

Oracle Life Sciences Identity and Access Management Service Administrator Guide



Release 26.2
G59814-01
September 2026

ORACLE®

Oracle Life Sciences Identity and Access Management Service Administrator Guide, Release 26.2

G59814-01

Copyright © 2026, Oracle and/or its affiliates.

Contents

1	About this guide	
	Federation guidelines	1
2	Choose the password reset flow	
3	Create a user account	
4	Assign roles	
	Assign one or more roles to the same user	1
	Assign the same role to multiple users	2
	Assign multiple roles to multiple users	2
	Role FAQs	2
	What application roles do I need to assign to users?	3
	How do I know if an Oracle Life Sciences application delegates role administration to Oracle Life Sciences IAMS?	3
	How do you assign application roles if the application does not delegate role management to Oracle Life Sciences IAMS?	3
	What are the different types of users in Oracle Life Sciences IAMS and the roles assigned to them?	3
	What roles do I need to assign to users of Oracle Health Sciences My Oracle Bookmarks?	4
5	Update user accounts	
	View or edit user details	1
	Update a user's name, email address, or user login	2
	Reset a user's password	2
	Remove roles	3
	Lock an account	4
	Unlock an account	4
	Terminate or reinstate an account	5

6	Role settings	
	Navigate to the Roles page	1
	Set the unauthorized access page for an application or study	1
	Set up approval for a role	2
	Request and assign the Approver role	3
	Activate approval for a role	3
	Deactivate approval	4
	Approve or reject access requests	4
	Set up self-service registration	6
	Activate self-service registration	6
	Deactivate self-service registration	7
	Grant external access to company applications or studies	7
	Allow another organization to view and assign one of your organization's roles	7
	View and remove external member access to a role	8
7	Perform user operations in bulk	
	Use Bulk Import	1
	Get the template	1
	Add operations to the template	2
	Check for errors	2
	Import data	3
	Review and reuse previous import files	4
8	Access customized reports	
	Request customized reports	1

1

About this guide

This guide provides instructions for organization-wide delegated administrators to manage user accounts and user access to your Oracle Life Sciences applications and studies hosted in Global Business Unit Cloud Services (GBUCS).

The operations described in this guide are performed from an organization-specific instance of the Oracle Identity Self Service console.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may see different navigation or page labels. If the navigation in a task does not match your environment, use the equivalent page or action in your current console.

You can manage users and privileges for your hosted Oracle Life Sciences products, except Oracle Life Sciences InForm. Oracle InForm administrators create and manage user accounts in Oracle Life Sciences User Management Tool.

- [Federation guidelines](#)

Federation guidelines

Keep the following guidelines in mind when using a federated account with Oracle Life Sciences IAMS.

Federation account linking

Some Oracle Life Sciences products, such as Oracle InForm, support federation with third-party identity providers, such as Exostar. To use federation, you must link your identity provider account with your Oracle Life Sciences IAMS account. For specific information on how to use federation with your product, see your product documentation.

Oracle Life Sciences IAMS supports Security Assertion Markup Language (SAML) federation between a customer identity provider (IDP) and Identity Cloud Service (IDCS) for use in Oracle Clinical One Platform.

Access control

- If you cannot access Oracle Life Sciences Cloud using your identity provider, you can sign in to Oracle systems directly using your Oracle Life Sciences SSO credentials.
- User accounts created through Oracle IDCS continue to receive Oracle Life Sciences IAMS new account and password expiration notification emails. Contact your Oracle Services lead to disable these notification emails.

Session security

- When signing out of Oracle Life Sciences Cloud, close your browser to ensure all sign-in sessions end. You may be signed in to Oracle in multiple browser windows or tabs. Signing

out in one browser window does not sign you out of all browser windows. Closing all open browsers ensures all sign-in sessions end.

- Your Oracle Life Sciences IAMS session can time out while your identity provider session is still active. Your system-wide session timeout is defined by your identity provider.
- The re-authentication period for your Oracle Life Sciences SSO session may be extended when you have an active identity provider session. Because the identity provider re-authentication time exceeds the Oracle Life Sciences IAMS time limit, someone may be able to sign in again on your computer without re-entering your sign-in credentials even after the Oracle Life Sciences IAMS timeout period. Your authentication period is extended to the authentication period defined by your identity provider when an identity provider session is in use. You can avoid this extension by closing your browser after signing out.

Electronic signatures

If you have signed in to Oracle Life Sciences Cloud using your identity provider credentials, the system requires you to re-authenticate using those same credentials for electronic signature.

When users are authenticated through federation with Oracle Identity Cloud Service (IDCS), they can eSign a document in an application using IDCS credentials.

2

Choose the password reset flow

You can choose how users in your organization reset their account passwords.

Note

After you switch to the **Email Link** flow, you cannot switch back to the **Security Questions** flow in Oracle Identity Self Service. To switch back, contact Oracle Life Sciences Support. You can switch back only if no users were created after the switch to the **Email Link** flow.

1. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

2. Select the **Users** tile.
3. Under the User Settings heading, select one of the following:
 - **Email Link:** When a new user is created or when a user selects **Trouble Signing In** on the Sign In page, the user receives an email with a link to set the account password.
 - **Security Questions:** When a new user is created or when a user selects **Trouble Signing In** on the Sign In page, the user receives an email containing the account password.
4. Select **Yes** on the Confirmation screen.

Note

Customers who move to the updated Oracle Identity Self Service console can use an email confirmation code for password reset. To enable this option, contact Oracle Life Sciences Support.

3

Create a user account

Create user accounts for users who need access to Oracle Life Sciences applications.

✓ Tip

If you need to create or update multiple accounts, it may be easier to use Bulk Import. See [Perform user operations in bulk](#) for details.

1. In the upper-right corner, select **Manage**.

📘 Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

2. Select the **Users** tile.
3. Under the Search Results heading, select **Create**.
4. Complete the fields with the new user's information. Required fields are marked with an asterisk (*).

📘 Note

Besides letters and numbers, a user's login can only contain the following special characters: hyphens (-), underscores (_), and dots (.).

✓ Tip

In the **Organization** field, enter your ShortOrgId.
If you don't know your ShortOrgId:

- a. Select the search icon  next to the Organization field.
- b. Select **Search** to do a blank search.
- c. In the Search Results, select the row where Company appears in the Type column.
- d. Select **Select**.

 Tip

If you specify an email address, you do not need to fill in the password fields. The user receives an email with instructions to set the account password.

5. Select **Submit** in the upper-right corner of the page.

A confirmation message appears and you are redirected to the User Details page for the new user.

6. Assign roles to the user, as appropriate. For instructions, see [Assign roles](#).

4

Assign roles

Assign roles to users to grant them access to applications or studies and, if available, to grant privileges in the target application.

- [Assign one or more roles to the same user](#)
Use these instructions when you created a new user and you need to assign roles to that user, or when you need to assign an additional role to an existing user.
- [Assign the same role to multiple users](#)
If you need to grant access to a broad group of users, you can allow users to request access themselves using self-service registration. This method is useful when, for example, your organization has acquired a new Oracle Life Sciences application or opened a new study.
- [Assign multiple roles to multiple users](#)
You can use Bulk Import to submit multiple user operations at the same time, including creating or terminating users, or assigning and removing roles.
- [Role FAQs](#)

Assign one or more roles to the same user

Use these instructions when you created a new user and you need to assign roles to that user, or when you need to assign an additional role to an existing user.

To assign roles to a user:

1. Navigate to the User Details page for the user.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Users** tile.
 - c. For the **Display Name**:
 - From the list, select **Equals**.
 - Enter the username in the field.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **User Login** column to open the User Details page.
2. Select the **Roles** tab.
 3. From the **Actions** list, select **Request**.

The Catalog page opens.

4. For each role you want to assign:
 - a. Enter the role name in the search box and press **Enter** or select  to search. See the [Role FAQs](#) for help.
 - b. In the search results, select the role you want to assign.
 - c. Select **Add to cart** at the right end of the row.
5. Select **Checkout** in the upper-right corner of the page.
6. Review the roles in the cart. To exclude a role from the cart, select **Remove** to the right of the role.
7. Select **Submit** in the upper-right corner. If approval is active for any of the roles, the Request Summary page opens and a confirmation message appears at the top of the screen. The role is assigned after the corresponding request is approved.

If approval is inactive for the selected roles, the Catalog page opens and a confirmation message appears at the top of the screen.

Assign the same role to multiple users

If you need to grant access to a broad group of users, you can allow users to request access themselves using self-service registration. This method is useful when, for example, your organization has acquired a new Oracle Life Sciences application or opened a new study.

For details, see [Set up self-service registration](#).

Assign multiple roles to multiple users

You can use Bulk Import to submit multiple user operations at the same time, including creating or terminating users, or assigning and removing roles.

See [Perform user operations in bulk](#) for details.

Role FAQs

- [What application roles do I need to assign to users?](#)
Every user needs the basic role that is associated with the Oracle Life Sciences application they need to work in. The role name includes your company ShortOrgId, in the format *ShortOrgId.basic_role*.
- [How do I know if an Oracle Life Sciences application delegates role administration to Oracle Life Sciences IAMS?](#)
See the documentation for the application for details.
- [How do you assign application roles if the application does not delegate role management to Oracle Life Sciences IAMS?](#)
For such cases, you assign application roles from the application itself.
- [What are the different types of users in Oracle Life Sciences IAMS and the roles assigned to them?](#)
These roles are specific to Oracle Life Sciences IAMS and control privileges that users have in the Oracle Life Sciences IAMS application.
- [What roles do I need to assign to users of Oracle Health Sciences My Oracle Bookmarks?](#)
If your organization uses Oracle Health Bookmarks, two additional roles are available in Oracle Life Sciences IAMS that control users' privileges in Oracle Health Bookmarks.

What application roles do I need to assign to users?

Every user needs the basic role that is associated with the Oracle Life Sciences application they need to work in. The role name includes your company ShortOrgId, in the format *ShortOrgId.basic_role*.

Additionally, if an Oracle Life Sciences application delegates role management to Oracle Life Sciences IAMS, you must also grant the application roles that users need to work in the application. These role names include your company ShortOrgId and the basic role, in the format *ShortOrgId.basic_role_app_role*. For details about specific application roles, see the documentation for the application.

How do I know if an Oracle Life Sciences application delegates role administration to Oracle Life Sciences IAMS?

See the documentation for the application for details.

How do you assign application roles if the application does not delegate role management to Oracle Life Sciences IAMS?

For such cases, you assign application roles from the application itself.

What are the different types of users in Oracle Life Sciences IAMS and the roles assigned to them?

These roles are specific to Oracle Life Sciences IAMS and control privileges that users have in the Oracle Life Sciences IAMS application.

The following types of users are available in Oracle Life Sciences IAMS:

- Customer Delegated Administrator
- System Administrator
- My Oracle Bookmarks Administrator
- Application End User

Customer Delegated Administrator

As the initial Customer Delegated Administrator (CDA) for your organization, you are assigned the following roles by default:

- **All Users:** Assigned to all users by default. This role lets users access their own record.
- **Role Authorizer:** Lets users grant and revoke business services for users in the organization.
- **Role Viewer:** Lets users view business services, user assignments, and profiles for assigned users in the organization.
- **User administrator:** Lets users create, modify, and terminate users; enable, disable, lock, and unlock users; and grant and revoke business services in the organization.
- **User Viewer:** Lets users view the organization, search for users, and view user profiles.

- **System-admin:** Lets users create OAuth clients. A CDA can assign this role to other users in the organization.

An initial CDA can contact Oracle Life Sciences Support to request an additional CDA in Oracle Life Sciences IAMS. The additional CDA is assigned the same default roles.

The following roles are not assigned to the initial CDA by default. The initial CDA can contact Oracle Life Sciences Support to request these roles:

- **Approver:** Added to your organization on request. This role lets users access the Approval Details page and claim, approve, or reject access requests for roles where approval is active. See [Request and assign the Approver role](#) for details.
- **HelpDesk:** Lets users force a password change and unlock an account that was locked because of too many failed sign-in attempts.

System Administrator

The primary responsibility of a system administrator is to set up OAuth clients. A system administrator cannot manage Oracle Life Sciences IAMS users, but can manage certain aspects of the Oracle Life Sciences IAMS application. System administrators are assigned the following roles:

- **All Users:** Assigned to all users by default. This role lets users access their own record.
- **System-admin:** Lets users create OAuth clients. The CDA is assigned this role by default and can assign it to other users.

My Oracle Bookmarks Administrator

My Oracle Bookmarks administrators are assigned the following roles:

- **All Users:** Assigned to all users by default. This role lets users access their own record.
- **Sponsor admin:** Lets users add descriptions and therapeutic areas, customize My Oracle Bookmarks, and create links to native, non-SSO Oracle InForm trials.

Application End User

Application end users are assigned only the **All Users** role. This role is assigned to all users by default and lets users access their own record.

What roles do I need to assign to users of Oracle Health Sciences My Oracle Bookmarks?

If your organization uses Oracle Health Bookmarks, two additional roles are available in Oracle Life Sciences IAMS that control users' privileges in Oracle Health Bookmarks.

The full role names include the ShortOrgId, in the format *ShortOrgId.FNTD_BIZ_SERVICE_app_role_name*, where *app_role_name* appears only for application roles.

FNTD_BIZ_SERVICE_FD_SP_USER: Assign this application role to users, often sponsor users, who need to see all application tiles, including tiles with Site Access turned off. This role is useful for reporting applications or other tools that are not broadly used within your organization. You can turn Site Access off for these applications and assign this role only to users who need access to them.

FNTD_BIZ_SERVICE_FD_SP_ADMIN: Assign this application role to users, often sponsor administrators, who manage the applications used to conduct clinical trials. Users with this role

can perform high-level maintenance in Oracle Health Bookmarks. They can add or edit the company name, view all application tiles, turn Site Access on or off for application tiles, view the study details page, and add or edit the description, therapeutic area, and program for studies.

For details about Oracle Health Bookmarks, see the *Oracle Life Sciences Identity and Access Management Service Release Notes* on the [Oracle Help Center](#).

5

Update user accounts

You can update user accounts in Oracle Identity Self Service to change user information, assign or remove roles, or to update account status.

- [View or edit user details](#)
- [Update a user's name, email address, or user login](#)
Update a user's name, email address, or user login.
- [Reset a user's password](#)
- [Remove roles](#)
Remove roles that a user no longer needs for access or privileges in an application.
- [Lock an account](#)
When a delegated administrator explicitly locks an account, the user cannot use the **Trouble Signing In** link to regain access. Lock a user account to prevent the user from signing in before you disable the account for termination of employment or for other reasons.
- [Unlock an account](#)
If an account was explicitly locked by a delegated administrator, unlock it before the user can sign in again. Users who lock their accounts after too many incorrect password attempts can use **Trouble Signing In** to reset their passwords.
- [Terminate or reinstate an account](#)
Terminate a user account when the user is no longer employed by your company.

View or edit user details

To find a user in Oracle Identity Self Service so that you can view or edit user details:

1. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

2. Select the **Users** tile.
3. For the **Display Name**:
 - From the list, select **Equals**.
 - Enter the user name in the field.
4. Select **Search**.
5. In the Search Results section, select the link in the **User Login** column to open the User Details page.

User information is grouped under tabs in the User Details page. Select a tab to view or update information.

Update a user's name, email address, or user login

Update a user's name, email address, or user login.

To update the information associated with a user account:

1. Navigate to the User Details page:
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Users** tile.
 - c. For the **Display Name**:
 - From the list, select **Equals**.
 - Enter the user name in the field.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **User Login** column to open the User Details page.
 2. In the upper-left corner, select **Modify**.
 3. Update the following fields as necessary:
 - First Name
 - Last Name
 - Email
 - User Login
 4. Select **Submit** in the upper-right corner.

Reset a user's password

To manually reset the password for a user account:

1. Navigate to the User Details page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Users** tile.
 - c. For the **Display Name**:

- From the list, select **Equals**.
 - Enter the user name in the field.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **User Login** column to open the User Details page.
2. In the row of controls at the top of the page, select **Reset Password**.
 3. Select **Send** on the Confirmation screen.

The user receives an email with instructions to reset the account password. The email content depends on your organization's password reset flow.

Remove roles

Remove roles that a user no longer needs for access or privileges in an application.

To remove roles for a user account:

1. Navigate to the User Details page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Users** tile.
 - c. For the **Display Name**:
 - From the list, select **Equals**.
 - Enter the user name in the field.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **User Login** column to open the User Details page.
2. Select the **Roles** tab.
 3. Select the role you want to remove.
 4. From the **Actions** list, select **Remove**.

The Remove Roles page opens.
 5. Review the roles in the cart. To exclude a role from the cart, select **Remove** to the right of the role.
 6. Select **Submit** in the upper-right corner.

The message *Successfully completed the operation* appears.

Note

If you need to remove delegated administrator roles from this account, contact Oracle Life Sciences Support for assistance.

Lock an account

When a delegated administrator explicitly locks an account, the user cannot use the **Trouble Signing In** link to regain access. Lock a user account to prevent the user from signing in before you disable the account for termination of employment or for other reasons.

1. Navigate to the User Details page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Users** tile.
 - c. For the **Display Name**:
 - From the list, select **Equals**.
 - Enter the user name in the field.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **User Login** column to open the User Details page.
2. In the row of controls at the top of the page, select **Lock Account**.
3. In the Lock Account confirmation dialog box, select **Lock**.

Unlock an account

If an account was explicitly locked by a delegated administrator, unlock it before the user can sign in again. Users who lock their accounts after too many incorrect password attempts can use **Trouble Signing In** to reset their passwords.

Before unlocking an account, check the reason for which it was locked and verify that the person asking to have the account unlocked is the owner. To help ensure system security, establish a process to confirm the requester's identity.

1. Navigate to the User Details page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Users** tile.
 - c. For the **Display Name**:
 - From the list, select **Equals**.
 - Enter the user name in the field.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **User Login** column to open the User Details page.
2. In the row of controls at the top of the page, select **Unlock Account**.
3. In the Unlock Account confirmation dialog box, select **Unlock**.
4. Reset the password. See [Reset a user's password](#) for details.

Terminate or reinstate an account

Terminate a user account when the user is no longer employed by your company.

To terminate a user account:

1. Navigate to the User Details page for the user account.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Users** tile.
 - c. For the **Display Name**:
 - From the list, select **Equals**.
 - Enter the user name in the field.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **User Login** column to open the User Details page.
2. Select **Lock Account** to prevent the account from being used.
3. In the Lock Account confirmation dialog box, select **Lock**.
4. Select the **Roles** tab.
5. Select the role you want to remove.
6. From the **Actions** list, select **Remove**.
The Remove Roles page opens.
7. Review the roles in the cart. To exclude a role from the cart, select **Remove** to the right of the role.
8. Select **Submit** in the upper-right corner.

The message *Successfully completed the operation* appears.

Note

If you need to remove delegated administrator roles from this account, contact Oracle Life Sciences Support for assistance.

9. Select the **X** button in the upper-right corner to close the dialog box.
10. On the User Details page, select **Disable User**.
11. On the Disable Users page, select **Submit** in the upper-right corner.
The message *Successfully completed the operation* appears after the user has been disabled.

To reinstate a user account that was terminated:

1. Navigate to the User Details page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Users** tile.
 - c. For the **Display Name**:
 - From the list, select **Equals**.
 - Enter the user name in the field.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **User Login** column to open the User Details page.
2. Select **Enable User**.
3. On the Enable Users page, select **Submit** in the upper-right corner.
The message *Successfully completed the operation* appears after the user has been enabled.
4. Update user information, if necessary. See [Update a user's name, email address, or user login](#) for details.
5. Assign roles to the user. See [Assign roles](#) for details.
6. Reset the account password. See [Reset a user's password](#) for details.

6

Role settings

Basic roles allow users to access your company resources: applications or studies. You can configure these roles as described in this section.

- [Navigate to the Roles page](#)
- [Set the unauthorized access page for an application or study](#)
You can edit a role to choose what type of page is displayed in the browser when an unauthorized user tries to access the application or study that is associated with the role.
- [Set up approval for a role](#)
By default, roles are assigned to the target user immediately after the request is submitted.
- [Set up self-service registration](#)
Self-service registration is a convenient way to provide multiple users with the ability to request and gain access to new resources, such as a new study or a new application instance.
- [Grant external access to company applications or studies](#)
Access to your company resources is controlled through organization-specific roles. Roles that correspond to your organization's applications or studies are only visible to users within your organization.

Navigate to the Roles page

To view or edit a role, navigate to the Roles page, search for the role, and open the role page:

1. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

2. Select the **Roles and Access Policies** tile.
3. In the Search section, for **Name**:
 - From the list, select **Equals**.
 - In the field, enter the role name without the ShortOrgId.
4. Select **Search**.
5. In the Search Results section, select the link in the **Name** column to open the role page.

Role information is grouped under tabs. Select a tab to view or edit the information.

Set the unauthorized access page for an application or study

You can edit a role to choose what type of page is displayed in the browser when an unauthorized user tries to access the application or study that is associated with the role.

1. Navigate to the Roles page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Roles and Access Policies** tile.
 - c. In the Search section, for **Name**:
 - From the list, select **Equals**.
 - In the field, enter the role name without the ShortOrgId.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **Name** column to open the role page.
2. In the row of icons near the top of the page, select **Set Unauthorized Access Page**.
3. Select one of the following:
 - **Authorization Error Page**: Displays a message indicating that the user does not have access to the resource.
 - **Resource Not Found Page**: Displays a message indicating that the page does not exist.
 - **Authorization Request Page**: Displays the self-service registration page where the user can submit a request for access. See [Set up self-service registration](#) for details.
4. Select **Submit**.
5. Select **OK**.
6. Select **X** to close the dialog box.

Set up approval for a role

By default, roles are assigned to the target user immediately after the request is submitted.

For basic roles, which control access to the application or study, you can activate approval so that the role can be assigned to a user only after the request is approved. With approval active for a role, an approval request is created when:

- You assign the role from Oracle Identity Self Service.
- A user submits an access request for the associated application or study through self-service registration. See [Set up self-service registration](#) for details. After a user submits an access request, approvers receive an email notification.

Users who have the Approver role can approve or reject access requests.

- [Request and assign the Approver role](#)
The Approver role is added to your organization on request. This role is required to use approval.
- [Activate approval for a role](#)

- [Deactivate approval](#)
- [Approve or reject access requests](#)
Users who have the Approver role can view, approve, and reject access requests.

Request and assign the Approver role

The Approver role is added to your organization on request. This role is required to use approval.

Users who have the Approver role can approve or reject access requests for roles where approval is active. These users cannot process their own access requests. Assign the role to a user who does not submit access requests, or assign it to more than one user.

1. Submit a request to Oracle Life Sciences Support to create the Approver role for your organization.
2. After the role is available, assign it to one or more users in your organization. See [Assign one or more roles to the same user](#) for instructions.

Activate approval for a role

1. If you haven't already, assign the Approver role to at least one user so that user can approve valid requests to grant the role. See [Request and assign the Approver role](#) for details.
2. Navigate to the Roles page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Roles and Access Policies** tile.
 - c. In the Search section, for **Name**:
 - From the list, select **Equals**.
 - In the field, enter the role name without the ShortOrgId.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **Name** column to open the role page.
3. In the row of controls at the top of the page, select **Set Approval Options**.
 4. In the dialog box, select **Activate Approval**.
 5. To send requesting users a notification after the access request is approved or rejected, select **Notify the user on request status**.
 6. Select **Submit**.

The message *Approval activated for the role* appears at the bottom if the operation succeeded.
 7. Select **X** to close the dialog box.

Deactivate approval

Warning

If self-service registration is active for this role and you deactivate approval, all access requests submitted by users through self-service registration will be approved automatically, granting the requesting user access to the associated application or study.

If this is not your intent, deactivate self-service registration before deactivating approval so that only delegated administrators can assign the role.

1. Navigate to the Roles page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Roles and Access Policies** tile.
 - c. In the Search section, for **Name**:
 - From the list, select **Equals**.
 - In the field, enter the role name without the ShortOrgId.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **Name** column to open the role page.
 2. In the row of controls at the top of the page, select **Set Approval Options**.
 3. In the dialog box, select **Deactivate Approval**.
 4. Select **Submit**.
 5. Select **X** to close the dialog box.

Approve or reject access requests

Users who have the Approver role can view, approve, and reject access requests.

These requests are created when:

- A delegated administrator assigns a role to a user when approval is active for the role.
- A user submits an access request through self-service registration. See [Set up self-service registration](#) for details. After a user submits an access request, approvers receive an email notification.

To customize columns on the Approval Details page:

The default information on the Approval Details page is the same for all requests. To help distinguish requests, customize the columns to include additional user identification and other information that you need to decide whether to approve or reject a request.

You can create a custom view for the Approval Details page by specifying the columns that you want to see.

1. Navigate to the Pending Approvals page.
2. On the Approval Details page, select the **Add View** icon  on the toolbar.
3. On the **Definition** tab, edit the **Name** field to give your view a name.
4. Select the task types to include in your view:
 - a. To the right of **Task Type**, select the search icon .
 - b. Press and hold **Ctrl**, and select **RoleLevelApprovalFlow** and **RoleLevelApprovalFlowNoMail**.
 - c. Select **OK**.
5. Select the columns to include in your view:
 - a. Select the **Display** tab.
 - b. Move columns from the **Available** list to the **Selected** list to add them to your view.
Suggested columns:
 - **Title**: Contains the link to the Request Details page.
 - **Requester**: Displays the requesting user's full name, including the ShortOrgId.
 - **RequesterDisplayName**: Shows the requesting user's display name.
 - **RequestID**: Unique identifier for the access request.
 - **Acquired By**: Shows the display name of the approver who claimed the request. This column is useful if there are multiple users with the Approver role in your organization.
 - c. Select **OK**.

Your new view is available from the **Views** menu, under **My Views**. This view is visible only to you. Other users cannot see it.

To approve or reject a pending request:

Approving a request grants the requested role to the target user.

1. Navigate to the Pending Approvals page.
2. If you have a custom view, select it under **My Views**.
3. If multiple users in your organization have the Approver role, claim a pending request before you approve or reject it. Otherwise, skip this step.
 - a. Select the row for the request.
 - b. From the **Actions** list at the top of the page, select **Claim**.
4. Double-click the row for the request.
5. Add a comment. A comment is optional when you approve a request, but required when you reject a request.

- a. Select the **Approval** tab.
 - b. In the upper-right corner of the **Comments** text box, select **Create**.
 - c. Enter your comment and select **OK**.
6. In the upper-right corner of the page, select **Approve** or **Reject**.

Set up self-service registration

Self-service registration is a convenient way to provide multiple users with the ability to request and gain access to new resources, such as a new study or a new application instance.

- [Activate self-service registration](#)
When self-service registration is active for a role, unauthorized users who navigate to the application or study that is associated with the role can submit an access request.
- [Deactivate self-service registration](#)
To deactivate self-service registration, set the unauthorized access page to something other than Authorization Request Page.

Activate self-service registration

When self-service registration is active for a role, unauthorized users who navigate to the application or study that is associated with the role can submit an access request.

1. Navigate to the Roles page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Roles and Access Policies** tile.
 - c. In the Search section, for **Name**:
 - From the list, select **Equals**.
 - In the field, enter the role name without the ShortOrgId.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **Name** column to open the role page.
2. If you want users' access requests to be reviewed and approved before granting the role, activate approval for this role. Approval is inactive by default. See [Activate approval for a role](#) for instructions.

If you want all requests to be automatically approved, skip this step. If approval is already active for the target role and you don't want to use it, you can deactivate it. See [Deactivate approval](#) for details.
 3. In the row of icons near the top of the page, select **Set Unauthorized Access Page**.
 4. Select **Authorization Request Page**.
 5. Select **Submit**.

6. Select **OK**.
7. Select **X** to close the dialog box.

Deactivate self-service registration

To deactivate self-service registration, set the unauthorized access page to something other than Authorization Request Page.

For details, see [Set the unauthorized access page for an application or study](#).

Also review the current approval setting for the role to make sure it is set as required. See [Set up approval for a role](#) for details.

Grant external access to company applications or studies

Access to your company resources is controlled through organization-specific roles. Roles that correspond to your organization's applications or studies are only visible to users within your organization.

If you need to make a resource available to users from other organizations—for Oracle employees to provide assistance, for example—you can publish the role externally so that it can be assigned to users outside of your organization. These users are called *external members* in relation to the role.

- [Allow another organization to view and assign one of your organization's roles](#)
After you make a role visible to an external organization, delegated administrators for the external organization can see the role and can assign it to users in their organization.
- [View and remove external member access to a role](#)

Allow another organization to view and assign one of your organization's roles

After you make a role visible to an external organization, delegated administrators for the external organization can see the role and can assign it to users in their organization.

Warning

You cannot undo this operation by yourself. To remove a role from an external organization, contact Oracle Life Sciences Support.

1. Navigate to the Roles page.
 - a. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Roles and Access Policies** tile.

- c. In the Search section, for **Name**:
 - From the list, select **Equals**.
 - In the field, enter the role name without the ShortOrgId.
- d. Select **Search**.
- e. In the Search Results section, select the link in the **Name** column to open the role page.

✓ **Tip**

Before making a role available to external organizations, consider activating approval for the role. When approval is active, requests to assign the role to external users must be approved by your organization. See [Activate approval for a role](#) for details.

2. In the row of controls at the top of the role page, select **Publish Role to External Organization**.
3. Select the checkboxes for the organizations to which you want to make the role available.
4. Select **Submit**.

The message *Role published to selected organizations* appears after the role has been published.
5. Select **X** to close the dialog box.
6. After the role is published, notify your point of contact in the external organization that the role is visible and that their delegated administrator can assign it to users, as needed.

📘 **Note**

If self-service registration is active for this role, users from the external organization can request access by going to your company link for the application or study. For details, see [Set up self-service registration](#).

If approval is active for the role, you must approve the request to grant the role to the external user. If approval is not active, the role is granted automatically when the external delegated administrator assigns it to their users. See [Activate approval for a role](#) for details.

View and remove external member access to a role

To view external members for a role that was published externally and remove the role from user accounts that belong to external organizations:

1. Navigate to the Roles page.
 - a. In the upper-right corner, select **Manage**.

📘 **Note**

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

- b. Select the **Roles and Access Policies** tile.
 - c. In the Search section, for **Name**:
 - From the list, select **Equals**.
 - In the field, enter the role name without the ShortOrgId.
 - d. Select **Search**.
 - e. In the Search Results section, select the link in the **Name** column to open the role page.
2. Select the **Members** tab.
 3. In the row of controls at the top of the tab, select **External Members**.

The External Members dialog box lists all users from external organizations to which the role is assigned.
 4. Select the checkboxes for the users that you want to remove, and select **Revoke**.

The message *Role revoked for the selected users* appears after the role has been removed.

 Note

This removes the role from external members, but the role continues to be visible to the external organization and can still be assigned to their users. To remove the role from the external organization, contact Oracle Life Sciences Support.

5. Select **X** to close the dialog box.

7

Perform user operations in bulk

If you need to create or terminate multiple users and grant or remove roles for multiple users, use Bulk Import to upload user operations in a spreadsheet. The system runs the operations for you.

During a bulk import, you can create or authorize users, including new users created in the same file. You can also deauthorize or disable users, including users deauthorized in the same file.

- [Use Bulk Import](#)
- [Get the template](#)
A spreadsheet template for the bulk import file is available in Oracle Identity Self Service. You can download it and reuse it as necessary to create bulk import files.
- [Add operations to the template](#)
Add the details for the user operations you want to run to a CSV or TXT file.
- [Check for errors](#)
Review the file to make sure that the format and content are correct. If a command does not pass validation, it will not run.
- [Import data](#)
When your bulk import file is ready, upload it. The system reads and runs the commands.
- [Review and reuse previous import files](#)
You can review all previous imports for your organization and download the bulk import file that was used.

Use Bulk Import

1. If necessary, download the bulk import file template.
See [Get the template](#) for details.
2. Create a bulk import file.
See [Add operations to the template](#) and [Check for errors](#) for details.
3. Import data.
See [Import data](#) for details.

Get the template

A spreadsheet template for the bulk import file is available in Oracle Identity Self Service. You can download it and reuse it as necessary to create bulk import files.

To download the template:

1. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

2. Select the **Bulk Import** tile.
3. Select **Import a File**.
4. Select **Help**.
5. Select **Download Sample File** to download and save the template file locally.

Add operations to the template

Add the details for the user operations you want to run to a CSV or TXT file.

1. Create a copy of the template file or of a previous import file and rename it for the current import.

See [Get the template](#) or [Review and reuse previous import files](#) for details.

2. Open the file using Microsoft Excel or a text editor, such as Notepad.
3. Enter data using one row for each command, as follows:
 - For each row, add the required data for the operation.
 - If you are using the template, replace the placeholder text in angle brackets with values for the target user operation.
 - Details for some placeholders:
 - <organization id>: Your company ShortOrgId.
 - <user login>: The name that the user uses to sign in, without the ShortOrgId.
 - <email id>: The email address associated with the target account.
 - <role name>: The name of the role you are granting or removing, including the ShortOrgId as a prefix. For example, mypharma.Approver.
 - <middle name>: The user's middle name. This value is optional. If you do not supply a middle name, leave the spreadsheet cell blank. If you are using a text editor, delete the placeholder but leave the comma.

For details about completing the import file, see [Check for errors](#).

4. Save the file in CSV or TXT format.

Check for errors

Review the file to make sure that the format and content are correct. If a command does not pass validation, it will not run.

Hints to prevent validation errors

- The file must not include angle brackets (<>). Replace the angle brackets and placeholder text in the template file with your data.
- Each operation description must begin on a new line and start with the command name.

- Do not include spaces before or after values.
- If you use a text editor, check that:
 - All values for an operation are on the same line.
 - There are no spaces between a value and the comma before or after it.
 - Each value is followed by a comma, except for the final value in a row.

Import data

When your bulk import file is ready, upload it. The system reads and runs the commands.

1. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

2. Select the **Bulk Import** tile.
3. Select **Import a File**.
4. On the Upload File page, select **Browse**.
5. Navigate to your bulk import file, select it, and select **Open**.

The file name appears in the **Select a file** field.

6. Select **Upload**.

After the file is uploaded, the Confirm Data to import page opens, showing a preview of the uploaded commands.

7. Review the commands for accuracy.

If the **Import** button is inactive, one or more commands are not valid. In this case:

- a. Identify the error. A red X icon  in the **Status** column indicates that the operation is not valid. Check the **Message** column for information about the error.
- b. Correct the errors in your bulk import file. Work with Oracle Life Sciences Support, if necessary, to correct the errors.
- c. Restart the process to upload the corrected file.

8. If the commands are correct, select **Import**.

9. On the Result Details page, review the **Status** column for all entries:

- A green checkmark  appears for successful operations.
- A red X  appears for operations that were not valid and were not run. Check the **Message** column for details about the error. Hold your cursor over a cell to see the full message.
You can also download the processed import file to view the full text of all messages. See [Review and reuse previous import files](#) for details.

To complete the operations that failed to run:

- If only a few operations failed, manually perform the remaining operations.

- If a large number of operations failed, resubmit the bulk import file with only those operations that failed, after correcting the errors. See [Check for errors](#) for additional information or contact Oracle Life Sciences Support for assistance.

Review and reuse previous import files

You can review all previous imports for your organization and download the bulk import file that was used.

1. In the upper-right corner, select **Manage**.

Note

Customers who have not yet migrated to the updated Oracle Identity Self Service console and continue to use OIM may not see the **Manage** button. Use the equivalent administration page in your current console.

2. Select the **Bulk Import** tile.
3. Select **View Imported Files**.
4. In the **File Name** column, select the item you want to review.
The Result Data page opens, showing the import details.
5. To download the file, select **Export** and save it locally.

8

Access customized reports

To access any of the following customized reports, submit a request through [Support Cloud](#). These reports are provided in Excel spreadsheet format, and timestamps are displayed in Greenwich Mean Time (GMT).

- **Authentication History Report:** Displays successful and failed sign-in attempts for an application URL, such as a single sign-on URL.
- **Federation Audit History Report:** Displays federated authentication data for Security Assertion Markup Language (SAML) assertions and eSignature events, including identity provider name, user information, and authentication time for an application URL.
- **First and Last Access Report:** Displays the first and last access date and time for each user for Oracle InForm, Oracle Central Coding, and Oracle Empirica Signal. This report is not available for Oracle Clinical One Platform.
- **Custom Role Membership Report:** Displays information about when each user had access to a role in Oracle Life Sciences IAMS. For Oracle InForm, a study is a role. For other applications, such as Oracle Clinical One Platform, Oracle Central Coding, or Oracle Empirica Signal, each application instance is a role.

This report contains the following information for each user: User ID, First Name, Last Name, Email, the date and time when the user was created in Oracle Life Sciences IAMS, current user status, user membership status, effective start date and time and end date and time for the membership status, and the Oracle Life Sciences IAMS user who created the user or changed the user's role membership status. If a user's membership status changed over time, the report contains multiple rows for that user.

To see when each user authorized for an Oracle InForm study had access to the study, use this report.

- [Request customized reports](#)

Request customized reports

To request a customized report:

1. Go to [Support Cloud](#).
2. Sign in with your Oracle Corp SSO credentials.
3. Select **Create Request**.
4. Select **Change Request**.
5. Select **Learn about your application**.
6. In the **Summary** field, enter Please provide IAMS (enter report name).
7. In **Severity**, select **Medium** from the list.
8. In the **Description** field, enter the required information for the report you need:
 - For Authentication History Report, provide the name of the study and a time frame.
 - For Federation Audit History Report, provide the customer ShortOrgId and a time frame.

- For First and Last Access Report, provide the name of the study and a time frame.
- For Custom Role Membership Report, provide the name of the study and a time frame.

Note

When providing a time frame, include day, month, and year. For example, 01-JAN-2018 through 31-DEC-2019 inclusive.

9. In **Category**, select **Service Request**, then **Application**, then **General**, and then **Information**.
10. In **Product**, select **UMT**.
11. In **Business Service**, select **UMT**.
12. In **Environment**, select **Prod/Live**.
13. In **Implementation Window**, select **As Soon As Possible**.
14. In **Date Required By**, select a valid date from the calendar.
15. In **Action**, select **Other**.
16. In **sFTP path**, provide a folder path where the generated report should be uploaded.
17. Select **Submit**.