

Oracle® Cloud

Administración del control de acceso para Oracle Enterprise
Performance Management Cloud

F28929-05

Oracle Cloud Administración del control de acceso para Oracle Enterprise Performance Management Cloud
F28929-05

Copyright © 2015, 2021, Oracle y/o sus filiales.

Autor principal: EPM Information Development Team

Tabla de contenidos

| | |
|--|-----|
| Accesibilidad a la documentación..... | v |
| Comentarios sobre la documentación..... | vii |
| 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..... | 1-2 |
| Modificación de grupos..... | 1-4 |
| Supresión de grupos..... | 1-5 |
| Importación de asignaciones de grupos de usuarios de un archivo..... | 1-5 |
| Asignación de un usuario a varios grupos..... | 1-6 |
| Uso de la función de búsqueda..... | 1-7 |
| 2 Gestión de asignaciones de roles en el nivel de aplicación | |
| Roles de aplicaciones de planificación y consolidación..... | 2-2 |
| Roles de aplicación de Oracle Enterprise Data Management Cloud..... | 2-3 |
| Asignación de roles a un grupo o un usuario..... | 2-4 |
| Eliminación de roles de nivel de aplicación asignados a un grupo o un usuario..... | 2-5 |
| 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.

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 de servicio pueden asignar usuarios a roles específicos de las aplicaciones de planificación, consolidación 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 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](#)

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
- Cierre y consolidación financieros
- Tax Reporting
- Rentabilidad y gestión de costes
- Account Reconciliation
- Oracle Enterprise Data Management Cloud

- Narrative Reporting
- Oracle Strategic Workforce Planning Cloud
- Oracle Sales Planning Cloud

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.
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 para **Oracle Enterprise Data Management Cloud y 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 que se utilicen durante el proceso de asignación de roles.

Los usuarios de EPM Cloud y otros grupos 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* .

- [Creación de grupos](#)
- [Modificación de grupos](#)
- [Supresión de grupos](#)

Nota: No puede utilizar el Control de acceso para importar información de grupo de un archivo para crear grupos. De igual modo, no podrá exportar información de grupos mediante Control de acceso. Puede utilizar Migración o el comando createGroups de EPM Automate para importar grupos.

Creación de grupos

Solo los administradores de servicio 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. Para evitar ambigüedades en informes de seguridad, EPM Cloud no le permite crear grupos con nombres idénticos a nombres de rol actuales o previos (administrador de servicio, usuario avanzado, usuario, visor, planificador, administrador de sistema, administrador de aplicación, administrador de biblioteca, administrador de informes).

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 coinciden con los criterios de búsqueda debajo de **Grupos disponibles**.

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.

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 pueden modificar las propiedades de los 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.

Nota: Los nombres de grupo pueden contener un máximo de 71 caracteres. Sin embargo, solo los primeros 34 caracteres aparecen en la lista mostrada en la columna **Grupos disponibles**.


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.
 - 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.
 - 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

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.
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**.

Importación de asignaciones de grupos de usuarios de un archivo

Los Administradores de servicio pueden importar asignaciones de grupos de usuarios de un archivo de valores separados por comas (CSV) para crear asignaciones nuevas en un grupo existente de Control de acceso. 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.



Para asignar un usuario a varios grupos:

1. Abra **Control de acceso**. Consulte [Apertura de Control de acceso](#).
2. Haga clic en **Gestionar usuarios**.
Aparecerá una lista de todos los usuarios del entorno actual.
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.
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.
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. Puede ordenar la lista de usuarios recuperados haciendo clic en cualquier cabecera de columna.

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. Puede ordenar la lista de grupos recuperados según el nombre de grupo o la descripción.

The screenshot shows the 'Create Group' interface. At the top, there are fields for '* Name:' (containing 'Example') and 'Description:'. Below these are tabs for 'Groups' and 'Users'. The 'Users' tab is active, showing a search bar with 'exam' and a magnifying glass icon. Below the search bar are two tables: 'Available Users' and 'Assigned Users'. The 'Available Users' table has columns for 'First Name', 'Last Name', 'Email', and 'User Login', and contains three rows of user data. The 'Assigned Users' table is empty, with the text 'No records were found.' below it. A double arrow button is positioned between the two tables.

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

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.

Gestión de asignaciones de roles en el nivel de aplicación

La asignación de roles en el nivel de aplicación se admite para las aplicaciones de planificación, consolidación y cierre, informes de impuestos y de Oracle Profitability and Cost Management Cloud. Las aplicaciones de planificación, consolidación y de Oracle Enterprise Data Management Cloud utilizan roles específicos de aplicaciones granulares para mejorar el acceso otorgado a través de roles predefinidos, mientras que Profitability and Cost Management asigna otorgamientos de datos de nivel de usuario y grupo para proteger el acceso a los datos de la aplicación.

Descripción general

Aunque los derechos de acceso generales se controlan con los roles de Oracle Enterprise Performance Management Cloud predefinidos, los administradores del servicio pueden otorgar roles específicos de la aplicación a los usuarios y grupos creados y gestionados en Control de acceso. Por ejemplo, un usuario, de manera predeterminada, no tiene el derecho necesario para diseñar el proceso de aprobaciones, que solo se conceden a los usuarios avanzados y los administradores del servicio. En Control de acceso, los administradores del servicio pueden asignar el rol de administrador de aprobaciones para permitir al usuario realizar actividades relacionadas con las aprobaciones.

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

Puede gestionar el proceso de asignación de roles mediante Control de acceso. Puede realizar las siguientes tareas:

- Cree grupos y agregue usuarios de EPM Cloud u otros grupos como miembros.
- Agregar o suprimir miembros del grupo
- Asignar roles de aplicación de planificación y consolidación a grupos o a usuarios
- Ver la lista de usuarios que son miembros de un grupo

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.

Roles de aplicaciones de planificación y consolidación

Los siguientes roles solo se aplican a las aplicaciones de informes de impuestos, consolidación y planificación. Consulte *Administración de Profitability and Cost Management* para obtener más información sobre la asignación de otorgamientos de datos de la aplicación Profitability and Cost Management.

De forma predeterminada, solo los administradores del servicio y usuarios avanzados pueden acceder a Data Management para trabajar en el proceso de integración de datos. Para permitir que los usuarios con el rol de dominio de identidad Usuario o Visor participen en el proceso de integración, los administradores del servicio les deberían asignar roles de Data Management (Crear integración, Ejecutar integración, Obtener detalles).

Administrador de aprobaciones

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 de Planning. 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.

Persona que asigna la propiedad de aprobaciones

Realiza todas las tareas que pueden realizar los usuarios con el rol Planificador. Además, 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.

Diseñador de procesos de aprobaciones

Realiza todas las tareas que pueden realizar los usuarios con los roles Planificador y 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.

Supervisor de aprobaciones

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.

Creador de cuadrícula ad hoc

Crea, visualiza, modifica y guarda cuadrículas ad hoc.

Usuario ad hoc

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

Usuario ad hoc 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.

Asignación masiva

Ejecuta reglas de asignación masiva en las cuadrículas de formularios.

Administrador de acceso a lista de tareas

Asigna tareas a otros usuarios.

Crear integración

Utiliza Data Management 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.

Ejecutar integración

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

Obtener detalles

Obtiene detalles del sistema de origen de los datos.

Roles de aplicación de Oracle Enterprise Data Management Cloud

Estos roles solo se aplican a aplicaciones de Oracle Enterprise Data Management Cloud.

Creador de aplicaciones

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.

Auditor

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.

Creador de vistas

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 a un grupo o un usuario


Durante este proceso, los administradores del servicio asignan roles de nivel de aplicación a los grupos y usuarios a los que se ha asignado un rol predeterminado.

Nota:

No puede asignar roles de aplicación a su propia cuenta de usuario.

Para permitirle ver las asignaciones de roles, Control de acceso muestra los roles de Oracle Enterprise Performance Management Cloud predeterminados como grupos. No puede asignarles roles de nivel de aplicación desde Control de acceso.

Para asignar roles de nivel de aplicación a 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.
4. Haga clic en  (**Acciones**) correspondiente al usuario o al grupo y, a continuación, seleccione **Asignar roles**.
5. En **Roles disponibles**, seleccione los roles que desea asignar al usuario o al grupo y, a continuación, haga clic en **Mover**.

Consulte estas secciones para obtener una descripción de los roles que pueden asignarse a usuarios y grupos.

- [Roles de aplicaciones de planificación y consolidación](#)
- [Roles de aplicación de Oracle Enterprise Data Management Cloud](#)


Los roles seleccionados se muestran en **Roles asignados**. Para eliminar roles asignados, seleccione los roles que desea eliminar en **Funciones asignadas** y, a continuación, haga clic en **Eliminar**.

6. Haga clic en **Aceptar**.
7. Haga clic en **Aceptar**.

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

Este proceso elimina 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 cómo utilizar la función de búsqueda.
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**.

Generación de informes

Estos informes se utilizan 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.

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

Los administradores del servicio utilizan el informe de asignación de roles para revisar los roles predefinidos y los roles de aplicación asignados de los usuarios. Los grupos a los que pertenece un usuario no se muestran si estos no se utilizan para asignar roles de aplicación al usuario. Este informe permite realizar el seguimiento del acceso de los usuarios para elaborar los informes de conformidad.

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 **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 cómo utilizar la función de búsqueda.
4. Haga clic en **Acción**  (**Acciones**) correspondiente al usuario o al grupo sobre el que desea generar el informe 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.
6. Haga clic en **Cerrar** para cerrar el informe.

Visualización de informes de asignación de roles para el entorno

Los administradores del servicio utilizan el informe de asignación de roles para revisar el acceso, asignado mediante roles predefinidos y roles de nivel de aplicación, de todos los usuarios. El informe muestra los roles predefinidos (por ejemplo, usuario avanzado) y de aplicación (como la asignación masiva, que es un rol de aplicación de Planning) asignados directamente al usuario.

Los roles heredados, así como la información de herencia, se muestran en una fila por usuario. Por ejemplo, asuma 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).

El informe de asignación de roles también identifica el número de usuarios que tienen autorización para acceder al entorno según sus roles predefinidos. 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.

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 pueden volver a generar este informe para un rango de fechas personalizado o para los 30 últimos días, 90 últimos días y 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.
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.

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. 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 cómo utilizar la función de búsqueda.
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.