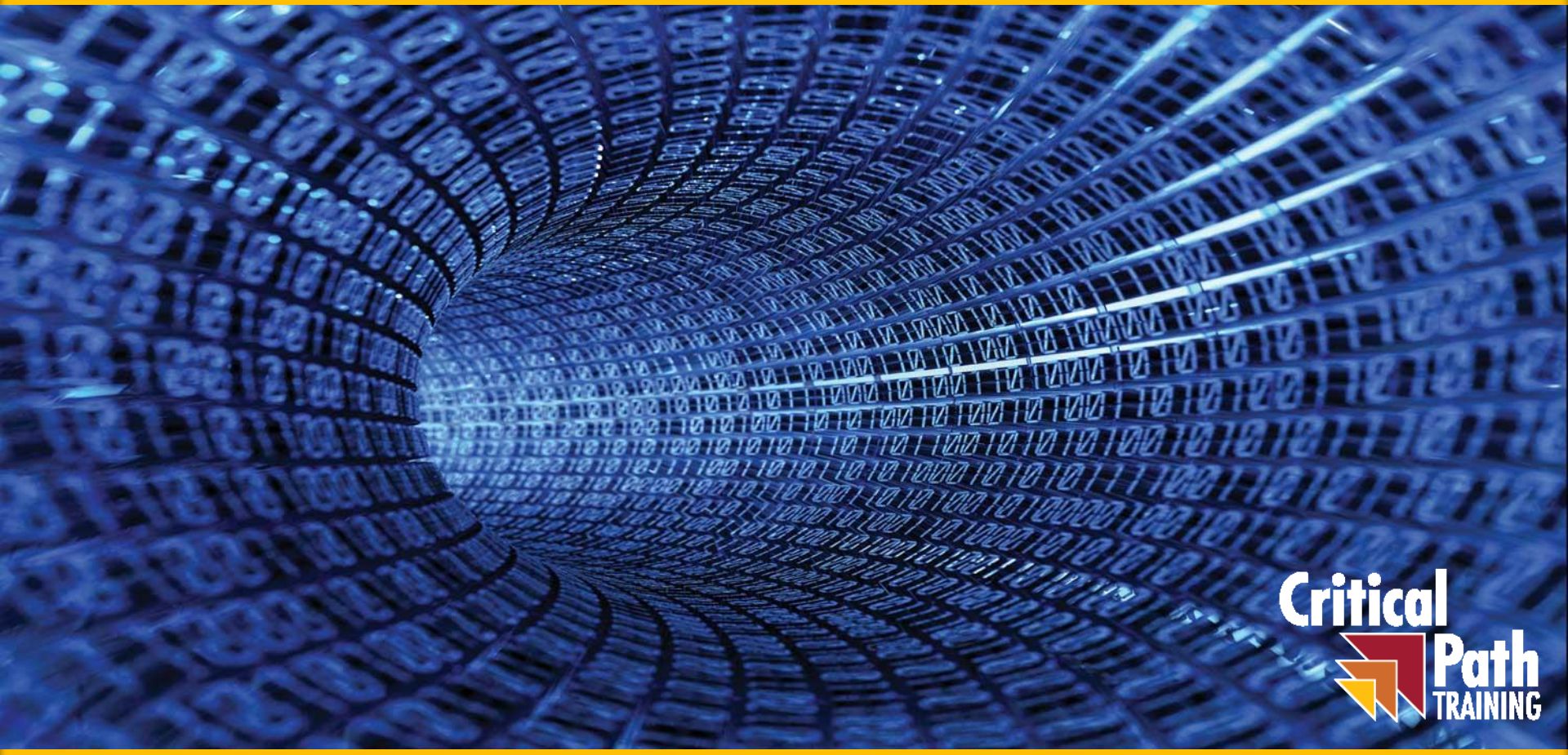
Configuring Power BI Security



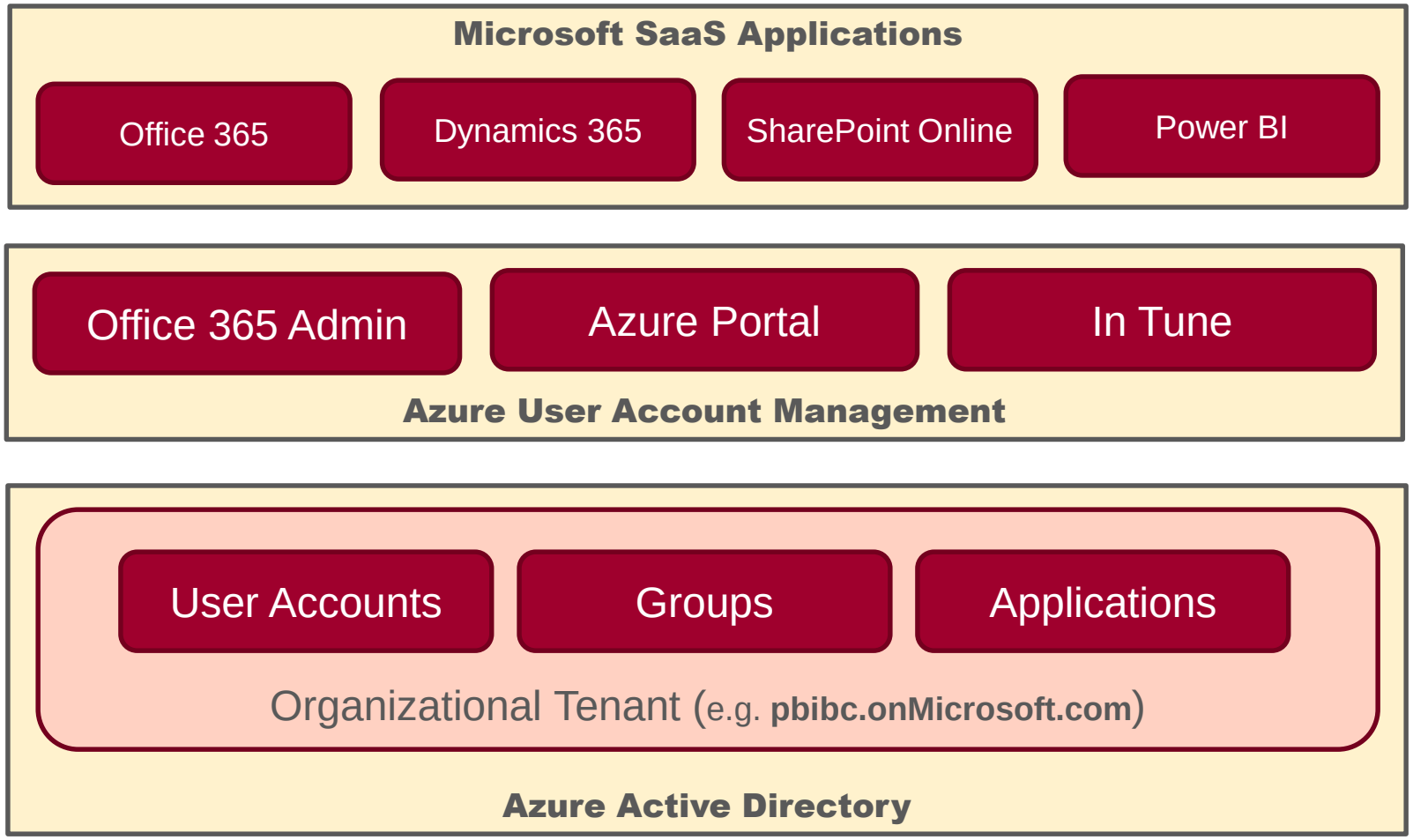
Agenda

- 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

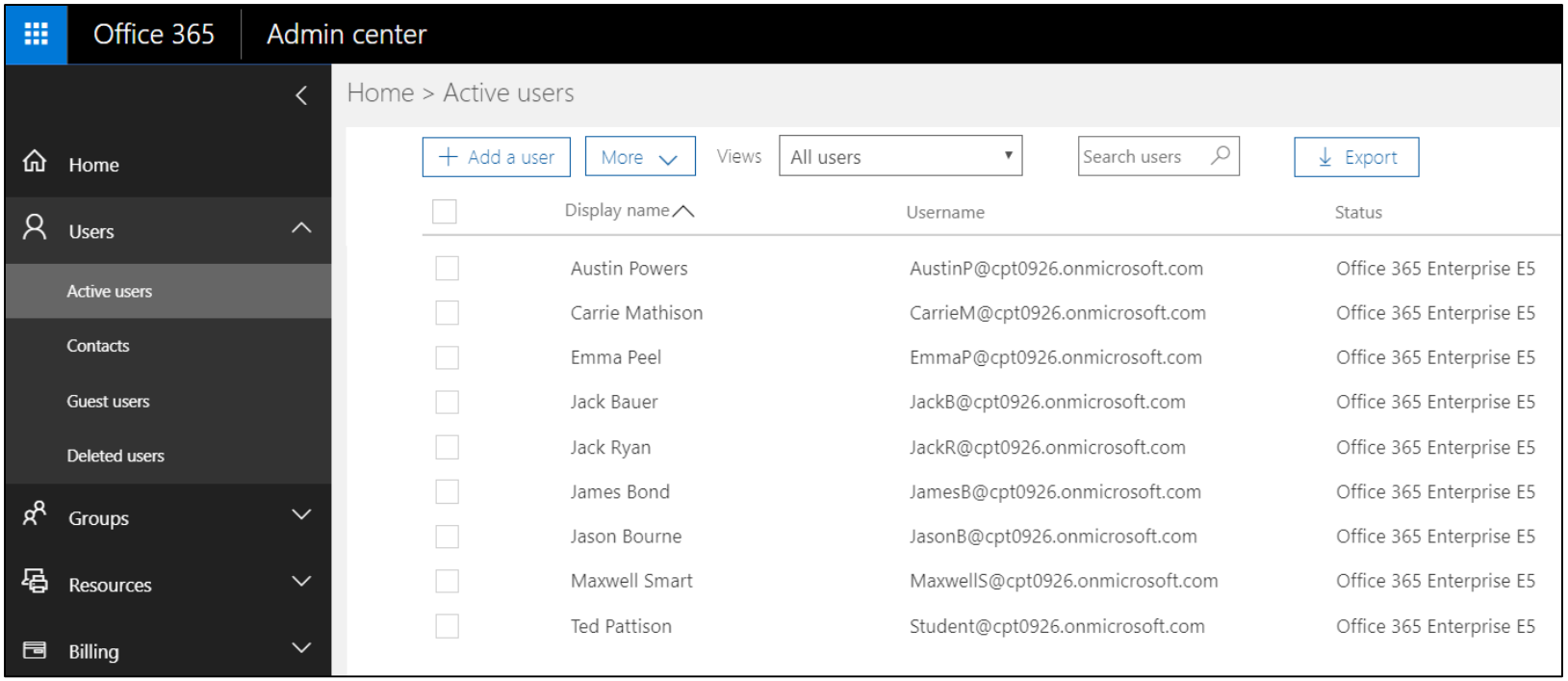
- Azure AD manages identity in Microsoft cloud
  - Organization creates user accounts & groups in Azure AD
  - Users accounts and groups created in scope of tenant
  - Azure AD provides user authentication service
- Azure AD manages licensing and permissions
  - Provides users authorized access to Office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



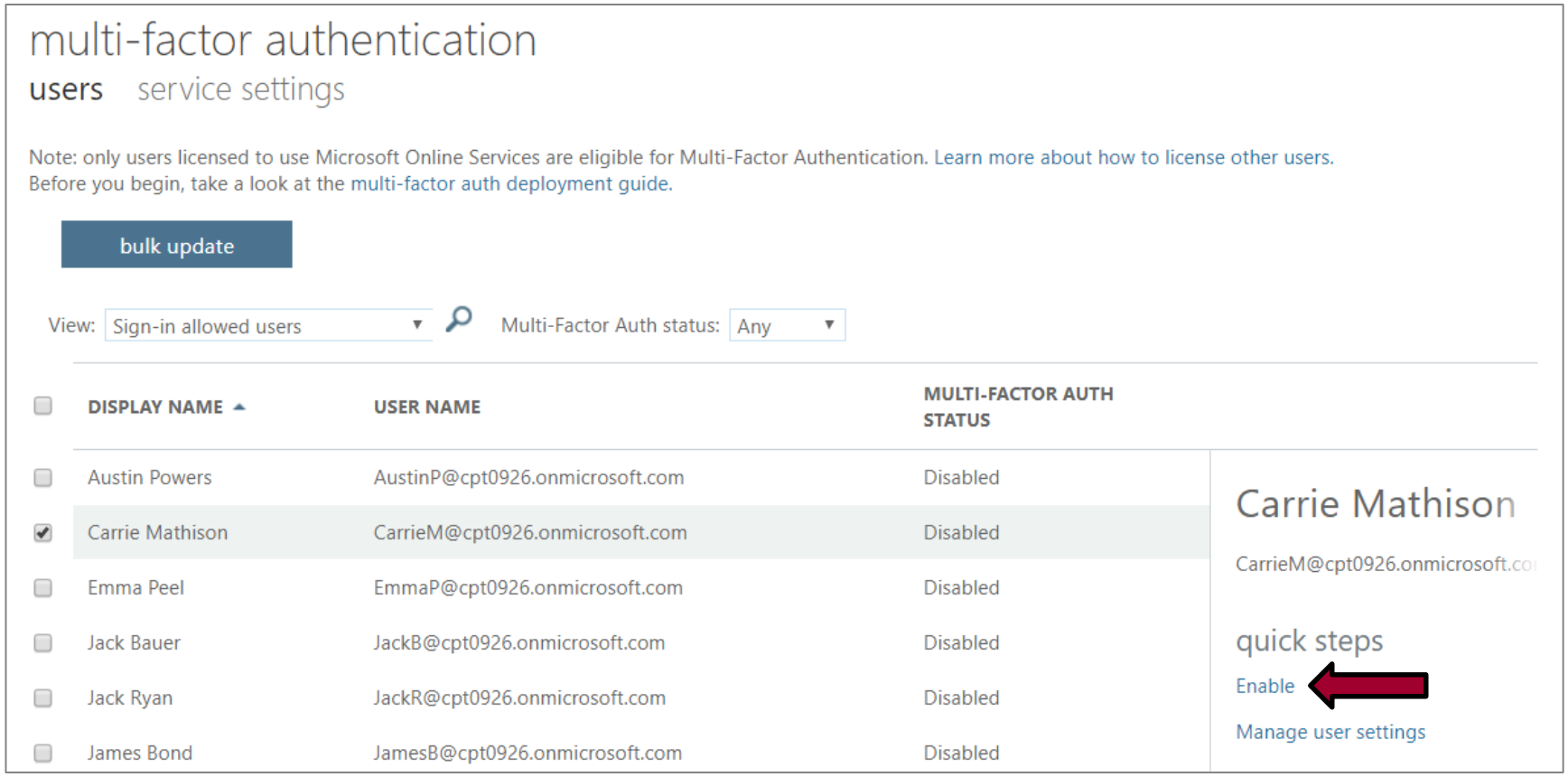
Azure AD User Accounts and Licensing

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



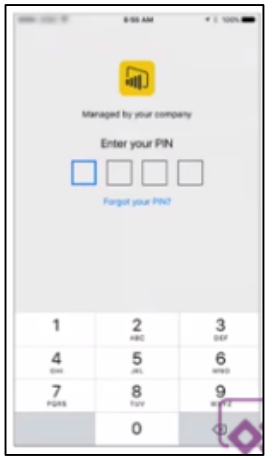
Multifactor Authentication

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



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



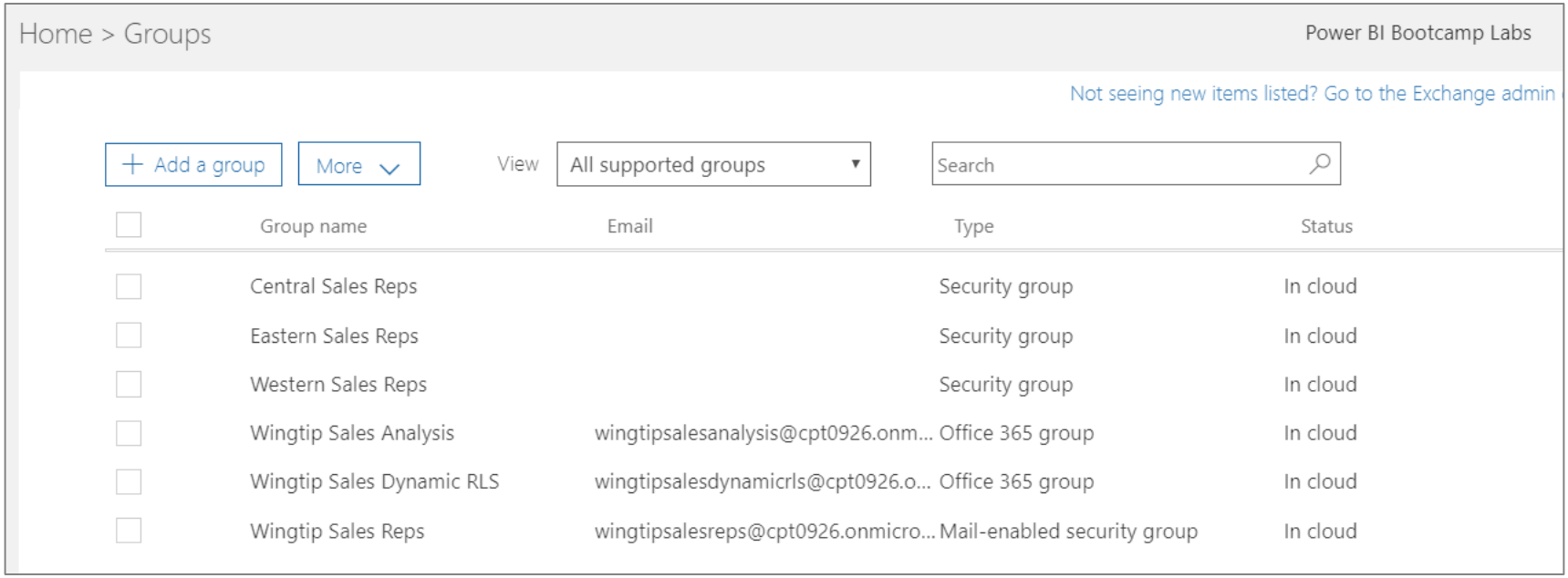
- Configuring the Power BI app with InTune
  1. Specify the Power BI app as the app to configure
  2. Configure policies (e.g. require PIN)
  3. Enable for deployment
  4. Users install Power BI app from company portal

Conditional Access for Web and Mobile

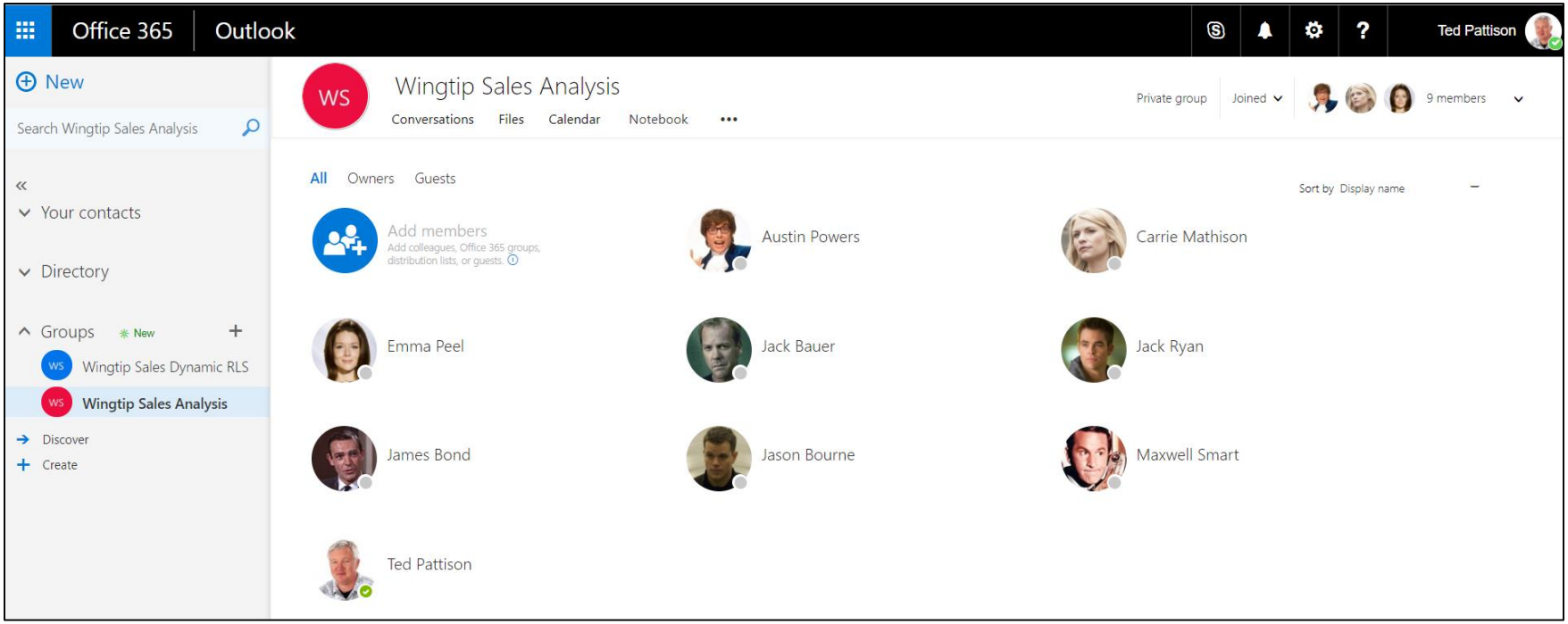
- Azure AD supports configuring conditional access
  - Control which IP address ranges can connect (Corp LAN)
  - Control which devices can connect
  - Configure access so only group members can connect
  - Configure which users or IP address ranges require 2FA
  - Lots more is possible

Azure AD Group Types

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



Office 365 Groups

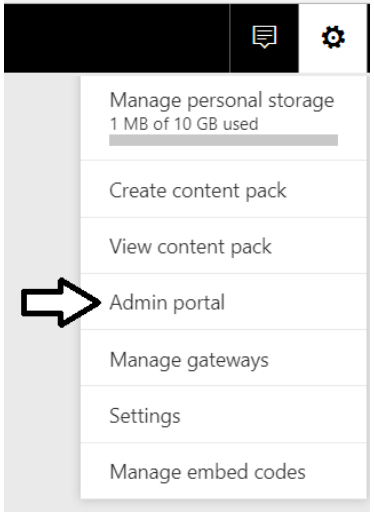


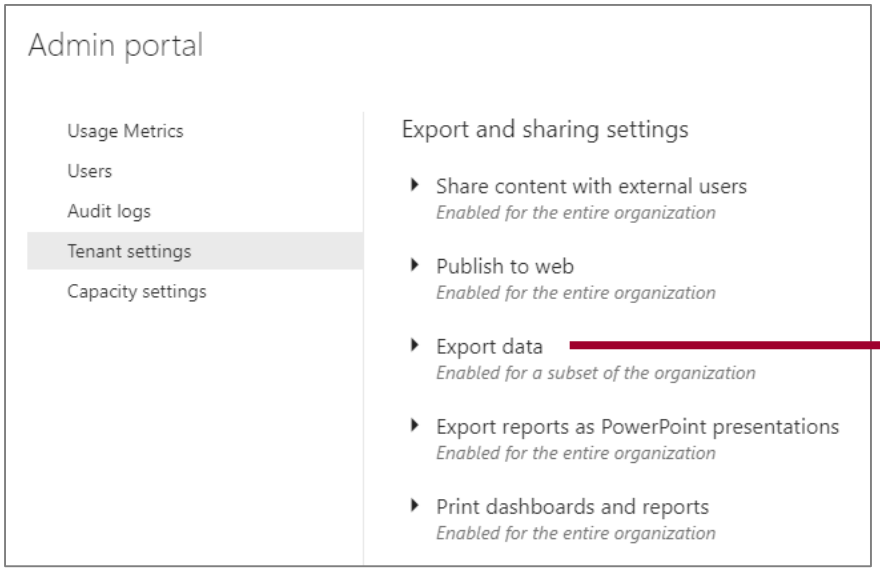
Agenda

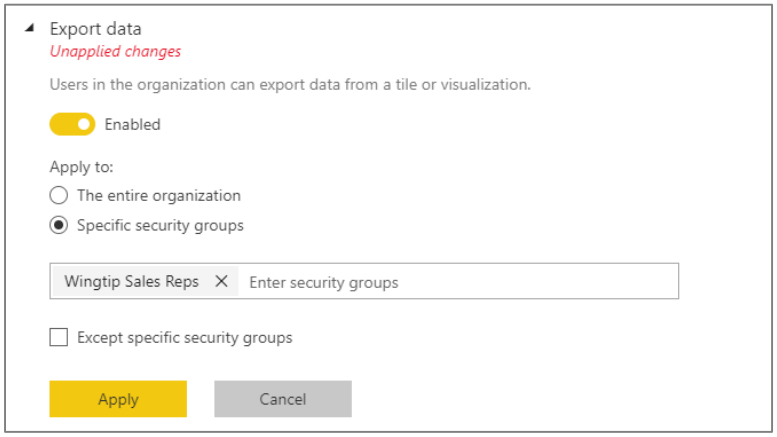
- ✓ User Authentication and Identity
- ➢ Power BI Tenant Administration
- Data Security
- App Workspaces
- Row Level Security
- Dynamic Row Level Security

Power BI Admin Portal

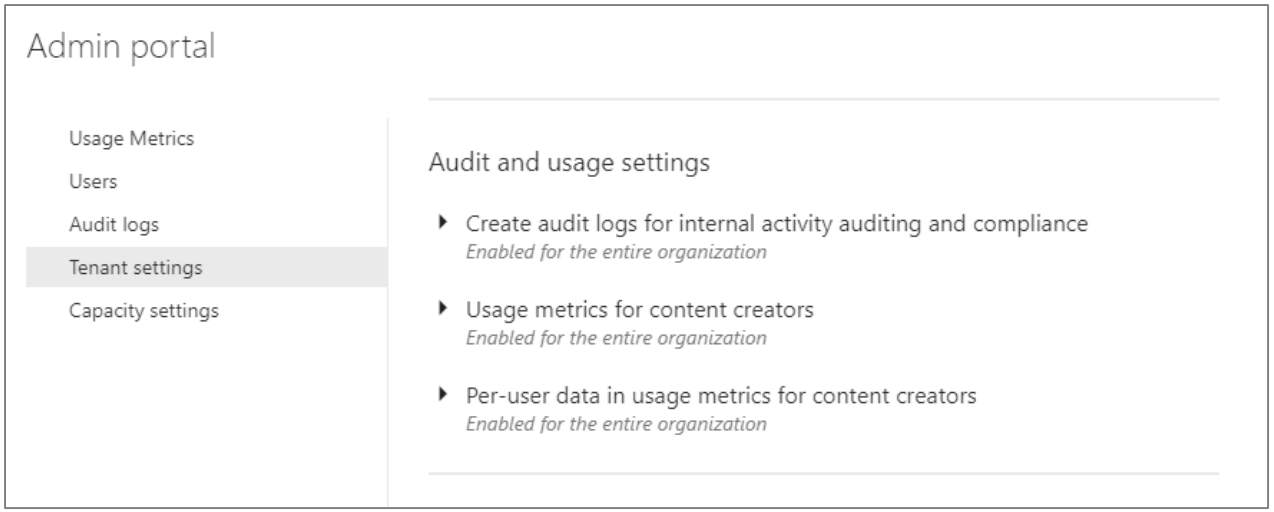
- Power BI Admins control tenant-level settings
  - Control whether users can self-register for Power BI
  - Control who can publish to web
  - Control who can export & share content
  - Control who can create content packs

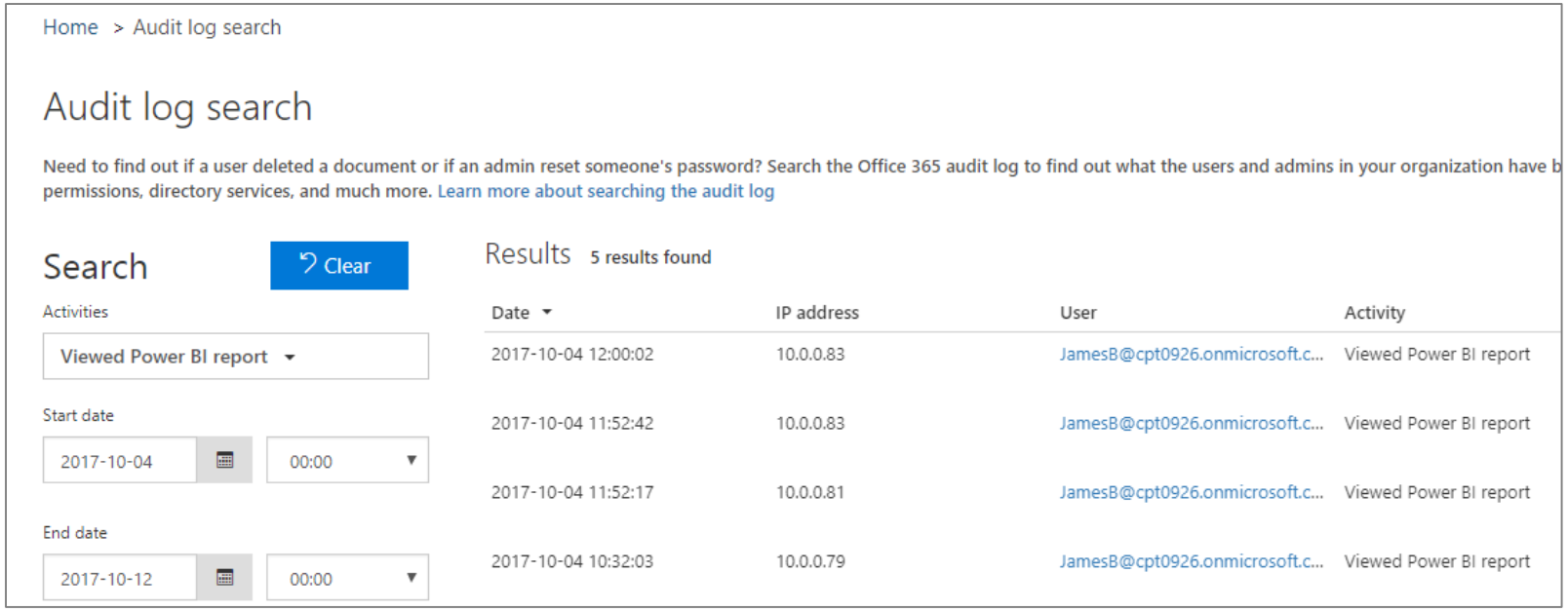




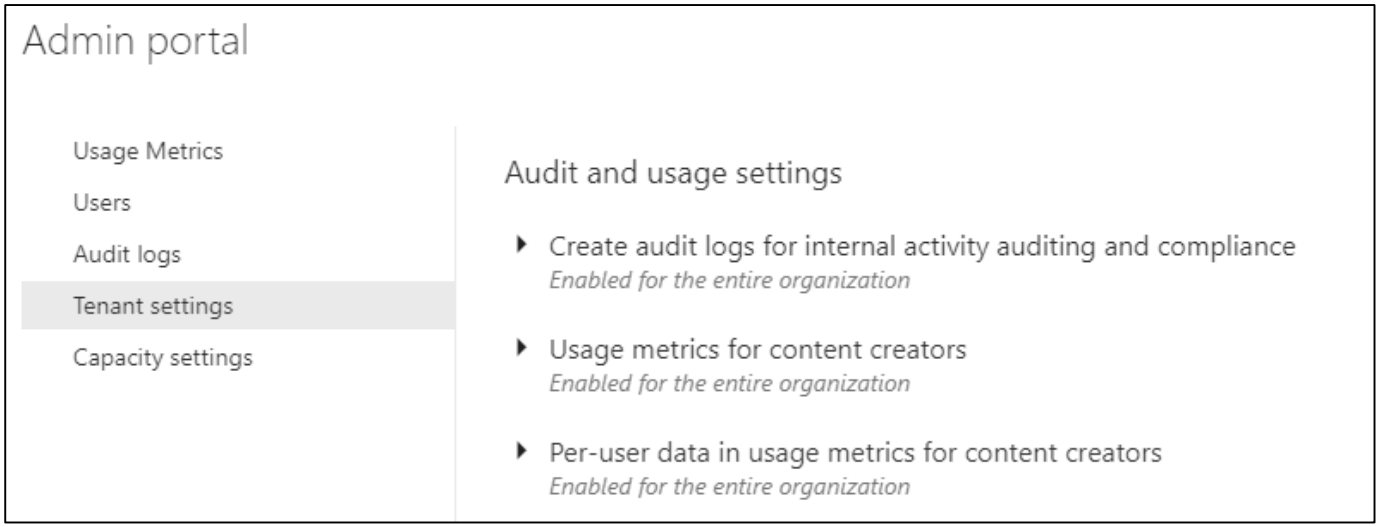


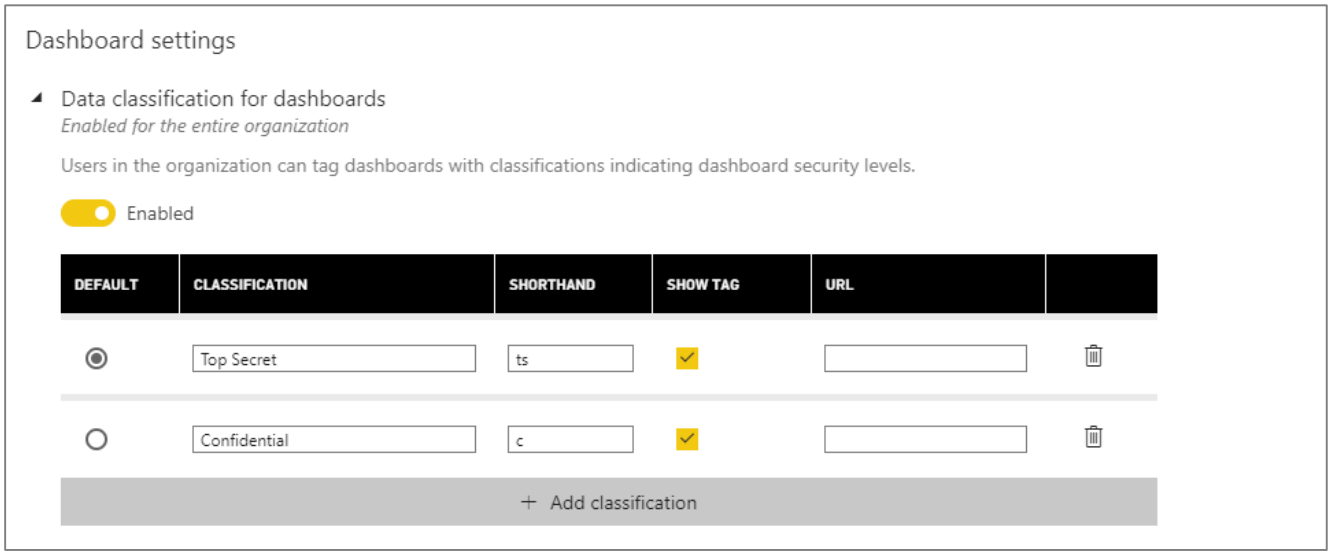
Power BI Audit Log





Data Classification for Dashboards



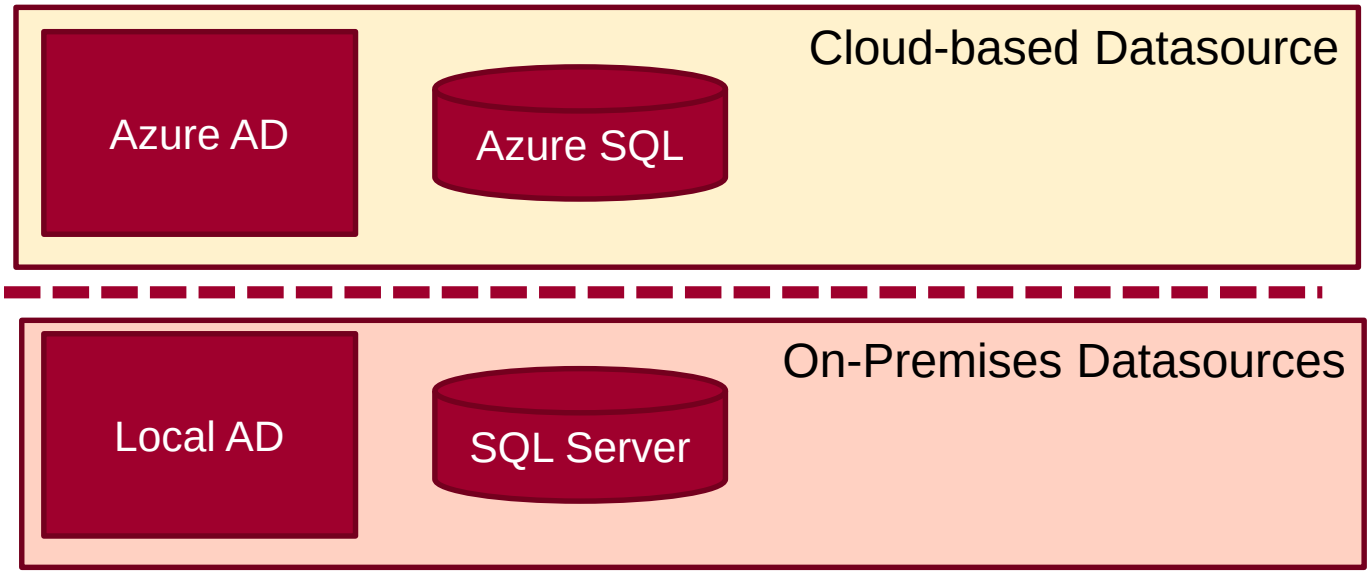


Agenda

- ✓ 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

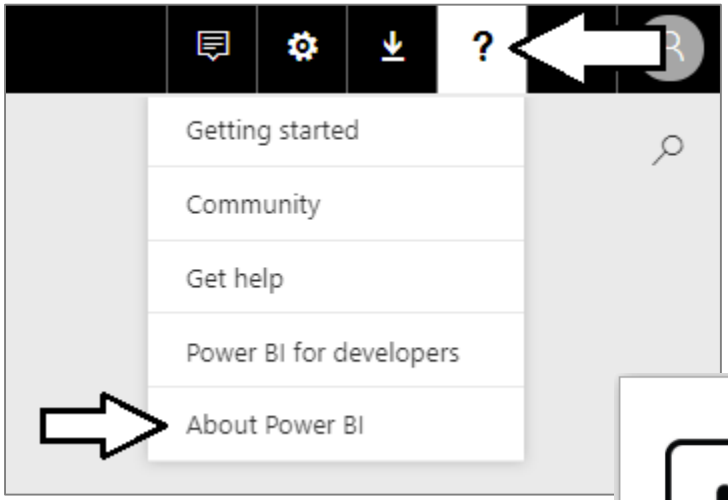
Data source	Data	Metadata	Credentials
Imported Data	Azure Blob Storage	Azure Blob Storage	Azure SQL
Direct Query	Nothing	Azure Blob Storage	Azure SQL
Live Connection	Nothing	Azure Blob Storage	Azure SQL
Push Dataset	Azure SQL	Azure Blob Storage	N/A

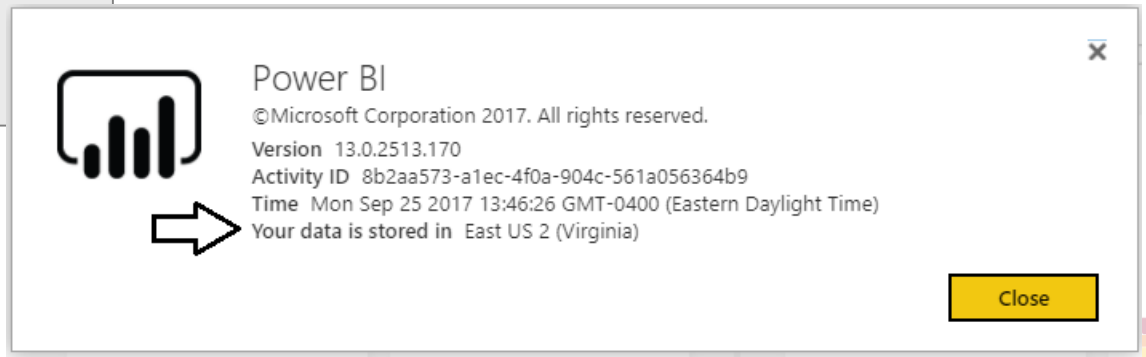
Data Encryption

- 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





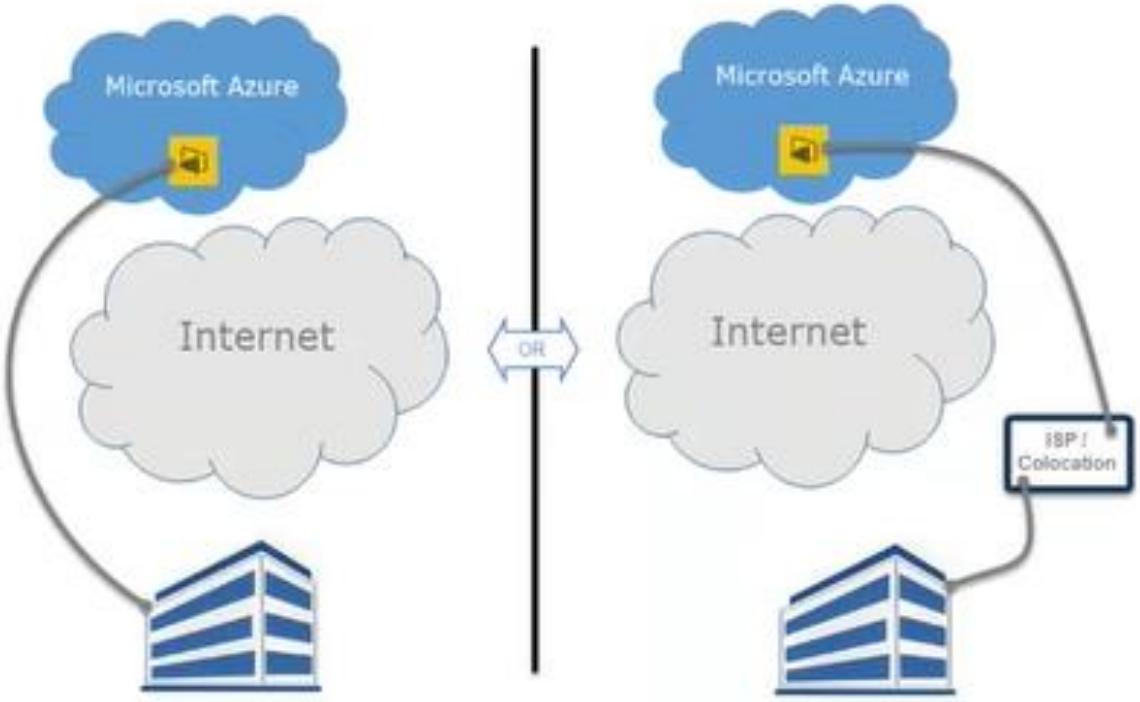
Data Residency and Azure Region Pairs

- 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	√

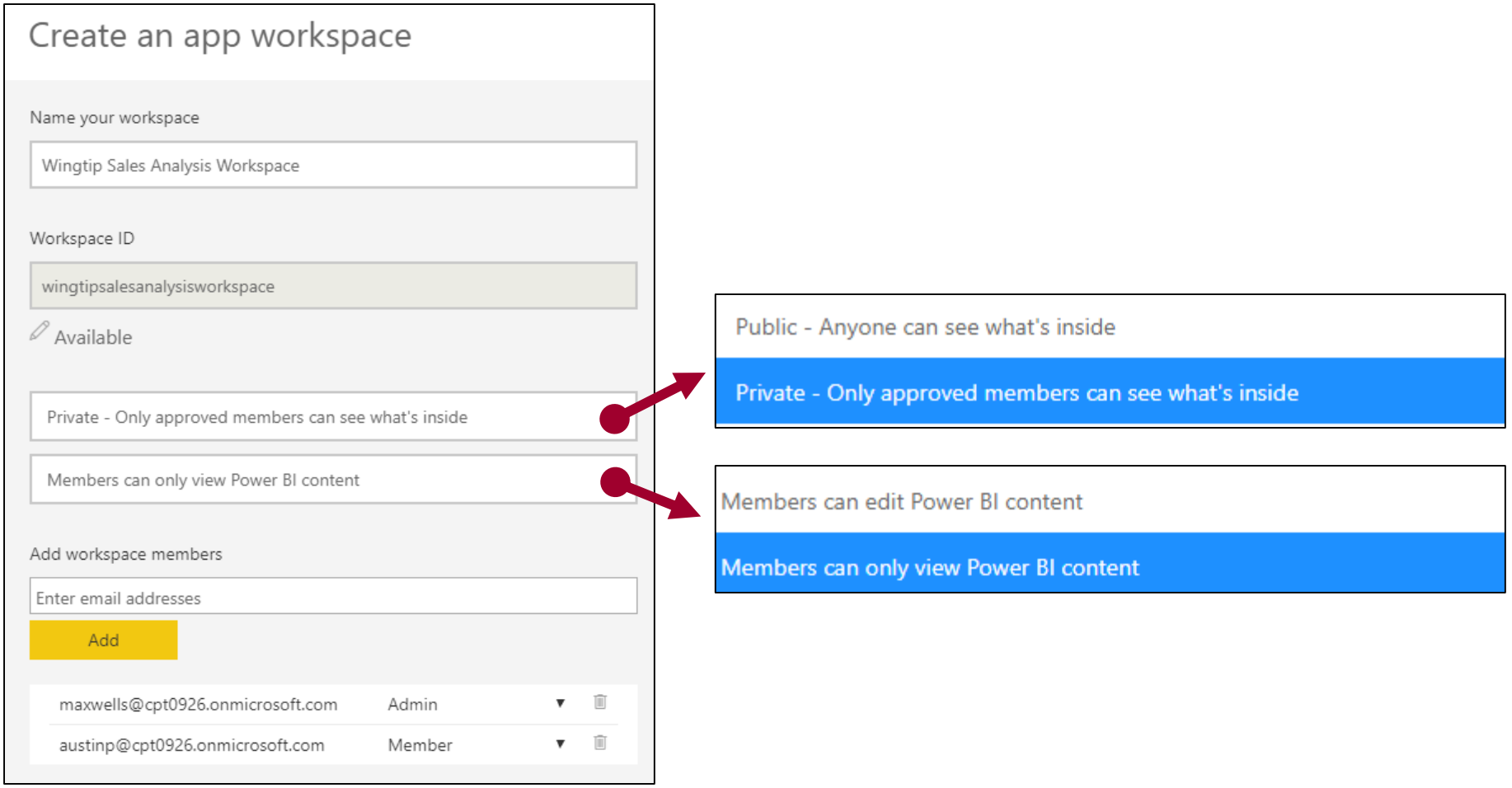
Agenda

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

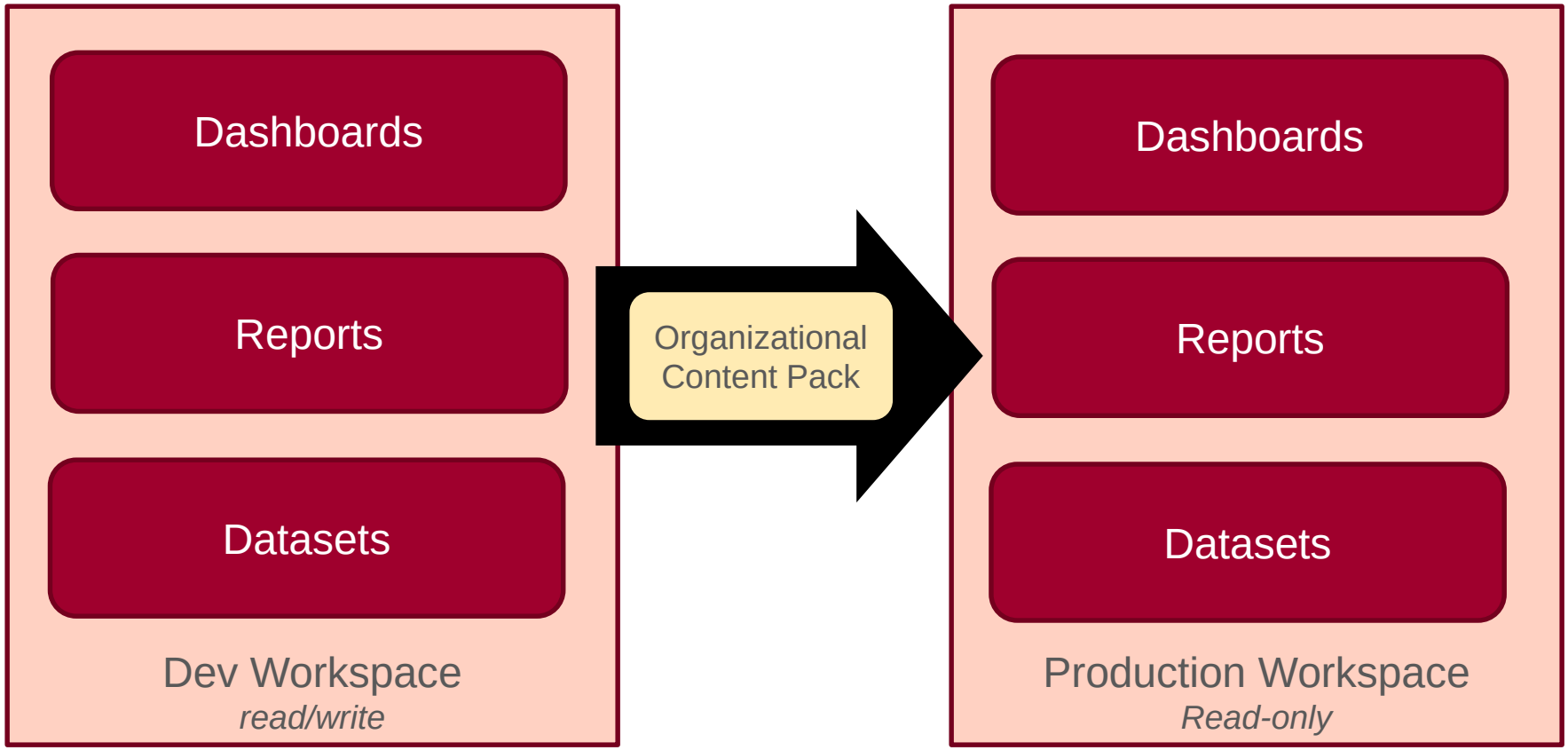
What Exactly is an App Workspace?

- 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

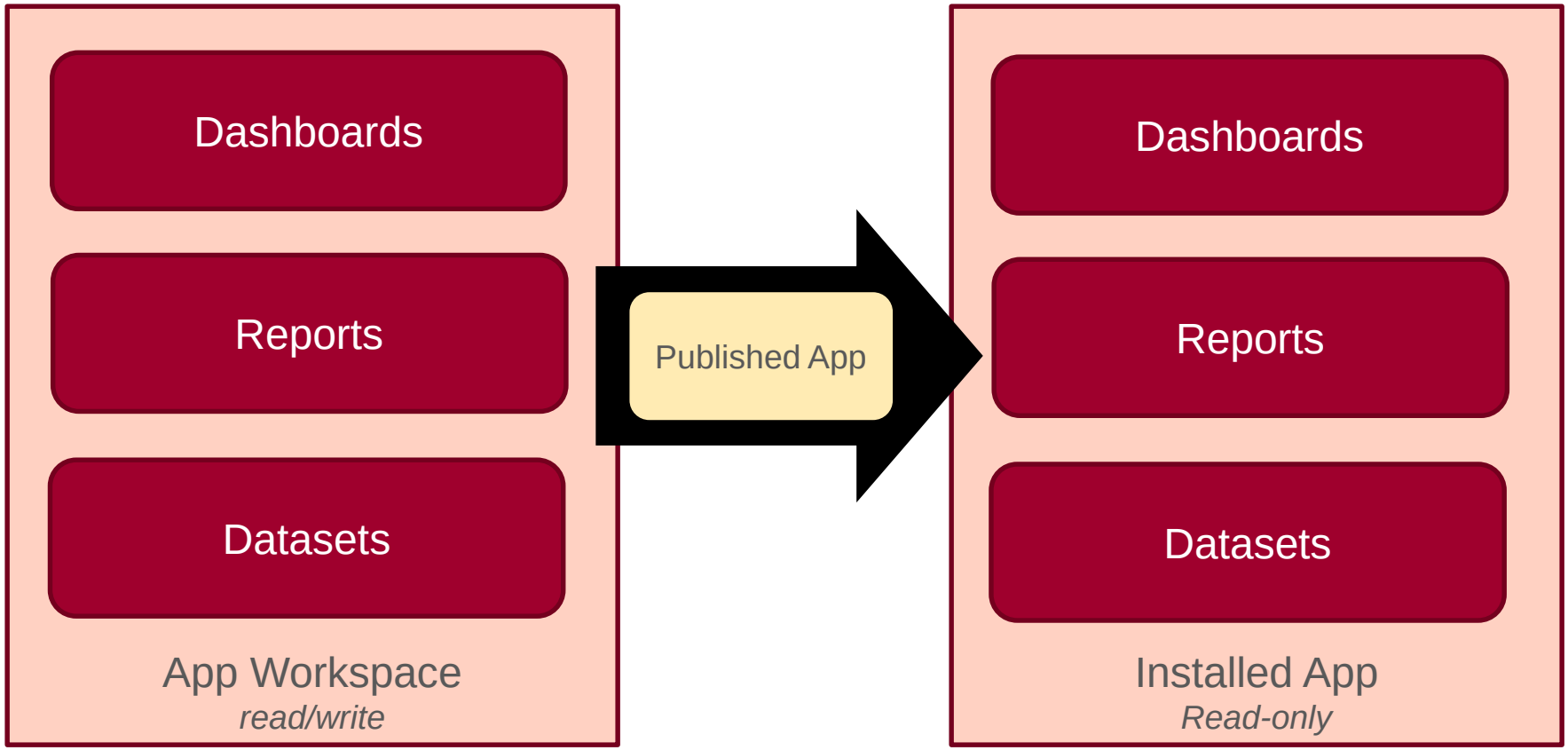
Creating an App Workspace



Old Distribution Model



New Distribution Model



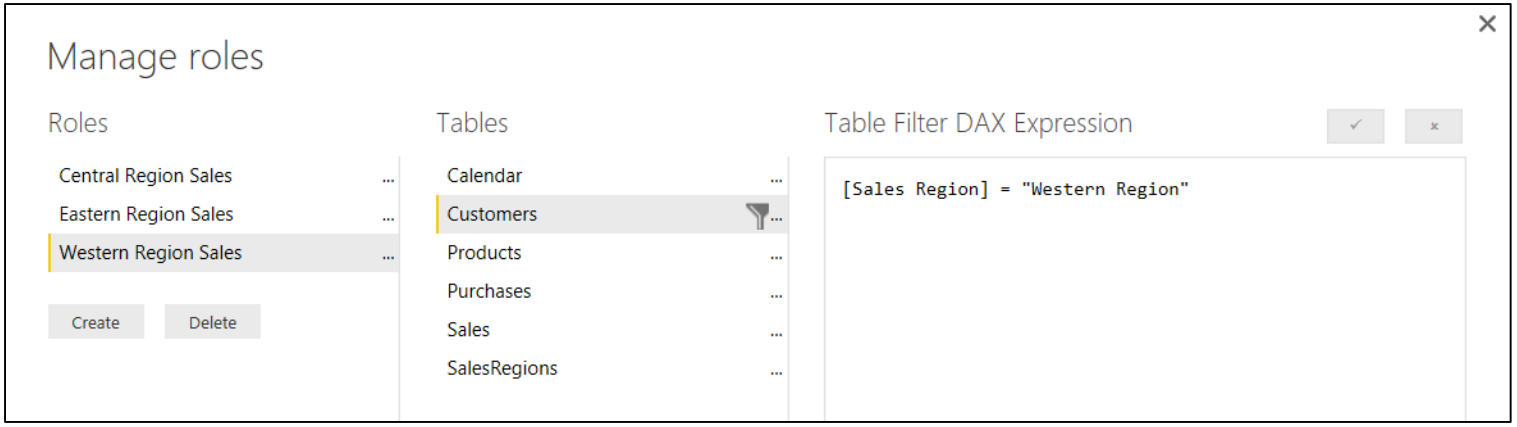
Agenda

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

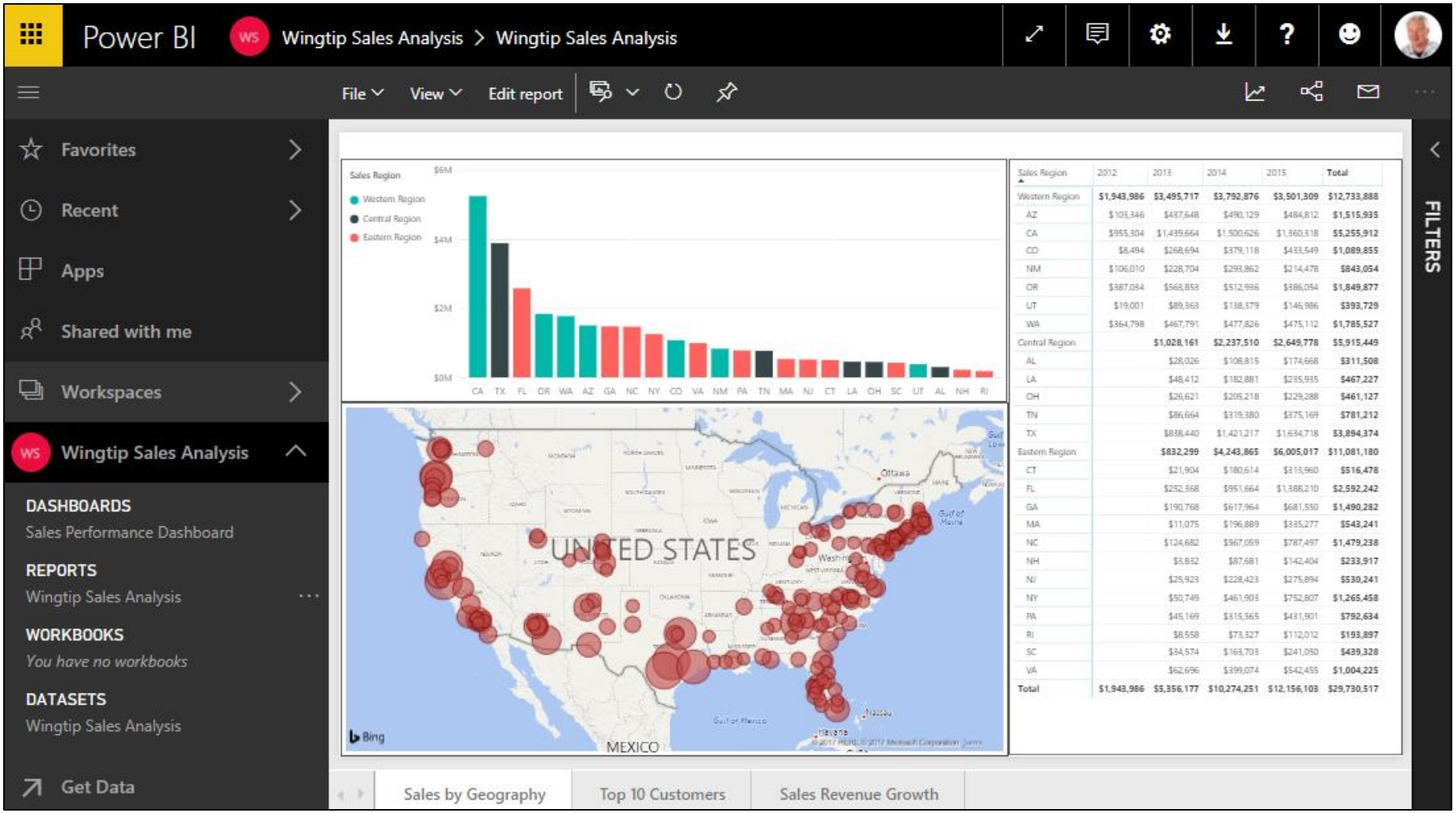
What Is Row-level Security (RLS)

- Security Scheme based on Named Roles
  - Roles are defined using Power BI Desktop
  - Each role is scoped to the dataset within a PBIX project

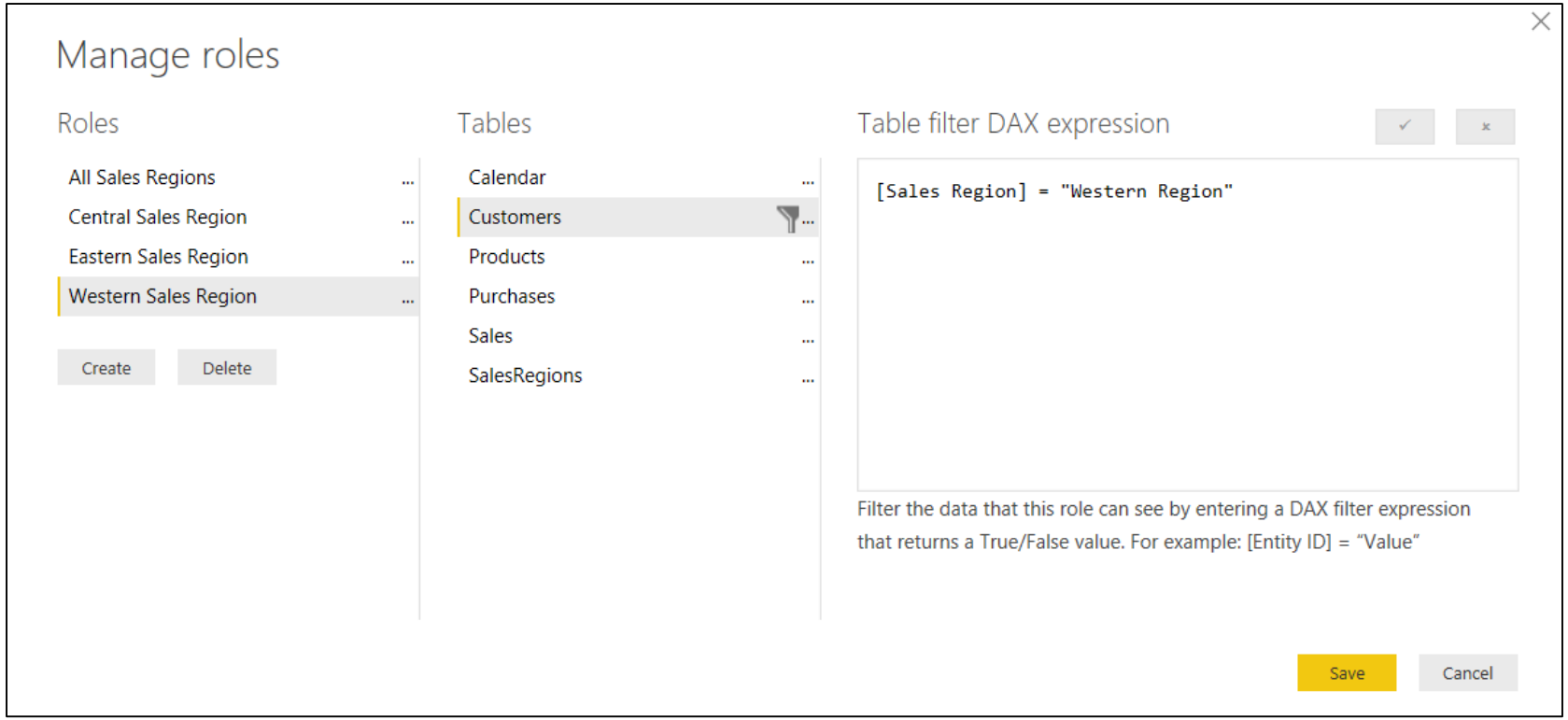
- Role defined using one or more DAX expressions
  - DAX expressions restrict which rows are accessible



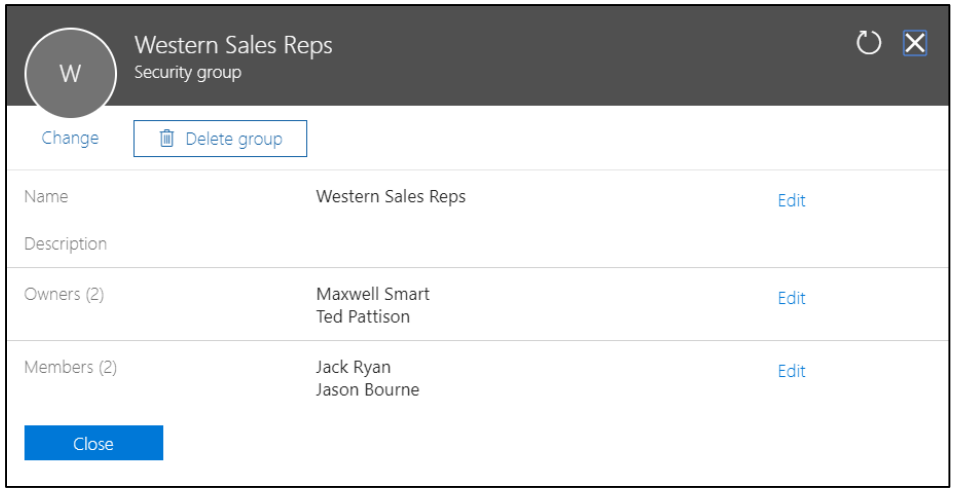
Common RLS Scenario

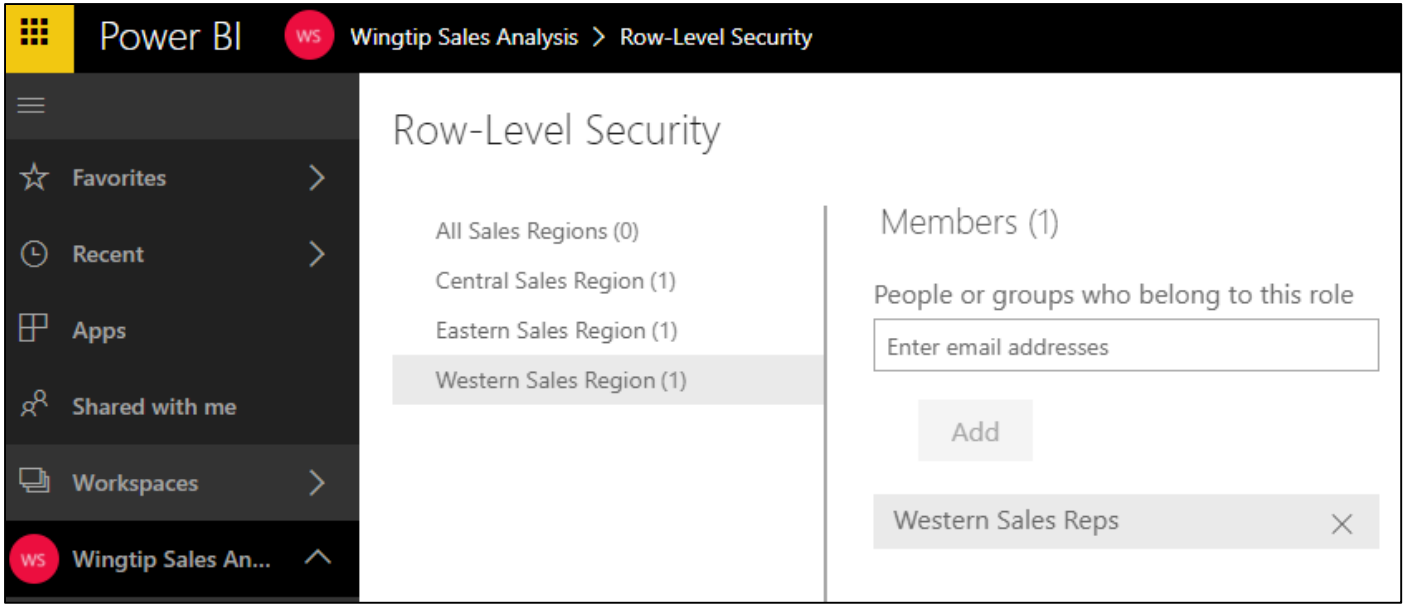


Configuring RLS in the Power BI Desktop

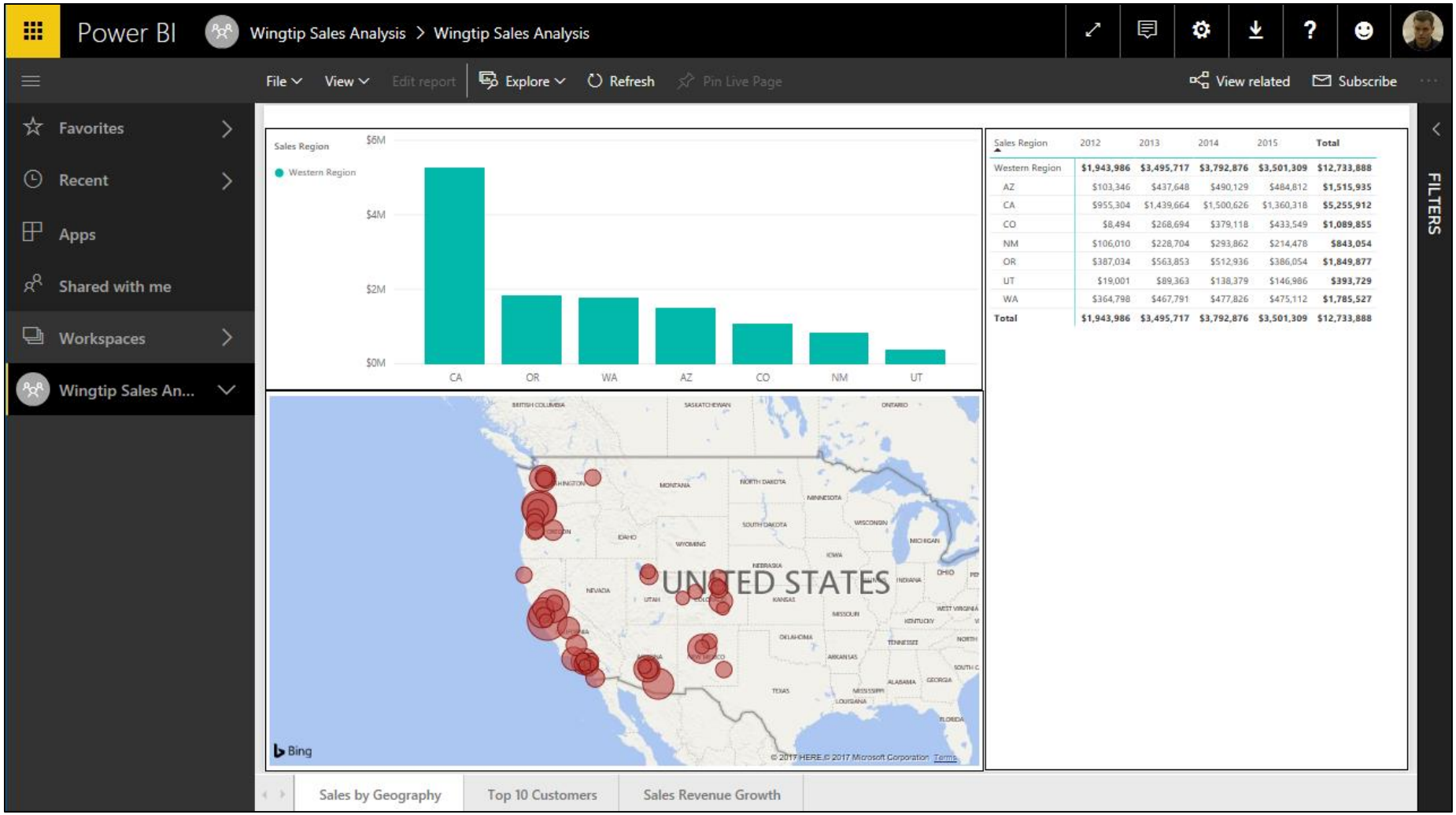


Configuring RLS in the Power BI Service





RLS Enforcement



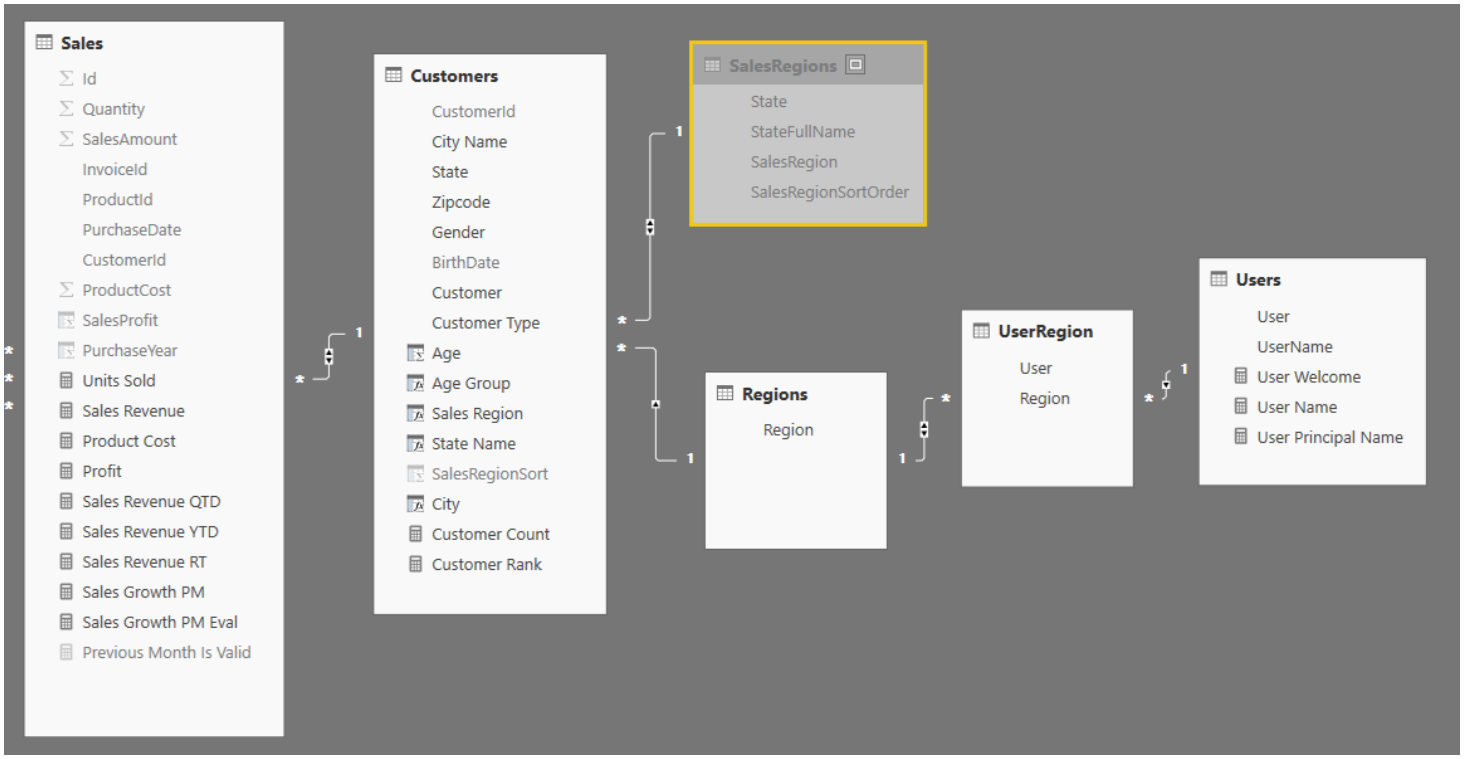

DEMO
Configuring Row-level Security

Agenda

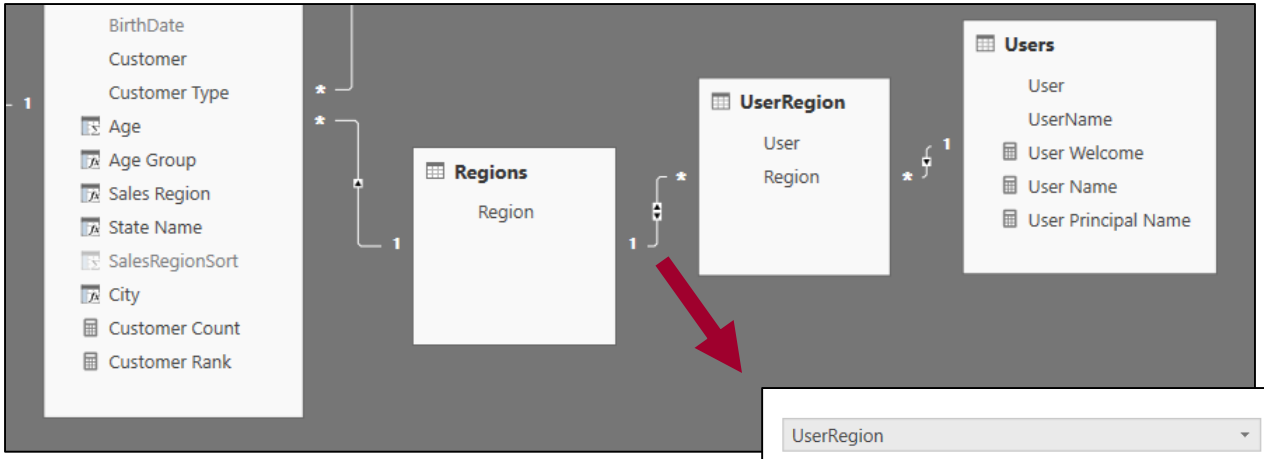
- ✓ User Authentication and Identity
- ✓ Power BI Tenant Administration
- ✓ Data Security
- ✓ App Workspaces
- ✓ Row Level Security
- ➢ Dynamic Row Level Security

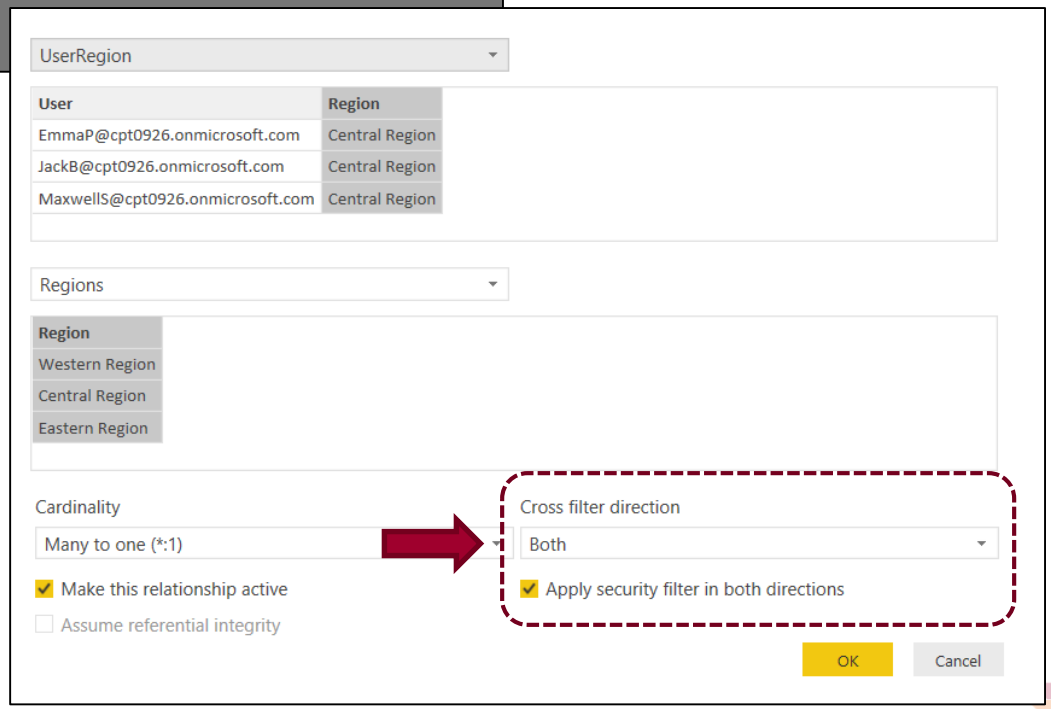
Dynamic RLS

- 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

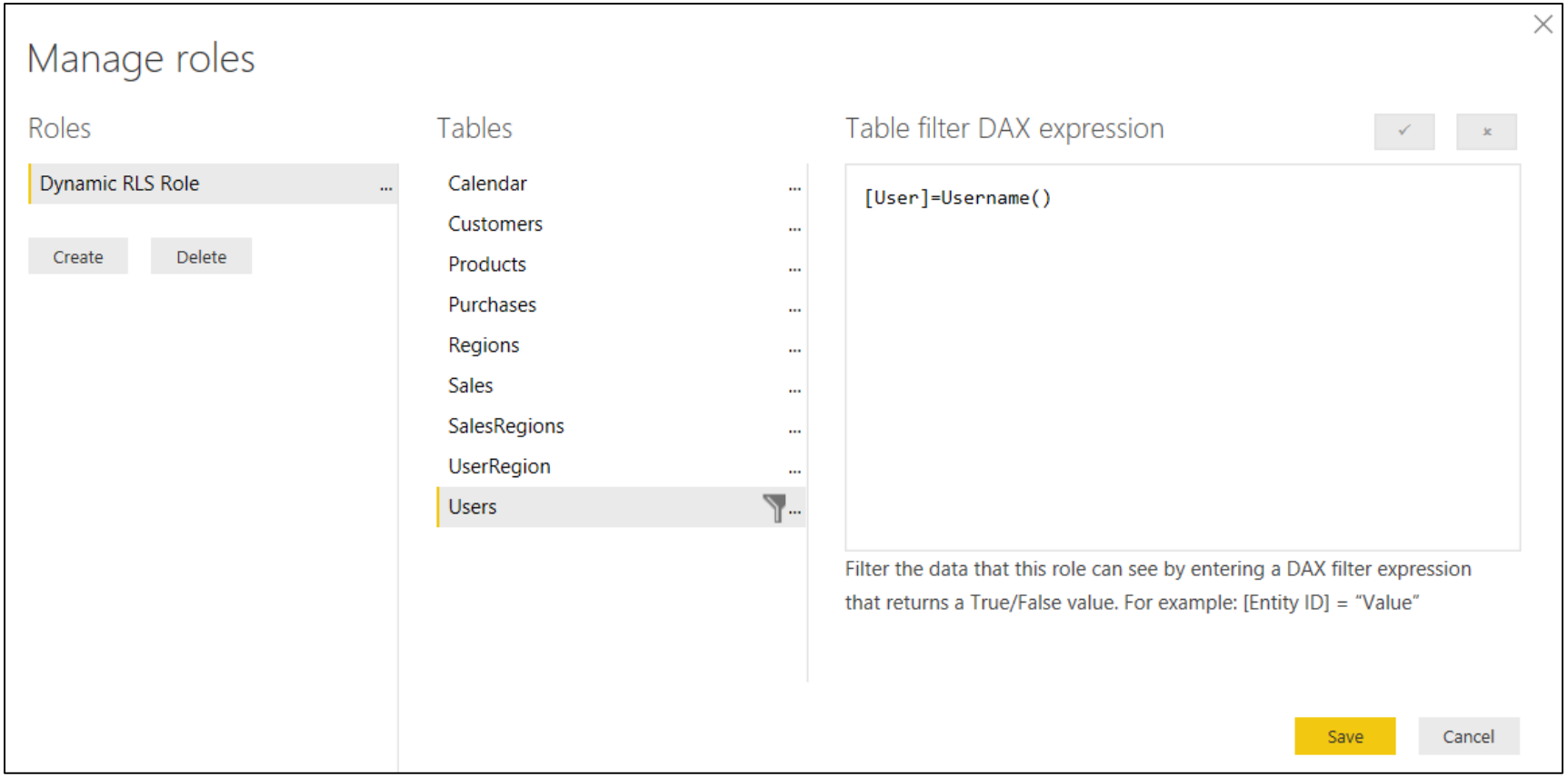


Configuring Cross-direction Filtering

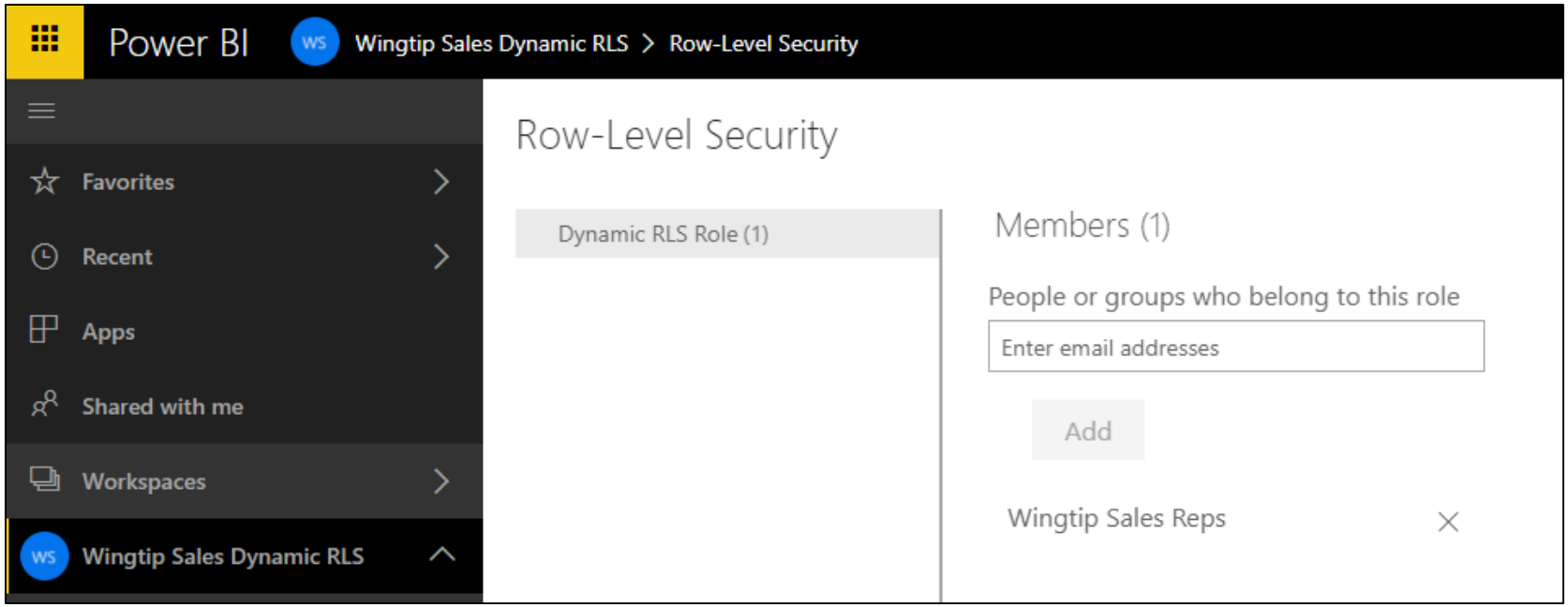




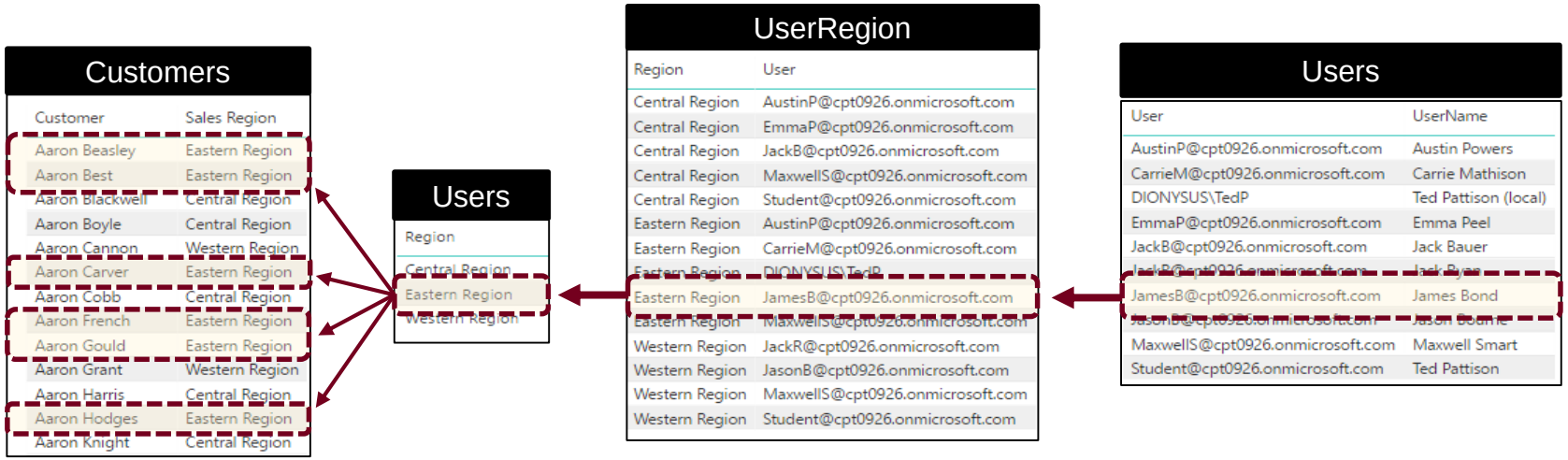
Dynamically Tracking the Current User



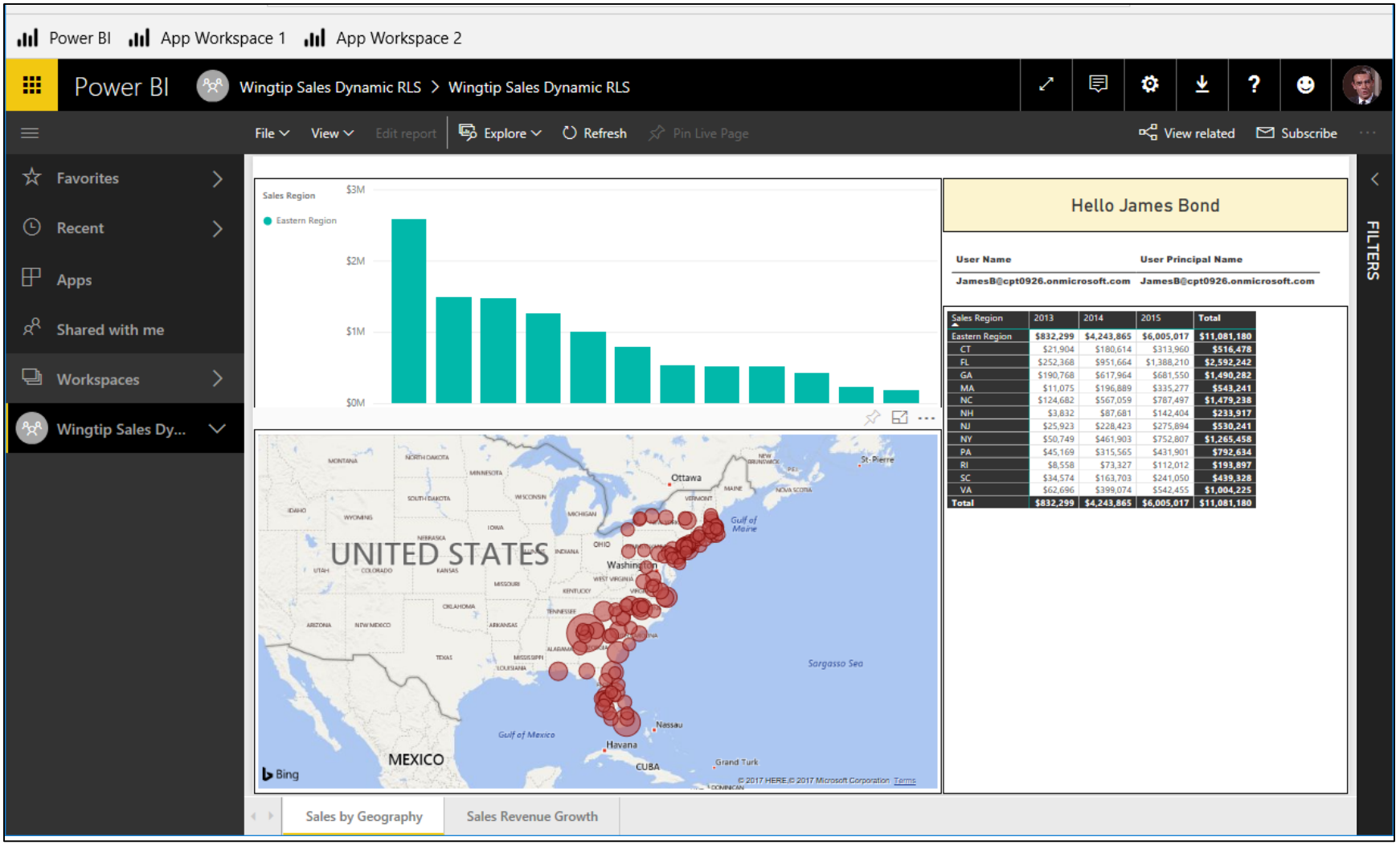
All Users Must Be Added To a Role



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