
2026
DYNAMICS
CON
Vegas

Mastering Dataverse Security

Kylie Kiser

Kylie Kiser

- Kylie K Consulting
- Microsoft MVP
- FastTrack Recognized Solution Architect

Agenda

Where do I start?

Security Roles

Business Units

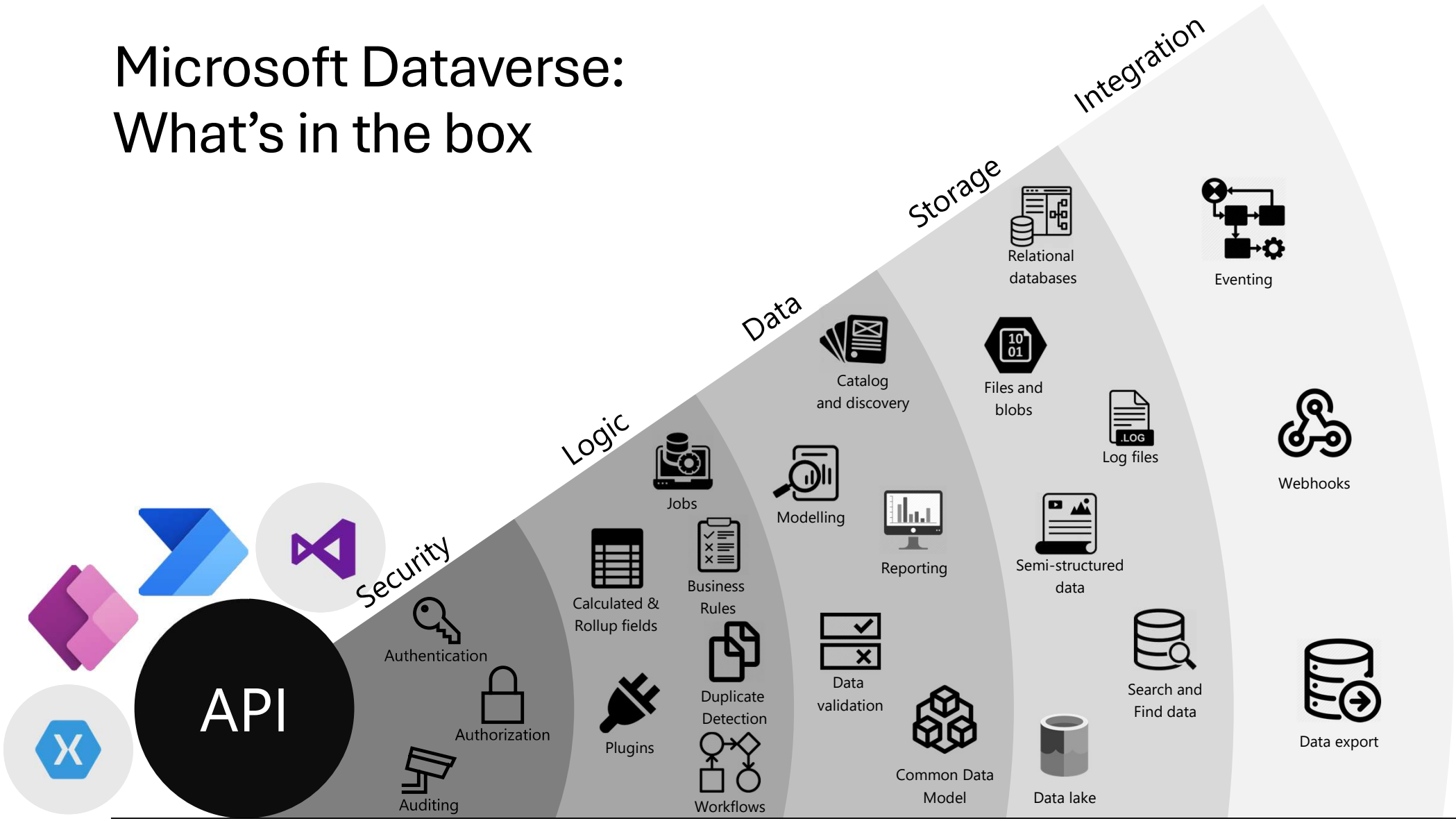
Teams

Additional Security

Other Stuff

Q&A

Microsoft Dataverse: What's in the box



Where Do I Start?

Definitions

Security: Protecting your system and the data which resides within

User Security: Who can access what Tables, Columns, Rows, etc. in the Dataverse

An individual's access is defined by a combination of their Security Roles, Business Unit, Teams, and so much more!

Security Role: Defines rights to Tables and miscellaneous privileges based off the user's Business Unit

Business Unit: Structure of how users "live" in the system

Root Business Unit: Top-most Business Unit, created by default, cannot be deleted or re-parented

Figure Out The Current State

Check out the Security Role report to save current status

Tip: You can also see all users in a specific role in the Power Platform Admin Center > Environment > Settings > Security Role > Open Role

Determine Business Unit Structure

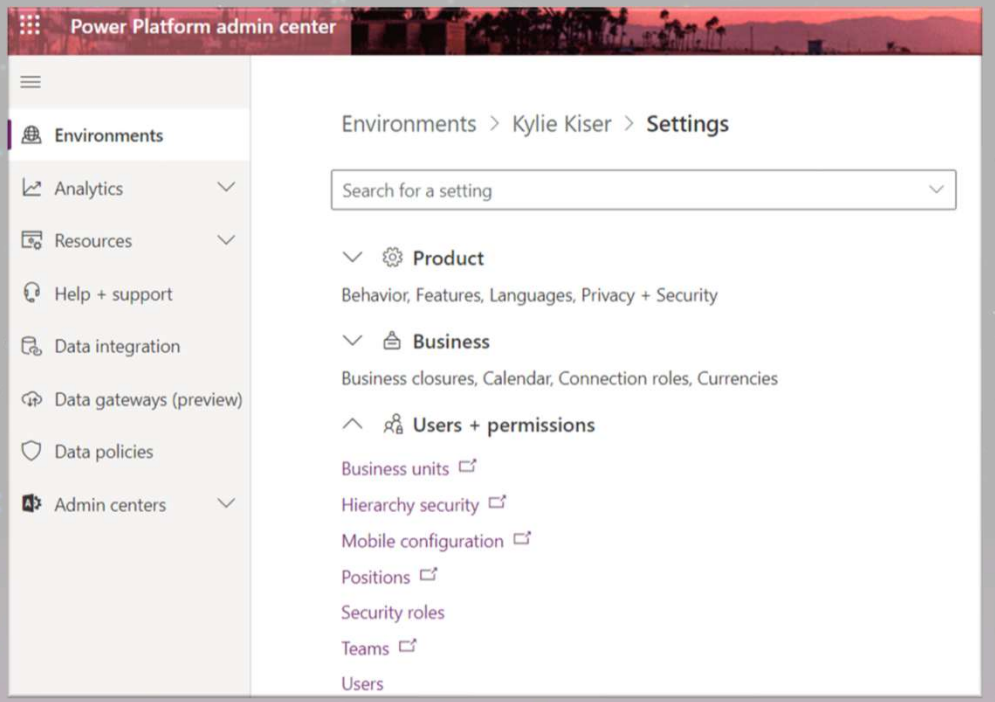
Review roles for dangerous permissions

Brand New?

- You do not need to model your security after your organization structure
- Keep it as simple as possible!
- All “exceptions” need good reasons
- Security decisions can quickly cause performance and usability issues

Where do I look?

- Power Platform Admin Center: aka.ms/ppac
- Select Environment > Settings > Users + Permissions



Quick Reminders

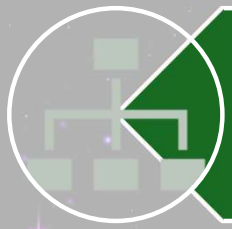
All security is cumulative. Users will get the least restrictive combination of all their roles

Security by Obscurity is not security. Be aware that just because someone can’t see data on a form, they may still be able to still find it.

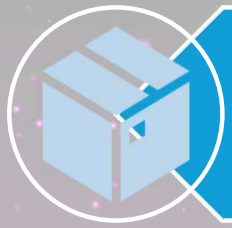
Security Roles

What is a Security Role?

Defines access rights to rows based on who owns the row, and the user's relationship to the owner.



Role is created in a specific business unit and a mirrored copy of the role is created for each child business unit.



Security Roles are solution aware when created at the Root Business Unit.

Out of the Box or Custom?

01

Be careful using Out of the Box roles as they generally have more access than you may want

02

Fully custom can be difficult to find all the minimum permissions needed

03

Best Practice: Copy an out of the box role and then remove unnecessary permissions.

04

Recommendation: Create one role for all users to get access to your Dynamics environment, then add extra roles on top of that for specialized permissions by job function

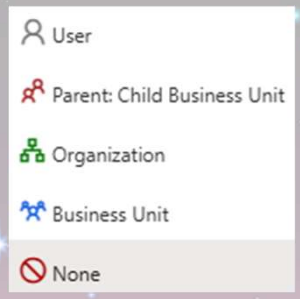
Privileges

Table ↓		Name	Create	Read	Write	Delete	Append	Append to	Assign	Share
Core Records (1)										
Account	...	account	None	None	None	None	None	None	None	None

- Create: Save a row for the first time. Must have the same or higher level of read access
- Read: View existing rows
- Write: Edit rows
- Delete: Don't give people this
- Append: Set a lookup on this rows
- Append To: Allow this to be selected in a lookup
- Assign: Change Owner
- Share: share with someone else

Access Levels

- None: No soup for you!
- User (Basic): Rows I Own
- Business Unit (Local): Rows anyone in my Business Unit Owns
- Parent: Child Business Unit (Deep): Rows anyone in my Business Unit or its child Business Units Own
- Organization (Global): All rows



Example

Security Role: Salesperson

Search by table name or table privilege n...

Details

Tables | Miscellaneous privileges | Privacy-related privileges

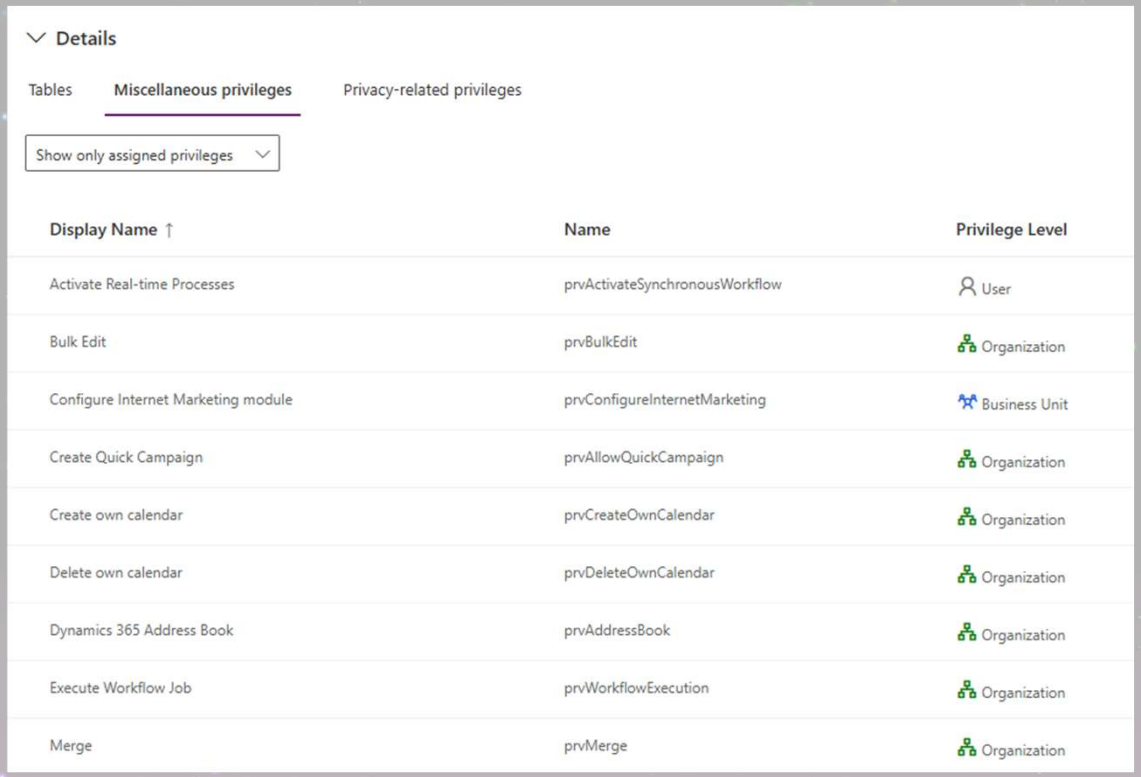
Show only assigned tables

Compact Grid View: On

Table ↑	Name	Create	Read	Write	Delete	Append	Append to	Assign	Share
Core Records (49)									
ACIViewMapper	aciviewmapper	None	Organization	None	None				
Account	account	User	Organization	Organization	User	Organization	Organization	User	Organization
Action Card	actioncard	User	User	User	None	User	Organization	None	
Action Card User Settings	actioncardusersettings	User	User	User	User				User
Activity	activitypointer	User	Organization	Business Unit	User	Business Unit	Business Unit	User	Organization

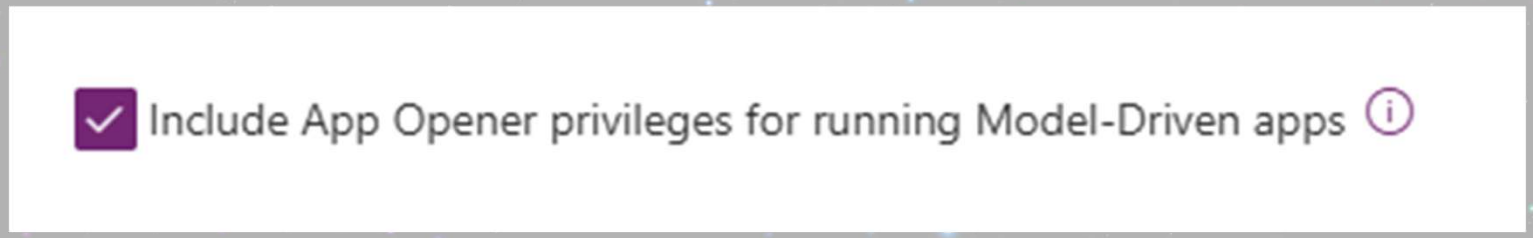
Miscellaneous Permissions

- Additional permissions that can be either On or Off



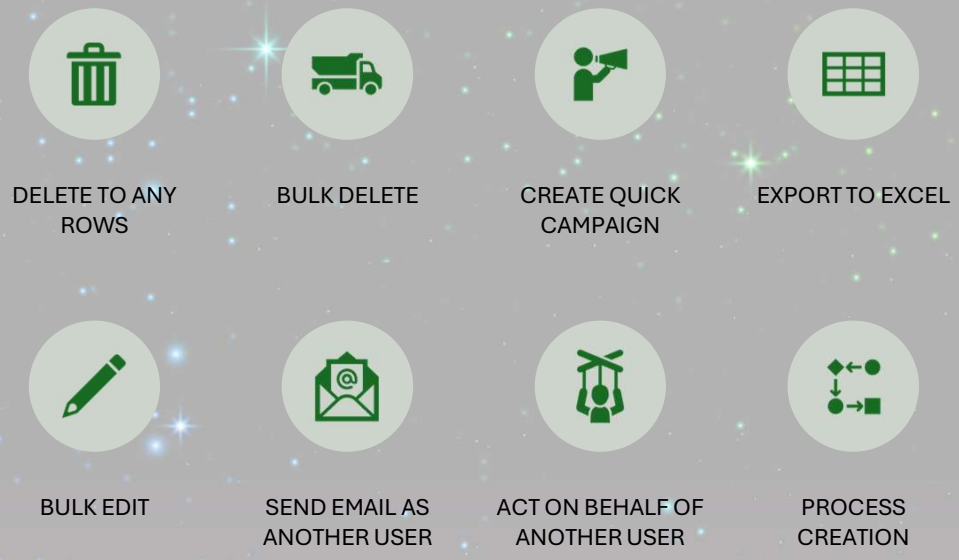
Core Privileges

- New Option when creating a new Security Role!



Dangerous Permissions

- Keep an eye out for these potentially dangerous permissions in your security roles:
    - Best Practice: Have your users Deactivate rows they no longer need instead of delete
- Ensure there is a business reason for all these permissions



Special Security Roles

There are a few *special* roles that users may need to access specific functionality	Roles for ISV/Partner solutions
• Ex. Dynamics 365 App for Outlook User	• **Best Practice:** Review roles provided with your ISV solutions to ensure they do not grant additional permissions you do not want your users to use. If changes are needed, discuss with the ISV and do not update. If you update, then there is a risk that a new version will overwrite your changes!

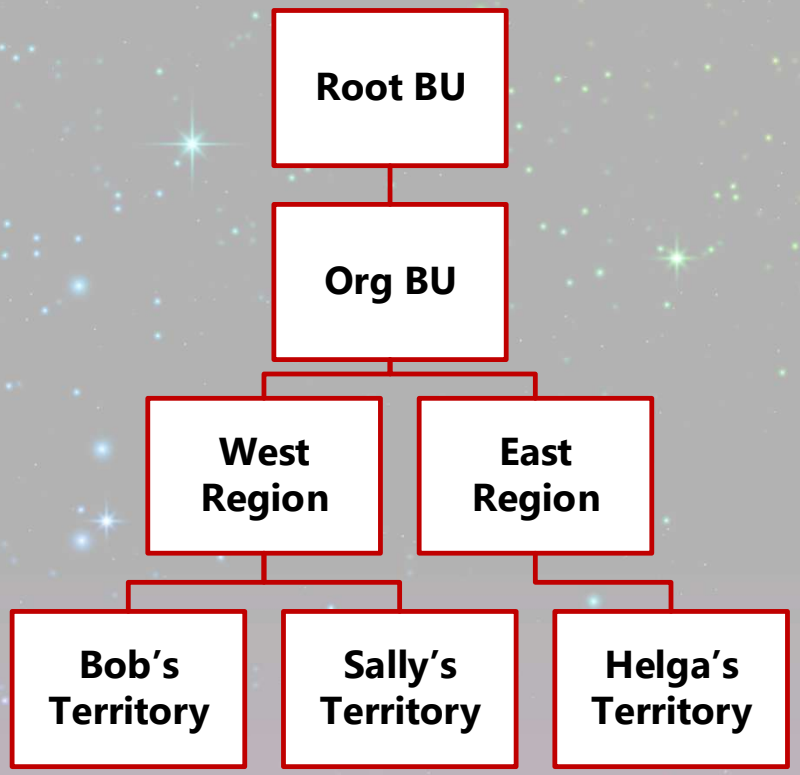
Business Units

Defining Your Structure

- Structure should be based on access needs not organization structure
- Determine data that cannot be shared
- Goal of Dynamics system is to share information, so we want the least-restrictive security possible
- Best Practice: Only administrator users should be in the root business unit. You always want to create at least one additional business unit

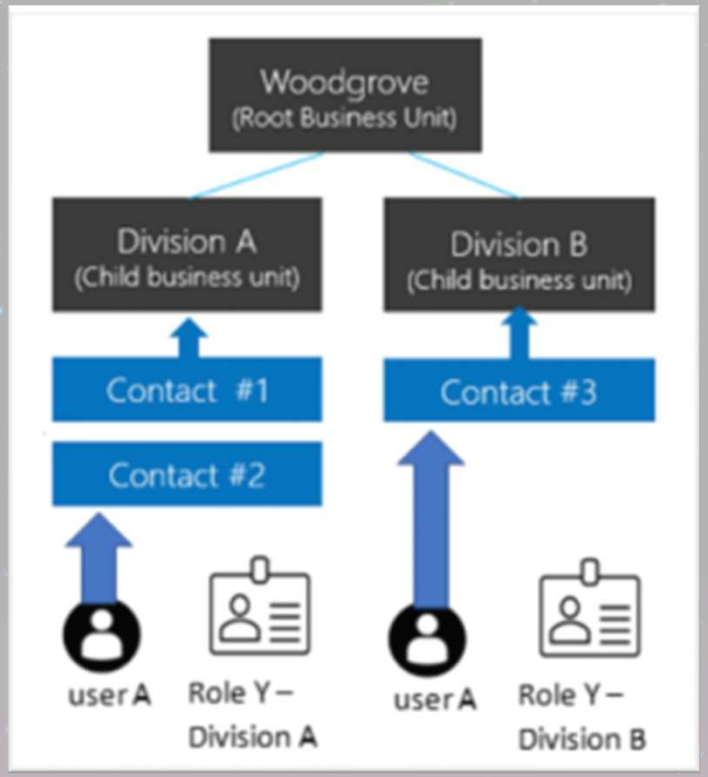
Example Business Unit Structure

- Where should Marketing live?
- How do we configure management?
- What about support staff? Are they dedicated to a territory or region? All the time?

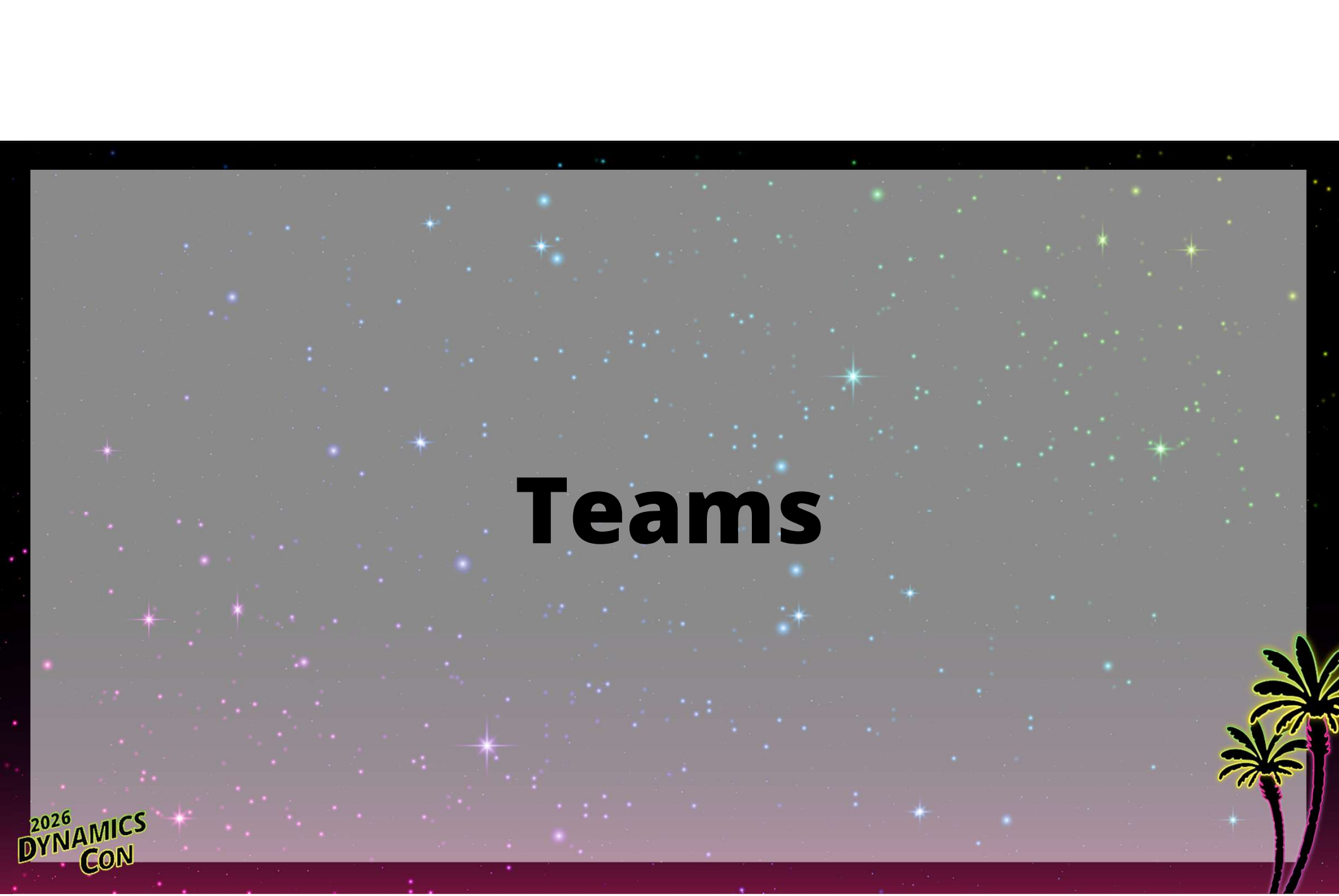


Modern Business Units

- Turn on Record Ownership Across Business Units
- When you assign a Security Role to a user you will select the Business Unit that is assigned
- User can choose the “Owning Business Unit” for records they work with
- When users change Business Units, the ownership can stay with the previous Business Unit



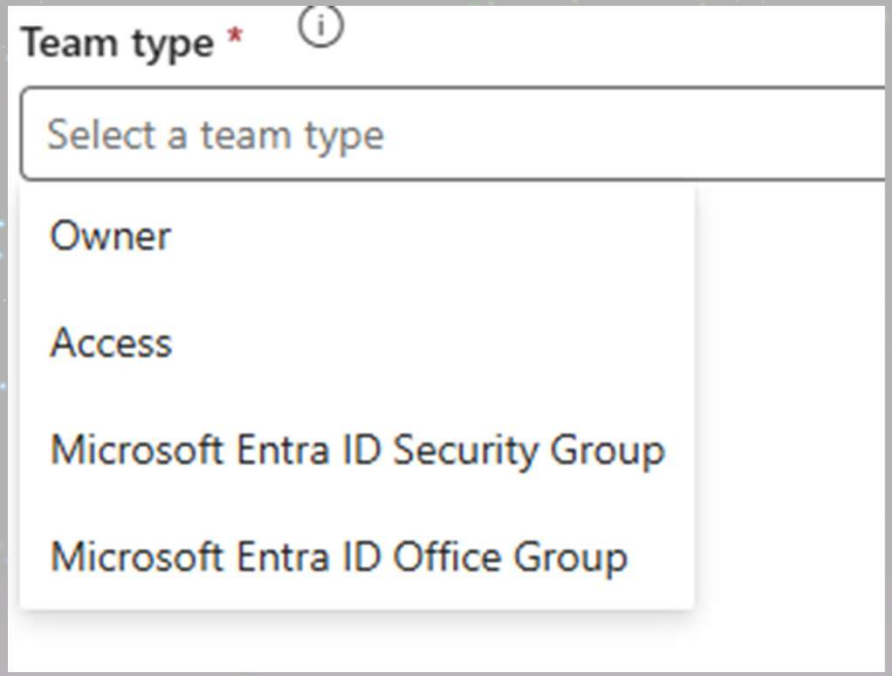
Teams



Overview

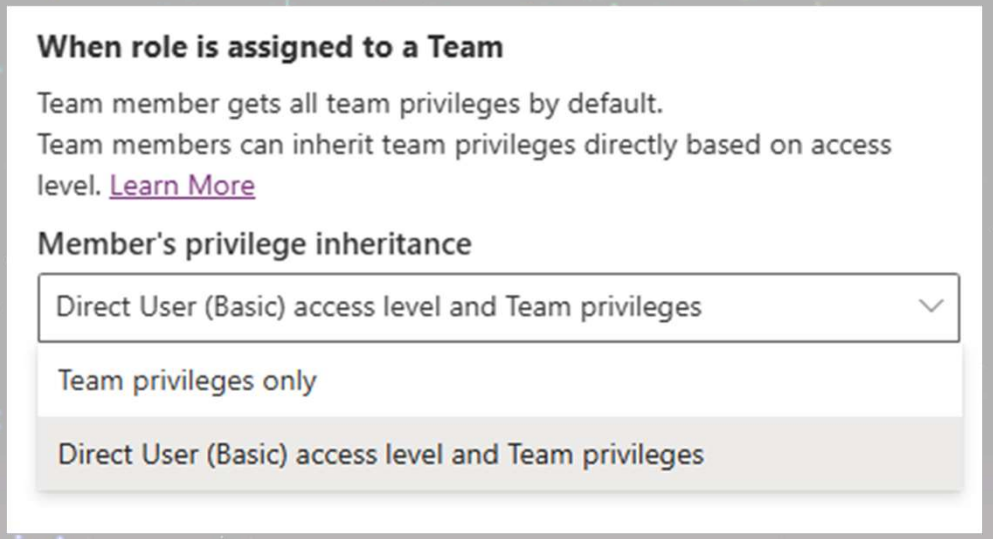
- A Team is a group of users
- Assigned to a specific Business Unit
- Default Queue is created for the Team
- Security Roles can be assigned to a team

- Types
  - Owner: Team can own rows
  - Access: Facilitates easier sharing of rows
  - AAD Security Group / AAD Office Group: Links your Dynamics security with Active Directory



Team Roles and Inheritance

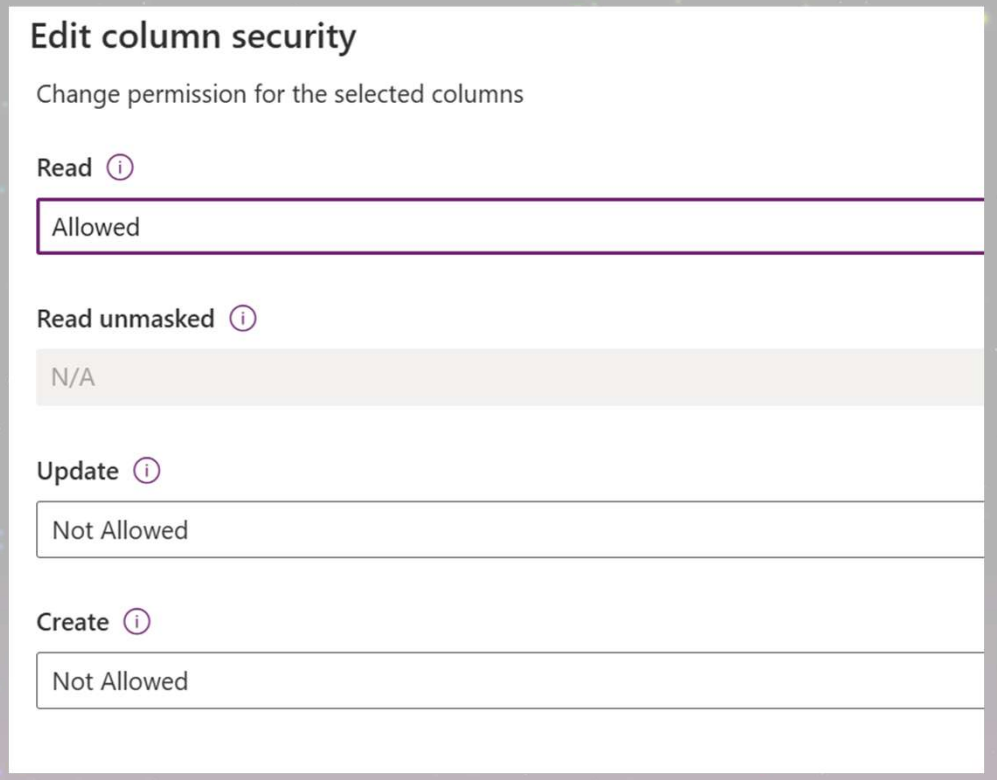
- Easy to manage security for a group
- Settings may grant the team roles to the user
  - Direct User (default): User has that role for themselves and the Team.
  - Team Only: The role only is only effective for that team.
- Ex. Role assigned at team with User read access to Accounts. User can see Accounts owned by the Team or owned by themselves (the user)



Additional Security

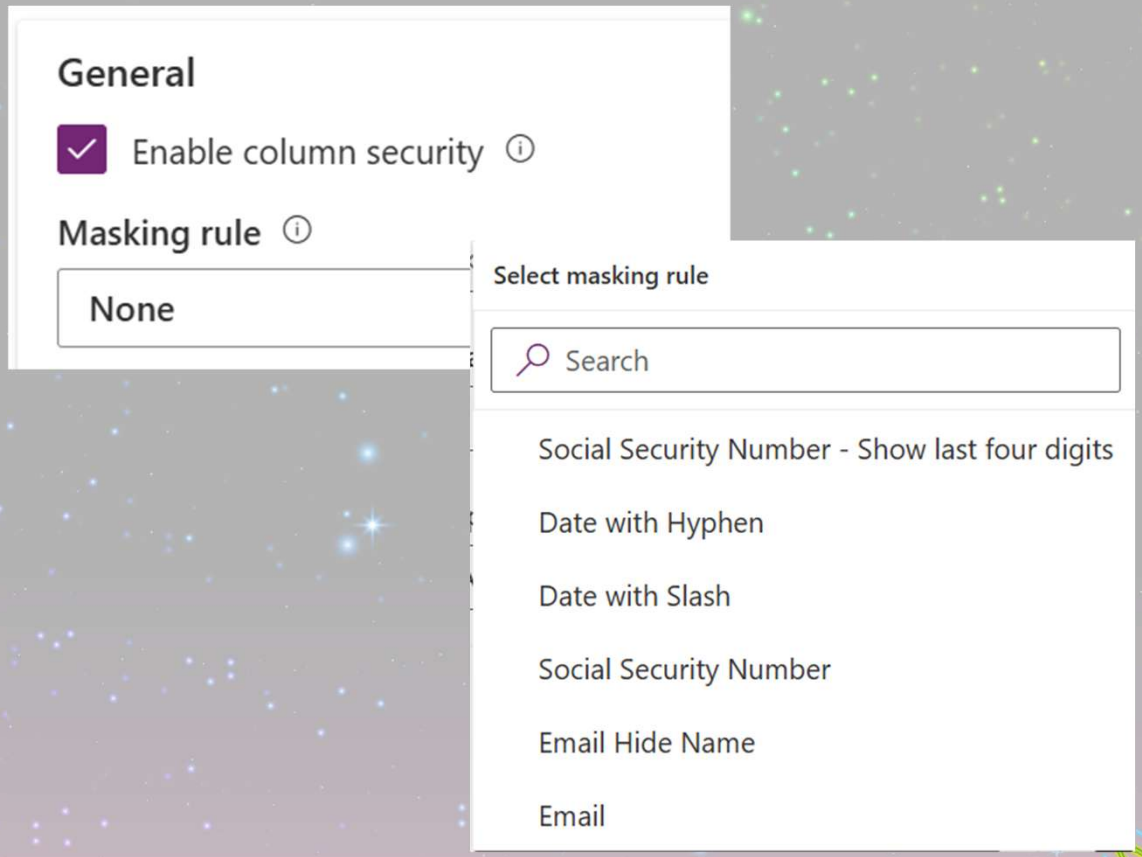
Column Level Security

- If this isn't enough, we can lock specific Columns down with Column Level Security
- Steps:
  - Enable Column Level Security on the Column
  - Create/Modify Column Security ProfileAdd users or Teams
- For each Column you set if they can Read, Update, and/or Create
- Users with System Administrator will automatically have full access to all Columns
- Potential for performance impact if used too frequently



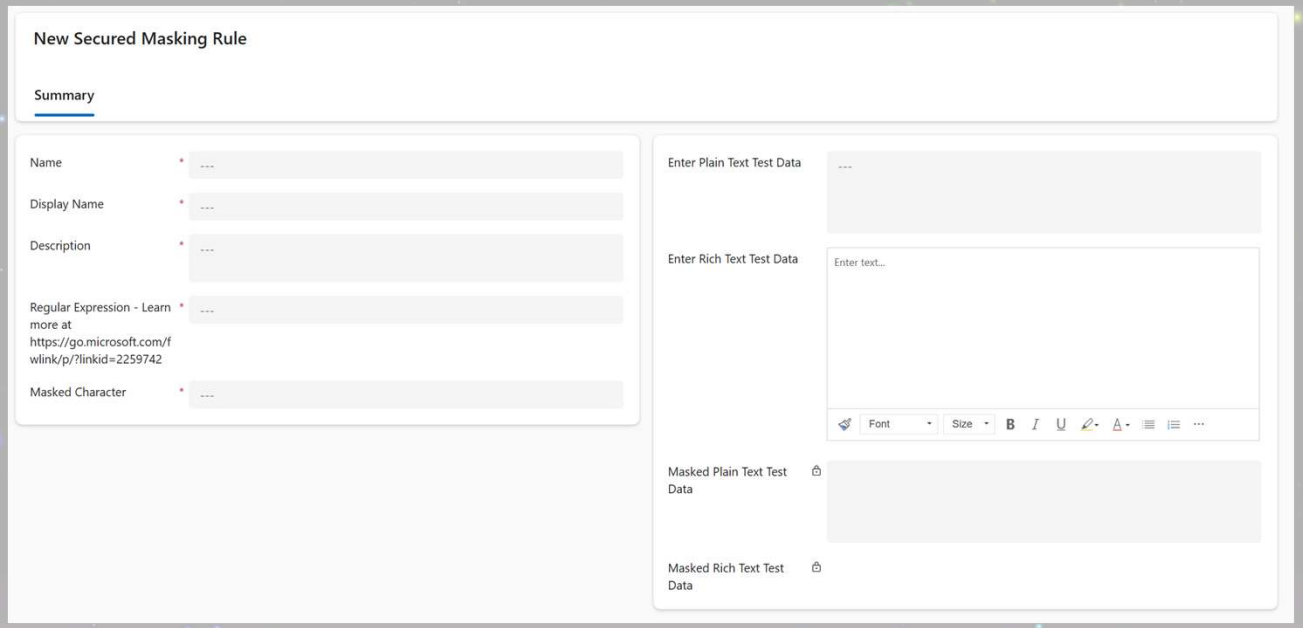
Column Masking Rule

- Permissions
  - Read (Masked Values)
  - Read Unmasked
    - Not Allowed
    - One Record
    - All Records
  - Create
  - Update



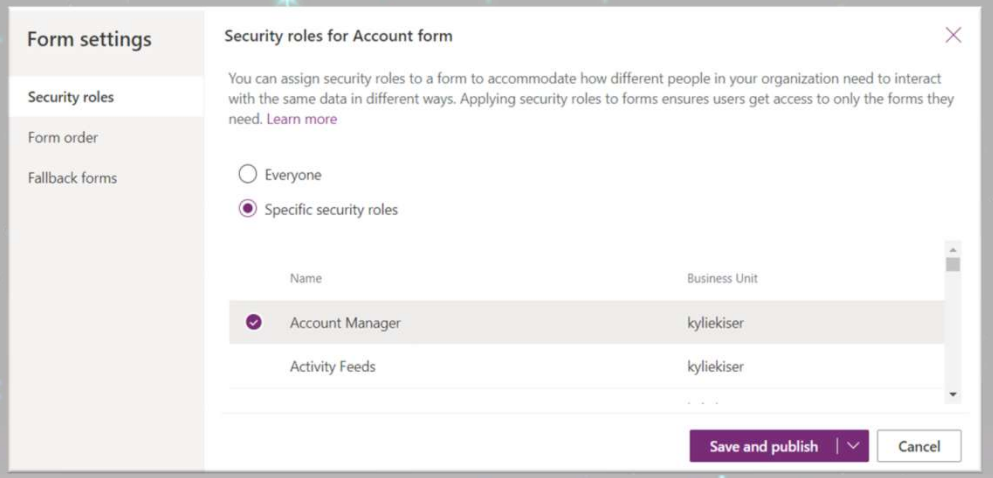
Secured Masking Rule

- Requires Managed Environment
- Use Regular Expressions to identify patterns
- Patterns detected and masked when the row is retrieved



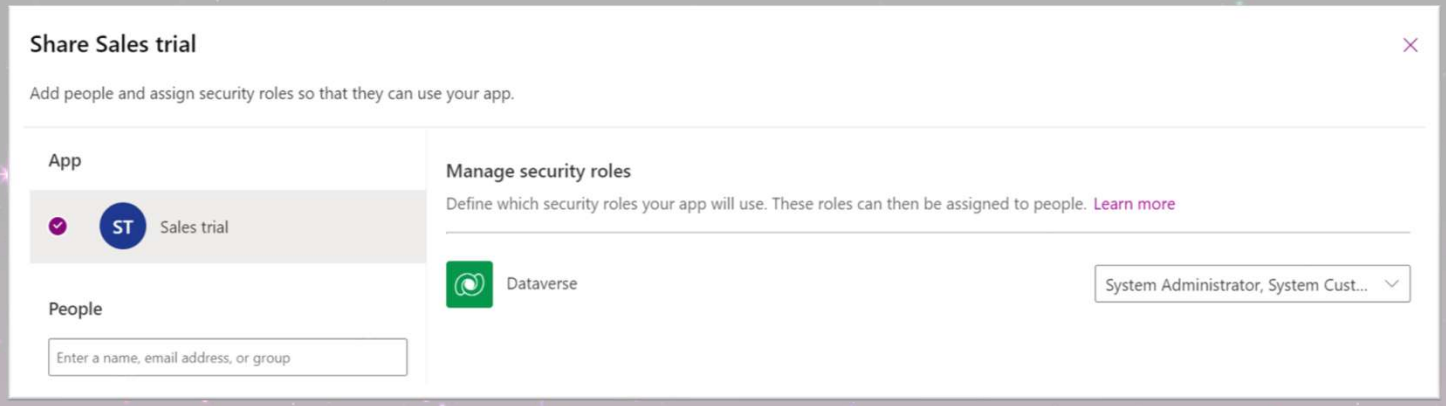
Form Security

- Select which roles can see each form
- Users can switch between all forms that are available to them
- This can be used to ensure each job function sees the most relevant information
- Data not on the form is still accessible via Advanced Find



Model Driven App

- Apps can be assigned to specific security roles as well
- Users can select between all the apps they have access to
- Within the app, the user still requires access to the Tables, forms, etc. that are included



Business Process Flows

- Access to Business Process Flows is granted via Security Role
- Users additionally need access to the Tables involved
- If multiple are available, configure order for them to be applied. User can switch the process as needed.

Table ↑		Name	Record owner...	Permission ...	Create	Read	Write	Delete	Append
Business Process Flows (2)									
New Process	...	newprocess	Organization	Full Access	Organization	Organization	Organization	Organization	Organization
Translation Process	...	translationprocess	Organization	Full Access	Organization	Organization	Organization	Organization	Organization

Other Stuff

2026 DYNAMICS CON

Environment Groups

Assign an Environment Group to each of your environments

Ensure that only users who need access have access

Create different groups for different environments

Sharing and Access Teams

Individual rows can be shared to grant access to other users

Access Teams are a method of sharing specific permissions quickly

This cannot be used to give access to Tables or Columns that the receiving user does not have

Sharing is not an effective security strategy and can be difficult to control and manage

Hierarchical Security

For more complex scenarios, security can be configured based on position or hierarchy

Manager hierarchy

Position hierarchy

An individual will have access to their own rows, the manager can see the rows for those they manage, etc.

A user can Read all data available to all reports in their hierarchy.

A user can Write / Append rows for their direct reports.

Thank You!

Ask Questions at
the Expert Booth!
Thursday
9-10 AM

Connect with me!
Kylie Kiser
Kylie K Consulting
Me@KylieKiser.com


2026
DYNAMICS
CON
Vegas