Contents

Documentation Accessibility

Documentation Feedback

1  Overview of Access Control

   About this Guide 1-1
   Opening Access Control 1-2
   Managing Groups 1-2
      Creating Groups 1-2
      Modifying Groups 1-3
      Deleting Groups 1-4
      Exporting Group Information to a File 1-4
      Importing Groups from a File 1-4

2  Managing Application-Level Provisioning

   Planning and Consolidation Application Roles 2-1
   Oracle Enterprise Data Management Cloud Application Roles 2-3
   Provisioning a Group or a User 2-4
   Deprovisioning a Group or a User 2-5

3  Generating Reports

   Generating a Provisioning Report for a User or Group 3-1
   Generating Service-Level Provisioning Report 3-2
   Generating User Login Report 3-3
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, send email to epmdoc_ww@oracle.com, or, in an Oracle Help Center topic, click the Feedback button located beneath the Table of Contents (you may need to scroll down to see the button).

Follow EPM Information Development on these social media sites:

LinkedIn - http://www.linkedin.com/groups?gid=3127051&goback=.gmp_3127051
Twitter - http://twitter.com/hyperionepminfo
Facebook - http://www.facebook.com/pages/Hyperion-EPM-Info/102682103112642
Google+ - https://plus.google.com/106915048672979407731/posts
YouTube - https://www.youtube.com/oracleepminthecloud
Overview of Access Control

Access to service components are controlled by the identity domain role granted to the user. Service Administrators can grant application-specific roles to users of planning, consolidation and data management applications to enable them to complete additional tasks in an environment. For example, Service Administrators can grant the Approval Administrator role of a planning or consolidation application to enable a user to perform approvals-related activities.

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

Application-level provisioning can only enhance the access rights of users; none of the privileges granted by an Oracle Identity Management role can be curtailed by application-level provisioning.

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

- Managing Groups
- Provisioning a Group or a User
- Generating a Provisioning Report for a User or Group
- Generating Service-Level Provisioning Report
- Generating User Login Report

About this Guide

Access Control applies to these Oracle Enterprise Performance Management Cloud services:

- Oracle Planning and Budgeting Cloud
- Oracle Enterprise Planning and Budgeting Cloud
- Oracle Financial Consolidation and Close Cloud
- Oracle Tax Reporting Cloud
- Oracle Profitability and Cost Management Cloud
- Oracle Account Reconciliation Cloud
- Oracle Enterprise Data Management Cloud
- Oracle Enterprise Performance Reporting Cloud
- 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 service 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 Oracle Enterprise Performance Reporting Cloud only: Click Access Control.

Managing Groups

The service uses an internal repository to support application-level provisioning and to store information on the groups that you use during the provisioning process.

Service 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 pre-defined Oracle Enterprise Performance Management Cloud roles as groups. You cannot modify or provision them from Access Control. Additionally, service users, who are assigned to pre-defined roles, are listed in Access Control so that they can be added as group members. See Understanding Pre-defined Roles in Getting Started with Oracle Enterprise Performance Management Cloud for Administrators.

- Creating Groups
- Modifying Groups
- Deleting Groups
- Exporting Group Information to a File
- Importing Groups from a File

Creating Groups

Service users and other groups can be members of a group.

Only Service Administrators can create and manage 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.
b. **Optional:** Enter a group description.

4. **Optional:** Add groups to create a nested group.
   
a. In **Available Groups**, enter a search string and then click (Search) to locate the groups that you can add as group members. Use * (asterisk) as the wildcard to retrieve all available groups.

   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 service users as members of the group. Only users who are assigned to a pre-defined role can be added as group members.
   
a. Click **Users**.
   
b. In **Available Users**, enter a search string and then click (Search) to locate the users (login names) that you can add as group members. Use * (asterisk) as the wildcard to retrieve all available users.
   
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.

To modify groups:

1. Open **Access Control**. See **Opening Access Control**.

2. **Optional:** In **Manage Groups**, enter a search string and then click (Search) to locate the group to modify.

3. Click (Action) in the row of the group you want to modify, and then select **Edit**.

4. Modify group assignment:
   
a. **Optional:** Add nested groups:

      • In **Available Groups**, enter a search string and then click (Search) to locate the groups that you want to add as group members. Use * (asterisk) as the wildcard to retrieve all available groups.

      • 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**.
5. **Modify user assignment:**
   a. Click **Users**.
   b. **Optional:** Add users to group:
      - In **Available Users**, enter a search string and then click (Search) to locate the users that you can assign as group members. Use * (asterisk) as the wildcard to retrieve all available users.
      - 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**.

6. Click **Save**.

7. 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**, enter a search string and then click (Search) to locate the group to delete.
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**.

**Exporting Group Information to a File**

Use this option to export group information to **Groups.csv** file, which you can use while migrating information from the current environment to another; for example from a development environment to a production environment.

To export group information:

1. Open **Access Control**. See **Opening Access Control**.
2. In **Manage Groups**, click **Export**.
3. Follow on-screen instructions to open or save **Groups.csv**.

**Importing Groups from a File**

You can import group information from a Comma Separated Value (.CSV) file to the environment to create groups; for example, to create many groups at once while migrating artifacts across environments.
Group names must be unique, and are not case-sensitive. For example, the name `group1` is considered identical to `GROUP1`. The following is a sample `Groups.csv` file that may be used to create three groups: `group1`, `group2`, and `group3` where `group3` is a nested group within `group1`:

```plaintext
#group,\,,
id,provider,name,description,internal_id
group1,Native Directory,group1,\,,
```

```plaintext
#group_children,\,,
id,group_id,group_provider,user_id,user_provider
group1,group3,Native Directory,\,,
```

To import groups from a file:

1. Open **Access Control**. See **Opening Access Control**.
2. In **Manage Groups**, click **Import**.
3. Using **Browse**, select the .CSV file that contains group information that you want to import.
4. Complete a step:
   - **Click** **Upload**.
   - **Oracle Enterprise Data Management Cloud only**: **Click** **Import**.
Managing Application-Level Provisioning

Overview

Note:
Application-level provisioning is supported for planning, consolidation and close, tax reporting, and Oracle Enterprise Data Management Cloud applications. Planning and consolidation and Oracle Enterprise Data Management Cloud applications use granular application-specific roles to enhance the access privileges granted through identity domain roles while Oracle Profitability and Cost Management Cloud assigns user and group level data grants to secure access to application data.

While the overall access rights are controlled by the pre-defined 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.

Application-level provisioning can only enhance the access rights of users; none of the privileges granted by a pre-defined role can be curtailed by application-level provisioning.

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

• Create groups and add service 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

Service Users

You create and manage service users in the identity domain associated with the environment to which the application 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 applications.

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 Oracle Profitability and Cost Management Cloud 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 grant 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.

Calculation Manager Administrator
Creates, updates, and deletes rules calculation objects. Also redefines launch access rights per the rules and rulesets of the application.

Note:
See Adding, Editing, and Removing Access to Rules in Administering Planning for Oracle Planning and Budgeting Cloud for details on managing access to rules.

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.

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.

Provisioning a Group or a User

During the provisioning process, Service Administrators assign application-level roles to groups and service users who are assigned a pre-defined role.

To provision a group or a user:

1. Open Access Control. See Opening Access Control.
2. Click Provision Roles.
3. Find the user or group to provision. Use * (asterisk) as the wildcard to retrieve all available groups or Oracle Identity Management users.
   - In Search, enter a search string and then click (Search) to locate the user that you want to provision.
   - From the drop down list, select Groups, then in Search, enter a search string, and then click (Search) to locate the group that you want to provision.
4. Click (Action) of the user or group that you want to provision, and then select Provision.
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.

Deprovisioning a Group or a User

Deprovisioning removes all the application roles that are assigned to the group or to the user. Deprovisioning does not affect the Oracle Identity Management roles of the user.

To deprovision a group or a user:

1. Open Access Control. See Opening Access Control.
2. Click Provision Roles.
3. Find the user or group to deprovision. Use * (asterisk) as the wildcard to retrieve all available groups or Oracle Identity Management users.
   - In Search, enter a search string and then click (Search) to locate the user that you want to deprovision.
   - From the drop down list, select Groups, then in Search, enter a search string and then click (Search) to locate the group that you want to deprovision.
4. Click (Action) of the user or group that you want to deprovision, and then select Deprovision.
5. Click Yes.
6. Click OK.
Generating Reports

You use these reports to analyze and manage provisioning:

- Generating a Provisioning Report for a User or Group
- Generating Service-Level Provisioning Report
- Generating User Login Report

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

About the CSV Version of the Provisioning Report

You can export a report to create a CSV version of the report. In addition to the number of provisioned users, the CSV version of the report lists the following:

- Application roles that are mapped to the pre-defined identity domain roles assigned to users. For example, if the user is assigned the Service Administrator role, the CSV version of the report lists one row for each application role mapped to the Service Administrator role.
- Groups to which users are assigned, even if the group is not assigned to any role.

Generating a Provisioning Report for a User or Group

Service Administrators use the Provisioning Report to review assigned pre-defined roles of users. The report also lists the roles assigned indirectly through groups. Groups to which a user belongs are not listed if the groups are not provisioned with an application role.

Provisioning Report enables you to track user access for compliance reporting.

To generate a user or group-level Provisioning Report:

1. Open Access Control. See Opening Access Control.
2. Click Provision Roles.
3. Find user or group for which you want to create provisioning report. Use * (asterisk) as the wildcard to retrieve all available groups or Oracle Identity Management users.
   - In Search, enter a search string and then click (Search) to locate a user.
   - From the drop down list, select Groups, then in Search, enter a search string, and then click (Search) to locate a group.
4. Click Action (Action) of the user or group for which you want to generate the report, and then select Provision Report.
5. Optional: Click Export to CSV to export the report into a Comma Separated Value (CSV) file.
6. Click **Close** to close the report.

**Generating Service-Level Provisioning Report**

Service Administrators use the Provisioning Report to review the access, both service-level and application-level, granted to all users. The report lists the service roles (for example, Service-name Power User) and application roles (for example, Mass Allocation, which is a Planning application role) granted directly to the user using the Provision Roles tab.

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 service-name User role of the service and that service-name user is a member of the example group, which is provisioned with the Approvals Approver Planning application role. In this scenario, the Provisioning Report displays the following as a part of the provisioning information for John Doe:

Approvals Approver (example->service-name User).

The Provisioning Report also identifies the number of provisioned users who are authorized to access the environment.

You can export the Provisioning Report as a Comma Separated Value File, which you can open using a program such as Microsoft Excel or save to your computer. The Provisioning Report in CSV format uses one row for each role assignment.
To open the Provisioning Report:

1. Open **Access Control**. See Opening Access Control.
2. Click **Provisioning Report**.
   The provisioning report is displayed.
3. Optional: Click **Export to CSV** to export the report into a Comma Separated Value (CSV) file.

### Generating User Login Report

The User Login Report contains information on the users who signed into an environment over a specified period of time. It shows the IP address of the computer from which the user logged in and the date and time at which the user accessed the environment.

The service provides you a default User Login Report that lists all users who signed in over the last day. Service Administrators can regenerate this report for a custom date range or for the last 30 days, last 90 days, and last 120 days.

**Note:**

The service 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 service 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. Skip this step if you are generating the report for all users.
   a. In the search box, type a search criterion. Use * (asterisk) as the wild card character in search strings.
   b. Click (Search).

5. **Optional**: Click Export to CSV to export the report into a Comma Separated Value (CSV) file.

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