

Oracle® Fusion Cloud EPM

Administración del control de acceso para
Oracle Enterprise Performance Management
Cloud



F28929-21

ORACLE®

Oracle Fusion Cloud EPM Administración del control de acceso para Oracle Enterprise Performance Management Cloud,

F28929-21

Copyright © 2015, 2024, Oracle y/o sus filiales.

Autor principal: 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.

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>.

Tabla de contenidos

Accesibilidad a la documentación

Comentarios sobre la documentación

1 Descripción general de Control de acceso

Acerca de esta guía	1-1
Apertura de Control de acceso	1-2
Gestión de grupos	1-2
Creación de grupos	1-3
Modificación de grupos	1-4
Supresión de grupos	1-5
Exportación de grupos de EPM Cloud a un archivo CSV	1-5
Importación de asignaciones de grupos de usuarios de un archivo	1-6
Asignación de un usuario a varios grupos	1-7
Uso de la función de búsqueda	1-8

2 Gestión de asignaciones de roles en el nivel de aplicación

Descripción general de la asignación de roles de la aplicación	2-1
Account Reconciliation	2-3
Roles de aplicación	2-3
Asignación de roles predefinidos	2-6
Enterprise Profitability and Cost Management	2-7
Roles de aplicación	2-7
Asignación de roles predefinidos	2-9
Planning, FreeForm, Financial Consolidation and Close y Tax Reporting	2-11
Roles de la plataforma EPM Cloud	2-11
Roles de Data Integration	2-13
Roles relacionados con asientos de consolidación	2-13
Roles del gestor de tareas	2-14
Asignación de roles predefinidos	2-15

Rentabilidad y gestión de costes	2-16
Roles de aplicación	2-16
Asignación de roles predefinidos	2-16
Oracle Enterprise Data Management Cloud y Enterprise Data Management	2-17
Roles de aplicación	2-17
Asignación de roles predefinidos	2-17
Asignación de roles de aplicación a un grupo o un usuario	2-18
Eliminación de roles de nivel de aplicación asignados a un grupo o un usuario	2-20

3 Generación de informes

Generación de informes de asignación de roles para un usuario o un grupo	3-1
Visualización de informes de asignación de roles para el entorno	3-2
Visualización del informe de inicio de sesión de usuario	3-3
Visualización y exportación del informe de grupo de usuarios	3-4

Accesibilidad a la documentación

Para obtener información acerca del compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Acceso a Oracle Support

Los clientes de Oracle que hayan adquirido soporte disponen de acceso a soporte electrónico a través de My Oracle Support. Para obtener información, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si tiene problemas de audición.

Comentarios sobre la documentación

Para hacernos llegar sus comentarios sobre esta documentación, haga clic en el botón Comentarios en la parte inferior de la página de cualquier tema de Oracle Help Center. También puede enviar un correo electrónico a epmdoc_ww@oracle.com.

1

Descripción general de Control de acceso

El acceso a los componentes de Oracle Enterprise Performance Management Cloud está controlado por los roles predefinidos del dominio de identidad al que estén asignados los usuarios. Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden asignar usuarios a roles específicos de aplicación de planificación, consolidación, conciliación de cuentas y gestión de datos para permitirles realizar tareas adicionales en un entorno.

Por ejemplo, los administradores de servicio pueden asignar un usuario al rol de administrador de aprobaciones de una aplicación de planificación o consolidación para permitir al usuario realizar actividades relacionadas con las aprobaciones.

Además, los administradores del servicio pueden crear grupos en Control de acceso que incluyan a los usuarios del dominio de identidad u otros grupos. La asignación de roles a estos grupos permite a los administradores de servicio otorgar roles a varios usuarios a la vez, lo cual reduce la sobrecarga administrativa.

La asignación de roles en el nivel de aplicación solo puede mejorar los derechos de acceso de los usuarios; ninguno de los privilegios que haya otorgado un rol predefinido puede restringirse mediante los roles asignados en el nivel de aplicación.

Control de acceso permite realizar estas actividades en un entorno:

- [Gestión de grupos](#)
- [Asignación de roles de aplicación a un grupo o un usuario](#)
- [Generación de informes de asignación de roles para un usuario o un grupo](#)
- [Visualización de informes de asignación de roles para el entorno](#)
- [Visualización del informe de inicio de sesión de usuario](#)

Enlace del tutorial

También puede seguir este tutorial [Configuración de seguridad en procesos de negocio de Cloud EPM](#) para obtener información sobre las capas de seguridad en los procesos de negocio de EPM Cloud y cómo gestionar la seguridad mediante el Control de acceso y los permisos de acceso.

Acerca de esta guía

El control de acceso se aplica a estos procesos de negocio de Oracle Enterprise Performance Management Cloud:

- Planning
- Módulos de Planning
- FreeForm
- Financial Consolidation and Close
- Tax Reporting

- Rentabilidad y gestión de costes
- Enterprise Profitability and Cost Management
- Account Reconciliation
- Oracle Enterprise Data Management Cloud
- Narrative Reporting
- Strategic Workforce Planning
- Sales Planning

Apertura de Control de acceso

Puede asignar roles específicos de la aplicación a grupos y usuarios desde **Control de Acceso**, que está disponible en la tarjeta **Herramientas** de la página de inicio.

Para abrir Control de acceso:

1. Acceda al entorno como administrador del servicio o un usuario con el rol de aplicación Control de acceso - Gestionar.
2. Realice un paso:
 - Haga clic en  (Navegador) y, a continuación, en **Control de acceso**.
 - Haga clic en **Herramientas** y, a continuación, en **Control de acceso**.
 - **Solo Narrative Reporting**: haga clic en **Control de acceso**.

Gestión de grupos

Oracle Enterprise Performance Management Cloud utiliza un repositorio interno para admitir las asignaciones de roles en el nivel de aplicación y almacenar información en los grupos de EPM Cloud que se utilicen durante el proceso de asignación de roles.

Los usuarios de EPM Cloud y otros grupos de usuarios pueden ser miembros de grupos que se mantienen con Control de acceso. Se puede otorgar roles de aplicación a los usuarios mediante la asignación de un rol al grupo.

Para que pueda ver las asignaciones de usuario, Control de acceso muestra los roles y los grupos predefinidos. No puede modificar ni asignarles los roles desde Control de acceso. Además, los usuarios de EPM Cloud, que están asignados a roles predefinidos, se muestran en Control de acceso de manera que puedan agregarse como miembros del grupo. Consulte Descripción de roles predefinidos en *Introducción a Oracle Enterprise Performance Management Cloud para administradores*.

En **Gestionar grupos**, los grupos se ordenan de forma predeterminada por valores **Nombre de grupo**. Para buscar un grupo específico, consulte [Uso de la función de búsqueda](#) para obtener instrucciones.

Puede gestionar los grupos de estas formas:

- [Creación de grupos](#)
- [Modificación de grupos](#)
- [Supresión de grupos](#)
- [Exportación de grupos de EPM Cloud a un archivo CSV](#)



Nota:

No puede utilizar el Control de acceso para importar información de grupo de un archivo para crear grupos. Puede utilizar Migración o el comando createGroups de EPM Automate para importar grupos.

Solución de problemas

Consulte Resolución de problemas de gestión de usuarios, roles y grupos en *Guía de operaciones de Oracle Enterprise Performance Management Cloud*.

Creación de grupos

Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden crear y gestionar grupos. Los usuarios de Oracle Enterprise Performance Management Cloud y otros grupos pueden ser miembros de un grupo.



Nota:

También puede utilizar Migración o el comando createGroups de EPM Automate para importar información de grupo de un archivo para crear grupos.

Para crear grupos:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. En **Gestionar grupos**, haga clic en **Crear**.
3. En **Crear grupo**, realice estos pasos:
 - a. En **Nombre**, introduzca un nombre de grupo único (256 caracteres como máximo). Los nombres de grupos no distinguen mayúsculas y minúsculas.
EPM Cloud no permite crear grupos que tengan los mismos nombres que los roles (Administrador del servicio, Usuario avanzado, Usuario, Planificador y Visor).
 - b. **Opcional:** Introduzca una descripción de grupo.
4. **Opcional:** Agregue grupos para crear un grupo anidado.
 - a. En **Grupos disponibles**, busque los grupos. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.
Se muestran los grupos que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Nombre de grupo**.
 - b. En **Grupos disponibles**, seleccione los grupos de miembros para el nuevo grupo.
 - c. Haga clic en **Mover**.
Los grupos seleccionados se muestran debajo de **Grupos asignados**. Para eliminar grupos asignados, seleccione los grupos que desea eliminar en **Grupos asignados** y, a continuación, haga clic en **Eliminar**.
5. **Opcional:** Agregue usuarios de EPM Cloud como miembros del grupo.
Solo los usuarios que están asignados a un rol predefinido pueden agregarse como miembros del grupo.

- a. Haga clic en **Usuarios**.
 - b. En **Usuarios disponibles**, busque usuarios. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones.

Se muestran los usuarios que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Conexión de usuario**.
 - c. En **Usuarios disponibles**, seleccione los usuarios que agregar al grupo.
 - d. Haga clic en **Mover**.
6. Haga clic en **Guardar**.
 7. Haga clic en **Aceptar**.

Modificación de grupos

Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden modificar propiedades de grupo, incluido el nombre de grupo. Los roles de aplicación asignados al grupo y otras asignaciones de seguridad no se ven afectados si se cambia el nombre de un grupo.

Para modificar los grupos:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. **Opcional:** En **Administrar grupos**, busque el grupo que desea modificar. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.

Se muestran los grupos que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Nombre de grupo**.

Nota:

Los nombres de grupo pueden contener un máximo de 256 caracteres. Los caracteres visibles, por ejemplo, en la columna **Grupos disponibles**, se pueden truncar en función de la resolución de la pantalla.

3. Haga clic en  (Acción) en la fila del grupo que desea modificar y, a continuación, seleccione **Editar**.
4. **Opcional:** modifique el nombre del grupo. Los cambios en el nombre del grupo no afectan a las asignaciones de seguridad realizadas utilizando el grupo.
5. Modifique la asignación de los grupos:
 - a. **Opcional:** Agregue grupos anidados:
 - En **Grupos disponibles**, busque los grupos. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.

Se muestran los grupos que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Nombre de grupo**.
 - En **Grupos disponibles**, seleccione los grupos y haga clic en **Mover**.

Los grupos seleccionados se muestran en la lista **Grupos asignados**.

- b. **Opcional:** Elimine los grupos anidados:
 - En **Grupos asignados**, seleccione el grupo que eliminar.
 - Haga clic en **Eliminar**.
6. Modifique la asignación de los usuarios:
 - a. Haga clic en **Usuarios**.
 - b. **Opcional:** Agregue usuarios al grupo:
 - En **Usuarios disponibles**, busque usuarios que pueda asignar como miembros de grupo. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.

Se muestran los usuarios que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Conexión de usuario**.

 - En **Usuarios disponibles**, seleccione los usuarios y haga clic en **Mover**.

Los usuarios seleccionados se muestran en la lista **Usuarios asignados**.
 - c. **Opcional:** Elimine usuarios del grupo:
 - En **Usuarios asignados**, seleccione los usuarios que eliminar.
 - Haga clic en **Eliminar**.
7. Haga clic en **Guardar**.
8. Haga clic en **Aceptar**.

Supresión de grupos

Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden suprimir grupos. La supresión de un grupo no suprime los miembros del grupo.

Para suprimir un grupo:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
 2. **Opcional:** En **Administrar grupos**, busque el grupo que desea suprimir. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.
- Se muestran los grupos que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Nombre de grupo**.
3. Haga clic en  (Acción) en la fila del grupo que desea suprimir y, a continuación, seleccione **Suprimir**.
 4. Haga clic en **Sí** para confirmar la operación de supresión.
 5. Haga clic en **Aceptar**.

Exportación de grupos de EPM Cloud a un archivo CSV

Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden exportar el nombre y las descripciones de grupo de Oracle Enterprise

Performance Management Cloud al archivo `Groups.csv` mediante **Exportar a CSV**. No se exportará ningún grupo predefinido.

La opción **Exportar a CSV** está desactivada si no existe ningún grupo de EPM Cloud. Debe haber al menos un grupo de EPM Cloud en Control de acceso para usar esta opción.

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
En el separador **Gestionar grupos** se muestran todos los grupos disponibles.
2. Haga clic en **Exportar a CSV** para exportar todos los grupos de EPM Cloud.
3. Siga las instrucciones en pantalla para abrir o guardar el archivo `Groups.csv`.

Importación de asignaciones de grupos de usuarios de un archivo

Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden importar asignaciones de grupos de usuarios de un archivo de valores separados por comas (CSV) para crear asignaciones nuevas en un grupo de Control de acceso existente. Oracle Enterprise Performance Management Cloud fuerza las asignaciones de seguridad a nivel de aplicación y de artefacto basadas en las nuevas asignaciones de grupo.



Nota:

Todas las conexiones de usuario identificadas en el archivo de importación deben existir en el dominio de identidad; todos los nombres de grupo que se incluyen en el archivo deben existir en el Control de acceso. No puede crear un grupo mediante este proceso de importación.

Solo puede crear nuevas asignaciones de grupo; no puede eliminar las asignaciones de grupo actuales de usuarios.

El formato de archivo CSV de importación puede ser como se muestra en las siguientes ilustraciones:

```
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
```

Este formato es idéntico a la versión CSV del informe de grupo de usuarios. Si utiliza este formato, el proceso de importación ignora todas las columnas que no sean conexión de usuario y grupo. Una manera fácil de crear un archivo de importación es

exportar el informe de grupo de usuarios y modificarlo según sea necesario. Consulte [Visualización y exportación del informe de grupo de usuarios](#).

Para importar asignaciones de grupo de usuarios:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en **Informe de grupos de usuarios**.
3. Haga clic en **Importar de CSV**.
4. Con **Buscar** en **Importar CSV de asignación de grupo de usuarios**, seleccione el archivo de importación.
5. Haga clic en **Importar**.
6. Haga clic en **Sí**.

Cuando complete el proceso de importación, se mostrará un cuadro de diálogo de confirmación, que identifica el número total de asignaciones procesadas y su estado.

Asignación de un usuario a varios grupos

Los usuarios de Oracle Enterprise Performance Management Cloud pueden ser miembros de varios grupos mantenidos mediante un Control de acceso. Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden asignar un usuario a varios grupos.



Nota:

En un momento dado, un usuario puede ser miembro de un máximo de 1000 grupos, ya sea directa o indirectamente.

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en **Gestionar usuarios**.
3. Busque el usuario que se va a asignar a los grupos. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.
Se muestran los usuarios que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Conexión de usuario**.
4. Haga clic en  (Acción) en la fila de la lista de usuarios y, a continuación, seleccione **Editar**.
Aparecerá la pantalla **Editar usuario**, que muestra información del usuario detallada, incluida su pertenencia a grupos actual (en **Grupos asignados**). En esta pantalla, solo puede modificar las asignaciones de grupos.
5. Busque los grupos para asignarlos al usuario. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.
Se muestran los grupos que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Nombre de grupo**.
6. Complete una acción:
 - Para asignar grupos adicionales al usuario, en **Grupos disponibles**, seleccione uno o más grupos y haga clic en  (**Mover**) para mover los grupos seleccionados a

Grupos asignados. También puede hacer clic en  (**Mover todo**) para mover todos los grupos de **Grupos disponibles** a **Grupos asignados**.

- Para eliminar los grupos asignados al usuario, en **Grupos asignados**, seleccione uno o más grupos y haga clic en  (**Eliminar**) para mover los grupos seleccionados a **Grupos disponibles**. También puede hacer clic en  (**Eliminar todo**) para mover todos los grupos de **Grupos asignados** a **Grupos disponibles**.

7. Haga clic en **Guardar**.

8. Haga clic en **Aceptar**.

Uso de la función de búsqueda

La búsqueda inteligente de artefactos de grupo y usuarios funciona del mismo modo en todo el Control de acceso.

Utilice una cadena de uno de los atributos de usuario (nombre de usuario, nombre, apellidos o ID de correo electrónico) o el nombre del grupo o del rol para buscar usuarios, grupos o roles específicos. No es necesario utilizar caracteres comodines en las cadenas de búsqueda. Por ejemplo, si utiliza la cadena `st` para buscar grupos, se mostrarán todos los nombres de grupos que contengan la cadena `st`, por ejemplo, `TestGroup`, `Strategic_Planner`, `AnalystsGroup`, etc. Del mismo modo, si utiliza la cadena `jd` para buscar usuarios, se mostrarán los usuarios cuyo nombre de usuario, nombre, apellido o dirección de correo electrónico contengan la cadena `jd`.

Nota:

Algunas pantallas de Control de acceso, por ejemplo, **Asignar roles de aplicación**, **Informe de asignación de roles** e **Informe de grupo de usuarios**, le ofrecen opciones de búsqueda. Haga una selección adecuada antes de empezar una búsqueda.

Para buscar usuarios:

1. Acceda a una pantalla, por ejemplo, **Gestionar usuarios**, donde la función de búsqueda de usuario esté disponible.
2. En el campo de búsqueda, introduzca una cadena parcial de un atributo de usuario (nombre de usuario, nombre, apellido o ID de correo electrónico).
3. Haga clic en  (Buscar).
Los resultados de búsqueda muestran todas las propiedades disponibles para los usuarios que coinciden con el criterio de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Conexión de usuario**.

Para buscar grupos:

- Acceda a una pantalla, por ejemplo, **Gestionar grupos**, donde la función de búsqueda de grupo esté disponible.
- En el campo de búsqueda, introduzca una cadena parcial de un nombre de grupo.
- Haga clic en  (Buscar).

Los resultados de búsqueda muestran el nombre y la descripción de grupos que coinciden con el criterio de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Nombre de grupo**.

The screenshot shows the 'Create Group' interface. At the top, there are 'Save' and 'Close' buttons. Below them, there are input fields for '* Name' (containing 'Example') and 'Description'. There are two tabs: 'Groups' and 'Users', with 'Users' being the active tab. Under the 'Users' tab, there is a search input field containing 'exam' and a search icon. Below this, there are two tables. The left table is titled 'Available Users' and contains three rows of user data. The right table is titled 'Assigned Users' and contains the text 'No records were found.' There is a double arrow button between the two tables.

First Name	Last Name	Email	User Login
John	Doe	john.doe@exam...	jdoe
Jane	Doe	jane.doe@exam...	jadoe31
Jane	Doe	jane.x.doe@exam	jadoe41

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

Para buscar usuarios según sus roles en el informe de asignación de roles:

- Acceda al separador **Informe de asignación de roles**.
- Seleccione **Usuarios** o **Roles** en la lista desplegable de búsqueda.
- En el campo de búsqueda, introduzca una cadena de búsqueda.
- Haga clic en  (Buscar).
Los resultados de búsqueda muestran toda la información disponible para los usuarios asignados a los roles que coinciden con el criterio de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Conexión de usuario**.

2

Gestión de asignaciones de roles en el nivel de aplicación

Related Topics

- [Descripción general de la asignación de roles de la aplicación](#)
- [Account Reconciliation](#)
- [Enterprise Profitability and Cost Management](#)
- [Planning, FreeForm, Financial Consolidation and Close y Tax Reporting](#)
- [Rentabilidad y gestión de costes](#)
- [Oracle Enterprise Data Management Cloud y Enterprise Data Management](#)
- [Asignación de roles de aplicación a un grupo o un usuario](#)
- [Eliminación de roles de nivel de aplicación asignados a un grupo o un usuario](#)

Descripción general de la asignación de roles de la aplicación

El control de acceso le permite ampliar las funciones de acceso del usuario de Oracle Enterprise Performance Management Cloud que no sean los roles predefinidos mediante la asignación de estos a nivel de aplicación (roles de aplicación).

Los roles predefinidos (Administrador del servicio, Usuario avanzado, Usuario y Visor) son jerárquicos; un rol superior hereda los privilegios incluidos en los roles inferiores. Por ejemplo, el rol Usuario hereda el acceso a la aplicación EPM Cloud otorgado mediante el rol Visor. Del mismo modo, el rol Usuario avanzado hereda los privilegios de acceso que otorga el usuario visor.

Los roles de aplicación solo pueden mejorar los derechos de acceso de los usuarios; ninguno de los privilegios que haya otorgado un rol predefinido se puede restringir. Puede gestionar el proceso de asignación de roles mediante Access Control y realizar estas tareas:

- Crear grupos y agregar usuarios de EPM Cloud u otros grupos como miembros.
- Agregar o suprimir miembros del grupo
- Asignar roles de aplicación a grupos o a usuarios incluido usted mismo
- Ver la lista de usuarios que son miembros de un grupo

Aunque los derechos de acceso generales se controlan con los roles predefinidos, los administradores del servicio o un usuario con el rol de aplicación Control de acceso - Gestionar pueden otorgar roles específicos de la aplicación a los usuarios y los grupos creados y gestionados en Control de acceso.

Asigne el rol de aplicación adecuado a los usuarios si necesitan ejecutar algunas funciones que vayan más allá de las asignadas en sus roles predefinidos. Por ejemplo, de forma predeterminada, solo los administradores del servicio y los usuarios avanzados pueden acceder a Data Integration. Para permitir que los usuarios con los roles predefinidos Usuario

o Visor participen en el proceso de integración, los administradores del servicio deben asignarles roles de Data Integration (Data Integration - Crear).

Procesos de negocio que soportan la asignación de roles de aplicación

Los procesos de negocio que soportan la asignación de roles de aplicación son:

- Planning, FreeForm, Financial Consolidation and Close y Tax Reporting
- Enterprise Profitability and Cost Management
- Oracle Enterprise Data Management Cloud
- Account Reconciliation

Otros procesos de negocio como Profitability and Cost Management y Narrative Reporting no soportan la asignación de roles de aplicación.

Mejor práctica para asignar roles de aplicación a un rol predefinido

La mejor práctica recomendada consiste en asignar el rol mínimo que se ajuste a los privilegios adicionales cuando sea necesario. Aquí se muestran algunos ejemplos de situaciones en las que puede que desee otorgar roles de aplicación a alguien que no tenga esos privilegios según su rol predefinido.

- Agregue el rol de aplicación **Preparador** a un Visor que tenga que preparar conciliaciones.
- Tenga un diseñador de informes que solo trabaje diseñando informes y no las demás funcionalidades de la aplicación. Puede asignarle el rol Visor y, a continuación, asignar el rol de aplicación **Gestionar informes**
- Permita a un Usuario avanzado gestionar tipos de alertas para que pueda asignar el rol de aplicación **Gestionar tipos de alerta**



Note:

Los privilegios otorgados son solo adicionales. Esto significa que los puede agregar a los privilegios que tenga un rol predefinido de un usuario, pero que no puede eliminar los privilegios que se otorguen automáticamente a ese rol predefinido.

Si desea migrar aplicaciones desde un entorno local a EPM Cloud, consulte "Asignación de roles para la migración a EPM en la nube" en *Administración de migración de Oracle Enterprise Performance Management Cloud* para comprender cómo debe asignar roles predefinidos a los usuarios.

Usuarios de EPM Cloud

Puede crear y gestionar usuarios de EPM Cloud en el dominio de identidad asociado al entorno al que pertenece el proceso de negocio. Solo a los usuarios asignados a roles predefinidos se les pueden asignar roles a nivel de aplicación para mejorar su acceso a la realización de tareas en un proceso de negocio.

Acerca de los roles predefinidos

Consulte estos temas en *Introducción a Oracle Enterprise Performance Management Cloud para administradores* para obtener información sobre los roles predefinidos:

- Acerca de la gestión de usuarios y funciones
- Descripción de los roles predefinidos
- Roles predefinidos de Planning, Planning Modules y FreeForm
- Roles predefinidos de Financial Consolidation and Close
- Roles predefinidos de Tax Reporting
- Roles predefinidos de Profitability and Cost Management
- Roles predefinidos de Enterprise Profitability and Cost Management
- Roles predefinidos en Account Reconciliation
- Roles predefinidos de Enterprise Data Management
- Roles predefinidos de Strategic Workforce Planning
- Roles predefinidos de Narrative Reporting
- Roles predefinidos de Sales Planning

Solución de problemas

Consulte Resolución de problemas de gestión de usuarios, roles y grupos en *Guía de operaciones de Oracle Enterprise Performance Management Cloud*.

Account Reconciliation

Related Topics

- [Roles de aplicación](#)
- [Asignación de roles predefinidos](#)

Roles de aplicación

Los siguientes roles se aplican solo a **Account Reconciliation**. De forma predeterminada, estos roles de aplicación se incluyen en los roles predefinidos. Consulte [Asignación de roles predefinidos](#). Los roles de aplicación se pueden asignar a los usuarios que necesiten llevar a cabo operaciones que no estén incluidas en los privilegios recibidos en sus roles predefinidos.

Tipos de alerta - Gestionar

Gestiona tipos de alerta para definir un procedimiento que seguir cuando se produce una determinada incidencia.

Anuncios - Gestionar

Gestiona anuncios que se muestran a los usuarios en el Panel de bienvenida. Estos pueden indicar próximos eventos, como el mantenimiento del sistema o la ejecución de trabajos.

Auditoría - Ver

Proporciona acceso a todos los detalles de auditoría. Sin embargo, este rol de aplicación no permite activar el inicio del cuadro de diálogo Acciones de conciliación, ya que Conciliaciones está fuera de su ámbito de seguridad.

Monedas - Gestionar

Configura Monedas, Tipos de cambio, y Depósitos de monedas. Los usuarios con este rol pueden controlar qué códigos de moneda están activos en el sistema.

Paneles - Gestionar

Crea y gestiona paneles personalizados. Los usuarios con este rol pueden:

- Configurar la conformidad
- Agregar, editar, duplicar y suprimir
- Importar y exportar

Data Integration - Administrador

Realiza todas las actividades funcionales en Data Integration. Los usuarios con este rol crean, realizan y ejecutan:

- Integraciones entre el sistema de origen y el sistema de destino
- Actividades del pipeline
- Extracción y transformación de datos y metadatos de orígenes locales utilizando el Agente de integración de EPM

Data Integration - Crear

Utiliza Data Integration para crear asociaciones con el fin de integrar datos entre el sistema de origen y el sistema de destino. Este rol puede definir reglas de datos con varias opciones de tiempo de ejecución.

Data Integration - Obtener detalles

Obtiene detalles del sistema de origen de los datos.

Data Integration - Ejecutar

En Data Integration, ejecuta reglas de datos con parámetros de tiempo de ejecución y visualiza logs de ejecución.

Cargas de datos - Gestionar

Define las definiciones de carga de datos para cargar datos mediante Data Integration y guardar esos mismos parámetros de carga de datos. Visualiza el estado más reciente de las cargas de datos y supervisa el procesamiento de las solicitudes de cambio del usuario.

Trabajos - Ver

Visualiza el trabajo y el estado de los trabajos de Account Reconciliation.

Tipos de confrontación - Gestionar

Los usuarios con este rol pueden gestionar tipos de confrontación, atributos de ajuste, atributos de soporte, columnas de asiento y atributos de grupo.

Tipos de confrontación - Ver

Los usuarios con este rol pueden visualizar los detalles de tipos de confrontación, atributos de ajuste, atributos de soporte y columnas de asiento.

Organizaciones - Gestionar

Asigna una estructura organizativa jerárquica a perfiles y conciliaciones.

Períodos - Gestionar

Gestiona las propiedades del período. También pueden definir el estado de los períodos, la carga de datos y realizar otras operaciones en los períodos existentes.

Períodos - Ver

Los usuarios con este rol pueden ver (solo acceso de lectura) el número de períodos asociados a las conciliaciones, así como cargar datos en el período.

Perfiles - Ver

Visualiza y reasigna perfiles.

Perfiles y conciliaciones - Gestionar

Gestiona los siguientes perfiles y conciliaciones: Segmentos de perfil, Proceso, Clasificación de riesgo, Frecuencias, Tipo de cuenta, Perfiles de validez y Símbolos de integración global. Oracle le recomienda que se asegure de que el ámbito de seguridad esté definido adecuadamente para este usuario.

Filtros y vistas públicos - Gestionar

Los filtros controlan los registros que ve el usuario en las vistas de lista e informes. Puede aplicar filtros en perfiles, conciliaciones o atributos de transacción de conciliación, incluidos atributos del sistema, balances y detalles de balances. Los usuarios con este rol pueden crear filtros y lógica complejos para determinar el orden en el que se aplican los filtros.

Conciliación - Comentarista

Visualice las conciliaciones y agregue comentarios a las conciliaciones o a las transacciones de la conciliación.

Conciliación - Preparador

Los usuarios con este rol preparan conciliaciones, asignan paneles, importan datos asignados y agregan adjuntos para enviar, reclamar y liberar conciliaciones.

Conciliación - Revisor

Los usuarios con este rol revisan conciliaciones, asignan paneles y agregan adjuntos para aprobar, rechazar, reclamar y liberar conciliaciones.

Informes - Gestionar

Configura los valores de la aplicación para mostrar los informes de conciliación.

Equipos - Gestionar

Los usuarios con este rol pueden agregar, editar o eliminar equipos, y gestionar miembros de los equipos.

Usuarios - Gestionar

Los usuarios con este rol pueden gestionar miembros de los equipos.

Asignación de roles predefinidos

Para obtener una lista de las actividades de Account Reconciliation que cada rol de aplicación puede realizar, consulte [Roles de aplicación](#).

Todos los roles de aplicación de Account Reconciliation se asignan el rol predefinido de administrador del servicio. Los usuarios con este rol pueden realizar todas las actividades que permiten los roles de aplicación individuales. Aquí se muestran solo los roles de aplicación de Account Reconciliation que están asignados al administrador del servicio.

- Tipos de alerta - Gestionar
- Anuncios - Gestionar
- Auditoría - Ver
- Monedas - Gestionar
- Data Integration - Administrador
- Data Integration - Crear
- Data Integration - Ejecutar
- Cargas de datos - Gestionar
- Organizaciones - Gestionar
- Períodos - Gestionar
- Filtros y vistas públicos - Gestionar
- Informes - Gestionar

Los siguientes roles de aplicación de Account Reconciliation se asignan a roles predefinidos distintos del Administrador del servicio.

Table 2-1 Roles de aplicación incluidos en roles predefinidos que no sean Administrador del servicio

Rol de aplicación	Incluido en estos roles predefinidos
Paneles - Gestionar	<ul style="list-style-type: none"> • Usuario avanzado • Usuarios • Visor
Trabajos - Ver	Usuario avanzado

Table 2-1 (Cont.) Roles de aplicación incluidos en roles predefinidos que no sean Administrador del servicio

Rol de aplicación	Incluido en estos roles predefinidos
Períodos - Ver	Usuario avanzado
Perfiles y conciliaciones - Gestionar	Usuario avanzado
Perfiles - Ver	<ul style="list-style-type: none"> • Usuario avanzado • Usuarios
Conciliación - Comentarista	<ul style="list-style-type: none"> • Usuario avanzado • Usuarios
Conciliación - Preparador	<ul style="list-style-type: none"> • Usuario avanzado • Usuarios
Conciliación - Revisor	<ul style="list-style-type: none"> • Usuario avanzado • Usuarios
Equipos - Gestionar	Usuario avanzado
Usuarios - Gestionar	Usuario avanzado

Enterprise Profitability and Cost Management

Related Topics

- [Roles de aplicación](#)
- [Asignación de roles predefinidos](#)

Roles de aplicación

Los siguientes roles se aplican solo a Enterprise Profitability and Cost Management.

De forma predeterminada, estos roles de aplicación se incluyen en los roles predefinidos. Consulte [Asignación de roles predefinidos](#). Los roles de aplicación se pueden asignar a los usuarios que necesiten llevar a cabo operaciones que no estén incluidas en los privilegios recibidos en sus roles predefinidos.

Ad hoc - Crear

Crea, visualiza, modifica y guarda cuadrículas ad hoc.

Ad hoc - Usuario de solo lectura

Realiza todas las funciones ad hoc, pero no puede reescribir en cuadrículas ad hoc ni cargar datos con Data Management.

Ad Hoc - Usuario

Ve y modifica las cuadrículas ad hoc y realiza operaciones ad hoc. Los usuarios ad hoc no pueden guardar las cuadrículas ad hoc.

Historial de cálculos - Suprimir

Suprime una instancia seleccionada de un cálculo completado de la página Análisis de cálculo. Al suprimir el historial de cálculos no se suprimen los datos. Simplemente se suprime la instancia registrada de un cálculo realizado.

Cálculo - Ejecutar

Calcula un modelo en la página Control de cálculo.

Historial de cálculos - Ver

Muestra los cálculos completados de la página Análisis de cálculo.

Data Integration - Crear

Utiliza Data Integration para crear asociaciones con el fin de integrar datos entre el sistema de origen y el sistema de destino. Los usuarios pueden definir reglas de datos con varias opciones de tiempo de ejecución.

Data Integration - Obtener detalles

Obtiene detalles del sistema de origen de los datos.

Data Integration - Ejecutar

En Data Integration, ejecuta reglas de datos con parámetros de tiempo de ejecución y visualiza logs de ejecución.

Modelo - Crear

Crea un nuevo modelo en la página Modelado.

Modelo - Suprimir

Suprime un modelo en la página Modelado. Si suprime un modelo también se suprimirán todas las reglas del modelo.

Modelo - Ver

Muestra modelos y sus reglas asociadas en la página Diseñador.

Validación de modelo - Ejecutar

Valida los modelos en la página Validación de modelo.

Datos de PDV - Borrar

Borra datos de un punto de vista en la página Control de cálculo sin eliminar el punto de vista.

Datos de PDV - Copiar

Copia datos de nuevo punto de vista en otro en la página Control de cálculo.

PDV - Crear

Crea un nuevo punto de vista en la página Control de cálculo.

PDV - Suprimir

Suprime un punto de vista en la página Control de cálculo. Al suprimir un punto de vista, también se suprimirán los datos asociados, así como la página de historial de cálculos para ese punto de vista. También elimina el punto de vista de la página Control de cálculo.

Estado de PDV - Editar

Cambia el estado de un punto de vista del cuadro de diálogo Editar punto de vista en la página Control de cálculo. Los estados disponibles de un punto de vista son Borrador, Publicado y Archivado.

Curva de ganancia - Crear

Crea curvas de ganancia en el separador Curvas de ganancia del cluster Intelligence.

Curva de ganancia - Editar

Edita curvas de ganancia en el separador Curvas de ganancia del cluster Intelligence.

Curva de ganancia - Ejecutar

Ejecuta curvas de ganancia en el separador Curvas de ganancia del cluster Intelligence.

Regla - Crear/Editar

Crea o edita una regla de asignación, una regla de cálculo personalizada o un conjunto de reglas en la página Diseñador.

Regla - Suprimir

Suprime una regla de asignación, una regla de cálculo personalizada o un conjunto de reglas en la página Diseñador.

Balance de reglas - Ejecutar

Muestra el informe Balance de reglas para que se vea el impacto de cada una de las reglas.

Reglas - Edición masiva

Accede al separador Edición masiva de la página Diseñador para hacer ediciones en varias reglas a la vez.

Lista de tareas - Gestionar acceso

Asigna tareas a otros usuarios.

Asignación de rastreo - Run

Realiza un seguimiento de los importes de asignación en el separador Rastrear asignaciones del cluster Intelligence.

Asignación de roles predefinidos

Para obtener una lista de las actividades de Enterprise Profitability and Cost Management que cada rol de aplicación puede realizar, consulte [Roles de aplicación](#).

Todos los roles de aplicación se asignan el rol predefinido de administrador del servicio. Los usuarios con este rol pueden realizar todas las actividades que permiten los roles de aplicación individuales. Aquí se muestran solo los roles de aplicación de Enterprise Profitability and Cost Management que están asignados al administrador del servicio.

- Ad hoc - Usuario de solo lectura
- Modelo - Suprimir
- PDV - Suprimir
- Estado de PDV - Editar

Los siguientes roles de aplicación de Enterprise Profitability and Cost Management se asignan a roles predefinidos distintos del Administrador del servicio.

Table 2-2 Roles de aplicación incluidos en roles predefinidos que no sean Administrador del servicio

Rol de aplicación	Incluido en estos roles predefinidos
Ad hoc - Crear	Usuario avanzado
Ad Hoc - Usuario	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Historial de cálculos - Suprimir	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Cálculo - Ejecutar	Usuario avanzado
Historial de cálculos - Ver	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Data Integration - Crear	Usuario avanzado
Data Integration - Obtener detalles	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Data Integration - Ejecutar	Usuario avanzado
Modelo - Crear	Usuario avanzado
Modelo - Ver	<ul style="list-style-type: none"> • Usuario avanzado • Usuario • Visor
Validación de modelo - Ejecutar	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Datos de PDV - Borrar	Usuario avanzado
Datos de PDV - Copiar	Usuario avanzado
PDV - Crear	Usuario avanzado
Curva de ganancia - Crear	Usuario avanzado
Curva de ganancia - Editar	Usuario avanzado
Curva de ganancia - Ejecutar	<ul style="list-style-type: none"> • Usuario avanzado • Usuario • Visor
Regla - Crear/Editar	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Regla - Suprimir	<ul style="list-style-type: none"> • Usuario avanzado • Usuario

Table 2-2 (Cont.) Roles de aplicación incluidos en roles predefinidos que no sean Administrador del servicio

Rol de aplicación	Incluido en estos roles predefinidos
Balance de reglas - Ejecutar	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Reglas - Edición masiva	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Lista de tareas - Gestionar acceso	Usuario avanzado
Asignación de rastreo - Run	<ul style="list-style-type: none"> • Usuario avanzado • Usuario • Visor

Planning, FreeForm, Financial Consolidation and Close y Tax Reporting



Note:

Planning incluye los tipos de aplicación Personalizada, FreeForm, Planning Modules, Strategic Workforce Planning y Sales Planning.

En esta sección, analizaremos los siguientes roles de aplicación:

- [Roles de la plataforma EPM Cloud](#) (Los roles de aprobaciones no se aplican a Financial Consolidation and Close ni a FreeForm)
- [Roles de Data Integration](#)
- [Roles relacionados con asientos de consolidación](#) (solo es aplicable a Financial Consolidation and Close)
- [Roles de gestor de tareas](#) (no es aplicable a FreeForm)

De forma predeterminada, estos roles de aplicación se incluyen en los roles predefinidos. Consulte [Asignación de roles predefinidos](#).

Roles de la plataforma EPM Cloud



Note:

Los roles de aprobaciones no se aplican a Financial Consolidation and Close ni a FreeForm.

Ad hoc - Crear

Crea, visualiza, modifica y guarda cuadrículas ad hoc.

Ad hoc - Usuario de solo lectura

Realiza todas las funciones ad hoc, pero no puede escribir en las cuadrículas ad hoc o los datos de carga con Data Management.

Ad Hoc - Usuario

Ve y modifica las cuadrículas ad hoc y realiza operaciones ad hoc. Los usuarios ad hoc no pueden guardar las cuadrículas ad hoc.

Aplicación - Asignación masiva

Ejecuta reglas de asignación masiva en las cuadrículas de formularios.

Aprobaciones - Administrar

Resuelve los problemas de aprobación apropiándose manualmente del proceso. Incluye los roles Persona que asigna la propiedad de aprobaciones, Diseñador de procesos de aprobaciones y Supervisor de aprobaciones.

Por lo general, este rol se asigna a usuarios de negocio encargados de una región que necesitan controlar el proceso de aprobaciones para la región, pero que no necesitan el rol de administrador del servicio. Pueden realizar las siguientes tareas:

- Controlar el proceso de aprobaciones
- Realizar acciones en unidades de Planning para las cuales dispongan de acceso de escritura.
- Asignar propietarios y revisores para la organización de la que están a cargo.
- Cambiar la dimensión secundaria o actualizar las reglas de validación.

Aprobaciones - Asignar propiedad

Realiza las siguientes tareas para cualquier miembro de la jerarquía de unidades de planificación para el que el usuario tenga acceso de escritura:

- Asignar propietarios
- Asignar revisores
- Especificar usuarios que recibirán notificaciones.

Aprobaciones - Diseñar proceso

Incluye el rol d persona que asigna la propiedad de aprobaciones. Además, realiza las siguientes tareas para cualquier miembro de la jerarquía de unidades de planificación para el que tenga acceso de escritura:

- Cambiar las dimensiones secundarias y los miembros de las entidades para los que el usuario tenga acceso de escritura.
- Cambiar la asignación de versión y escenario para una jerarquía de unidades de planificación.
- Editar reglas de validación de datos de formularios de datos para los que el usuario tenga acceso.

Aprobaciones - Supervisar

Realiza las siguientes tareas para cualquier miembro de la jerarquía de unidades de planificación al que el usuario tenga acceso de escritura, incluso si el usuario no es propietario de la unidad de planificación. Este usuario no puede cambiar los datos en las unidades de planificación de las cuales no sea propietario.

- Detener e iniciar una unidad de planificación.
- Realizar cualquier acción relacionada con una unidad de planificación.

Lista de tareas - Gestionar acceso

Asigna tareas a otros usuarios.

Roles de Data Integration

Data Integration - Crear

Utiliza Data Integration para crear asociaciones con el fin de integrar datos entre el sistema de origen y el sistema de destino. Los usuarios pueden definir reglas de datos con varias opciones de tiempo de ejecución.

Data Integration - Obtener detalles

Obtiene detalles del sistema de origen de los datos.

Data Integration - Ejecutar

En Data Integration, ejecuta reglas de datos con parámetros de tiempo de ejecución y visualiza logs de ejecución.

Roles relacionados con asientos de consolidación



Note:

Los roles relacionados con asientos de consolidación solo se pueden aplicar a Financial Consolidation and Close.

Asientos de consolidación: Aprobar

Apruebe un asiento de consolidación que se haya enviado para su aprobación, o rechace un asiento enviado.

Asientos de consolidación: Contabilizar automáticamente tras la aprobación

Permite que un asiento de consolidación se contabilice automáticamente una vez que lo haya aprobado el aprobador. El usuario que ha aprobado el asiento también será el usuario de contabilización.

Asientos de consolidación: Crear

Cree, modifique y suprima asientos de consolidación y plantillas de asientos de consolidación.

Asientos de consolidación: Gestionar periodos

Abra los periodos de tiempo para asientos de consolidación o cierre periodos de tiempo de asientos. Si hay asientos aprobados o asientos de retrocesiones automáticas no contabilizados en el periodo, no puede cerrarlo. Si selecciona cerrar un periodo que contiene asientos En curso o Enviado, se muestra una advertencia que indica que no se han encontrado asientos no contabilizados para el periodo, pero puede cerrarlo.

Asientos de consolidación: Contabilizar

Contabilice un asiento de consolidación que se haya completado o enviado y aprobado. En primer lugar, debe abrir el periodo de tiempo para cada escenario en el que se vayan a contabilizar los asientos de consolidación.

Asientos de consolidación: Enviar

Envíe un asiento de consolidación para su aprobación, o rechace un asiento de consolidación con el estado Completado.

Asientos de consolidación: Anular contabilización

Anule la contabilización de un asiento de consolidación. Debe tener acceso de escritura a los miembros del asiento.

Roles del gestor de tareas



Note:

Los roles basados en el gestor de tareas no se aplican a FreeForm.

Task Manager - Paneles operativos - Gestionar

Configura el panel de control

Task Manager - Informes personalizados - Gestionar

Diseña los informes personalizados

Gestor de tareas - Aprobador

Puede ser aprobador en tareas del gestor de tareas

Gestor de tareas - Persona asignada

Puede ser persona asignada en tareas del gestor de tareas

Task Manager - Artefactos - Gestionar

Gestiona todos los artefactos del gestor de tareas, tales como alertas, monedas y organización

Task Manager - Servicios y configuración del sistema - Gestionar

Define los servicios y la configuración del sistema para una aplicación

Task Manager - Filtros y vistas públicos - Gestionar

Publica filtros y vistas para proporcionar acceso a todo el mundo

Task Manager - Tareas - Gestionar

Diseña y gestiona las tareas, plantillas y programas

Task Manager - Usuarios y equipos - Gestionar

Gestiona usuarios y equipos

Task Manager - Auditoría - Ver

Ve la información del historial de auditorías

Asignación de roles predefinidos

A menos que se especifique lo contrario, todos los roles de aplicación de plataforma de EPM Cloud se asignan al rol predefinido de administrador del servicio. Los usuarios con este rol pueden realizar todas las actividades que permiten los roles de aplicación individuales. A continuación, se muestran solo los roles de aplicación que están asignados al administrador del servicio.

- Ad hoc - Usuario de solo lectura
- Aprobaciones - Diseñar proceso
- Task Manager - Paneles operativos - Gestionar
- Task Manager - Informes personalizados - Gestionar
- Task Manager - Artefactos - Gestionar
- Task Manager - Servicios y configuración del sistema - Gestionar
- Task Manager - Auditoría - Ver

Los **roles relacionados con el asiento de consolidación** no se asignan a ningún rol predefinido. Estos roles de aplicación se deben asignar por separado a cada usuario o grupo. Si estos roles no se asignan, el usuario no puede realizar ninguna actividad relacionada con el asiento de consolidación que no sea la visualización de asientos.

Los siguientes roles de aplicación se asignan a roles predefinidos distintos al de administrador del servicio.

Table 2-3 Roles de aplicación incluidos en roles predefinidos que no sean Administrador del servicio

Rol de aplicación	Incluido en este rol predefinido
Ad hoc - Crear	Usuario avanzado
Ad Hoc - Usuario	Usuario
Aprobaciones - Asignar propiedad	Usuario avanzado
Aprobaciones - Supervisar	Usuario avanzado
Data Integration - Crear	Usuario avanzado
Data Integration - Obtener detalles	<ul style="list-style-type: none"> • Usuario avanzado • Usuario

Table 2-3 (Cont.) Roles de aplicación incluidos en roles predefinidos que no sean Administrador del servicio

Rol de aplicación	Incluido en este rol predefinido
Data Integration - Ejecutar	Usuario avanzado
Lista de tareas - Gestionar acceso	Usuario avanzado
Gestor de tareas - Aprobador	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Gestor de tareas - Persona asignada	<ul style="list-style-type: none"> • Usuario avanzado • Usuario
Task Manager - Tareas - Gestionar	Usuario avanzado
Task Manager - Usuarios y equipos - Gestionar	Usuario avanzado
Task Manager - Filtros y vistas públicos - Gestionar	Usuario avanzado

Rentabilidad y gestión de costes

Related Topics

- [Roles de aplicación](#)
- [Asignación de roles predefinidos](#)

Roles de aplicación

El siguiente rol de aplicación se aplica solo a Profitability and Cost Management.

Data Integration - Administrador

Realiza todas las actividades funcionales en Data Integration. Los usuarios con este rol crean, realizan y ejecutan:

- Integraciones entre el sistema de origen y el sistema de destino
- Actividades del pipeline
- Extracción y transformación de datos y metadatos de orígenes locales utilizando el Agente de integración de EPM

Migraciones - Administrador

Utiliza la migración para exportar e importar instantáneas y artefactos desde la aplicación. Los usuarios con este rol pueden crear aplicaciones mediante la migración de instantáneas, y pueden suprimir aplicaciones que hayan creado.

Los usuarios con este rol no pueden clonar los entornos.

Asignación de roles predefinidos

Para obtener una lista de las actividades de Profitability and Cost Management que cada rol de aplicación puede realizar, consulte [Roles de aplicación](#).

Todos los roles de aplicación se asignan el rol predefinido de administrador del servicio. Los usuarios con este rol pueden realizar todas las actividades que permiten los roles de aplicación individuales.

Oracle Enterprise Data Management Cloud y Enterprise Data Management

Related Topics

- [Roles de aplicación](#)
- [Asignación de roles predefinidos](#)

Roles de aplicación

Los siguientes roles solo se aplican a procesos de negocio de Oracle Enterprise Data Management Cloud y Enterprise Data Management. De forma predeterminada, estos roles de aplicación se incluyen en los roles predefinidos. Consulte [Asignación de roles predefinidos](#). Los roles de aplicación se pueden asignar a los usuarios que necesiten llevar a cabo operaciones que no estén incluidas en los privilegios recibidos en sus roles predefinidos. No puede migrar roles de aplicación desde la ubicación local a Oracle Enterprise Data Management Cloud.

Control de acceso - Gestionar

Los usuarios con este rol pueden gestionar grupos, y asignar roles de aplicación a un grupo o un usuario. También pueden generar informes sobre la seguridad de los usuarios.

Aplicación - Crear

Registra aplicaciones en Oracle Enterprise Data Management Cloud. Al usuario que registra una aplicación se le otorga el permiso Propietario de aplicación. Este usuario también está asignado como propietario de vista de la vista de aplicación predeterminada.

Auditoría

Visualiza la información de auditoría relacionada, como el historial de transacciones y las solicitudes de cambios en los datos, en Oracle Enterprise Data Management Cloud.

Migraciones - Administrar

Utiliza la migración para exportar e importar instantáneas y artefactos desde la aplicación. Los usuarios con este rol pueden crear aplicaciones mediante la migración de instantáneas, y pueden suprimir aplicaciones que hayan creado.

Los usuarios con este rol no pueden clonar los entornos.

Vistas - Crear

Crea vistas en una aplicación de Oracle Enterprise Data Management Cloud. Al usuario que crea una vista se le otorga el permiso Propietario de vista para la vista.

Asignación de roles predefinidos

Para obtener una lista de las actividades de Oracle Enterprise Data Management Cloud que cada rol de aplicación puede realizar, consulte [Roles de aplicación](#). Todos los roles de aplicación se asignan el rol predefinido de administrador del servicio. Los usuarios con este rol pueden realizar todas las actividades que permiten los roles de aplicación individuales.

Aquí se muestran solo los roles de aplicación de Oracle Enterprise Data Management Cloud que están asignados al administrador del servicio.

- Control de acceso - Gestionar
- Aplicación - Crear
- Auditoría
- Migraciones - Administrar
- Vistas - Crear

Asignación de roles de aplicación a un grupo o un usuario

Durante este proceso, los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden asignar o anular la asignación de roles de aplicación a grupos y usuarios que tengan un rol predefinido. También pueden asignar roles de aplicación a sí mismos.

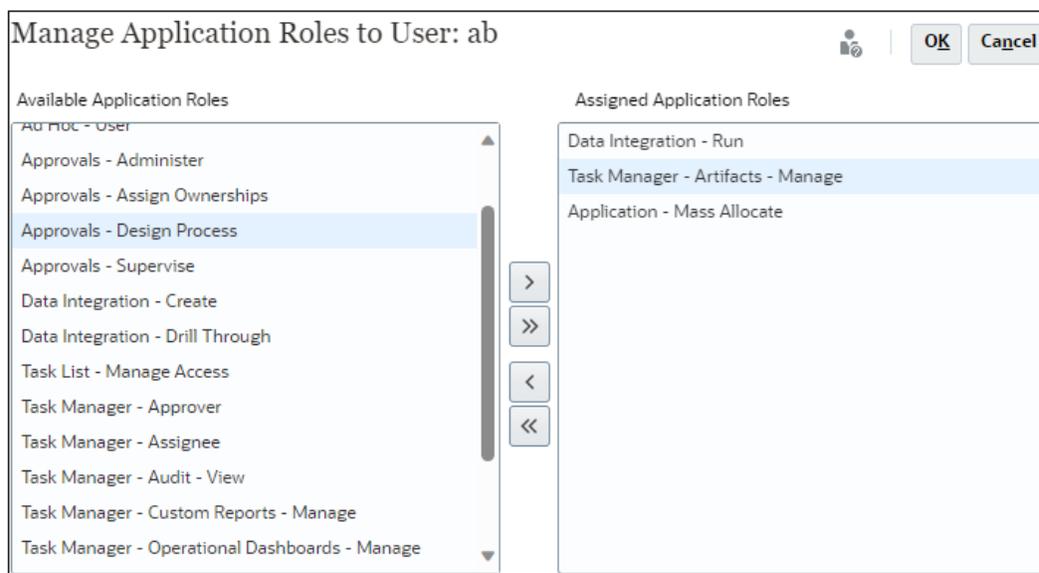
Para obtener información sobre grupos y usuarios asignados a grupos, consulte [Gestión de grupos](#).

Para asignar o anular la asignación de roles de aplicación a un grupo o usuario:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en el separador **Gestionar roles de aplicación**.
3. Busque un usuario o un grupo. En la lista desplegable, seleccione **Usuarios** o **Grupos**. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.

Se muestran los usuarios o grupos que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Conexión de usuario** y, a continuación, por los de **Nombre de grupo** (para las búsquedas de grupo).

4. Haga clic en  (**Acciones**) del usuario o grupo y, a continuación, seleccione **Gestionar roles**.
5. Para asignar un rol de aplicación al usuario o grupo, selecciónelo en la lista **Roles de aplicación disponibles** y, a continuación, haga clic en el botón de flecha derecha.

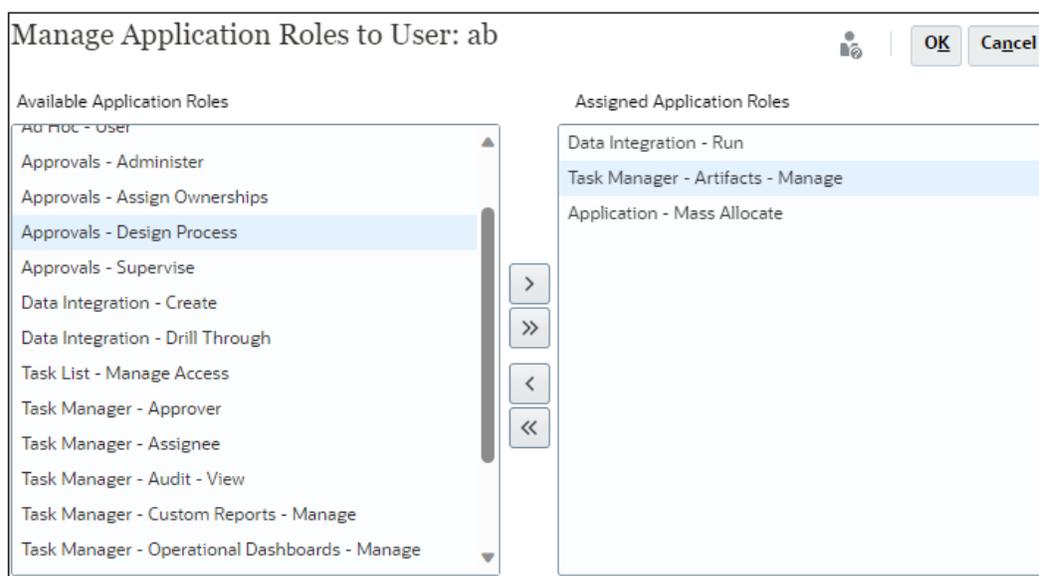


Para saber qué roles de aplicación se aplican a cada proceso de negocio, consulte el tema correspondiente:

- [Roles de aplicación en Account Reconciliation](#)
- [Roles de aplicaciones de Enterprise Profitability and Cost Management](#)
- [Planning, FreeForm, Financial Consolidation and Close y Tax Reporting Roles de aplicación](#)
- [Roles de aplicación de Oracle Enterprise Data Management Cloud](#)

Otros procesos de negocio como Profitability and Cost Management y Narrative Reporting no soportan la asignación de roles de aplicación.

6. Si desea anular la asignación de un rol de aplicación, selecciónelo en la lista **Roles de aplicación asignados** y, a continuación, haga clic en la tecla de flecha izquierda.



7. Haga clic en **Aceptar** para completar la asignación de roles de aplicación para el usuario o grupo.
8. Haga clic en **Aceptar** de nuevo para volver al separador **Gestionar roles de aplicación**.

Eliminación de roles de nivel de aplicación asignados a un grupo o un usuario

Durante este proceso, los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden eliminar todos los roles de aplicación asignados al grupo o al usuario. La eliminación de la asignación de roles de nivel de aplicación no afecta a los roles predefinidos del usuario.

Para eliminar roles de nivel de aplicación de un grupo o un usuario

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en **Asignar roles de aplicación**.
3. Busque un usuario o un grupo. En la lista desplegable, seleccione **Usuarios** o **Grupos**. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.

Se muestran los usuarios o grupos que coincidan con los criterios de búsqueda. De forma predeterminada, la lista se ordena por los valores de **Conexión de usuario** y, a continuación, por los de **Nombre de grupo** (para las búsquedas de grupo).

4. Haga clic en  (Acciones) correspondiente al usuario o al grupo y, a continuación, seleccione **Anular asignación de roles**.
5. Haga clic en **Sí**.
6. Haga clic en **Aceptar**.

3

Generación de informes

Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar pueden generar estos informes para analizar y gestionar asignaciones de roles:

- [Generación de informes de asignación de roles para un usuario o un grupo](#)
- [Visualización de informes de asignación de roles para el entorno](#)
- [Visualización del informe de inicio de sesión de usuario](#)
- [Visualización y exportación del informe de grupo de usuarios](#)

La hora de generación de informe indicada en los informes refleja la hora en función de la zona horaria del explorador (reloj del sistema local).

Acerca de la versión CSV del informe

Puede exportar un informe para crear una versión de valores separados por comas (CSV) del informe. Además de un recuento del número de usuarios asignados a roles predefinidos, la versión CSV del informe muestra lo siguiente:

- Roles predefinidos a los que se asigna cada usuario. Cada rol predefinido asignado a un usuario aparece en una fila distinta. Los roles de aplicación incluidos en roles predefinidos no se muestran.
- Roles de aplicación a los que se asigna un usuario directamente o mediante un grupo. Cada rol de aplicación asignado a un usuario aparece en una fila separada.
- Los grupos a los que están asignados los usuarios no se muestran si no están asignados a ningún rol.
- Solo se exporta al CSV la información de la vista actual del informe. Por ejemplo, si filtra el informe para ver las asignaciones de roles de un usuario específico, el archivo CSV exportado solo contiene las asignaciones de ese usuario.

Solución de problemas

Consulte Solución de problemas de informes en *Guía de operaciones de Oracle Enterprise Performance Management Cloud*.

Generación de informes de asignación de roles para un usuario o un grupo

El informe Asignación de roles le permite realizar el seguimiento del acceso de los usuarios para elaborar los informes de conformidad.

En este informe se muestran todos los usuarios activos a los que se les haya asignado un rol predefinido. Los usuarios desactivados no se reflejan en este informe. Los grupos a los que pertenece un usuario no se muestran si estos no se utilizan para asignar roles de aplicación al usuario. Los administradores del servicio o los usuarios con el rol de aplicación Administrador de control de acceso pueden acceder al informe de asignación de roles para revisar los roles predefinidos y los roles de aplicación asignados de un usuario o grupo.

Para generar un informe de asignación de roles para un usuario o un grupo:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en el separador **Gestionar roles de aplicación**.
3. Busque un usuario o un grupo. En la lista desplegable, seleccione **Usuarios o Grupos**. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.

Se muestran los usuarios o grupos que coincidan con los criterios de búsqueda. De forma predeterminada, el informe se ordena en función de los valores de **Conexión de usuario** y después en función de los valores de **Nombres de grupo** (para búsquedas de grupo).

4. Haga clic en  del usuario o grupo y, a continuación, seleccione **Informe de asignación de roles**.
5. **Opcional:** haga clic en **Exportar a CSV** si desea exportar el informe a un archivo CSV.

Visualización de informes de asignación de roles para el entorno

Los administradores del servicio o los usuarios con el rol de aplicación Control de acceso - Gestionar utilizan el informe de asignación de roles para revisar el acceso, asignado mediante roles predefinidos (en negrita) y roles de nivel de aplicación, de todos los usuarios. En este informe se muestran todos los usuarios activos a los que se les haya asignado un rol predefinido. Los usuarios desactivados no se reflejan en este informe.

Los roles heredados, así como la información de herencia, se muestran en una fila por usuario. Por ejemplo, suponga que el usuario John Doe tiene asignado el rol predefinido User y que User es miembro del grupo example al que está asignado el rol de aplicación de Planning Approvals Administrator. En este escenario, el informe de asignación de roles muestra lo siguiente como parte de la información de asignación de roles para John Doe:

Approvals - Administrator (example->User).

En un entorno de OCI (Gen 2), si se asigna un rol predefinido a un grupo de IDCS, el informe de asignación de roles mostrará ese rol predefinido asignado directamente a todos los usuarios de ese grupo. No muestra los roles de aplicación incluidos en los roles predefinidos ni los roles de componente de roles de aplicación asignados al usuario. Si necesita un informe en el que se muestren estos detalles, puede generar la versión clásica del informe con el comando provisionReport de EPM Automate.



User	First Name	Last Name	Email	Roles
jdoe	John	Doe	john.doe@example.com	Planner, Power User, Service Administrator, Viewer Mass Allocation (example ->Power User), Run Integration
jane.doe@example.com	Jane	Doe	jane.doe@example.com	Planner, Power User, Viewer Mass Allocation (example)

Puede exportar el informe de asignación de roles como un archivo CSV, que se puede abrir posteriormente con un programa como Microsoft Excel o guardar en el equipo. El informe de asignación de roles con formato CSV utiliza una fila por asignación de rol.

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

Para abrir el informe de asignación de roles:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en **Informe de asignación de roles**.
Se mostrará el informe de asignación de roles.
3. **Opcional:** Filtre el informe para mostrar los siguientes elementos:
 - Asignaciones de roles de un usuario específico. Seleccione **Usuarios** de la lista desplegable y, a continuación, introduzca una cadena de búsqueda parcial. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.
 - Usuarios asignados a un rol específico. Seleccione **Roles** de la lista desplegable y, a continuación, introduzca el nombre parcial de un rol. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.

Nota:

A los usuarios se les pueden asignar muchos roles. En estos casos, el informe muestra todos los roles del usuario, incluso si los filtra para un rol específico.

Se mostrará el informe de asignación de roles. De forma predeterminada, el informe se ordena por los valores de **Conexión de usuario** y, a continuación, por los roles de aplicación de **Roles** (para las búsquedas por roles). Los roles predefinidos se muestran en fuente negrita, mientras que los roles de aplicación se muestran en fuente no negrita.

4. **Opcional:** haga clic en **Exportar a CSV** si desea exportar el informe a un archivo CSV. Tenga en cuenta que solo se exporta al CSV la información de la vista actual del informe.

Visualización del informe de inicio de sesión de usuario

El informe de inicio de sesión de usuario contiene, de forma predeterminada, información sobre los usuarios que han iniciado sesión en el entorno a lo largo de las últimas 24 horas.

Muestra la dirección IP del equipo desde el que inició sesión el usuario y la fecha y hora en las que el usuario accedió al entorno.

Los administradores del servicio o los usuarios con el rol Control de acceso - Gestionar pueden volver a generar este informe para un rango de fechas personalizado o para los 30 últimos días, los 90 últimos días y los 120 últimos días. También pueden filtrar el informe para ver solo la información de determinados usuarios mediante el uso de una cadena parcial del nombre, los apellidos o el ID de usuario de los usuarios como cadena de búsqueda.

**Nota:**

Oracle Enterprise Performance Management Cloud mantiene el historial de auditorías de conexiones del usuario solo de los últimos 120 días.

Para volver a generar Informe de conexión de usuario:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en **Informe de conexión de usuario**.
Aparece un informe que muestra todos los usuarios que iniciaron sesión en el entorno a lo largo del último día.
3. Seleccione el periodo (Últimos 1 días, Últimos 30 días, Últimos 90 días o Últimos 120 días) para el que desee generar el informe. Para especificar un rango de fechas personalizado, seleccione **Rango de fecha** y, a continuación, una fecha de inicio y una fecha de finalización.
4. **Opcional:** Seleccione los usuarios que desea incluir en el informe. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.
Se mostrará el informe de conexión de usuario. De forma predeterminada, el informe se ordena por los valores de **Fecha y hora de acceso**.
5. **Opcional:** Haga clic en **Exportar a CSV** si desea exportar el informe mostrado como archivo CSV.
6. Haga clic en **Cancelar** para cerrar el informe.

Visualización y exportación del informe de grupo de usuarios

El informe de grupos de usuarios muestra la pertenencia directa o indirecta de los usuarios asignados a grupos en Control de acceso. Los administradores del servicio o los usuarios con el rol Control de acceso - Gestionar pueden generar este informe.

Se considera que los usuarios son miembros directos de un grupo si están asignados al grupo; se considera que son miembros indirectos si están asignados a un grupo que es hijo de otro grupo. Para cada usuario asignado a un grupo, el informe muestra información como el identificador de inicio de sesión, el nombre y el apellido, el identificador de correo electrónico y una lista de grupos separados por comas a los que está asignado el usuario de forma directa o indirecta. Los grupos directos se muestran en fuente negra, mientras que los grupos indirectos se muestran en fuente

no negrita. La versión CSV del informe indica si el usuario está asignado de forma directa o indirecta a un grupo mediante **Yes** o **No**.



Nota:

Este informe no es aplicable a Account Reconciliation ni a Narrative Reporting.

Para volver a generar el informe de grupos de usuarios:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en **Informe de grupos de usuarios**.
3. **Opcional:** filtre el informe. En la lista desplegable, seleccione **Usuarios** o **Grupos**. Consulte [Uso de la función de búsqueda](#) para obtener instrucciones sobre el uso de la función de búsqueda.

Se mostrará el informe de grupos de usuarios. De forma predeterminada, el informe se ordena por los valores de **Conexión de usuario**.

4. **Opcional:** haga clic en **Exportar a CSV** si desea exportar el informe a un archivo CSV.
5. Haga clic en **Cancelar** para cerrar el informe.