Oracle® Cloud

Administering Access Control for Oracle Enterprise Performance Management Cloud

E96250-18

Oracle Cloud Administering Access Control for Oracle Enterprise Performance Management Cloud,

E96250-18

Primary Author: EPM Information Development Team

Contents

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.

Documentation Feedback

To provide feedback on this documentation, click the Feedback button at the bottom of the page in any Oracle Help Center topic. You can also send email to epmdoc_ww@oracle.com.

1 Overview of Access Control

Access to Oracle Enterprise Performance Management Cloud components are controlled by the predefined roles in the identity domain to which users are assigned. Service Administrators can assign users to application-specific rolesof planning, consolidation, and data management applications to enable them to complete additional tasks in an environment.

For example, Service Administrators can assign a user to the Approval Administrator role of a planning or consolidation application to enable the user to perform approvals-related activities.

Additionally, Service Administrators can, from Access Control, create groups comprising identity domain users or other groups. Assigning roles to such groups enables Service Administrators to grant roles to many users at once, thereby reducing administrative overheads.

Assigning roles at the application-level can only enhance the access rights of users; none of the privileges granted by a predefined role can be curtailed by roles assigned at the application-level.

Access Control enables you to complete these activities in an environment:

- Managing Groups
- Assigning Roles to a Group or a User
- Generating a Role Assignment Report for a User or Group
- Viewing the Role Assignment Report For Your Environment
- Viewing the User Login Report

About this Guide

Access Control applies to these Oracle Enterprise Performance Management Cloud business processes:

- Planning
- Planning Modules
- Financial Consolidation and Close
- Tax Reporting
- Profitability and Cost Management
- Account Reconciliation
- Oracle Enterprise Data Management Cloud
- Narrative Reporting
- Oracle Strategic Workforce Planning Cloud
- Oracle Sales Planning Cloud

Opening Access Control

You can assign application-specific roles to groups and users from **Access Control**, which is available in the **Tools** card on the Home Page.

To open Access Control:

1. Access the environment as a Service Administrator.
2. Complete a step:
   - Click (Navigator), and then **Access Control**.
   - Click **Tools** and then **Access Control**.
   - **Oracle Enterprise Data Management Cloud and Narrative Reporting only:** Click **Access Control**.

Managing Groups

Oracle Enterprise Performance Management Cloud uses an internal repository to support role assignments at the application-level and to store information on the groups that you use during the role assignment process.

EPM Cloud users and other groups can be members of groups maintained using Access Control. Users can be granted application roles by assigning a role to the group.

To enable you to view user assignments, Access Control lists the predefined roles as groups. You cannot modify or assign roles to them from Access Control. Additionally, EPM Cloud users, who are assigned to predefined roles, are listed in Access Control so that they can be added as group members. See Understanding Predefined Roles in *Getting Started with Oracle Enterprise Performance Management Cloud for Administrators*.

- Creating Groups
- Modifying Groups
- Deleting Groups

> **Note:**
>
> You can no longer use Access Control to import group information from a file to create groups. Similarly you cannot export group information using Access Control. You may use Migration or EPM Automate commands to export and import groups.

Creating Groups

Only Service Administrators can create and manage groups. Oracle Enterprise Performance Management Cloud users and other groups can be members of a group.

> **Note:**
>
> You may also use Migration or EPM Automate commands to import group information from a file to create groups.

To create groups:

1. Open **Access Control**. See Opening Access Control.
2. In **Manage Groups**, click **Create**.
3. In **Create Group**, complete these steps:
   a. In **Name**, enter a unique group name (maximum 256 characters).

      Group names are not case-sensitive. You cannot use reserved words such predefined role names as group name.
   b. **Optional:** Enter a group description.
4. **Optional:** Add groups to create a nested group.
   a. In **Available Groups**, search for groups. See Using Search for instructions on using the Search feature.

      Groups that match the search criterion are listed under **Available Groups**.
   b. From **Available Groups**, select the member groups for the new group.
   c. Click **Move**.

      The selected groups are listed under **Assigned Groups**. To remove assigned groups, from **Assigned Groups**, select the group to remove, and then click **Remove**.
5. **Optional:** Add EPM Cloud users as members of the group. Only users who are assigned to a predefined role can be added as group members.
   a. Click **Users**.
   b. In **Available Users**, click (**Search**) to locate all the users that you can add as group members. You can search for specific users by entering a partial string from the user name. You do not need to use wildcards in search strings.
   c. From **Available Users**, select the users to add to the group.
   d. Click **Move**.
6. Click **Save**.
7. Click **OK**.

Modifying Groups

Service Administrators can modify group properties, including group name. The application roles assigned to the group and other security assignments are not affected if you rename a group.

To modify groups:

1. Open **Access Control**. See Opening Access Control.
2. **Optional:** In **Manage Groups**, locate the group to modify. See Using Search for instructions on using the Search feature.

   > **Note:**
   >
   > Group names may contain up to 71 characters. However, only the first 34 characters appear in the list displayed in the **Available Groups** column.

3. Click (Action) in the row of the group you want to modify, and then select **Edit.**
4. **Optional:** Modify group name. Changes to the group name does not impact the security assignments made using the group.
5. Modify group assignment:
   a. **Optional:** Add nested groups:
      - In **Available Groups**, search for groups. See Using Search for instructions on using the Search feature.
      - From **Available Groups**, select groups and click **Move**.

        Selected groups are listed in the **Assigned Groups** list.
   b. **Optional:** Remove nested groups:
      - From **Assigned Groups**, select the group to remove.
      - Click **Remove**
6. Modify user assignment:
   a. Click **Users**.
   b. **Optional:** Add users to group:
      - In **Available Users**, click (**Search**) to locate all the users that you can assign as group members. Alternatively, enter a partial string from one of the user attributes (user name, first name, last name or email ID) to find specific users. You do not need to use a wildcards with search strings. For example, using the string `fr` displays user names of Frank, Freddy, and so on. search for users you can add as group members.
      - From **Available Users**, select users and click **Move**.

        Selected users are listed in the **Assigned Users** list.
   c. **Optional:** Remove users from the group:
      - From **Assigned Users**, select the users to remove.

- Click **Remove**.

7. Click **Save**.
8. Click **OK**.

Deleting Groups

Deleting a group does not delete group members.

To delete a group:

1. Open **Access Control**. See Opening Access Control.
2. **Optional:** In **Manage Groups**, search for the group to delete. See Using Search for instructions on using the Search feature.
3. Click (Action) in the row of the group you want to delete, and then select **Delete**.
4. Click **Yes** to confirm the delete operation.
5. Click **OK**.

Importing Group Assignments of Users from a File

Service Administrators can import group assignments of users from a Comma Separated Value (CSV) file to create new assignments in an existing Access Control group. Oracle Enterprise Performance Management Cloud enforces application-level and artifact-level security assignments based on the new group assignments.

> **Note:**
>
> All User Logins identified in the import file must exist in the identity domain; all group name included in the file must exist in Access Control. You cannot create a group using this import process.
> You can only create new group assignments; you cannot remove users' current group assignments.

The import CSV file format can be as shown in the following illustrations:

```
User Login,Group
jdoe, Example_grp1
jane.doe@example.com, Example_grp2
```

```
User Login,First Name,Last Name,Email,Direct,Group
jdoe, John, Doe, jdoe@example.com, Yes, Example_grp1
jane.doe@example.com, Jane, Doe, jane.doe@example.com, No, Example_grp2
```

This format is identical to the CSV version of the User Group report. If you use this format, the import process ignores all columns other than User Login and Group. An easy way to create an import file is to export the current User Group Report and then modify it as needed. See Viewing and Exporting the User Group Report.

To import group assignments of users:

1. Open **Access Control**. See Opening Access Control.
2. Click **User Group Report**.
3. Click **Import from CSV**.
4. Using **Browse** in **Import User Group Assignment CSV**, select the import file.
5. Click **Import**.
6. Click **Yes**.

   On completing the import process, a confirmation dialog box, which identifies the total number of processed assignments and status, is displayed.

Assigning a User to Many Groups

Oracle Enterprise Performance Management Cloud users can be members of many groups maintained using Access Control.

To assign a user to many groups:

1. Open **Access Control**. See Opening Access Control.
2. Click **Manage Users**.

   A list of all users of the current environment is displayed.
3. Search for the user who is to be assigned to groups. See Using Search for instructions on using the Search feature.
4. Click (Action) in the row of the user listing, and then select **Edit**.

   The **Edit User** screen, which lists detailed user information, including current group membership (in **Assigned Groups**), is displayed. On this screen, you can modify group assignments only.
5. Find groups to assign to the user. See Using Search for instructions on using the Search feature.
6. Complete an action:
   - To assign additional groups to the user, from **Available Groups**, select one or more groups and click (**Move**) to move the selected groups to **Assigned Groups**. Alternatively, click (**Move All**) to move all the groups in **Available Groups** to **Assigned Groups**.
   - To remove groups assigned to the user, from **Assigned Groups**, select one or more groups and click (**Remove**) to move the selected groups to **Available Groups**. Alternatively, click (**Remove All**) to move all the groups in **Assigned Groups** to **Available Groups**.
7. Click **Save**.
8. Click **OK**.

Using Search

The intelligent search for user and group artifacts works in an identical manner across Access Control.

You use a string from one of the user attributes (user name, first name, last name or email ID) or the group name or role name to find specific users, groups or roles. You do not need to use wildcards in search strings. For example, using the string `st` to search for groups displays groups such as TestGroup, Strategic_Planner, AnalystsGroup, and so on. Similarly, using the string `jd` to search for users lists users whose user name, first name, last name or email address containing the string `jd`.

To search for users, groups, or roles in Access Control:

1. Access the screen, for example, **Create Group**, where the search feature is available.
2. Find users or groups:
   - To search for a specific group, in the search field for groups, enter a partial string from a group name and then click (Search).
   - To search for a specific user, in the search field for users, enter a partial string from one of the user attributes (user name, first name, last name or email ID), and then click (Search).

2 Managing Role Assignments at the Application Level

Role assignment at the application level is supported for planning, consolidation and close, tax reporting, and Oracle Enterprise Data Management Cloud applications. Planning, consolidation, and Oracle Enterprise Data Management Cloud applications use granular application-specific roles to enhance the access granted through predefined roles while Profitability and Cost Management assigns user and group level data grants to secure access to application data.

Overview

While the overall access rights are controlled by the predefined Oracle Enterprise Performance Management Cloud roles, Service Administrators can grant application-specific roles and data grants to users and to groups created and managed in Access Control. For example, a User, by default, does not have the right to design the approvals process, which is granted only to Power Users and Service Administrators. From Access Control, Service Administrators can assign the Approvals Administrator role to enable the user to perform approvals-related activities.

Role assignments at the application level can only enhance the access rights of users; none of the privileges granted by a predefined role can be curtailed by assigning role at the application-level.

You manage the role assignment process using Access Control. You can perform these tasks:

- Create groups and add EPM Cloud users or other groups as members.
- Add or delete group members
- Assign planning and consolidation application roles to groups or to users
- View a list of users who are members of a group

EPM Cloud Users

You create and manage EPM Cloud users in the identity domain associated with the environment to which the business process belongs. Only the users who are assigned to predefined roles can be assigned application-level roles to enhance the access they have to perform tasks within a business process.

Planning and Consolidation Application Roles

The following roles apply to planning, consolidation, and tax reporting applications only. See *Administering Oracle Profitability and Cost Management Cloud* for information on assigning data grants from the Profitability and Cost Management application.

By default, only Service Administrators and Power Users can access Data Management to work on the data integration process. To enable users with the

User or Viewer identity domain role to participate in the integration process, Service Administrators should assign Data Management roles (Create Integration, Run Integration, and Drill Through) to them.

Approvals Administrator

Resolves approval issues by manually taking ownership of the process. Comprises the Approvals Ownership Assigner, Approvals Process Designer, and Approvals Supervisor roles.

Typically, this role is assigned to business users in charge of a region who need to control the approvals process for the region but do not require the Planning Administrator role. They can perform these tasks:

- Control the approvals process
- Perform actions on Planning units to which they have write access
- Assign owners and reviewers for the organization under their charge
- Change the secondary dimension or update validation rules

Approvals Ownership Assigner

Performs all tasks that users with the Planner role can complete. Additionally, performs the following tasks for any member of the planning unit hierarchy to which the user has write access:

- Assign owners
- Assign reviewers
- Specify users to be notified

Approvals Process Designer

Performs all tasks that users with the Planner and Approvals Ownership Assigner role can complete. Additionally, performs the following tasks for any member of the planning unit hierarchy to which they have write access:

- Change secondary dimensions and members of entities to which the user has write access
- Change the scenario and version assignment for a planning unit hierarchy
- Edit data validation rules of data forms to which the user has access

Approvals Supervisor

Performs the following tasks for any member of the planning unit hierarchy to which the user has write access even if the user does not own the planning unit. This user cannot change data in planning units that the user does not own.

- Stop and start a planning unit
- Take any action on a planning unit

Ad Hoc Grid Creator

Creates, views, modifies, and saves ad hoc grids.

Ad Hoc User

Views and modifies ad-hoc grids and performs ad hoc operations. Ad Hoc Users cannot save ad-hoc grids.

Ad Hoc Read Only User

Performs all ad hoc functions, but cannot write back into ad hoc grids or load data using Data Management.

Mass Allocation

Runs mass allocation rules within form grids.

Task List Access Manager

Assigns tasks to other users.

Create Integration

Uses Data Management to create mappings to integrate data between source and target systems. Users can define data rules with various run time options.

Run Integration

From Data Management, executes data rules with runtime parameters and views execution logs.

Drill Through

Drills through to the source system of the data.

Oracle Enterprise Data Management Cloud Application Roles

These roles apply to Oracle Enterprise Data Management Cloud applications only.

Application Creator

Registers applications in Oracle Enterprise Data Management Cloud. The user who registers an application is assigned Application Owner permission. This user also is assigned as the view owner of the default application view.

Auditor

Views audit related information such as transaction history and requests for changes to data in Oracle Enterprise Data Management Cloud.

View Creator

Creates views in a Oracle Enterprise Data Management Cloud application. The user who creates a view is assigned View Owner permission to the view.

Assigning Roles to a Group or a User

During this process, Service Administrators assign application-level roles to groups and users who are assigned a predefined role.

> **Note:**
>
> You cannot assign application roles to your own user account.
>
> To enable you to view role assignments, Access Control lists the predefined Oracle Enterprise Performance Management Cloud roles as groups. You cannot assign application-level roles to them from Access Control.

To assign application-level roles to a group or a user:

1. Open **Access Control**. See Opening Access Control.
2. Click **Assign Application Roles**.
3. Find a user or group. From the drop down list select **Users** or **Groups**. See Using Search for instructions on using the Search feature.
4. Click (**Actions**) of the user or group, and then select **Assign Roles**.
5. From **Available Roles**, select the roles that you want to assign to the user or group and then click **Move**.

   See these sections :for descriptions of the roles that can be assigned to users and groups.

   - Planning and Consolidation Application Roles
   - Oracle Enterprise Data Management Cloud Application Roles

   Selected roles are listed under **Assigned Roles**. To remove assigned roles, from **Assigned Roles**, select the role to remove, and then click **Remove**.
6. Click **OK**.
7. Click **OK**.

Removing Application-Level Roles Assigned to a Group or a User

This process removes all the application roles that are assigned to the group or to the user. Removal of application-level role assignment does not affect the predefined roles of the user.

To remove the application-level roles of a group or a user:

1. Open **Access Control**. See Opening Access Control.
2. Click **Assign Application Roles**.
3. Find a user or group. From the drop down list select **Users** or **Groups** See Using Search for instructions on using the Search feature.

4. Click (Actions) of the user or group, and then select **Unassign Roles**.
5. Click **Yes**.
6. Click **OK**.

3 Generating Reports

You use these reports to analyze and manage role assignments:

- Generating a Role Assignment Report for a User or Group
- Viewing the Role Assignment Report For Your Environment
- Viewing the User Login Report
- Viewing and Exporting the User Group Report

Report generation time indicated on reports reflects the time based on browser time zone (local system clock).

About the CSV Version of the Report

You can export a report to create a Comma Separated Value (CSV) version of the report. In addition to a count of the number of users assigned to predefined roles, the CSV version of the report lists the following:

- Predefined roles to which each user is assigned. Each predefined role assigned to a user appears in a separate row. Application roles subsumed into predefined roles are not listed.
- Application roles to which a user is assigned either directly or through group. Each application role assigned to a user appears in a separate row.
- Groups to which a users are assigned are not listed if the groups are not assigned to any role.
- Only the information from the current view of the report is exported to CSV. For example, if you filter the report to view the role assignments of a specific user, the exported CSV file contains only the assignments of that user.

Generating a Role Assignment Report for a User or Group

Service Administrators use the Role Assignment Report to review assigned predefined roles and application roles of users. Groups to which a user belong are not listed if the groups are not used to assign application roles to the user. This report enables you to track user access for compliance reporting.

To generate a Role Assignment Report for a user or a group:

1. Open **Access Control**. See Opening Access Control.
2. Click **Assign Application Roles**.
3. Find a user or group. From the drop down list select **Users** or **Groups** See Using Search for instructions on using the Search feature.
4. Click **Action** (**Actions**) of the user or group for which you want to generate the report, and then select **Role Assignment Report**.
5. **Optional**: Click **Export to CSV** to export the report into a CSV file.

6. Click **Close** to close the report.

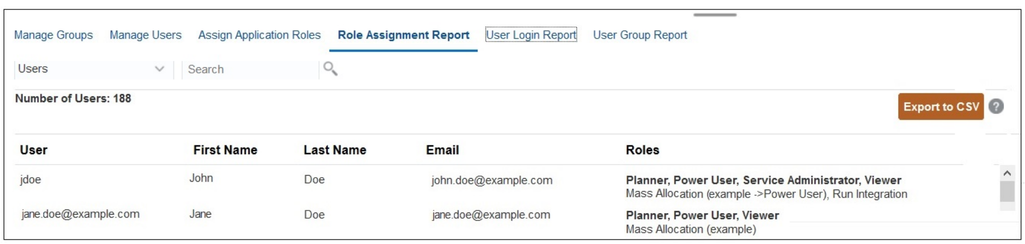
Viewing the Role Assignment Report For Your Environment

Service Administrators use the Role Assignment Report to review the access, assigned through predefined roles and application-level roles, of all users. The report lists the predefined roles (for example, Power User) and application roles (for example, Mass Allocation, which is a Planning application role) assigned to the user.

Inherited roles, as well as information on inheritance, are displayed in one row for each user. For example, assume that user `John Doe` is assigned the `User` predefined role and that `User` is a member of the `example` group to which the `Approvals Administrator` Planning application role is assigned. In this scenario, the Role Assignment Report displays the following as a part of the role assignment information for `John Doe`:

`Approvals Administrator (example->User).`

The Role Assignment Report also identifies the number of users who are authorized to access the environment based on their predefined roles. It does not list the application roles that are subsumed into predefined roles or the component roles of application roles assigned to the user. If you need a report showing such details, you may generate the classic version of the report using the `provisionReport` EPM Automate command. See *Working with EPM Automate for Oracle Enterprise Performance Management Cloud* for detailed information.



You can export the Role Assignment Report as a CSV file, which can then be opened using a program such as Microsoft Excel or saved to your computer. The Role Assignment Report in CSV format uses one row for each role assignment.

	A	B	C	D	E	F
1	User Login	First Name	Last Name	Email	Role	Granted through Group
2	Jdoe	John	Doe	jdoe@example.com	Planner	
3	jdoe	John	Doe	jdoe@example.com	Power User	
4	Jdoe	John	Doe	jdoe@example.com	Service Administrator	
5	jdoe	John	Doe	jdoe@example.com	Viewer	
6	Jdoe	John	Doe	jdoe@example.com	Mass Allocation	example->Power User
7	jdoe	John	Doe	jdoe@example.com	Run Integration	
8	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Planner	
9	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Power User	
10	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Viewer	
11	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Mass Allocation	example

To open the Role Assignment Report:

1. Open **Access Control**. See Opening Access Control.
2. Click **Role Assignment Report**.

The Role Assignment Report is displayed.

3. **Optional**: Filter the report to display the following:
   - Role assignments of a specific user. Select **Users** from the drop down list and then enter a partial search string. See Using Search for instructions on using the Search feature.
   - Users assigned to a specific role. Select **Roles** from the drop down list and then enter a partial role name. See Using Search for instructions on using the Search feature.

   > **Note:**
   >
   > Users may be assigned to many roles. In such cases, the report lists all the roles of the user even if you filer it for a specific role.

4. **Optional**: Click **Export to CSV** to export the report into a CSV file. Note that only the information from the currently displayed report is exported to CSV.

Viewing the User Login Report

The User Login Report, by default, contains information on the users who signed into the environment over the last 24 hours. It lists the IP address of the computer from which the user logged in and the date and time (UTC) at which the user accessed the environment.

Service Administrators can regenerate this report for a custom date range or for the last 30 days, last 90 days, and last 120 days. They can also filter the report to view only the information of specific users by using a partial string of the users' first name, last name or userid as the search string.

> **Note:**
>
> Oracle Enterprise Performance Management Cloud maintains user login audit history for the last 120 days only.

To regenerate the User Login Report:

1. Open **Access Control**. See Opening Access Control.
2. Click **User Login Report**.

   A report that lists all users who signed into the environment over the last day is displayed.
3. Select a period—Last 1 Day, Last 30 Days, Last 90 Days, or Last 120 Days—for which you want to generate the report. To specify a custom date range, select **Date Range** and then select a start date and end date.
4. **Optional:** Select the users to include in the report. See Using Search for instructions on using the Search feature.
5. **Optional**: Click **Export to CSV** to export the displayed report as a CSV file.
6. Click **Cancel** to close the report.

Viewing and Exporting the User Group Report

The User Group Report lists the direct or indirect membership of users assigned to groups in Access Control.

Users are deemed to be direct members of a group if they are assigned to the group; they are considered indirect members if they are assigned to a group which is a child of another group. For each user assigned to a group, the report lists information such as the login ID, first and last name, email ID, and a list of comma separated groups to which the user is directly or indirectly assigned. The CSV version of the report indicates whether the user is directly or indirectly assigned to a group by using `Yes` or `No`.

> **Note:**
>
> This report is not applicable to Account Reconciliation and Narrative Reporting.

To regenerate the User Group Report:

1. Open **Access Control**. See Opening Access Control.
2. Click **User Group Report**.
3. **Optional:** Filter the report. From the drop down list select **Users** or **Groups** See Using Search for instructions on using the Search feature.
4. **Optional**: Click **Export to CSV** to export the report into a CSV file.
5. Click **Cancel** to close the report.