# SECURITY CONSOLE

Working with the Security Console

Using the Security Console

Use the Security Console to manage application security in your Oracle Applications Cloud service. Use the IT Security Manager role to perform security-related tasks pertinent to role management, role analysis, user-account management, and certificate management.

Security Console Tasks

You can perform these tasks in the Security Console:

|  |  |
| --- | --- |
| Security Area | Tasks |
| Roles | Create job, abstract, and duty roles.  Edit custom roles.  Copy roles.  Compare roles.  Visualize role hierarchies and assignments to users.  Review Navigator menus available to roles or users, identifying roles that grant access to Navigator items and privileges required for that access. |
| Users | Create user accounts.  Review, edit, lock, or delete existing user accounts.  Assign roles to user accounts.  Reset passwords. |
| Analytics | Review statistics concerning role categories, the roles belonging to each category, and the components of each role.  View the data security policies, roles, and users associated with each database resource. |
| Certificates | Generate, export, or import PGP or X.509 certificates, which establish encryption keys for data exchanged between Oracle Cloud applications and other applications.  Generate signing requests for X.509 certificates. |
| Administration | Establish rules for the generation of user names.  Set password policies.  Create standards for role definition, copying, and visualization.  Review the status of role-copy operations.  Define templates for notifications of user-account events such as password expiration. |

Security Console Access

You must have the IT Security Manager role to use the Security Console. This role inherits the following duty roles:

Security Management

Security Reporting

Running Security Background Processes

To prepare the Security Console for use, arrange to run background processes that replenish security data. Also use Security Console Administration pages to select general and role-oriented options, track the status of role-copy jobs, and select, edit, or add notification templates. These generate messages to notify users of events that concern them, such as password-expiration warnings.

Run two background processes:

The Retrieve Latest LDAP Changes process copies data from the LDAP directory to Oracle Cloud Applications Security tables. Run it once, during implementation. Select Setup and Maintenance from the Navigator. In the Setup and Maintenance work area, search for and select the Run User and Roles Synchronization Process task.

The Import User and Role Application Security Data process copies users, roles, privileges, and data security policies from the identity store, policy store, and ApplCore grants schema to Oracle Cloud Applications Security tables. Schedule it to run regularly to update those tables: Select Scheduled Processes in the Tools work area, and then select the process from the Schedule New Process option.

General Administration Options

Select the Security Console Administration tab, and then the General tab on the Administration page, to set these options:

User Preferences

Select the format of the User Name, the value that identifies a user as he signs in. It is generated automatically in the format you select. Options include first and last name delimited by a period, email address, first-name initial and full last name, and person or party number.

Select the check box labeled "Generate system user name when generation rule fails" to enable the automatic generation of User Name values if the selected generation rule cannot be implemented.

Password Policy

Establish the number of days a password remains valid. Set the number of days before expiration that a user receives a warning to reset the password. And define the period in which a user must respond to a notification to reset his password ("Hours Before Password Reset Token Expiration").

Select a password format.

Determine whether a previous password may be reused.

Determine whether an administrator can manually modify passwords in the Reset Password dialog, available from a given user's record in the Users tab. This option applies only to the manual-reset capability. An administrator can always use the Reset Password dialog to initiate the automatic reset of a user's password.

Certificate Preferences: Set the default number of days for which a certificate remains valid. (Certificates establish keys for the encryption and decryption of data that Oracle Cloud applications exchange with other applications.)

Synchronization Process Preferences: Specify a number of hours since the last run of the Import User and Role Application Security Data process. When a user selects the Security Console Roles tab, a warning message appears if the process has not been run in this period.

Role Administration Options

Select the Security Console Administration tab, and then the Roles tab on the Administration page, to set these options:

Role prefixes and suffixes: Create the prefix and suffix added to the name and code of role copies. Each role has a Role Name (a display name) and a Role Code (an internal name). A role copy adopts the name and code of the source role, with this prefix or suffix (or both) added. The addition distinguishes the copy from its source. By default there is no prefix, the suffix for a role name is "Custom," and the suffix for a role code is "\_CUSTOM."

Graph node limit: Set the maximum number of nodes a visualization graph can display. When a visualization graph would contain a greater number of nodes, the visualizer displays a message advising the user to select the table view.

Enable edit of data security policies: Determine whether users can enter data in the Data Security Policies page of the role-creation and role-edit trains available from the Roles tab.

Enable edit of user role membership: Determine whether users can enter data in the Users page of the role-creation and role-edit trains available from the Roles tab.

Enable default table view: Determine whether visualizations generated from the Roles tab default to the table view or, if this option is cleared, the radial graph view.

Role Copy Status

Select the Security Console Administration tab, and then the Role Copy Status tab on the Administration page, to view records of jobs to copy roles. These jobs are initiated in the Roles page. Job status is updated automatically until a final status, typically Completed, is reached. You can delete the row representing a copy job; click its x icon.

Running Retrieve Latest LDAP Changes

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

You run Retrieve Latest LDAP Changes if you believe data-integrity or synchronization issues may have occurred between Oracle Cloud Applications and your LDAP directory server. For example, you may notice differences between roles on the Security Console and roles on the Create Role Mapping page. On-premises customers should also run this process after applying monthly updates.

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

Open the Scheduled Processes work area.

Click Schedule New Process in the Search Results section of the Overview page.

The Schedule New Process dialog box opens.

In the Name field, search for and select the Retrieve Latest LDAP Changes process.

Click OK to close the Schedule New Process dialog box.

In the Process Details dialog box, click Submit.

Click OK, then Close.

On the Scheduled Processes page, click the Refresh icon.

Repeat this step periodically until the process completes.

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

Security Visualizations

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

You can select either of two views:

Radial: Nodes form circular (or arc) patterns. The nodes in each circular pattern relate directly to a node at the center. That focal node represents the item you select to generate a visualization, or one you expand in the visualization.

Layers: Nodes form a series of horizontal lines. The nodes in each line relate to one node in the previous line. This is the item you select to generate a visualization, or the one you expand in the visualization.

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

The Radial view would initially show nodes representing the duty roles encircling a node representing the job role.

The Layers view would initially show the duty-role nodes in a line after the job-role node.

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

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

Working with a Visualization Graph

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

To select one of the views, click Switch Layout in the Control Panel, which is a set of buttons on the visualization. Then select Radial or Layers.

Node Labels

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

If the image is large enough, each node displays the name of the item it represents.

If the image is smaller, symbols replace the names: U for user, R for role, S for predefined role, P for privilege, and A for aggregate privilege.

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

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

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

Expanding or Collapsing Nodes

To expand a node is to reveal roles, privileges, or users to which it connects. To collapse a node is to hide those items. To perform these actions:

Select a node and right-click.

Select one of these options:

Expand reveals nodes to which the selected node connects directly, and Collapse hides those nodes.

Expand All reveals all generations of connecting nodes, and Collapse All hides those nodes.

Alternatively, double-click a collapsed node to expand it, or an expanded node to collapse it.

Using Control Panel Tools

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

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

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

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

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

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

Control Panel: Hide or expose the Control Panel.

Using the Legend

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

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

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

Hide or expose the Legend by clicking its button.

Using the Overview

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

As an alternative, click the background of the visualization, and move the entire image in any direction.

Refocusing the Image

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

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

Working with a Visualization Table

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

If you select a privilege as the focus of your visualization, select the Expand Toward Users option. Otherwise the table shows no results. Then use the Show option to list records of either roles or users who inherit the privilege.

If you select a user as the focus of your visualization, select the Expand Toward Privileges option. Otherwise the table shows no results. Then use the Show option to list records of either roles or privileges assigned to the user.

If you select any type of role or an aggregate privilege as the focus of your visualization, you can expand in either direction.

If you expand toward privileges, use the Show option to list records of either roles lower in hierarchy, or privileges related to your focus role.

If you expand toward users, use the Show option to list records of either roles higher in hierarchy, or users related to your focus role.

Tables are all-inclusive:

A Roles table displays records for all roles related directly or indirectly to your focus item. For each role, inheritance columns specify the name and code of a directly related role.

A Privileges table displays records for all privileges related directly or indirectly to your focus item. For each privilege, inheritance columns display the name and code of a role that directly owns the privilege.

A Users table displays records for all users assigned roles related directly or indirectly to your focus item. For each user, Assigned columns display the name and code of a role assigned directly to the user.

Use a field on a column to enter search text, then press Enter. The table displays records whose column values contain text matching your search text.

You can export a table to Excel. Click the Export to Excel button. You may either open the Excel file directly or save it. If you opt to save the file, you're prompted to define a path.

Generating a Visualization

To generate a visualization:

Select the Roles tab in the Security Console.

Search for the security item on which you want to base the visualization.

In a Search field, select any combination of item types, for example job role, duty role, privilege, or user.

In the adjacent field, enter at least three characters. The search returns items of the types you selected, whose names contain the characters you entered.

Select one of those items. Or, click the Search button to load all the items in a Search Results column, and select an item there.

Select either a Show Graph button or a View as Table button.

Note: In a page for role administration, you can determine which of these is the default view.

In the Expand Toward list, select Privileges to trace paths from your selected item toward items lower in its role hierarchy. Or select Users to trace paths from your selected item toward items higher in its hierarchy.

If the Table view is active, select an item type in the Show list: Roles, Privileges, or Users. (The options available to you depend on your Expand Toward selection.) The table displays records of the item type you select. Note that an aggregate privilege is considered to be a role.

Security Console Analytics for Roles

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

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

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

Roles

Role memberships (roles belonging to other roles within the category)

Security policies created for those roles

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

Roles in Category. Click a category in the Role Categories grid to list roles belonging to that category. For each role, the Roles in Category grid also shows the number of:

Role memberships

Security policies

Users assigned the role

Individual role statistics. Click the name of a role in the Roles in Category grid to list the security policies and users associated with the role. The page also presents collapsible diagrams of hierarchies to which the role belongs.

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

Data Security Policies

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

To begin, select the Analytics tab, and then the Database Resources tab on the Analytics page. Select the resource you want to review in the Database Resource field. Then click Go.

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

Each row documents a policy, specifying by default:

The data privileges it grants.

The condition that defines how data is selected from the database resource.

The policy name and description.

A role that includes the policy.

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

Authorized Roles

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

Include one or more data security policies that grant access to the database resource. The Authorized Roles table includes one row for each policy belonging to the role.

Inherit access to the database resource from one or more roles in its hierarchy. The Authorized Roles table includes one row for each inheritance.

By default, each row specifies:

The name of the role it documents.

The name of a subordinate role from which access is inherited, if any. (If the row documents access provided by a data security policy assigned directly to the subject role, this cell is blank.)

The data privileges granted to the role.

The condition that defines how data is selected from the database resource.

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

Authorized Users

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

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

Manipulating the Results

In any of these three tables, you can:

Add or remove columns. Select View - Columns.

Search among the results. Select View - Query by Example to add a search field on each column in a table.

Export results to a spreadsheet. Select the Export to Excel option available for each table.

Types of Secured Information

Information can be private, personally identifiable, or sensitive information.

Private information is confidential in some contexts.

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

Some PII information is sensitive.

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

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

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

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

Working with Roles in the Security Console

This topic describes the tasks associated with roles that you complete using the Security Console.

You can use the Security Console to perform a variety of tasks related to roles, including:

View the roles assigned to a user.

Identify users who have a specific role.

Copying existing roles.

Create duty, job, or abstract roles.

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

Viewing the Roles Assigned to a User

Open the Security Console.

On the Roles tab, search for and select the user.

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

Select the role and right-click.

Select Expand. Repeat these steps as required to move down the hierarchy.

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

Identifying Users Who Have a Specific Role

On the Roles tab of the Security Console, search for and select the role.

Depending on the enterprise setting, either a table or a graphical representation of the role hierarchy appears. Switch to the graphical representation if it doesn't appear by default.

Set Expand Toward to Users.

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

In the refreshed graph, user names appear on hover. Users may inherit roles either directly or indirectly from other roles. Expand a role to view its hierarchy.

In the Legend, click the Tabular View icon for the User icon. The table lists all users who have the role. You can export this information to Microsoft Excel.

Reviewing Role Hierarchies

On the Security Console you can review the role hierarchy of a job role, an abstract role, or a duty role.

On the Roles tab of the Security Console, ensure that Expand Toward is set to Privileges.

Search for and select the role. Depending on the enterprise setting, either a table or a graphical representation of the role appears.

If the table doesn't appear by default, click the View as Table icon. The table lists every role inherited either directly or indirectly by the selected role. Set Show to Privileges to switch from roles to privileges.

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

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

Comparing Roles

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

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

Select the Roles tab in the Security Console.

Do any of the following:

Click the Compare Roles button.

Create a visualization graph, right-click one of its roles, and select the Compare Roles option.

Generate a list of roles in the Search Results column of the Roles page. Select one of them, and click its menu icon. In the menu, select Compare Roles.

Select roles for comparison:

If you began by clicking the Compare Roles button, select roles in both First Role and Second Role fields.

If you began by selecting a role in a visualization graph or the Search Results column, the First Role field displays the name of the role you selected. Select another role in the Second Role field.

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

Select two roles for comparison.

Use the Filter Criteria field to filter for any combination of these artifacts in the two roles:

Function security policies

Data security policies

Inherited roles

Use the Show field to determine whether the comparison returns:

All artifacts existing in each role

Those that exist only in one role, or only in the other role

Those that exist only in both roles

Click the Compare button.

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

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

Adding Policies to a Role

Select two roles for comparison.

As the First Role, select a role in which policies already exist.

As the Second Role, select the role to which you are adding the policies. This must be a custom role. You cannot modify a predefined role.

Ensure that your selection in the Filter Criteria field excludes the Inherited roles option. You may select Data security policies, Function security policies, or both.

As a Show value, select Only in first role.

Click the Compare button.

Among the artifacts returned by the comparison, select those you want to copy.

An Add to Second Role option becomes active. Select it.

Custom Role Considerations

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

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

Providing Basic Information

On a Basic Information page:

In the Role Name field, create a display name, for example North America Accounts Receivable Specialist.

In the Role Code field, create an internal name for the role, such as AR\_NA\_ACCOUNTS\_RECEIVABLE\_SPECIALIST\_JOB.

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

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

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

Optionally, describe the role in the Description field.

Adding Function Security Policies

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

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

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

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

Select Add Function Security Policy.

In a Search field, select the value Privileges or types of role in any combination and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.

Select a privilege or role. If you select a privilege, click Add Privilege to Role. If you select a role, click Add Selected Privileges.

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

Click a privilege to view details of the code resource it secures.

Delete a privilege. You may, for example, have added the privileges associated with a role. If you want to use only some of them, you must delete the rest. To delete a privilege, click its x icon.

Note: Do not add data security policies manually to the Public Sector Compliance and Regulation services.

Configuring the Role Hierarchy

A Role Hierarchy page displays either a visualization graph, with the role you are creating as its focus, or a visualization table. Select the Show Graph button or View as Table button to select between them. In either case, link the role you are creating to other roles from which it is to inherit function and data security privileges.

If you are creating a duty role, you can add duty roles or aggregate privileges to it. In effect, you are creating an expanded set of duties for incorporation into a job or abstract role.

If you are creating a job or abstract role, you can add aggregate privileges, duty roles, or other job or abstract roles to it.

To add a role:

Select Add Role.

In a Search field, select a combination of role types and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.

Select the role you want, and click Add Role Membership. You add not only the role you have selected, but also its entire hierarchy.

In the graph view, you can use the visualization Control Panel, Legend, and Overview tools to manipulate the nodes that define your role hierarchy.

Adding Users to Roles

On a Users page, you can select users to whom you want to assign a job or abstract role you are creating. (You cannot assign a duty role directly to users.)

Note: For the Users page to be active, you must select an "Enable edit of user role membership" option. To locate it, select the Administration tab, and then the Roles tab on the Administration page. If this option is not selected, the Users page is read-only.

To add a user:

Select Add User.

In a Search field, select the value Users or types of role in any combination and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.

Select a user or role. If you select a user, click Add User to Role. If you select a role, click Add Selected Users; this adds all its assigned users to the role you are creating.

The Users page lists all selected users. You can delete a user. You may, for example, have added all the users associated with a role. If you want to assign your new role only to some of them, you must delete the rest. To delete a user, click its x icon.

Copying and Editing Roles

Rather than create a role from scratch, you can copy a role, then edit the copy to create a new role. Or you can edit existing custom roles.

Note: Do not edit roles delivered by Oracle.

Initiate a copy or an edit from the Roles tab in the Security Console. Do either of the following:

Create a visualization graph and select any role in it. Right-click and select Copy Role or Edit Role.

Generate a list of roles in the Search Results column of the Roles page. Select one of them, and click its menu icon. In the menu, select Copy Role or Edit Role.

If you are copying a role, select one of two options in a Copy Option dialog:

Copy role: You copy only the role you have selected. The source role has links to roles in its hierarchy, and the copy inherits links to the original versions of those roles. If you select this option, subsequent changes to the inherited roles affect not only the source highest role, but also your copy.

Copy role and inherited roles: You copy not only the role you have selected, but also all of the roles in its hierarchy. Your copy of the highest role is connected to the new copies of subordinate roles. If you select this option, you insulate the copied role from changes to the original versions of the inherited roles.

Next, an editing train opens. You follow the same process in editing a role as you would to create one. However, note the following:

In the Basic Information page, a Predefined role box is checked if you selected the Edit Role option for a role shipped by Oracle. In that case, you can:

Add custom data security policies. Modify or remove those custom data security policies.

Add or remove users if the role is a job, abstract, or discretionary role.

You cannot:

Modify, add, or remove function security policies.

Modify or remove data security policies provided by Oracle.

Modify the role hierarchy.

The Predefined role check box is cleared if you are editing a custom role or if you have copied a role. In that case, you can make any changes to role components.

By default, the name and code of a copied role match the source role's, except a prefix, suffix, or both are appended. In the Roles Administration page, you can configure the default prefix and suffix for each value.

A copied role cannot inherit users from a source job or abstract role. You must select users for the copied role. (They may include users who belong to the source role.)

When you copy a role, the Role Hierarchy page displays all roles subordinate to it. However, you can add roles only to, or remove them from, the highest role you copied.

To monitor the status of a role-copy job, select the Administration tab, and then the Role Copy Status tab of the Administration page.

Copying a Top Role

When you copy a role on the Security Console, you select one of the following options:

Copy top role

Copy top role and inherited roles

If you select the Copy top role option, then only the top role from the selected role hierarchy is copied. Memberships are created for the copy in the roles of which the original is a member. That is, the copy of the top role references the inherited role hierarchy of the source role. Any changes made to those inherited roles appear in both the source role and the copy. Therefore, you must take care when you edit the role hierarchy of the copy. You can:

Add roles directly to the copy without affecting the source role.

Remove any role from the copy that it inherits directly without affecting the source role. However, if you remove any role that's inherited indirectly by the copy, then any role that inherits the removed role's parent role is affected.

Add or remove function and data security privileges that are granted directly to the copy of the top role.

If you copy a custom role and edit any inherited role, then the changes affect any role that inherits the edited role.

The option of copying the top role is referred to as a shallow copy, where the copy references the same instances of the inherited roles as the source role. No copies are made of the inherited roles.

The option of copying the top role is referred to as a shallow copy. This figure summarizes the effects of a shallow copy. It shows that the copy references the same instances of the inherited roles as the source role. No copies are made of the inherited roles.

You're recommended to create a shallow copy unless you must make changes that could affect other roles or that you couldn't make to predefined roles. To edit the inherited roles without affecting other roles, you must first make copies of those inherited roles. To copy the inherited roles, select the Copy top role and inherited roles option.

Tip: The Copy Role: Summary and Impact Report page provides a useful summary of your changes. Review this information to ensure that you haven't accidentally made a change that affects other roles.

Copy a Top Role and the Inherited Roles

Selecting Copy top role and inherited roles is a request to copy the entire role hierarchy. These rules apply:

Inherited aggregate privileges are never copied. Instead, membership is added to each aggregate privilege for the copy of the source role.

Inherited duty roles are copied if a copy with the same name doesn't already exist. Otherwise, membership is added to the existing copies of the duty roles for the new role.

When inherited duty roles are copied, custom duty roles are created. Therefore, you can edit them without affecting other roles. Equally, changes made subsequently to the source duty roles don't appear in the copies of those roles. For example, if those duty roles are predefined and are updated during upgrade, then you may have to update your copies manually after upgrade.

This option is referred to as a deep copy, where copies of the inherited duty roles with the same name don't already exist. Therefore, the inherited duty roles are copied when you copy the top role. Aggregate privileges are referenced from the new role.

Copying Job and Abstract Roles

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

On the Roles tab of the Security Console, search for the role to copy.

Select the role in the search results. The role hierarchy appears in tabular format by default.

Tip: Tip: Click the Show Graph icon to show the hierarchy in graphical format.

In the search results, click the down arrow for the selected role and select Copy Role.

In the Copy Options dialog box, select a copy option.

Click Copy Role.

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

Tip: The role name and code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. You can overwrite these values for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make on the Copy Role: Basic Information page.

Click the Summary and Impact Report train stop.

Click Submit and Close, then OK to close the confirmation message.

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

If you prefer, you can visit the intermediate train stops after the Copy Role: Basic Information page and edit your copy of the role before you save it.

Editing Job and Abstract Roles

You can create a role by copying a predefined job role or abstract role and editing the copy.

Note: It is not recommended to create job or abstract roles from scratch in the Public Sector Compliance and Regulation services, except for any custom roles specifically documented in Functional Setup Manager. Copy existing roles and modify as needed.

On the Roles tab of the Security Console, search for and select your custom role.

In the search results, click the down arrow for the selected role and select Edit Role.

On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.

Click Next.

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear on the Privileges tab. Select a privilege to view details of the code resources that it secures in the Details section of the page.

To remove a privilege from the role, select the privilege and click the Delete icon. To add a privilege to the role:

Click Add Function Security Policy.

In the Add Function Security Policy dialog box, search for and select a privilege or role.

If you select a role, then click Add Selected Privileges to add all function security privileges from the selected role to your custom role. If you select a single privilege, then click Add Privilege to Role.

Click OK to close the confirmation message.

Repeat from step 2 for additional privileges.

Close the Add Function Security Policy dialog box.

Click Next.

Note: If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. As you can't grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can't edit these values.

Make no changes on the Copy Role: Data Security Policies page.

Note: Whether this page is enabled for edit depends on the current setting of the Enable edit of data security policiesoption. Set this option on the Roles subtab of the Security Console Administration tab.

Click Next.

The Edit Role: Role Hierarchy page shows the copied role and its inherited aggregate privileges and duty roles. The hierarchy is in tabular format by default. You can add or remove roles.

To remove a role:

Select the role in the table.

Click the Delete icon.

Click OK to close the confirmation message.

To add a role:

Click the Add Role icon.

In the Add Role Membership dialog box, search for and select the role to add.

Click Add Role Membership.

Click OK to close the confirmation message.

Repeat from step 2 for additional roles.

Close the Add Role Membership dialog box.

The Edit Role: Role Hierarchy page shows the updated role hierarchy.

Click Next.

To provision the role to users, you must create a role mapping. Don't provision the role to users on the Security Console.

Note: Whether this page is enabled for edit depends on the current setting of the Enable edit of user role membershipoption. Set this option on the Roles subtab of the Security Console Administration tab.

Click Next.

Copying and Editing Duty Roles

You can copy a duty role and edit the copy to create a duty role. Copying duty roles is the recommended way of creating duty roles.

On the Roles tab of the Security Console, search for the duty role to copy.

Select the role in the search results. The role hierarchy appears in tabular format by default.

Tip: Click the Show Graph icon to show the hierarchy in graphical format.

In the search results, click the down arrow for the selected role and select Copy Role.

In the Copy Options dialog box, select a copy option.

Click Copy Role.

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

Tip: The role name and code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. You can overwrite these values for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make on the Copy Role: Basic Information page.

Click the Summary and Impact Report train stop.

Click Submit and Close, then OK to close the confirmation message.

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

To edit the role:

On the Roles tab of the Security Console, search for and select your copy of the duty role.

In the search results, click the down arrow for the selected role and select Edit Role.

On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.

Click Next.

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear on the Privileges tab. Select a privilege to view details of the code resources that it secures.

To remove a privilege from the role, select the privilege and click the Delete icon. To add a privilege to the role:

Click Add Function Security Policy.

In the Add Function Security Policy dialog box, search for and select a privilege or role.

If you select a role, then click Add Selected Privileges to grant all function security privileges from the selected role to your custom role. If you select a single privilege, then click Add Privilege to Role.

Click OK to close the confirmation message.

Repeat from step 2 for additional privileges.

Close the Add Functional Security Policies dialog box.

Click Next.

Note: If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. As you can't grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can't edit these values.

Make no changes on the Edit Role: Data Security Policies page.

Note: Whether this page is enabled for edit depends on the current setting of the Enable edit of data security policiesoption. Set this option on the Roles subtab of the Security Console Administration tab.

Click Next.

The Edit Role: Role Hierarchy page shows the copied duty role and any duty roles and aggregate privileges that it inherits. The hierarchy is in tabular format by default. You can add or remove roles.

To remove a role:

Select the role in the table.

Click the Delete icon.

Click OK to close the information message.

To add a role:

Click Add Role.

In the Add Role Membership dialog box, search for and select the role to add.

Click Add Role Membership.

Click OK to close the confirmation message.

Repeat from step 2 for additional roles.

Close the Add Role Membership dialog box.

The Edit Role: Role Hierarchy page shows the updated role hierarchy.

Click Next.

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

Click Save and Close to save the role.

Click OK to close the confirmation message.

The role is available immediately.

Managing Implementation Users

This topic describes the tasks associated with the initial users of the implementation team.

Implementation Users

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

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

Setup users are usually not part of your Oracle Applications Cloud organization.

You don't assign them product-specific work or make it possible for them to view product-specific data.

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

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

Application Diagnostic Administrator

Application Implementation Consultant

Employee

IT Security Manager

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

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

Managing User Accounts

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

The user's login, first name, and last name, in a User column.

Whether the account is active, whether it is locked, and the user's password-expiration date, in a Status column.

It may also provide:

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

Party information, if the user account was created in conjunction with a party record created in CRM. This may include party number and party usage.

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

Reviewing details of, editing, or deleting existing accounts.

Adding new accounts.

Locking accounts.

Resetting users' passwords.

To begin working with user accounts:

Select the Users tab in the Security Console.

In a Search field, select any combination of user states and enter at least three characters.

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

Reviewing and Editing User Accounts

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

These details always include:

User information, which consists of user, first, and last name values, and an e-mail address. It also includes an external identifier if one has been created. This is an external-system identifier, such as a single sign-on account ID if single sign-on is enabled.

Account information, which comprises the user's password-expiration date, whether the account is active, and whether it is locked.

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

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

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

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

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

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

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

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

Adding User Accounts

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

To add a user account in the Security Console:

Select the Users tab in the Security Console to open the User Accounts page.

Click the Add User Account button.

Select a value for Associated Person Type: Worker if this account is to be linked to a worker record in HCM, or None if not.

By default, the account is set to be active and unlocked in the Account Information area. Typically these values are appropriate, but you may modify them.

Select the User Category with which you want to associate the user.

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

Enter name, e-mail, and password values in the User Information region as per the following guidance.

You need not enter a User Name value. It is generated automatically according to the user-name-generation rule selected in the General Administration page.

The First Name value is not required. However, you are expected to enter one if the selected user-name-generation rule makes use of the first name or the first-name initial.

The Password value must conform to the password policy established in the General Administration page. The Confirm Password value must match the Password value.

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

Click Add Autoprovisioned Roles, to assign roles for which role-provisioning rules make the user eligible.

Click Add Roles to assign other roles. Search for roles you want to assign, select them, then click Add Role Membership. Select Done when you are finished.

In the Roles table, select Assignable for any role that can be delegated to another user.

Click Save and Close.

Resetting Passwords

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

A new password must conform to your password policy. You establish this policy in the General Administration page. The page in which you reset the password displays the policy.

To reset a password:

In the User Accounts page, search for the user whose password you want to change.

In that user's row, click the Action icon, then Reset Password.

As an alternative, open the user's account for editing: click the User Login value in the User Accounts page, then Edit in a User Account Details page. In that page, select Reset Password.

In a Reset Password dialog, select whether to generate the password automatically or change it manually. For a manual change, also enter a new password value and a confirmation value, which must match the new value.

Note: The option to reset a password to an automatically generated value is always available. For the manual-reset option to be available, an "Administrator can manually reset password" option must be selected on the General Administration page.

Click the Reset Password button.

Locking and Unlocking User Accounts

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

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

To complete the first procedure:

In the user's row, click the Action icon, then Lock Account.

Respond Yes to a confirmation message.

To complete the second procedure:

Open the user's account for editing: click the User Login value in the User Accounts page, then Edit in a User Account Details page.

In the Edit User Account page, select the Locked check box in the Account Information region.

Select Save and Close.

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

Deleting User Accounts

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

Open the User Accounts page and search for the user whose account you want to delete.

In the user's row, click the Action icon, then Delete.

Respond Yes to a confirmation message.

Defining Notification Templates

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

To work with templates, click the User Categories tab in the Security Console. Then select a user category and on the User Category: Details page, click the Notifications tab. You must click the Edit button to make any changes.

There are eight events, and a predefined template exists for each event. Only one template linked to a given event can be enabled at a time. To use notification templates, ensure that notifications are enabled. To do that, select the Enable Notifications check box in the Notification Preferences region.

Even so, you can enable or disable templates, edit them, or create templates to replace existing ones. To create a template:

On the User Category: Notifications page, click Add Template.

Enter a name for the template and, optionally, a description.

Select an event. When you do, values for Message Subject and Message are copied from an already-configured template for which the same event is selected.

Edit the message subject, message text, or both. Note that message text may include tokens, which are replaced in runtime by literal values appropriate for a given user or account.

Select the Enabled check box to use the template immediately. If you do, the application automatically disables the template that had been enabled for that event. Or, leave the check box cleared to hold the template in reserve.

Click Save and Close.

To edit a template, select it from the templates listed in the Notification Templates table. Then follow essentially the same process as you would to create a template. Note, however, that you cannot modify the event selected for a template that has been saved. You may enable or disable an individual template by selecting or clearing its Enabled check box as you edit it.

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

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

The following table lists the tokens you can use in the message text for a template

|  |  |
| --- | --- |
| Token | Meaning |
| ${userLoginId} | The user name of the person whose account is being created or modified. |
| ${firstName} | The given name of the person whose account is being created or modified. |
| ${lastName} | The surname of the person whose account is being created or modified. |
| ${managerFirstName} | The given name of the person who manages the person whose account is being created or modified. |
| ${managerLastName} | The surname of the person who manages the person whose account is being created or modified. |
| ${loginUrl} | The web address to sign in to Oracle Cloud. The user can sign in and use the Preferences page to change a password that is about to expire. Or, without signing in, the user can engage a forgot-password procedure to change a password that has already expired. |
| ${resetUrl} | A one-time web address expressly for the purpose of resetting a password, used in the Password Generated, Password Reset, New Account, and New Account Manager templates. |
| ${CRLFX} | Insert line break. |
| ${SP4} | Insert four spaces. |

Synchronizing User and Role Information

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

Follow these steps:

Sign in to your Oracle Applications Cloud service environment as the service administrator.

Select Navigator Others Setup and Maintenance to open the Setup and Maintenance work area.

In the Setup and Maintenance work area, select the Run User and Roles Synchronization Process task in the Initial Users functional area.

The process submission page for the Retrieve Latest LDAP Changes process opens.

Click Submit.

Click OK to close the confirmation message.

Resetting the Cloud Service Administrator Sign-In Details

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

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

In the Setup and Maintenance work area, select the Create Implementation Users task in the Initial Users functional area.

The User Accounts page of the Security Console opens.

Search for your service administrator user name, which is typically your email. Your service activation mail contains this value.

In the search results, click your service administrator user name to open the User Account Details page.

Click Edit.

Change the User Name value to ServiceAdmin.

Delete any value in the First Name field.

Change the value in the Last Name field to ServiceAdmin.

Delete the value in the Email field.

Click Save and Close.

Sign out of your Oracle Applications Cloud service.

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

Managing User Categories

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

Users have different preferences in receiving automated notifications from the Security Console. For example, employees of your organization using the organization's single sign-on don't require notifications from the Security Console about creating new users, password expiry, or password reset. However, the suppliers of your organization who aren't using the organization's single sign-on, must receive such notifications from the Security Console.

You have built an external application for a group of users using the REST APIs of Oracle Fusion Applications. You intend to redirect this user group to the external application when using the Security Console to reset passwords or create new users.

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

|  |  |
| --- | --- |
| Task | Description |
| Segregate users into categories | Create user categories and add existing users to them. All existing users are automatically assigned to the Default user category unless otherwise specified. You may create more categories depending upon your requirement and assign users to those categories.  Note: You can assign a user to only one category. |
| Specify Next URL | Specify a URL to redirect your users to a website or an application instead of going back to the Sign In page, whenever they reset their password. For example, a user places a password reset request and receives an Email for resetting the password. After the new password is authenticated, the user can be directed to a website or application. If nothing is specified, the user is directed to Oracle Applications Cloud Sign In page. You can specify only one URL per user category. |
| Enable notifications | Notifications are enabled by default, but you can disable them if required. You can also enable or disable notifications separately for each user category. If users belonging to a specific category don't want to receive any notification, you can disable notifications for all life cycle events. Alternatively, if users want to receive notifications only for some events, you can selectively enable the functionality for those events.  Notifications are sent for a set of predefined events. To trigger a notification, you must create a notification template and map it to the required event. Depending on the requirement, you can add or delete a template that is mapped to a particular event.  Note: You can't edit or delete predefined notification templates that begin with the prefix ORA. You can only enable or disable them. However, you can update or delete the user-defined templates.  User Category feature supports both SCIM protocol and HCM Data Loader for performing any bulk updates. |

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

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

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

Create a user category and add users to it

Add users to an existing user category

Specify the user category for an existing user

Note: You can create and delete a user category only using the Security Console. Once the required user categories are available in the application, you can use them in SCIM REST APIs and data loaders. You can't rename a user category.

Adding Users to a New User Category

To create a user category and add users:

On the Security Console, click User Categories Create.

Click Edit, specify the user category details, and click Save and Close.

Click the Users tab and click Edit.

On the Users Category: Users page, click Add.

In the Add Users dialog box, search for and select the user, and click Add.

Repeat adding users until you have added the required users and click Done.

Click Done on each page until you return to the User Categories page.

Adding Users to an Existing User Category

To add users to an existing user category:

On the Security Console, click User Categories and click an existing user category to open it.

Click the Users tab and click Edit.

On the Users Category: Users page, click Add.

On the Add Users dialog box, search for and select the user, and click Add.

Repeat adding users until you have added the required users and click Done.

Click Done on each page until you return to the User Categories page.

Specifying the User Category for an Existing User

To add an existing user to a user category:

On the Security Console, click Users.

Search for and select the user for whom you want to specify the user category.

On the User Account Details page, click Edit.

In the User Information section, select the User Category. The Default user category remains set for a user until you change it.

Click Save and Close.

On the User Account Details page, click Done.

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

Managing Notifications

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

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

Click the Notifications tab and click Edit.

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

Click Done.

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