Oracle® Fusion Cloud EPM
管理访问控制

F28916-23

Oracle Fusion Cloud EPM 管理访问控制

F28916-23

版权所有 © 2015, 2025, Oracle 和/或其附属公司。

第一作者：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.

目录

文档可访问性

文档反馈

1 访问控制概述

打开访问控制 1-1
管理组 1-2
- 创建 EPM 组 1-3
- 编辑 EPM 组 1-4
- 删除 EPM 组 1-5
- 将云 EPM 组导出到 CSV 文件 1-5

从文件导入用户的组分配 1-6
将一个用户分配给许多组 1-7
使用搜索 1-7

2 在应用程序级别管理角色分配

应用程序角色分配概览 2-1
- Account Reconciliation 2-2
- Enterprise Profitability and Cost Management 2-4
- Financial Consolidation and Close 2-6
- 自由形式 2-8
- Narrative Reporting 2-9
- Oracle Enterprise Data Management 2-9
- Planning 2-10
- Profitability and Cost Management 2-12
- Tax Reporting 2-13

为组或用户分配应用程序角色 2-15

3 生成报表

为用户或组生成角色分配报表 3-1

查看环境的角色分配报表 3-2
查看用户登录报表 3-3
查看用户组报表 3-3

文档可访问性

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

获得 Oracle 支持

购买了支持服务的 Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

文档反馈

要提供有关此文档的反馈，请单击任意 Oracle 帮助中心主题中页面底部的“反馈”按钮。还可以向 epmdoc_ww@oracle.com 发送电子邮件。

1
访问控制概述

Oracle Fusion Cloud Enterprise Performance Management 和 Oracle Fusion Cloud Enterprise Data Management 环境使用多层保护措施进行保护。通过使用基于角色的访问（预定义角色），限制只有授权的用户具有访问权限。预定义角色分配使用 Oracle Cloud 控制台进行管理。例如，要允许用户 `John Doe` 查看属于 Planning 测试环境的报表，应为其分配该环境的查看者角色。有关详细信息，请参阅《管理员入门指南》中的“了解预定义角色”。

为了能够对使用云 EPM 业务流程或 Oracle Enterprise Data Management Cloud 进行更细粒度的控制，可以通过访问控制进一步为用户分配特定于应用程序的角色。例如，可以在 Planning 应用程序中为用户或组分配“审批管理员”角色，以便他们能够执行与审批相关的活动。

务必注意，在应用程序级别分配角色只会增强用户的访问权限。这些特定于应用程序的角色无法撤消或限制预定义角色授予的权限。

通过访问控制，可以在环境中完成下列活动：

- **管理组**。请参阅“管理组”
- **管理用户**。请参阅“将一个用户分配给许多组”
- **管理应用程序角色**。请参阅“在应用程序级别管理角色分配”
- **角色分配报表**。请参阅：
  - 为用户或组生成角色分配报表
  - 查看环境的角色分配报表
- **用户登录报表**。请参阅“查看用户登录报表”
- **用户组报表**。请参阅“查看用户组报表”

Account Reconciliation 的**访问控制**提供特定功能。有关更多详细信息，请参阅《管理 *Account Reconciliation*》中的以下主题：

- 使用团队
- 管理用户
- Account Reconciliation 中的超级用户安全性

教程链接

按照此教程“Setting Up Security in Cloud EPM Business Processes（设置 Cloud EPM 业务流程中的安全性）”来了解云 EPM 业务流程中的安全层，以及如何使用访问控制和访问权限来管理安全性。

打开访问控制

要打开访问控制：

1. 以服务管理员或具有“访问控制 - 管理”应用程序角色的用户身份访问环境。
2. 完成一个步骤：
   - 依次单击 （导航器）和**访问控制**。

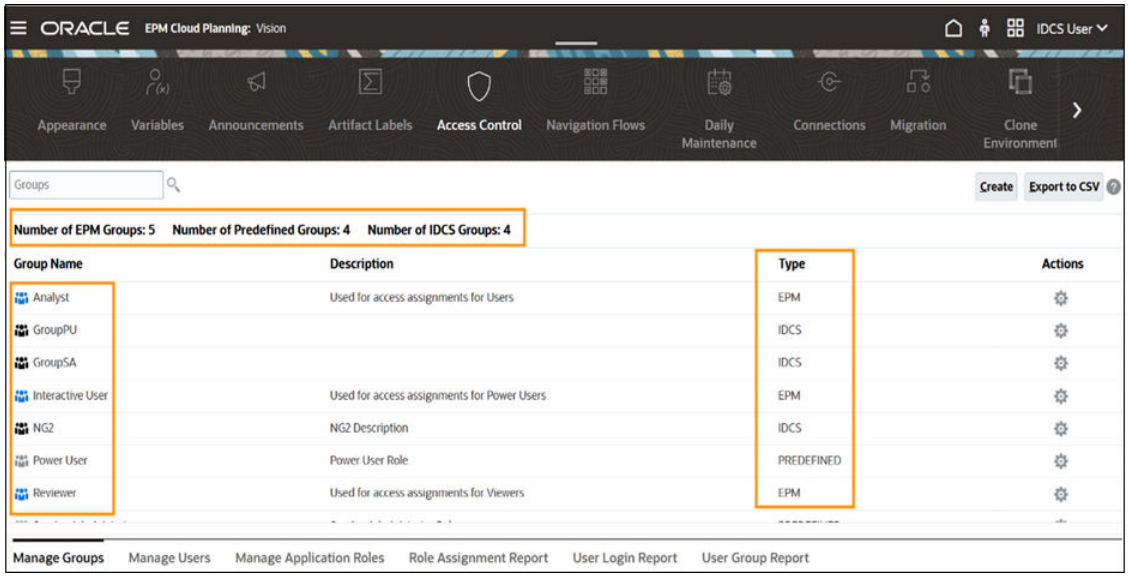
- 依次单击**工具**和**访问控制**。
- 仅限 **Narrative Reporting**：单击**访问控制**。

管理组

Oracle Fusion Cloud Enterprise Performance Management 可识别三种类型的组：

- PREDEFINED：这些组是为每个预定义角色自动创建的。系统会根据用户的预定义角色（例如“超级用户”）将所有用户分配到 PREDEFINED 组。
- EPM：这些是您在访问控制中创建的组。无法在身份控制台中创建它们。它们也不会显示在身份控制台中。
- IDCS：这些是您在 Oracle Identity Cloud 中创建的组。可以使用身份提供程序（例如 Okta 或 Azure AD）同步它们。它们会显示在访问控制中，但您无法通过访问控制创建他们。

在**管理组**选项卡中，组按类型和图像分类以便于区分。要搜索特定组，请参阅“使用搜索”以获取相关说明。



PREDEFINED 组

为支持您查看用户分配，“访问控制”以 PREDEFINED 组的形式列出预定义角色的用户。

主要注意事项：

- PREDEFINED 组可以分配为 EPM 组的成员。
- PREDEFINED 组不可编辑。
  要查看 PREDEFINED 组，请在该组对应的“操作”下选择**查看**。您可以查看分配到组的所有云 EPM 用户列表。

有关预定义角色的详细信息，请参阅《管理员入门指南》中的“了解预定义角色”。

EPM 组

您可以使用**管理组**屏幕上的以下选项创建和管理 EPM 组。

- **创建**按钮 - 创建新 EPM 组。请参阅“创建 EPM 组”

- **导出到 CSV** 按钮 - 将 EPM 组导出到 CSV 文件。请参阅“将云 EPM 组导出到 CSV 文件”
- **编辑** （操作）- 编辑所选的一行组列表中的 EPM 组。请参阅“编辑 EPM 组”
- **删除** （操作）- 删除所选的一行组列表中的 EPM 组。请参阅“删除 EPM 组”

主要注意事项：

- EPM 组可以分配为更大 EPM 组的成员。
- 无法使用访问控制从文件中导入组信息以创建组。可以使用迁移或 createGroups EPM Automate 命令导入组。

IDCS 组

您可以使用 IDCS 组为多个云 EPM 用户分配预定义角色。请参阅《管理员入门指南》中的“在 Oracle Cloud Identity Console 中使用 Identity Cloud Service 组为用户分配预定义角色”或“在 Oracle Cloud 控制台中使用 Identity Cloud Service 组为用户分配预定义角色”。

主要注意事项：

- IDCS 组不可编辑。
  要查看 IDCS 组，请在该组对应的“操作”下选择**查看**。您可以查看分配到组的所有云 EPM 用户列表。
- IDCS 组可以分配到应用程序角色和 EPM 组。

> **注意：**
>
> 如果 IDCS 组与 EPM 或 PREDEFINED 组的名称相同，或者名称超过 256 个字符，它将不会显示在访问控制中。务必了解，此类 IDCS 组中的用户无法登录。

故障排除

请参阅《运维指南》中的“解决用户、角色和组管理问题”。

创建 EPM 组

服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以创建 EPM 组。Oracle Fusion Cloud Enterprise Performance Management 用户和其他组可以是一个组的成员。您无法使用此选项创建 IDCS 或 PREDEFINED 组。

> **注：**
>
> 您还可以使用迁移或 createGroups EPM Automate 命令从文件导入组信息以创建组。

要创建组：

1. 打开**访问控制**。请参阅“打开访问控制”。
2. 在**管理组**中，单击**创建**。
3. 在**创建组**中，完成下列步骤：
   a. 在**名称**中，输入唯一的组名称（最多不超过 256 个字符）。组名不区分大小写。
      云 EPM 不允许创建名称与 IDCS 或 PREDEFINED 组相同的组。

b. **可选**：输入组说明。

4. **可选**：添加组以创建嵌套组。

   a. 在**可用组**中，搜索组。有关使用搜索功能的说明，请参阅“使用搜索”。

      将列出符合搜索条件的所有类型的组。默认情况下，此列表按**组名**值排序。

   b. 从**可用组**中选择新组的成员组。

   c. 单击**移动**。

      选定的组将列在**分配的组**下。要删除分配的组，请从**分配的组**中选择要删除的组，然后单击**删除**。

5. **可选**：将云 EPM 用户添加为组的成员。

   只有分配给预定义角色的用户才能作为组成员进行添加。

   a. 单击**用户**。

   b. 在**可用用户**中，搜索用户。有关说明，请参阅“使用搜索”。

      将列出符合搜索条件的用户。默认情况下，此列表按**用户登录**值排序。

   c. 从**可用用户**中，选择要添加到组中的用户。

   d. 单击**移动**。

6. 单击**保存**。

7. 单击**确定**。

编辑 EPM 组

服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以编辑 EPM 组属性（包括组名）。重命名组不影响分配给组的应用程序角色和其他安全分配。您无法使用此选项编辑 IDCS 或 PREDEFINED 组。

要编辑组：

1. 打开**访问控制**。请参阅“打开访问控制”。

2. **可选**：在**管理组**中，找到要编辑的组。有关使用搜索功能的说明，请参阅“使用搜索”。

   将列出符合搜索条件的所有类型的组。默认情况下，此列表按**组名**值排序。

   > **注：**
   >
   > 组名称最多可包含 256 个字符。可见字符（例如**可用组**列中的字符）可能会被截断，具体取决于您的屏幕分辨率。

3. 单击要编辑的组所在行中的 （操作），然后选择**编辑**。

4. **可选**：编辑组名称。更改组名称不影响使用组做出的安全分配。您无法重命名名称与所列 IDCS 或 PREDEFINED 组相同的组。

5. 编辑组分配：

   a. **可选**：添加嵌套组：

      - 在**可用组**中，搜索组。有关使用搜索功能的说明，请参阅“使用搜索”。

        将列出符合搜索条件的所有类型的组。默认情况下，此列表按**组名**值排序。

- 从**可用组**中，选择组并单击**移动**。

  选定的组将列在**分配的组**列表中。

b. **可选**：删除嵌套组：

- 从**分配的组**中，选择要删除的组。
- 单击**删除**

6. 编辑用户分配：

a. 单击**用户**。

b. **可选**：向组添加用户：

- 在**可用用户**中，搜索可分配为组成员的用户。有关使用搜索功能的说明，请参阅“使用搜索”。

  将列出符合搜索条件的用户。默认情况下，此列表按**用户登录**值排序。

- 从**可用用户**中，选择用户并单击**移动**。

  选定的用户将列在**分配的用户**列表中。

c. **可选**：从组中删除用户：

- 从**分配的用户**中，选择要删除的用户。
- 单击**删除**。

7. 单击**保存**。
8. 单击**确定**。

删除 EPM 组

服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以删除 EPM 组。删除 EPM 组不会删除组成员。您无法使用此选项删除 IAM 或 PREDEFINED 组。

要删除组：

1. 打开**访问控制**。请参阅“打开访问控制”。
2. **可选**：在**管理组**中，搜索要删除的组。有关使用搜索功能的说明，请参阅“使用搜索”。

   将列出符合搜索条件的组。默认情况下，此列表按**组名**值排序。

3. 单击要删除的 EPM 组所在行中的 （操作），然后选择**删除**。
4. 单击**是**确认删除操作。
5. 单击**确定**。

将云 EPM 组导出到 CSV 文件

服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以使用**导出到 CSV** 将 EPM 组名和说明导出到 `Groups.csv` 文件。PREDEFINED 或 IDCS 组无法使用此选项导出。

如果不存在任何 EPM 组，则**导出到 CSV** 处于禁用状态。访问控制中应该至少有一个 EPM 组才能使用此选项。

1. 打开**访问控制**。请参阅“打开访问控制”。

   管理组选项卡会列出所有可用组。

2. 单击**导出到 CSV** 以导出所有 EPM 组。

3. 按照屏幕上的说明打开或保存 `Groups.csv` 文件。

从文件导入用户的组分配

服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以从逗号分隔值 (Comma Separated Value, CSV) 文件导入用户的 EPM 组分配，以在现有访问控制组中创建新分配。Oracle Fusion Cloud Enterprise Performance Management 基于新的组分配强制实施应用程序级别和对象级别的安全分配。

> **注：**
>
> 在导入文件中标识的所有用户登录必须在身份域中存在；导入文件中包括的所有组名必须在访问控制中存在。不能使用此导入过程创建组。
> 您只能创建新的组分配，而不能删除用户的当前组分配。

导入 CSV 文件格式可以如下图中所示：

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

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

此格式与用户组报表的 CSV 版本相同。如果您使用此格式，则导入过程会忽略“用户登录”和“组“以外的所有列。创建导入文件的一个简便方式是：导出当前的用户组报表，然后根据需要对该报表进行修改。请参阅“查看用户组报表”。

要导入用户的组分配：

1. 打开**访问控制**。请参阅“打开访问控制”。
2. 单击**用户组报表**。
3. 单击**从 CSV 导入**。
4. 使用**导入用户组分配 CSV** 中的**浏览**，选择导入文件。
5. 单击**导入**。
6. 单击**是**。

   完成导入过程时，将显示一个确认对话框，其中会标识已处理的分配总数和状态。

将一个用户分配给许多组

Oracle Fusion Cloud Enterprise Performance Management 用户可以是使用访问控制维护的许多组的成员。服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以将用户分配给多个组。

> **注：**
>
> 在任何给定时间，用户最多可以是 1,000 个组的成员（直接或间接）。

1. 打开**访问控制**。请参阅“打开访问控制”。
2. 单击**管理用户**。
3. 搜索要分配到多个组的用户。有关使用搜索功能的说明，请参阅“使用搜索”。

   将列出符合搜索条件的用户。默认情况下，此列表按**用户登录**值排序。
4. 单击用户列表行中的 （操作），然后选择**编辑**。

   此时将显示**编辑用户**屏幕，其中列出了详细的用户信息，包括当前组成员身份（在**分配的组**中）。在此屏幕上，您只能修改组分配。
5. 查找要分配给用户的组。有关使用搜索功能的说明，请参阅“使用搜索”。

   将列出符合搜索条件的 EPM 组。默认情况下，此列表按**组名**值排序。
6. 完成一项操作：
   - 要将更多组分配给用户，请从**可用组**中，选择一个或多个组，然后单击 （**移动**），以将所选的组移动到**分配的组**。或者，单击 （**移动全部**），以将**可用组**中的所有组移动到**分配的组**。
   - 要删除分配给用户的组，请从**分配的组**中，选择一个或多个组，然后单击 （**删除**），以将所选的组移动到**可用组**。或者，单击 （**全部删除**），以将**分配的组**中的所有组移动到**可用组**。
7. 单击**保存**。
8. 单击**确定**。

使用搜索

用户和组对象的智能搜索在访问控制中以相同的方式工作。

使用用户属性之一（用户名、名字、姓氏或电子邮件 ID）、组名或角色名中的字符串来查找特定的用户、组或角色。例如，使用字符串 `st` 搜索组将显示包含字符串 `st` 的所有组名（例如，TestGroup、Strategic_Planner、AnalystsGroup 等）。同样，使用字符串 `jd` 搜索用户将列出其用户名、名字、姓氏或电子邮件地址包含字符串 `jd` 的用户。

搜索选项不支持通配符 (*)。

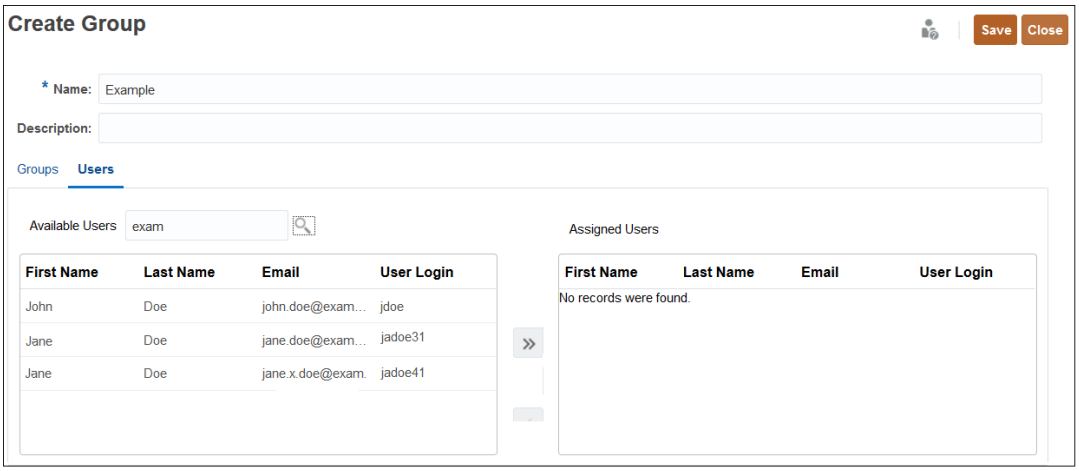
> **注：**
>
> 一些访问控制屏幕（例如，**分配应用程序角色**、**角色分配报表**和**用户组报表**）为您提供了搜索选项。请在开始搜索之前选择适当的选项。

要搜索用户：

1. 访问可以在其中使用用户搜索功能的屏幕，例如，**管理用户**。
2. 在搜索字段中，输入用户属性（用户名、名字、姓氏或电子邮件 ID）的部分字符串。
3. 单击 （搜索）。
   搜索结果显示对于满足搜索条件的用户可用的所有属性。默认情况下，此列表按**用户登录**值排序。

要搜索组：

- 访问可以在其中使用组搜索功能的屏幕，例如，**管理组**。
- 在搜索字段中，输入组名称的部分字符串。
- 单击 （搜索）。
  搜索结果显示满足搜索条件的组的名称和说明。默认情况下，此列表按**组名**值排序。



要基于用户在角色分配报表中的角色搜索用户：

- 访问**角色分配报表**选项卡。
- 从“搜索”下拉列表中选择**用户**或**角色**。
- 在搜索字段中，输入搜索字符串。
- 单击 （搜索）。
  搜索结果显示对于某些用户可用的所有信息，针对这些用户分配了满足搜索条件的角色。默认情况下，此列表按**用户登录**值排序。

2
在应用程序级别管理角色分配

访问控制适用于以下 Oracle Fusion Cloud Enterprise Performance Management 业务流程：

- Account Reconciliation
- Enterprise Profitability and Cost Management
- Financial Consolidation and Close
- 自由形式
- Narrative Reporting
- Oracle Fusion Cloud Enterprise Data Management
- Planning
- Profitability and Cost Management
- Tax Reporting

应用程序角色分配概览

借助访问控制，您可以通过在应用程序级别为 Oracle Fusion Cloud Enterprise Performance Management 用户分配角色，在预定义角色的基础上扩展这些用户的访问权限。这些角色称为应用程序角色。服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以将特定于应用程序的角色和数据授权授予访问控制中创建和管理的用户和组。

例如，默认情况下，只有服务管理员和超级用户才能访问数据集成。要允许具有用户或查看者预定义角色的用户参与集成流程，服务管理员可以为他们分配“数据集成 - 创建”应用程序角色。

> **Note:**
>
> 应用程序角色只能增强用户的访问权限；不会削减预定义角色授予的权限。要详细了解预定义角色，请参阅《管理员入门指南》中的“了解预定义角色”。

有关可用云 EPM 应用程序角色及其预定义角色映射的详细信息，请参阅：

- Account Reconciliation
- Enterprise Profitability and Cost Management
- Financial Consolidation and Close
- 自由形式
- Narrative Reporting
- Oracle Enterprise Data Management
- Planning
- Profitability and Cost Management
- Tax Reporting

> **Note:**
>
> 如果您要将应用程序从内部部署环境迁移到云 EPM，请参阅《管理迁移》中的“用于迁移到云 EPM 的角色映射”。

分配应用程序角色的最佳做法

建议的最佳做法是分配适合的最低级别角色，并根据需要授予额外权限。下面列举了一些属于以下情况的示例：您可能想为其预定义角色没有相应权限的人员授予应用程序角色。

- 为需要编制调节的查看者添加**编制者**应用程序角色。
- 报表设计者只能设计报表但不能使用其余应用程序功能。您可以为其提供查看者角色，然后分配**管理报表**应用程序角色
- 超级用户能够管理警报类型，因此您可以分配**管理警报类型**应用程序角色

> **Note:**
>
> 授予权限只是叠加操作。这意味着您可以在用户的预定义角色拥有的权限之上增加权限，但不能删除自动提供给预定义角色的权限。

Account Reconciliation

下表列出并介绍了 Account Reconciliation 应用程序角色，并将这些角色与预定义角色对应。

> **Note:**
>
> 所有预定义角色都能够根据其对 Account Reconciliation 中数据的访问权限穿透钻取到数据交换详细数据。

Table 2-1 Account Reconciliation 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	使用访问控制执行所有活动，包括管理组，为组或用户分配应用程序角色，以及生成和查看可用报表。	服务管理员
访问控制 - 查看	使用访问控制，生成并查看与用户安全相关的报表，例如角色分配报表、用户登录报表、组分配报表和用户组报表。具有此角色的用户无法在访问控制中分配应用程序角色、管理组或修改设置。	服务管理员
警报类型 - 管理	管理警报类型，以定义在出现某些问题时应遵循的过程。	服务管理员
公告 - 管理	管理在欢迎面板上向用户显示的公告。这些可能指示即将发生的事件，例如系统维护或运行作业。	服务管理员
审核 - 查看	提供对所有审核详细信息的访问权限。但是，此应用程序角色不允许启动“调节操作”对话框，因为“调节”超出了其安全范围。	服务管理员
货币 - 管理	配置货币、汇率类型和货币组。具有此角色的用户可以控制哪些货币代码在系统中处于活动状态。	服务管理员

Table 2-1 (Cont.) Account Reconciliation 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
仪表板 - 管理	构造和管理自定义仪表板。具有此角色的用户可以： • 配置合规性 • 添加、编辑、复制和删除 • 导入和导出	服务管理员
数据集成 - 管理员	执行数据集成中的所有功能活动。具有此角色的用户可创建、执行和运行： • 源系统与目标系统之间的集成 • 管道活动 • 使用 EPM 集成代理从内部部署源提取和转换数据和元数据	服务管理员
数据集成 - 创建	使用数据集成创建映射以在源系统与目标系统之间集成数据。此角色可以为数据规则定义各种运行时选项。	服务管理员
数据集成 - 运行	具有此角色的用户可使用数据集成在源和目标之间运行集成。 如果这是分配给用户的唯一角色，并且他们不是超级用户或服务管理员，则他们还可以查看集成详细信息，但无法进行任何更改。	服务管理员
数据加载 - 管理	定义数据加载定义，以便使用数据集成来加载数据并保存相同的数据加载参数。 查看数据加载的最新状态，并监视用户更改请求的处理。	服务管理员
作业 - 查看	查看 Account Reconciliation 作业和作业状态。	• 超级用户 • 服务管理员
匹配类型 - 管理	具有此角色的用户可以管理匹配类型、调整属性、支持属性、日记帐列和组属性。	服务管理员
匹配类型 - 查看	具有此角色的用户可以查看匹配类型、调整属性、支持属性和日记帐列的详细信息。	服务管理员
组织 - 管理	将分层组织单位结构分配给配置文件和调节。	服务管理员
期间 - 管理	管理期间属性。他们还可以设置期间的状态，加载数据以及对现有期间执行其他操作。	服务管理员
期间 - 查看	具有此角色的用户可以查看（仅读取访问权限）与调节关联的期间数，还可以根据期间加载数据。	• 超级用户 • 服务管理员
配置文件 - 查看	具有此角色的用户可以访问为其分配了工作流的配置文件，这与他们可以查看的调节一致。	• 超级用户 • 服务管理员 • 用户
配置文件和调节 - 管理	管理配置文件、调节和属性 您可以在**超级用户安全性**屏幕中为此角色设置安全范围。	• 超级用户 • 服务管理员
公共筛选器和视图 - 管理	筛选器控制您可以在列表视图和报表中看到哪些记录。您可以针对配置文件、调节或调节事务属性（包括系统属性、余额和余额详细信息）应用筛选器。 具有此角色的用户可以创建复杂筛选器和逻辑来确定筛选器的应用顺序。	服务管理员
Reconciliation - 注释者	查看调节，并为调节或调节事务添加注释。	• 超级用户 • 服务管理员 • 用户
Reconciliation - 编制者	具有此角色的用户可编制调节、分配面板、导入预映射的数据以及添加附件，以提交、申请和发布调节。	• 超级用户 • 服务管理员 • 用户

Table 2-1 (Cont.) Account Reconciliation 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
Reconciliation - 审核者	具有此角色的用户可审核调节、分配面板以及添加附件，以批准、驳回、申请和发布调节。	• 超级用户 • 服务管理员 • 用户
报表 - 管理	配置应用程序设置以显示调节报表。	服务管理员
团队 - 管理	具有此角色的用户可以添加、编辑或删除团队，以及管理团队成员。	• 超级用户 • 服务管理员
用户 - 管理	具有此角色的用户可以管理团队成员。	• 超级用户 • 服务管理员

Enterprise Profitability and Cost Management

下表列出并介绍了 Enterprise Profitability and Cost Management 应用程序角色，并将这些角色与预定义角色对应。

Table 2-2 Enterprise Profitability and Cost Management 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	使用访问控制执行所有活动，包括管理组，为组或用户分配应用程序角色，以及生成和查看可用报表。	服务管理员
访问控制 - 查看	使用访问控制，生成并查看与用户安全相关的报表，例如角色分配报表、用户登录报表、组分配报表和用户组报表。具有此角色的用户无法在访问控制中分配应用程序角色、管理组或修改设置。	服务管理员
即席 - 创建	创建、查看、修改和保存即席网格。	超级用户
即席 - 只读用户	执行所有即席功能，但不能回写到即席网格或使用数据管理加载数据。	请参阅“脚注”
即席 - 用户	查看和修改即席网格以及执行即席操作。即席用户不能保存即席网格。	用户
应用程序 - 批量分配	在表单网格内运行批量分配规则。	服务管理员
公告 - 管理	管理在欢迎面板上向用户显示的公告。这些可能指示即将发生的事件，例如系统维护或运行作业。	服务管理员
计算 - 运行	在“计算控制”页面中计算模型。	• 超级用户 • 服务管理员 • 用户
计算历史记录 - 删除	从“计算分析”页面中删除所选的已完成计算的实例。删除计算历史记录不会删除任何数据。这仅删除记录的已运行计算的实例。	• 超级用户 • 服务管理员 • 用户
计算历史记录 - 查看	在“计算分析”页面中查看已完成的计算。	• 超级用户 • 服务管理员 • 用户

Table 2-2 (Cont.) Enterprise Profitability and Cost Management 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
仪表板 - 管理	构造和管理规划和运行仪表板。具有此角色的用户可以： • 根据对仪表板设置的权限添加、编辑、复制和删除仪表板 • 导入和导出仪表板	服务管理员
数据集成 - 创建	使用数据集成创建映射以在源系统与目标系统之间集成数据。用户可以为数据规则定义各种运行时选项。	超级用户
数据集成 - 穿透钻取	穿透钻取到数据的源系统。	• 超级用户 • 用户
数据集成 - 运行	具有此角色的用户可使用数据集成在源和目标之间运行集成。 如果这是分配给用户的唯一角色，并且他们不是超级用户或服务管理员，则他们还可以查看集成详细信息，但无法进行任何更改。	超级用户
文档 - 管理	构造和管理文档。具有此角色的用户可以： • 根据对文档设置的权限添加、编辑、复制和删除文档 • 导入和导出文档	服务管理员
模型 - 创建	在“建模”页面中创建新的模型。	• 超级用户 • 服务管理员
模型 - 删除	在“建模”页面中删除模型。删除模型还会删除模型中的所有规则。	服务管理员
模型 - 查看	在设计器页面中查看模型及其关联的规则。	• 超级用户 • 服务管理员 • 用户 • 查看者
模型验证 - 运行	在“模型验证”页面中验证模型。	• 超级用户 • 服务管理员 • 用户
POV - 创建	在“计算控制”页面中创建新的视点。	• 超级用户 • 服务管理员
POV - 删除	在“计算控制”页面中删除视点。删除视点还会删除关联的数据以及该视点的计算历史记录页面。此外，还会将该视点从“计算控制”页面中删除。	服务管理员
POV 数据 - 清除	清除“计算控制”页面的视点中的数据，但不删除视点。	• 超级用户 • 服务管理员
POV 数据 - 复制	在“计算控制”页面中将数据从一个视点复制到另一视点。	• 超级用户 • 服务管理员
POV 状态 - 编辑	在“计算控制”页面的“**编辑视点**”对话框中更改视点的状态。视点的可用状态包括“草稿”、“已发布”和“已存档”。	服务管理员
利润曲线 - 创建	在“商务智能”群集的**利润曲线**选项卡上创建利润曲线。	• 超级用户 • 服务管理员
利润曲线 - 编辑	在“商务智能”群集的**利润曲线**选项卡上编辑利润曲线。	• 超级用户 • 服务管理员

Table 2-2 (Cont.) Enterprise Profitability and Cost Management 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
利润曲线 - 运行	在“商务智能”群集的**利润曲线**选项卡上运行利润曲线。	• 超级用户 • 服务管理员 • 用户 • 查看者
规则 - 创建/编辑	在设计器页面中创建或编辑分配规则、自定义计算规则或规则集。	• 超级用户 • 服务管理员 • 用户
规则 - 删除	在设计器页面中删除分配规则、自定义计算规则或规则集。	• 超级用户 • 服务管理员 • 用户
规则平衡 - 运行	查看“规则平衡”报表以了解每个规则的影响。	• 超级用户 • 服务管理员 • 用户
规则 - 批量编辑	在设计器页面中访问“**批量编辑**”选项卡，以便一次编辑多个规则。	• 超级用户 • 服务管理员 • 用户
跟踪分配 - 运行	在“商务智能”群集的**跟踪分配**选项卡上跟踪分配金额。	• 超级用户 • 服务管理员 • 用户 • 查看者
脚注：此角色未映射到任何预定义角色，因此需要将其分配给用户或组才能将其激活。		

Financial Consolidation and Close

下表列出并介绍了以下应用程序的 Financial Consolidation and Close 角色，并将这些角色与预定义角色对应：

表 2-3 Financial Consolidation and Close 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	管理组，为组或用户分配应用程序角色，以及生成用户安全报表。	服务管理员
访问控制 - 查看	查看用户安全报表（例如角色分配报表、用户登录报表和用户组报表），但无法在访问控制中分配应用程序角色、管理组或执行任何其他更新操作。	服务管理员
即席 - 创建	创建、查看、修改和保存即席网格。	超级用户
即席 - 只读用户	执行所有即席功能，但不能回写到即席网格或使用数据管理加载数据。	请参阅“脚注”
即席 - 用户	查看和修改即席网格以及执行即席操作。即席用户不能保存即席网格。	用户
公告 - 管理	构造和管理公告。具有此角色的用户可以添加、编辑、复制和删除公告。	服务管理员
应用程序 - 批量分配	在表单网格内运行批量分配规则。	服务管理员

表 2-3 （续） Financial Consolidation and Close 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
合并日记帐 - 批准	批准已提交进行审批的合并日记帐，或驳回已提交的日记帐。	参阅脚注
合并日记帐 - 审批后自动推送	允许在批准者批准合并日记帐后自动推送该合并日记帐。批准日记帐的用户也将是推送用户。	参阅脚注
合并日记帐 - 创建	创建、修改和删除合并日记帐与合并日记帐模板。	参阅脚注
合并日记帐 - 管理期间	打开合并日记帐的期间或关闭日记帐期间。如果期间中存在批准的日记帐或取消推送的自动冲销日记帐，无法将其关闭。如果您选择关闭包含正在处理或已提交的日记帐的期间，则系统会显示一条警告消息，指明在该期间发现未推送的日记帐，但是您可以关闭该期间。	参阅脚注
合并日记帐 - 推送	推送已完成或已提交并批准的合并日记帐。必须先打开要向其推送合并日记帐的每个方案的期间。	参阅脚注
合并日记帐 - 提交	提交合并日记帐进行审批，或驳回状态为“已完成”的合并日记帐。	参阅脚注
合并日记帐 - 取消推送	取消推送合并日记帐。您必须对日记帐中的成员具有写入访问权限。	参阅脚注
数据集成 - 创建	使用数据集成创建映射以在源系统与目标系统之间集成数据。用户可以为数据规则定义各种运行时选项。	超级用户
仪表板 - 管理	构造和管理所有仪表板，包括运行仪表板。具有此角色的用户可以： • 添加、编辑、复制和删除仪表板 • 导入和导出仪表板	• 服务管理员 • 超级用户
数据集成 - 穿透钻取	穿透钻取到数据的源系统。	• 超级用户 • 用户
数据集成 - 运行	具有此角色的用户可使用数据集成在源和目标之间运行集成。 如果这是分配给用户的唯一角色，并且他们不是超级用户或服务管理员，则他们还可以查看集成详细信息，但无法进行任何更改。	超级用户
文档 - 管理	构造和管理文档。具有此角色的用户可以： • 根据对文档设置的权限添加、编辑、复制和删除文档 • 导入和导出文档	服务管理员
任务列表 - 管理访问	向其他用户分配任务。	超级用户
任务管理器 - 批准者	有资格作为任务管理器中任务的批准者	• 超级用户 • 服务管理员 • 用户
任务管理器 - 对象 - 管理	管理所有任务管理器对象，例如警报、货币和组织	服务管理员
任务管理器 - 接受者	有资格作为任务管理器中任务的接受者	• 超级用户 • 服务管理员 • 用户
任务管理器 - 审核 - 查看	查看审核历史记录信息	服务管理员
任务管理器 - 自定义报表 - 管理	设计自定义报表	服务管理员

表 2-3 （续） Financial Consolidation and Close 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
任务管理器 - 运行仪表板 - 管理	配置运行仪表板	服务管理员
任务管理器 - 公共筛选器和视图 - 管理	发布筛选器和视图以使其可供所有人访问	• 超级用户 • 服务管理员
任务管理器 - 系统服务和设置 - 管理	定义应用程序的系统服务和系统设置	服务管理员
任务管理器 - 任务 - 管理	设计并管理任务、模板和计划	• 超级用户 • 服务管理员
任务管理器 - 用户和团队 - 管理	管理用户和团队	• 超级用户 • 服务管理员
脚注：此角色未映射到任何预定义角色，因此需要将其分配给用户或组才能将其激活。		

自由形式

下表列出并介绍了自由形式应用程序角色，并将这些角色与预定义角色对应。

> **Note:**
>
> 应用程序中缺少与预定义角色对应的角色需要单独分配给用户或组。如果未进行此类分配，用户将无法进行与其应用程序角色相关的活动。例如，需要明确向用户授予“即席 - 只读用户”角色（未与下表中的任何预定义角色关联）才能激活其功能。此功能不会自动包含在任何预定义角色中。

Table 2-4 自由形式应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	管理组，为组或用户分配应用程序角色，以及生成用户安全报表。	服务管理员
访问控制 - 查看	查看用户安全报表（例如角色分配报表、用户登录报表和用户组报表），但无法在访问控制中分配应用程序角色、管理组或执行任何其他更新操作。	服务管理员
即席 - 创建	创建、查看、修改和保存即席网格。	超级用户
即席 - 只读用户	执行所有即席功能，但不能回写到即席网格或使用数据管理加载数据。	请参阅“脚注”
即席 - 用户	查看和修改即席网格以及执行即席操作。即席用户不能保存即席网格。	用户
公告 - 管理	构造和管理公告。具有此角色的用户可以添加、编辑、复制和删除公告。	服务管理员
应用程序 - 批量分配	在表单网格内运行批量分配规则。	服务管理员
数据集成 - 创建	使用数据集成创建映射以在源系统与目标系统之间集成数据。用户可以为数据规则定义各种运行时选项。	超级用户

Table 2-4 (Cont.) 自由形式应用程序角色

应用程序角色	说明	包括在以下预定义角色中
数据集成 - 穿透钻取	穿透钻取到数据的源系统。	• 超级用户 • 用户
数据集成 - 运行	具有此角色的用户可使用数据集成在源和目标之间运行集成。 如果这是分配给用户的唯一角色，并且他们不是超级用户或服务管理员，则他们还可以查看集成详细信息，但无法进行任何更改。	超级用户
仪表板 - 管理	构造和管理规划和运行仪表板。具有此角色的用户可以： • 根据对仪表板设置的权限添加、编辑、复制和删除仪表板 • 导入和导出仪表板	服务管理员
文档 - 管理	构造和管理文档。具有此角色的用户可以： • 根据对文档设置的权限添加、编辑、复制和删除文档 • 导入和导出文档	服务管理员
任务列表 - 管理访问	向其他用户分配任务。	超级用户
脚注：此角色未映射到任何预定义角色，因此需要将其分配给用户或组才能将其激活。		

Narrative Reporting

下表列出并介绍了 Narrative Reporting 应用程序角色，并将这些角色与预定义角色对应。

Table 2-5 Narrative Reporting 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	管理组，为组或用户分配应用程序角色，以及生成用户安全报表。	服务管理员
访问控制 - 查看	查看用户安全报表（例如角色分配报表、用户登录报表和用户组报表），但无法在访问控制中分配应用程序角色、管理组或执行任何其他更新操作。	服务管理员
库 - 管理	创建文件夹，包括根级别文件夹。	• 库管理员 • 超级用户 • 服务管理员
报表 - 管理	创建报表包、报表、帐簿和分别输出定义。	• 超级用户 • 报表管理员 • 服务管理员

Oracle Enterprise Data Management

下表列出并介绍了 Oracle Enterprise Data Management 应用程序角色，并将这些角色与预定义角色对应。

Table 2-6 Oracle Enterprise Data Management 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	管理组，为组或用户分配应用程序角色，以及生成用户安全报表。	服务管理员
访问控制 - 查看	查看用户安全报表（例如角色分配报表、用户登录报表和用户组报表），但无法在访问控制中分配应用程序角色、管理组或执行任何其他更新操作。	服务管理员
应用程序 - 创建	在 Oracle Enterprise Data Management 中注册应用程序。注册应用程序的用户分配有应用程序所有者权限。此用户还分配为默认应用程序视图的视图所有者。	服务管理员
审核	查看与审核相关的信息，例如事务历史记录，以及请求更改 Oracle Enterprise Data Management 中的数据。	服务管理员
迁移 - 管理	使用 EPM Automate 或应用程序屏幕，修改日常维护开始时间。使用迁移在应用程序中导出和导入快照和对象。具有此角色的用户可以通过迁移快照创建应用程序，并且可以删除自己创建的应用程序。 具有此角色的用户无法克隆环境。	服务管理员
视图 - 创建	具有此角色的用户可以创建视图以使用元数据。他们是默认所有者，因此他们也能够向其他用户授予对视图的权限。他们有权编辑或删除视图。	服务管理员

Planning

下表列出并介绍了 Planning 应用程序角色，并将这些角色与预定义角色对应。Planning 应用程序类型，包括自定义、自由形式、Planning 模块、预测性现金预测、战略性人员规划和销售规划。

Table 2-7 Planning 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	管理组，为组或用户分配应用程序角色，以及生成用户安全报表。	服务管理员
访问控制 - 查看	查看用户安全报表（例如角色分配报表、用户登录报表和用户组报表），但无法在访问控制中分配应用程序角色、管理组或执行任何其他更新操作。	服务管理员
即席 - 创建	创建、查看、修改和保存即席网格。	超级用户
即席 - 只读用户	执行所有即席功能，但不能回写到即席网格或使用数据管理加载数据。	参阅脚注
即席 - 用户	查看和修改即席网格以及执行即席操作。即席用户不能保存即席网格。	用户
公告 - 管理	构造和管理公告。具有此角色的用户可以添加、编辑、复制和删除公告。	服务管理员
应用程序 - 批量分配	在表单网格内运行批量分配规则。	服务管理员

Table 2-7 (Cont.) Planning 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
审批 - 管理	通过手动获取流程的所有权来解决审批问题。包含审批所有权分配者、审核流程设计者以及审批超级用户角色。通常，此角色分配给负责某个地区的业务用户，他们需要控制该地区的审批流程，但不需要服务管理员角色。他们可执行以下任务： • 控制审批流程 • 在其具有写入访问权限的 Planning 单元上执行操作 • 为其负责的组织分配所有者和审核者 • 更改次级维或更新验证规则	服务管理员
审批 - 分配所有权	可对其具有写入访问权限的规划单元层次的任何成员执行下列任务： • 分配所有者 • 分配审核者 • 指定要通知的用户	超级用户
审批 - 设计流程	包括审批所有权分配者角色。此外，还可对其具有写入访问权限的规划单元层次的任何成员执行下列任务： • 更改用户具有写入访问权限的次级维和实体的成员 • 更改规划单元层次的方案和版本分配 • 编辑用户具有访问权限的数据表单的数据验证规则	请参阅“脚注”
审批 - 监管	可对用户具有写入访问权限的规划单元层次的任何成员执行下列任务，即使该用户不拥有该规划单元。此用户不能更改不归其所有的规划单元中的数据。 • 停止和启动规划单元 • 在规划单元上执行任何操作	超级用户
仪表板 - 管理	构造和管理规划和运行仪表板。具有此角色的用户可以： • 根据对仪表板设置的权限添加、编辑、复制和删除仪表板 • 导入和导出仪表板	服务管理员
数据集成 - 创建	使用数据集成创建映射以在源系统与目标系统之间集成数据。用户可以为数据规则定义各种运行时选项。	超级用户
数据集成 - 穿透钻取	穿透钻取到数据的源系统。	• 超级用户 • 用户
数据集成 - 运行	具有此角色的用户可使用数据集成在源和目标之间运行集成。 如果这是分配给用户的唯一角色，并且他们不是超级用户或服务管理员，则他们还可以查看集成详细信息，但无法进行任何更改。	超级用户
文档 - 管理	构造和管理文档。具有此角色的用户可以： • 根据对文档设置的权限添加、编辑、复制和删除文档 • 导入和导出文档	服务管理员
任务列表 - 管理访问	向其他用户分配任务。	超级用户
任务管理器 - 批准者	有资格作为任务管理器中任务的批准者	• 服务管理员 • 超级用户 • 用户
任务管理器 - 对象 - 管理	管理所有任务管理器对象，例如警报、货币和组织	服务管理员

Table 2-7 (Cont.) Planning 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
任务管理器 - 接受者	有资格作为任务管理器中任务的接受者	• 超级用户 • 服务管理员 • 用户
任务管理器 - 审核 - 查看	查看审核历史记录信息	服务管理员
任务管理器 - 自定义报表 - 管理	设计自定义报表	服务管理员
任务管理器 - 运行仪表板 - 管理	配置运行仪表板	服务管理员
任务管理器 - 公共筛选器和视图 - 管理	发布筛选器和视图以使其可供所有人访问	• 超级用户 • 服务管理员
任务管理器 - 系统服务和设置 - 管理	定义应用程序的系统服务和系统设置	服务管理员
任务管理器 - 任务 - 管理	设计并管理任务、模板和计划	• 超级用户 • 服务管理员
任务管理器 - 用户和团队 - 管理	管理用户和团队	• 超级用户 • 服务管理员
脚注：此角色未映射到任何预定义角色，因此需要将其分配给用户或组才能将其激活。		

Profitability and Cost Management

下表列出并介绍了 Profitability and Cost Management 应用程序角色，并将这些角色与预定义角色对应。

Table 2-8 Profitability and Cost Management 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	管理组，为组或用户分配应用程序角色，以及生成用户安全报表。	服务管理员
访问控制 - 查看	查看用户安全报表（例如角色分配报表、用户登录报表和用户组报表），但无法在访问控制中分配应用程序角色、管理组或执行任何其他更新操作。	服务管理员
数据集成 - 管理员	执行数据集成中的所有功能活动。具有此角色的用户可创建、执行和运行： • 源系统与目标系统之间的集成 • 管道活动 • 使用 EPM 集成代理从内部部署源提取和转换数据和元数据	服务管理员
迁移 - 管理	可以在应用程序中导出和导入快照和对象，通过迁移快照创建应用程序，以及删除之前创建的应用程序。但是，无法克隆环境。此外，还可以查看和调整日常维护开始时间和时区。	服务管理员

Tax Reporting

下表列出并介绍了 Tax Reporting 应用程序角色，并将这些角色与预定义角色对应。

> **Note:**
>
> 应用程序中缺少与预定义角色对应的角色需要单独分配给用户或组。如果未进行此类分配，用户将无法进行与其应用程序角色相关的活动。例如，需要明确向用户授予“即席 - 只读用户”角色（未与下表中的任何预定义角色关联）才能激活其功能。此功能不会自动包含在任何预定义角色中。

Table 2-9 Tax Reporting 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
访问控制 - 管理	使用访问控制执行所有活动，包括管理组，为组或用户分配应用程序角色，以及生成和查看可用报表。	服务管理员
访问控制 - 查看	使用访问控制，查看用户安全报表，例如角色分配报表、用户登录报表和用户组报表。但是，他们无法在访问控制中分配应用程序角色、管理组或执行任何其他更新操作。	服务管理员
即席 - 创建	创建、查看、修改和保存即席网格。	超级用户
即席 - 只读用户	执行所有即席功能，但不能回写到即席网格或使用数据管理加载数据。	请参阅“脚注”
即席 - 用户	查看和修改即席网格以及执行即席操作。即席用户不能保存即席网格。	用户
公告 - 管理	管理在欢迎面板上向用户显示的公告。这些可能指示即将发生的事件，例如系统维护或运行作业。	超级用户
应用程序 - 批量分配	在表单网格内运行批量分配规则。	服务管理员
审批 - 管理	通过手动获取流程的所有权来解决审批问题。包含审批所有权分配者、审核流程设计者以及审批超级用户角色。通常，此角色分配给负责某个地区的业务用户，他们需要控制该地区的审批流程，但不需要服务管理员角色。他们可执行以下任务： • 控制审批流程 • 在其具有写入访问权限的 Planning 单元上执行操作 • 为其负责的组织分配所有者和审核者 • 更改次级维或更新验证规则	服务管理员
审批 - 分配所有权	可对其具有写入访问权限的规划单元层次的任何成员执行下列任务： • 分配所有者 • 分配审核者 • 指定要通知的用户	超级用户
审批 - 设计流程	包括审批所有权分配者角色。此外，还可对其具有写入访问权限的规划单元层次的任何成员执行下列任务： • 更改用户具有写入访问权限的次级维和实体的成员 • 更改规划单元层次的方案和版本分配 • 编辑用户具有访问权限的数据表单的数据验证规则	参阅脚注

Table 2-9 (Cont.) Tax Reporting 应用程序角色

应用程序角色	说明	包括在以下预定义角色中
审批 - 监管	可对用户具有写入访问权限的规划单元层次的任何成员执行下列任务，即使该用户不拥有该规划单元。此用户不能更改不归其所有的规划单元中的数据。 • 停止和启动规划单元 • 在规划单元上执行任何操作	超级用户
仪表板 - 管理	构造和管理自定义仪表板。具有此角色的用户可以： • 配置合规性 • 添加、编辑、复制和删除 • 导入和导出	服务管理员
数据集成 - 创建	使用数据集成创建映射以在源系统与目标系统之间集成数据。用户可以为数据规则定义各种运行时选项。	超级用户
数据集成 - 穿透钻取	穿透钻取到数据的源系统。	• 超级用户 • 用户
数据集成 - 运行	具有此角色的用户可使用数据集成在源和目标之间运行集成。 如果这是分配给用户的唯一角色，并且他们不是超级用户或服务管理员，则他们还可以查看集成详细信息，但无法进行任何更改。	超级用户
文档 - 管理	构造和管理文档。具有此角色的用户可以： • 根据对文档设置的权限添加、编辑、复制和删除文档 • 导入和导出文档	服务管理员
任务列表 - 管理访问	向其他用户分配任务。	超级用户
任务管理器 - 批准者	有资格作为任务管理器中任务的批准者	• 超级用户 • 服务管理员 • 用户
任务管理器 - 对象 - 管理	管理所有任务管理器对象，例如警报、货币和组织	服务管理员
任务管理器 - 接受者	有资格作为任务管理器中任务的接受者	• 超级用户 • 服务管理员 • 用户
任务管理器 - 审核 - 查看	查看审核历史记录信息	服务管理员
任务管理器 - 自定义报表 - 管理	设计自定义报表	服务管理员
任务管理器 - 运行仪表板 - 管理	配置仪表板	服务管理员
任务管理器 - 公共筛选器和视图 - 管理	发布筛选器和视图以使其可供所有人访问	• 超级用户 • 服务管理员
任务管理器 - 系统服务和设置 - 管理	定义应用程序的系统服务和系统设置	服务管理员
任务管理器 - 任务 - 管理	设计并管理任务、模板和计划	• 超级用户 • 服务管理员
任务管理器 - 用户和团队 - 管理	管理用户和团队	• 超级用户 • 服务管理员

Table 2-9 (Cont.) Tax Reporting 应用程序角色

应用程序角色	说明	包括在以下预定义角色中

脚注：此角色未映射到任何预定义角色，因此需要将其分配给用户或组才能将其激活。

为组或用户分配应用程序角色

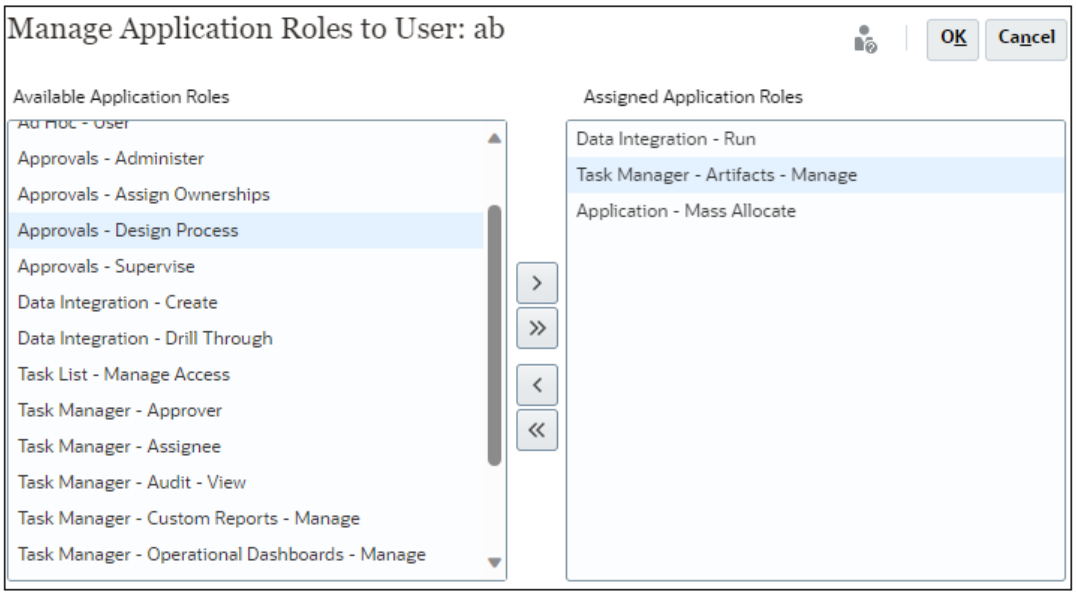
在此过程中，服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以为具有预定义角色的 EPM 和 IDCS 组和用户分配或取消分配应用程序角色。他们还可以为自己分配应用程序角色。

有关组和分配给组的角色的信息，请参阅“管理组”。

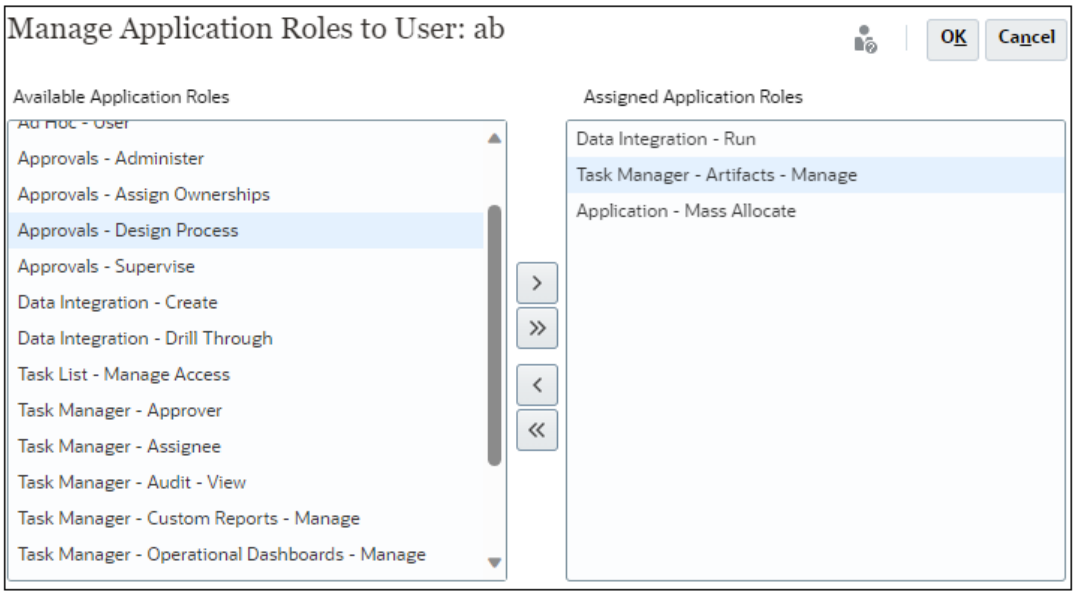
要为组或用户分配或取消分配应用程序角色：

1. 打开**访问控制**。请参阅“打开访问控制”。
2. 单击**管理应用程序角色**选项卡。
3. 查找某个用户或组。从下拉列表中选择**用户**或**组**。有关使用搜索功能的说明，请参阅“使用搜索”。

   将列出符合搜索条件的用户或组（EPM 或 IDCS）。默认情况下，列表先按照**用户登录**值排序，然后按照**组名**值排序（适用于组搜索）。
4. 单击用户或组的 （**操作**），然后选择**管理角色**。
5. 要为用户或组分配应用程序角色，请从**可用的应用程序角色**列表中进行选择，然后单击右箭头按钮。



   要了解适用于各个业务流程的应用程序角色，请参阅“在应用程序级别管理角色分配”。
6. 如果要取消分配应用程序角色，请从**分配的应用程序角色**列表中进行选择，然后单击左箭头键。



7. 单击**确定**完成用户或组的应用程序角色分配。
8. 再次单击**确定**以返回**管理应用程序角色**选项卡。

3
生成报表

服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以生成以下报表来分析和管理角色分配：

- 为用户或组生成角色分配报表
- 查看环境的角色分配报表
- 查看用户登录报表
- 查看用户组报表

报表中指示的报表生成时间所反映的时间基于浏览器时区（本地系统时钟）。

关于报表的 CSV 版本

可以导出报表来创建该报表的逗号分隔值 (CSV) 版本。除了分配给预定义角色的用户数量计数，报表的 CSV 版本还列出以下项：

- 分配给每个用户的预定义角色。分配给用户的每个预定义角色都在单独的一行中显示。已纳入预定义角色的应用程序角色将不会列出。
- 直接或通过组分配给用户的应用程序角色。分配给用户的每个应用程序角色都在单独的一行中显示。
- 如果用户所分配到的组未分配任何角色，则该组不会列出。
- 仅报表的当前视图中的信息会导出到 CSV。例如，如果您筛选报表，以查看特定用户的角色分配，则导出的 CSV 文件仅包含该用户的分配情况。

故障排除

请参阅《运维指南》中的“对报表问题进行故障排除”。

为用户或组生成角色分配报表

使用角色分配报表，可以跟踪用户访问权限以进行合规性报告。

此报表显示为其分配了预定义角色的所有活动用户。已停用的用户不反映在此报表中。如果用户所属的 IDCS 或 EPM 组未用于将应用程序角色分配给用户，将不列出这些组。服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以访问角色分配报表来查看为用户或组分配的预定义角色和应用程序角色。
要为用户或组生成角色分配报表：

1. 打开**访问控制**。请参阅“打开访问控制”。
2. 单击**管理应用程序角色**选项卡。
3. 查找某个用户或组。从下拉列表中，选择**用户**或**组**。有关使用搜索功能的说明，请参阅“使用搜索”。

   将列出符合搜索条件的用户或组。默认情况下，报表先按照**用户登录**值排序，然后按照**组名**排序（适用于组搜索）。
4. 单击用户或组的 ⚙，然后选择**角色分配报表**。

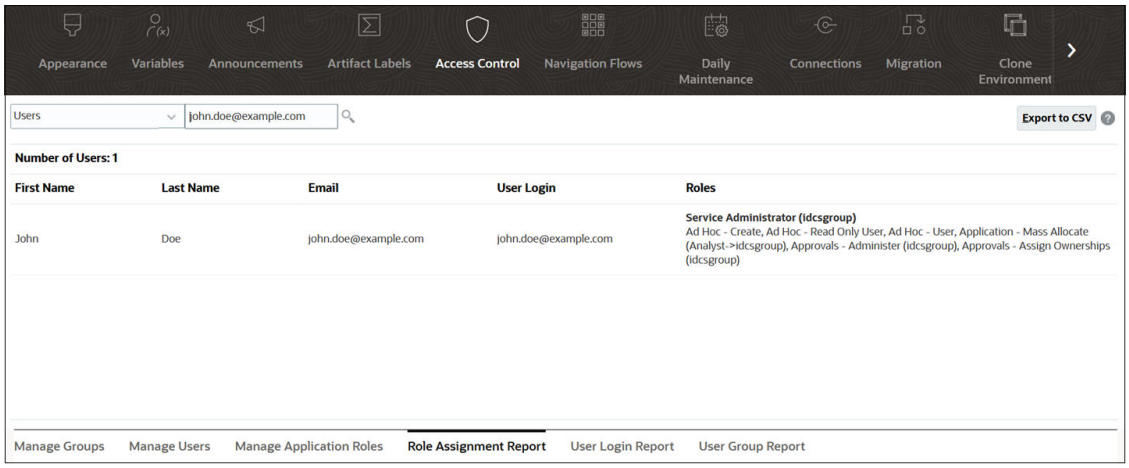
5. **可选：**单击**导出到 CSV** 以将报表导出为 CSV 文件。

查看环境的角色分配报表

服务管理员或具有“访问控制 - 管理”应用程序角色的用户可使用角色分配报表查看通过预定义角色（粗体）和应用程序级角色分配给所有用户的访问权限。此报表显示为其分配了预定义角色的所有活动用户。已停用的用户不反映在此报表中。

对于每个用户，继承的角色以及有关继承的信息将显示在一行中。

如果为 IDCS 组分配了预定义角色或应用程序角色，该报表将显示通过 IDCS 组间接分配给用户的预定义角色。例如，假定用户 John Doe 分配为 idcsgroup 的成员，且此组分配到服务管理员预定义角色。在这种情况下，角色分配报表显示以下内容作为 John Doe 的角色分配信息的一部分：



可以将角色分配报表导出为 CSV 文件，然后可以使用 Microsoft Excel 等程序打开该文件或将其保存到计算机。CSV 格式的角色分配报表针对每个角色分配显示一行。

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

要打开角色分配报表：

1. 打开**访问控制**。请参阅“打开访问控制”。
2. 单击**角色分配报表**。

   此时将显示角色分配报表。
3. **可选：**筛选报表，使其显示以下内容：
   - 特定用户的角色分配。从下拉列表中选择**用户**，然后输入部分搜索字符串。有关使用搜索功能的说明，请参阅“使用搜索”。
   - 分配给特定角色的用户。从下拉列表中选择**角色**，然后输入部分角色名称。有关使用搜索功能的说明，请参阅“使用搜索”。

> **注：**
>
> 可以将用户分配给许多角色。在这种情况下，报表会列出用户的所有角色，即使您在报表中筛选了特定角色也是如此。

此时将显示角色分配报表。默认情况下，报表先按照**用户登录**值排序，然后按照**角色**下的应用程序角色排序（适用于按角色进行的搜索）。预定义角色以粗体显示，而应用程序角色以非粗体显示。

4. **可选：**单击**导出到 CSV** 以将报表导出为 CSV 文件。请注意，仅当前显示的报表中的信息会导出到 CSV。

查看用户登录报表

用户登录报表默认情况下包含有关过去 24 小时内登录过环境的用户的相关信息。该报表列出用户从中登录的计算机的 IP 地址以及用户访问环境的日期和时间 (UTC)。

服务管理员或具有“访问控制 - 管理”应用程序角色的用户可以基于自定义日期范围或系统提供的时间段（过去 30 天、过去 90 天和过去 120 天）重新生成此报表。他们还可以通过使用用户名字、姓氏或用户 ID 的部分字符串作为搜索字符串来筛选报表，以仅查看特定用户的信息。

> **注：**
>
> Oracle Fusion Cloud Enterprise Performance Management 仅保留过去 120 天的用户登录审核历史记录。

要重新生成用户登录报表：

1. 打开**访问控制**。请参阅“打开访问控制”。
2. 单击**用户登录报表**。

   此时将显示一个报表，其中列出了前一天登录到环境的所有用户。
3. 选择生成报表所基于的期间（前 1 天、过去 30 天、过去 90 天或过去 120 天）。要指定自定义日期范围，请选择**日期范围**并选择开始日期和结束日期。
4. **可选：**选择要包含在报表中的用户。有关使用搜索功能的说明，请参阅“使用搜索”。

   将显示用户登录报表。默认情况下，报表按**访问日期和时间**值排序。
5. **可选：**单击**导出到 CSV** 以将显示的报表导出为 CSV 文件。
6. 单击**取消**可关闭报表。

查看用户组报表

用户组报表列出在访问控制中分配到 EPM 组的用户的直接或间接成员身份。具有“访问控制 - 管理”应用程序角色的用户可以生成此报表。

如果将用户分配到组，则他们被认为是该组的直接成员；如果将用户分配到另一个组的子组，则他们被认为是间接成员。对于分配到组的每个用户，报表将列出以下信息：登录 ID、名字和姓氏、电子邮件 ID、将用户直接或间接分配到的组的逗号分隔列表等等。直接组以粗体显示，而间接组以非粗体显示。

报表的 CSV 版本将使用是或否指明用户是直接还是间接分配到组。

> **注：**
>
> 此报表不适用于 Account Reconciliation 和 Narrative Reporting。

要生成用户组报表：

1. 打开**访问控制**。请参阅“打开访问控制”。
2. 单击**用户组报表**。
3. **可选：**筛选报表。从下拉列表中，选择**用户**或**组**。有关使用搜索功能的说明，请参阅“使用搜索”。

   将显示用户组报表。默认情况下，报表按**用户登录**值排序。
4. 单击**取消**可关闭报表。
5. **可选：**单击**导出到 CSV** 以将 EPM 组名称和说明导出到 `Groups.csv` 文件。

   PREDEFINED 或 IAM 组无法使用此选项导出。如果不存在任何 EPM 组，则**导出到 CSV** 处于禁用状态。访问控制中应该至少有一个 EPM 组才能使用此选项。
6. **可选：**单击**从 CSV 导入**以将 CSV 文件中的 EPM 用户的组分配导入到访问控制中。

   有关 CSV 文件格式的信息和其他详细信息，请参阅“从文件导入用户的组分配”。