Oracle Fusion Cloud Customer Experience

Securing Sales and Fusion Service

Oracle Fusion Cloud Customer Experience
Securing Sales and Fusion Service

F77857-11

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

Contents

Get Help

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

Get Help in the Applications

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 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.

Share Your Feedback

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

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

Thanks for helping us improve our user assistance!

1 About This Guide

Introduction to Securing Oracle Sales and Oracle Fusion Service

This guide provides you with some basic concepts and procedures to help you implement and administer security for Oracle Sales and Oracle Fusion Service. Most of the basic concepts and procedures also apply to other Oracle CX applications like Oracle Subscription Management.

During implementation, you perform security-related tasks from a functional area task list. Once the implementation is complete, you can perform most security-related tasks on the Security Console or the Sales and Service Access Management work area. Any exceptions are identified in relevant topics.

Additional Resources

In addition to the information in this guide, consult the playbooks available in the *Create and manage users* section of the *Playbooks* page in the *Oracle Sales Help Center*.

To get started creating or importing users, see the *Set Up Users* section in the *How do I get started with Oracle Sales for Redwood?* playbook. This playbook's located in the *Get started with Oracle Sales for Redwood* playbook on the *Playbooks* page in the *Oracle Sales Help Center*.

2 Authentication

Authentication and Identity Management

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

Standard Authentication for Cloud Applications

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

Identity Store

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

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

Single Sign-On Authentication

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

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

3 Location Based Access

Overview

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

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

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

What Happens When You Enable Location-Based Access

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

Prerequisite

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

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

Related Topics

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

How Location-Based Access Works

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

Scenarios

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

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

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

Related Topics

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

Enable and Disable Location-Based Access

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

Before You Start

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

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

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

Enable Location-Based Access

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

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

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

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

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

Disable Location-Based Access

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

Related Topics

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

FAQs for Location Based Access

What is allowlisting?

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

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

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

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

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

How can I make a role public?

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

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

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

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

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

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

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

Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINSTER_SECURITY_PRIV

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

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

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

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

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

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

Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Location Based Access Disabled Confirmation Template

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

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

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

Here's how you enable the profile option:

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

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

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

Do these steps:

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

5. Click **Submit**.

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

4 Single Sign-On (SSO)

Oracle Applications Cloud as the Single Sign-On (SSO) Service Provider

Your users are likely to access different internal and external applications to perform their tasks. They might require access to different applications hosted by partners, vendors, and suppliers.

Certainly, users won't like authenticating themselves each time they access a different application. This is where you as the IT Manager can make a difference. You can provide your users with a seamless single sign-on experience, when you set up Oracle Applications Cloud as a single sign-on service provider.

Your users are registered with identity providers who store and manage their identity and credentials. In Security Console, you can add those identity providers so that you can verify those users without having to store that information.

> **Note:** The identity service associated with your Oracle Fusion Cloud Applications is getting upgraded to the Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) identity domain.If your environment is yet to be upgraded, you can continue to use the Security Console to configure the Single Sign-On settings with the information provided in this section. After your environment is upgraded, see *Federating with Identity Providers* to federate an Oracle Fusion Cloud Applications environment identity domain. See also *How do I find the identity domain for a Fusion Applications environment?*

Initial Sign-in

On a typical working day, when users sign in for the first time, they request access to an application or a web page. Oracle Applications Cloud, which is set up as a service provider, sends a verification request to the user's identity provider who's already added to the Security Console. The identity provider verifies the user credentials and sends the authorization and authentication response back to the service provider. After successful authentication, users are granted access to the required application or web page. Because the authentication is valid across your enterprise network, users don't have to sign in again when accessing different applications available on the same network. This entire trust chain between the service provider and the various identity providers is established using the Security Assertion Markup Language (SAML) 2.0 standards.

Final Sign-out

Single sign-on also applies to signing out of the enterprise network. When users sign out from one application, they're automatically signed out from all applications on the network. This is to prevent unauthorized access and to ensure that data remains secure all the time.

Prerequisite

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

- A valid email

- The IT Security Manager role
- Email notifications are enabled

Configure Single Sign-On

To enable single sign-on in your environment, complete the settings in the Single Sign-on Configuration section on the Security Console. This configuration lets you enable a login page and a page to which users must be redirected to after logging out of the application.

Do these steps:

1. On the Security Console, click the **Single Sign-On** tab.
2. In the Single Sign-On Configuration section, click **Edit**.
3. Enter the **Sign Out URL**. Users are redirected to this page once they sign out from the application.

   Note: The Sign Out URL is the same for all the identity providers that you configure.

4. If **Enable Chooser Login Page** isn't enabled already, select it to display the service provider's single sign-on page along with your company's login page.
5. Click **Save**.

To configure Oracle Applications Cloud as the service provider, you must do the following:

- Review the service provider details
- Add an identity provider
- Test the identity provider
- Enable the identity provider

On the Security Console, go to the Single Sign-On tab and click **Create Identity Provider**.

Note: Oracle Cloud Applications support all SAML 2.0 compatible federation servers.

Review Service Provider Details

- Service provider metadata. The URL references to an XML file that you can download and view.
- Service provider signing certificate.
- Service provider encryption certificate.

You must share these details with the identity providers so that they can use them to configure your application as the associated service provider.

Add an Identity Provider

You can add as many identity providers as required to facilitate single sign-on for all your users. However, one of them must be the default identity provider.

Before you begin:

One of the important steps in adding an identity provider is to import the metadata content of the identity provider. The metadata file contains the authentication information and also the signed and encrypted certificates of the identity

provider. Make sure you have the metadata XML file or the URL readily available. Without the file, the setup isn't complete.

Note: Including encryption certificate in the metadata file is optional.

1. On the Security Console, click **Single Sign-On** > **Create Identity Provider**.
2. On the Identity Provider Details page, click **Edit** and enter the identity provider details:
    - Provide a **Name** and **Description** for the identity provider. Ensure that the identity provider name is unique for the partnership.
    - Select the relevant Name ID Format. If you have an email as the name of the identity provider, select **Email**. Otherwise, leave it as **Unspecified**.
    - Enter the **Relay State URL**. Users are directed to this URL to sign and authenticate irrespective of which application they want to access.
    - Select the **Default Identity Provider** check box to make this identity provider the default one.
3. Import the identity provider metadata:
    - If it's an XML file, click **Browse** and select it.
    - If it's available on a web page, select the **External URL** check box and enter the URL. External URL isn't stored in this configuration and is used only for importing the identity provider metadata during identity provider creation or modification.

    Note: The metadata XML file must be Base64 encoded.
4. Click **Save and Close**.

    Note: Oracle Applications Cloud can't be used as an identity provider.

Test the Identity Provider

Click the Diagnostics and Activation tab to verify if the identity provider that you added works as expected.

1. Click the **Test** button to run the diagnostics. The Initiate Federation SSO page appears.
2. Click the **Start SSO** button. You're prompted to enter the user credentials of any user registered with the identity provider. The test validates whether the federation single sign-on is successful or not. The result summary includes the following details:
    - Status of authentication: success or failure
    - The attributes passed in the assertion
    - The assertion message in XML

You can review the log messages that appear in the Federation Logs section to identify if there are any configuration issues with the identity provider.

Note: You must run the test whenever there's a change in the identity provider configuration.

Enable the Identity Provider

If everything looks fine, you can go ahead and enable the identity provider. While you're on the Diagnostics and Activation page, click **Edit** and select the **Enable Identity Provider** check box. The identity provider is now active.

Note: You can enable an identity provider only after you import service provider metadata into the identity provider.

FAQs on Single Sign-On

Does the service provider store user passwords?

No. Passwords are stored with the identity providers. When a user signs in, the identity provider authenticates the password, authorizes the request to access an application, and sends that confirmation back to the service provider.

The service provider then allows users to access the application or web page.

Can I set up an identity provider without enabling it?

Yes, you can set up an identity provider and test it thoroughly before enabling it. By default, an identity provider remains disabled. You can disable an identity provider at any time.

How can I allow my users to sign in using their company's credentials?

On the Security Console, go to Single Sign-On Identity Provider Details page and make sure that the Enable Chooser Login Page check box is selected.

When your users access the main portal page, they can sign in using one of the following options:

- The single sign-on credentials registered with the identity provider
- The single sign-on credentials registered with their company

What should I do to extend the validity of certificates provided by the identity provider?

Pay attention to the notifications you receive about certificate expiry. Request your identity provider to share with you the updated metadata file containing renewed certificate validity details.

Once you upload the metadata file, the validity of the certificate is automatically renewed. You will have to monitor this information at intervals to ensure that the certificates remain valid at all times.

How can the identity provider obtain renewed certificates from the service provider?

The identity provider can submit a service request to the service provider asking for the renewed signing and encryption certificates.

How can I disable Single Sign-On when I am not signed in to the application?

You must request access to the Administration Activity page using the URL provided to the administrators.

Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINSTER_SECURITY_PRIV

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

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

Click the URL and you're directed to a secure Administrator Activity page. Select the **Disable Single Sign On** option and click **Submit**. You receive a confirmation that single sign-on is disabled. Immediately, you're redirected to the Oracle Applications Cloud page where you can sign in using your registered user name and password.

How can I disable Single Sign-On when I am locked out of the application?

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

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

Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Single Sign-On Disabled Confirmation Template

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

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

- When an administrator requests access to the Administration Activity page to disable single sign-on
- When the single sign-on functionality is disabled using the Administration Activity page, notification is sent to that user who disabled SSO.
- When the external identity provider's signing certificate is about to expire
- When the service provider's signing certificate is about to expire
- When the service provider's encryption certificate is about to expire
- To receive notifications, users must be assigned the Administer SSO (ASE_ADMINISTER_SSO_PRIV) privilege. To make sure that recipients don't miss the notifications, they're sent thrice:
    - First notification: 60 days before the expiry date
    - Second notification: 30 days before the expiry date
    - Last notification: 10 days before the expiry date

In the environments that have upgraded to the OCI IAM identity domain, the IdP/SP SSO signing certificate expiry warning notifications are managed by the OCI IAM identity domain. For more information, see *About Email Notifications*.

How do I reimport Identity Provider metadata?

Whenever you get an updated metadata file from the Identity Provider you must reimport the file into the application to continue using SSO configuration.

1. On the Identity Provider Details page, click **Edit**.
2. Import the identity provider metadata:
    - If it's an XML file, click **Browse** and select it.
    - If it's available on a web page, select the **External URL** check box and enter the URL.

    > **Note:** The metadata XML file must be Base64 encoded.
3. Click **Save and Close**.

> **Note:** Remember to test the Identity Provider after reimport.

5 API Authentication

Configure Outbound API Authentication Using JWT Custom Claims

A system account is an account used for integrating Oracle Applications Cloud with third-party applications. This account isn't associated with a user but it must have roles with access to REST APIs.

System account uses basic authentication to authenticate users even if single sign-on is enabled. Security Console's password policy applies to a system account and so the password of this account expires based on the password policy.

Critical tasks such as batch operations or data synchronizations must continue without any interruption or the need to re-authenticate at intervals. To support such tasks, you need to define custom parameters for authentication. Using Security Console, you can define a JSON Web Token (JWT) that can be used by REST APIs to automate system authentication without you having to authenticate manually.

JWT is an access token that contains custom claim name and claim values. Custom claims are name and value pairs that you can define in a JWT. To uniquely identify a user, you can add the user's email address to the token along with the standard user name and password.

Example, suppose you want to integrate Oracle Applications Cloud with a third-party application. This integration uses the JWT Custom Claims to authenticate the users who sign into Oracle Applications Cloud to access the third-party application.

Do these steps to define a JWT that will be used for integration with third-party application:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**, **Edit**.
3. Enter a name and description for the external client application that you want to create.
4. In the **Select Client Type** drop-down list, select **JWT Custom Claims** and click **Save and Close**.
5. Click the JWT Custom Claims Details tab and click **Edit**.
6. In the Token Settings section, if required, update the **Token Expiration Time** and **Signing Algorithm**. Default values are 30 minutes and RS256 respectively.
7. Click **Save**.
8. In the JWT Custom Claims section, click **Add**. You can either select a name from the predefined values in the drop-down list or select **Other** and enter a name of your choice.
9. Select a value for the custom claim. If you select **Free-form**, enter the value in the following text box. You can add more JWT custom claims using the **Add** button.
10. Click **Save**. You can add more parameters as required.
11. Click **Done** to return to the JWT Custom Claims Details page.

    You can view the token created for authentication using the **View JWT** button on the JWT Custom Claims Details page. The View JWT window displays the header and payload of the JWT.
12. Click **Done** again to return to the API Authentication page. You can view the newly created JWT Custom Claim in this page.

You can delete a JWT custom claim on the API Authentication page.

Configure Outbound API Authentication Using Three Legged OAuth Authorization Protocol

OAuth is an open industry standard protocol that allows applications access information from other third-party applications, on behalf of the users. The OAuth authorization protocol manages access securely without revealing any passwords to the client application, such as Oracle Applications Cloud.

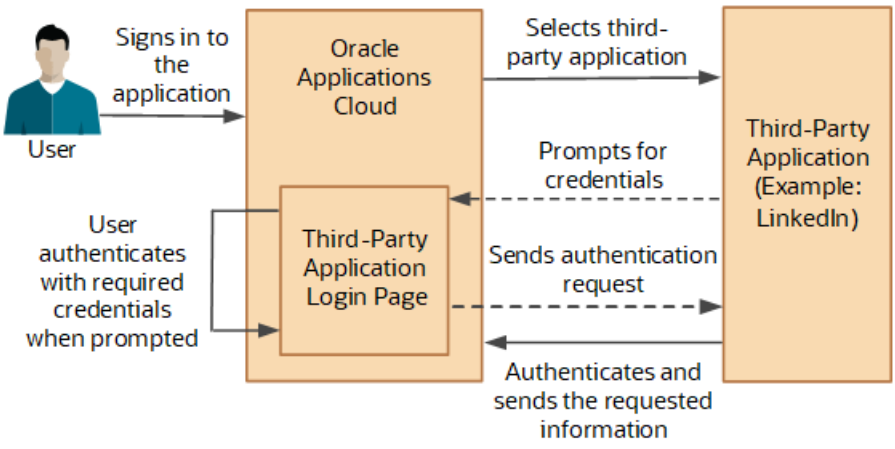
To understand the OAuth authorization protocol, let's take the example of a LinkedIn user who wants to access profile information from LinkedIn and display it in Oracle Applications Cloud. When Oracle Applications Cloud prompts for LinkedIn credentials, the user authenticates and provides the required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

As you notice, there are three parties involved in the entire authentication process: Oracle Applications Cloud, the user who owns information on LinkedIn, and LinkedIn's authorization server. This authorization protocol always requires three such parties for the authentication to complete. Therefore, this protocol is called three-legged OAuth authorization protocol.

Here's the sequential representation of the end-to-end authorization process between Oracle Applications Cloud and the LinkedIn server:

1. Oracle Applications Cloud registers the Client ID and Client Secret and other settings required for authorization.
2. When an Oracle Applications Cloud user wants to access profile information, the LinkedIn login page appears, where the user authenticates using the required credentials.
3. On successful authentication, LinkedIn's authorization server sends an authorization code to Oracle Applications Cloud.
4. Oracle Applications Cloud receives the authorization code and sends an access token request to LinkedIn. LinkedIn processes the access token request and returns an access token.
5. Oracle Applications Cloud uses the access token to call LinkedIn APIs on behalf of the user to access the required information. At runtime, Oracle Web Services Manager manages the entire authorization process.

The following graphic shows the entire authorization process between Oracle Applications Cloud and the LinkedIn server:



Using the Security Console, you configure the three-legged OAuth authorization settings for Oracle Applications Cloud. Once configured, users can access their information from a third-party application, within Oracle Applications Cloud.

Before you proceed, you must enable a profile option to get the OAuth Three-Legged option on the External Client Applications Details page. See the Related Information section for more information.

Here's how you configure three-legged OAuth authorization:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**.
3. On the External Client Application Details page, click **Edit**.
4. Enter a name and description for the external client application that you want to create.
5. In the **Select Client Type** drop-down list, select **OAuth Three-Legged**.
6. Click **Save and Close** to return to the External Client Application Details page.
7. Click the OAuth Details tab.
8. On the Three-Legged OAuth Details page, click **Edit**.
9. Enter the appropriate values in the following required fields:
    - Authorization URL - The authorization code link that the authorization server sends to the application.
    - Redirect URL - The page to which the user is redirected to after successful authorization of application.
    - Access Token URL - The access token that's sent from the authorization server to the application.
    - Servlet Application URL - The access token that's sent from the authorization server to the application.
    - Client ID - The access token that's sent from the authorization server to the application.
    - Client Secret - The access token that's sent from the authorization server to the application.
    - Client Scope - The access token that's sent from the authorization server to the application.
10. Enter the appropriate values in the following optional fields, if required:
    - Server Scope - The access token that's sent from the authorization server to the application.
    - Federated Client Token - The access token that's sent from the authorization server to the application.
    - Include Client Credential - The access token that's sent from the authorization server to the application.
    - Client Credential Type - The access token that's sent from the authorization server to the application.
11. Click **Save and Close**.
12. Click **Done** to return to the Three-Legged OAuth Details page.
13. Click **Done** again to return to the API Authentication page. You can view the newly created three-legged OAuth configuration here.

Related Topics

- Enable OAuth Three-Legged Authentication for Creating External Client Application

Enable OAuth Three-Legged Authentication for Creating External Client Application

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

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

Here are the steps:

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

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

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

Configure Inbound Authentication

Third-party application users can access a service of Oracle Applications Cloud if inbound authentication is configured for them. You can use an Oracle API Authentication Provider to configure inbound authentication for such users.

To configure inbound authentication, you need a public certificate and a trusted issuer which contains the tokens.

Oracle Applications Cloud supports the JSON Web Token (JWT), Security Assertion Markup Language (SAML), and Security Token Service (STS) tokens. Use the Security Console to configure the trusted issuer and public certificate details. The default trusted issuer is Oracle (www.oracle.com) and you can't delete it.

We recommend that you use JWT for inbound authentication for a system account that's created for a specific application. For authentication, JWT uses a combination of a public certificate and trusted issuer whereas a system account's password expires soon based on the security policy. In addition, you must ensure that the system account's credentials are valid.

> **Note:** For more information about how to configure a JWT for inbound authentication, see Configure JWT Authentication Provider in the Related Topics section.

How Inbound Authentication Works

When a third-party application user sends an authentication request to access a service of Oracle Applications Cloud, these actions occur in the background:

1. The third-party application generates a JWT that includes trusted issuer and public certificate information.
2. Oracle Web Services Manager authenticates the generated JWT by verifying whether the trusted issuer and public certificate are valid.
3. On successful authentication, the third-party application gets access to the Oracle Applications Cloud service.

Here's how you configure an Oracle API Authentication Provider for inbound authentication:

1. On the Security Console, click **API Authentication**.
2. Click **Create Oracle API Authentication Provider**.
3. On the Oracle API Authentication Provider Details page, click **Edit**.
4. On the API Authentication Configuration Details page, enter a name for the **Trusted Issuer**. Ensure that the name of Trusted Issuer matches the value of ISS in the JWT token.
5. Select one or more token types that you want to include in the trusted issuer.
6. Click **Save and Close**.
7. On the Oracle API Authentication Provider Details page, click the Inbound API Authentication Public Certificates tab and click **Edit**. You can use the default Oracle public certificate or add a new one.
8. On the Inbound API Authentication Public Certificates page, click **Add New Certificate** to add a different public certificate.
9. Enter the **Certificate Alias** name

10. Click **Browse** and select the public certificate that you want to import.

    Note: If the public certificate includes a certificate chain then import the complete chain.

11. Click **Save**. The newly added certificate alias is displayed on the Inbound API Authentication Public Certificates page.
12. Click **Done** to return to the API Authentication page.

Related Topics

- Configure JWT Authentication Provider
- Reset User Password
- Use JSON Web Token for Authorization

Is there a recommended format for the public certificate?

Yes. Oracle recommends that the public certificate you upload must contain only line feed (denoted by the code \n) to indicate separation of lines. Because carriage return isn't supported, make sure that the certificate doesn't contain carriage return along with the line feeds.

6 Export and Import of Security Setup Data

Overview of Security Data Import and Export

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

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

Related Topics

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

Export and Import of Security Console Data

You can move the Security Console setup data from one environment to another using the CSV file export and import functionality.

Let's assume you have spent lot of time and effort in configuring and setting up the Security Console in your primary environment. You test the setup and find that everything's working as intended. You can now quickly replicate the same setup in another environment by exporting the setup data and then importing it into the other environment.

Export and Import the Data

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

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

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

What Gets Exported and Imported

The Security Console setup data consists of information that you see on the Administration and User Categories tabs of the Security Console. The following business objects help in packaging those details into CSV files so that the data can be easily exported and imported.

- Security Console Administration Settings
- Security Console User Category
- Security Console User Category Notifications

Note: Lists of users or information about any specific user is never a part of this export and import process.

In this table, you will find information about the contents of each business object.

Business Object	Information Included in Export and Import
Security Console Administration Settings	• General administration details • Role preferences • Location-based access settings **Note:** If location-based access isn't enabled (if the tab doesn't appear on the Security Console), nothing gets included in the export or import.
Security Console User Category	• User category details • Password policy information
Security Console User Category Notifications	Notification preferences. **Note:** For notifications, only the custom template information is exported from the default user category. The predefined notifications are excluded because they're available in the target environment.

When the export process successfully completes, you get the following CSV files:

- Administration Settings CSV
- User Category CSV
- User Category Notifications CSV

Note: If there are language packs installed on your application, additional CSV files may be generated containing the translated data.

To import data into another environment, bundle these files into a .zip file to create the CSV file package and follow the process for importing setup data.

Related Topics

- Export and Import CSV File Packages
- Key Information About Setup Data Export and Import Processes

Export and Import of Custom Roles, Role Hierarchies, and Role-to-Privilege Assignments

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

Export and Import the Data

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

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

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

What Gets Exported and Imported

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

- Functional Security Custom Roles

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

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

Business Object	Information Included in Export and Import
Functional Security Custom Roles	The custom role includes the following details: • Role Code • Role Name • Role Description • Role Category • All IP Address Access. Indicates that a role is granted access to the Security Control irrespective of the IP address from where it's signed in. **Note:** The scope is limited to User Assignable roles only.
Functional Security Custom Role Hierarchy	The role hierarchy includes the following details: • Parent Role • Member Role • Add or Remove Role Membership
Functional Security Custom Role Privilege Membership	The role privilege membership includes the following details: • Parent Role • Member Privilege • Add or Remove Privilege Membership

What's Not Included

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

Related Topics

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

7 User and Role Reports

User and Role Access Audit Report

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

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

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

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

User and Role Access Audit Report Parameters

Population Type

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

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

User Name

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

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

Role Name

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

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

From User Name Starting With

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

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

To User Name Starting With

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

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

User Role Name Starts With

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

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

Data Security Policies

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

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

Debug

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

Viewing the Report Results

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

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

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

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

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

Report Type	File Suffix	File Format	File Contents
Any	DataSec	CSV	Data security policies. The .zip file contains one file for all users or

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

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

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

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

User Role Membership Report

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

To run the report process:

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

User Role Membership Report Parameters

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

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

User Name Begins With

Enter one or more characters of the user name.

First Name Begins With

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

Last Name Begins With

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

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Viewing the Report

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

The following table lists a brief description of these columns:

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

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

User Password Changes Audit Report

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

To run the User Password Changes Audit Report:

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

User Password Changes Audit Report Parameters

Search Type

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

User Name

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

User Name Pattern

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

Start Date

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

To Date

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

Sort By

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

Viewing the Report Results

The report produces these files:

- **UserPasswordUpdateReport.csv**
- **UserPasswordUpdateReport.xml**

- **Diagnostics_[process ID].log**

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

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

Inactive Users Report

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

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

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

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

Inactive Users Report Parameters

All parameters except Days Since Last Activity are optional.

User Name Begins With

Enter one or more characters.

First Name Begins With

Enter one or more characters.

Last Name Begins With

Enter one or more characters.

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Days Since Last Activity

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

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

Last Activity Start Date

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

Last Activity End Date

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

Viewing the Report

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

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

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

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

Related Topics

- Schedule the Import User Login History Process

User History Report

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

To run the report, you must inherit the ORA_PER_MANAGE_USER_AND_ROLES_DUTY_OBI (Manage Users) duty role. Several predefined job roles, including IT Security Manager, inherit this duty role.

Follow these steps to run the report.

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

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

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

This report is identical to the HCM Person User Information report, which authorized users can run in the HCM Reports and Analytics work area. Information is provided in this report for sales resources who are also defined as users in HCM.

Report Contents

For the selected user, the report includes:

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

8 Review and Analyze Roles on the Security Console

Overview of Reviewing Roles

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

You can perform these tasks from the Roles tab:

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

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

From the Analytics tab, you can perform these tasks:

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

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

Graphical and Tabular Role Visualizations

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

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

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

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

The Tabular View

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

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

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

The Graphical View

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

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

In the Control Panel, you can:

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

Review Role Hierarchies

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

To review a role's hierarchy:

1. On the Roles tab of the Security Console, ensure that **Expand Toward** is set to **Privileges**.
2. Search for and select the role.

   Depending on the enterprise setting, either a table or a graphical representation of the role is displayed.
3. If the table doesn't appear by default, click the **View as Table** icon.

   The table lists every role inherited either directly or indirectly by the selected role. To view the privileges inherited by the role, set the **Show** field to **Privileges**.

   > **Tip:** Enter text in a column search field and press **Enter** to show only those roles or privileges that contain the specified text.
4. Click **Export to Excel** to export the current table data to Microsoft Excel.

Simulate Navigator Menus

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

Simulate the Navigator for a Role

Follow these steps:

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

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

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

View Roles That Grant Access to a Navigator Entry

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

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

View Privileges Required for Menu

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

- The Navigator entry
- Tasks in the associated work area

Follow these steps:

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

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

Simulate the Navigator for a User

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

Review Role Assignments

You can use the Security Console to either view the roles assigned to a user, or to identify the users who have a specific role.

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

View the Roles Assigned to a User

Follow these steps:

1. Open the Security Console.
2. On the Roles tab, search for and select the user.

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

    a. Select the role and right-click.
    b. Select **Expand**. Repeat these steps as required to move down the hierarchy.

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

Identify Users Who Have a Specific Role

Follow these steps:

1. On the Roles tab of the Security Console, search for and select the role.
2. Depending on the enterprise setting, either a table or a graphical representation of the role hierarchy appears. Switch to the graphical representation if it doesn't appear by default.
3. Set **Expand Toward** to **Users**.

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

   In the refreshed graph, user names appear on hover. Users may inherit roles either directly or indirectly from other roles. Expand a role to view its hierarchy.
4. In the Legend, click the **Tabular View** icon for the **User** icon. The table lists all users who have the role. You can export this information to Microsoft Excel.

Compare Roles

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

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

Selecting Roles for Comparison

1. Select the Roles tab in the Security Console.
2. Do any of the following:
   - Click the **Compare Roles** button.
   - Create a visualization graph, right-click one of its roles, and select the **Compare Roles** option.
   - Generate a list of roles in the Search Results column of the Roles page. Select one of them, and click its menu icon. In the menu, select **Compare Roles**.
3. Select roles for comparison:
   - If you began by clicking the **Compare Roles** button, select roles in both **First Role** and **Second Role** fields.
   - If you began by selecting a role in a visualization graph or the Search Results column, the **First Role** field displays the name of the role you selected. Select another role in the **Second Role** field.

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

Comparing Roles

1. Select two roles for comparison.
2. Use the **Filter Criteria** field to filter for any combination of these artifacts in the two roles:
    - Function security policies
    - Data security policies
    - Inherited roles
3. Use the **Show** field to determine whether the comparison returns:
    - All artifacts existing in each role
    - Those that exist only in one role, or only in the other role
    - Those that exist only in both roles
4. Click the **Compare** button.

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

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

Adding Policies to a Role

1. Select two roles for comparison.
    - As the **First Role**, select a role in which policies already exist.
    - As the **Second Role**, select the role to which you're adding the policies. This must be a custom role. You can't modify a predefined role.
2. Ensure that your selection in the Filter Criteria field excludes the **Inherited roles** option. You may select **Data security policies**, **Function security policies**, or both.
3. As a Show value, select **Only in first role**.
4. Click the **Compare** button.
5. Among the artifacts returned by the comparison, select those you want to copy.
6. An **Add to Second Role** option becomes active. Select it.

Compare Users

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

Users with the following privileges can compare users:

- Create User Account (ASE_CREATE_USER_ACCOUNT_PRIV)

- Edit User Account (ASE_EDIT_USER_ACCOUNT_PRIV)
- View User Account (ASE_VIEW_USER_ACCOUNT_PRIV)
- Delete User Account (ASE_DELETE_USER_ACCOUNT_PRIV)
- Lock and Unlock User Account (ASE_LOCK_UNLOCK_USER_PRIV)
- Update Password for User Account (ASE_UPDATE_PASSWORD_FOR_USER_PRIV)

On the User Accounts page, you can compare users in two different ways:

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

Follow these steps:

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

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

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

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

Copy Roles from One User to Another

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

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

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

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

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

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

Using the Copy User Option

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

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

Using the Add Role Button

1. On the Security Console, click **Users**.
2. On the User Accounts page, click **Add User Account**.
3. On the Add User Account page, select a user category and enter the details of the user.
4. Click **Add Role**.
5. Select **Users** from the **Search** drop-down list and search for the user from which you want to copy the roles.
6. Select the user and click **Add Role Membership from User**. A confirmation message appears.
7. Click **OK** and click **Done**.
8. Click **Save and Close**.

Related Topics

- Role Copying or Editing

Analytics for Roles

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

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

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

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

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

  In addition, a Roles by Category pie chart compares the number of roles in each category with those in other categories.
- Roles in Category. Click a category in the Role Categories grid to list roles belonging to that category. For each role, the Roles in Category grid also shows the number of:

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

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

Analytics for Data Resources

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

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

   Results are presented in three tables.

Data Security Policies

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

Each row documents a policy, specifying by default:

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

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

Authorized Roles

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

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

By default, each row specifies the following:

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

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

Authorized Users

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

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

Manipulating the Results

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

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

View Role Information Using Security Dashboard

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

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

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

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

Here are the steps to view the Security Dashboard:

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

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

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

9 Create and Edit Job, Abstract, and Duty Roles

Overview of Security Configuration

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

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

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

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

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

Related Topics

- Overview of Data Security Configuration

Guidelines for Copying Roles

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

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

Role-Copy Options

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

- Copying the Top Role

  If you select the **Copy top role** option, you copy only the role you have selected. The source role has links to roles in its hierarchy, and the copy inherits links to the original versions of those roles. Subsequent changes to the inherited roles affect not only the source top role, but also your copy. The result of selecting the Copy top role option, therefore, is as follows:

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

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

- Copying the Top Role and Inherited Roles

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

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

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

Reviewing the Role Hierarchy

When you copy a predefined job, abstract or duty role, it's recommended that you first review the role hierarchy to identify any inherited roles that you want to either copy, add, or delete in your custom role. You can review the role hierarchy on the Roles tab of the Security Console in either graphical or tabular format. You can also:

- Export the role hierarchy to a spreadsheet from the Roles tab.
- Review the role hierarchy and export it to a spreadsheet from the Analytics tab.
- Run the User and Role Access Audit Report.

Job and abstract roles inherit function security privileges and data security policies from the roles that they inherit. Function security privileges and data security policies may also be granted directly to a job or abstract role. Review these directly granted privileges on the Roles tab of the Security Console, as follows

- In the graphical view of a role, its inherited roles and function security privileges are visible at the same time.

- In the tabular view, you set the **Show** value to switch between roles and function security privileges. You can export either view to a spreadsheet.

Once your custom role exists, edit it to add or remove directly granted function security privileges.

> **Note:** Data security policies are visible only when you edit your role; they don't display in the graphical or tabular role views. However, you can view the data security policies assigned to a role from the Analytics tab of the Security Console.

Naming Copied Roles

By default, a copied role has the same name as its source role with the suffix **Custom**. The role codes of copied roles have the suffix **_CUSTOM**. Copied roles lose the prefix **ORA_** automatically from their role codes. You can define a local naming convention for custom roles, with a prefix, suffix, or both, on the Roles subtab of the Security Console Administration tab.

> **Note:** Copied roles take their naming pattern from the default values specified on the Roles subtab of the Security Console Administration tab. You can override this pattern on the Copy Role: Basic Information page for the role that you're copying. However, the names of roles inherited by the copied role are unaffected. For example, if you perform a deep copy of the Employee role, then duty roles inherited by that role take their naming pattern from the default values.

If any role in the hierarchy already exists when you copy a role, then no copy of that role is made. For example, if you make a second copy of the Employee role, then copies of the inherited duty roles might already exist. In this case, the copied role inherits links to the existing **copies** of the roles. To create unique copies of inherited roles, you must enter unique values on the Administration tab of the Security Console before you perform a deep copy. To retain links to the predefined job or abstract role hierarchy, perform a shallow copy of the predefined role.

Copying Roles and Access Groups

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

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

Report and Analytics Roles

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

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

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

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

Related Topics

- Role Preferences

Copy Job or Abstract Roles

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

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

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

Copy a Role

To copy a job or abstract role:

1. On the Roles tab of the Security Console, search for the role to copy.
2. Select the role in the search results. The role hierarchy appears in tabular format by default.

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

3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, review and edit the **Role Name**, **Role Code**, **Description,** and **Enable Role for Access from All IP Addresses** values, as appropriate. **Enable Role for Access from All IP Addresses** appears only if location-based access is enabled.

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

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

Related Topics

- Guidelines for Copying Roles
- Guidance for Assigning Predefined Roles

Edit Your Custom Job or Abstract Roles

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

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

Edit the Role

To edit a job or abstract role:

1. On the Roles tab of the Security Console, search for and select your custom role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code. If location-based access is enabled, then you can also manage the Enable Role for Access from All IP Addresses option (see *Overview of Location-Based Access*).
4. Click **Next**.

Manage Functional Security Privileges

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

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

To add a privilege to the copied role:

1. Click **Add Function Security Policy**.
2. In the Add Function Security Policy dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from the role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Function Security Policy** dialog box.
   All the privileges you selected are listed on the Edit Role: Function Security Policies page.
7. Click **Next**.

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

Manage Data Security Privileges

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

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

Add or Remove Inherited Roles

The Edit Role: Role Hierarchy page shows the copied role and its inherited duty roles. You can add or remove roles.

To remove a role:

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

To add a role:

1. Click the **Add Role** icon.
2. In the **Add Role Membership** dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the **Add Role Membership** dialog box.

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

Assign a Role to Users

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

To remove user access to a role:

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

To add user access to a role:

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

Review a Role

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

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

The role is available immediately.

Related Topics

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

Create Job and Abstract Roles

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

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

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

Enter Basic Information

Follow these steps:

1. On the Roles tab of the Security Console, click **Create Role**.
2. On the Create Role: Basic Information page, enter the role's display name in the **Role Name** field. For example, enter **Digital Sales Manager**.
3. Enter a unique **Role Code**. For example, enter DIGITAL_SALES_MGR_JOB.
   Abstract roles have the suffix **_ABSTRACT**, and job roles have the suffix **_JOB**.
4. In the **Role Category** field, select the appropriate role category, for example, **CRM - Job Roles**.
5. If you're using location-based access, then you see the **Enable Role for Access from All IP Addresses** option. If you select this option, users who have the role can access the tasks that the role secures from any IP address.
6. Click **Next**.

Add Functional Security Policies

When you create a role from scratch, you're most likely to add one or more duty roles to your role. You're less likely to grant function security privileges directly to the role. If you're not granting function security privileges, then click **Next**. Otherwise, to grant function security privileges to the role:

1. On the Create Role: Functional Security Policies page, click **Add Function Security Policy**.
2. In the **Add Function Security Policy** dialog box, search for and select a privilege or role.
   You can either add an individual privilege or copy all the privileges that belong to an existing role.
3. If you select a role, then click **Add Selected Privileges** to add all the function security privileges assigned to the selected role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Function Security Policy** dialog box.
   All the privileges you added are listed on the Create Role: Functional Security Policies page. You can:
   - Click on a privilege to view details of the code resource that it secures.

- Delete any privilege by selecting the privilege and clicking the Delete icon.

7. Click **Next**.

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

Add Data Security Policies

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

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

Build the Role Hierarchy

The Create Role: Role Hierarchy page shows the hierarchy of your custom role in tabular format by default. You can add one or more job, abstract, and duty roles to the new role. Typically, when creating a job or abstract role you add duty roles. Roles are always added directly to the role that you're creating.

To add a role:

1. Click the **Add Role** icon.
2. In the **Add Role Membership** dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the **Add Role Membership** dialog box.

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

Assign the Role to Users

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

To assign the role to a user:

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

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

Review the Role

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

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

Your custom role is available immediately on the Security Console.

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

Related Topics

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

Copy and Edit Duty Roles

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

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

Copy a Duty Role

To copy a duty role:

1. On the Roles tab of the Security Console, search for the duty role to copy.
2. Select the role in the search results.

   The role is displayed in tabular format by default. Click the Show Graph icon to show the hierarchy in graphical format.
3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
   - If you select **Copy top role**, then only the selected role is copied. The copied role inherits the same role instances as the source role.
   - If you select **Copy top role and inherited roles**, then a copy is made of every role in the role hierarchy provided that a copy of the role with the same name doesn't already exist.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

   > **Tip:** The **Role Name** and **Role Code** values are assigned the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. The prefix **ORA_** is also removed from the role code. You can overwrite the default prefix and suffix for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make here.

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

Edit the Copied Duty Role

To edit the copied role, perform the following steps:

1. On the Roles tab of the Security Console, search for and select your copy of the duty role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.
4. Click **Next**.

Manage Functional Security Policies

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

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

To add a privilege to the role:

1. Click **Add Function Security Policy**.
2. In the **Add Function Security Policy** dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privilege** to grant all function security privileges from the role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Function Security Policy** dialog box.

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

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

Manage Data Security Policies

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

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

Add and Remove Inherited Roles

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

To remove a role:

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

To add a role:

1. Click **Add Role**.
2. In the **Add Role Membership** dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the **Add Role Membership** dialog box.

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

View Users Assigned the Role

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

Review the Role

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

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

The role is available immediately.

Related Topics

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

Create a Custom Role with Limited Access

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

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

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

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

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

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

Related Topics

- View Locked Users and Unlock Users
- Reset Passwords

10 Access Groups

Use Access Groups to Secure Data

For information on using access groups to secure data to your Oracle CX applications, see the *How do I create and manage security access groups in CX?* playbook on the *Playbooks* page in the *Oracle Sales Help Center*.