

Oracle® Fusion Cloud EPM

Administering Access Control



E96250-68



Oracle Fusion Cloud EPM Administering Access Control,

E96250-68

Copyright © 2015, 2026, Oracle and/or its affiliates.

Primary Author: EPM Information Development Team

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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.

Contents

Documentation Accessibility

Documentation Feedback

1 Overview of Access Control

Opening Access Control	1
Managing Groups	2
Creating EPM Groups	3
Editing EPM Groups	4
Deleting EPM Groups	6
Exporting Cloud EPM Groups to a CSV File	6
Importing Group Assignments of Users from a File	6
Assigning a User to Many Groups	7
Using Search	8

2 Managing Granular Roles with Access Control

Mapping Granular Roles with Predefined Roles	2
Account Reconciliation Granular Roles Mapping	2
Enterprise Profitability and Cost Management Granular Roles Mapping	4
Financial Consolidation and Close Granular Roles Mapping	9
FreeForm Granular Roles Mapping	12
Narrative Reporting Granular Roles Mapping	14
Oracle Enterprise Data Management Granular Roles Mapping	15
Planning Granular Roles Mapping	16
Profitability and Cost Management Granular Roles Mapping	19
Tax Reporting Granular Roles Mapping	20
Assigning Granular Roles to a Group or a User	24

3 Generating Reports

Generating a Role Assignment Report for a User or Group	1
---	---

Viewing the Role Assignment Report for the Environment	2
Viewing the User Login Report	3
Viewing the User Group Report	4

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

The Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments are secured with multiple layers of protection. Access is restricted to authorized users using role-based access (predefined roles). Predefined role assignments are managed using the [Oracle Cloud Console](#). For example, to permit user John Doe to view reports belonging to a Planning test environment, he should be assigned to the Viewer role of the environment. For more information, see Understanding Predefined Roles in *Getting Started Guide for Administrators* .

To enable more granular control over the use of Cloud EPM business processes or Cloud EDM, users can further be assigned business process-specific roles through Access Control. These roles, known as granular roles, define permissions within a business process. For example, assigning the Approvals - Administer role in the Planning business process allows a user or group to perform approval-related tasks.

It's important to note that assigning roles at the business process-level will only enhance the user's access rights. These business process specific roles cannot revoke or restrict the privileges granted by predefined roles.

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

- **Manage Groups.** See [Managing Groups](#)
- **Manage Users.** See [Assigning a User to Many Groups](#)
- **Manage Granular Roles.** See [Managing Granular Roles with Access Control](#)
- **Role Assignment Report.** See:
 - [Generating a Role Assignment Report for a User or Group](#)
 - [Viewing the Role Assignment Report for the Environment](#)
- **User Login Report.** See [Viewing the User Login Report](#)
- **User Group Report.** See [Viewing the User Group Report](#)

Access Control for Account Reconciliation provides specific features. For more details, refer to the following topics in *Administering Account Reconciliation*:


- Using Teams
- Managing Users
- Power User Security in Account Reconciliation

Tutorial Link

Follow this tutorial [Setting Up Security in Cloud EPM Business Processes](#) to learn about the layers of security in Cloud EPM business processes and how to manage security using Access Control and access permissions.

Opening Access Control

To open Access Control:

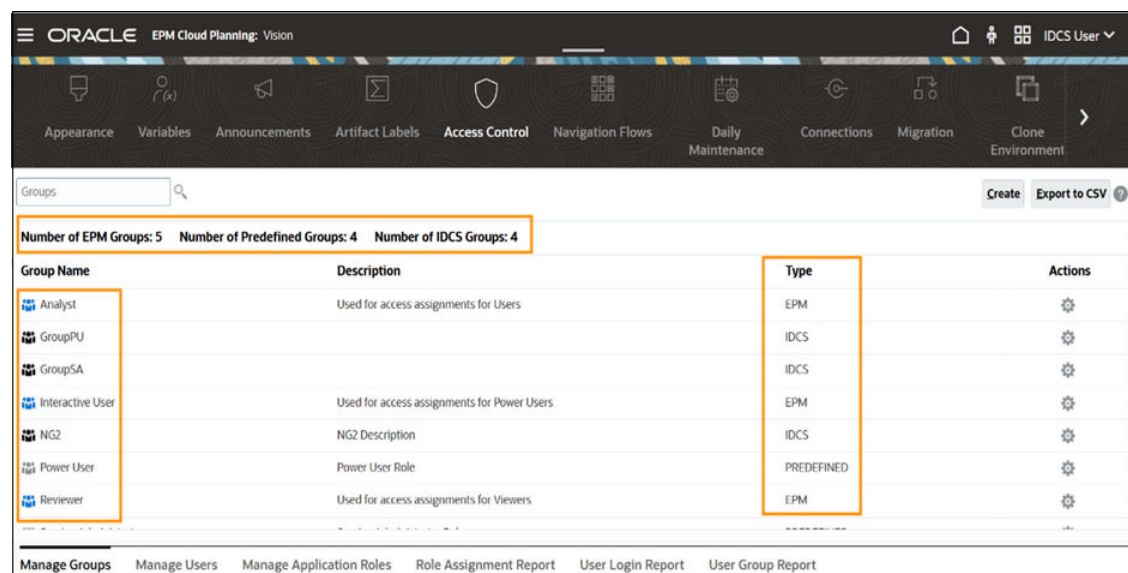
1. Access the environment as a Service Administrator or a user with Access Control - Manage granular role.
2. Complete a step:
 - Click  (Navigator), and then **Access Control**.
 - Click **Tools** and then **Access Control**.
 - **Narrative Reporting only:** Click **Access Control**.

Managing Groups

Oracle Fusion Cloud Enterprise Performance Management recognizes three types of groups:

- **PREDEFINED:** These groups are automatically created for each predefined role. Every user is assigned to a PREDEFINED group based on their predefined role, for example, Power User.
- **EPM:** These groups are created and managed in Access Control. They are not visible in the [Oracle Cloud Console](#).
- **IDCS:** These groups are created and managed in [Oracle Cloud Console](#). They can be synchronized with an external identity provider, such as Okta or Azure AD. IDCS groups are visible in Access Control but they cannot be created or modified here.

In **Manage Groups** tab, groups are categorized by type and image to differentiate easily. To search for a specific group, see [Using Search](#) for instructions.



Group Name	Description	Type	Actions
Analyst	Used for access assignments for Users	EPM	
GroupPU		IDCS	
GroupSA		IDCS	
Interactive User	Used for access assignments for Power Users	EPM	
NG2	NG2 Description	IDCS	
Power User	Power User Role	PREDEFINED	
Reviewer	Used for access assignments for Viewers	EPM	

PREDEFINED Groups

To enable you to view user assignments, Access Control lists the users in predefined roles as PREDEFINED groups.

Key Considerations:



- PREDEFINED groups can be assigned as members of EPM groups.
- PREDEFINED groups are not editable.

To view a PREDEFINED group, select **View** under Actions against that group. You can see a list all the Cloud EPM users assigned to the group.

For more information on predefined roles, see Understanding Predefined Roles in *the Getting Started Guide for Administrators*

EPM Groups

You can use the following options on the **Manage Groups** screen to create and manage EPM groups.

- **Create** button - Creates a new EPM group. See [Creating EPM Groups](#)
- **Export to CSV** button - Exports the EPM groups to a CSV file. See [Exporting Cloud EPM Groups to a CSV File](#)
- **Edit**  (Action) - Edits the EPM Group in the selected row of the group listing. See [Editing EPM Groups](#)
- **Delete**  (Action) - Deletes the EPM Group in the selected row of the group listing. See [Deleting EPM Groups](#)

Key Considerations:

- EPM groups can be assigned as members to larger EPM groups.
- You cannot use Access Control to import group information from a file to create groups. You may use Migration or the createGroups EPM Automate command to import groups.

IDCS Groups

You can use IDCS groups to assign predefined roles to multiple Cloud EPM users. See Using IDCS Groups to Assign Predefined Roles to Users in *Getting Started with Oracle Enterprise Performance Management Cloud for Administrators*

Key Considerations:

- IDCS groups are not editable.
To view an IDCS group, select **View** under Actions against that group. You can see a list of all the Cloud EPM users assigned to the group.
- IDCS groups can be assigned to granular roles and EPM groups.

Caution

If an IDCS group shares its name with an EPM or a PREDEFINED group, or if the name exceeds 256 characters, it will not display in Access Control. It is crucial to understand that users in such IDCS groups won't be able to log in.

Troubleshooting

See Resolving User, Role, and Group Management Issues in the *Operations Guide*.

Creating EPM Groups

Service Administrators or users with Access Control - Manage granular role can create EPM groups. Oracle Fusion Cloud Enterprise Performance Management users and other groups

can be members of a group. You cannot create an IDCS or PREDEFINED group using this option.

Note

You may also use Migration or the createGroups EPM Automate command 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.

Cloud EPM does not allow you to create groups with names identical to an IDCS or a PREDEFINED group.
 - 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 of all types that match the search criterion are listed. By default, this list is sorted by **Group Name** values.
 - 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 Cloud EPM 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**, search for users. See [Using Search](#) for instructions.

Users that match the search criterion are listed. By default, this list is sorted by **User Login** values.
 - c. From **Available Users**, select the users to add to the group.
 - d. Click **Move**.
6. Click **Save**.
7. Click **OK**.

Editing EPM Groups

Service Administrators or users with Access Control - Manage granular role can edit EPM group properties, including group name. The granular roles assigned to the group and other security assignments are not affected if you rename a group.


To edit groups:

1. Open **Access Control**. See [Opening Access Control](#).
2. **Optional:** In **Manage Groups**, locate the group to edit. See [Using Search](#) for instructions on using the Search feature.

Groups of all types that match the search criterion are listed. By default, this list is sorted by **Group Name** values.

 **Note**

Group names may contain up to 256 characters. The visible characters, for example, in the **Available Groups** column, may get truncated based on your screen resolution.


3. Click  (Action) in the row of the group you want to edit, and then select **Edit**.
4. **Optional:** Edit group name. Changes to the group name does not impact the security assignments made using the group. You cannot edit an IDCS or PREDEFINED group, nor can you rename the group using a name that matches an existing IDCS or PREDEFINED group.
5. Edit group assignment:
 - a. **Optional:** Add nested groups:
 - In **Available Groups**, search for groups. See [Using Search](#) for instructions on using the Search feature.
Groups of all types that match the search criterion are listed. By default, this list is sorted by **Group Name** values.
 - 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. Edit user assignment:
 - a. Click **Users**.
 - b. **Optional:** Add users to group:
 - In **Available Users**, search for users that you can assign as group members. See [Using Search](#) for instructions on using the Search feature.
Users that match the search criterion are listed. By default, this list is sorted by **User Login** values.
 - 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 EPM Groups

Service Administrators or users with Access Control - Manage granular role can delete EPM groups. Deleting an EPM group does not delete group members. You cannot delete an IAM or PREDEFINED group using this option.

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.

Groups that match the search criterion are listed. By default, this list is sorted by **Group Name** values.
3. Click  (Action) in the row of the EPM group you want to delete, and then select **Delete**.
4. Click **Yes** to confirm the delete operation.
5. Click **OK**.

Exporting Cloud EPM Groups to a CSV File

Service Administrators or users with Access Control - Manage granular role can export EPM group name and descriptions to `Groups.csv` file using **Export to CSV**. PREDEFINED or IDCS groups cannot be exported using this option.

Export to CSV is disabled if no EPM groups exists. There should be at least one EPM group in Access Control to use this option.

1. Open **Access Control**. See [Opening Access Control](#).

The **Manage Groups** tab lists all available groups.
2. Click **Export to CSV** to export all EPM groups.
3. Follow on-screen instructions to open or save `Groups.csv` file.

Importing Group Assignments of Users from a File

Service Administrators or users with Access Control - Manage granular role can import EPM group assignments of users from a Comma Separated Value (CSV) file to create new assignments in an existing Access Control group. Oracle Fusion Cloud Enterprise Performance Management enforces business process 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 example:

```
User Login,First Name,Last Name,Email,Direct,Group
```

```
jdoe,John,Doe,jdoe@example.com,Yes,AllRole
```

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 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 Fusion Cloud Enterprise Performance Management users can be members of many groups maintained using Access Control. Service Administrators or users with Access Control - Manage granular role can assign a user to many groups.

Note





At any given time, a user can be a member of maximum 1,000 groups either directly or indirectly.

1. Open **Access Control**. See [Opening Access Control](#).
2. Click **Manage Users**.
3. Search for the user who is to be assigned to groups. See [Using Search](#) for instructions on using the Search feature.

Users that match the search criterion are listed. By default, this list is sorted by **User Login** values.
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.

EPM Groups that match the search criterion are listed. By default, this list is sorted by **Group Name** values.
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. For example, using the string `st` to search for groups displays all groups names that contain the string `st`, for example, `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 contain the string `jd`.

The search option does not support wildcards (*).


Note

Some Access Control screens, for example, **Manage Granular Roles**, **Role Assignment Report**, and **User Group Report**, offer you a search choice. Make an appropriate selection before starting a search.

To search for users:

1. Access a screen, for example, **Manage Users**, where the user search feature is available.
2. In the search field, enter a partial string from a user attribute (user name, first name, last name or email ID).
3. Click  (Search).
The search results display all available properties for the users who match the search criterion. By default, this list is sorted by **User Login** values.

To search for groups:

- Access a screen, for example, **Manage Groups**, where the group search feature is available.
- In the search field, enter a partial string from a group name.
- Click  (Search).
The search results display the name and description of groups that match the search criterion. By default, this list is sorted by **Group Name** values.

Create Group

* Name: Example

Description:

Groups **Users**

Available Users

First Name	Last Name	Email	User Login
John	Doe	john.doe@exam...	jdoe
Jane	Doe	jane.doe@exam...	jdoe31
Jane	Doe	jane.x.doe@exam.	jdoe41

Assigned Users

First Name	Last Name	Email	User Login
No records were found.			

To search for users based on their roles in the Role Assignment Report:

- Access the **Role Assignment Report** tab.
- Select **Users** or **Roles** from the search drop down list.
- In the search field, enter a search string.
- Click (Search).
The search results display all available information for the users assigned to the roles that match the search criterion. By default, this list is sorted by **User Login** values.

2

Managing Granular Roles with Access Control

Access Control allows you to extend a Oracle Fusion Cloud Enterprise Performance Management user's access beyond their predefined role by assigning roles at the business process-level. These business process-level roles are referred to as granular roles.

Service Administrators, or user with Access Control - Manage granular role can assign granular roles and data grants to users and to groups created and managed in Access Control.

For example, by default, only Service Administrators and Power Users can access Data Integration. To allow users with the User or Viewer predefined roles to participate in the integration process, Service Administrators can assign Data Integration - Create granular roles to those users.

Note

Granular roles can only extend the user's access. They do not revoke or restrict any privileges granted by a predefined role. To learn more about predefined roles, see Understanding Predefined Roles in the *Getting Started Guide for Administrators*.

Note

If you are migrating business processes from an on-premises environment to Cloud EPM, see Role Mapping for Migrating to Cloud EPM in *Administering Migration*.

Best Practice for Assigning Granular Roles

As a best practice, assign the lowest-level granular role required to provide the necessary additional privileges. Grant granular roles only when a user needs capabilities beyond those provided by their predefined role.

Examples:

- Assign the **Preparer** granular role to a Viewer who needs to prepare reconciliations
- Assign the **Reports - Manage** granular role to a Viewer who designs reports but does not require broader business process functionality
- Assign the **Alert Types - Manage** granular role to a Power User who needs to manage alert definitions.

Note

Granting privileges are additive only. This means that you can add to the privileges that a user's predefined role has, but cannot remove privileges that are automatically given to that predefined role.

Mapping Granular Roles with Predefined Roles

You can map business process-level granular roles with predefined roles for the following business processes:

- [Account Reconciliation Granular Roles Mapping](#)
- [Enterprise Profitability and Cost Management Granular Roles Mapping](#)
- [Financial Consolidation and Close Granular Roles Mapping](#)
- [FreeForm Granular Roles Mapping](#)
- [Narrative Reporting Granular Roles Mapping](#)
- [Oracle Enterprise Data Management Granular Roles Mapping](#)
- [Planning Granular Roles Mapping](#)
- [Profitability and Cost Management Granular Roles Mapping](#)
- [Tax Reporting Granular Roles Mapping](#)

Account Reconciliation Granular Roles Mapping

The following table lists and describes the Account Reconciliation granular roles and shows how they map to predefined roles.

Note

All predefined roles can drill through to Data Exchange detail data based on their data access in Account Reconciliation.

Table 2-1 Account Reconciliation Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Alert Types - Manage	Manages alert types that define procedures to follow when specific issues occur.	Service Administrator
Announcements - Manage	Manages announcements displayed to users on the Welcome Panel, such as notifications for system maintenance or running of jobs.	Service Administrator
Audit - View	Provides access to audit details. This role does not allow users to launch the Reconciliation Actions dialog.	Service Administrator
Currencies - Manage	Configures Currencies, Rate Types, and Currency Buckets. Users with this role can control which currency codes are active in the system.	Service Administrator

Table 2-1 (Cont.) Account Reconciliation Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Dashboards - Manage	Constructs and manages custom dashboards. Users with this role can: <ul style="list-style-type: none"> • Configure Compliance • Add, Edit, Duplicate and Delete • Import and Export 	Service Administrator
Data Integration - Administrator	Performs all functional activities in Data Integration. Users with this role can create, perform, and run: <ul style="list-style-type: none"> • Integrations between source and target systems • Pipeline activities • Extraction and transformation of data and metadata from on-premises sources using the EPM Integration Agent 	Service Administrator
Data Integration - Create	Uses Data Integration to create mappings to integrate data between source and target systems. This role can define data rules with various run time options.	Service Administrator
Data Integration - Run	Users with this role use Data Integration to run an integration between the source and target. If this is the only role assigned to the user, and if they are not a Power User or Service Administrator, they can also view the integration details, but are not able to make any changes.	Service Administrator
Data Loads - Manage	Defines data load definitions in order to load data using Data Integration and save those same data load parameters. Views the latest status of data loads and monitor the processing of user change requests.	Service Administrator
Jobs - View	Views Account Reconciliation jobs and jobs status.	<ul style="list-style-type: none"> • Power User • Service Administrator
Match Types - Manage	Can manage match types, adjustment attributes, support attributes, journal columns, and group attributes.	Service Administrator
Match Types - View	Can view the details of match types, adjustment attributes, support attributes, and journal columns.	Service Administrator
Migrations - Administer	Can: <ul style="list-style-type: none"> • Export snapshots and artifacts from the business process • Import snapshots and artifacts into the business process • Create business processes by migrating snapshots • Delete business processes created through migration • Clone the environment - To clone users and roles, the target user must have both the Identity Domain Administrator and Service Administrator roles • View and adjust the daily maintenance start time and time zone 	Service Administrator
Organizations - Manage	Assigns a hierarchical organizational unit structure to profiles and reconciliations.	Service Administrator
Periods - Manage	Manages the period properties. They can also set the status of the periods, load data and do other operations on the existing periods.	Service Administrator

Table 2-1 (Cont.) Account Reconciliation Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Periods - View	Users with this role can view (read access only) the number of periods associated with the reconciliations, and also load data against the period.	<ul style="list-style-type: none"> Power User Service Administrator
Profiles - View	Users with this role can access profiles for which they have been assigned workflows, aligning with Reconciliations they can view.	<ul style="list-style-type: none"> Power User Service Administrator User
Profiles and Reconciliations - Manage	Manages profiles, reconciliations, and attributes. You can set the security scope for this role in the Power User Security screen.	<ul style="list-style-type: none"> Power User Service Administrator
Public Filters and Views - Manage	Filters control the records that you see in list views and reports. You can apply filters against profiles, reconciliations, or reconciliation transaction attributes, including system attributes, balances, and balance details. Users with this role can create complex filters and logics to determine the order in which filters are applied.	Service Administrator
Reconciliation - Commentator	View the reconciliations and add comments to the reconciliation or to transactions of the reconciliation.	<ul style="list-style-type: none"> Power User Service Administrator User
Reconciliation - Preparer	Users with this role prepare Reconciliations, assign panels, import pre-mapped data, and add attachments to submit, claim and release reconciliations.	<ul style="list-style-type: none"> Power User Service Administrator User
Reconciliation - Reviewer	Users with this role review reconciliations, assign panels and add attachments to approve, reject, claim, and release reconciliations.	<ul style="list-style-type: none"> Power User Service Administrator User
Reports - Manage	Configures the business process settings to display reconciliation reports.	Service Administrator
Teams - Manage	Users with this role may add, edit or remove teams, and manage members of the teams.	<ul style="list-style-type: none"> Power User Service Administrator
Users - Manage	Users with this role can manage members of the teams.	<ul style="list-style-type: none"> Power User Service Administrator

Enterprise Profitability and Cost Management Granular Roles Mapping

The following table lists and describes the Enterprise Profitability and Cost Management granular roles and shows how they map to predefined roles.

Table 2-2 Enterprise Profitability and Cost Management Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Ad Hoc - Create	Creates, views, modifies, and saves ad hoc grids.	Power User
Ad Hoc - Read Only User	Performs all ad hoc functions but cannot write back into ad hoc grids or load data using Data Management.	Unmapped. See footnote
Ad Hoc - User	Views and modifies ad-hoc grids and performs ad hoc operations. Ad Hoc Users cannot save ad-hoc grids.	User
Application - Mass Allocate	Runs mass allocation rules within form grids.	Service Administrator
Announcements - Manage	Manages announcements that are displayed to users on the Welcome Panel. These may indicate upcoming events, such as system maintenance or the running of jobs.	Service Administrator
Approvals - Administer	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 Service Administrator role. They can perform these tasks: <ul style="list-style-type: none"> 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 	Service Administrator
Approvals - Assign Ownerships	Performs the following tasks for any member of the planning unit hierarchy to which the user has write access: <ul style="list-style-type: none"> Assign owners Assign reviewers Specify users to be notified 	Power User

Table 2-2 (Cont.) Enterprise Profitability and Cost Management Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Approvals - Design Process	Includes Approvals Ownership Assigner role. Additionally, performs the following tasks for any member of the planning unit hierarchy to which they have write access: <ul style="list-style-type: none"> 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 	Unmapped. See footnote
Approvals - Supervise	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. <ul style="list-style-type: none"> Stop and start a planning unit Take any action on a planning unit 	Power User
Audit - Manage	Can view and delete the audit records.	Service Administrator
Audit - View	Can view audit records.	Unmapped. See footnote
Calculation - Run	Calculates a model in the Calculation Control page.	<ul style="list-style-type: none"> Power User Service Administrator User
Calculation History - Delete	Deletes a selected instance of a completed calculation from the Calculation Analysis page. Deleting calculation history does not delete any data. It merely deletes the recorded instance of a calculation that was run.	<ul style="list-style-type: none"> Power User Service Administrator User
Calculation History - View	Views completed calculations from the Calculation Analysis page.	<ul style="list-style-type: none"> Power User Service Administrator User
Dashboards - Manage	Constructs and manages planning and operational dashboards. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete dashboards based on permissions set on them Import and export dashboards 	Service Administrator
Data Integration - Administrator	Performs all functional activities in Data Integration. Users with this role can create, perform, and run: <ul style="list-style-type: none"> Integrations between source and target systems Pipeline activities Extraction and transformation of data and metadata from on-premises sources using the EPM Integration Agent 	Service Administrator
Data Integration - Create	Uses Data Integration to create mappings to integrate data between source and target systems. Users can define data rules with various run time options.	Power User

Table 2-2 (Cont.) Enterprise Profitability and Cost Management Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Data Integration - Drill Through	Drills through to the source system of the data.	<ul style="list-style-type: none"> Power User User
Data Integration - Run	Users with this role use Data Integration to run an integration between the source and target. If this is the only role assigned to the user, and if they are not a Power User or Service Administrator, they can also view the integration details, but are not able to make any changes.	Power User
Documents - Manage	Constructs and manages documents. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete documents based on the permissions set on them Import and export documents 	Service Administrator
IPM - Manage	Manages and configures Intelligent Performance Management (IPM) jobs including Insights, Auto Predict, and Advanced Prediction. Users with this role: <ul style="list-style-type: none"> Can view, edit, and manage only the jobs they have created Cannot view or manage jobs created by other users 	Service Administrator
Jobs - Manage	Can view and delete job status records for any user.	Service Administrator
Jobs - View	Can view job status records for all users in the environment, but can only delete their own job status records.	Unmapped. See footnote
Model - Create	Creates a new model in the Modeling page.	<ul style="list-style-type: none"> Power User Service Administrator
Model - Delete	Deletes a model in the Modeling page. Deleting a model will also delete all of the rules in the model.	Service Administrator
Model - View	Views models and their associated rules in the Designer page.	<ul style="list-style-type: none"> Power User Service Administrator User Viewer
Model Validation - Run	Validates models in the Model Validation page.	<ul style="list-style-type: none"> Power User Service Administrator User
POV - Create	Creates a new point of view in the Calculation Control page.	<ul style="list-style-type: none"> Power User Service Administrator
POV - Delete	Deletes a point of view in the Calculation Control page. Deleting a point of view will also delete the associated data, as well as the calculation history page for that point of view. It also removes the point of view from the Calculation Control page.	Service Administrator

Table 2-2 (Cont.) Enterprise Profitability and Cost Management Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
POV Data - Clear	Clears data from a point of view in the Calculation Control page without removing the point of view.	<ul style="list-style-type: none"> Power User Service Administrator
POV Data - Copy	Copies data from one point of view to another in the Calculation Control page.	<ul style="list-style-type: none"> Power User Service Administrator
POV Status - Edit	Changes the status of a point of view from the Edit Point of View dialog box in the Calculation Control page. The available statuses for a point of view are Draft, Published, and Archived.	Service Administrator
Profit Curve - Create	Creates profit curves on the Profit Curves tab in the Intelligence cluster.	<ul style="list-style-type: none"> Power User Service Administrator
Profit Curve - Edit	Edits profit curves on the Profit Curves tab in the Intelligence cluster.	<ul style="list-style-type: none"> Power User Service Administrator
Profit Curve - Run	Runs profit curves on the Profit Curves tab in the Intelligence cluster.	<ul style="list-style-type: none"> Power User Service Administrator User Viewer
Reports - Manage	Constructs and manages reporting artifacts (reports, snapshots, books and bursting definitions). Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete reporting artifacts based on permissions set Import and export reporting artifacts 	Service Administrator
Rule - Create / Edit	Creates or edits an Allocation Rule, Custom Calculation Rule, or Rule Set in the Designer page.	<ul style="list-style-type: none"> Power User Service Administrator User
Rule - Delete	Deletes an Allocation Rule, Custom Calculation Rule, or Rule Set in the Designer page.	<ul style="list-style-type: none"> Power User Service Administrator User
Rule Balancing - Run	Views the Rule Balancing report to see the impact of each rule.	<ul style="list-style-type: none"> Power User Service Administrator User
Rules - Mass Edit	Accesses the Mass Edit tab in the Designer page to make edits to multiple rules at once.	<ul style="list-style-type: none"> Power User Service Administrator User
Trace Allocation - Run	Traces allocation amounts on the Trace Allocations tab of the Intelligence cluster.	<ul style="list-style-type: none"> Power User Service Administrator User Viewer

Table 2-2 (Cont.) Enterprise Profitability and Cost Management Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Footnote: This role is not mapped to any predefined role and requires assignment to users or groups to activate it.		

Financial Consolidation and Close Granular Roles Mapping

The following table lists and describes the Financial Consolidation and Close granular roles and shows how they map to predefined roles.

Table 2-3 Financial Consolidation and Close Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Ad Hoc - Create	Creates, views, modifies, and saves ad hoc grids.	Power User
Ad Hoc - Read Only User	Performs all ad hoc functions, but cannot write back into ad hoc grids or load data using Data Management.	Unmapped. See footnote
Ad Hoc - User	Views and modifies ad-hoc grids and performs ad hoc operations. Ad Hoc Users cannot save ad-hoc grids.	User
Announcements - Manage	Constructs and manages announcements. Users with this role can add, edit, duplicate and delete announcements.	Service Administrator
Application - Mass Allocate	Runs mass allocation rules within form grids.	Service Administrator

Table 2-3 (Cont.) Financial Consolidation and Close Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Approvals - Administer	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 Service Administrator role. They can perform these tasks: <ul style="list-style-type: none"> 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 	Service Administrator
Approvals - Assign Ownerships	Performs the following tasks for any member of the planning unit hierarchy to which the user has write access: <ul style="list-style-type: none"> Assign owners Assign reviewers Specify users to be notified 	Power User
Approvals - Design Process	Includes Approvals Ownership Assigner role. Additionally, performs the following tasks for any member of the planning unit hierarchy to which they have write access: <ul style="list-style-type: none"> 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 	Unmapped. See footnote
Approvals - Supervise	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. <ul style="list-style-type: none"> Stop and start a planning unit Take any action on a planning unit 	Power User
Audit - Manage	Can view and delete the audit records.	Service Administrator
Audit - View	Can view audit records.	Unmapped. See footnote
Consolidation Journals - Approve	Approve a consolidation journal that has been submitted for approval or reject a submitted journal.	Unmapped. See footnote
Consolidation Journals - Auto-Post after Approval	Allows a consolidation journal to be automatically posted after the approver has approved it. The user who approved the journal will also be the posting user.	Unmapped. See footnote
Consolidation Journals - Create	Create, modify, and delete consolidation journals and consolidation journal templates.	Unmapped. See footnote

Table 2-3 (Cont.) Financial Consolidation and Close Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Consolidation Journals - Manage Periods	Open time periods for consolidation journals or close journal time periods. If there are Approved journals or unposted Auto-reversal journals in the period, you cannot close it. If you select to close a period that contains Working or Submitted journals, a warning message is displayed that non-posted journals were found for the period, but you can close it.	Unmapped. See footnote
Consolidation Journals - Post	Post a consolidation journal that has been completed or submitted and approved. You must first open the time period for each scenario to which consolidation journals are to be posted.	Unmapped. See footnote
Consolidation Journals - Submit	Submit a consolidation journal for approval or reject a consolidation journal with Completed status.	Unmapped. See footnote
Consolidation Journals - Un-Post	Unpost a consolidation journal. You must have Write access to the members in the journal.	Unmapped. See footnote
Dashboards - Manage	Constructs and manages all dashboards, including operational dashboards. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete dashboards Import and export dashboards 	<ul style="list-style-type: none"> Service Administrator Power User
Data Integration - Administrator	Performs all functional activities in Data Integration. Users with this role can create, perform, and run: <ul style="list-style-type: none"> Integrations between source and target systems Pipeline activities Extraction and transformation of data and metadata from on-premises sources using the EPM Integration Agent 	Service Administrator
Data Integration - Create	Uses Data Integration to create mappings to integrate data between source and target systems. Users can define data rules with various run time options.	Power User
Data Integration - Drill Through	Drills through to the source system of the data.	<ul style="list-style-type: none"> Power User User
Data Integration - Run	Users with this role use Data Integration to run an integration between the source and target. If this is the only role assigned to the user, and if they are not a Power User or Service Administrator, they can also view the integration details, but are not able to make any changes.	Power User
Documents - Manage	Constructs and manages documents. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete documents based on the permissions set on them Import and export documents 	Service Administrator
Jobs - Manage	Can view and delete job status records for any user.	Service Administrator
Jobs - View	Can view job status records for all users in the environment, but can only delete their own job status records.	Unmapped. See footnote

Table 2-3 (Cont.) Financial Consolidation and Close Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Reports - Manage	Constructs and manages reporting artifacts (reports, snapshots, books and bursting definitions). Users with this role can: <ul style="list-style-type: none"> • Add, edit, duplicate and delete reporting artifacts based on permissions set • Import and export reporting artifacts 	Service Administrator
Task List - Manage Access	Assigns tasks to other users.	Power User
Task Manager - Approver	Eligible to be an approver on tasks from Task Manager	<ul style="list-style-type: none"> • Power User • Service Administrator • User
Task Manager - Artifacts - Manage	Manages all Task Manager artifacts such as alerts, currencies, and organization	Service Administrator
Task Manager - Assignee	Eligible to be an assignee on tasks from Task Manager	<ul style="list-style-type: none"> • Power User • Service Administrator • User
Task Manager - Audit - View	Views the audit history information	Service Administrator
Task Manager - Custom Reports - Manage	Designs custom reports	Service Administrator
Task Manager - Operational Dashboards - Manage	Configures operational dashboard	Service Administrator
Task Manager - Public Filters and Views - Manage	Publishes filters and views to make them accessible to all	<ul style="list-style-type: none"> • Power User • Service Administrator
Task Manager - System Services and Settings - Manage	Defines the system services and system settings for a business process	Service Administrator
Task Manager - Tasks - Manage	Designs and manages the tasks, templates, and schedules	<ul style="list-style-type: none"> • Power User • Service Administrator
Task Manager - Users and Teams - Manage	Manages Users and Teams	<ul style="list-style-type: none"> • Power User • Service Administrator
Footnote: This role is not mapped to any predefined role and requires assignment to users or groups to activate it.		

FreeForm Granular Roles Mapping

The following table lists and describes the FreeForm granular roles and shows how they map to predefined roles.

Note

Roles within the business process that lack mapping to predefined roles require individual assignments to users or groups. Without such assignments, users are unable to engage in activities related to their granular roles. For instance, the *Ad Hoc - Read Only User* role, which is not associated with any granular role in the subsequent table, needs to be explicitly granted to a user to activate its features. This functionality is not automatically included in any predefined role.

Table 2-4 FreeForm Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Ad Hoc - Create	Creates, views, modifies, and saves ad hoc grids.	Power User
Ad Hoc - Read Only User	Performs all ad hoc functions, but cannot write back into ad hoc grids or load data using Data Management.	Unmapped. See footnote
Ad Hoc - User	Views and modifies ad-hoc grids and performs ad hoc operations. Ad Hoc Users cannot save ad-hoc grids.	User
Announcements - Manage	Constructs and manages announcements. Users with this role can add, edit, duplicate and delete announcements.	Service Administrator
Application - Mass Allocate	Runs mass allocation rules within form grids.	Service Administrator
Audit - Manage	Can view and delete the audit records.	Service Administrator
Audit - View	Can view audit records.	Unmapped. See footnote
Data Integration - Administrator	Performs all functional activities in Data Integration. Users with this role can create, perform, and run: <ul style="list-style-type: none"> Integrations between source and target systems Pipeline activities Extraction and transformation of data and metadata from on-premises sources using the EPM Integration Agent 	Service Administrator
Data Integration - Create	Uses Data Integration to create mappings to integrate data between source and target systems. Users can define data rules with various run time options.	Power User
Data Integration - Drill Through	Drills through to the source system of the data.	<ul style="list-style-type: none"> Power User User

Table 2-4 (Cont.) FreeForm Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Data Integration - Run	Users with this role use Data Integration to run an integration between the source and target. If this is the only role assigned to the user, and if they are not a Power User or Service Administrator, they can also view the integration details, but are not able to make any changes.	Power User
Dashboards - Manage	Constructs and manages planning and operational dashboards. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete dashboards based on permissions set on them Import and export dashboards 	Service Administrator
Documents - Manage	Constructs and manages documents. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete documents based on the permissions set on them Import and export documents 	Service Administrator
IPM - Manage	Manages and configures Intelligent Performance Management (IPM) jobs including Insights, Auto Predict, and Advanced Prediction. Users with this role: <ul style="list-style-type: none"> Can view, edit, and manage only the jobs they have created Cannot view or manage jobs created by other users 	Service Administrator
Jobs - Manage	Can view and delete job status records for any user.	Service Administrator
Jobs - View	Can view job status records for all users in the environment, but can only delete their own job status records.	Unmapped. See footnote
Reports - Manage	Constructs and manages reporting artifacts (reports, snapshots, books and bursting definitions). Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete reporting artifacts based on permissions set Import and export reporting artifacts 	Service Administrator
Task List - Manage Access	Assigns tasks to other users.	Power User
Footnote: This role is not mapped to any predefined role and requires assignment to users or groups to activate it.		

Narrative Reporting Granular Roles Mapping

The following table lists and describes the Narrative Reporting granular roles and shows how they map to predefined roles.

Table 2-5 Narrative Reporting Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Library - Administer	Creates folders, including root-level folders.	<ul style="list-style-type: none"> • Library Administrator • Power User • Service Administrator
Report - Administer	Creates report packages, reports, books and bursting definitions.	<ul style="list-style-type: none"> • Power User • Report Administrator • Service Administrator

Oracle Enterprise Data Management Granular Roles Mapping

The following table lists and describes the Oracle Enterprise Data Management granular roles and shows how they map to predefined roles.

Table 2-6 Oracle Enterprise Data Management Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Application - Create	Registers business processes in Oracle Enterprise Data Management. The user who registers a business process is assigned Application Owner permission. This user also is assigned as the view owner of the default business process view.	Service Administrator
Audit	Views audit related information such as transaction history and requests for changes to data in Oracle Enterprise Data Management.	Service Administrator

Table 2-6 (Cont.) Oracle Enterprise Data Management Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Migrations - Administer	<p>Can:</p> <ul style="list-style-type: none"> Export snapshots and artifacts from the business process Import snapshots and artifacts into the business process Create business processes by migrating snapshots Delete business processes created through migration Clone the environment - To clone users and roles, the target user must have both the Identity Domain Administrator and Service Administrator roles View and adjust the daily maintenance start time and time zone 	Service Administrator
Views - Create	Users with this role can create Views to work with metadata. They are the default Owners so they have the ability to grant other users permission to the Views as well. They retain the privilege to edit or delete the View.	Service Administrator

Planning Granular Roles Mapping

The following table lists and describes the Planning granular roles and shows how they map to predefined roles.

Planning business process types includes Custom, FreeForm, Planning Modules, Predictive Cash Forecasting, Strategic Workforce Planning, and Sales Planning.

Table 2-7 Planning Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Ad Hoc - Create	Creates, views, modifies, and saves ad hoc grids.	Power User
Ad Hoc - Read Only User	Performs all ad hoc functions, but cannot write back into ad hoc grids or load data using Data Management.	Unmapped. See footnote

Table 2-7 (Cont.) Planning Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Ad Hoc - User	Views and modifies ad-hoc grids and performs ad hoc operations. Ad Hoc Users cannot save ad-hoc grids.	User
Announcements - Manage	Constructs and manages announcements. Users with this role can add, edit, duplicate and delete announcements.	Service Administrator
Application - Mass Allocate	Runs mass allocation rules within form grids.	Service Administrator
Approvals - Administer	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 Service Administrator role. They can perform these tasks: <ul style="list-style-type: none"> 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 	Service Administrator
Approvals - Assign Ownerships	Performs the following tasks for any member of the planning unit hierarchy to which the user has write access: <ul style="list-style-type: none"> Assign owners Assign reviewers Specify users to be notified 	Power User
Approvals - Design Process	Includes Approvals Ownership Assigner role. Additionally, performs the following tasks for any member of the planning unit hierarchy to which they have write access: <ul style="list-style-type: none"> 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 	Unmapped. See footnote
Approvals - Supervise	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. <ul style="list-style-type: none"> Stop and start a planning unit Take any action on a planning unit 	Power User
Audit - Manage	Can view and delete the audit records.	Service Administrator
Audit - View	Can view audit records.	Unmapped. See footnote

Table 2-7 (Cont.) Planning Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Dashboards - Manage	Constructs and manages planning and operational dashboards. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete dashboards based on permissions set on them Import and export dashboards 	Service Administrator
Data Integration - Administrator	Performs all functional activities in Data Integration. Users with this role can create, perform, and run: <ul style="list-style-type: none"> Integrations between source and target systems Pipeline activities Extraction and transformation of data and metadata from on-premises sources using the EPM Integration Agent 	Service Administrator
Data Integration - Create	Uses Data Integration to create mappings to integrate data between source and target systems. Users can define data rules with various run time options.	Power User
Data Integration - Drill Through	Drills through to the source system of the data.	<ul style="list-style-type: none"> Power User User
Data Integration - Run	Uses Data Integration to run an integration between the source and target systems. If this is the only role assigned to the user, and if they are not a Power User or Service Administrator, they can also view the integration details, but are not able to make any changes.	Power User
Documents - Manage	Constructs and manages documents. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete documents based on the permissions set on them Import and export documents 	Service Administrator
IPM - Manage	Manages and configures Intelligent Performance Management (IPM) jobs including Insights, Auto Predict, and Advanced Prediction. Users with this role: <ul style="list-style-type: none"> Can view, edit, and manage only the jobs they have created Cannot view or manage jobs created by other users 	Service Administrator
Jobs - Manage	Can view and delete job status records for any user.	Service Administrator
Jobs - View	Can view job status records for all users in the environment, but can only delete their own job status records.	Unmapped. See footnote
Reports - Manage	Constructs and manages reporting artifacts (reports, snapshots, books and bursting definitions). Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete reporting artifacts based on permissions set Import and export reporting artifacts 	Service Administrator
Task List - Manage Access	Assigns tasks to other users.	Power User

Table 2-7 (Cont.) Planning Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Task Manager - Approver	Eligible to be an approver on tasks from Task Manager	<ul style="list-style-type: none"> Service Administrator Power User User
Task Manager - Artifacts - Manage	Manages all Task Manager artifacts such as alerts, currencies, and organization	Service Administrator
Task Manager - Assignee	Eligible to be an assignee on tasks from Task Manager	<ul style="list-style-type: none"> Power User Service Administrator User
Task Manager - Audit - View	Views the audit history information	Service Administrator
Task Manager - Custom Reports - Manage	Designs custom reports	Service Administrator
Task Manager - Operational Dashboards - Manage	Configures operational dashboards	Service Administrator
Task Manager - Public Filters and Views - Manage	Publishes filters and views to make them accessible to all	<ul style="list-style-type: none"> Power User Service Administrator
Task Manager - System Services and Settings - Manage	Defines the system services and system settings for a business process	Service Administrator
Task Manager - Tasks - Manage	Designs and manages the tasks, templates, and schedules	<ul style="list-style-type: none"> Power User Service Administrator
Task Manager - Users and Teams - Manage	Manages Users and Teams	<ul style="list-style-type: none"> Power User Service Administrator
Footnote: This role is not mapped to any predefined role and requires assignment to users or groups to activate it.		

Profitability and Cost Management Granular Roles Mapping

The following table lists and describes the Profitability and Cost Management granular roles and shows how they map to predefined roles.

Table 2-8 Profitability and Cost Management Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator

Table 2-8 (Cont.) Profitability and Cost Management Granular Roles and Predefined Roles Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Data Integration - Administrator	Performs all functional activities in Data Integration. Users with this role can create, perform, and run: <ul style="list-style-type: none"> Integrations between source and target systems Pipeline activities Extraction and transformation of data and metadata from on-premises sources using the EPM Integration Agent 	Service Administrator
Migrations - Administer	Can: <ul style="list-style-type: none"> Export snapshots and artifacts from the business process Import snapshots and artifacts into the business process Create business processes by migrating snapshots Delete business processes created through migration Clone the environment - To clone users and roles, the target user must have both the Identity Domain Administrator and Service Administrator roles View and adjust the daily maintenance start time and time zone 	Service Administrator

Tax Reporting Granular Roles Mapping

The following table lists and describes the Tax Reporting granular roles and shows how they map to predefined roles.

Note

Roles within the business process that lack mapping to predefined roles require individual assignments to users or groups. Without such assignments, users are unable to engage in activities related to their granular roles. For instance, the *Ad Hoc - Read Only User* role, which is not associated with any predefined role in the subsequent table, needs to be explicitly granted to a user to activate its features. This functionality is not automatically included in any predefined role.

Table 2-9 Tax Reporting Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Access Control - Manage	Performs all Access Control activities including managing groups, assigning granular roles to users and groups, and generating and viewing available reports.	Service Administrator
Access Control - View	Generates and views user security-related reports such as the Role Assignment Report, User Login Report, Group Assignment Report, and User Group Report. Users with this role cannot assign granular roles, manage groups, or modify Access Control settings.	Service Administrator
Ad Hoc - Create	Creates, views, modifies, and saves ad hoc grids.	Power User
Ad Hoc - Read Only User	Performs all ad hoc functions, but cannot write back into ad hoc grids or load data using Data Management.	Unmapped. See footnote
Ad Hoc - User	Views and modifies ad-hoc grids and performs ad hoc operations. Ad Hoc Users cannot save ad-hoc grids.	User
Announcements - Manage	Manages announcements that are displayed to users on the Welcome Panel. These may indicate upcoming events, such as system maintenance or the running of jobs.	Power User
Application - Mass Allocate	Runs mass allocation rules within form grids.	Service Administrator
Approvals - Administer	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 Service Administrator role. They can perform these tasks: <ul style="list-style-type: none"> 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 	Service Administrator
Approvals - Assign Ownerships	Performs the following tasks for any member of the planning unit hierarchy to which the user has write access: <ul style="list-style-type: none"> Assign owners Assign reviewers Specify users to be notified 	Power User

Table 2-9 (Cont.) Tax Reporting Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Approvals - Design Process	Includes Approvals Ownership Assigner role. Additionally, performs the following tasks for any member of the planning unit hierarchy to which they have write access: <ul style="list-style-type: none"> 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 	Unmapped. See footnote
Approvals - Supervise	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. <ul style="list-style-type: none"> Stop and start a planning unit Take any action on a planning unit 	Power User
Audit - Manage	Can view and delete the audit records.	Service Administrator
Audit - View	Can view audit records.	Unmapped. See footnote
Dashboards - Manage	Constructs and manages custom dashboards. Users with this role can: <ul style="list-style-type: none"> Configure Compliance Add, Edit, Duplicate and Delete Import and Export 	Service Administrator
Data Integration - Administrator	Performs all functional activities in Data Integration. Users with this role can create, perform, and run: <ul style="list-style-type: none"> Integrations between source and target systems Pipeline activities Extraction and transformation of data and metadata from on-premises sources using the EPM Integration Agent 	Service Administrator
Data Integration - Create	Uses Data Integration to create mappings to integrate data between source and target systems. Users can define data rules with various run time options.	Power User
Data Integration - Drill Through	Drills through to the source system of the data.	<ul style="list-style-type: none"> Power User User
Data Integration - Run	Users with this role use Data Integration to run an integration between the source and target. If this is the only role assigned to the user, and if they are not a Power User or Service Administrator, they can also view the integration details, but are not able to make any changes.	Power User
Documents - Manage	Constructs and manages documents. Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete documents based on the permissions set on the documents Import and export documents 	Service Administrator
Jobs - Manage	Can view and delete job status records for any user.	Service Administrator

Table 2-9 (Cont.) Tax Reporting Granular Roles and Predefined Role Mapping

Granular Role	Description	Included in this Predefined Role
Jobs - View	Can view job status records for all users in the environment, but can only delete their own job status records.	Unmapped. See footnote
Reports - Manage	Constructs and manages reporting artifacts (reports, snapshots, books and bursting definitions). Users with this role can: <ul style="list-style-type: none"> Add, edit, duplicate and delete reporting artifacts based on permissions set Import and export reporting artifacts 	Service Administrator
Task List - Manage Access	Assigns tasks to other users.	Power User
Task Manager - Approver	Eligible to be an approver on tasks from Task Manager	<ul style="list-style-type: none"> Power User Service Administrator User
Task Manager - Artifacts - Manage	Manages all Task Manager artifacts such as alerts, currencies, and organization	Service Administrator
Task Manager - Assignee	Eligible to be an assignee on tasks from Task Manager	<ul style="list-style-type: none"> Power User Service Administrator User
Task Manager - Audit - View	Views the audit history information	Service Administrator
Task Manager - Custom Reports - Manage	Designs the custom reports	Service Administrator
Task Manager - Operational Dashboards - Manage	Configures the dashboard	Service Administrator
Task Manager - Public Filters and Views - Manage	Publishes filters and views to make them accessible to all	<ul style="list-style-type: none"> Power User Service Administrator
Task Manager - System Services and Settings - Manage	Defines the system services and system settings for a business process	Service Administrator
Task Manager - Tasks - Manage	Designs and manages the tasks, templates, and schedules	<ul style="list-style-type: none"> Power User Service Administrator
Task Manager - Users and Teams - Manage	Manages Users and Teams	<ul style="list-style-type: none"> Power User Service Administrator
Footnote: This role is not mapped to any predefined role and requires assignment to users or groups to activate it.		

Assigning Granular Roles to a Group or a User


During this process, Service Administrators or users with Access Control - Manage granular role can assign or unassign granular roles to EPM and IDCS groups and users who have a predefined role. They can also assign granular roles to themselves.

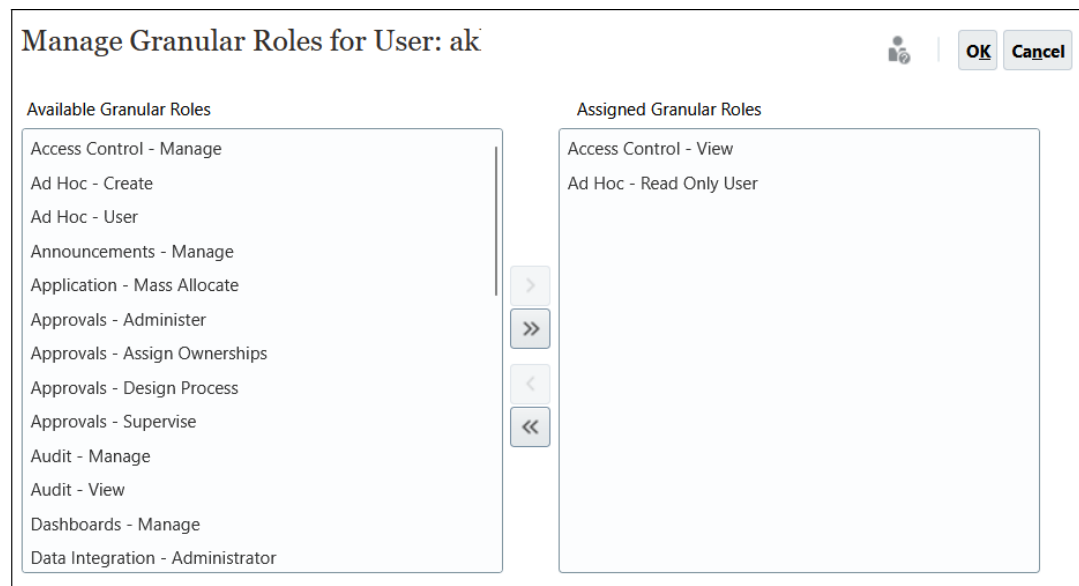
For information on groups and assigned users to groups, see [Managing Groups](#).

To assign or unassign granular roles to a group or a user:

1. Open **Access Control**. See [Opening Access Control](#).
2. Click **Manage Granular Roles** tab.
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.

Users or groups (EPM or IDCS) that match the search criterion are listed. By default, the list is sorted by **User Login** values, and then by **Group Name** values (for group searches).

4. Click  (**Actions**) of the user or group, and then select **Manage Roles**.
5. To assign a granular role to the user or group, select from the list of **Available Granular Roles**, and then click right- arrow button.



Manage Granular Roles for User: ak

Available Granular Roles

- Access Control - Manage
- Ad Hoc - Create
- Ad Hoc - User
- Announcements - Manage
- Application - Mass Allocate
- Approvals - Administer
- Approvals - Assign Ownerships
- Approvals - Design Process
- Approvals - Supervise
- Audit - Manage
- Audit - View
- Dashboards - Manage
- Data Integration - Administrator

Assigned Granular Roles

- Access Control - View
- Ad Hoc - Read Only User

To learn which granular roles apply to each business process, see [Managing Granular Roles with Access Control](#).

6. If you want to unassign a granular role, select from the list of **Assigned Granular Roles**, and then click left-arrow key.
7. Click **OK** to complete granular role assignment for the user or group.
8. Click **OK** again to return to **Manage Granular Roles** tab.

3

Generating Reports

Service Administrators or users with Access Control - Manage or Access Control - View granular role can generate these reports:

- [Generating a Role Assignment Report for a User or Group](#)
- [Viewing the Role Assignment Report for the Environment](#)
- [Viewing the User Login Report](#)
- [Viewing the User Group Report](#)

Note

These Access Control reports display only active users. Any users who are inactive or have been removed from IAM do not appear in the reports.

Report Time Zone

The report generation time shown in the reports reflects the local time zone of the user's browser (based on the 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. Granular roles subsumed into predefined roles are not listed.
- Granular roles to which a user is assigned either directly or through group. Each granular role assigned to a user appears in a separate row.
- Groups to which the 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.

Troubleshooting

See Troubleshooting Reports Issues in the *Operations Guide*.

Generating a Role Assignment Report for a User or Group

The Role Assignment Report enables you to track user access for compliance reporting.


This report displays all active users who have been assigned a predefined role. Deactivated users are not included in the report. IDCS or EPM groups to which a user belongs are not listed unless those groups are used to assign granular roles to the user. Service Administrators

or users with Access Control - Manage or Access Control - View granular role can access the Role Assignment Report to review the application roles and granular roles assigned to a user or group.

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

1. Open **Access Control**. See [Opening Access Control](#).
2. Click **Manage Granular Roles** tab.
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.

Users or groups that match the search criterion are listed. By default, the report is sorted by **User Login** values, and then by **Group Names** (for group searches).

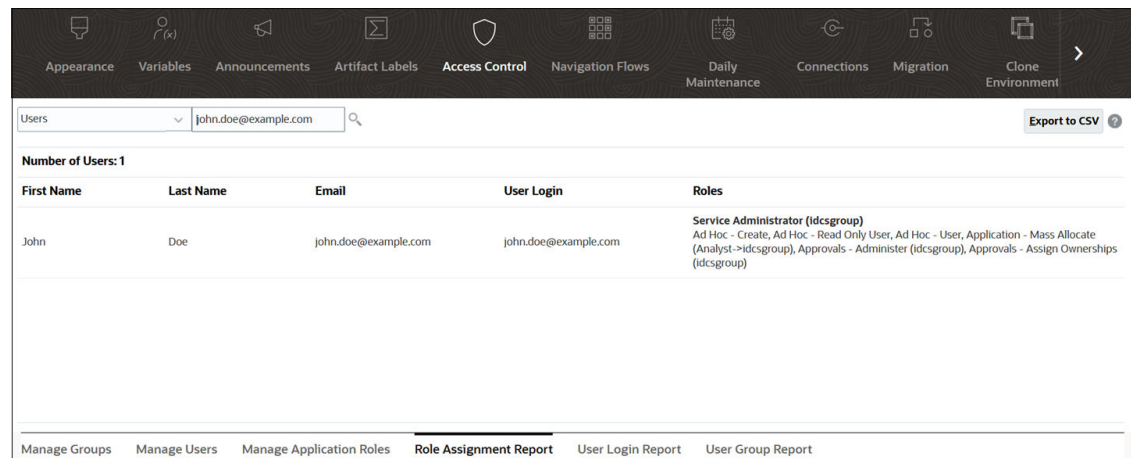
4. Click  of the user or group, and then select **Role Assignment Report**.
5. **Optional:** Click **Export to CSV** to export the report into a CSV file.

Viewing the Role Assignment Report for the Environment

Service Administrators, or users with Access Control - Manage or Access Control - View granular role use the Role Assignment Report to review the user access assigned through predefined roles (in bold), and granular roles. This report shows all active users that have been assigned a predefined role. Deactivated users are not included.

Inherited roles, along with inheritance details, are displayed in a single row for each user.

If a predefined role or a granular role is assigned to an IDCS group, the report will show that predefined role assigned indirectly to the user through IDCS group. For example, assume that user John Doe is assigned as member of idcsgroup and this group is assigned to Service Administrator predefined role. In this scenario, the Role Assignment Report displays the following as a part of the role assignment information for John Doe:



First Name	Last Name	Email	User Login	Roles
John	Doe	john.doe@example.com	john.doe@example.com	Service Administrator (idcsgroup) Ad Hoc - Create, Ad Hoc - Read Only User, Ad Hoc - User, Application - Mass Allocate (Analyst->idcsgroup), Approvals - Administer (idcsgroup), Approvals - Assign Ownerships (idcsgroup)

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.

User Login	First Name	Last Name	Email	Role	Granted through Group
john.doe@example.com	John	Doe	john.doe@example.com	Service Administrator	idcsgroup
john.doe@example.com	John	Doe	john.doe@example.com	Ad Hoc - Create	
john.doe@example.com	John	Doe	john.doe@example.com	Ad Hoc - Read Only User	
john.doe@example.com	John	Doe	john.doe@example.com	Ad Hoc - User	
john.doe@example.com	John	Doe	john.doe@example.com	Application - Mass Allocate	Analyst->idcsgroup
john.doe@example.com	John	Doe	john.doe@example.com	Approvals - Administer	idcsgroup
john.doe@example.com	John	Doe	john.doe@example.com	Approvals - Assign Ownerships	idcsgroup

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 filter it for a specific role.

The Role Assignment report is displayed. By default, the report is sorted by **User Login** values and then by granular roles under **Roles** (for searches by roles). The predefined roles are displayed in bold font, while the granular roles are in non-bold font.

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 or users with Access Control - Manage or Access Control - View granular role 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 Fusion Cloud Enterprise Performance Management 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.

The User Login report is displayed. By default, the report is sorted by **Access Date and Time** values.

5. **Optional:** Click **Export to CSV** to export the displayed report as a CSV file.

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

Viewing the User Group Report

The User Group Report lists the direct or indirect membership of users assigned to EPM groups in . Service Administrators or users with Access Control - Manage or Access Control - View granular role can generate this report.

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 direct groups are displayed in bold font, while the indirect groups are in non-bold font.

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 generate 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.

The User Groups report is displayed. By default, the report is sorted by **User Login** values.

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

5. **Optional:** Click **Export to CSV** to export EPM group name and descriptions to `Groups.csv` file.

PREDEFINED or IAM groups cannot be exported using this option. **Export to CSV** is disabled if no EPM group exists. There should be at least one EPM group in Access Control to use this option.

6. **Optional:** Click **Import from CSV** to import group assignments of EPM Users from a CSV file into Access Control.

For information on CSV file format and other details, see [Importing Group Assignments of Users from a File](#).