

# Configuring Power BI Security



# Agenda

- User Authentication and Identity
  - Power BI Tenant Administration
  - Data Security
  - App Workspaces
  - Row Level Security
  - Dynamic Row Level Security



# Power BI Built on Azure Active Directory

- Azure AD manages identity in Microsoft cloud
  - Organization creates user accounts & groups in Azure AD
  - Users accounts and groups created in scope of tenant
  - Azure AD provides user authentication service
- Azure AD manages licensing and permissions
  - Provides users authorized access to Office 365
  - Provides users authorized access to SharePoint Online
  - Provides users authorized access to Dynamics 365
  - Provides users authorized access to Power BI



# Managing User Accounts and Groups

## Microsoft SaaS Applications

Office 365

Dynamics 365

SharePoint Online

Power BI

Office 365 Admin

Azure Portal

In Tune

## Azure User Account Management

User Accounts

Groups

Applications

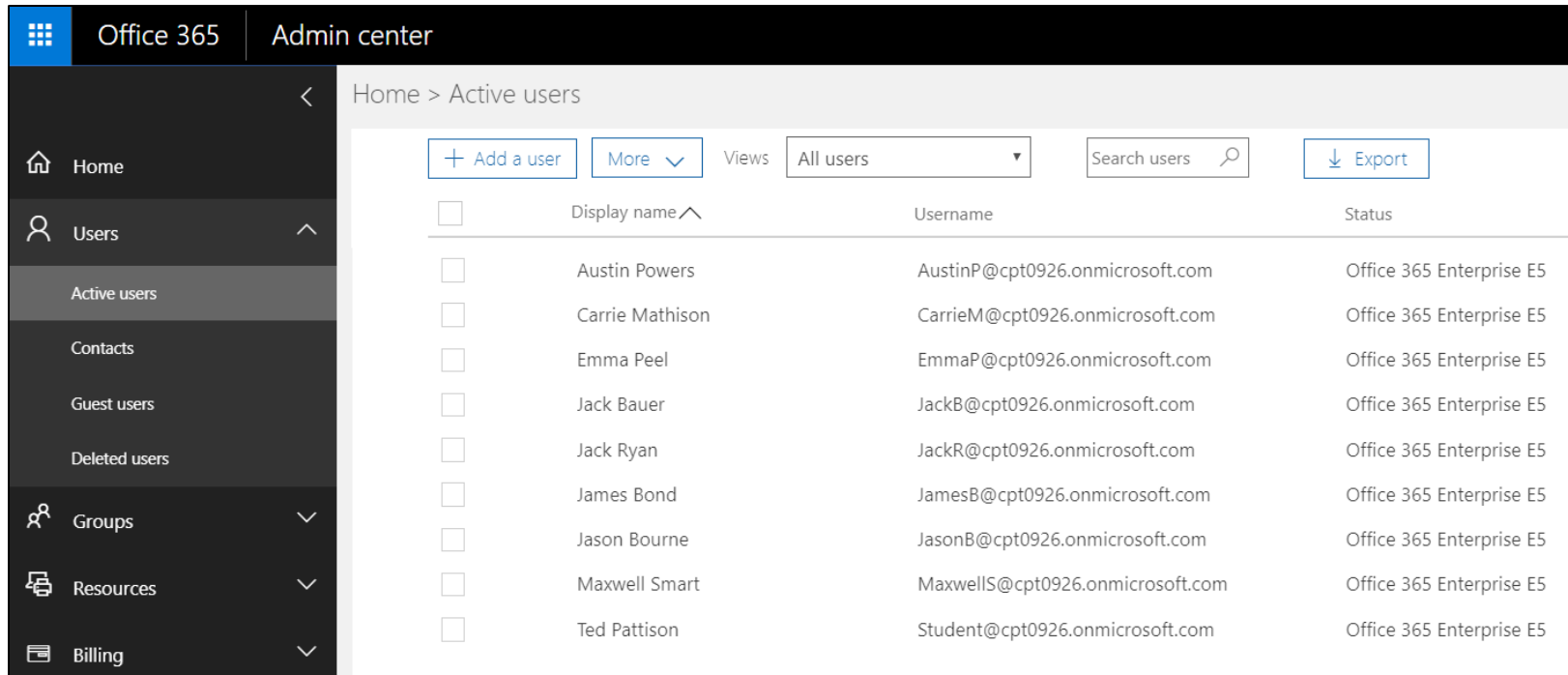
Organizational Tenant (e.g. pbibc.onMicrosoft.com)

## Azure Active Directory



# Azure AD User Accounts and Licensing

- User account created within scope of tenant
  - Office 365 admin create accounts and assigns licenses



The screenshot shows the Office 365 Admin center interface. The left sidebar contains navigation links: Home, Users, Active users (selected), Contacts, Guest users, Deleted users, Groups, Resources, and Billing. The main content area is titled 'Home > Active users'. It includes a '+ Add a user' button, a 'More' dropdown, a 'Views' dropdown set to 'All users', a 'Search users' search bar, and an 'Export' button. Below these controls is a table of active users.

<input type="checkbox"/>	Display name ^	Username	Status
<input type="checkbox"/>	Austin Powers	AustinP@cpt0926.onmicrosoft.com	Office 365 Enterprise E5
<input type="checkbox"/>	Carrie Mathison	CarrieM@cpt0926.onmicrosoft.com	Office 365 Enterprise E5
<input type="checkbox"/>	Emma Peel	EmmaP@cpt0926.onmicrosoft.com	Office 365 Enterprise E5
<input type="checkbox"/>	Jack Bauer	JackB@cpt0926.onmicrosoft.com	Office 365 Enterprise E5
<input type="checkbox"/>	Jack Ryan	JackR@cpt0926.onmicrosoft.com	Office 365 Enterprise E5
<input type="checkbox"/>	James Bond	JamesB@cpt0926.onmicrosoft.com	Office 365 Enterprise E5
<input type="checkbox"/>	Jason Bourne	JasonB@cpt0926.onmicrosoft.com	Office 365 Enterprise E5
<input type="checkbox"/>	Maxwell Smart	MaxwellS@cpt0926.onmicrosoft.com	Office 365 Enterprise E5
<input type="checkbox"/>	Ted Pattison	Student@cpt0926.onmicrosoft.com	Office 365 Enterprise E5



# Multifactor Authentication

- Enabled through admin portal
  - Requires Office 365 or Azure AD Premium

## multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)  
Before you begin, take a look at the [multi-factor auth deployment guide](#).

[bulk update](#)

View: Sign-in allowed users  Multi-Factor Auth status: Any

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Austin Powers	AustinP@cpt0926.onmicrosoft.com	Disabled
<input checked="" type="checkbox"/>	Carrie Mathison	CarrieM@cpt0926.onmicrosoft.com	Disabled
<input type="checkbox"/>	Emma Peel	EmmaP@cpt0926.onmicrosoft.com	Disabled
<input type="checkbox"/>	Jack Bauer	JackB@cpt0926.onmicrosoft.com	Disabled
<input type="checkbox"/>	Jack Ryan	JackR@cpt0926.onmicrosoft.com	Disabled
<input type="checkbox"/>	James Bond	JamesB@cpt0926.onmicrosoft.com	Disabled

### Carrie Mathison

CarrieM@cpt0926.onmicrosoft.com

**quick steps**

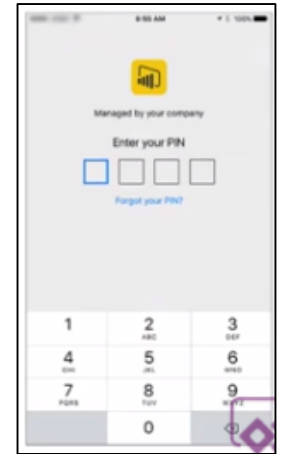
[Enable](#) 

[Manage user settings](#)



# User Access Control for Mobile Devices

- Mobile Device Power BI App Management
  - Controlled via InTune for iPhone (iOS7) and Android
  - Policy can be configured to make users enter PIN
  - Account locked after max number of failed PIN logins
- Configuring the Power BI app with InTune
  1. Specify the Power BI app as the app to configure
  2. Configure policies (e.g. require PIN)
  3. Enable for deployment
  4. Users install Power BI app from company portal



# Conditional Access for Web and Mobile

- Azure AD supports configuring conditional access
  - Control which IP address ranges can connect (Corp LAN)
  - Control which devices can connect
  - Configure access so only group members can connect
  - Configure which users or IP address ranges require 2FA
  - Lots more is possible





# Azure AD Group Types

- Azure AD Group Types
  - Security Groups
  - Mail-enabled Security Groups
  - Office 365 Groups

Home > Groups Power BI Bootcamp Labs

[+ Add a group](#) [More ▾](#) View All supported groups ▾

[Not seeing new items listed? Go to the Exchange admin](#)

<input type="checkbox"/>	Group name	Email	Type	Status
<input type="checkbox"/>	Central Sales Reps		Security group	In cloud
<input type="checkbox"/>	Eastern Sales Reps		Security group	In cloud
<input type="checkbox"/>	Western Sales Reps		Security group	In cloud
<input type="checkbox"/>	Wingtip Sales Analysis	wingtipsalesanalysis@cpt0926.onm...	Office 365 group	In cloud
<input type="checkbox"/>	Wingtip Sales Dynamic RLS	wingtipsalesdynamicrls@cpt0926.o...	Office 365 group	In cloud
<input type="checkbox"/>	Wingtip Sales Reps	wingtipsalesreps@cpt0926.onmicro...	Mail-enabled security group	In cloud



# Office 365 Groups

The screenshot displays the Microsoft Office 365 Groups interface within the Outlook application. The top navigation bar shows 'Office 365' and 'Outlook'. The left sidebar contains a 'New' button, a search bar for 'Wingtip Sales Analysis', and a 'Groups' section with a 'New' button and a list of groups: 'Wingtip Sales Dynamic RLS' and 'Wingtip Sales Analysis'. The main content area shows the 'Wingtip Sales Analysis' group, which is a private group with 9 members. The group's header includes a red 'WS' icon, the group name, and tabs for 'Conversations', 'Files', 'Calendar', and 'Notebook'. The members are listed in a grid, including Austin Powers, Carrie Mathison, Emma Peel, Jack Bauer, James Bond, Jack Ryan, Jason Bourne, Maxwell Smart, and Ted Pattison. The interface also shows a 'Sort by Display name' option and a 'Joined' status.



# Agenda

- ✓ User Authentication and Identity
- Power BI Tenant Administration
  - Data Security
  - App Workspaces
  - Row Level Security
  - Dynamic Row Level Security



# Power BI Admin Portal

- Power BI Admins control tenant-level settings
  - Control whether users can self-register for Power BI
  - Control who can publish to web
  - Control who can export & share content
  - Control who can create content packs



A screenshot showing the 'Admin portal' page and a settings dialog. The 'Admin portal' page has a left sidebar with 'Tenant settings' selected. The main content area shows 'Export and sharing settings' with a list of options: 'Share content with external users', 'Publish to web', 'Export data', 'Export reports as PowerPoint presentations', and 'Print dashboards and reports'. A red arrow points from 'Export data' to a settings dialog. The dialog is titled 'Export data' and shows 'Unapplied changes'. It has a toggle switch for 'Enabled' which is turned on. Below the toggle, it says 'Apply to:' with two radio buttons: 'The entire organization' and 'Specific security groups'. The 'Specific security groups' option is selected. There is a text input field containing 'Wingtip Sales Reps' and a placeholder 'Enter security groups'. At the bottom, there are 'Apply' and 'Cancel' buttons.



# Power BI Audit Log

## Admin portal

Usage Metrics

Users

Audit logs

Tenant settings

Capacity settings

### Audit and usage settings

- ▶ Create audit logs for internal activity auditing and compliance  
*Enabled for the entire organization*
- ▶ Usage metrics for content creators  
*Enabled for the entire organization*
- ▶ Per-user data in usage metrics for content creators  
*Enabled for the entire organization*

Home > Audit log search

## Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have done. Search for activities such as permissions, directory services, and much more. [Learn more about searching the audit log](#)

### Search

↺ Clear

Activities

Viewed Power BI report ▼

Start date

2017-10-04



00:00 ▼

End date

2017-10-12



00:00 ▼

### Results 5 results found

Date ▼	IP address	User	Activity
2017-10-04 12:00:02	10.0.0.83	<a href="#">JamesB@cpt0926.onmicrosoft.c...</a>	Viewed Power BI report
2017-10-04 11:52:42	10.0.0.83	<a href="#">JamesB@cpt0926.onmicrosoft.c...</a>	Viewed Power BI report
2017-10-04 11:52:17	10.0.0.81	<a href="#">JamesB@cpt0926.onmicrosoft.c...</a>	Viewed Power BI report
2017-10-04 10:32:03	10.0.0.79	<a href="#">JamesB@cpt0926.onmicrosoft.c...</a>	Viewed Power BI report



# Data Classification for Dashboards

## Admin portal

Usage Metrics

Users

Audit logs

Tenant settings

Capacity settings

### Audit and usage settings

- ▶ Create audit logs for internal activity auditing and compliance  
*Enabled for the entire organization*
- ▶ Usage metrics for content creators  
*Enabled for the entire organization*
- ▶ Per-user data in usage metrics for content creators  
*Enabled for the entire organization*

## Dashboard settings

- ◀ Data classification for dashboards  
*Enabled for the entire organization*

Users in the organization can tag dashboards with classifications indicating dashboard security levels.

☒ Enabled

DEFAULT	CLASSIFICATION	SHORTHAND	SHOW TAG	URL	
<input checked="" type="radio"/>	<input type="text" value="Top Secret"/>	<input type="text" value="ts"/>	<input checked="" type="checkbox"/>	<input type="text"/>	
<input type="radio"/>	<input type="text" value="Confidential"/>	<input type="text" value="c"/>	<input checked="" type="checkbox"/>	<input type="text"/>	
<a href="#">+ Add classification</a>					



# Agenda

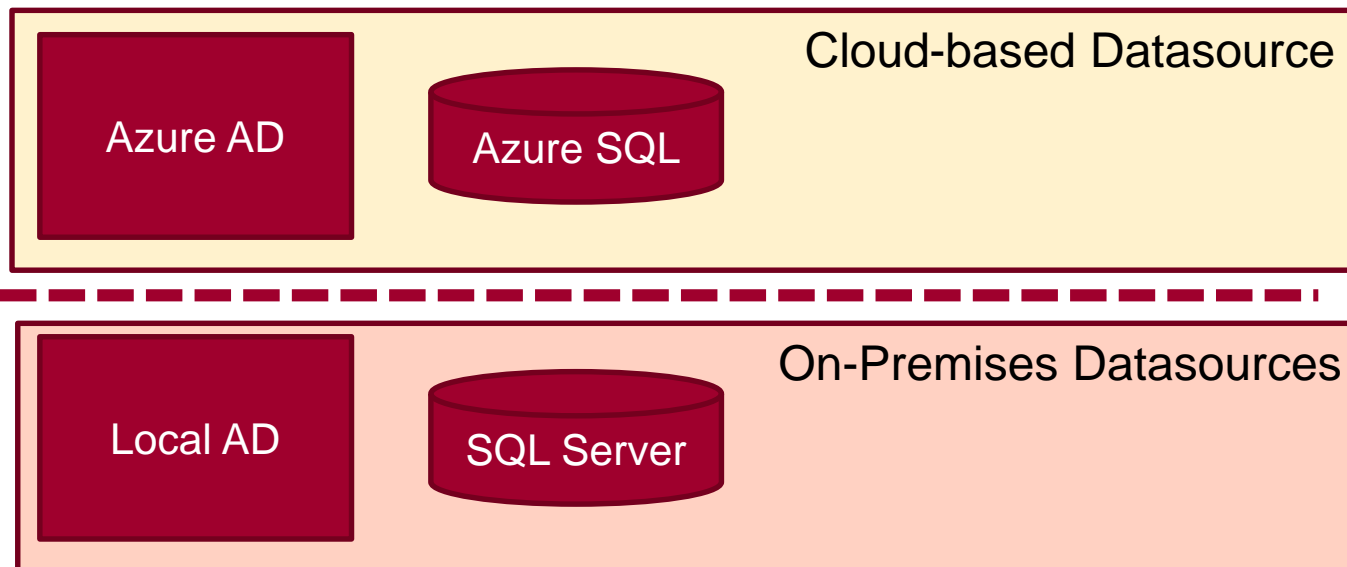
- ✓ User Authentication and Identity
- ✓ Power BI Tenant Administration
- Data Security
  - App Workspaces
  - Row Level Security
  - Dynamic Row Level Security





# Types of Data

- Imported Data (aka ETL Data)
  - Data cached in Power BI and refreshed using saved credentials
- Live Connection or Direct Query
  - Data pulled into Power BI at query time using saved credentials
- Pushed Data
  - Data pushed into Power BI by external application



# Data Is Always in One of Three States

- Data can be ***In Transit***
  - Moving between data source, Power BI and client
  - Data is always encrypted using HTTPS or Azure Service Bus
- Data can be ***In Process***
  - Data loaded into cloud-based memory
- Data can be ***At Rest***
  - Data stored in cloud-based storage
  - Data encrypted using internally managed encryption keys



# Storage of Data At Rest

- What types of data must be stored at rest?
  - Data (i.e. Dataset)
  - Credentials
  - Metadata for report and dashboard layouts

Data source	Data	Metadata	Credentials
Imported Data	Azure Blob Storage	Azure Blob Storage	Azure SQL
Direct Query	Nothing	Azure Blob Storage	Azure SQL
Live Connection	Nothing	Azure Blob Storage	Azure SQL
Push Dataset	Azure SQL	Azure Blob Storage	N/A



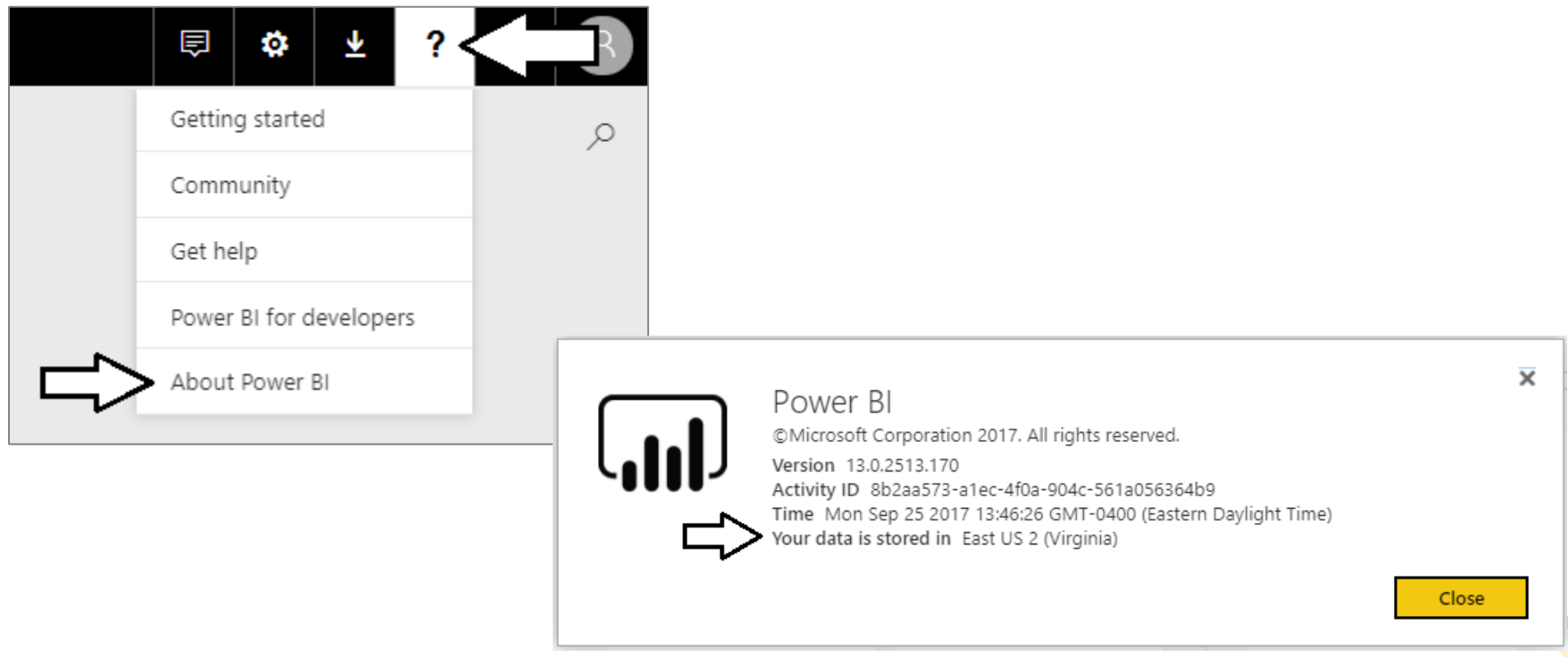
# Data Encryption

- Power BI uses encryption keys for blob storage
  - Keys stored in separate location from Power BI service
  - Fully managed by internal Microsoft service
- Azure SQL manages encryption internally
  - Power BI relies on Azure SQL TDE Technology
  - Used to encrypt credentials to cloud-based sources
- For credentials to access on-premises sources
  - Encryption key created in on-premises data gateway
  - Encryption key used to encrypt creds stored in cloud



# Data Storage Location

- Data storage location can be important
  - Especially with European rules and regulations
- Organization has tenant in specific data center



# Data Residency and Azure Region Pairs

- Data stored in specific Azure Region
  - Azure region defined data residency
  - Within a region, data centers are paired

Geography	Paired regions	
North America	North Central US	South Central US
North America	East US	West US
North America	US East 2	US Central
North America	West US 2	West Central US
Europe	North Europe	West Europe
Asia	South East Asia	East Asia
China	East China	North China
Japan	Japan East	Japan West
Brazil	Brazil South (1)	South Central US
Australia	Australia East	Australia Southeast
US Government	US Gov Iowa	US Gov Virginia
India	Central India	South India
Canada	Canada Central	Canada East
UK	UK West	UK South



# Connecting Through Express Route

- Allows you to create private network connection
  - Connect to Power BI without going through public Internet
  - Can also connect through ISP's colocation facility
  - Azure Express route with Power BI uses public peering





# Compliance and Market Availability

## COMPLIANCE

## AVAILABILITY

ISO/IEC 27001: 2013	✓
ISO/IEC 27018:2014	✓
HIPAA BAA	✓
EU Model Clause	✓
Data Processing Terms	✓
PCI Security Standards Council	✓
CSA STAR Certification	✓
G-Cloud (UK)	✓
Section 508 VPATs	✓
SOC 1 & SOC 2 (SSAE 16)	Coming soon
Sarbanes-Oxley	Coming soon
FedRAMP High (in Azure government environment)	✓

## REGIONS DATA LOCATIONS

## AVAILABILITY

Asia Pacific	✓
Australia	✓
Brazil	✓
Canada	✓
Europe	✓
India	✓
Japan	✓
United Kingdom	✓
United States	✓

## NATIONAL CLOUDS

## AVAILABILITY

US Government	✓
China	✓
Germany	✓



# Agenda

- ✓ User Authentication and Identity
- ✓ Power BI Tenant Administration
- ✓ Data Security
- App Workspaces
  - Row Level Security
  - Dynamic Row Level Security



# What Exactly is an App Workspace?

- App Workspace is Power BI resource container
  - Provides storage for datasets, reports and dashboards
- App Workspace created as Office 365 Group
  - Acts as both a security group and distribution list
  - Requires provisioning SharePoint team site
- On the Power BI Roadmap
  - Creating workspace without SharePoint provisioning




# Creating an App Workspace

## Create an app workspace

Name your workspace

Workspace ID



 Available

Private - Only approved members can see what's inside

Members can only view Power BI content

Add workspace members

Add

maxwells@cpt0926.onmicrosoft.com	Admin	▼	
austinp@cpt0926.onmicrosoft.com	Member	▼	

Public - Anyone can see what's inside

Private - Only approved members can see what's inside

Members can edit Power BI content

Members can only view Power BI content



# Old Distribution Model



# New Distribution Model



# Agenda

- ✓ User Authentication and Identity
- ✓ Power BI Tenant Administration
- ✓ Data Security
- ✓ App Workspaces
- Row Level Security
  - Dynamic Row Level Security





# What Is Row-level Security (RLS)

- Security Scheme based on Named Roles
  - Roles are defined using Power BI Desktop
  - Each role is scoped to the dataset within a PBIX project
- Role defined using one or more DAX expressions
  - DAX expressions restrict which rows are accessible



# Common RLS Scenario



# Configuring RLS in the Power BI Desktop

## Manage roles

Roles

All Sales Regions

Central Sales Region

Eastern Sales Region

Western Sales Region

Create

Delete

Tables

Calendar

Customers

Products

Purchases

Sales

SalesRegions

Table filter DAX expression

[Sales Region] = "Western Region"

Filter the data that this role can see by entering a DAX filter expression that returns a True/False value. For example: [Entity ID] = "Value"

Save

Cancel



# Configuring RLS in the Power BI Service

W

Western Sales Reps  
Security group

↺

✕

[Change](#) [Delete group](#)

Name	Western Sales Reps	<a href="#">Edit</a>
Description		
Owners (2)	Maxwell Smart Ted Pattison	<a href="#">Edit</a>
Members (2)	Jack Ryan Jason Bourne	<a href="#">Edit</a>

Close

Power BI

WS Wingtip Sales Analysis > Row-Level Security

≡

☆ Favorites >

🕒 Recent >

🗑 Apps

👤 Shared with me

📁 Workspaces >

WS Wingtip Sales An... ^

Row-Level Security

All Sales Regions (0)

Central Sales Region (1)

Eastern Sales Region (1)

Western Sales Region (1)

Members (1)

People or groups who belong to this role

Add

Western Sales Reps ✕



# RLS Enforcement







**DEMO**

## **Configuring Row-level Security**

# Agenda

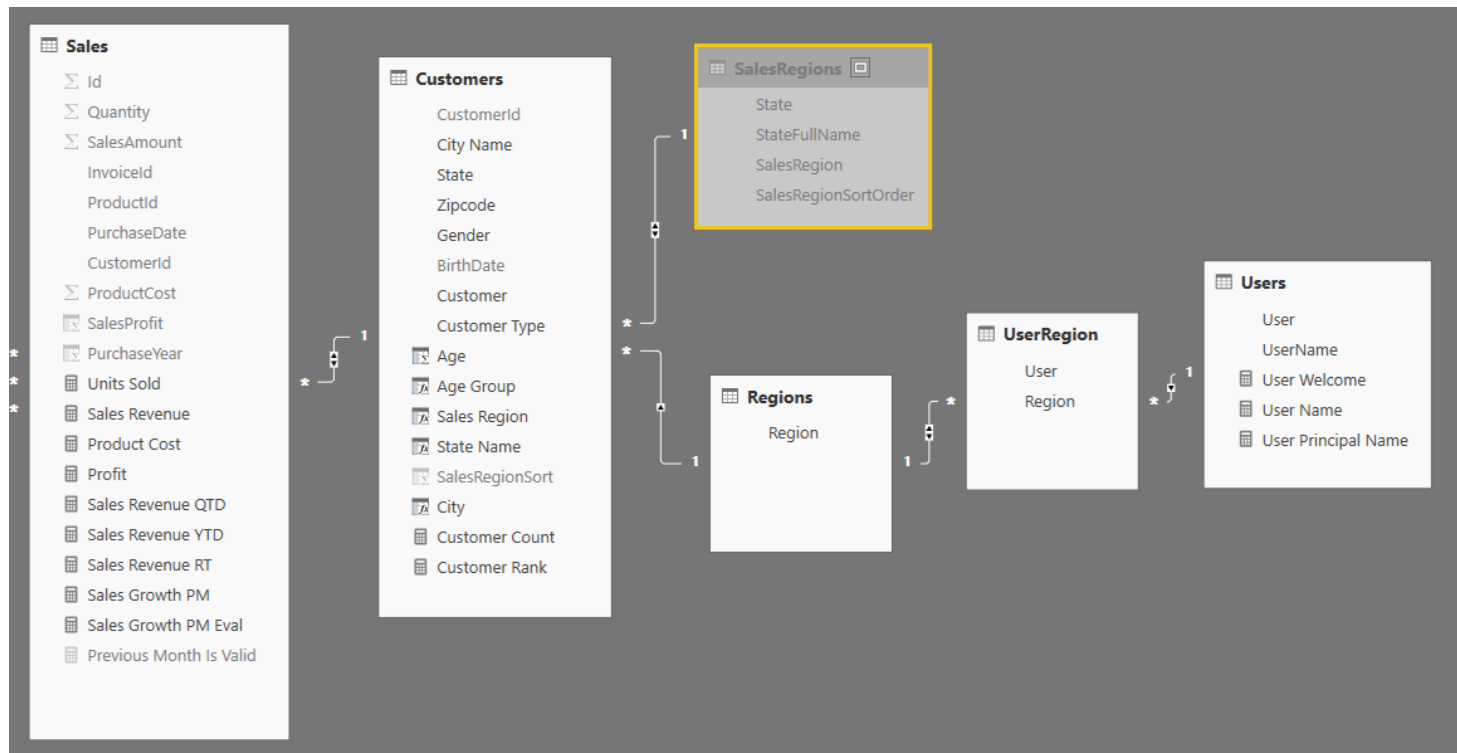
- ✓ User Authentication and Identity
- ✓ Power BI Tenant Administration
- ✓ Data Security
- ✓ App Workspaces
- ✓ Row Level Security
- Dynamic Row Level Security





# Dynamic RLS

- Design pattern for data-driven security
  - RLS set up to use login name of current user
  - Permission assignments are included as part of dataset
  - Implemented using bi-directional cross-filtering



# Configuring Cross-direction Filtering

The diagram illustrates the database schema and the configuration for cross-direction filtering on the UserRegion relationship.

**Database Schema:**

- Customers** (1) is related to **Regions** (\*) via BirthDate, Customer, and Customer Type.
- Regions** (1) is related to **UserRegion** (\*) via Region.
- UserRegion** (\*) is related to **Users** (1) via User and Region.

**UserRegion Relationship Configuration:**

**UserRegion**

User	Region
EmmaP@cpt0926.onmicrosoft.com	Central Region
JackB@cpt0926.onmicrosoft.com	Central Region
MaxwellS@cpt0926.onmicrosoft.com	Central Region

**Regions**

Region
Western Region
Central Region
Eastern Region

**Cardinality:** Many to one (\*:1)

**Cross filter direction:** Both

☒ Make this relationship active

☐ Assume referential integrity

☒ Apply security filter in both directions

OK Cancel

# Dynamically Tracking the Current User

## Manage roles

### Roles

Dynamic RLS Role ...

CreateDelete

### Tables

Calendar ...

Customers ...

Products ...

Purchases ...

Regions ...

Sales ...

SalesRegions ...

UserRegion ...

Users ...

### Table filter DAX expression

✓✕

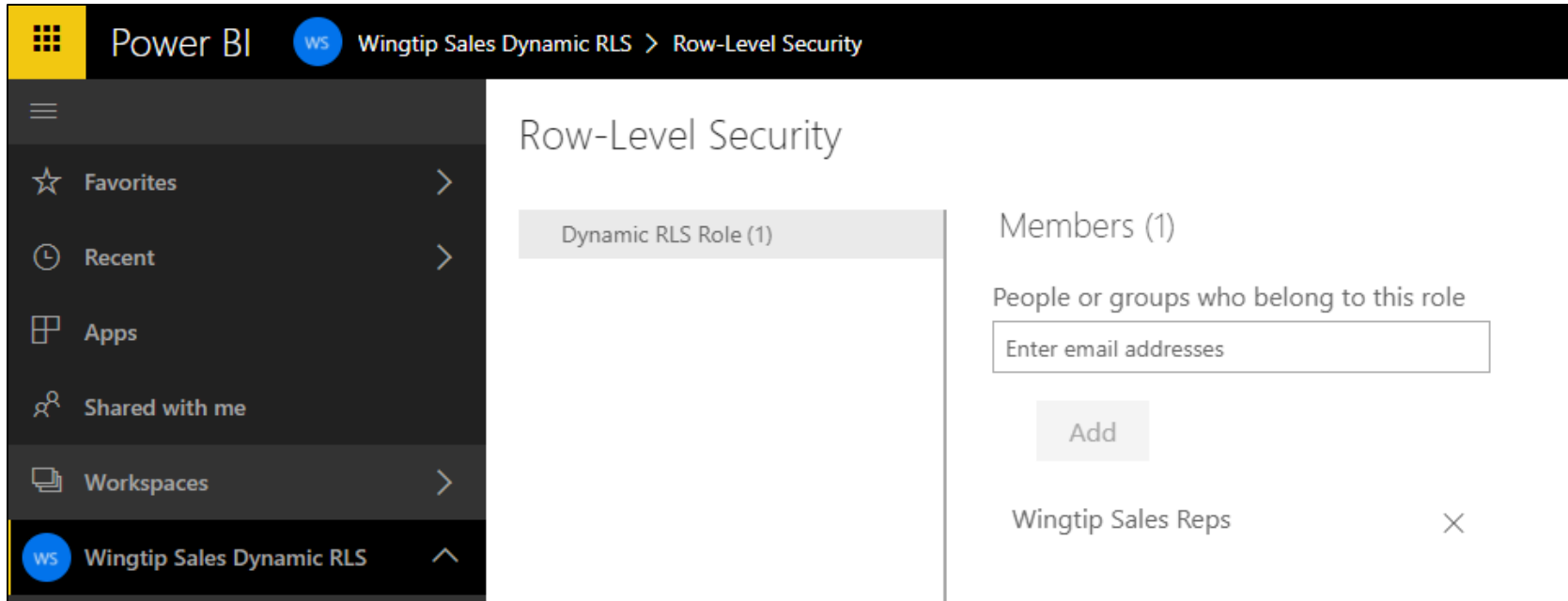
[User]=Username()

Filter the data that this role can see by entering a DAX filter expression that returns a True/False value. For example: [Entity ID] = "Value"

SaveCancel



# All Users Must Be Added To a Role



The screenshot shows the Power BI interface for configuring Row-Level Security (RLS). The top navigation bar includes the Power BI logo, a workspace icon labeled 'ws', and the breadcrumb 'Wingtip Sales Dynamic RLS > Row-Level Security'. The left sidebar contains navigation options: Favorites, Recent, Apps, Shared with me, Workspaces, and the active workspace 'Wingtip Sales Dynamic RLS'. The main content area is titled 'Row-Level Security' and is divided into two panels. The left panel, 'Dynamic RLS Role (1)', is currently empty. The right panel, 'Members (1)', shows the list of users assigned to the role. It includes a text input field labeled 'Enter email addresses' and an 'Add' button. Below the input field, the user 'Wingtip Sales Reps' is listed with a close icon (X) to its right.

Power BI ws Wingtip Sales Dynamic RLS > Row-Level Security

Row-Level Security

Dynamic RLS Role (1)

Members (1)

People or groups who belong to this role

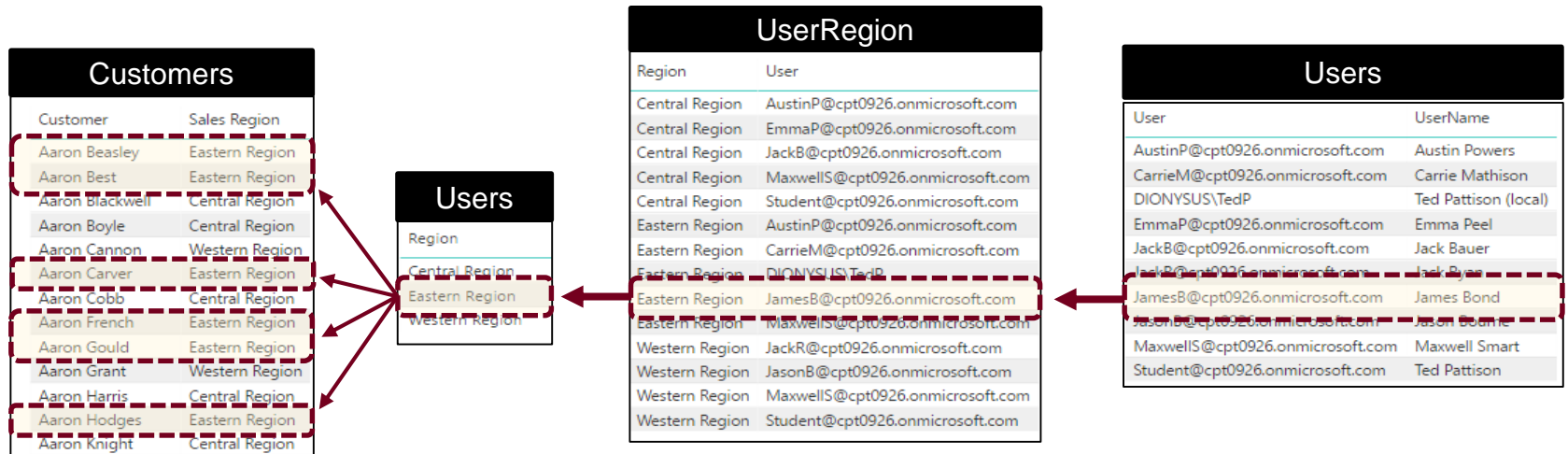
Enter email addresses

Add

Wingtip Sales Reps X



# Dynamic RLS Table Filtering



# Dynamic RLS Enforcement







**DEMO**

# Configuring Dynamic Row-level Security

# Summary

- ✓ User Authentication and Identity
- ✓ Power BI Tenant Administration
- ✓ Data Security
- ✓ App Workspaces
- ✓ Row Level Security
- ✓ Dynamic Row Level Security

