Administrating and Configuring Security in Power BI

Agenda

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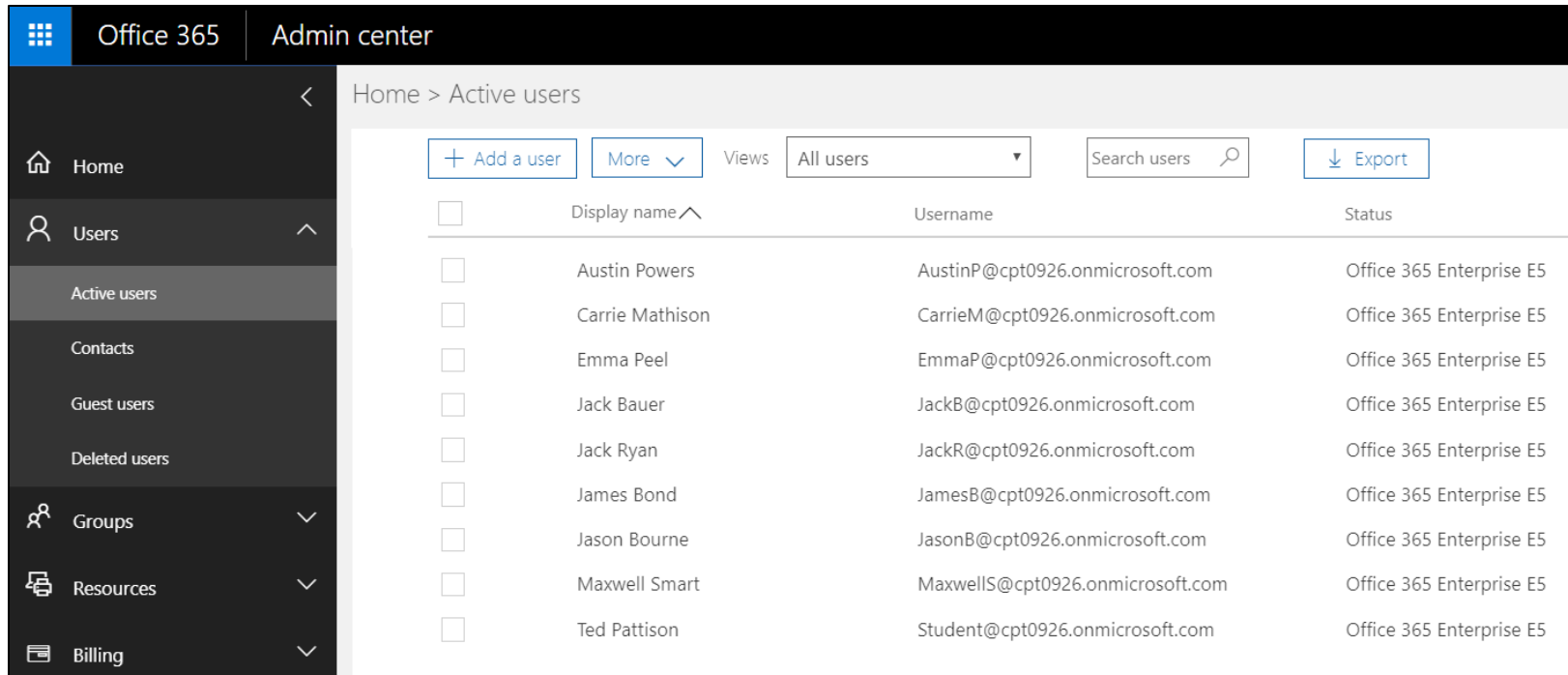- Row Level Security
- Dynamic Row Level Security

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

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

Agenda

- ✓ User Authentication and Identity
- ➢ Power BI Tenant Administration
- • Data Security
- • 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
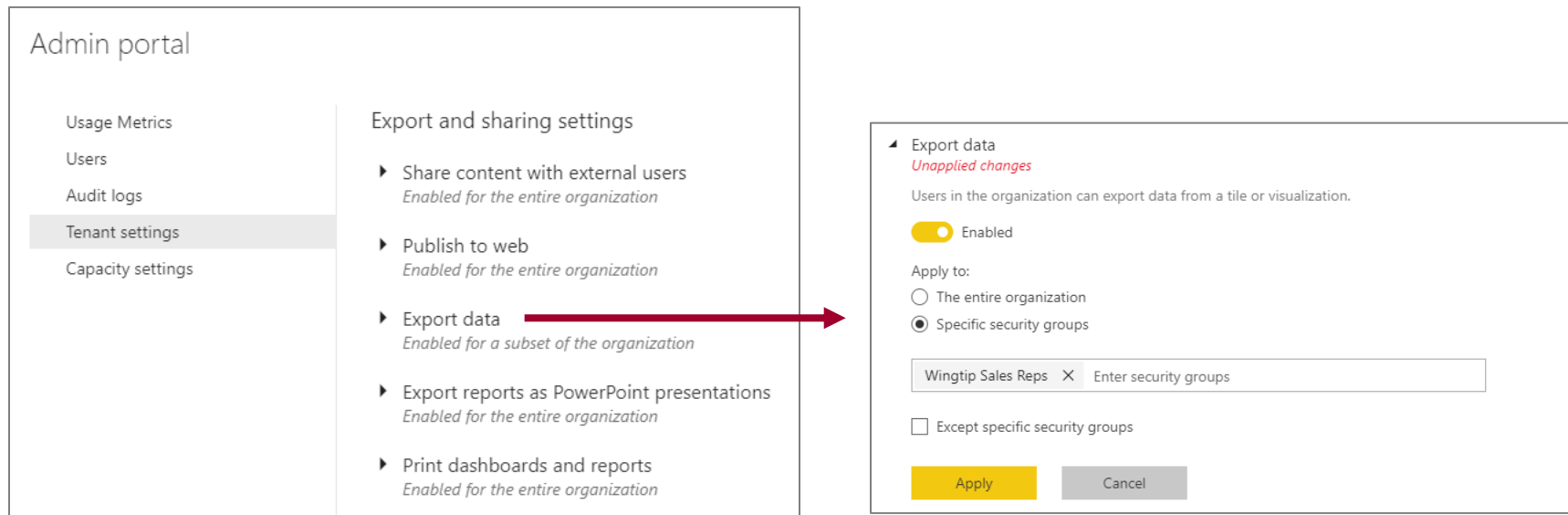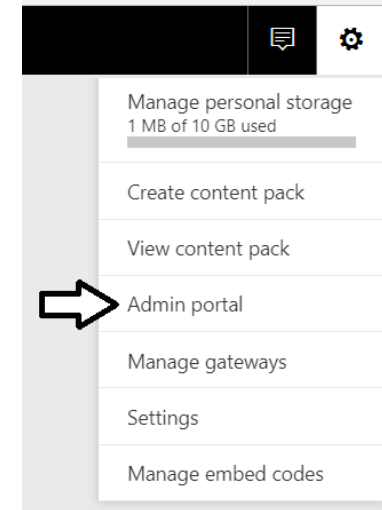 - Control who can export & share content
  - Control who can create content packs

Power BI Audit Log

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 b
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	JamesB@cpt0926.onmicrosoft.c...	Viewed Power BI report
2017-10-04 11:52:42	10.0.0.83	JamesB@cpt0926.onmicrosoft.c...	Viewed Power BI report
2017-10-04 11:52:17	10.0.0.81	JamesB@cpt0926.onmicrosoft.c...	Viewed Power BI report
2017-10-04 10:32:03	10.0.0.79	JamesB@cpt0926.onmicrosoft.c...	Viewed Power BI report

Agenda

- ✓ User Authentication and Identity
- ✓ Power BI Tenant Administration
- ➢ Data Security
- • 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

Cloud-based Datasource

Azure AD

Azure SQL

On-Premises Datasources

Local AD

SQL Server
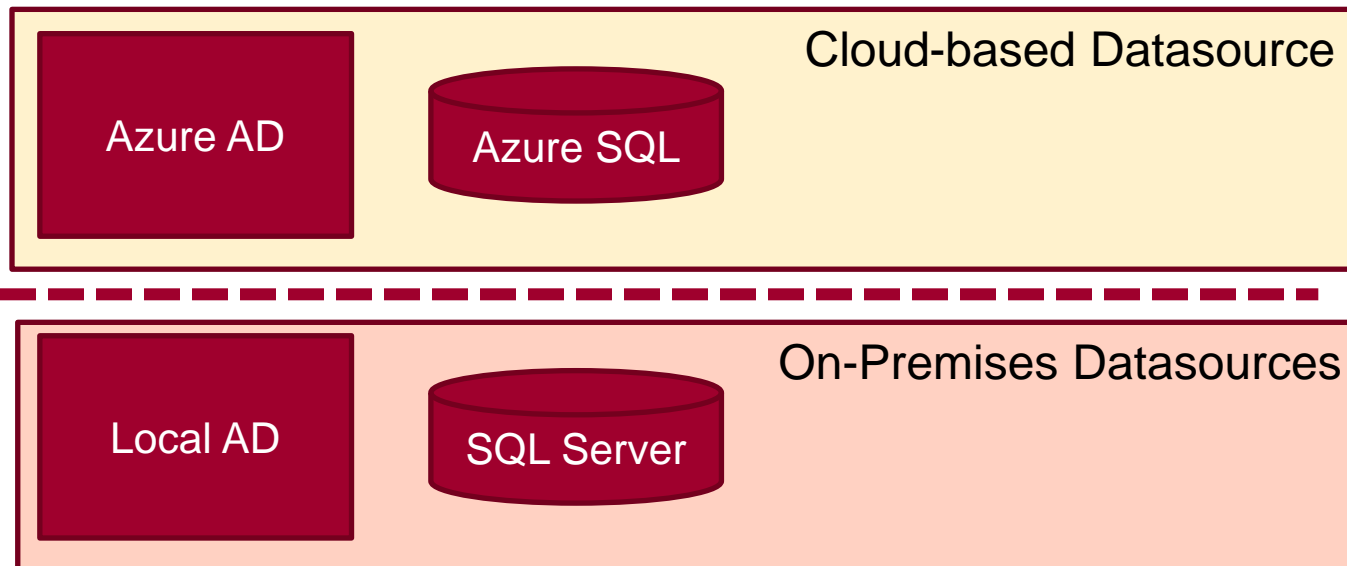
Power BI Data Encryption

- 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 *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
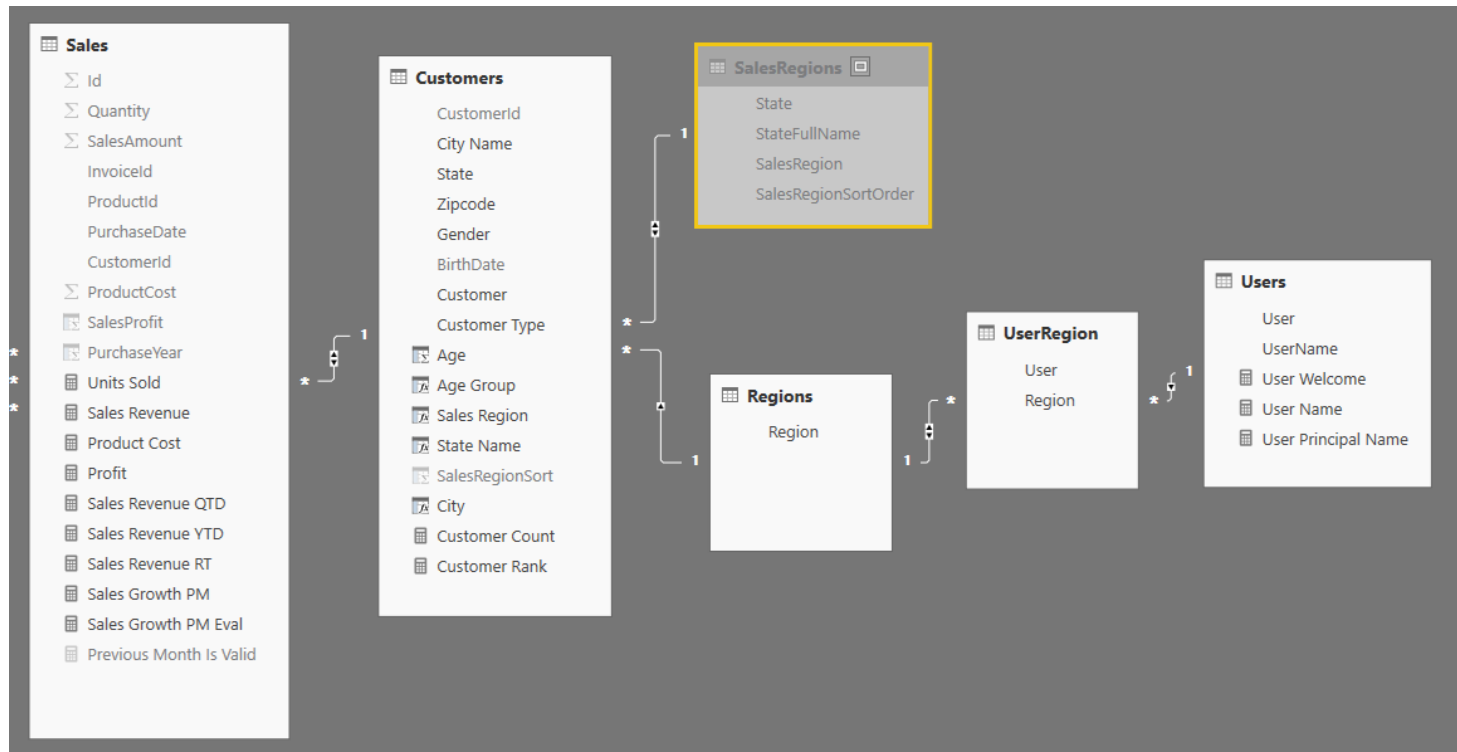 - Encryption key used to encrypt creds stored in cloud

Agenda

- ✓ User Authentication and Identity
- ✓ Power BI Tenant Administration
- ✓ Data Security
- ➤ 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
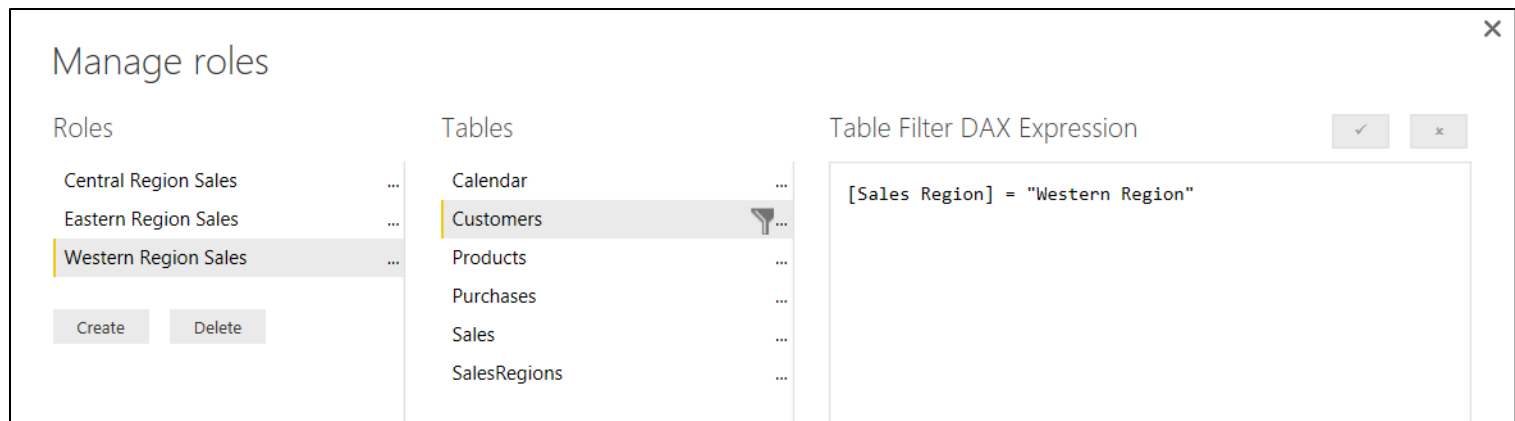
Common RLS Scenario
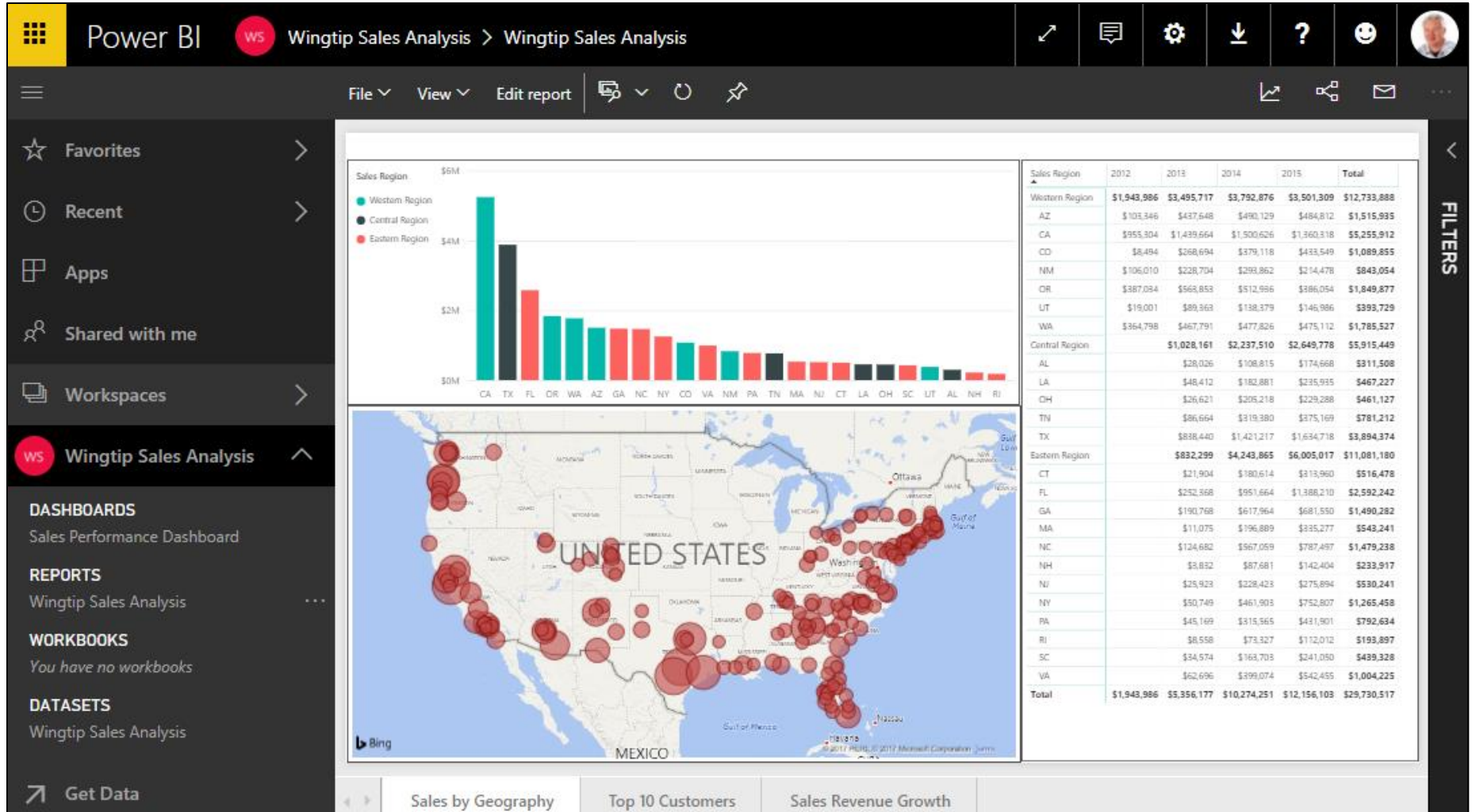
Configuring RLS in the Power BI Desktop

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
- ✓ 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
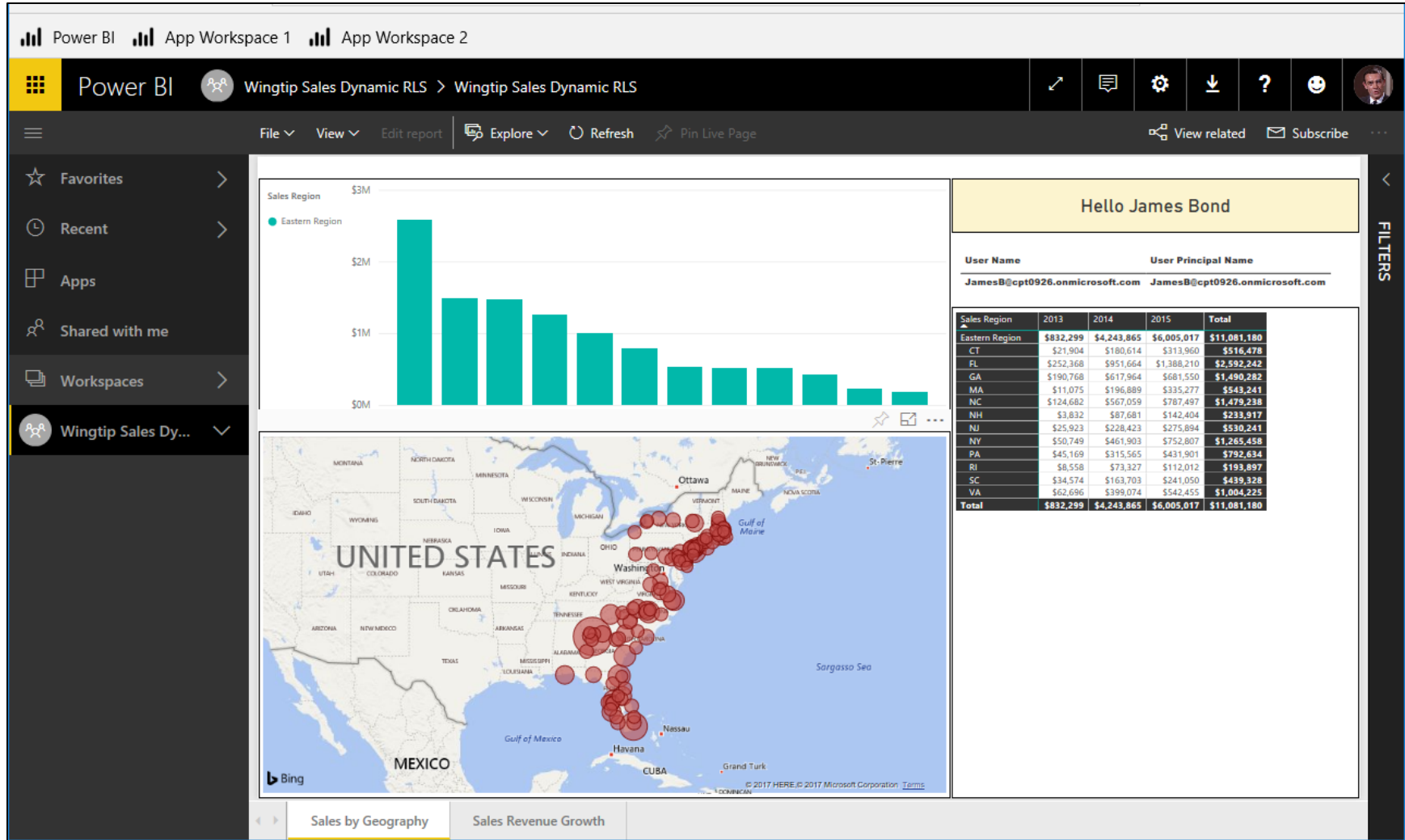
Dynamic RLS Table Filtering
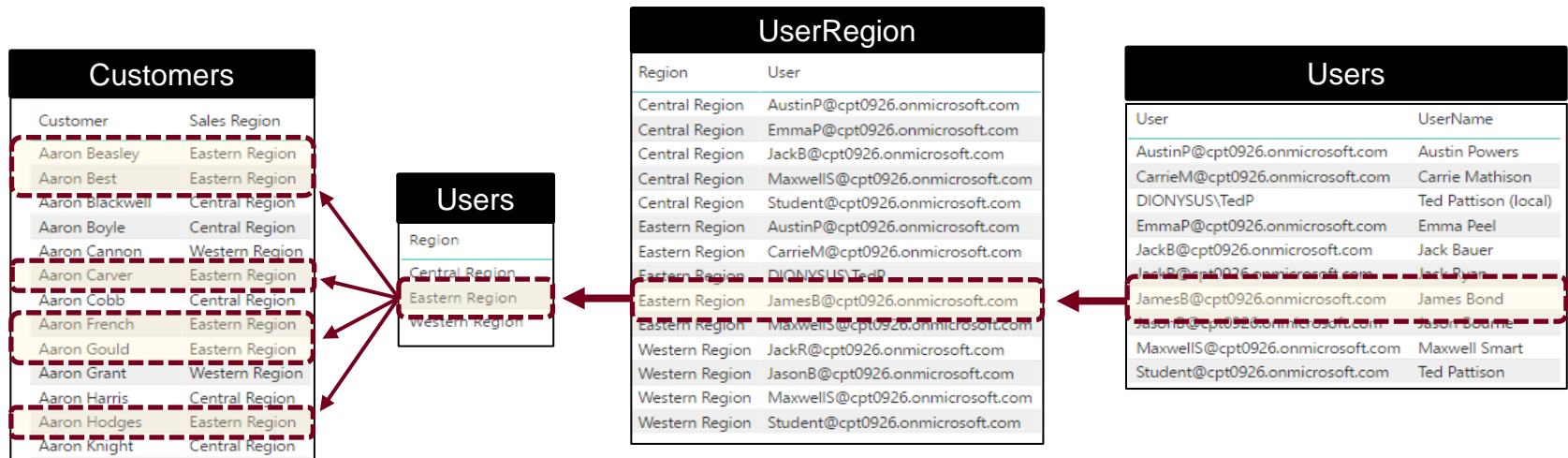
Dynamic RLS Enforcement

Configuring Dynamic Row-level Security

Summary

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