



Tot plugin PowerBI

<b>Control de versiones</b>	<b>3</b>
<b>Servicios disponibles en el plugin</b>	<b>4</b>
<b>Modelo de integración</b>	<b>4</b>
Extracción de metadatos	4
Gestión de accesos (En Roadmap)	5
<b>Credenciales requeridas</b>	<b>5</b>
Extracción de metadatos	5
Gestión de accesos (En Roadmap)	7
<b>Configuración</b>	<b>7</b>
<b>Anexos</b>	<b>8</b>
Asignación grupo a Report	8
Asignación de grupos a Dashboard	10
Asignación de grupo a Modelo Semántico	12
Asignación de grupo a APP	14

## Control de versiones

Versión	Fecha modificación	Responsable	Aprobador	Resumen de cambios
1.0	30/08/2024	Jose Angel González	Ana Melcón	Creación del documento
2.0	24/12/2024	Alberto Montero	Ana Melcón	Se añade punto 3

# Servicios disponibles en el plugin

- Listado y extracción de metadatos
- Gestión de accesos (delegada sobre AzureAD)(en Roadmap)

## Modelo de integración

### Extracción de metadatos

Para la extracción de metadata de un objeto se utilizan las APIs:

- <https://learn.microsoft.com/en-us/rest/api/power-bi/admin/groups-get-groups-as-admin>
- <https://learn.microsoft.com/en-us/rest/api/power-bi/admin/apps-get-apps-as-admin>

Con estas APIs el plugin es capaz de extraer los siguientes tipos de objeto de PowerBI:

- APP
- Dataset (modelo de datos)
- Report
- Dashboard

El plugin extrae los siguientes atributos, que deben llamarse igual en la tabla attribute\_definition, (campo name) para que aparezcan en la plantilla:

Nombre de atributo	Tipo de atributo	Descripción
physicalName, name	INPUT_TEXT	nombre del objeto
path	INPUT_TEXT	ruta al objeto
infrastructure	SELECT	valor seleccionado
technology	SELECT	valor seleccionado
zone	SELECT	valor seleccionado

Además, la propia API de Azure permite extraer más atributos de los objetos con lo que, si se incluyen estos atributos en la plantilla del objeto, la extracción completará su valor. En caso de duda del valor devuelto para un atributo, el tipo INPUT\_TEXT siempre aceptará insertar cualquier valor.

**NOTA: El atributo ID presente en todos los objetos de PowerBI no puede ser configurado en Anjana Data por el momento al ser un identificador interno de la aplicación**

Para más detalles sobre los atributos que potencialmente se pueden extraer de cada objeto consultar los siguientes enlaces.

Dashboard:

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/groups-get-groups-as-admin#admindashboard>

Dataset (modelo de datos) :

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/groups-get-groups-as-admin#admindataset>

App:

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/apps-get-apps-as-admin#adminapp>

Report:

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/groups-get-groups-as-admin#adminreport>

## Gestión de accesos (En Roadmap)

Dado que la API de PowerBI no tiene accesible la gestión de accesos, la única manera de hacerlo posible es mediante la delegación de estos a través de AzureAD. Para ello habrá dos actuaciones manuales requeridas para que este mecanismo funcione:

1. Asignación de permisos:
  - a. Crear un DSA y añadir objetos de Power BI.
    - i. En el campo `physical_name` deberá informarse el nombre del grupo.
  - b. Este grupo habrá que asignarlo a cada objeto de Power BI (mirar [Anexos](#))
2. Sincronización:
  - a. El proceso de sincronización entre Azure y PowerBI no es automático ni instantáneo.
  - b. Forzarlo si es posible

## Credenciales requeridas

### Extracción de metadatos

Se necesitan los siguientes permisos:

- Tenant.Read.All

Estos permisos se deben dar sobre el service principal que se vaya a usar para el cometido del plugin. Estos permisos no pueden ser consentimiento de Administración si no que tienen que ser permisos delegados:

1. Configuración del App Registration
  - a. Ir al Azure Portal.
  - b. Navegar a Azure Active Directory > App registrations > + New registration.
  - c. Proporcionar un nombre para la aplicación y seleccionar el tipo de cuenta (lo más común es Accounts in this organizational directory only).
2. Configurar los Permisos API
  - a. Dentro de la App Registration, navegar a API permissions.
  - b. Hacer clic en + Add a permission.
  - c. Seleccionar Microsoft Power BI.
  - d. Seleccionar **Delegated permissions** (no Application permissions).
  - e. Buscar y seleccionar los permisos que la aplicación necesita mencionados anteriormente.
3. Generar un grupo de seguridad en Azure específico para consumir las APIs de PowerBI
  - a. Meter dentro del grupo la APP generada

b. Meter al grupo dentro de la siguiente opción existente en PowerBI (ver captura)

#### Configuración de la **API** de administración

- ↳ Las entidades de servicio pueden acceder a las **API** de administración de solo lectura  
*Habilitado para un subconjunto de la organización*

Las aplicaciones web registradas en Microsoft Entra ID pueden usar entidades de servicio, en lugar de credenciales de usuario, para autenticarse en las **API** de administración de solo lectura.

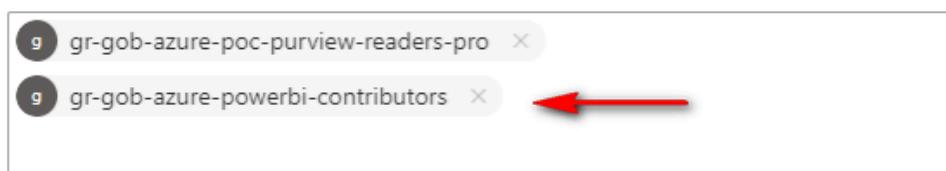
- Para permitir que una aplicación use una entidad de servicio como método de autenticación, la entidad de servicio debe agregarse a un grupo de seguridad permitido. Las entidades de servicio incluidas en los grupos de seguridad permitidos tendrán acceso de solo lectura a toda la información disponible a través de las **API** de administración, que puede incluir nombres de usuario y correos electrónicos, y metadatos detallados sobre modelos semánticos e informes. [Más información](#)



Aplicar a:

Toda la organización

Grupos de seguridad específicos



Excepto grupos de seguridad específicos

- c. Meter en Powerbi a la Aplicación generada en el punto 1 dentro del grupo de seguridad

**NOTA: En la mayoría de escenarios no es necesario la concesión de permisos delegados (*Tenant.Read.All*) siempre y cuando cumplamos con el punto 3 anteriormente descrito**

Los endpoint utilizados para realizar la extracción de los objetos de PowerBI son los siguientes:

- APP

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/apps-get-apps-as-admin>

- Dataset (modelo de datos)

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/datasets-get-datasets-as-admin>

- Report

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/reports-get-reports-as-admin>

- Dashboard

<https://learn.microsoft.com/en-us/rest/api/power-bi/admin/dashboards-get-dashboards-as-admin>

## Gestión de accesos (En Roadmap)

Para la gestión de accesos el usuario encargado de la asignación de un grupo a un objeto de PowerBI (dentro de la aplicación de PowerBI) deberá tener permiso de **Owner o Member sobre el Workspace** donde reside el objeto o desde el que se publica una App.

## Configuración

Para la configuración del plugin será necesario tener disponible las siguientes propiedades:

- *TenantId*: tenant sobre el que se va a actuar en la integración
- *ClientId*: *Id de la aplicación que se ha registrado (ver apartado [Credenciales Requeridas](#))*
- *ClientSecret*(*el value no el Id del secret*): serán las claves de acceso con las que se comunicará el plugin, estas deben de ser de un service principal

Además será necesario tipar en el YAML una conversión de subtipos de objeto de Anjana con los tipos de objeto PowerBI que se pueden extraer, deberán estar escritos de la misma manera que aparecen en la tabla `object_subtype` del esquema anjana de base de datos. Los tipos de objeto son los descritos en [Modelo de integración](#).

Ejemplo YAML de configuración del plugin.

```
server:
  port: 15016

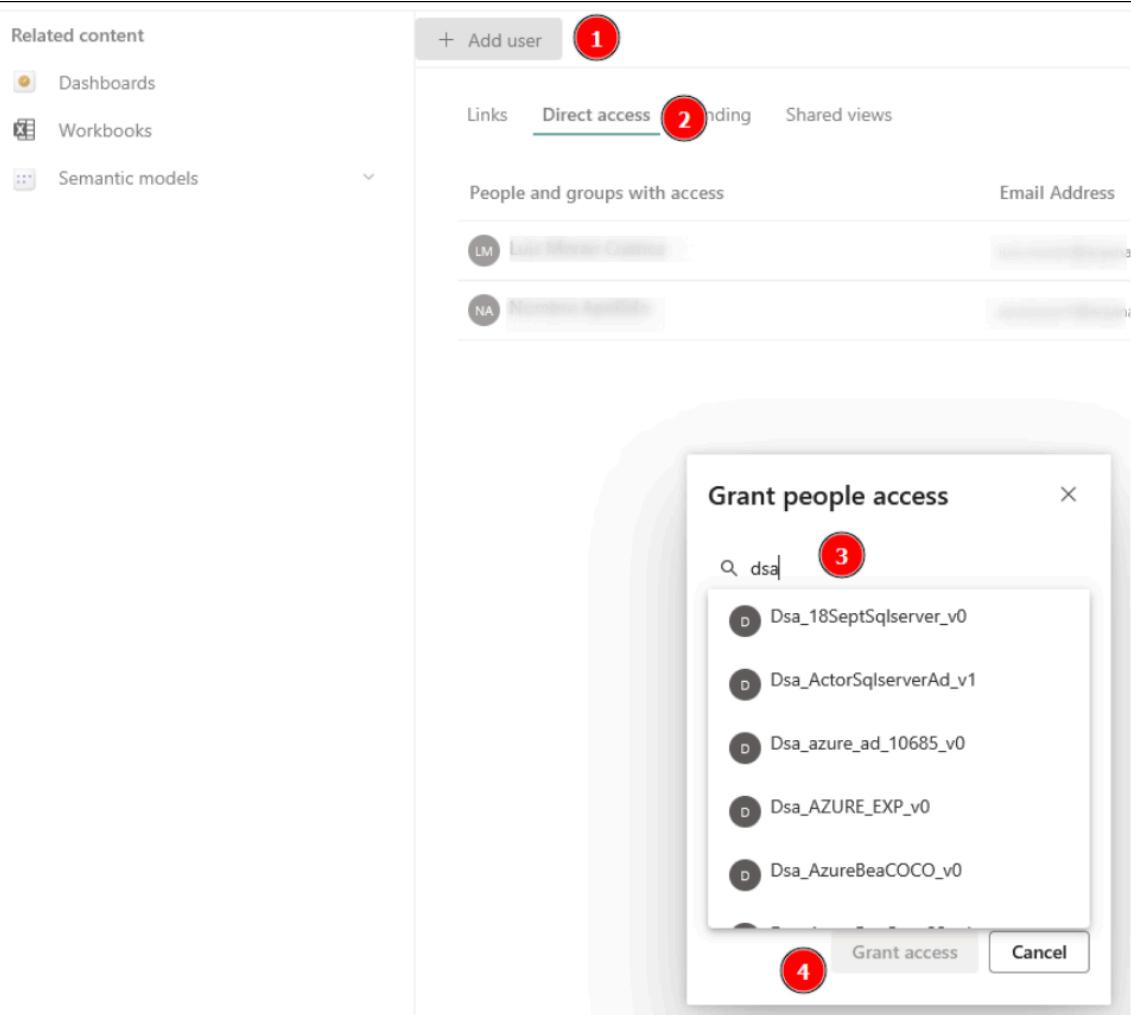
totplugin:
  server:
    urls:
      - http://tot1server:15000/tot/
  aris:
    - ari: "anja:totplugin:extract:/Azure/PowerBI/Cliente/"
  connection:
    tenant: <tenant-id>
    clientId: <client-id>
    clientSecret: <client-secret>
  mapping:
    app: POWERBI-APP
    dashboard: POWERBI-DASHBOARD
    report: POWERBI-REPORT
    semantic-model: POWERBI-MODEL
```

```
eureka:
  instance:
    hostname: totpluginpowerbi1server
  client:
    serviceUrl:
      defaultZone: http://hecate1server:15000/tot/eureka
```

# Anexos

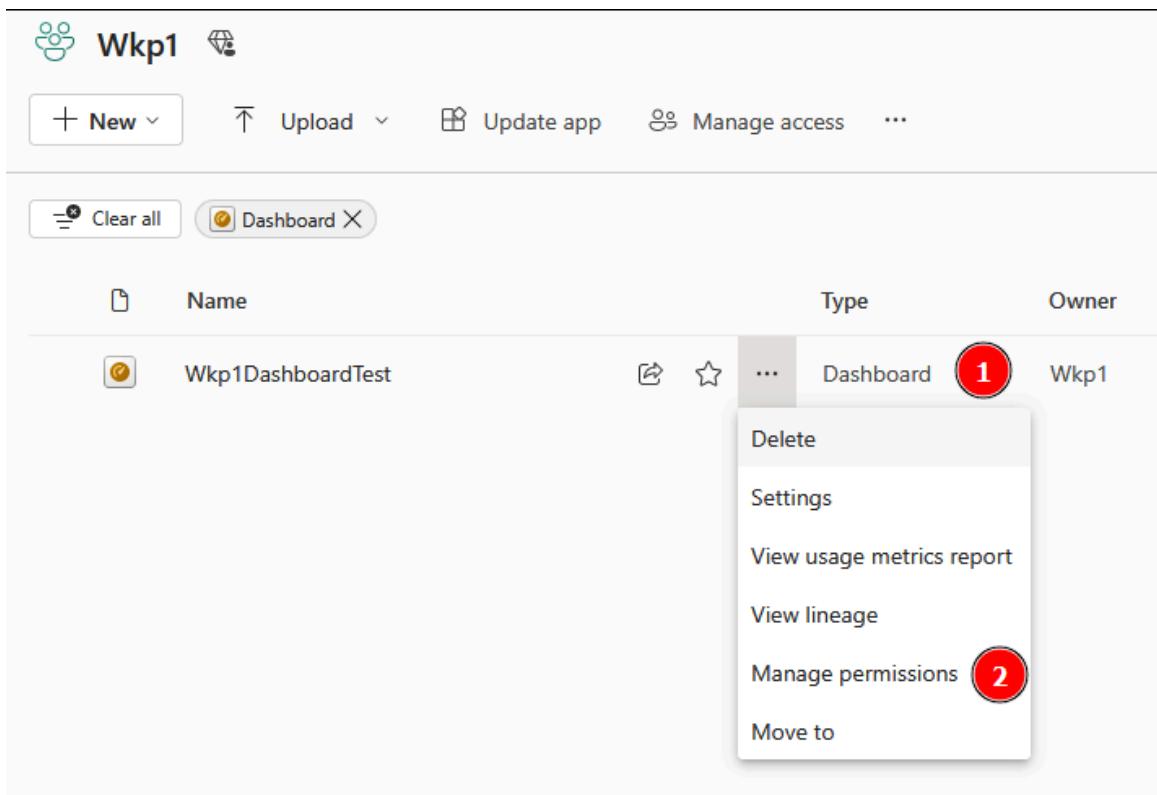
## Asignación grupo a Report

Name	Type	Owner
Carga_Incremental_Todo_Imported_Mismo...	Report	Wkp1
Carga_Incremental_Todo_Imported_Mismo_Modelo_No	Explore this data (preview)	Wkp1
Prueba_composite_model_and_roles_demo_limpio	Analyze in Excel	Wkp1
Prueba_composite_model_and_roles_demo_limpio	Delete	Wkp1
	Quick insights	
	Save a copy	
	Settings	
	View usage metrics report	
	View lineage	
	Create paginated report	
	Manage permissions	2
	Move to	



The screenshot shows the Anjana Data interface with a 'Grant people access' dialog box overlaid. The interface includes a 'Related content' sidebar with 'Dashboards', 'Workbooks', and 'Semantic models' options. The main area has tabs for 'Links', 'Direct access' (which is selected and highlighted with a red circle labeled '1'), 'Pending' (with a red circle labeled '2'), and 'Shared views'. Below these tabs is a table titled 'People and groups with access' with columns for 'Email Address' and 'Pending'. The dialog box has a search bar with 'dsa' typed in (labeled '3') and a list of results: 'Dsa\_18SeptSqlserver\_v0', 'Dsa\_ActorSqlserverAd\_v1', 'Dsa\_azure\_ad\_10685\_v0', 'Dsa\_AZURE\_EXP\_v0', and 'Dsa\_AzureBeaCOCO\_v0'. At the bottom of the dialog are 'Grant access' and 'Cancel' buttons (labeled '4').

## Asignación de grupos a Dashboard

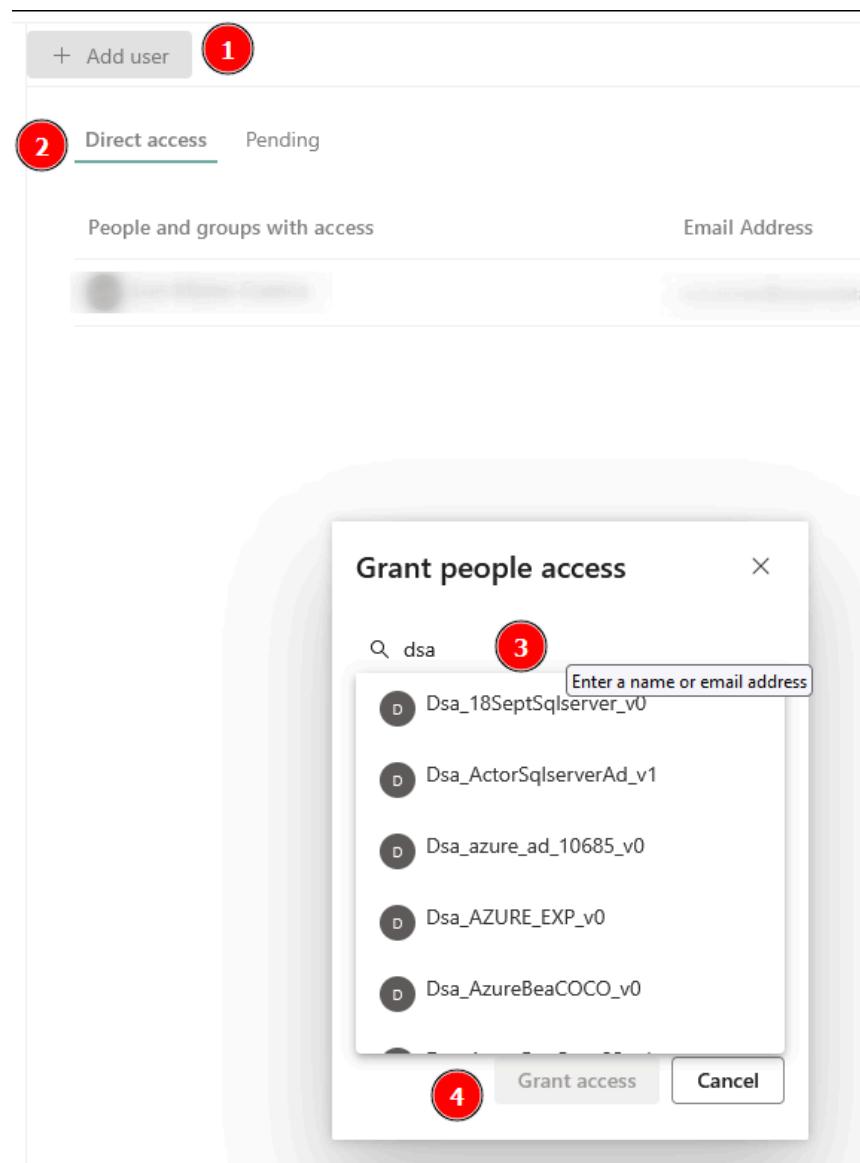


The screenshot shows the Anjana Data interface with the workspace name "Wkp1" at the top. The main area displays a table with columns: Name, Type, and Owner. A single row is visible, representing a "Dashboard" named "Wkp1DashboardTest" owned by "Wkp1". A context menu is open over this row, with the "Manage permissions" option highlighted. The entire context menu is enclosed in a red circle labeled "1". Within the menu, the "Manage permissions" link is also highlighted with a red circle labeled "2".

	Name	Type	Owner
	Wkp1DashboardTest	Dashboard	Wkp1

Context menu options (highlighted with red circles):

- Delete
- Settings
- View usage metrics report
- View lineage
- Manage permissions **2**
- Move to



The screenshot shows a user interface for managing access. At the top, there is a button labeled "+ Add user" with a red circle containing the number 1. Below it, there are two tabs: "Direct access" (which is selected, indicated by a red circle with the number 2) and "Pending".

Under the "Direct access" tab, there are two sections: "People and groups with access" and "Email Address". Below these sections, there is a blurred list of users.

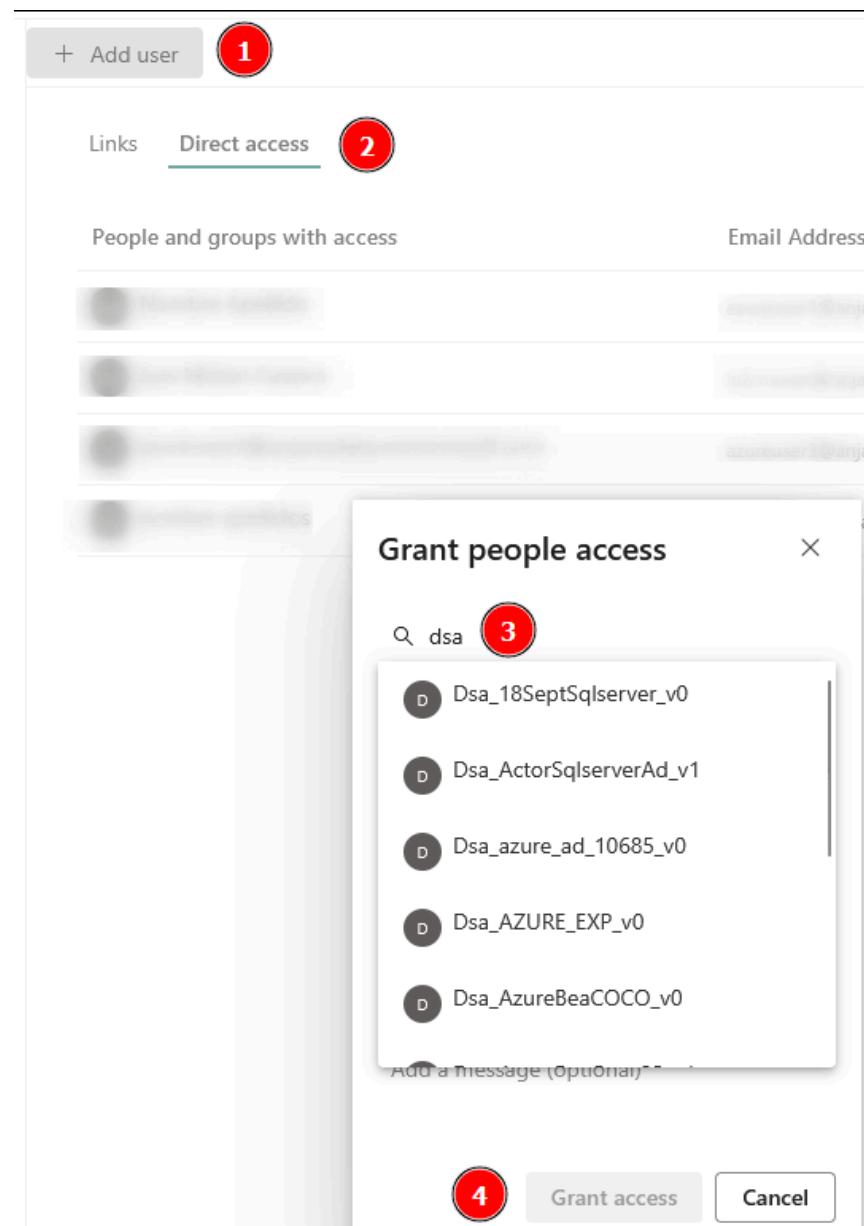
A modal dialog box titled "Grant people access" is displayed in the center. It contains a search bar with the placeholder "Enter a name or email address" and a red circle containing the number 3. Below the search bar is a list of users:

- Dsa\_18SeptSqlserver\_v0
- Dsa\_ActorSqlserverAd\_v1
- Dsa\_azure\_ad\_10685\_v0
- Dsa\_AZURE\_EXP\_v0
- Dsa\_AzureBeaCOCO\_v0

At the bottom of the dialog, there are two buttons: "Grant access" (which is highlighted with a red circle containing the number 4) and "Cancel".

## Asignación de grupo a Modelo Semántico

	Name	Type	Owner
	Carga_Incremental_Todo_Imported_Mismo_Modelo_No_Co...	Report	Wkp1Pro
	Carga_Incremental_Todo_Imported_Mism...	   ... Semantic model	Wkp1Pro
	Prueba_composite_model_and_roles_demo_limpio	 Explore this data (preview)	Wkp1Pro
	Prueba_composite_model_and_roles_demo_limpio	Analyze in Excel Create report Auto-create report Create paginated report Delete Quick insights Security Rename Open data model Settings Download this file Manage permissions	Wkp1Pro



The screenshot shows a user interface for managing access. At the top, there is a button labeled "+ Add user" with a red circle containing the number 1. Below it, there are two tabs: "Links" and "Direct access", with "Direct access" being the active tab, indicated by a red circle containing the number 2. The main area is titled "People and groups with access" and shows a list of users with blurred names and email addresses. To the right, there is a column for "Email Address". A modal dialog box is open in the center, titled "Grant people access". It contains a search bar with the text "Q dsa" and a red circle containing the number 3. A list of users is displayed, including "Dsa\_18SeptSqlserver\_v0", "Dsa\_ActorSqlserverAd\_v1", "Dsa\_azure\_ad\_10685\_v0", "Dsa\_AZURE\_EXP\_v0", and "Dsa\_AzureBeaCOCO\_v0". At the bottom of the dialog, there is a text input field labeled "Add a message (Optional)" and two buttons: "Grant access" (highlighted with a red circle containing the number 4) and "Cancel".

## Asignación de grupo a APP

### Apps

Apps are collections of dashboards and reports in one easy-to-find place.

	Name	Publisher
	Wkp1App	<span>1</span> ... Luis Moran Cuenca
	Microsoft Fabric Capacity Metrics	<span>2</span> Edit Delete Manage permissions Settings

Wkp1App																							
<span>1</span> + Add user	<span>2</span> Manage audiences	Pending requests	Pending invitations																				
<table border="1"> <thead> <tr> <th>People and groups with access</th> <th>Email Address</th> <th>Audiences</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td>Workspace users</td> <td>All</td> <td></td> <td></td> </tr> <tr> <td> [REDACTED]</td> <td>Wkp1App</td> <td>...</td> <td></td> </tr> <tr> <td> [REDACTED]</td> <td>Wkp1App</td> <td>...</td> <td></td> </tr> <tr> <td> [REDACTED]</td> <td>Wkp1App</td> <td>...</td> <td></td> </tr> </tbody> </table>				People and groups with access	Email Address	Audiences	Options	Workspace users	All			 [REDACTED]	Wkp1App	...		 [REDACTED]	Wkp1App	...		 [REDACTED]	Wkp1App	...	
People and groups with access	Email Address	Audiences	Options																				
Workspace users	All																						
 [REDACTED]	Wkp1App	...																					
 [REDACTED]	Wkp1App	...																					
 [REDACTED]	Wkp1App	...																					

**Grant access**

Add a person or security group to an audience to give them access to this app.

**Audience**

3 Wkp1App

**Add people**

4 Dsa\_18SeptSqlserver\_v0

Enter a name or email

5 Grant access Cancel