

Distribute Power BI content to external guest users using Azure Active Directory B2B

**Summary:** This is a technical whitepaper outlining how to distribute content to users outside the organization using the integration of Azure Active Directory Business-to-business (AAD B2B).

**Writers:** Ajay Anandan, Kasper de Jonge

**Technical Reviewers:** Adam Wilson, Sirui Sun, Sergei Gundorov, Jacob Grimm, Adam Saxton

Published: March 2018

Contents

[Introduction 3](#_Toc497743985)

[Scenario 3](#_Toc497743986)

[Option 1: Create duplicate identities for partner users 4](#_Toc497743987)

[Option 2: Create a custom Power BI embedded application using custom authentication 5](#_Toc497743988)

[Power BI + AAD B2B – Step-by-Step instructions 5](#_Toc497743989)

[1. Create BI portal in Power BI 5](#_Toc497743990)

[2. Invite Guest Users 7](#_Toc497743991)

[a. Planned Invites 7](#_Toc497743992)

[b. Ad-hoc Invites 8](#_Toc497743993)

[3. Distribute Content 8](#_Toc497743994)

[Under the hood: How is Lucy from Supplier1 able to access Power BI content from Contoso’s tenant? 10](#_Toc497743995)

[Licensing 11](#_Toc497743996)

[Approach 1: Contoso uses Power BI Premium 11](#_Toc497743997)

[Approach 2: Contoso assigns Power BI Pro licenses to guest users 12](#_Toc497743998)

[Approach 3: Guest users bring their own Power BI Pro license 12](#_Toc497743999)

[User based security 13](#_Toc497744000)

[Dynamic Row level security 16](#_Toc497744001)

[Connecting on premises data sources 20](#_Toc497744002)

[Governance 21](#_Toc497744003)

[Control guest invites 21](#_Toc497744004)

[Conditional Access policies for guest users 21](#_Toc497744005)

[FAQ 21](#_Toc497744006)

# Introduction

Power BI gives organizations a 360-degree view of their business and empowers everyone in these organizations to make intelligent decisions using data. Many of these organizations have strong and trusted relationships with external partners, clients and contractors. These organizations need to provide secure access to Power BI dashboards and reports to users in these external partners.

Power BI integrates with Azure Active Directory Business-to-business (AAD B2B) to allow secure distribution of Power BI content to guest users outside the organization – while still maintaining control over the internal data.

This white paper will cover the all the details you need to know about Power BI’s integration with Azure Active Directory B2B. We will cover its most common use case, set-up, licensing, and row level security.

(Note: Throughout this white paper, we will refer to Azure Active Directory as AAD and Azure Active Directory Business to Business as AAD B2B.).

# Scenario

Contoso is an automotive manufacturer and works with many diverse suppliers who provide it with all the components, materials and services necessary to run its manufacturing operations. Contoso wants to streamline its supply chain logistics and plans to use Power BI to monitor key performance metrics of its supply chain.

To achieve this, Contoso would like to build a BI portal with Power BI and give its own employees and guest users from partner organizations access to this BI portal. Contoso uses Azure Active Directory (AAD) as its Identity provider.

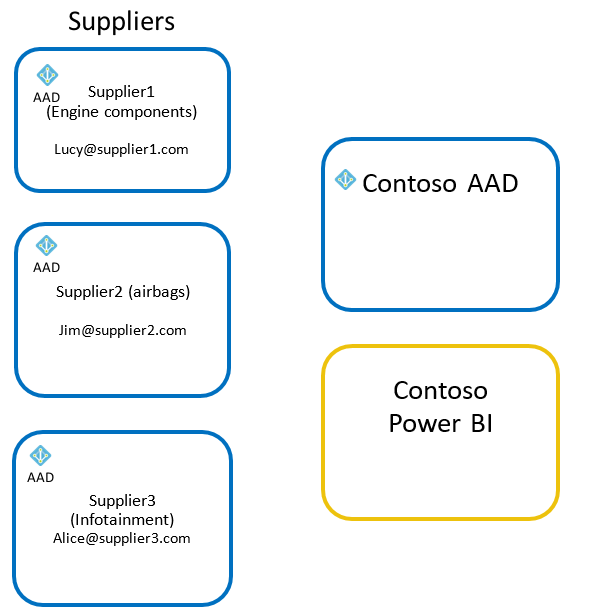


Figure 1

Before Power BI’s integration with AAD B2B, Contoso had two options:

## Option 1: Create duplicate identities for partner users

With this option, Contoso had to manually create duplicate identities for each partner user in the Contoso Tenant (Figure 2). Contoso This approach had three main issues:

1. Guest users from partner organizations must remember two sets of credentials now – one to access content from their own organization and the other to access content from Contoso. This is a hassle for these guest users and many guest users are confused by this experience.
2. Contoso might want to enforce more stringent authorization and governance policies for external users compared to internal users. To achieve this, Contoso needs to create an in-house nomenclature for external users and all Contoso users need to be educated about this nomenclature.
3. Contoso’s administrators must manage the identities for these guest users. If a guest user leaves his/her organization, Contoso needs to manually remove access to this guest user from its own AAD. If Contoso has lots of guest users, this becomes an identity management nightmare.

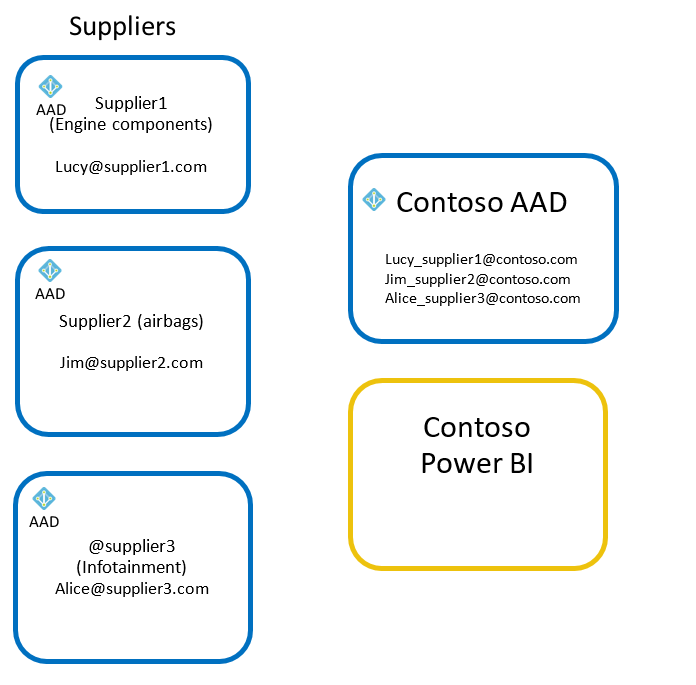


Figure 2

## Option 2: Create a custom Power BI embedded application using custom authentication

The other option is for Contoso to build its own custom embedded Power BI application with custom authentication (‘App owns data’ approach). Many organizations do not have the time or resources to create a custom application just to distribute Power BI content to their external partners.

# Power BI + AAD B2B – Step-by-Step instructions

Power BI’s integration with AAD B2B gives Contoso a seamless, hassle-free way to provide guest users with secure access to its BI portal. Contoso can set this up with three steps:

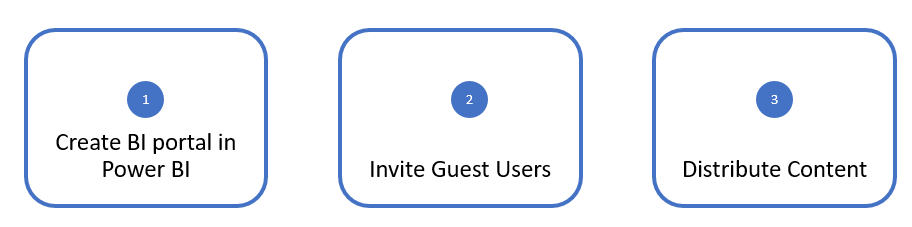
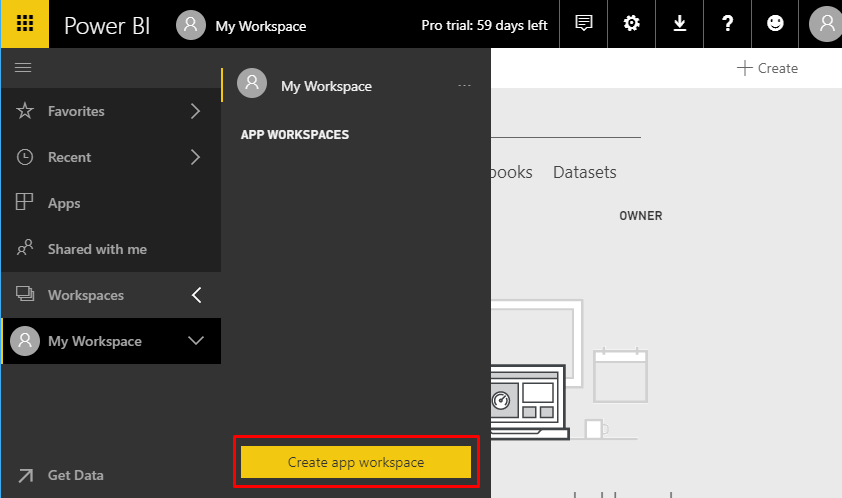


Figure 3

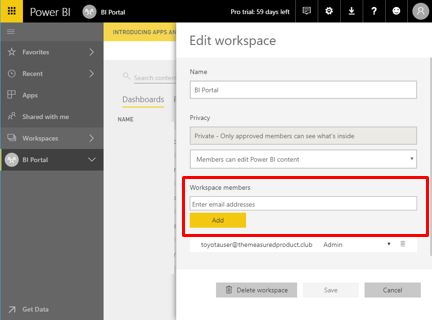
## Create BI portal in Power BI

The first task for Contoso is to create their BI portal in Power BI. Contoso’s BI portal will consist of a collection of purpose-built dashboards and reports that will be made available to many internal and guest users. The recommended way for doing this in Power BI is to build a Power BI app. Learn more about [apps in Power BI](https://powerbi.microsoft.com/en-us/blog/distribute-to-large-audiences-with-power-bi-apps/).

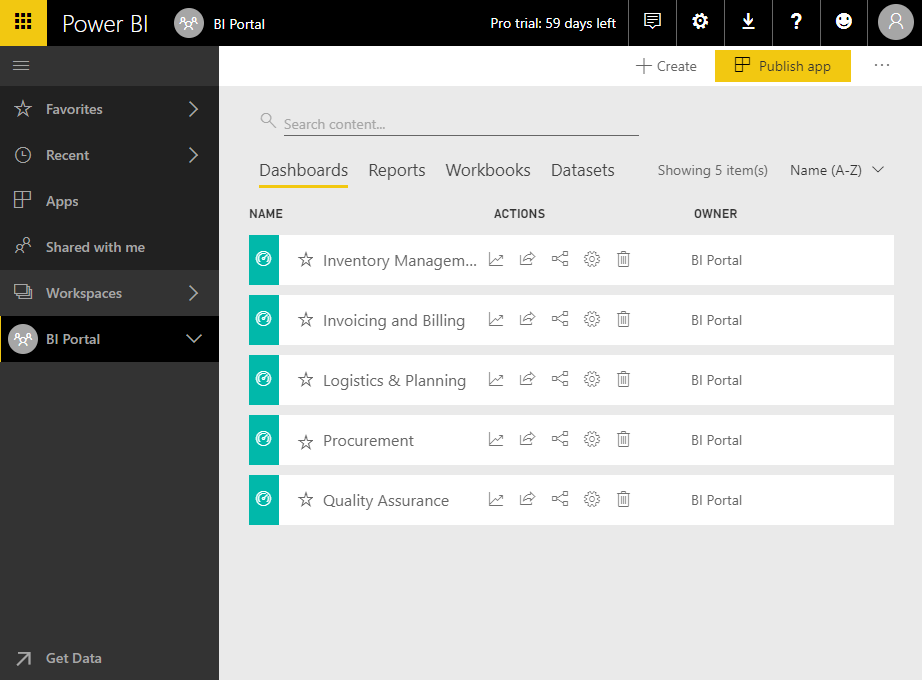
* Contoso’s BI team creates an App workspace in Power BI



* Other authors are added to the workspace



* Content is created inside the workspace



Now that the content is created in an app workspace, Contoso is ready to invite guest users in partner organizations to consume this content.

## Invite Guest Users

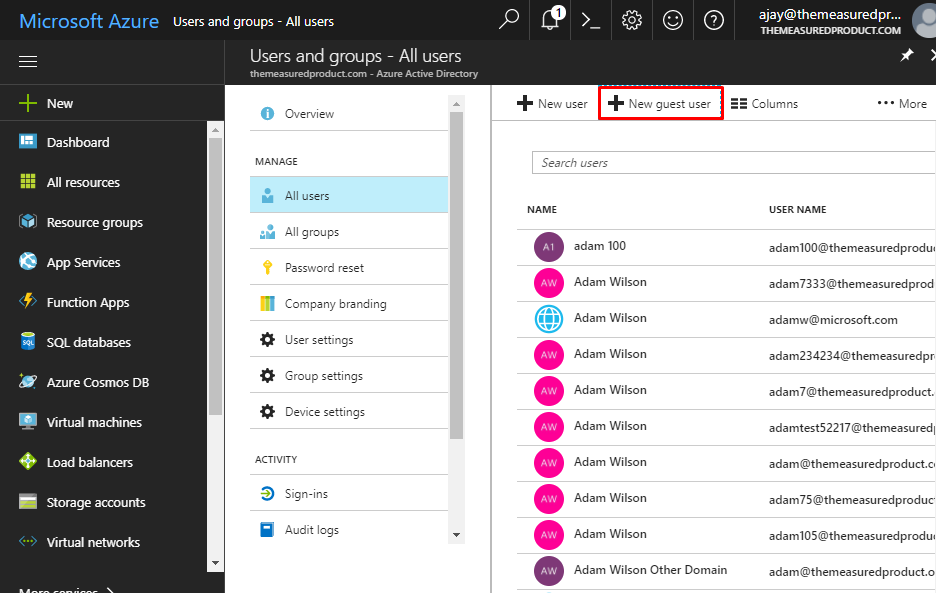
There are two ways for Contoso to invite guest users to its BI portal in Power BI:

1. Planned Invites
2. Ad-hoc Invites

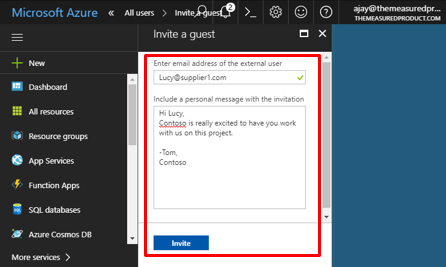
### Planned Invites

In this approach, Contoso invites the guest users to its AAD ahead of time and then distributes Power BI content to them. Contoso can invite guest users from the AAD portal or using PowerShell. Here are the steps to invite guest users from the AAD portal:

* Contoso’s AAD administrator navigates to **AAD portal > Azure Active Directory > Users and groups > All users > New guest user**



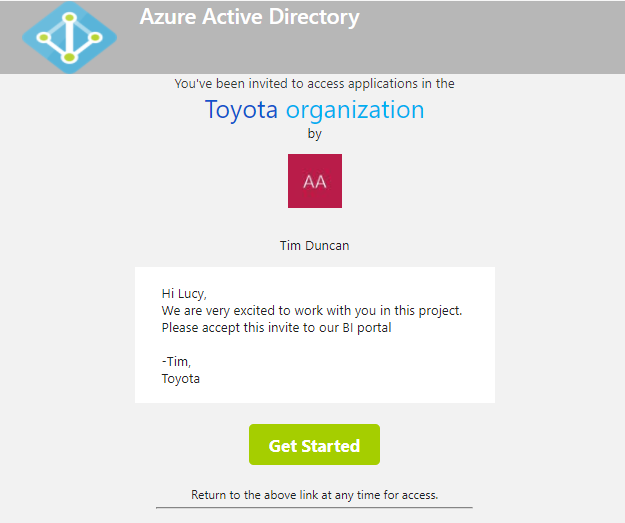
* Add an invitation message for the guest users and click Invite



**Note:** To invite guest users from the AAD portal, you need to an administrator for the Azure Active Directory of your tenant.

If Contoso wants to invite many guest users, they can do so using PowerShell. Contoso’s AAD administrator stores the email addresses of all the guest users in a CSV file. Here are [Azure Active Directory B2B collaboration code and PowerShell samples](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-code-samples) and instructions.

After the invitation, guest users will receive an email with the invitation link.



Contoso Organization

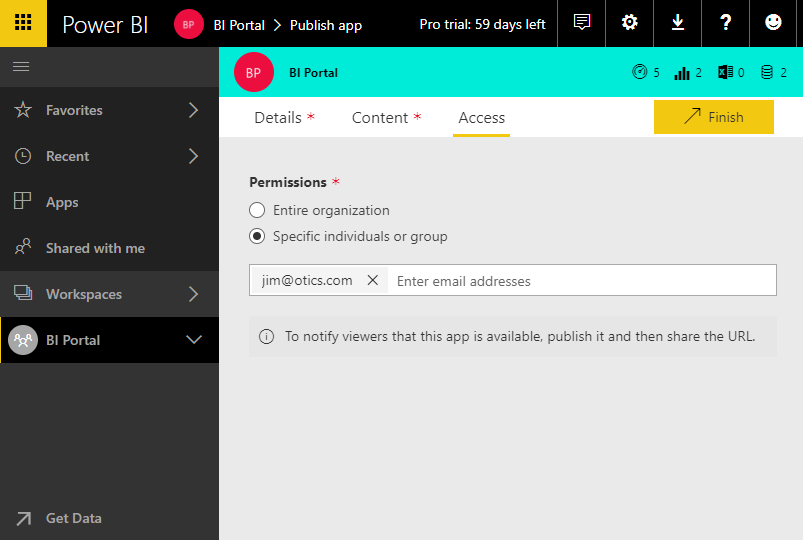
Once the guest user clicks the link, he/she will be added as a guest user to the Contoso AAD tenant.

**Note**: It is possible to change the layout of the invitation email using the AAD branding feature as described [here](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-invitation-email).

### Ad-hoc Invites

What if Contoso does not know all the guest users it wants to invite ahead of time? Or, what if the analyst in Contoso who created the BI portal wants to distribute content to guest users herself? We also support this scenario in Power BI with ad-hoc invites.

The analyst can just add the external users to the access list of the app when she is publishing it. The guest user will get an invite and once they accept it, they will be automatically redirected to the Power BI content.

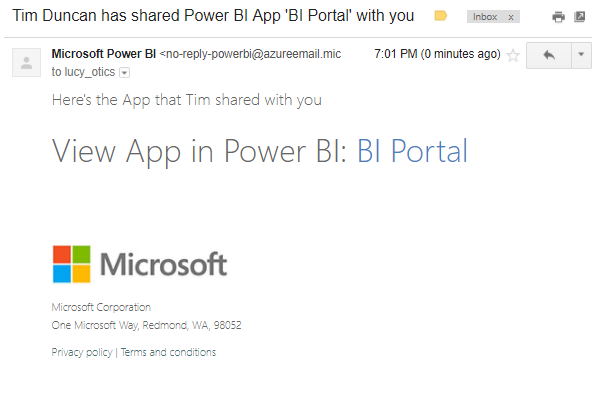


**Note:** Invites are needed only the first time an external user is invited to your organization.

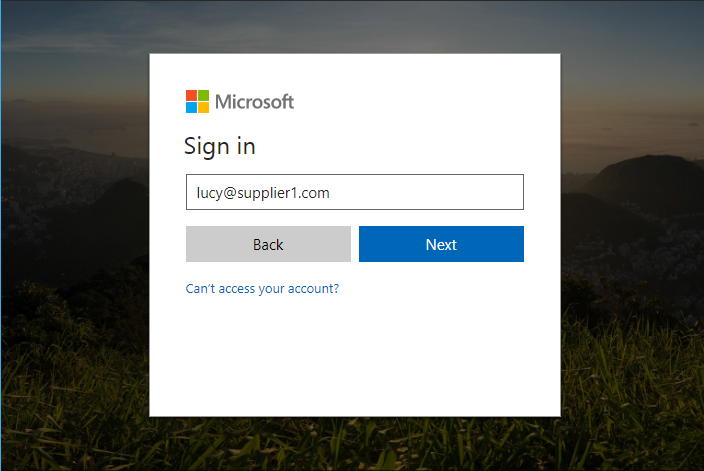
## Distribute Content

Now that Contoso’s BI team has created the BI portal and invited guest users, they can distribute their portal to their end users by giving guest users access to the app and publishing it. Power BI auto-completes names of guest users who have been previously added to the Contoso tenant. Adhoc invitations to other guest users can also be added at this point.

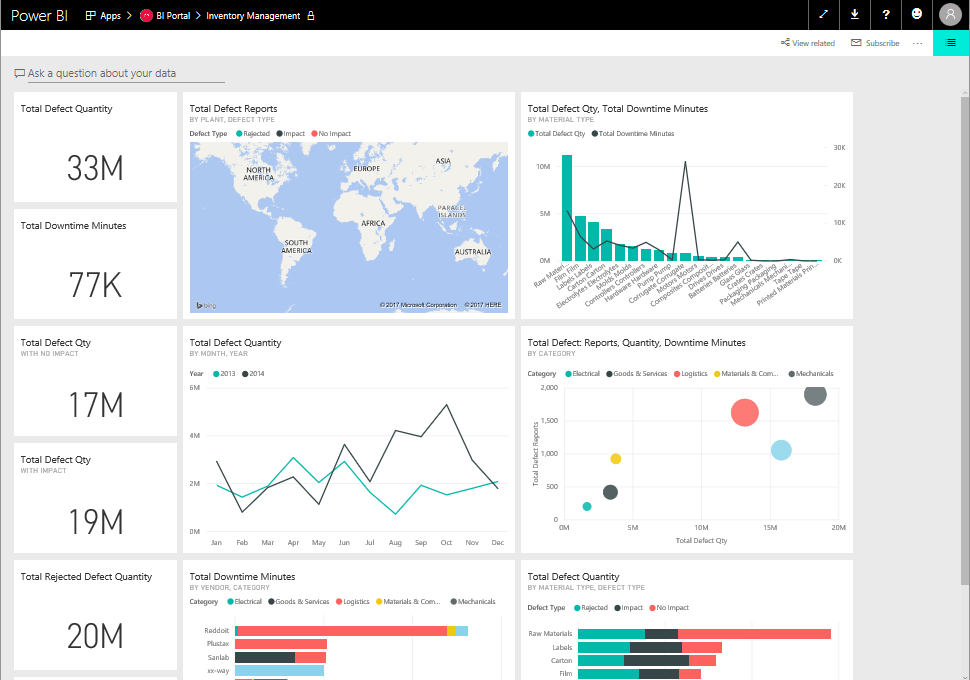
Guest users get an email with a link to the app.



On clicking this link, guest users will be asked to authenticate with their own organization’s identity.



Once they are successfully authenticated, they will be redirected to Contoso’s BI app.



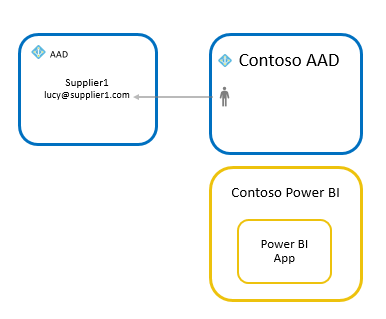
Guest users can subsequently get to Contoso’s app by clicking the link in the email or bookmarking the link. Contoso can also make it easier for guest users by adding this link to any existing extranet portal that the guest users already use.

## Under the hood: How is Lucy from Supplier1 able to access Power BI content from Contoso’s tenant?

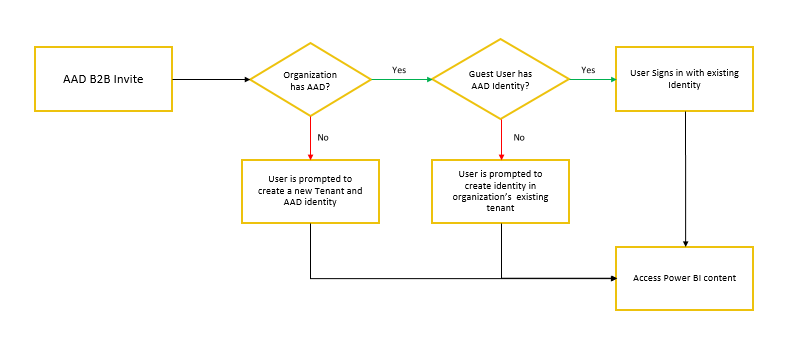
Now that we have seen how Contoso is able to seamlessly distribute Power BI content to guest users in partner organizations, let’s look at how this works under the hood.

When Contoso invited [lucy@supplier1.com](mailto:lucy@supplier1.com) to its directory, AAD creates a link between [Lucy@supplier1.com](mailto:Lucy@supplier1.com) and the Contoso AAD tenant. This link lets AAD know that Lucy@supplier1.com can access content in the Contoso tenant.

When Lucy tries to access Contoso’s Power BI app, AAD verifies that Lucy can access the Contoso tenant and then provides Power BI a token that indicates that Lucy is trying access content in the Contoso tenant. Power BI uses this token to authorize and ensure that Lucy has access to Contoso’s Power BI app.



Power BI’s integration with AAD B2B works with all business email addresses. If the user does not have an AAD identity, they will be prompted to create one. Here is the detailed flow:



It is important to recognize that the AAD account will be used or created in the external parties AAD, this will make it possible that Lucy can use her own username and password and her login will automatically be removed whenever she leaves the company when her organization also uses AAD.

# Licensing

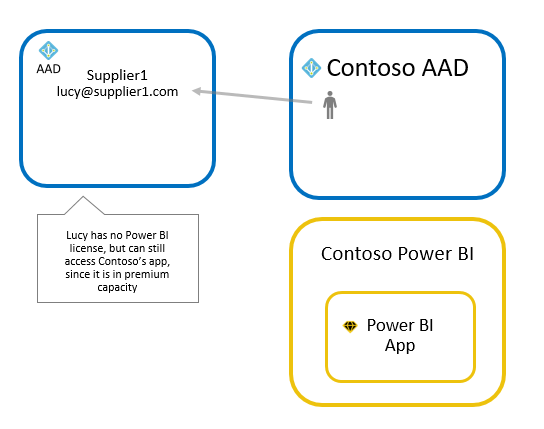
Contoso has three approaches to license guest users from its partner organizations.

**Note:** Guest users are limited to consumption of content only. Guests can view apps, dashboards, reports, export data and create email subscriptions for dashboards and reports. They can't access workspaces or publish their own content.

## Approach 1: Contoso uses Power BI Premium

With this approach, Contoso purchases Power BI Premium capacity and assigns it’s BI portal content to this capacity. This allows guest users from partner organizations to access Contoso’s Power BI app without any Power BI license.

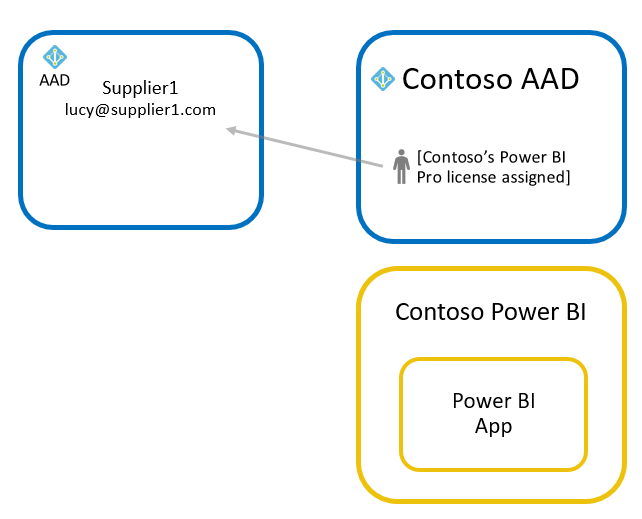
Contoso can also take advantage of other Power BI premium capabilities for its apps like increased refresh rates, dedicated capacity and large model sizes.



## Approach 2: Contoso assigns Power BI Pro licenses to guest users

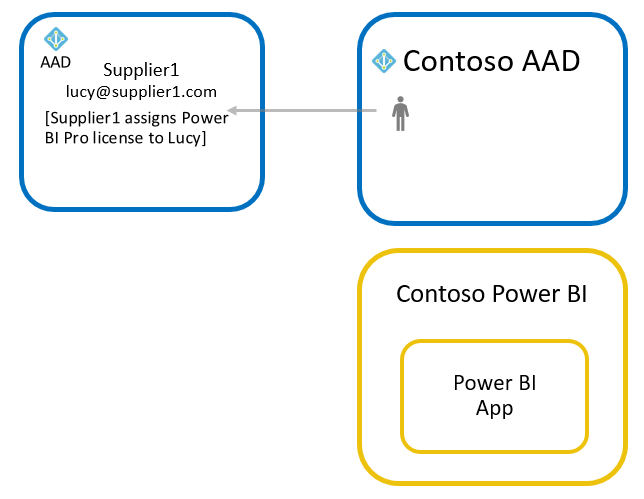
With this approach, Contoso assigns pro licenses to guest users from partner organizations – this can be done from Contoso’s Office 365 admin portal. This allows guest users from partner organizations to access Contoso’s Power BI app without purchasing a license themselves.

**Note:** Contoso’s pro license applies to guest users only when they access content in the Contoso tenant.



## Approach 3: Guest users bring their own Power BI Pro license

With this approach, Supplier 1 assigns a Power BI pro license to Lucy. She can then access Contoso’s Power BI app with this license.



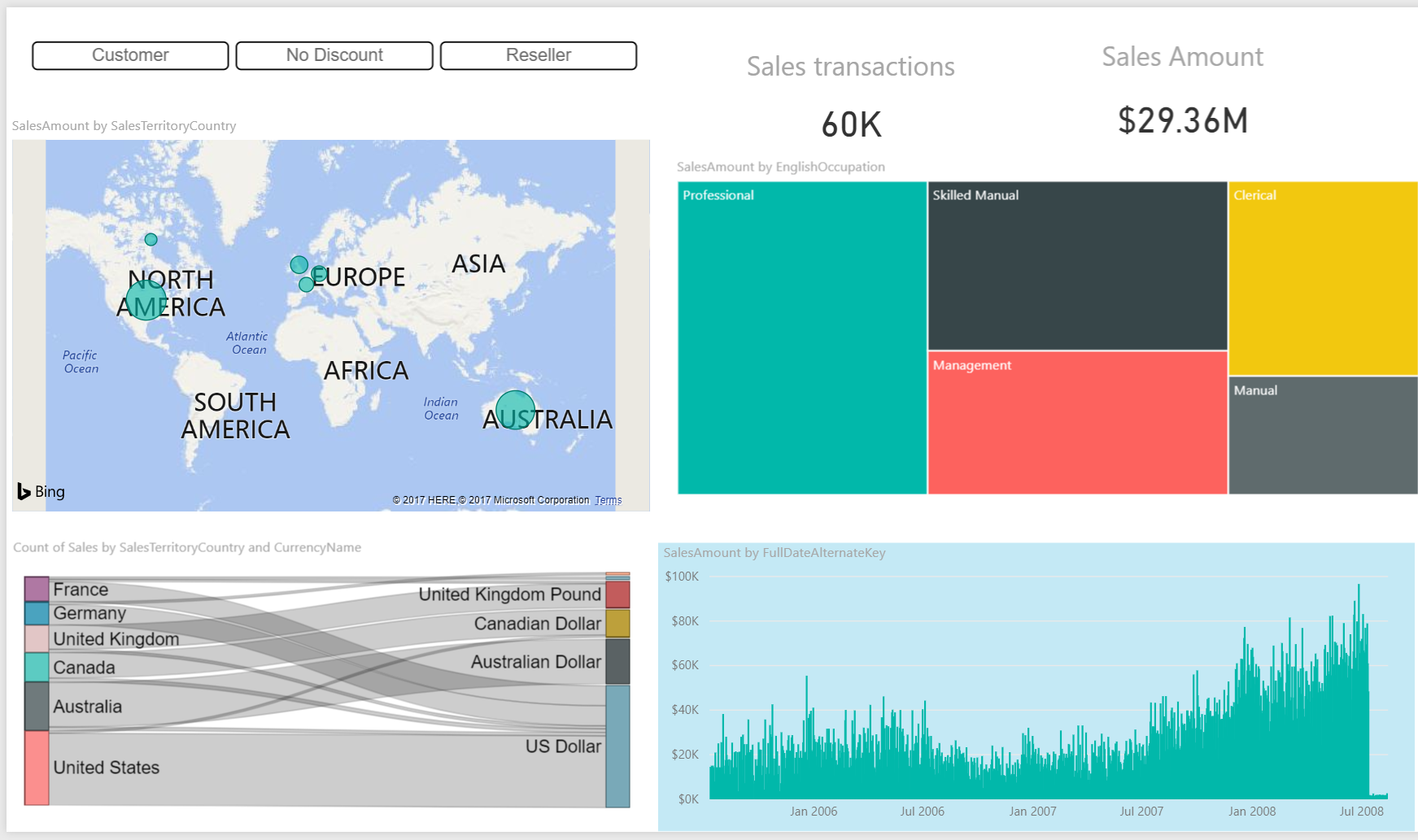
# User based security

One of the most powerful features of Power BI is Row Level Security. This feature allows Contoso to create a single report and dataset but still have different security rules described for different users. For an in-depth explanation, see [Row-level security (RLS)](https://powerbi.microsoft.com/en-us/documentation/powerbi-admin-rls/).

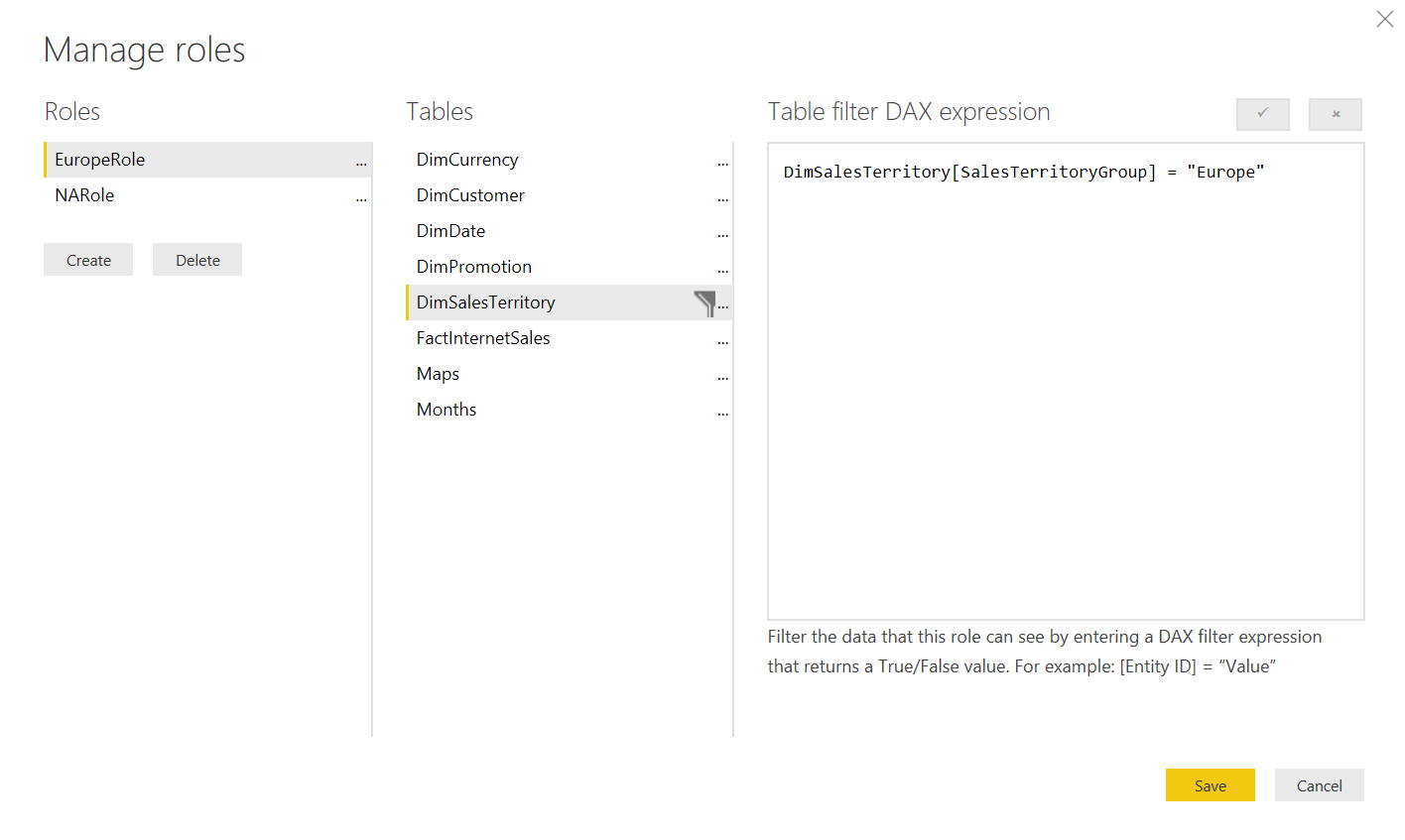
Power BI’s integration with AAD B2B allows Contoso to assign Row Level Security rules to guest users as soon as they are invited to the Contoso tenant. As we have seen before, Contoso can add guest users through either planned or ad-hoc invites. If Contoso wants to enforce row level security, it is recommended to use planned invites to add the guest users ahead of time and assigning them to the security roles before sharing the content. If Contoso instead uses ad-hoc invites, there might be a short period of time where the guest users will not be able to see any data.

Let’s walk through this with an example.

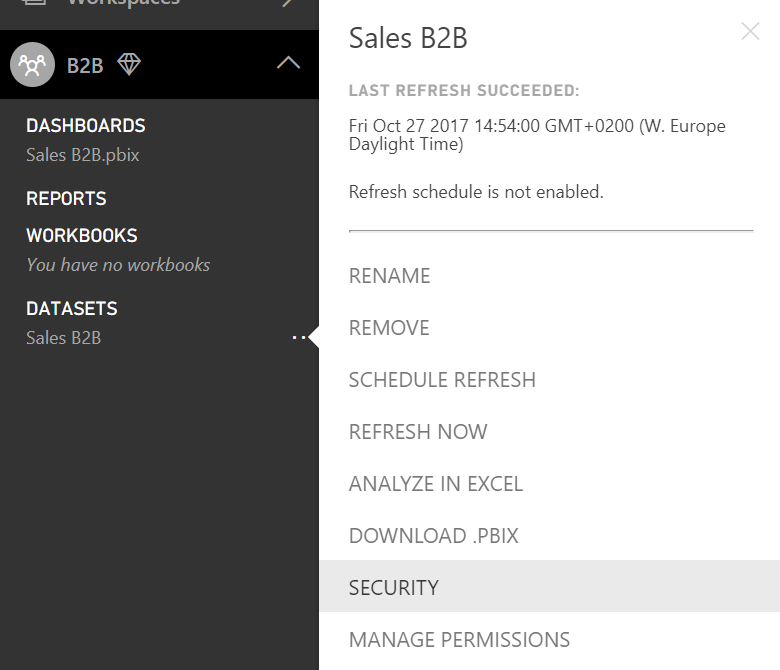
As mentioned before, Contoso has suppliers around the globe and they want to make sure that the users from their supplier organizations get insights from data from just their territory. But users from Contoso can access all the data. Instead of creating several different reports, Contoso creates a single report and filter the data based on who is consuming the report.



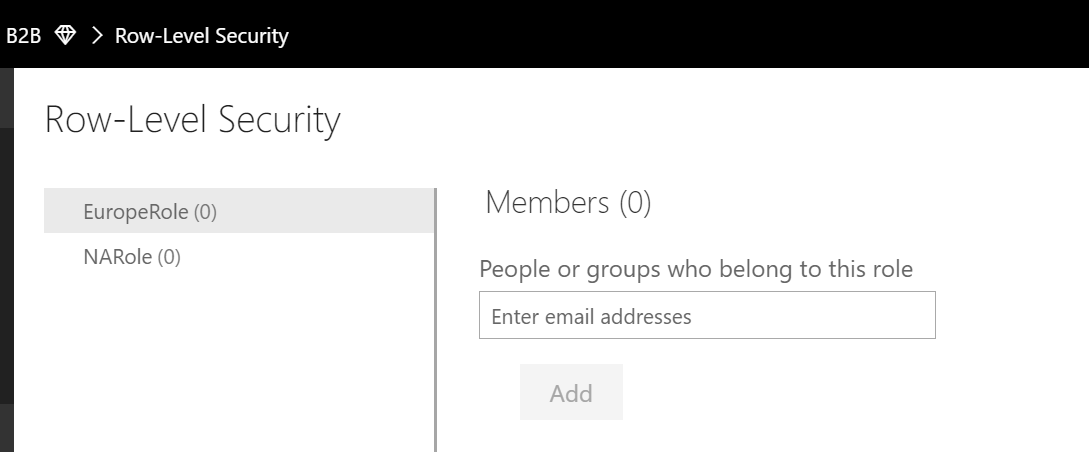
To make sure Contoso can filter data based on who is connecting, two roles are created in Power BI desktop. One to filter all the data from the SalesTerritory “Europe” and another for “North America”.



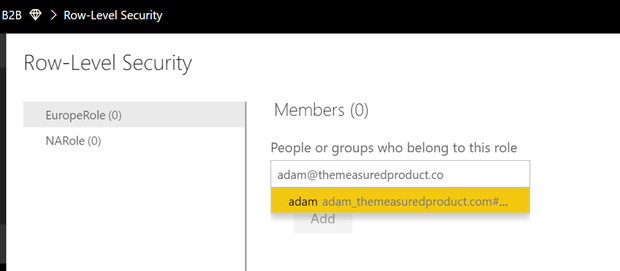
Whenever roles are defined in the mode, a user must be assigned to a role for them to get access to any data. The assignment of roles happens inside the Power BI service (Datasets>Security)



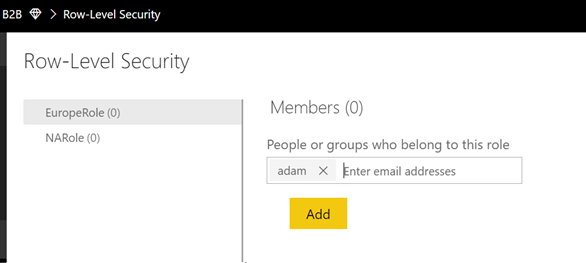
This opens a page where Contoso’s BI team can see the two roles they created. Now Contoso’s BI team can assign users to the roles.



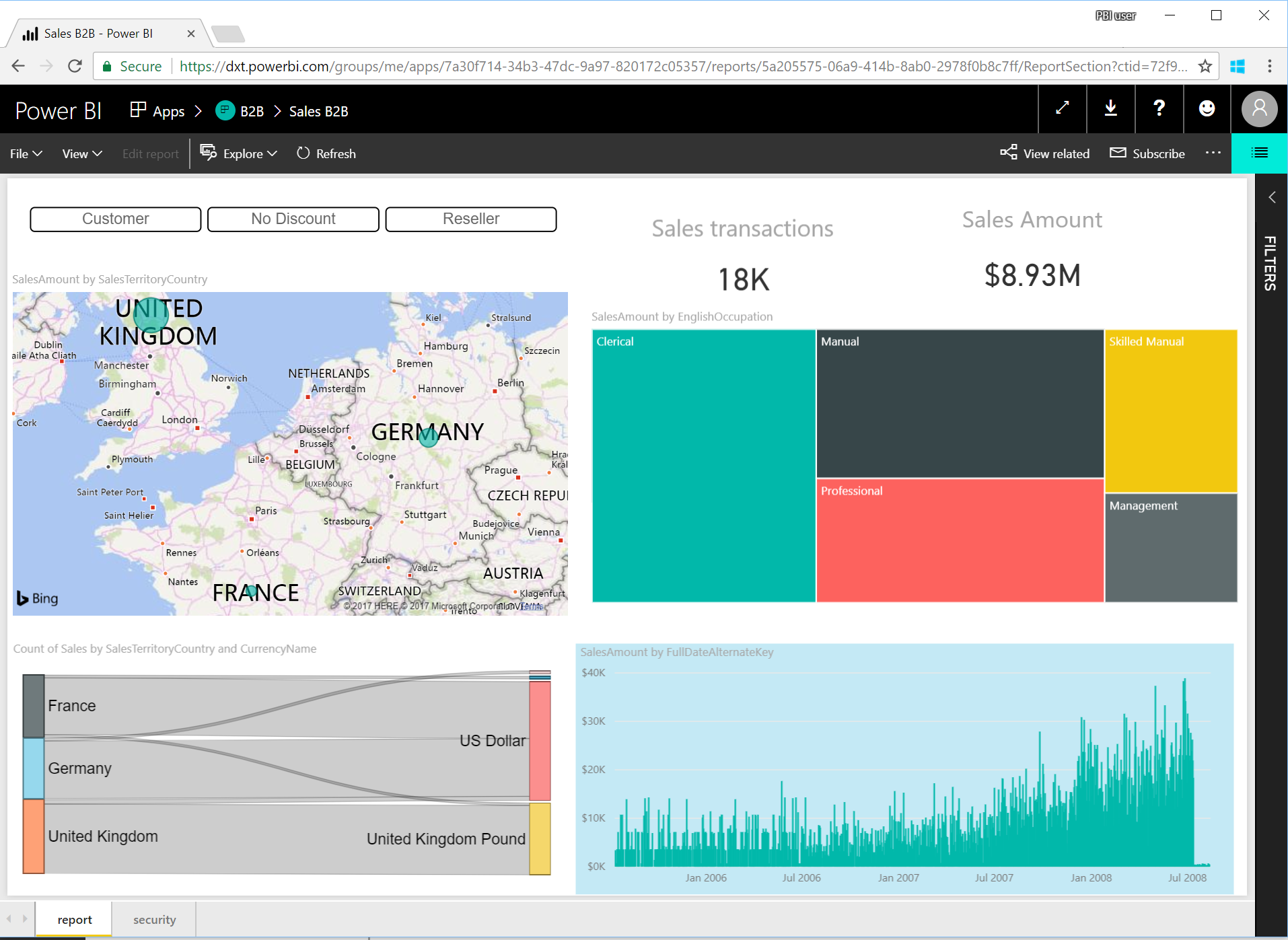
In the example Contoso is adding a user in a partner organization with email address “[adam@themeasuredproduct.com](mailto:adam@themeasuredproduct.com)” to the Europe role:



When this gets resolved by AAD, Contoso can see the name show up in the window ready to be added:



Now when this user opens the app that was shared with him, he will only see a report with data from Europe:

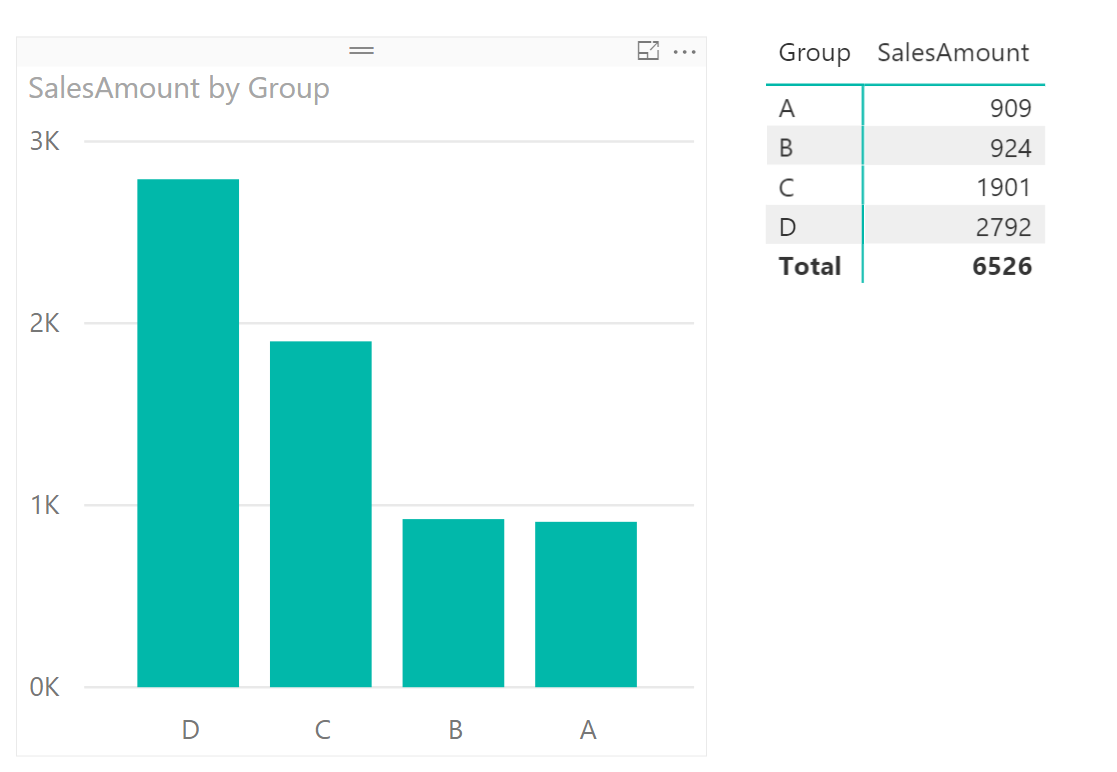


# Dynamic Row level security

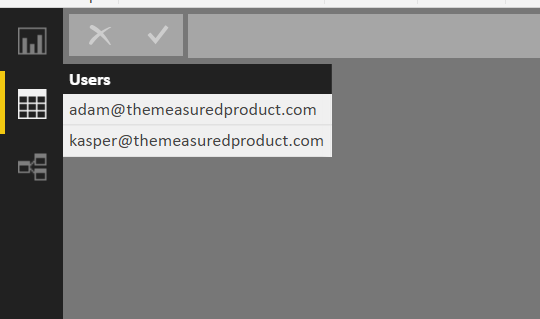
Another interesting topic is to see how dynamic row level security (RLS) work with B2B.

In short, Dynamic row level security works by filtering data in the model based on the username of the person connecting to Power BI. Instead of adding multiple roles for groups of users, you define the users in the model. We won’t describe the pattern in detail here. Kasper de Jong offers a detailed writeup on all the flavors of row level security in [Power BI Desktop Dynamic security cheat sheet](https://www.kasperonbi.com/power-bi-desktop-dynamic-security-cheat-sheet/), and in [this whitepaper](https://msdn.microsoft.com/en-us/library/jj127437.aspx) .

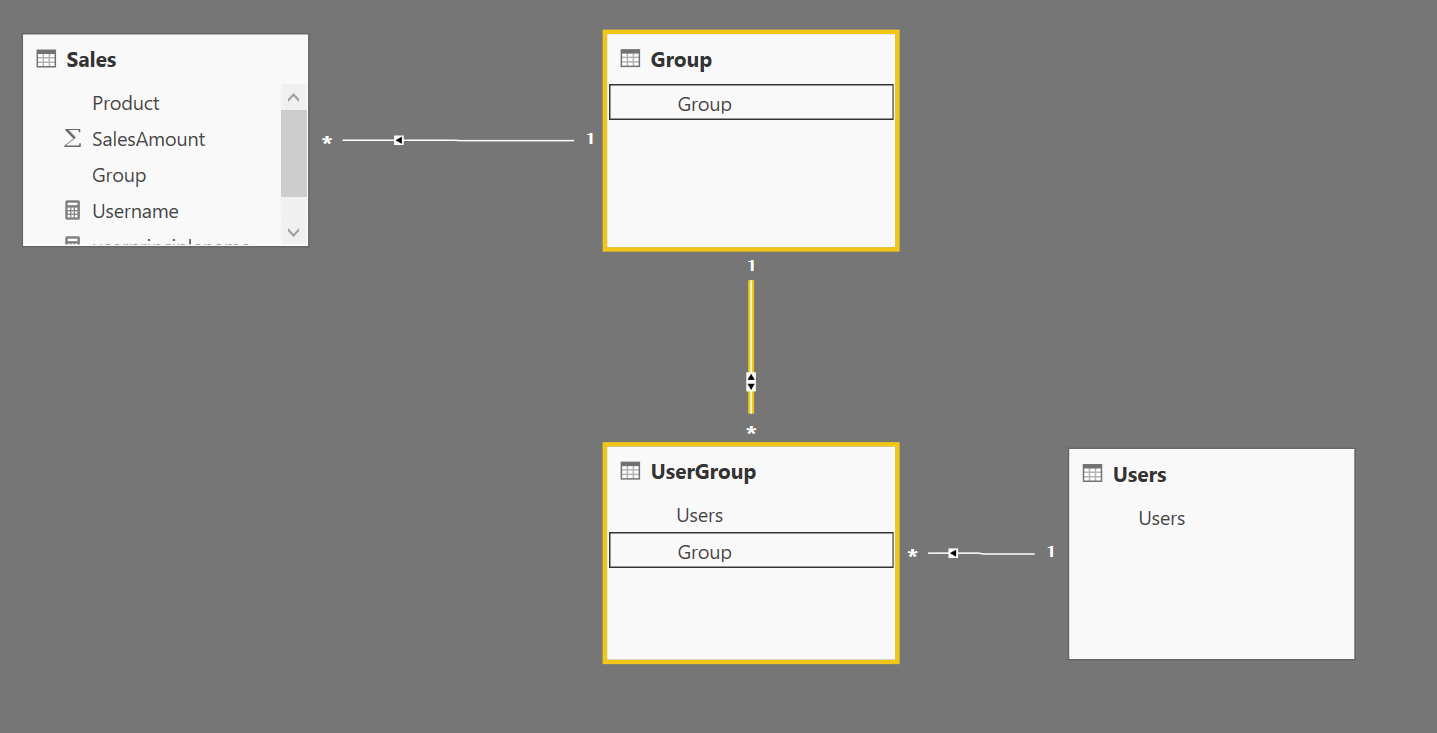
Let’s look at a small example - Contoso has a simple report on sales by groups:



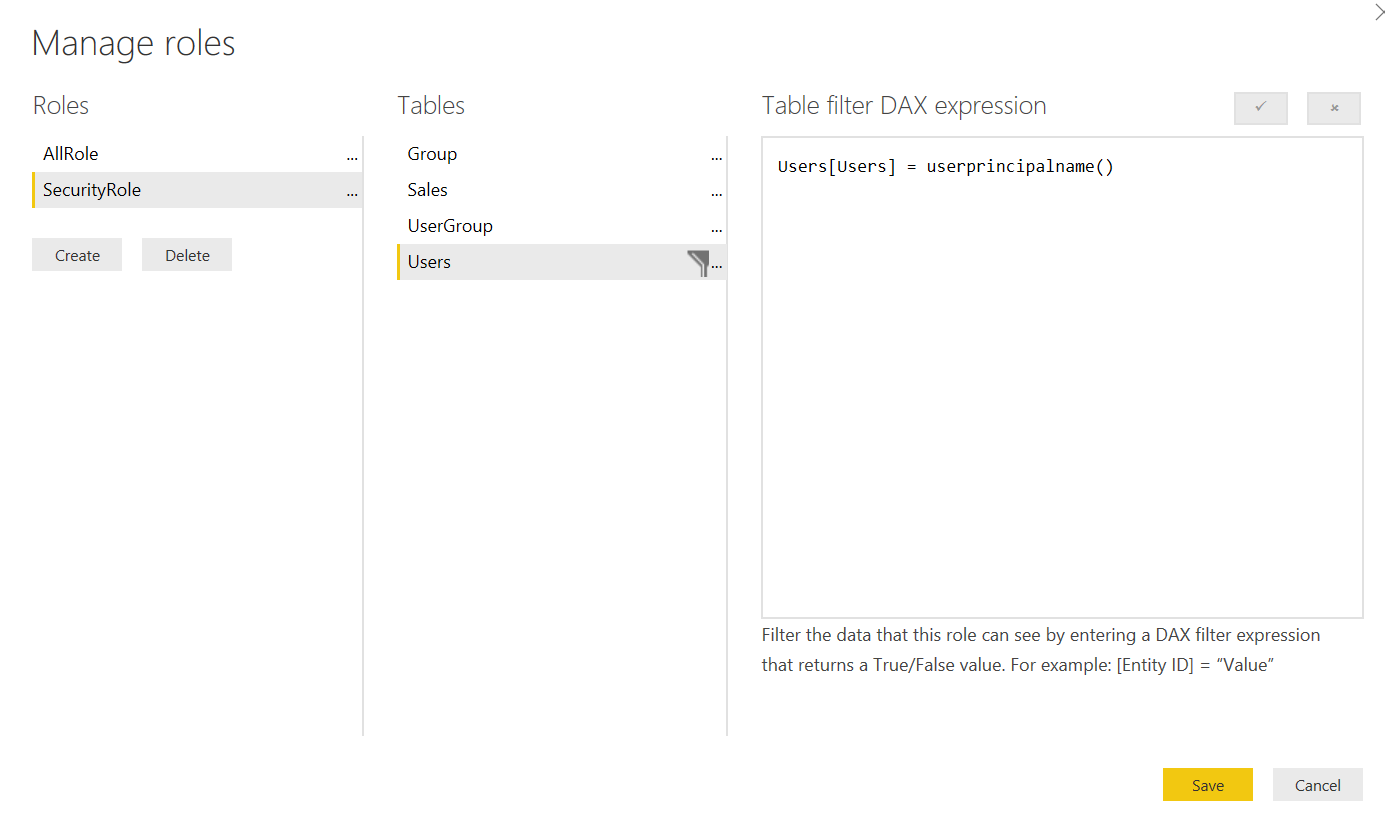
Now this report needs to be shared with two guest users and an internal user - the internal user can see everything, but the guest users can only see the groups they have access to. This means we only must filter the data for the guest users. To filter the data appropriately, Contoso uses the Dynamic RLS pattern as described in the whitepaper and blog post. This means, Contoso adds the usernames to the data itself:



Then, Contoso creates the right data model that will filter the data appropriately with the right relationships:



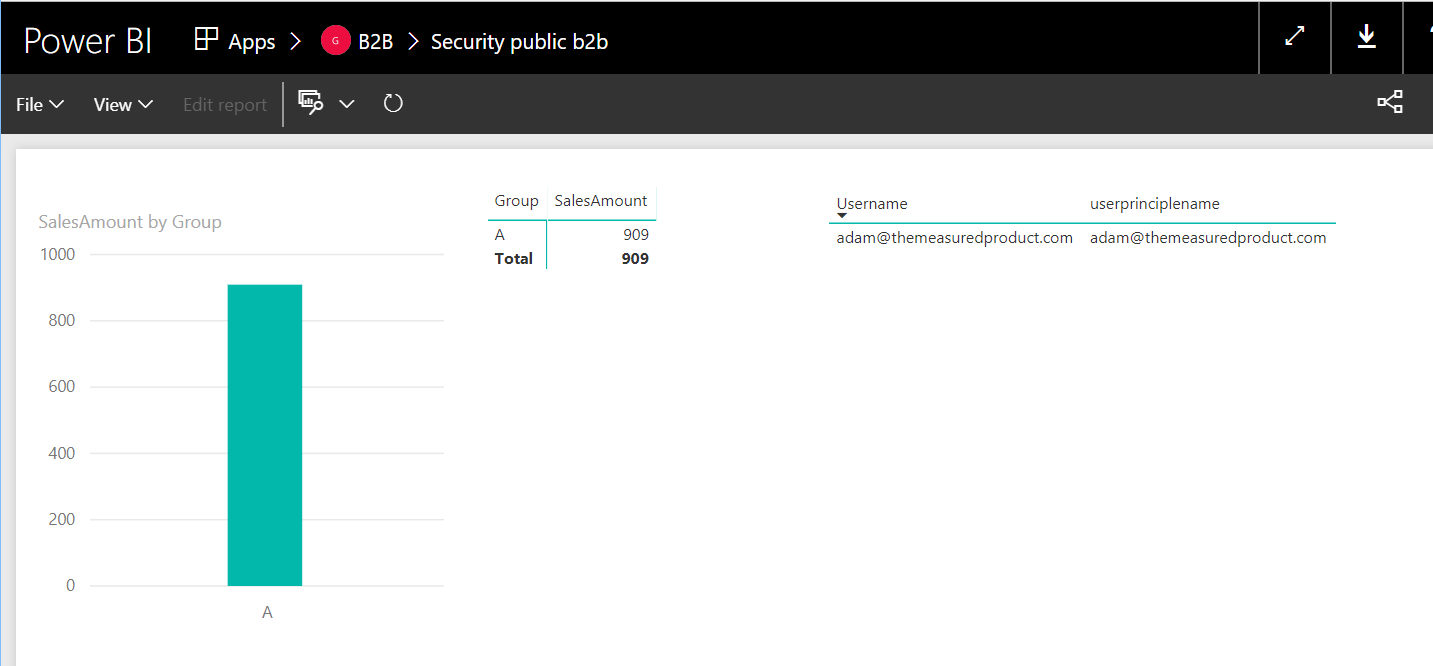
To filter the data automatically based on who is logged in, Contoso needs to create a role that passes in the user who is connecting. In this case, Contoso creates 2 roles – the first is the “securityrole” that filters the Users table with the current username of the user logged in to Power BI (this will work even for AAD B2B guest users).



Contoso also creates another “AllRole” for its internal users who can see everything – this role does not have any security predicate.

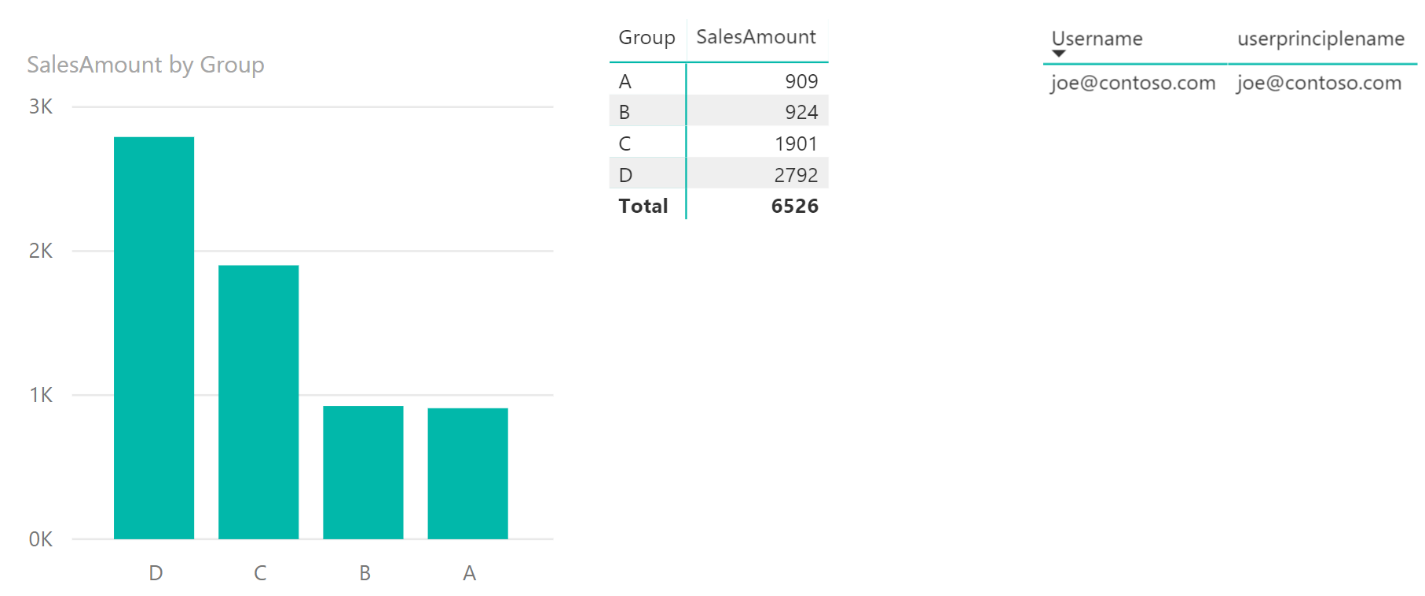
After uploading the Power BI desktop file to the service, Contoso can assign guest users to the “SecurityRole” and internal users to the “AllRole”

Now, when the guest user now opens the report, he only sees sales from group A:



In the matrix to the right you can see the result of the USERNAME() and USERPRINCIPALNAME() function both return the guest users email address.

Now the internal user gets to see all the data:



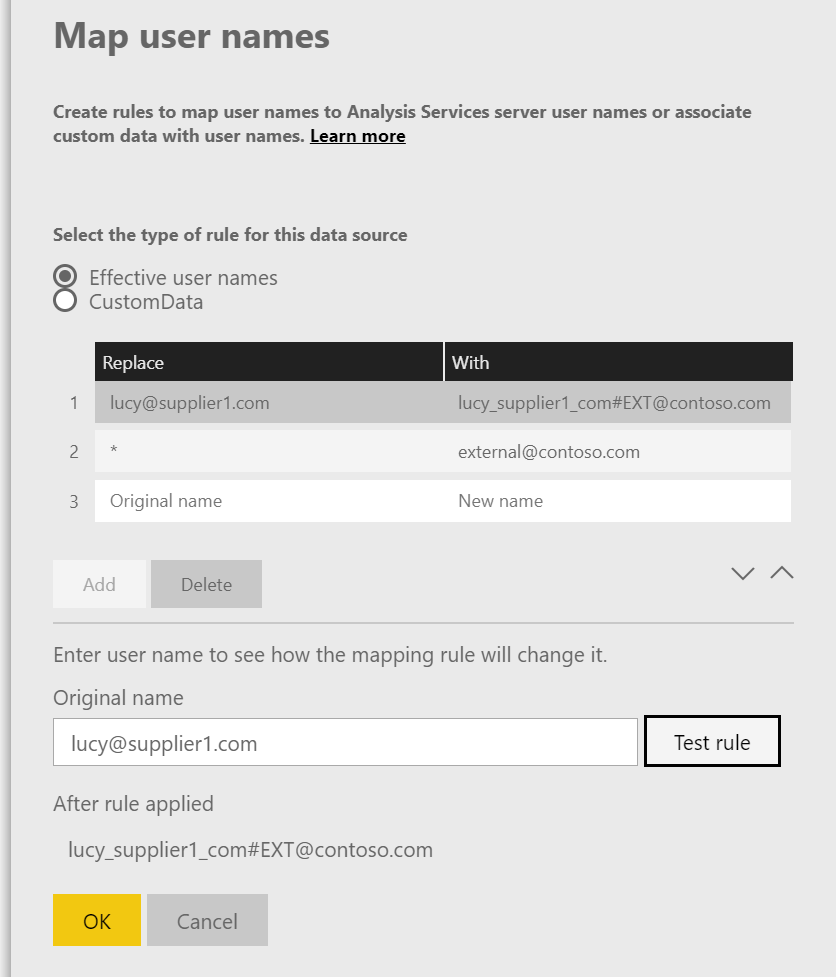
As you can see, Dynamic RLS works with both internal or guest users.

**Note:** This scenario also works when using a model in Azure Analysis Services. Usually your Azure Analysis Service is connected to the same AAD as your Power BI - in that case, Azure Analysis Services will also know the guest users invited through AAD B2B.

# Connecting on premises data sources

Power BI offer the capability for Contoso to leverage on premises data sources like [SQL Server Analysis Services](https://powerbi.microsoft.com/en-us/documentation/powerbi-gateway-enterprise-manage-ssas/) or [SQL Server](https://powerbi.microsoft.com/en-us/documentation/powerbi-gateway-kerberos-for-sso-pbi-to-on-premises-data/) directly thanks to the [On-Premises data gateway](https://powerbi.microsoft.com/en-us/documentation/powerbi-gateway-onprem/). It is even possible to sign on to those data sources with the same credentials as used with Power BI.

For external users, this might be more complicated as the external users are usually not known to the on-premises AD. Power BI offers a workaround for this by allowing Contoso administrators to map the external usernames to internal usernames as described in [Manage your data source - Analysis Services](https://powerbi.microsoft.com/en-us/documentation/powerbi-gateway-enterprise-manage-ssas/). For example [lucy@supplier1.com](mailto:lucy@supplier1.com) can be mapped to [lucy\_supplier1\_com#EXT@contoso.com](mailto:lucy_supplier1_com).



This method is fine if Contoso only has a handful of users or if Contoso can map all the external users to a single internal account. For more complex scenario’s where each user needs their own credentials, there is a more advanced approach that uses [custom AD attributes](https://technet.microsoft.com/en-us/library/cc961737.aspx) to do the mapping as described in [Manage your data source - Analysis Services](https://powerbi.microsoft.com/en-us/documentation/powerbi-gateway-enterprise-manage-ssas/). This would allow the Contoso administrator to define a mapping for every user in your AAD (also external B2B users). These attributes can be set through the AD object model using scripts or code so Contoso can fully automate the mapping on invite or on a scheduled cadence.

# Governance

## Control guest invites

Power BI administrators can control external sharing just for Power BI by visiting the Power BI admin portal. But tenant administrators can also control external sharing with various AAD policies. These policies allow tenant administrators to

* + Turn off invitations by end users
  + Only admins and users in the Guest Inviter role can invite
  + Admins, the Guest Inviter role, and members can invite
  + All users, including guests, can invite

You can read more about these policies in [Delegate invitations for Azure Active Directory B2B collaboration](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-delegate-invitations).

All Power BI actions by external users are also [audited in our auditing portal](https://powerbi.microsoft.com/en-us/documentation/powerbi-admin-auditing/).

## Conditional Access policies for guest users

Contoso can enforce conditional access policies for guest users who access content from the Contoso tenant. You can find detailed instructions in [Conditional access for B2B collaboration users](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-mfa-instructions).

# FAQ

**Can Contoso send an invitation that is automatically redeemed, so that the user is just “ready to go”? Or does the user always have to click through to the redemption URL?**

Invitations that are sent by a user in the inviting organization who is also a member of the partner organization do not require redemption by the B2B user.

We recommend that you invite one user from the partner organization to join the inviting organization. [Add this user to the guest inviter role in the resource organization](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-add-guest-to-role). This user can invite other users in the partner organization by using the sign-in UI, PowerShell scripts, or APIs. Then, B2B collaboration users from that organization aren't required to redeem their invitations.

**Can Contoso force multi-factor authentication for guest users if its partners don't have multi-factor authentication?**

Yes. For more information, see [Conditional access for B2B collaboration users](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-mfa-instructions).

**How does B2B collaboration work when the invited partner is using federation to add their own on-premises authentication?**

If the partner has an Azure AD tenant that is federated to the on-premises authentication infrastructure, on-premises single sign-on (SSO) is automatically achieved. If the partner doesn't have an Azure AD tenant, an Azure AD account is created for new users.

**Can I invite guest users with consumer email accounts?**

Inviting guest users with consumer email accounts is supported in Power BI. This includes domains such as hotmal.com, outlook.com and gmail.com.