Oracle Fusion Cloud Sales Automation

How do I create and manage security access groups in Oracle CX?

Oracle Fusion Cloud Sales Automation
How do I create and manage security access groups in Oracle CX?

G25874-07

Author: Carmen Myrick

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

Some application pages have help icons to give you access to contextual help. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. If the page has contextual help, help icons will appear.

Get Support

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

Get Training

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

Join Our Community

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

Learn About Accessibility

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

Share Your Feedback

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

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

Thanks for helping us improve our user assistance!

1 How do I create and manage security access groups in Oracle CX?

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.

Data Privileges and Access Groups

If you started using Oracle Sales application for the first time in Update 22B or later, your database resources are secured through system (predefined) access groups and rules and not through data security policies.

When you assign job roles to users, users are automatically assigned membership in an associated system access group. They 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 made up of:

- The business object that's being accessed, for example, Opportunity.

- An access level that defines the actions allowed 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 as long as 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.

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 an Access Group

After you've identified a group of resource users that need more security access, create an access group for the users and rules.

Note: You must be assigned the IT Security Manager job role or the Sales Administrator job role to create and manage access groups.

Create an Access Group

1. Sign in to the application as the sales administrator or as a user with the IT Security Manager job role.
2. In Setup and Maintenance, go to: **Sales offering Users and Security functional area Sales and Service Access**.
   Or, click **Navigator** > **Tools** > **Sales and Service Access Management**.
3. In the Access Groups page, click **Create** and enter the required information in the Create Access Group page.
4. Click **Save and Continue** to save your new group.

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 **Account**.
4. Enter a **Name** for your new rule, for example, **Account_Access**. Group member is owner of account territory.
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** checkbox for the rule is checked.
7. Optionally, select one of the predefined rules.
8. In the Conditions area, add a row to the table where you'll specify the rule conditions.
9. Add the rule conditions. For example, you might specify that group members have access to account records when the company is over a certain size.
10. Select **Save and Publish** from the Actions menu to publish the rule so it's available for assignment processing.

    Note: For any more rules you create for this group, you don't need to publish them. You only need to publish a rule once.

11. Save and close the page.
12. From the Monitor tab, 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*.

Add Members to the Group

Finally, add resources to your new, custom access group. You can add users to the group in these ways:

- Manually add users in the UI.
- Create group membership rules to automatically add users.
- 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** from the Actions menu to publish the rule.
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. 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.

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.

   > **Tip:** The default search shows only custom access groups. To view system access groups, select **System Groups - Role** from the search drop-down list.
3. What you can do depends on whether you're editing a custom or a system 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.

     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.
   - Here's what you can change for custom groups:
     - Change 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.
     - Remove all group members who were added to the group manually or delete individual members from the group.

       > **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 an 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.
- 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 run.

Delete an 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.
3. On the Edit Access Group page, select **Delete Group** from the Actions menu.
4. 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 and then click **Create Rule**.
3. On the Create Group Membership Rule page, enter a **Name** for the group membership rule.
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. Don't use custom attributes that aren't based on database columns, such as attributes based on a formula field.
Operator	Select the operator for your condition. For example, select **Equals** or **Is blank**.
Value	Enter a value for the attribute, if relevant. If you're entering more than one value, separate each value with a comma.

Enter the conditions.

> **Note:** The use of the Contains operator in a security rule isn't recommended because it leads to broad matching. Broad matching checks whether a specific substring exists, leading to broader matches than might be intended. Further, there's a practical limitation for the Contains operator regarding the total allowable characters within a rule. For example, if a rule's condition uses the Contains string of 1,000 characters, no more than four such rules can be applied per attribute. Similarly, if each Contains string is 500 characters long, a maximum of eight rules can be enforced using one attribute condition. Be aware of this limitation and plan and prioritize rule conditions accordingly to stay within the bounds of application capabilities.

This table lists example values for the fields in an example rule condition:

Conditions Field:	Object	Attribute	Operator	Value
	Resources	Roles	Equals	Sales Representative
	Resources Hierarchy	Parent Organization	Equals	NA Computers

6. From the **Actions** menu, select **Save and Publish** to ensure that your changes get included in the assignment processing.
7. 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. If you edit a rule, it's a good idea to run the process immediately.

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.

To edit a group membership rule, select the rule from the Edit Access Group: Group Membership Rules page. You can also delete or inactivate a 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 runs.

For information about running scheduled processes, see the *Understanding Scheduled Processes* guide.

Related Topics

- How do I configure real-time and near real-time access for access group object records?
- How do I create and manage access groups?
- Can I rename a custom role in an access group?
- How do I enable team-based access to custom objects when using access groups?

Manage System Access Groups

Overview of System Access Groups

System access groups and rules provide users with access to object data based on 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 supplies 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 tell which access groups are predefined: 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 and have the Predefined checkbox checked.

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 with 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 You Can Change for System Access Groups

You can add more predefined or custom object sharing rules to system groups.

However, you can't create 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.

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.

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 more 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
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 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.**

Related Topics

- How do I create membership rules for custom access groups?
- How do I create and manage access groups?
- Can I rename a custom role in an access group?
- How do I enable team-based access to custom objects when using access groups?

Scheduling Options for Object Sharing Rules Assignment Processing

You can specify whether the object sharing rules processing occurs automatically, and how often the process runs.

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. After 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 Scheduled 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 Object Sharing Rules

After you've created an access group, you can create rules to give the group access to an object's records.

> **Note:** You must be assigned the IT Security Manager job role or the Sales Administrator job role to create and manage access groups.

You can find more information on how to create and manage access groups in this topic: *How do I create and manage access groups?*

When you create a custom object sharing rule, you specify:

- The type of access
- The conditions for the access
- The groups to share the rule with

You then publish the rule to the Sales assignment engine so that the group members get assigned to the group.

Finally, the *Perform Object Sharing Rule Assignment Processing* scheduled process runs to enable access to the object for the salespeople (sales resources) in the 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 change 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**.
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**.
7. Deselect the **Active** checkbox 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 more information on this functionality, see *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, 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

Keep in these points 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 *Enable Additional Attributes for Access Group Object Sharing Rules*.
- Support for the object attributes listed in this table has been discontinued, so don't use them.

Object	Attribute
Resource	Phone
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. For example, don't use attributes that are based on a formula field that's not based a database column.

12. Enter any other 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, click **Apply** and then click **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. The levels and meanings are listed in this table:

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. Select **Publish Rules** from the Actions menu.
18. When the status indicator shows that 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.

Publish Rules

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 on 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

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 edit the object sharing rules from either of these locations:

- The Edit Access Group: Object Rules subtab (in which case there's a 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 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 *Edit Access Groups*.
- The Object Rules tab on the Access Groups page (in which case there's an object context)

  You can review or edit predefined and custom object sharing rules and access extension rules that have been created for a specific object on the Object Sharing Rules page.

  To delete a custom rule, or edit an access extension rule, you can only do it 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.
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 that you've created. To use either type of rule, the rule must be active. To activate a rule, or inactivate a rule you no longer need, select or deselect the **Active** checkbox.
6. If you're editing a custom object sharing rule you created, you can delete the rule by selecting **Delete** from the Actions menu. As long as 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 *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** checkbox.
   - 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:

i. Select the **Select and Add** option from the Actions menu.
ii. 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 and click **Apply**.
iii. Add any other groups and, when you've completed your selections, click **Done**.

> **Note:** For a predefined rule that Oracle has created the rule-system group association for, 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're done editing, 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. To apply the changes immediately, you can run the process manually using the steps outlined in *Run the Perform Object Sharing Rule Assignment Process*.

Related Topics

- How do I run the Perform Object Sharing Rule Assignment Scheduled 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.
Publish Rules	After you create or edit an object sharing rule or a group membership rule for an access group,	This process runs when you select the **Publish Rules** option from the **Actions** menu on the

Process	Description	Initiated
Runs the Perform Assignment Data Publish, Refresh, and Synchronization process.	this process makes the object sharing rules effective and eligible for the subsequent object assignment process stage.	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 Scheduled 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 Scheduled Process?

How do I run the Perform Object Sharing Rule Assignment Scheduled Process?

The Perform Object Sharing Rule Assignment scheduled process assigns rules to access group assignment objects each time you add an access group and publish the rules. You schedule and run this process from the access groups Monitor page.

Unless you create a schedule for it to run, the process runs automatically at certain times to make sure all object data for your access groups is up-to-date. You can also run the process manually to get 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 *Scheduling Options for Object Sharing Rules Assignment Processing*.

Run the Access Group Assignment 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 Most of the time, you'll select the Records Since Last Run option. This option runs the job for only those records that were updated since the last time 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 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.

Field	Entry
	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

To provide a group of users with access to data based on 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 based on 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 based on 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:

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:

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 sync 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. After you've 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. After the Perform Object Sharing Rule Assignment Processing process 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*.

> **Tip:** 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 more information about creating custom attributes and making them visible on a UI, see the *Configuring Applications Using Application Composer* guide. For more information about importing and exporting data, see the *Understanding Import and Export Management for Sales and Fusion Service* guide.

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** checkbox 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** checkbox 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.

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 Oracle Sales before Update 22B, the predefined job roles and any custom job roles you create gives users 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 that 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**.

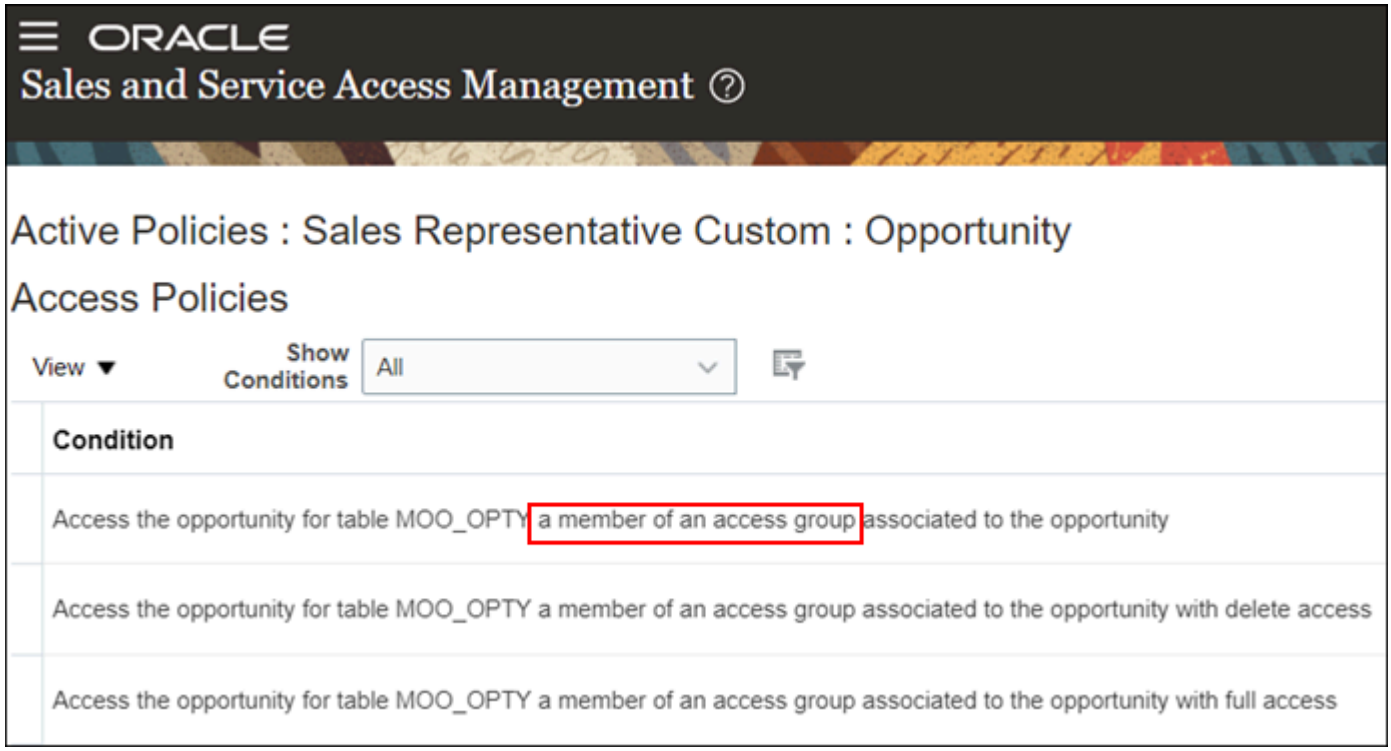
   The Active Policies table lists all the active data security policies for the opportunity object that are assigned to the Sales Representative Custom job role.
6. Click the Edit icon.

   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.

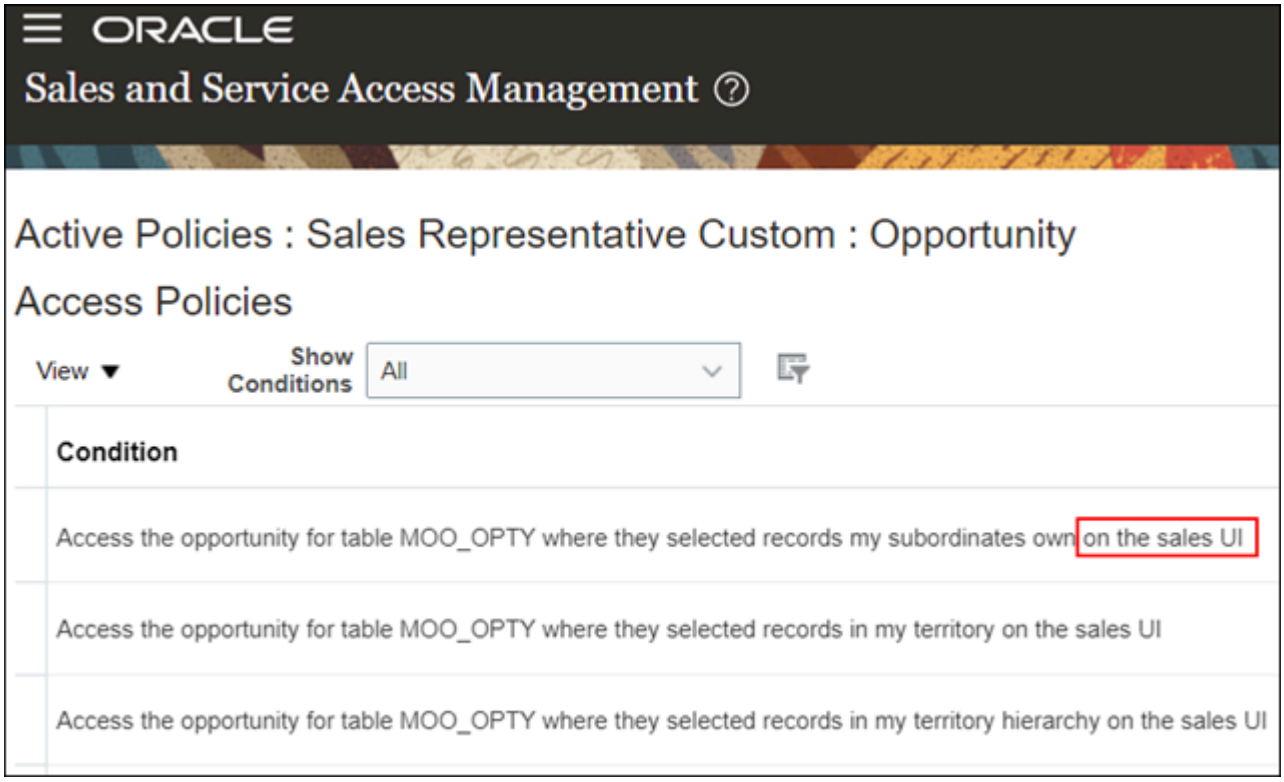
   Don't edit any policy where the Condition name of the policy includes a reference to `access group`. These policies, shown in the screenshot, are required for users to get access to object data through access groups and must remain associated with the custom role.



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 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

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

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 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
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

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 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
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	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

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
		with the sales account					
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
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

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 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 where they are in the management chain of a delegator only of an activity	ACTIVITY	Activity Delegator Hierarchy	ActivityPR4	Activities where the access group member is in the management chain of a delegator on the activity	ACTIVITYDELEGATORHIER
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	ACTIVITY	All Activity Templates	ActivityPR6	Access to all activity templates	ALLACTIVITYTEMPLATES

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
		activities in the enterprise.					
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 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 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 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	ACTIVITY	Activity Appointment and Call Report Delegator	ActivityPR10	Call reports and appointments where the access group	ACTIVITYAPPTANDCRDELE

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.				member is the delegator	
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 where they are either the owner or a delegator 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 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

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 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
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	ACTIVITY	All Nonprivate Activities for	ActivityPR18	Activities where the	ACTIVITYNONPRIVATEPAR

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 partner users are resources in the activity		Child Partner Companies		access group member is a member of an ancestor partner company related to the activity	
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 ZMM_ACTY_ ACTIVITIES where they are a participant on the 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 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

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 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
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 either a resource or a delegator of an activity	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 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	Activity Assignee	Delegator of Related Task	ActivityAssignee/	Predefined rule for delegator of related task.	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
		or a delegator of a call report 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	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 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 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 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

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 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 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	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 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

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 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
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	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 either a resource or a delegator of a task or an owner or a delegator of an appointment or a call report activity		of Related Appointment		or delegator of related appointment.	
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 users are resources in the activity	Activity Assignee	Partner Resource of Related Activity	ActivityAssignee/	Predefined rule for partner resource of related activity.	ActivityToActivityAssignee

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

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 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 management chain of a resource who is a sales party team member of the asset owner party	Asset	Assets of Related Asset Owner Account Team Hierarchy	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Team Hierarchy.	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 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	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

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
		team member of the asset owner 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 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 the asset owner party	Asset	Assets of Related Asset Owner Account Territory Owner Hierarchy	AccountAssetRul	Predefined rule for assets of Related Asset Owner Account Territory Owner Hierarchy.	AccountToAssets
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	Asset	Assets of Related All Asset Owner Account Customers	AccountAssetRul	Predefined rule for assets of Related All Asset Owner Account Customers.	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
		owner party is a customer					
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 ZCA_ASSET where user is a sales party team member of the asset owner party with edit access	Asset	Assets of Related Asset Owner Contact Team with Edit Access	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Team with Edit Access.	ContactToAssets
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

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 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 party with full access	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
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	Asset	Assets of Related Asset Owner Contact Territory Team	ContactAssetRule	Predefined rule for assets of Related Asset Owner Contact Territory Team.	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
		associated with the asset owner party					
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
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

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	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_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	Business Plan	Draft Business Plan Team with Edit or Full Access	BusinessPlanPR4	Business plans where the access group member is a resource on the business plan team with edit or full access and business plan status is draft or in revision	BPDRAFTTEAMEDITORFUL
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	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	BPTEAMRESHIER

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				business plan team	
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 team, with access level of edit or full, and business plan status is draft or in revision	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 business plan team with edit or full access and business plan status is draft or in revision	BPDRAFTTEAMEDITORFUL
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	Business Plan	Partner Business Plan Team	BusinessPlanPR1	Business plans where the access group member is a resource on the business plan team and	BPPARTNERBPTEAM

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
		is member of business plan team				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, 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_BP_BUSINESS_PLANS where the business plan class is partner and user is a contact of partner account	Business Plan	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	BPFORPARTNERRES
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

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

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

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 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 user is in the management chain of a resource who is on the sales contact team	Contact	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
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	CONTACTTEAMHIERWITH
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	Contact	Contact Team Hierarchy with Full Access	ContactPR8	Contacts where the access group member is on the contact team with full access	CONTACTTEAMHIERWITH

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 team with full access					
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
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

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	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 all people in the enterprise	Contact	Person Social Security Number	ContactPR16	Access person social security number	SOCIAL
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	Contact	Person Mobile Phone Number	ContactPR19	Access person mobile phone number	MOBILE

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
		personal phone numbers					
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
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

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	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 participant or observer of contest	Contest	Contest Resource	ContestPR4	Contests where the access group member is a contest participant or observer	CONTESTRESOURCE
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 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	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 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	NA	NA	NA	NA	NA

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 enterprise 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 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 team with view, edit or full access	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 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 or full access and deal status is Draft, Return or Withdrawn	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 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	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 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
		by internal resource					
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 or full access and deal status is Pending Approval or Approved	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 in the partner organization and deal status is Draft, Return or Withdrawn	Deal Registration	All Deal Registrations for Partner Company	DealRegistration	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	DealRegistration	Deal registrations where the access group member is a member of the partner company related to the deal registration	DEALREGISTRATIONFORPA

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	Deal Registration	Deal Registration Owner	DealRegistrationI	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	DealRegistrationI	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	Duplicate Identification Batch	All Duplicate Identification Batches	DuplicateIdentific	Access all duplicate identification batches	GLOBAL_DUPLICATEIDENTIFICATIO

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 all duplicate identification batches in the enterprise					

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	TerritoryForecastI	Territory Forecast where the access group member is a delegate of the territory	FCSTDELEGATE
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 Hierarchy	TerritoryForecastI	Territory Forecast where the access group member is the delegate of a parent territory in the territory hierarchy	FCSTDELEGATEHIER
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	TerritoryForecastI	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	TerritoryForecastI	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	Forecast Territory Details	Territory Forecast Old Owner	TerritoryForecastI	Territory Forecast where the access group member is the previous owner	FCSTPREVOWNER

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
		they owned previously for the active forecast					
NA	NA	NA	Forecast Territory Details	All Territory Forecasts	TerritoryForecastI	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	Goal	Goal Resource Hierarchy	GoalPR5	Goals where the access group member is in the management	GOALRESHIER

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 participant of goal				chain of a goal participant	

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	GoalParticipantPl	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	GoalParticipantPl	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	GoalParticipantPl	Goal participants where the access group member is the creator of the goal	GOALPARTICIPANTCREATO
Goal Participant	ZCAGOALPARTIC	Access the sales goal participants for table ZCA_GOAL_ PARTICIPANTS where user is participant of goal	Goal Participant	Goal Participant	GoalParticipantPl	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	Goal Participant	Goal Participant Resource Hierarchy	GoalParticipantPl	Goal participants where the access group member	GOALPARTICIPANTRESHIE

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 their subordinate is a participant of goal				is in the management chain of the goal participant	

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	HOUSEHOLDTEAMHIER

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
						households team	
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 team with edit access	HOUSEHOLDTEAMHIERWI
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

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	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
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
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

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 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
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	Lead	Lead Territory Team	LeadPR8	Leads where the access group member is a member of a territory associated with the lead	LEADTERRITORY

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 sales lead territory team or a territory resource with a descendant territory in the sales lead territory team					
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 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
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	Lead	Lead Owner Hierarchy	LeadPR3	Leads where the access group member is in the	LEADOWNERHIER

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 a manager in the management hierarchy of the owner of the sales lead				management chain of the lead owner	
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	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 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

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 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	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 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	Lead	Account Team	AccountPR3	Accounts where the access group member is on the account team	ACCOUNTTEAM

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
		upward territory hierarchy					
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 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 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	Lead	Lead Team	LeadPR4	Leads where the access group member is on the lead team	LEADTEAM

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
		upward territory hierarchy					
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 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	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	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	MDFBUDGETTEAMEDITOR

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
		with edit or full access				team with edit or full access	
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
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	MDFCLAIMPARTHIER

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 is a member of an ancestor partner company related to the MDF claim	
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
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

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, 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
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

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' 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 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	All MDF Claims with Status-Based Access Level	MDFClaimsPR8	Access all MDF claims where access level is status based	ALLMDFCLAIMS
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	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

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 failed or withdrawn Access the MDF claim for table MKT_BDT_ CLAIMS for all MDF claims in the partner organization					

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	MDF Request	All MDF Requests with Status-Based Access Level	MDFRequestsPR	Access all MDF requests where access level is status based	ALLMDFREQUESTS

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
		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	NA	NA	MDF Request	All MDF Requests for Child Partner Companies	MDFRequestsPR	MDF requests where the access group member is a member of an ancestor partner company related to the MDF request	MDFREQUESTPARTHIER
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	MDF Request	MDF Request Team Hierarchy	MDFRequestsPR	MDF requests where the access group member is in the management chain of a resource on the	MDFREQUESTTEAMHIER

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, or they are in the management chain of a resource on the MDF request team				MDF request team	
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, 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	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 MDF request team with edit access	MDFREQUESTTEAMHIERE
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	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

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 status is draft					
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 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	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
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	MDF Request	All MDF Requests for Partner Company	MDFRequestsPR	MDF requests where the access group member is a member of the partner company related	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
		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 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				to the MDF request	

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	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
		they are the author of the note					
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
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

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	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 the deploying company or external notes created by partner where they belong to the deploying company	Note	All Notes Created by Partner Company	NotePR4	Notes created by partner company	ALLNONPVTMYPARTNERC
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

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_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	Note	Nonprivate Opportunity Notes of	AccountNoteRule	Predefined rule for nonprivate opportunity notes of an	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
		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		Account Territory Team		account territory team.	
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	OpportunityNote	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	OpportunityNote	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	OpportunityNote	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
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	OpportunityNote	Predefined rule for nonprivate notes of an opportunity.	OpportunityToNonPrivateN
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	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
		and the note is external					
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
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.	OpportunityRevenueToNon
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	Note	Nonprivate notes of Partner	PartnerNoteRule	Predefined rule for nonprivate notes of a partner.	PartnerToNonPrivateNote

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
		of a partner organization on the opportunity and the note is not private					
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

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 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 records in my territory on the sales UI	Opportunity	Opportunity Territory Owner	OpportunityPR9	Opportunities where the access group member is the owner of a territory associated with the opportunity	OPTYTERRITORYOWNER
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

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_ 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 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	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

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_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
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

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_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 territory team or a territory resource with a descendant territory in the opportunity territory team	Opportunity	Opportunity Territory Team	OpportunityPR11	Opportunities where the access group member is a member of a territory associated with the opportunity	OPTYTERRITORY
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_	Access the opportunity for table MOO_	Opportunity	Opportunity Owner Hierarchy	OpportunityPR2	Opportunities where the access group	OPTYOWNERHIER

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
	OPTYTEAM_MGR	OPTY where they are in the management chain of an opportunity sales team member with view, edit, or full access				member is in the management chain of the opportunity owner	
Opportunity	MOO_OPTY_VIEW_OPTYTEAM_REPS	Access the opportunity for table MOO_OPTY where they are an opportunity sales team member with view, edit, or full access	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	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

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	OpportunityPR11	Opportunities where the access group member is a member of a territory associated with the opportunity	OPTYTERRITORY
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 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
		opportunity account team, account territory team or upward territory hierarchy				on the account team	
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	AccountPR9	Accounts where the access group member is a member of the territory associated with the account	ACCOUNTTERRITORY
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	Opportunity	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
		where they are member or in management chain of opportunity account team, account territory team or upward territory hierarchy				management chain of a resource who is on the contact team	
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 Territory	ContactPR9	Contacts where the access group member is a member of the territory associated with the contact	CONTACTTERRITORY
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 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

Data Security Policy Business Object	Data Security Policy Advanced Permission Name	Access Group Object	Predefined Rule Name	Access Level
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	Opportunity	Opportunities of Related Household of Type Account (Consumer) Territory	AccountOpportu	Predefined rule for opportunities of related household of type account (consumer) territory.	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
		or a territory resource with a descendant territory in the opportunity sales account territory team					
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 Hierarchy	AccountOpportu	Predefined rule for opportunities of related household of type account (consumer) territory hierarchy.	HouseholdToOpportunity

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	Partner	Partner Owner	PartnerPR2	Partners where the access group member	PARTNEROWNER

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
		organization party for table HZ_PARTIES all partner profiles where I am the partner account owner				is the partner owner	
Partner	HZPARTIESHZ52	Access the trading community organization party for table HZ_PARTIES all partner profiles where I am on the management chain of the partner account owner	Partner	Partner Owner Hierarchy	PartnerPR3	Partners where the access group member is in the management chain of the partner owner	PARTNEROWNERHIER
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	Partner Territory Team	PartnerPR10	Partners where the access group member is a member of the territory associated with the partner	PARTNERTERRITORY

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 account territory					
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
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	ZCASALESORDE	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	ZCASALESORDE	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	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

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
		upward territory hierarchy					
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 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 Hierarchy	OpptySalesOrder	Predefined rule for quotes and orders of related opportunity household of type account (consumer) territory hierarchy.	HouseholdToSalesOrderHe
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	AccountSalesOrd	Predefined rule for quotes and	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
				Related Household of Type Account (Consumer) Territory		orders of related household of type account (consumer) territory.	
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

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 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	ResourceUserPR	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

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 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
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	Sales Resource Quota	Resource Quota Territory Owner	ResourceQuotaPI	Predefined rule for resource	RESOURCEQUOTAOWNER

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 where they are the owner of the territory to which the quota is assigned				quota territory owner	
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
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	NONCOMPLETEDQUOTAPI

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
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	Sales Territory	Draft Territory Owner	TerritoryPR6	Territories where the access group member is	TERRITORYDRAFTOWNER

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 territory owner				owner of the draft territory	
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 the owner of a parent territory in the territory hierarchy	Sales Territory	Draft Territory Owner In Territory Hierarchy	TerritoryPR8	Territories where the access group member is owner of the draft parent territory in the territory hierarchy	TERRITORYDRAFTOWNERI
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

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:

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** checkbox.

   > **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 correct roles can see the custom object's UI (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 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 Scheduled 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 must sync the object to make it available for access groups and rules processing.

Here's how to sync 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.

After the custom object successfully syncs, here's what happens:

- 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 more 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.

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 hierarchical 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
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

Attribute	Description	Import Validations	Creating a Rule	Updating an Existing Rule	Deleting an Existing Rule
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.
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

Attribute	Description	Import Validations	Creating a Rule Condition	Updating an Existing Rule Condition	Deleting an Existing Rule Condition
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
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.
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.

Attribute	Description
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
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

Attribute	Description	Import Validations	Creating a Rule	Updating an Existing Rule	Deleting an Existing Rule
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
ReadAccessPermissionF	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

Attribute	Description	Import Validations	Creating Rule Details	Updating Existing Rule Details	Deleting Existing Rule Details
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've 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. Sync 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 need 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*.