

# Oracle® Health Sciences Identity and Access Management Service

Administrator Guide

Release 1.4.2

E95436-01

June 2018

---

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 (OHSIAMS) **Oracle Identity Self Service** console.

The delegated administrator manages users and privileges for your hosted Oracle Health Sciences products, except InForm. InForm administrators create and manage user accounts in Oracle® Health Sciences User Management Tool (UMT).

## 1 Create a user account


**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.

Oracle users can no longer be created or disabled in UMT and OHSIAMS. They are now required to request access in Oracle's corporate Identity Manager (OIM), which gets synchronized in OHSIAMS and into UMT.

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:

1. Click the search icon  next to the Organization field.
2. Click **Search** to do a blank search.
3. In the Search Results, select the row where Company appears in the Type column.
4. Click **Select**.

**Tip:** If you specify an email address, the system generates an initial password and emails it to the user, so there is no need to fill in the password fields.

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](#).

## 2 Assign roles

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


### What do you want to do?

- [Assign one or more roles to the same user](#)
- [Assign the same role to multiple users](#)
- [Assign multiple roles to multiple users](#)
- [Role FAQs](#)

### 2.1 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.

The Request Summary page opens and a confirmation message appears at the top of the screen. If approval is active for any of the roles, the role is only assigned after the corresponding request is approved.

## 2.2 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](#).

## 2.3 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.

## 2.4 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*.

Additionally, if an Oracle Health Sciences application delegates role management to OHSIAMS, 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 OHSIAMS?

See the documentation for the application for details.

### How do you assign application roles if the application does not delegate role management to OHSIAMS?

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

### Why are the ALL USERS, Approver, User Viewer, User Administrator, or Role Authorizer roles assigned to a user and what do they do?

These roles are specific to OHSIAMS and they control privileges that users have in the OHSIAMS Oracle Identity Self Service application.

ALL USERS: assigned to all accounts by default.

Approver: grants the right to access the Pending Approvals page, to claim, approve, or reject access requests for those roles where approval is active. See [Request and assign the Approver role](#) for details. This role is not available by default. If you are using approval for a role, submit a request to Oracle Support to ask that they add the role for your organization.

User Viewer, User Administrator, and Role Authorizer: assigned only to delegated administrators by Oracle staff to grant required privileges in OHSIAMS Oracle Identity Self Service.

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

If your organization uses My Oracle Bookmarks, three additional roles are available in OHSIAMS Oracle Identity Self Service that control users' privileges in My Oracle 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 My Oracle Support, article ID **1964916.1**.

### 3 Update user accounts

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

#### 3.1 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.

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

---

---

**Note:** 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.

### 3.3 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. 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 checkbox **E-mail the new password to the user**.

---

---

4. Click **Reset Password**.

### 3.4 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. Click **Remove Roles**.
  4. In the dialog box, select all the checkboxes and click **Revoke**.

### 3.5 Lock an account

When a delegated administrator explicitly locks an account, the user cannot use the **Forgot Password** 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 confirmation dialog, click **Lock**.

### 3.6 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 **Forgot Password** link on the login 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 confirmation dialog, click **Unlock**.
4. Reset the password. See [Reset a password](#) for details.

### 3.7 Terminate or reinstate accounts

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 the **Lock Account** button to prevent the account from being used.
3. In the Lock Account confirmation dialog box, click **Lock**.
4. Select the **Roles** tab.
5. Click **Remove Roles**.
6. In the dialog box, select all the checkboxes and click **Revoke**.

The message *Selected Roles are removed successfully* appears at the bottom if the operation succeeded.

---

---

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

---

---

7. Click the x button in the top right corner to close the dialog box.
8. On the User Details page, click the **Disable User** button.
9. 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 the **Enable User** button.
  3. Update user information, if necessary. See [Update a user's name, email address, or user login](#) for details.
  4. Assign roles to the user. See [Assign roles](#) for details.
  5. Reset the account password. See [Reset a password](#) for details.

## 4 Role settings

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

### 4.1 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.

### 4.2 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 **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 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 x to close the dialog box.

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

With approval active for a role, an approval request is created when:

- You assign the role from OHSIAMS 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](#)).

#### 4.3.1 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.

#### 4.3.2 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**.
7. Click x to close the dialog box.

### 4.3.3 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** and click **Submit**.
4. Click x to close the dialog box.



### 4.3.4 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.

**4.3.4.1 Customize columns on the Pending Approvals 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 Pending Approvals 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 Pending Approvals 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 Pending Approvals 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.

**4.3.4.2 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. Under the **Requests** menu on the left, click **Pending Approvals**.
  - b. If you have a custom view, select it under **My Views** on the left.
  - c. Highlight the row of the request.
  - d. 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**.

## 4.4 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.

### 4.4.1 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** and click **Submit**.
5. Click **x** to close the dialog box.

### 4.4.2 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.

## 4.5 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.

#### 4.5.1 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**. A confirmation message appears at the bottom of the dialog box.
5. Click **x** to close the dialog box.

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.

#### 4.5.2 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 **Remove**.

---

---

**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.

## 5 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 do any or all of the following:

- Create users.
- Authorize users (assign roles), including new users created in the same file.
- Deauthorize users (remove roles).
- Disable (terminate) users, including users deauthorized in the same file.

### 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.

## 5.1 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.

## 5.2 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.

## 5.3 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.

## 5.4 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 [Section 5.3, "Check for errors"](#) for additional information or contact Oracle Support for assistance.



## 5.5 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.

## 6 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 My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

---

Oracle Health Sciences Identity and Access Management Service Administrator Guide, Release 1.4.2  
E95436-01

Copyright © 2017, 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

**U.S. GOVERNMENT END USERS:** Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

