES_DEFAULT	Notes Default Instance Set	Note	Note Author	NotePR1	Note author	NOTEAUTHOR
NOTE	ZMM_NOTES_DEFAULT	Notes Default Instance Set	Note	All Nonprivate Notes	NotePR2	All nonprivate notes visible to internal users	ALLNONPRIVATENOTE
NOTE	ZMM_NOTES_ALL	All Notes Instance set	Note	Note Author	NotePR1	Note author	NOTEAUTHOR
NOTE	ZMM_NOTES_ALL	All Notes Instance set	Note	All Nonprivate Notes	NotePR2	All nonprivate notes visible to internal users	ALLNONPRIVATENOTE
NOTE	ZMM_NOTES_ALL	All Notes Instance set	Note	All External Notes	NotePR3	All external notes visible to channel and partner users	ALLEXTERNALNOTE
NOTE	ZMM_NOTES_AUTHOR_AND_PUBLIC	Access the Opportunity Note for table ZMM_NOTES Where they are the author of the note or the note is not a private note	Note	Note Author	NotePR1	Note author	NOTEAUTHOR
NOTE	ZMM_NOTES_AUTHOR_AND_PUBLIC	Access the Opportunity Note for table ZMM_NOTES Where they are the author of the note or the note is not a private note	Note	All Nonprivate Notes	NotePR2	All nonprivate notes visible to internal users	ALLNONPRIVATENOTE

Access Extension Rules for Note

For each of the data security policies available for the Note object, this table shows the access extension rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
Note	ZMM_NOTES_DEFAULT	Notes Default Instance Set	Note	Nonprivate Notes of Activity	ActivityNoteRule	Predefined rule for nonprivate notes of an activity.	ActivityToNonPrivateNote
NA	NA	NA	Note	Nonprivate Notes of Account	AccountNoteRule	Predefined rule for nonprivate notes of an account.	AccountToNonPrivateNote
Note	ZMM_NOTES_OPTY_TERR_HIER_RES	Access the opportunity note for table ZMM_NOTES where they are a territory resource in the opportunity territory team or a territory resource with a descendant territory in the opportunity territory team and the note is not private	Note	Nonprivate Opportunity Notes of Account Territory Team	AccountNoteRule	Predefined rule for nonprivate opportunity notes of an account territory team.	AccountToOpportunityNote
Note	ZMM_NOTES_OPTYACCTERR_HIER_RES	Access the opportunity note for table ZMM_NOTES where they are a territory resource in the opportunity sales account territory team or a territory resource with a descendant territory in the opportunity sales account territory team and the note is not private	Note	Nonprivate Opportunity Notes of Account Territory Team	AccountNoteRule	Predefined rule for nonprivate opportunity notes of an account territory team.	AccountToOpportunityNote

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
Note	ZMM_NOTES_MANAGE_OPTYTEAM_REP	Access the opportunity note for table ZMM_NOTES where they are an opportunity sales team member with full access and the note is not private	Note	Nonprivate Notes of Opportunity	OpportunityNotel	Predefined rule for nonprivate notes of an opportunity.	OpportunityToNonPrivateN
Note	ZMM_NOTES_MANAGE_OPTYTEAM_MGR	Access the opportunity note for table ZMM_NOTES where they are in the management chain of an opportunity sales team member with full access and the note is not private	Note	Nonprivate Notes of Opportunity	OpportunityNotel	Predefined rule for nonprivate notes of an opportunity.	OpportunityToNonPrivateN
Note	ZMM_NOTES_MANAGE_OPTYTEAM_REP	Access the opportunity note for table ZMM_NOTES where they are an opportunity sales team member with full access and the note is not private	Note	Nonprivate Notes of Opportunity	OpportunityNotel	Predefined rule for nonprivate notes of an opportunity.	OpportunityToNonPrivateN
Note	ZMM_NOTES_MANAGE_OPTYTEAM_MGR	Access the opportunity note for table ZMM_NOTES where they are in the management chain of an opportunity sales team member with full access and the note is not private	Note	Nonprivate Notes of Opportunity	OpportunityNotel	Predefined rule for nonprivate notes of an opportunity.	OpportunityToNonPrivateN

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
NA	NA	NA	Note	Nonprivate Notes of Opportunity	OpportunityNote	Predefined rule for nonprivate notes of an opportunity.	OpportunityToNonPrivateN
Note	ZMM_NOTES_MANAGE_PRTNR_SLS_REP	Access the opportunity note for table ZMM_NOTES where they are an opportunity sales team member with full access and the note is external	Note	External Notes of Opportunity	OpportunityNote	Predefined rule for external notes of an opportunity.	OpportunityToExternalNote
Note	ZMM_NOTES_MANAGE_PRTNR_SLS_MGR	Access the opportunity note for table ZMM_NOTES where they are an opportunity sales team member with full access and the note is external	Note	External Notes of Opportunity	OpportunityNote	Predefined rule for external notes of an opportunity.	OpportunityToExternalNote
Note	ZMM_NOTES_PRTNR_ADMIN	Access the opportunity note for table ZMM_NOTES where they are a member of a partner resource organization whose partner organization is on the opportunity and the note is external	Note	External Opportunity Notes of Opportunity Revenue Partner	OpportunityNote	Predefined rule for external opportunity notes of an opportunity revenue partner.	OpportunityRevenuePartne
Note	ZMM_NOTES_PRTNR_EXT	Access the opportunity note for table ZMM_NOTES for all opportunities having a partner organization and the note is external	Note	External Opportunity Notes of Opportunity Revenue Partner	OpportunityNote	Predefined rule for external opportunity notes of an opportunity revenue partner.	OpportunityRevenuePartne

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
Note	ZMM_NOTES_PRTNR_NOT_PRV	Access the opportunity note for table ZMM_NOTES for all opportunities having a partner organization and the note is not private	Note	Nonprivate Opportunity Notes of Partner Account Team	OpportunityNote	Predefined rule for nonprivate opportunity notes of a partner account team.	OpportunityRevenueToNor
Note	ZMM_NOTES_EDIT_ZPM_ENR_NOTES	Edit enrollment notes for table ZMM_NOTES which are not private if user is in the partner account team with edit access	Note	Nonprivate Notes of Program Enrollments	ProgramEnrollme	Predefined rule for nonprivate notes of program enrollment.	ProgramEnrollmentToNonP
NA	NA	NA	Note	Nonprivate Notes of Contact	ContactNoteRule	Predefined rule for nonprivate notes of a contact.	ContactToNonPrivateNote
Note	ZMMNOTESHZ12	Access the trading community resource note for table ZMM_NOTES for all resource notes	Note	All Notes of Resource	ResourceNoteRul	Predefined rule for all notes of a resource.	ResourceToAllNote
Note	ZMM_NOTES_VIEW_CHNL_ACCT_MGR	Access the opportunity note for table ZMM_NOTES where they are a member of the account team of a partner organization on the opportunity and the note is not private	Note	Nonprivate notes of Partner	PartnerNoteRule1	Predefined rule for nonprivate notes of a partner.	PartnerToNonPrivateNote
NA	NA	NA	Note	Nonprivate notes of Partner	PartnerNoteRule1	Predefined rule for nonprivate notes of a partner.	PartnerToNonPrivateNote

Opportunity Object Mapping

For each of the data security policies available for the Opportunity object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Opportunity	MOOOPTYMOO1	Access the opportunity for table MOO_OPTY where they selected records where I am on the team on the sales UI	Opportunity	Opportunity Team	OpportunityPR3	Opportunities where the access group member is on the opportunity team	OPTYTEAM
Opportunity	MOOOPTYMOO1	Access the opportunity for table MOO_OPTY where they selected records I own on the sales UI	Opportunity	Opportunity Owner	OpportunityPR1	Opportunities where the access group member is the opportunity owner	OPTYOWNER
Opportunity	MOOOPTYMOO1	Access the opportunity for table MOO_OPTY where they selected records my subordinates own on the sales UI	Opportunity	Opportunity Owner Hierarchy	OpportunityPR2	Opportunities where the access group member is in the management chain of the opportunity owner	OPTYOWNERHIER
Opportunity	MOOOPTYMOO1	Access the opportunity for table MOO_OPTY where they selected records where my subordinates are on the team on the sales UI_1	Opportunity	Opportunity Team Hierarchy	OpportunityPR6	Opportunities where the access group member is in the management chain of a resource who is on the opportunity team	OPTYTEAMHIER
Opportunity	MOOOPTYMOO1	Access the opportunity for table MOO_OPTY where they selected	Opportunity	Opportunity Territory Owner	OpportunityPR9	Opportunities where the access group member is the owner	OPTYTERRITORYOWNER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		records in my territory on the sales UI				of a territory associated with the opportunity	
Opportunity	MOOOPTYMOO1	Access the opportunity for table MOO_OPTY where they selected records in my territory hierarchy on the sales UI	Opportunity	Opportunity Territory Owner Hierarchy	OpportunityPR10	Opportunities where the access group member is the owner of a territory that is an ancestor of a territory associated with the opportunity	OPTYTERRITORYOWNERH
Opportunity	MOOOPTYMOO8	Access the opportunity for table MOO_OPTY for all opportunities in the enterprise	Opportunity	All Opportunities	OpportunityPR14	Access all opportunities	GLOBAL_OPPORTUNITY
Opportunity	MOO_OPTYACCTERR_HIER_RES	Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity sales account territory team or a territory resource with a descendant territory in the opportunity sales account territory team	Opportunity	Account Territory Team	AccountPR9	Accounts where the access group member is a member of the territory associated with the account	ACCOUNTTERRITORY
Opportunity	MOO_OPTYACCTERR_HIER_RES	Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity sales account territory team or a territory resource with a descendant territory in the opportunity	Opportunity	Account Territory Team Hierarchy	AccountPR10	Accounts where the access group member is a member of the territory that is an ancestor of the territory associated with the account	ACCOUNTTERRITORYHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		sales account territory team					
Opportunity	MOO_OPTY_ADMIN_SALES_ADMIN	Access the opportunity for table MOO_OPTY for all opportunities in the business units that they are authorized within	Opportunity	Business Unit Opportunities	OpportunityPR15	Opportunities in the business units that the access group member is associated with	BUOPPORTUNITIES
Opportunity	MOO_OPTY_EDIT_OPTYTEAM_MGR	Access the opportunity for table MOO_OPTY where they are in the management chain of an opportunity sales team member with edit or full access	Opportunity	Opportunity Team Hierarchy with Edit or Full Access	OpportunityPR7	Accounts where the access group member is in the management chain of a resource who is on the opportunity team with edit or full access	OPTYTEAMHIERWITHEDIT
Opportunity	MOO_OPTY_EDIT_OPTYTEAM_REPS	Access the opportunity for table MOO_OPTY where they are an opportunity sales team member with edit or full access	Opportunity	Opportunity Team with Edit Or Full Access	OpportunityPR4	Opportunities where the access group member is on the opportunity team with edit or full access	OPTYTEAMWITHEDITORFU
Opportunity	MOO_OPTY_FOR_ANY_PRTORG	Access the opportunity for table MOO_OPTY for all opportunities having a partner organization	Opportunity	Opportunity Partner	OpportunityPR13	Opportunities associated with a partner organization	OPTYANYPARTNERORG
Opportunity	MOO_OPTY_FOR_MYPRTACNT_PRTORG	Access the opportunity for table MOO_OPTY where they are a member of the account team of a partner organization on the opportunity	Opportunity	Partner Team	PartnerPR4	Partners where the access group member is a resource on the partner team	PARTNERTEAM

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Opportunity	MOO_OPTY_FOR_MY_PRTORG	Access the opportunity for table MOO_OPTY where they are a member of a partner resource organization whose partner organization is on the opportunity	Opportunity	Opportunity Partner Company	OpportunityPR16	Opportunities where the access group member is a member of the partner company associated with the opportunity	OPTYPARTNERCOMP
NA	NA	NA	Opportunity	Opportunity Partner Company Hierarchy	OpportunityPR17	Opportunities where the access group member is a member of the child partner company associated with the opportunity	OPTYPARTNERHIER
Opportunity	MOO_OPTY_FULL_OPTYTEAM_MGR	Access the opportunity for table MOO_OPTY where they are in the management chain of an opportunity sales team member with full access	Opportunity	Opportunity Team Hierarchy with Full Access	OpportunityPR8	Opportunities where the access group member is in the management chain of a resource who is on the opportunity team with full access	OPTYTEAMHIERWITHFULL
Opportunity	MOO_OPTY_FULL_OPTYTEAM_REPS	Access the opportunity for table MOO_OPTY where they are an opportunity sales team member with full access	Opportunity	Opportunity Team with Full Access	OpportunityPR5	Opportunities where the access group member is on the opportunity team with full access	OPTYTEAMWITHFULL
Opportunity	MOO_OPTY_TERR_HIER_RES	Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity	Opportunity	Opportunity Territory Team	OpportunityPR11	Opportunities where the access group member is a member of a territory associated with the opportunity	OPTYTERRITORY

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		territory team or a territory resource with a descendant territory in the opportunity territory team					
Opportunity	MOO_OPTY_TERR_HIER_RES	Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity territory team or a territory resource with a descendant territory in the opportunity territory team	Opportunity	Opportunity Territory Team Hierarchy	OpportunityPR12	Opportunities where the access group member is a member of a territory that is an ancestor of a territory associated with the opportunity	OPTYTERRITORYHIER
Opportunity	MOO_OPTY_VIEW_ACCTTEAM_MGR	Access the opportunity for table MOO_OPTY where they are in the management chain of an opportunity sales account team member	Opportunity	Account Team	AccountPR3	Accounts where the access group member is on the account team	ACCOUNTTEAM
Opportunity	MOO_OPTY_VIEW_OPTYTEAM_MGR	Access the opportunity for table MOO_OPTY where they are in the management chain of an opportunity sales team member with view, edit, or full access	Opportunity	Opportunity Owner Hierarchy	OpportunityPR2	Opportunities where the access group member is in the management chain of the opportunity owner	OPTYOWNERHIER
Opportunity	MOO_OPTY_VIEW_OPTYTEAM_REPS	Access the opportunity for table MOO_OPTY where they are an opportunity sales team member with	Opportunity	Opportunity Team	OpportunityPR3	Opportunities where the access group member is on the opportunity team	OPTYTEAM

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		view, edit, or full access					
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity sales team with view, edit or full access, member of territory team or upward territory hierarchy	Opportunity	Opportunity Team	OpportunityPR3	Opportunities where the access group member is on the opportunity team	OPTYTEAM
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity sales team with view, edit or full access, member of territory team or upward territory hierarchy	Opportunity	Opportunity Team Hierarchy	OpportunityPR6	Opportunities where the access group member is in the management chain of a resource who is on the opportunity team	OPTYTEAMHIER
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity sales team with view, edit or full access, member of territory team or upward territory hierarchy	Opportunity	Opportunity Territory Team	OpportunityPR11	Opportunities where the access group member is a member of a territory associated with the opportunity	OPTYTERRITORY

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity sales team with view, edit or full access, member of territory team or upward territory hierarchy	Opportunity	Opportunity Territory Team Hierarchy	OpportunityPR12	Opportunities where the access group member is a member of a territory that is an ancestor of a territory associated with the opportunity	OPTYTERRITORYHIER
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy	Opportunity	Account Team	AccountPR3	Accounts where the access group member is on the account team	ACCOUNTTEAM
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy	Opportunity	Account Team Hierarchy	AccountPR4	Accounts where the access group member is in the management chain of a resource who is on the account team	ACCOUNTTEAMHIER
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team,	Opportunity	Account Territory Team	AccountPR9	Accounts where the access group member is a member of the territory associated with the account	ACCOUNTTERRITORY

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		account territory team or upward territory hierarchy					
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy	Opportunity	Account Territory Team Hierarchy	AccountPR10	Accounts where the access group member is a member of the territory that is an ancestor of the territory associated with the account	ACCOUNTTERRITORYHIER
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy	Opportunity	Contact Team	ContactPR3	Contacts where the access group member is on the contact team	CONTACTTEAM
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy	Opportunity	Contact Team Hierarchy	ContactPR4	Contacts where the access group member is in the management chain of a resource who is on the contact team	CONTACTTEAMHIER
Opportunity	MOOOPTYZBS99	Access the opportunity for table MOO_OPTY where they are member or in	Opportunity	Contact Territory	ContactPR9	Contacts where the access group member is a member of the territory	CONTACTTERRITORY

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		management chain of opportunity account team, account territory team or upward territory hierarchy				associated with the contact	
Opportunity	MOOOPTYZBS9	Access the opportunity for table MOO_OPTY where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy	Opportunity	Contact Territory Hierarchy	ContactPR10	Contacts where the access group member is a member of the territory that is an ancestor of the territory associated with the contact	CONTACTTERRITORYHIER

Advanced permissions are defined for some of the Opportunity data security policies. Advanced permissions let you refine the access provided by a data security policy. This table shows how the advanced permissions available with Opportunity data security policies map to predefined access group rules.

Data Security Policy Business Object	Data Security Policy Advanced Permission Name	Access Group Object	Predefined Rule Name	Access Level
Opportunity	Manage Opportunity General Profile	Opportunity	Any predefined rule	Update, Full
Opportunity	Manage Opportunity Restricted Profile	Opportunity	Any predefined rule	Delete, Full
Opportunity	Manage Opportunity Revenue	Opportunity	Any predefined rule	Full
Opportunity	Manage Opportunity Team	Opportunity	Any predefined rule	Full
Opportunity	View Opportunity	Opportunity	Any predefined rule	Read, Update, Delete, Full

Access Extension Rules for Opportunity

For each of the data security policies available for the Opportunity object, this table shows the access extension rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
Opportunity	MOO_OPTY_VIEW_ACCTTEAM_REPS	Access the opportunity for table MOO_OPTY where they are a member of the opportunity sales account team	Opportunity	Opportunities of Related Household of Type Account (Consumer) Team	AccountOpportu	Predefined rule for opportunities of related household of type account (consumer) team.	HouseholdToOpportunity
Opportunity	MOO_OPTY_VIEW_ACCTTEAM_MGR	Access the opportunity for table MOO_OPTY where they are in the management chain of an opportunity sales account team member	Opportunity	Opportunities of Related Household of Type Account (Consumer) Team Hierarchy	AccountOpportu	Predefined rule for opportunities of related household of type account (consumer) team hierarchy.	HouseholdToOpportunity
Opportunity	MOO_OPTYACCTERR_HIER_RES	Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity sales account territory team or a territory resource with a descendant territory in the opportunity sales account territory team	Opportunity	Opportunities of Related Household of Type Account (Consumer) Territory	AccountOpportu	Predefined rule for opportunities of related household of type account (consumer) territory.	HouseholdToOpportunity
Opportunity	MOO_OPTYACCTERR_HIER_RES	Access the opportunity for table MOO_OPTY where they are a territory resource in the opportunity sales account territory team or a territory	Opportunity	Opportunities of Related Household of Type Account (Consumer) Territory Hierarchy	AccountOpportu	Predefined rule for opportunities of related household of type account (consumer) territory hierarchy.	HouseholdToOpportunity

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		resource with a descendant territory in the opportunity sales account territory team					

Partner Object Mapping

For each of the data security policies available for the Partner object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles of all partner accounts in the enterprise	Partner	All Partners	PartnerPR1	Access all partners	GLOBAL_ PARTNER
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where I am the partner account owner	Partner	Partner Owner	PartnerPR2	Partners where the access group member is the partner owner	PARTNEROWNER
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where I am on the management	Partner	Partner Owner Hierarchy	PartnerPR3	Partners where the access group member is in the management chain of the partner owner	PARTNEROWNERHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		chain of the partner account owner					
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where I am on the partner account team	Partner	Partner Team	PartnerPR4	Partners where the access group member is a resource on the partner team	PARTNERTEAM
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where my subordinates are on the partner account team	Partner	Partner Team Hierarchy	PartnerPR7	Partners where the access group member is in the management chain of a resource who is on the partner team	PARTNERTEAMHIER
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where I am the owner or a member of the partner account territory	Partner	Partner Territory Team	PartnerPR10	Partners where the access group member is a member of the territory associated with the partner	PARTNERTERRITORY
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where I am the owner or a member of a territory that is an ancestor of the partner account territory	Partner	Partner Territory Team Hierarchy	PartnerPR11	Partners where the access group member is a member of the territory that is an ancestor of the territory associated with the partner	PARTNERTERRITORYHIER

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where I am on an ancestor partner organization in the partner hierarchy	Partner	Child Partner Companies	PartnerPR13	Partners where the access group member is a member of an ancestor partner company	PARTNERHIER
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where I am on the partner organization	Partner	Partner Company	PartnerPR12	Partner where the access group member is member of the partner company	PARTNERORG

Note: When you provide users with access to partner records using access groups, users automatically receive the same access to the partner contact records. So to give users access to partner contact data, you must grant them access to the associated partner through access group membership.

Price Book Header Object Mapping

For the data security policy available for the Price Book Header object, this topic shows the access group rule that provides equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Price Book Header	QSCPRICEBOOKH	Access the price book for table QSC_PRICEBOOK_HEADERS_B for all price books in the enterprise	Price Book Header	All Price Book Headers	PriceBookHeader	Access all price book headers	GLOBAL_PRICEBOOKHEADER

Product Object Mapping

For the data security policy available for the Product object, this topic shows the access group rule that provides equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Product	QSCPRODUCTSB	Access the products for table QSC_PRODUCTS_B for all products in the enterprise	Product	All Products	ProductPR1	Access all products	GLOBAL_PRODUCT

Product Group Object Mapping

For the data security policy available for the Product Group object, this topic shows the access group rule that provides equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Product Group	QSCPRODGRPDE	Access the product group for table QSC_PROD_GRP_DETAILS for all product groups in the enterprise	Product Group	All Product Groups	ProductGroupPR	Access all product groups	GLOBAL_PRODUCTGROUP

Quote and Order Object Mapping

For each of the data security policies available for the Quote and Order object, this topic shows the access extension rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
Quotes and Orders	ZCASALESORDEI	Access the sales order for table ZCA_SALES_ORDER_HEADERS where they are member or in management chain of associated opportunity account team, account territory team or upward territory hierarchy	Quote and Order	Quotes and Orders of Related Opportunity Household of Type Account (Consumer) Team	OpptySalesOrder	Predefined rule for quotes and orders of related opportunity household of type account (consumer) team.	HouseholdToSalesOrderHe
Quotes and Orders	ZCASALESORDEI	Access the sales order for table ZCA_SALES_ORDER_HEADERS where they are member or in management chain of associated opportunity account team, account territory team or upward territory hierarchy	Quote and Order	Quotes and Orders of Related Opportunity Household of Type Account (Consumer) Team Hierarchy	OpptySalesOrder	Predefined rule for quotes and orders of related opportunity household of type account (consumer) team hierarchy.	HouseholdToSalesOrderHe
Quotes and Orders	ZCASALESORDEI	Access the sales order for table ZCA_SALES_ORDER_HEADERS where they are member or in management chain of associated opportunity account team, account territory team or upward territory hierarchy	Quote and Order	Quotes and Orders of Related Opportunity Household of Type Account (Consumer) Territory	OpptySalesOrder	Predefined rule for quotes and orders of related opportunity household of type account (consumer) territory.	HouseholdToSalesOrderHe
Quotes and Orders	ZCASALESORDEI	Access the sales order for table ZCA_SALES_ORDER_HEADERS where they are	Quote and Order	Quotes and Orders of Related Opportunity Household of Type Account	OpptySalesOrder	Predefined rule for quotes and orders of related opportunity household of type account	HouseholdToSalesOrderHe

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Access Extension Rule Name	Predefined Access Extension Rule Number	Predefined Access Extension Rule Description	Relationship Name
		member or in management chain of associated opportunity account team, account territory team or upward territory hierarchy		(Consumer) Territory Hierarchy		(consumer) territory hierarchy.	
NA	NA	NA	Quote and Order	Quotes and Orders of Related Household of Type Account (Consumer) Team	AccountSalesOrd	Predefined rule for quotes and orders of related household of type account (consumer) team.	HouseholdToSalesOrderHe
NA	NA	NA	Quote and Order	Quotes and Orders of Related Household of Type Account (Consumer) Team Hierarchy	AccountSalesOrd	Predefined rule for quotes and orders of related household of type account (consumer) team hierarchy.	HouseholdToSalesOrderHe
NA	NA	NA	Quote and Order	Quotes and Orders of Related Household of Type Account (Consumer) Territory	AccountSalesOrd	Predefined rule for quotes and orders of related household of type account (consumer) territory.	HouseholdToSalesOrderHe
NA	NA	NA	Quote and Order	Quotes and Orders of Related Household of Type Account (Consumer) Territory Hierarchy	AccountSalesOrd	Predefined rule for quotes and orders of related household of type account (consumer) territory hierarchy.	HouseholdToSalesOrderHe

Resource Object Mapping

For each of the data security policies available for the Resource object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Trading Community Party	HZPARTIESHZ22	Access the trading community resource for table HZ_ PARTIES for all trading community resources.	Resource	All Resources	ResourceUserPR1	All resources	ALLRESOURCES
Trading Community Party	NA	NA	Resource	All External Resources	ResourceUserPR2	All external resources	ALLEXTERNALRESOURCES
Trading Community Resource Profile	JTFRSRESOURCE	Access the trading community resource for table JTF_RS_ RESOURCE_ PROFILES for their resource record	Resource	Self Resource	ResourceUserPR3	My resource	MYRESOURCE
Trading Community Resource Profile	JTFRSRESOURCE	Access the trading community resource skill for table JTF_ RS_RESOURCE_ PROFILES for the resource skills of persons who they manage	Resource	Resource Hierarchy	ResourceUserPR7	My resource hierarchy	RESOURCEHIERARCHY

Sales Resource Quota Object Mapping

For each of the data security policies available for the Sales Resource Quota object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MOT_QM_ RESOURCE_ QUOTAS	MOTQMRESOUR	Access the sales resource quota for table MOT_QM_ RESOURCE_ QUOTAS where they are the owner of a parent territory in the territory hierarchy where the quota is assigned	Sales Resource Quota	Resource Quota Territory Owner Hierarchy	ResourceQuotaPI	Predefined rule for resource quota territory owner hierarchy	RESOURCEQUOTAOWNERH
MOT_QM_ RESOURCE_ QUOTAS	MOTQMRESOUR	Access the sales resource quota for table MOT_QM_ RESOURCE_ QUOTAS where they are the owner of the root territory, if the resource quota is for the root territory	Sales Resource Quota	Resource Quota Root Territory Owner	ResourceQuotaPI	Predefined rule for resource quota root territory owner	RESOURCEQUOTAROOTOW
MOT_QM_ RESOURCE_ QUOTAS	MOTQMRESOUR	Access the sales resource quota for table MOT_QM_ RESOURCE_ QUOTAS where they are an administrator of the territory to which the quota is assigned	Sales Resource Quota	Resource Quota Territory Administrator	ResourceQuotaPI	Predefined rule for resource quota territory administrator	RESOURCEQUOTAADMIN
MOT_QM_ RESOURCE_ QUOTAS	MOTQMRESOUR	Access the sales resource quota for table MOT_QM_ RESOURCE_ QUOTAS where they are an administrator of a parent territory in the territory hierarchy where the quota is assigned	Sales Resource Quota	Resource Quota Territory Administrator Hierarchy	ResourceQuotaPI	Predefined rule for resource quota territory administrator hierarchy	RESOURCEQUOTAADMINH

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MOT_QM_RESOURCE_QUOTAS	MOTQMRESOUR	Access the sales resource quota for table MOT_QM_RESOURCE_QUOTAS where they are the administrator of the root territory, if the resource quota is for the root territory	Sales Resource Quota	Resource Quota Root Territory Administrator	ResourceQuotaPI	Predefined rule for resource quota root territory administrator	RESOURCEQUOTAROOTAD
MOT_QM_RESOURCE_QUOTAS	MOTQMRESOUR	Access the sales resource quota for table MOT_QM_RESOURCE_QUOTAS where they are assigned the quota	Sales Resource Quota	Resource Quota Territory Member	ResourceQuotaPI	Predefined rule for resource quota territory member	RESOURCEQUOTAMEMBEI
MOT_QM_RESOURCE_QUOTAS	MOTQMRESOUR	Access the sales resource quota for table MOT_QM_RESOURCE_QUOTAS where they are the owner of the territory to which the quota is assigned	Sales Resource Quota	Resource Quota Territory Owner	ResourceQuotaPI	Predefined rule for resource quota territory owner	RESOURCEQUOTAOWNER
MOT_QM_RESOURCE_QUOTAS	MOTQMRESOUR	Access the sales resource quota for table MOT_QM_RESOURCE_QUOTAS for all sales resource quota objects in the enterprise	Sales Resource Quota	All Resource Quotas	ResourceQuotaPI	Predefined rule for all resource quotas	GLOBAL_RESOURCEQUOTA
MOT_QM_QUOTA_PLANS_B	MOTQMQUOTAP	Access the sales quota plan for table MOT_QM_QUOTA_PLANS_B for all sales quota plans	Sales Quota Plan	All Quota Plans	QuotaPlanPR1	Predefined rule for access to all quota plans	GLOBAL_QUOTAPLAN

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
MOT_QM_QUOTA_PLANS_B	MOTQMQUOTAP	Access the sales quota plan for table MOT_QM_QUOTA_PLANS_B for all sales quota plans that are active	Sales Quota Plan	All Active Quota Plans	QuotaPlanPR2	Predefined rule for access to active quota plans	ACTIVEQUOTAPLANS
MOT_QM_QUOTA_PLANS_B	MOTQMQUOTAP	Access the sales quota plan for table MOT_QM_QUOTA_PLANS_B for all sales quota plans that are new, pending activation, or active	Sales Quota Plan	All Not Completed Quota Plans	QuotaPlanPR3	Predefined rule for access to quota plans that are not in completed status	NONCOMPLETEDQUOTAPL

Sales Territory Object Mapping

For each of the data security policies available for the Sales Territory object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
NA	NA	NA	Sales Territory	All Territories	TerritoryPR0	Access all territories	GLOBAL_TERRITORY
Sales Territory	MOTTERRITORIE	Access the sales territory for table MOT_TERRITORIES where they are an administrator of the territory	Sales Territory	Active Territory Administrator	TerritoryPR1	Territories where the access group member is administrator of the active territory	TERRITORYACTIVEADMIN
Sales Territory	MOTTERRITORIE	Access the sales territory for table MOT_TERRITORIES where they are an administrator of the territory	Sales Territory	Draft Territory Administrator	TerritoryPR2	Territories where the access group member is administrator of the draft territory	TERRITORYDRAFTADMIN

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Sales Territory	MOTTERRITORIE	Access the sales territory for table MOT_ TERRITORIES where they are an administrator of a parent territory in the territory hierarchy	Sales Territory	Active Territory Administrator In Territory Hierarchy	TerritoryPR3	Territories where the access group member is administrator of the active parent territory in the territory hierarchy	TERRITORYACTIVEADMINH
Sales Territory	MOTTERRITORIE	Access the sales territory for table MOT_ TERRITORIES where they are an administrator of a parent territory in the territory hierarchy	Sales Territory	Draft Territory Administrator In Territory Hierarchy	TerritoryPR4	Territories where the access group member is administrator of the draft parent territory in the territory hierarchy	TERRITORYDRAFTADMINH
Sales Territory	MOTTERRITORIE	Access the sales territory for table MOT_ TERRITORIES where they are the territory owner	Sales Territory	Active Territory Owner	TerritoryPR5	Territories where the access group member is owner of the active territory	TERRITORYACTIVEOWNER
Sales Territory	MOTTERRITORIE	Access the sales territory for table MOT_ TERRITORIES where they are the territory owner	Sales Territory	Draft Territory Owner	TerritoryPR6	Territories where the access group member is owner of the draft territory	TERRITORYDRAFTOWNER
Sales Territory	MOTTERRITORIE	Access the sales territory for table MOT_ TERRITORIES where they are the owner of a parent territory in the territory hierarchy	Sales Territory	Active Territory Owner In Territory Hierarchy	TerritoryPR7	Territories where the access group member is owner of the active parent territory in the territory hierarchy	TERRITORYACTIVEOWNER
Sales Territory	MOTTERRITORIE	Access the sales territory for table MOT_ TERRITORIES where they are	Sales Territory	Draft Territory Owner In Territory Hierarchy	TerritoryPR8	Territories where the access group member is owner of the	TERRITORYDRAFTOWNERI

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
		the owner of a parent territory in the territory hierarchy				draft parent territory in the territory hierarchy	
Sales Territory For additional mapping information, see the note following the table.	MOTTERRITORIE	Access the sales territory for table MOT_TERRITORIES where they are a member of the territory team	Sales Territory	Active Territory Team	TerritoryPR9	Territories where the access group member is part of the active territory team	TERRITORYACTIVETEAM
NA	NA	NA	Sales Territory	Deleted Territory Owner	TerritoryPR10	Territories where the access group member is owner of the deleted territory	TERRITORYDELETEDOWNE
NA	NA	NA	Sales Territory	Deleted Territory Administrator	TerritoryPR11	Territories where the access group member is administrator of the deleted territory	TERRITORYDELETEDADMI

Note: The data security policy for the Sales Territory MOTTERRITORIESMOT26 instance set provides access to territory team members of both active and draft territories. This data security policy is mapped to the Active Territory Team (TerritoryPR9) predefined rule, which provides access to team members of active territories only. Team members of draft territories aren't assigned access through a predefined rule.

Sales Territory Proposal Object Mapping

For each of the data security policies available for the Sales Territory Proposal object, this topic shows the access group rules that provide equivalent data access.

Data Security Policy Business Object	Data Security Policy Predefined Instance Set	Data Security Policy Condition Name	Access Group Object	Predefined Rule Name	Predefined Rule Number	Predefined Condition Name	Predefined Condition Code
Sales Territory Proposal	MOTTERRPROPC	Access the sales territory proposal for table MOT_TERR_PROPOSALS where they are the proposal owner	Sales Territory Proposal	Proposal Owner	TerritoryProposal	Access the sales territory proposal for table MOT_TERR_PROPOSALS where they are the proposal owner	PROPOSALOWNER
Sales Territory Proposal	MOTTERRPROPC	Access the sales territory proposal for table MOT_TERR_PROPOSALS where they are an administrator of a territory owned by the proposal owner	Sales Territory Proposal	Proposal Territory Administrator	TerritoryProposal	Access the sales territory proposal for table MOT_TERR_PROPOSALS where they are an administrator of a territory owned by the proposal owner	PROPOSALTERRITORYADM
Sales Territory Proposal	MOTTERRPROPC	Access the sales territory proposal for table MOT_TERR_PROPOSALS where they are the owner of a territory administered by the proposal owner	Sales Territory Proposal	Proposal Territory Owner	TerritoryProposal	Access the sales territory proposal for table MOT_TERR_PROPOSALS where they are the owner of a territory administered by the proposal owner	PROPOSALTERRITORYOWN
NA	NA	NA	Sales Territory Proposal	All Proposals	TerritoryProposal	Access all PROPOSALS	GLOBAL_TERRITORYPROPOSAL

21 Security and Reporting

Security for Sales Analytics and Reports

Security for the analytics and reports that are delivered with the sales application is based on the roles that use each report. For example, sales managers can access sales analytics and reports that salespeople don't have access to.

Analytics are available throughout the sales application as embedded analytics and also in standalone mode by way of the transactional work areas. Sales users interact with information in Oracle Transactional Business Intelligence using Oracle Transactional Business Intelligence components, such as dashboards.

If you want to create new analytics or reports or edit existing ones, you should become familiar with sales security concepts and how access is secured to Oracle Transactional Business Intelligence subject areas, catalog folders, and 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, Sales Managerial Transaction Analysis Duty). Access to a subject area is needed to run or create reports for that subject area.

Catalog Folders

Catalog folders are functionally secured using the same duty roles that secure access to the subject areas. Therefore, a user who inherits the Sales Managerial Transaction Analysis Duty can access both the Sales Manager folder in the Catalog and the Sales Manager subject areas.

Reports

Analyses are secured based on the folders in which they're stored. If you haven't secured reports using the report permissions, then they're secured at the folder level by default. You can set permissions against folders and reports for roles, catalog groups, or users.

Information about Security and Reporting

When you receive your sales application, access to its functionality and data is secured using role-based access control. For more information about creating and securing reports, see the following guides on the Oracle Help Center at http://docs.oracle.com:

- Security Reference for Sales and Fusion Service

  Describes the sales application security reference implementation and includes descriptions of all the predefined data that is included in the security reference implementation for an offering.
- Creating and Administering Analytics for Sales and Fusion Service

  Explains how to view and work with analytics and reports.

- Subject Areas for Transactional Business Intelligence in Sales and Fusion Service

  Provides information about each subject area and the job roles and duty roles that secure access to the subject area.

Related Topics

- Security Reference for Sales and Fusion Service
- Creating and Administering Analytics for Sales and Fusion Service
- Subject Areas for Transactional Business Intelligence in Sales and Fusion Service

Permissions for Catalog Objects

The Business Intelligence Catalog stores business intelligence objects such as dashboards, dashboard pages, folders, and analyses. Users can view only the objects for which they're authorized.

Note that the owner of an object or folder can't automatically access the object or folder. To access an object or folder, the user must have the proper permission assigned in the object or folder's permission dialog.

What Are Permissions?

An object's owner or a user who has been given the proper privileges and permissions can assign permissions to catalog objects. Permissions are authorizations that you grant to a user or role to perform a specific action or group of actions on a catalog object. For example, if you work in the sales department and created a dashboard that contains quarterly sales projections, then you can give read access to this dashboard to all sales people, but give read, write, and delete access to sales directors and vice presidents.

> **Note:** Permissions are a part of the Oracle BI EE security model, and how permissions are initially assigned is based on how users, roles, and groups were set up on your application, and which privileges the Oracle BI EE administrator granted those users, roles, and groups.

Permission Definitions

To control access to objects (such as a folder in the catalog or a section in a dashboard), you assign permissions to roles, catalog groups, and users. The permissions that you can assign vary depending on the type of object with which you are working.

The following table shows the main types of permissions encountered for sales users:

Permission	Definition
Full Control	Use this option to give authority to perform all tasks (modify and delete, for example) on the object.
Modify	Use this option to give authority to read, write, and delete the object.
Traverse	Use this option to give authority to access objects within the selected folder when the user does not have permission to the selected folder. Access to these objects is required when the objects in the

Permission	Definition
	folder, such as analyses, are embedded in a dashboard or Oracle WebCenter Portal application page that the user has permission to access. For example, if you grant users the Traverse permission to the /Shared Folders/Test folder, then they can access objects, through the BI Presentation Catalog or embedded in dashboards or Oracle WebCenter Portal application pages, stored in the/Shared Folders/Test folder and stored in sub-folders, such as the /Shared Folders/Test/Guest folder. However, users cannot access (meaning view, expand, or browse) the folder and sub-folders from the Catalog.
Open	Use this option to give authority to access, but not modify, the object. If you are working with an Oracle BI Publisher object, this option enables you to traverse the folder that contains the object.
No Access	Use this option to deny access to the object. Explicitly denying access takes precedence over any other permission.
Custom	Use this option to display the Custom Permissions dialog, where you grant read, write, execute, and delete permissions.

For additional information about catalog object permissions, see Creating Analyses and Dashboards in Oracle Transactional Business Intelligence on Oracle Help Center at http://docs.oracle.com/.

Transaction Analysis Duty Roles

Oracle Transactional Business Intelligence secures reporting objects and data through a set of delivered OTBI Transactional Analysis Duty roles. These duty roles control which subject areas and analyses a user can access and what data a user can see in the application.

These are some of the OTBI Transactional Analysis Duty roles used in the sales application:

- Partner Channel Transaction Analysis Duty
- Partner Channel Administrative Transaction Analysis Duty
- Sales Administrative Transaction Analysis Duty
- Sales Executive Transaction Analysis Duty
- Sales Managerial Transaction Analysis Duty
- Sales Transaction Analysis Duty
- Incentive Compensation Transaction Analysis Duty

This table lists analytics and reports available to sales users. It also shows the predefined job roles that can access the different analytics and reports, and the OTBI Transactional Analysis Duty roles that provide the access.

Analytic or Report Name	Job Role	OTBI Transactional Analysis Duty Role
• Forecast vs. Quota • Sales Stage by Age	Sales VP	Sales Executive Transaction Analysis Duty

Analytic or Report Name	Job Role	OTBI Transactional Analysis Duty Role
• Sales Performance Trend • Top Open Opportunities		
• Forecast Vs Open Pipeline: My Team • My Team's Activities (By Type) • My Team's Leads • My Team's Performance • My Team's Pipeline • My Team's Tasks on Open Opportunities • My Team's Top Open Opportunities • Team Leadership Board • Top Accounts by My Team's Activities	Sales Manager	Sales Managerial Transaction Analysis Duty
• My Open Leads by Age • My Top Open Opportunities • My Forecast vs. Open Pipeline • My Open Leads by Source • My Open Tasks • My Performance • My Pipeline • My Stalled Opportunities • My Top Accounts by Open Opportunities • My Unaccepted Leads by Age • My Won Opportunities • Top Accounts by My Activities	Sales Representative	Sales Transaction Analysis Duty
• Evaluating My Partners' Pipeline • Evaluating My Partners' Quarterly and Yearly Closed Revenue • Evaluating My Partners' Current Quarterly Sales • Evaluating My Partners' Win Rate	Channel Account Manager	Partner Channel Transaction Analysis Duty

Note: The predefined Transaction Analysis Duty roles provide permissions to view but not create analyses and reports. Permissions to create reports are assigned at the job role level using Business Intelligence roles.

For additional information about the job roles that secure access to sales and service subject areas, and the OTBI Transactional Analysis Duty roles assigned to each job role, see the guide Subject Areas for Transactional Business Intelligence in Sales and Fusion Service.

Business Intelligence Roles

Business Intelligence roles grant access to analytics functionality, such as the ability to run or author reports. Assign users one or more of these roles, in addition to roles that grant access to reports, subject areas, catalog folders, and sales data.

Business Intelligence roles apply to both Oracle Analytics Publisher and Oracle Transactional Business Intelligence (OTBI).

These are the Business Intelligence roles.

Business Intelligence Role	Description
BI Consumer Role	Runs Business Intelligence reports.
BI Author Role	Creates and edits reports.
BI Administrator Role	Performs administrative tasks such as creating and editing dashboards and modifying security permissions for reports, folders, and so on.
BI Publisher Data Model Developer Role	Creates and edits data models.

BI Consumer Role

The predefined OTBI Transaction Analysis Duty roles inherit the BI Consumer Role. You can configure custom roles to inherit BI Consumer Role so that they can run reports but not author them.

BI Author Role

BI Author Role inherits BI Consumer Role. Users with BI Author Role can create, edit, and run OTBI reports. All predefined sales job roles that inherit an OTBI Transaction Analysis Duty role are also assigned the BI Author Role at the job role level, except for the Sales Representative job role which isn't assigned the BI Author role.

BI Administrator Role

BI Administrator Role is a superuser role. It inherits BI Author Role, which inherits BI Consumer Role. The predefined sales and service job roles don't have BI Administrator Role access.

BI Publisher Data Model Developer Role

BI Publisher Data Model Developer Role is inherited by the Application Developer role, which is inherited by the Application Implementation Consultant role. Users with either of these predefined job roles can manage BI Publisher data models.

Configure Security for Oracle Transactional Business Intelligence

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, for example, Sales Managerial Transaction Analysis Duty. 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 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 the application, or the associated security privileges. You also can't copy any role with a role code prefix of OBIA, for example, Business Intelligence Applications Analysis Duty (OBIA_ANALYSIS_GENERIC_DUTY). But you can configure reporting security according to your security requirements as described here.

Modifying Transaction Analysis Duty Role Assignments

If you want to change the subject areas that users have access to, then create a job role and provide the custom 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 partner and sales team subject areas by assigning both the Sales Managerial Transaction Analysis Duty and the Partner Channel Transaction Analysis Duty to the custom 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 the sales application 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 sales job roles that inherit a Transaction Analysis Duty role are also assigned the BI Author Role by default, except for the Sales Representative job role. However, you can optionally create copies of the predefined job roles and add or remove the BI Author Role from the custom roles as required. You can also add the BI Administrator Role to custom job roles if you have users who need to be able to perform high-level tasks in Business Intelligence, such as work with catalog groups.

Related Topics

- BI Administrator Permissions

View Reporting Roles

Viewing reporting roles can help you to understand Oracle Transactional Business Intelligence security. This topic explains how to view the following:

- The reporting roles that a job role inherits
- The reporting roles you are assigned

View the Reporting Roles Assigned to a Job Role

To view the OTBI reporting roles that a job role inherits, perform the following steps:

1. Sign in to the application with the IT Security Manager job role.
2. Select **Navigator** > **Tools** > **Security Console**.
3. On the Security Console, search for and select a job role. For example, search for the Sales 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.
4. Notice that the Sales Manager job role inherits the BI Author Role directly. The Sales Manager job role also inherits a number of Transaction Analysis Duty roles, such as the Sales Managerial Transaction Analysis Duty role and the Marketing Lead Transaction Analysis Duty role.
5. Click the Show Graph icon to switch to a graphical view of the Sales Manager job role.
6. Locate and expand one of the OTBI roles, for example, expand the Sales Managerial Transaction Analysis Duty role.

   Notice that the role inherits the BI Consumer Role. It also inherits the Transactional Analysis Duty role which is required to run queries and reports.

View the Reporting Roles You Are Assigned

To view all of the duty roles that you are assigned, including Business Intelligence roles and Transaction Analysis Duty roles, perform the following steps:

1. Select **Navigator** > **Tools** > **Reports and Analytics** to open the Reports and Analytics work area.
2. Click the **Browse Catalog** button.

   The Catalog page opens.
3. Click your user name in the global header, then select **My Account**.
4. Click the Application Roles tab.

   All the duty roles you are assigned are listed, including Transaction Analysis Duty roles and Business Intelligence roles.
5. Click **OK** to return to the Catalog page.
6. Click **Sign Out** to return to the Oracle Applications Cloud window.

Display Direct Report Data in Participant Manager Reports

This topic applies only to Incentive Compensation. You must enable the Secure by Manager Hierarchy person security profile before participant managers can see direct report participant data in their business intelligence reports. The application automatically generates and associates data grants using this security profile.

In the Setup and Maintenance work area:

1. Add the security profile.
2. Refresh the manager hierarchy.

Add the Security Profile

Only users with either View All HCM Data or IT Security access can do these steps.

1. In the setup and Maintenance work area, go to the following:
    - Offering: Sales
    - Functional Area: Users and Security
    - Task: Manage Data Role and Security Profiles
2. Search for roles staring with **Incentive**.
3. In the Search Results section, select **Incentive Compensation Participant Manager**.
4. On the toolbar, click **Assign** to open the Assign Data Role: Role Details page.
5. Click **Next** to open the Security Criteria page.
6. In the Person Security Profile field, select **View Manager Hierarchy**.
7. Click the **Secure by Manager** check box if it isn't already selected.
8. Click **Review**.
9. Click **Submit** to return to the Manage Data Role and Security Profiles page.
10. Click **Done** to return to the All Tasks tab.

Refresh the Manager Hierarchy

You must run and schedule the Refresh Manager Hierarchy process to populate the HR Foundation Person tables with the manager hierarchy information. Reporting data is unavailable until you run the process.

1. On the Navigator menu within Tools, select **Scheduled Processes**.
2. On the Search Results section toolbar, click **Schedule New Process**.
3. In the **Name** field, search for and select **Refresh Manager Hierarchy**.
4. Click **OK** to return to Schedule New Process.
5. Click **OK** to open Process Details.
6. Click **Submit**, which causes the Confirmation to appear.
7. Click **OK** to return to Process Details.
8. Click **Cancel** to return to the Overview page.

FAQs for Security and Reporting

Can I configure Oracle Transactional Business Intelligence duty roles?

You can't modify the predefined OTBI duty roles or the associated security privileges. But you can configure Oracle Transactional Business Intelligence reporting security by assigning different OTBI duty roles to a custom job role if necessary.

22 Security and Personally Identifiable Information

Overview

Securing and protecting confidential customer information against data breaches, data theft, or unauthorized access is an increasing concern for enterprises. To address this issue, Oracle restricts access to certain information, known as Personally Identifiable Information (PII), that's considered private to an individual.

Read this chapter to learn how personally identifiable information is secured in Oracle Applications Cloud.

For additional information about managing PII data, or about configuring access to PII data, see the guide Implementing Customer Data Management for CX Sales and Fusion Service at http://docs.oracle.com.

Related Topics

- Implementing Customer Data Management for Sales and Fusion Service

How to Protect Personally Identifiable Information

The data or information that's used to uniquely identify a contact, or locate a person is called personally identifiable information (PII). Examples are 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 Applications Cloud, the PII data is secured and can be accessed only by the following job roles with the exception of mobile phone data:

- Sales Administrator
- Enterprise Scheduler Job Application Identity for CRM
- Oracle Data Integrator Application Identity for CRM
- Web Services Application Identity for CRM

Mobile phone data is accessible to all seeded job roles. However, if access to mobile phone data is needed for custom job roles, the IT Security Manager must assign the required PII data policies to the custom job role in the Security Console. The IT Security Manager can also add data policies for other PII data to seeded job roles.

The following table lists the PII attributes that are secured in Oracle Applications Cloud.

Note: You can search privileges in Security Console using the Privilege Titles listed in the following table.

PII Attribute	Table Name	Privilege Title
Taxpayer Identification Number (Social Security Number)	HZ_PERSON_PROFILES	View Trading Community Person Social Security
Taxpayer Identification Number (Social Security Number)	HZ_PERSON_PROFILES	Manage Trading Community Person Social Security
Citizenship Number	HZ_CITIZENSHIP	View Trading Community Person Citizenship Number
Citizenship Number	HZ_CITIZENSHIP	Manage Trading Community Person Citizenship Number
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
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
Home Phone	HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL	View Trading Community Person Contact
Home Phone	HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL	Manage Trading Community Person Contact
Mobile Phone	HZ_CONTACT_POINTS rows with phone_type or phone_line_type value MOBILE	View Trading Community Person Mobile Phone Number
Mobile Phone	HZ_CONTACT_POINTS rows with phone_type or phone_line_type value MOBILE	Manage Trading Community Person Mobile Phone Number
Home Email	HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL	View Trading Community Person Contact
Home Email	HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL	Manage Trading Community Person Contact
Additional Identifiers	All rows that belong to PERSON party in HZ_ADDTNL_PARTY_IDS	View Trading Community Person Additional Identifier
Additional Identifiers	All rows that belong to PERSON party in HZ_ADDTNL_PARTY_IDS	Manage Trading Community Person Additional Identifier

23 Advanced Data Security

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.