Oracle® Health Sciences Identity and Access Management Service

Administrator Guide

Release 22.2
F56887-02
May 2022

ORACLE

Oracle Health Sciences Identity and Access Management Service Administrator Guide, Release 22.2

F56887-02

Contents

Preface

This preface contains the following sections:

Documentation accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Health Sciences Customer Support Portal (https://hsgbu.custhelp.com/)
- Japanese interface of Oracle Health Sciences Customer Support Portal (https://hsgbu-jp.custhelp.com/)

You can also call our 24x7 help desk. For information, visit http://www.oracle.com/us/support/contact/health-sciences-cloud-support/index.html or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Additional copyright information

This documentation may include references to materials, offerings, or products that were previously offered by Phase Forward Inc. Certain materials, offerings, services, or products may no longer be offered or provided. Oracle and its affiliates cannot be held responsible for any such references should they appear in the text provided.

1

About this guide

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

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

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

> **Note:**
>
> If you want to navigate from the Oracle Health IAMS Oracle Identity Self Service console to the Oracle Health Sciences My Oracle Bookmarks or the Oracle Health Science Cloud landing page, click Home on the left menu.

Federation guidelines

Keep the following guidelines in mind when using a federated account with Oracle Health Sciences Identity and Access Management Service (Oracle Health IAMS).

Federation account linking

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

Oracle Health 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 Health Sciences Cloud using your identity provider, you can log into Oracle systems directly using your Oracle Health Sciences SSO credentials.

Session security

- When logging out of Oracle Health Sciences Cloud, close your browser to ensure all logins are terminated. You may be logged into Oracle in multiple browser windows or tabs. Logging out in one browser window does not log you out of all browser windows. Closing all open browsers ensures all logins are terminated.

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

Electronic signatures

If you have logged into the Oracle Health 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

If your organization was earlier using the Oracle Health IAMS 1.4.2 release, you have an option to choose the way users in your organization can reset their account password.

1. Under the **Administration** menu on the left, click **Users**.
2. Under the User Settings heading, select one of the following:
   - **Email Link**: When a new user is created or when a user clicks on Trouble Signing In on the Sign In page, an email with a link to set the account password is sent to the user.
   - **Security Questions**: This is selected by default if your organization was earlier using the OHSIAMS 1.4.2 release. When a new user is created or when a user clicks on Trouble Signing In on the Sign In page, an email containing the account password is sent to the user.

> **Note:**
>
> Once the password reset flow is set to Email Link, you cannot change it to Security Questions.

3. Click **Yes** on the Confirmation screen.

- Password Reset Using Email Link: FAQs

Password Reset Using Email Link: FAQs

- Is there anything else required other than enabling the Email Link flow?
  Email templates have been updated in release 1.5. If you want to customize the email templates, contact your Oracle representative to do so before you enable the Email Link flow.
- Where can I test the Email Link flow?
  Create a tenant and a CDA user under the UAT environment. Contact Health Sciences Support for assistance.
- Is enabling the Email Link flow at the user, trial, or tenant level?
  Enabling the Email Link flow is at the tenant level, and is applicable to all users within the tenant.
- After enabling Email Link flow, can I switch back to the Security Questions flow?
  You cannot switch back to the Security Questions flow through the Oracle Health IAMS . Contact Health Sciences Support to switch back to the Security Questions flow, provided there are no users created when switching from Email Link to Security Questions flow.
- How do I enable the Email Link flow if my organization was not using Oracle Health IAMS release 1.4.2?
  The Email Link flow is enabled by default for an organization that started using Oracle Health IAMS from release 1.5.

Is there anything else required other than enabling the Email Link flow?

Email templates have been updated in release 1.5. If you want to customize the email templates, contact your Oracle representative to do so before you enable the Email Link flow.

If you want to use the default email templates, you can directly enable the Email Link flow.

Where can I test the Email Link flow?

Create a tenant and a CDA user under the UAT environment. Contact Health Sciences Support for assistance.

Is enabling the Email Link flow at the user, trial, or tenant level?

Enabling the Email Link flow is at the tenant level, and is applicable to all users within the tenant.

After enabling Email Link flow, can I switch back to the Security Questions flow?

You cannot switch back to the Security Questions flow through the Oracle Health IAMS . Contact Health Sciences Support to switch back to the Security Questions flow, provided there are no users created when switching from Email Link to Security Questions flow.

How do I enable the Email Link flow if my organization was not using Oracle Health IAMS release 1.4.2?

The Email Link flow is enabled by default for an organization that started using Oracle Health IAMS from release 1.5.

3
Create a user account

Oracle users can no longer be created or disabled in Oracle Health Sciences User Management Tool and Oracle Health IAMS. They are now required to request access in Oracle Identity Manager (OIM), which gets synchronized in Oracle Health IAMS and into Oracle InForm User Management Tool.

> **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. Under the **Administration** menu on the left, click **Users**.
2. Under the Search Results heading, click **Create**.
3. Fill in the fields with the new user's information.

> **Tip:**
>
> In the **Organization** field, type your ShortOrgId.
> If you don't know your ShortOrgId:
>
> a. Click the search icon  next to the Organization field.
> b. Click **Search** to do a blank search.
> c. In the Search Results, select the row where Company appears in the Type column.
> d. Click **Select**.

> **Tip:**
>
> If you specify an email address, there is no need to fill in the password fields. Depending on the password reset flow chosen by you, the system generates an initial password email or an email with a link to set the account password, and emails it to the user.

4. Click **Submit** in the top right of the page. A confirmation message appears and you are redirected to the User Details page for the new user.
5. 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 Health 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. Under **Administration** in the menu on the left, click **Users**.
   b. For the **Display Name**:
      - From the list, select **Equals**.
      - Type the user name in the field.
   c. Click **Search** on the right.
   d. In the Search Results section, click 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. Type the role name in the search box and press **Enter** or click  to search. See the Role FAQs for help.
   b. In the search results, select the role you want to assign.
   c. Click **Add to cart** at the right end of the row.

5. Click **Checkout** in the top right corner of the page.
6. Review the roles in the cart. You can click **Remove** to the right of a role to exclude it from the cart.
7. Click **Submit** in the top right. 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 only assigned after the corresponding request is approved.

   If the 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 Health 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 Health 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 Health Sciences application delegates role administration to Oracle Health 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 Health IAMS?
  For such cases, you assign application roles from the application itself.
- What are the different types of users in Oracle Health IAMS and the roles assigned to them?
  These roles are specific to Oracle Health IAMS and they control privileges that users have in the Oracle Health 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 Health 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 Health Sciences application they need to work in. The role name includes your company ShortOrgId, in the format *ShortOrgId*.*basic_role*.

Additionally, if an Oracle Health Sciences application delegates role management to Oracle Health IAMS, you must also grant those 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 Health Sciences application delegates role administration to Oracle Health 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 Health IAMS?

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

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

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

The following are the different types of users in Oracle Health IAMS:

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

Customer Delegated Administrator

As an initial Customer Delegated Administrator (CDA) of your organization, by default, you will have the following roles:

- • All Users: This is a default role assigned to all users that allows a user to access their own record.
- • Role Authorizer: Allows to grant and revoke business services to a user in the organization.
- • Role Viewer: Allows to view business services, user assignments, and the profiles of assigned users within the organization.
- • User administrator: Allows to create, modify, and terminate users, enable, disable, lock and unlock, and grant and revoke business services within the organization.

- • User Viewer: Allows to view organization, search for users, and view user profiles.
- • System-admin: Allows to create OAuth clients. A CDA can assign this role to other users in the organization.

An initial CDA has the permission to submit a ticket in Health Sciences Support to request for an additional CDA in Oracle Health IAMS. The additional CDA will have all the above mentioned roles assigned to them.

The following are the roles that are not assigned to the initial CDA by default. The initial CDA can submit a ticket in Health Sciences Support to request for these roles:

- • Approver: The Approver role is added to your organization on request. This role allows a CDA to access the Approval Details page, to claim, approve, or reject access requests for those roles where approval is active. See Request and assign the Approver role for details.
- • HelpDesk: Allows to force a password change and unlock an account only if it is locked due to maximum failed login attempts, you must have the “HelpDesk” role.

System Administrator

The primary responsibility of a system administrator is to set up OAuth clients. A system administrator does not have the permission to manage Oracle Health IAMS users but has the permission to manage certain aspects of the Oracle Health IAMS application. As a system administrator, you will have the following roles:

- • All Users: This is a default role assigned to all users that allows a user to access their own record.
- • System-admin: Allows the user to create OAuth clients. The CDA gets this role by default but CDA could assign it to other users.

My Oracle Bookmarks Administrator

If you are the My Oracle Bookmarks administrator, you will have the following roles:

- • All Users: This is a default role assigned to all users that allows a user to access their own record.
- • Sponsor admin: Allows user to add descriptions, therapeutic area, customize My Oracle Bookmarks, and create links to native (non-SSO) InForm trials.

Application End User

Application end users will have only the “All Users” role assigned to them. This is a default role that allows a user to 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 Health 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 the application roles.

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

FNTD_BIZ_SERVICE_FD_SP_ADMIN: Assign this application role to users of organizations, often a sponsor administrator, who manage the applications used to conduct clinical trials. Users with this role can perform high-level maintenance in My Oracle 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 My Oracle Bookmarks, see the section on enhancements introduced in release 1.4.1.1 in the *Oracle Health Sciences Identity and Access Management Service Release Notes* on the Oracle Help Center.

5

Update user accounts

You can update user accounts in Oracle Health IAMS 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
  You cannot update the account information for Oracle users. It can be updated *only* in corporate OIM. However, you can update the contact information of an Oracle user.
- Reset a password
- Remove roles
  If a user no longer needs access or privileges in an application or when the user leaves the company, we recommend that you remove unnecessary roles.
- 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 logging in before you disable the account for termination of employment or for other reasons.
- Unlock an account
  If the account was explicitly locked by a delegated administrator, you need to unlock the account before it can be used again. Users who lock their accounts by entering an incorrect password too many times can use the **Trouble Signing In** link on the Sign In page to reset their passwords and unlock their account.
- Terminate or reinstate an account
  We recommend that you 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. Under **Administration** in the menu on the left, click **Users**.
2. For the **Display Name**:
   - From the list, select **Equals**.
   - Type the user name in the field.
3. Click **Search** on the right.
4. In the Search Results section, click 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

You cannot update the account information for Oracle users. It can be updated *only* in corporate OIM. However, you can update the contact information of an Oracle user.

To update the information associated with a user account:

1. Navigate to the User Details page:
    a. Under **Administration** in the menu on the left, click **Users**.
    b. For the **Display Name**:
        - From the list, select **Equals**.
        - Type the user name in the field.
    c. Click **Search** on the right.
    d. In the Search Results section, click the link in the **User Login** column to open the User Details page.
2. In the top left, click **Modify User**.
3. Update the following fields as necessary:
    - First Name
    - Last Name
    - E-mail
    - User Login
4. Click **Submit** in the top right.

Reset a password

To manually reset the password for a user account:

1. Navigate to the User Details page.
    a. Under **Administration** in the menu on the left, click **Users**.
    b. For the **Display Name**:
        - From the list, select **Equals**.
        - Type the user name in the field.
    c. Click **Search** on the right.
    d. In the Search Results section, click 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, click **Reset Password**.
3. Perform one of the following depending on the password reset flow you have set:
    - If you are using Email Link as the password reset flow, click **Send** on the Confirmation screen.
    - If you are using Security Questions as the password reset flow:
        a. Select **Auto-generate the Password**.

> **Note:**
>
> Although it is not recommended, you can manually define a new password:
> Select **Manually change the Password**, fill in the password fields, and select the **E-mail the new password to the user** checkbox.

b. Click **Reset Password**.

Remove roles

If a user no longer needs access or privileges in an application or when the user leaves the company, we recommend that you remove unnecessary roles.

To remove roles for a user account:

1. Navigate to the User Details page.
   a. Under **Administration** in the menu on the left, click **Users**.
   b. For the **Display Name**:
      - From the list, select **Equals**.
      - Type the user name in the field.
   c. Click **Search** on the right.
   d. In the Search Results section, click 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. You can click **Remove** to the right of a role to exclude it from the cart.
6. Click **Submit** in the top right.

   The message *Successfully completed the operation* appears.

> **Note:**
>
> If you need to remove delegated administrator roles from this account, contact Health 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 logging in before you disable the account for termination of employment or for other reasons.

1. Navigate to the User Details page.

a. Under **Administration** in the menu on the left, click **Users**.
b. For the **Display Name**:
   - From the list, select **Equals**.
   - Type the user name in the field.
c. Click **Search** on the right.
d. In the Search Results section, click 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, click **Lock Account**.
3. In the Lock Account confirmation dialog box, click **Lock**.

Unlock an account

If the account was explicitly locked by a delegated administrator, you need to unlock the account before it can be used again. Users who lock their accounts by entering an incorrect password too many times can use the **Trouble Signing In** link on the Sign In page to reset their passwords and unlock their account.

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

1. Navigate to the User Details page.
   a. Under **Administration** in the menu on the left, click **Users**.
   b. For the **Display Name**:
      - From the list, select **Equals**.
      - Type the user name in the field.
   c. Click **Search** on the right.
   d. In the Search Results section, click 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, click **Unlock Account**.
3. In the Unlock Account confirmation dialog box, click **Unlock**.
4. Reset the password. See Reset a password for details.

Terminate or reinstate an account

We recommend that you 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. Under **Administration** in the menu on the left, click **Users**.

b. For the **Display Name**:
   - From the list, select **Equals**.
   - Type the user name in the field.

c. Click **Search** on the right.

d. In the Search Results section, click the link in the **User Login** column to open the User Details page.

2. Click **Lock Account** to prevent the account from being used.
3. In the Lock Account confirmation dialog box, click **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. You can click **Remove** to the right of a role to exclude it from the cart.
8. Click **Submit** in the top right.
   The message *Successfully completed the operation* appears.

> **Note:**
>
> If you need to remove delegated administrator roles from this account, contact Health Sciences Support for assistance.

9. Click the **x** button in the top right corner to close the dialog box.
10. On the User Details page, click **Disable User**.
11. On the Disable Users page, click **Submit** in the top right.
    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. Under **Administration** in the menu on the left, click **Users**.

b. For the **Display Name**:
   - From the list, select **Equals**.
   - Type the user name in the field.

c. Click **Search** on the right.

d. In the Search Results section, click the link in the **User Login** column to open the User Details page.

2. Click **Enable User**.
3. On the Enable Users page, click **Submit** in the top right.

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 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.

- Open the role 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.

Open the role page

To view or edit a role, search for it and open the role page:

1. Under the **Administration** menu on the left, click **Roles**.
2. In the Search section, for **Display Name**:
   - From the list, select **Equals**.
   - In the field, type the role name, without the ShortOrgId.
3. Click **Search**.
4. In the Search Results, click the link in the **Display 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. Open the role page.
   a. Under the **Administration** menu on the left, click **Roles**.
   b. In the Search section, for **Roles**:
      - From the list, select **Equals**.

- In the field, type the role name, without the ShortOrgId.

c. Click **Search**.

d. In the Search Results, click the link in the **Display Name** column to open the role page.

2. In the row of icons near the top of the page, click **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. Click **Submit**.
5. Click **OK**.
6. Click **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 only be assigned to a user if the request is approved. With approval active for a role, an approval request is created when:

- You assign the role from Oracle Health IAMS 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). After a user submits an access request, an email is sent to the approver(s) detailing a request is pending for their action to be taken.

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 see and 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.

Users who have the Approver role will be able to approve or reject access requests for roles where approval is active. These users cannot process their own access requests, so we recommend that you assign the role to a user who would not submit access requests or assign it to more than one user.

1. Submit a request to Oracle 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. Open the role page.
   a. Under the **Administration** menu on the left, click **Roles**.
   b. In the Search section, for **Display Name**:
      - From the list, select **Equals**.
      - In the field, type the role name, without the ShortOrgId.
   c. Click **Search**.
   d. In the Search Results, click the link in the **Display Name** column to open the role page.
3. In the row of controls at the top of the page, click **Set Approval Options**.
4. In the dialog box, select **Activate Approval**.
5. If you want requesting users to receive a notification once the access request is approved or rejected, select **Notify the user on request status**.
6. Click **Submit**.

   The message *Approval activated for the role* appears at the bottom if the operation succeeded.
7. Click **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 instantly, 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. Open the role page.
   a. Under the **Administration** menu on the left, click **Roles**.
   b. In the Search section, for **Display Name**:
      - From the list, select **Equals**.
      - In the field, type the role name, without the ShortOrgId.
   c. Click **Search**.
   d. In the Search Results, click the link in the **Display Name** column to open the role page.
2. In the row of controls at the top of the page, click **Set Approval Options**.
3. In the dialog box, select **Deactivate Approval**.
4. Click **Submit**.
5. Click **x** to close the dialog box.

Approve or reject access requests

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

These requests are created when:

- A delegated administrator assigns a role to a user if approval is active for the role.
- A user submits a request through self-service registration. See Set up self-service registration for details. After a user submits an access request, an email is sent to the approver(s) detailing a request is pending for their action to be taken.

To customize columns on the Approval Details page:
The information that is displayed on this page by default appears to be the identical for all requests, making it difficult to tell requests apart. We recommend that you customize the columns on the Approval Details page to include additional user identification and other information you need so you can decide if you want to approve or reject a request.
You can create your own custom view for the Approval Details page by specifying the columns you want to see in it.

1. Under the **Requests** menu on the left, click **Pending Approvals**.
2. On the Approval Details page, click 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 that appear in your view:
   a. To the right of Task Type, click the search icon.
   b. Holding down the **Ctrl** key, select **RoleLevelApprovalFlow** and **RoleLevelApprovalFlowNoMail**.
   c. Click **OK**.
5. Select the columns that appear 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**: OHSIAMS unique identifier for the access request.
      - **Acquired By**: Shows the display name of the Approver who claimed the request, useful if there are multiple users with the Approver role in your organization.
   c. Click **OK**.

Your new view is available from the **Views** menu, under **My Views**. This view is only visible to you, other users can't see it.

To approve or reject a pending request:
Approving a request grants the requested role to the target user.

1. Under the **Requests** menu on the left, click **Pending Approvals**.
2. If you have a custom view, select it under **My Views** on the left.
3. If multiple users in your organization have the Approver role, you must claim a pending request before you can approve or reject it. Otherwise skip this step.
   a. Highlight the row of the request.
   b. From the **Actions** list at the top of the page, select **Claim**.
4. Double-click the row of the request.
5. Add a comment (optional to approve, but required to reject):
   a. Select the **Approval** tab.
   b. In the upper right of the Comments text box, click **Create**.
   c. Type your comment and click **OK**.
6. In the top right of the page, click **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. Open the role page.
   a. Under the **Administration** menu on the left, click **Roles**.
   b. In the Search section, for **Display Name**:
      - From the list, select **Equals**.
      - In the field, type the role name, without the ShortOrgId.
   c. Click **Search**.
   d. In the Search Results, click the link in the **Display 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, click **Set Unauthorized Access Page**.
4. Select **Authorization Request Page**.
5. Click **Submit**.
6. Click **OK**.
7. Click **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, you must submit a request to Oracle Support.

1. Open the role page.
   a. Under the **Administration** menu on the left, click **Roles**.
   b. In the Search section, for **Display Name**:
      - From the list, select **Equals**.
      - In the field, type the role name, without the ShortOrgId.
   c. Click **Search**.
   d. In the Search Results, click the link in the **Display Name** column to open the role page.

> **Tip:**
>
> We recommend that you make sure that approval is active for this role before making it available to external organizations. That way, when someone wants to assign the role to one of their users, this will create a request that must be approved by your organization to assign the role. See Activate approval for a role for details.

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

   The message *Role published to selected organizations* appears after the role has been published.
5. Click **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. Open the role page.
   a. Under the **Administration** menu on the left, click **Roles**.
   b. In the Search section, for **Display Name**:
      - From the list, select **Equals**.
      - In the field, type the role name, without the ShortOrgId.
   c. Click **Search**.
   d. In the Search Results, click the link in the **Display Name** column to open the role page.
2. Select the **Members** tab.
3. In the row of controls at the top of the tab, click **External Members**.

   The External Members dialog box lists all users from external organizations to which the role is assigned.
4. Select the checkboxes for those users that you want to remove and click **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, submit a request to Oracle Support.

5. Click **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 the Bulk Import feature to upload all user operations using a spreadsheet and the system executes them for you.

During a bulk import, you can create or authorize users (assign roles), including new users created in the same file. You can also deauthorize users (remove roles) or disable (terminate) 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 execute 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 execute.
- Import data
  When your bulk import file is ready, upload it. The system reads the commands and executes them.
- 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. Under the **Administration** menu on the left, click **Bulk Import**.
2. Click **Import a File**.

3. Click **Help**.
4. Click **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 execute 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, as expected for each type of operation.
   - If using the template, replace the placeholder text (surrounded with angled brackets) with values for the target user operation.
   - Details for some placeholders:
     - `<organization id>`: Your company ShortOrgId.
     - `<user login>`: Name with which the user logs in, without the ShortOrgId.
     - `<email id>`: 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>`: User's middle name, optional. If you do not supply a middle name leave the cell in the spreadsheet blank (or, if using a text editor, delete the placeholder but leave the comma).

   For further details on correctly filling in 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 execute.

Hints to prevent validation errors:

- The file must not include angle brackets (<>). Replace the angle brackets and text in the template file with your data.
- Each operation description must begin on a new line and start with the command name.
- There should be no 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 the commands and executes them.

1. Under the **Administration** menu on the left, click **Bulk Import**.
2. Click **Import a File**.
3. On the Upload File page, click **Browse**.
4. Navigate to your bulk import file, select it, and click **Open**.

   The file name appears in the **Select a file** field.
5. Click **Upload**.

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

   If the **Import** button is inactive, it means that 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 Support, if necessary, to correct the errors.

   c. Restart the process to upload the corrected file.
7. If the commands are correct, click **Import**.
8. 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 executed. 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 execute:

- 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 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. Under the **Administration** menu on the left, click **Bulk Import**.
2. Click **View Imported Files**.

3. In the **File Name** column, click the item you want to review.

   The Result Data page opens, showing the import details.

4. To download the file, click **Export** and save it locally.

8

Access customized reports

To get access to any of the following customized reports, request through Support Cloud. These reports are in Excel spreadsheet format and the time is displayed in the Greenwich Mean Time (GMT) time zone.

- Authentication History Report: This report displays successful and failed login attempts into an application URL. For example, for a given single sign-on trial URL.
- Federation Audit History Report: This report displays federated authentication data for Security Assertion Markup Language (SAML) assertions and eSignature events, including Identity Provider name, user information, and time of authentications into an application URL.
- First and Last Access Report: This report displays the first and last access date/time for each user for an Oracle InForm, Oracle Central Coding, Oracle Empirica Signal. This report is not available for Oracle Clinical One Platform.
- Custom Role Membership Report: This report displays information about when each user had an access to a role in Oracle Health IAMS. For Oracle InForm, a study is a role. For other applications likeOracle 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, date and time when the user was created in Oracle Health IAMS, current user status, membership status of the user, effective start date/time and end date/time for the membership status, Oracle Health IAMS user who created this user or changed the role membership status of the user. If a user's membership status changed over time, there will be multiple rows for that user.

  If you want to see when each user authorized to an InForm study had access to the study, you can use this report.
- Request customized reports

Request customized reports

To request a customized report:

1. Go to Support Cloud.
2. Log in with your Oracle Corp SSO credentials.
3. Click **Create Request**.
4. Click **Change Request**.
5. Click **Learn about your application**.
6. In the Summary field, write "Please provide IAMS (*enter report name*)".
7. In Severity, select **Medium** from the drop-down menu.
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 short Org-ID 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. Click **Submit**.