



Microsoft Power Platform CONFERENCE

POWER BI

POWER AUTOMATE

POWER APPS

POWER VIRTUAL AGENTS

POWER PAGES

Introduction to Dataverse Security

Kylie Kiser

Kylie.Kiser@RSMCanada.com





The official event app for the **Microsoft Power Platform Conference – Fall 2023**



Join the event app to access:

- ➔ Event announcements
- ➔ Personalized agenda, session details
- ➔ Speaker & attendee profiles
- ➔ Networking, meet-ups, messages
- ➔ Event documents

Event Invitation Code:
PPCFall2023

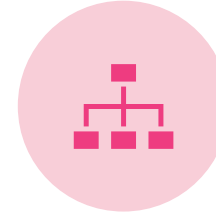
Agenda



WHERE DO I
START?



SECURITY
ROLES



BUSINESS
UNITS



TEAMS



ADDITIONAL
SECURITY



OTHER
STUFF

Kylie Kiser

5x Microsoft Business Applications MVP

Solution Architect, Dynamics 365 CE at
RSM Canada

10+ Years working with Dynamics and
the Power Platform

Washington, DC User Group Chapter
Leader



KylieKiser.com



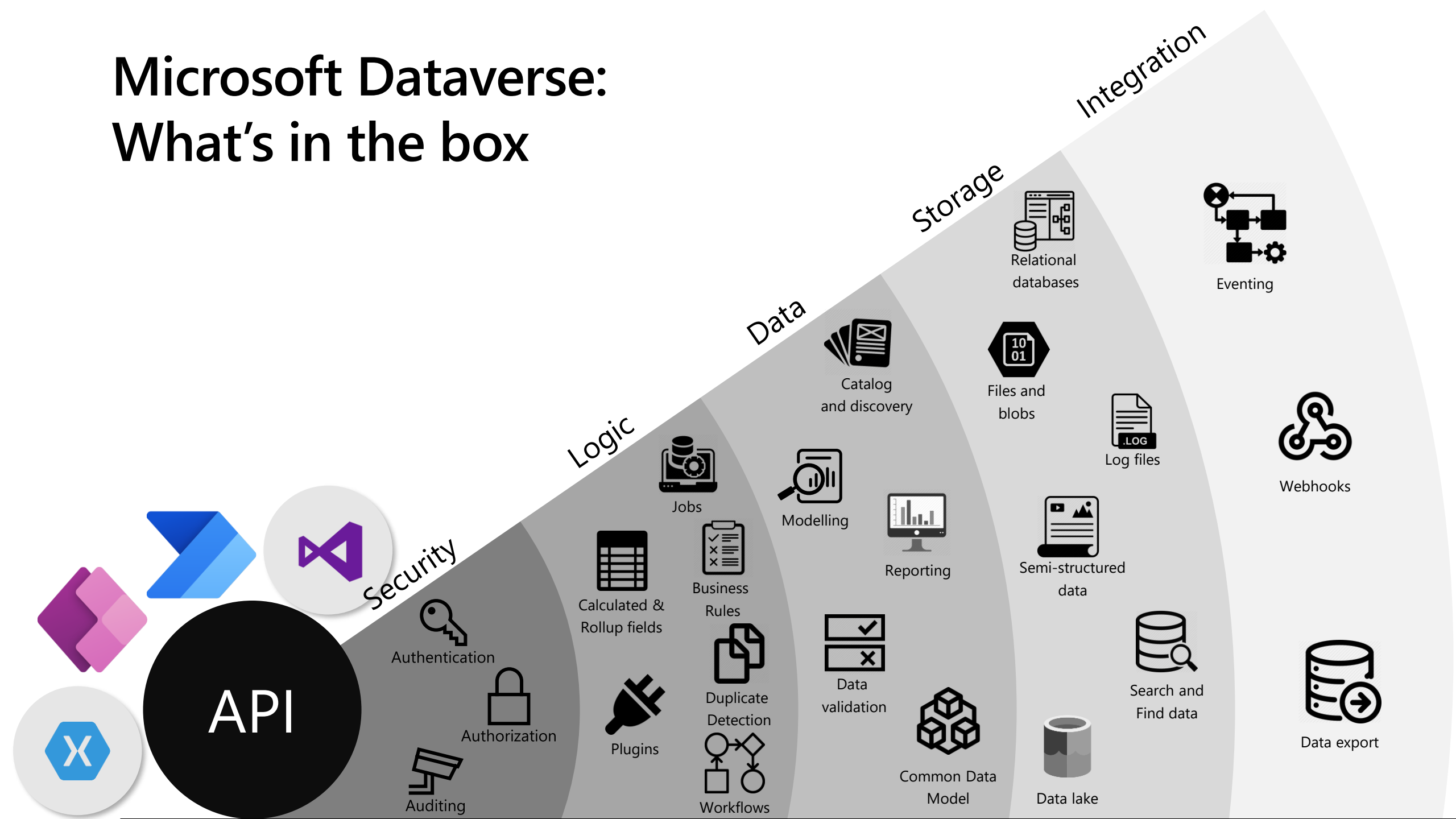
[@KylieKiser](https://twitter.com/KylieKiser)



Youtube.com/KylieKiserPowerPlatform



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

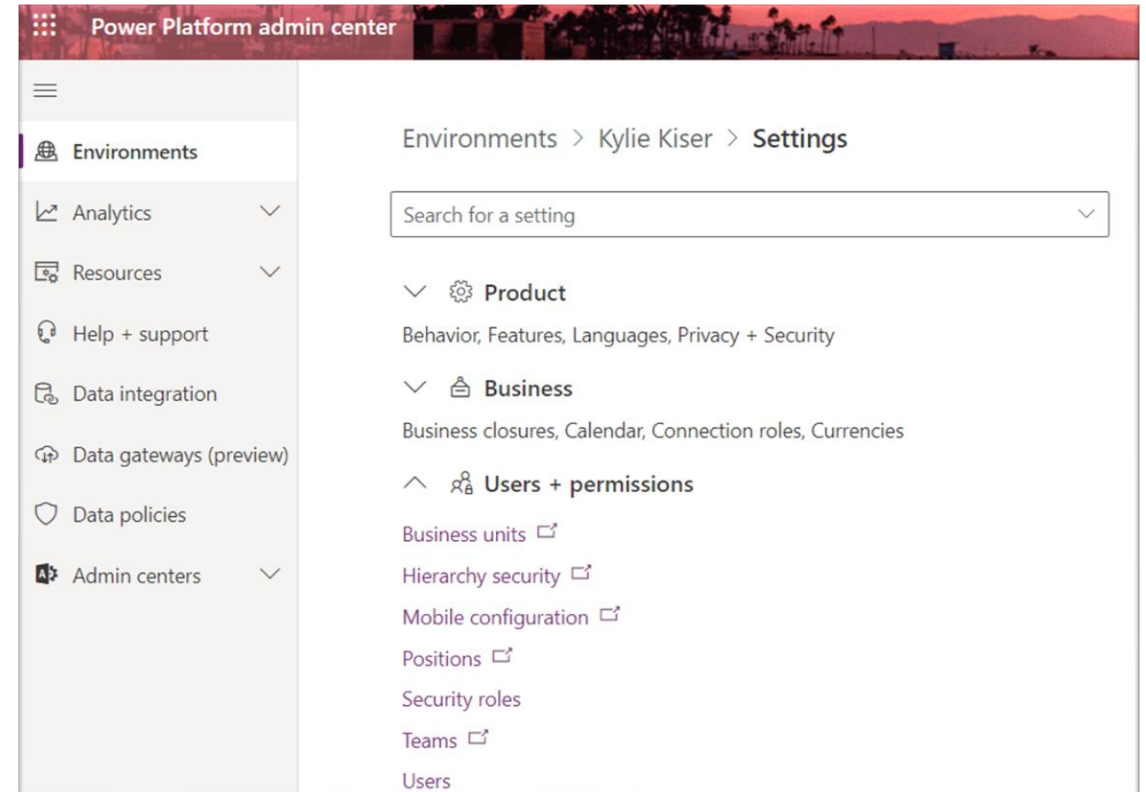
Security decisions can quickly cause performance and usability issues



Where do I look?

Power Platform Admin Center:
aka.ms/ppac

Select Environment >
Settings >
Users + Permissions



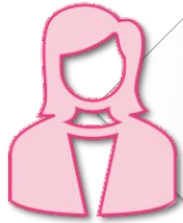
Quick Reminders

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

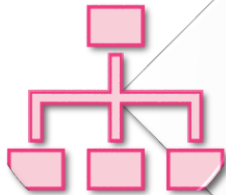
**Security by Obscurity is not
security. Be aware that just
because someone can't see
data on a form, they may
still be able to still find it.**

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?

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

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

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

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

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

Security Role: Salesperson Working on solution: Default Solution

| Entity | Create | Read | Write | Delete | Append | Append To | Assign | Share |
|--------------|--------|------|-------|--------|--------|-----------|--------|-------|
| Account | | | | | | | | |
| ACViewMapper | | | | | | | | |

Key

| | | | | |
|---------------|------|---------------|------------------------------|--------------|
| None Selected | User | Business Unit | Parent: Child Business Units | Organization |
|---------------|------|---------------|------------------------------|--------------|



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



Key

○ None Selected

👤 User

🏢 Business Unit

🌳 Parent: Child Business Units

🌐 Organization

Miscellaneous Permissions

Additional permissions that can be either On or Off

Miscellaneous Privileges

| | | | |
|---|-----------------------|--|-----------------------|
| Add Reporting Services Reports | <input type="radio"/> | Bulk Delete | <input type="radio"/> |
| Delete Audit Partitions | <input type="radio"/> | Delete Audit Record Change History | <input type="radio"/> |
| Manage Data Encryption key - Activate | <input type="radio"/> | Manage Data Encryption key - Change | <input type="radio"/> |
| Manage Data Encryption key - Read | <input type="radio"/> | Manage User Synchronization Filters | <input type="radio"/> |
| Promote User to Microsoft Dynamics 365 Administrator Role | <input type="radio"/> | Publish Duplicate Detection Rules | <input type="radio"/> |
| Publish Email Templates | <input type="radio"/> | Publish Mail Merge Templates to Organization | <input type="radio"/> |
| Publish Reports | <input type="radio"/> | Run SharePoint Integration Wizard | <input type="radio"/> |
| Turn On Tracing | <input type="radio"/> | View Audit History | <input type="radio"/> |
| View Audit Partitions | <input type="radio"/> | View Audit Summary | <input type="radio"/> |



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



DELETE TO ANY ROWS



BULK DELETE



CREATE QUICK CAMPAIGN



EXPORT TO EXCEL



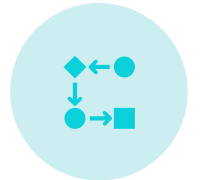
BULK EDIT



SEND EMAIL AS ANOTHER USER



ACT ON BEHALF OF ANOTHER USER



PROCESS CREATION



Modern Security Role Editor

Tables Miscellaneous privileges Privacy-related privileges

Show only assigned tables

Compact Grid View ☒ On

| Table ↑ | | Name | Record owner... | Permission Se... | Create | Read | Write | Dele |
|-------------------|---------------------------|------|------------------------|------------------|-----------|------|--------------|--------------|
| Core Records (48) | | | | | | | | |
| | ACIViewMapper | ... | aciviewmapper | Organization | Reference | None | Organization | None |
| ✓ | Account | ... | account | User or Team | Custom | User | Organization | Organization |
| | Action Card | ... | actioncard | User or Team | Custom | User | User | User |
| | Action Card User Settings | ... | actioncardusersettings | User or Team | Private | User | User | User |





Modern Security Role Editor

Allows you to see only tables with privileges Assigned

Allows you to search for tables and privileges

Modify columns to focus on the items you want to review

Does not allow clicking on a row or column to change all permissions

Special Security Roles

There are a few *special* roles that users may need to access specific functionality

- Ex. Dynamics 365 App for Outlook User

Roles for ISV/Partner solutions

- **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

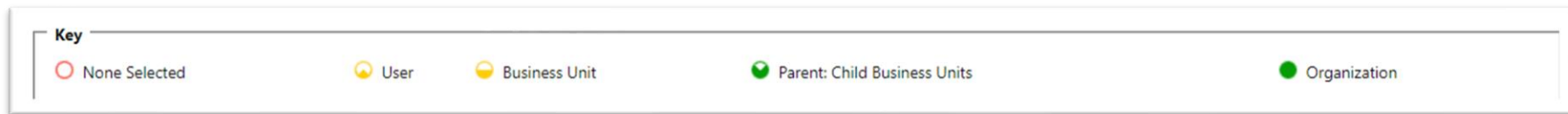
Defining Your Structure

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

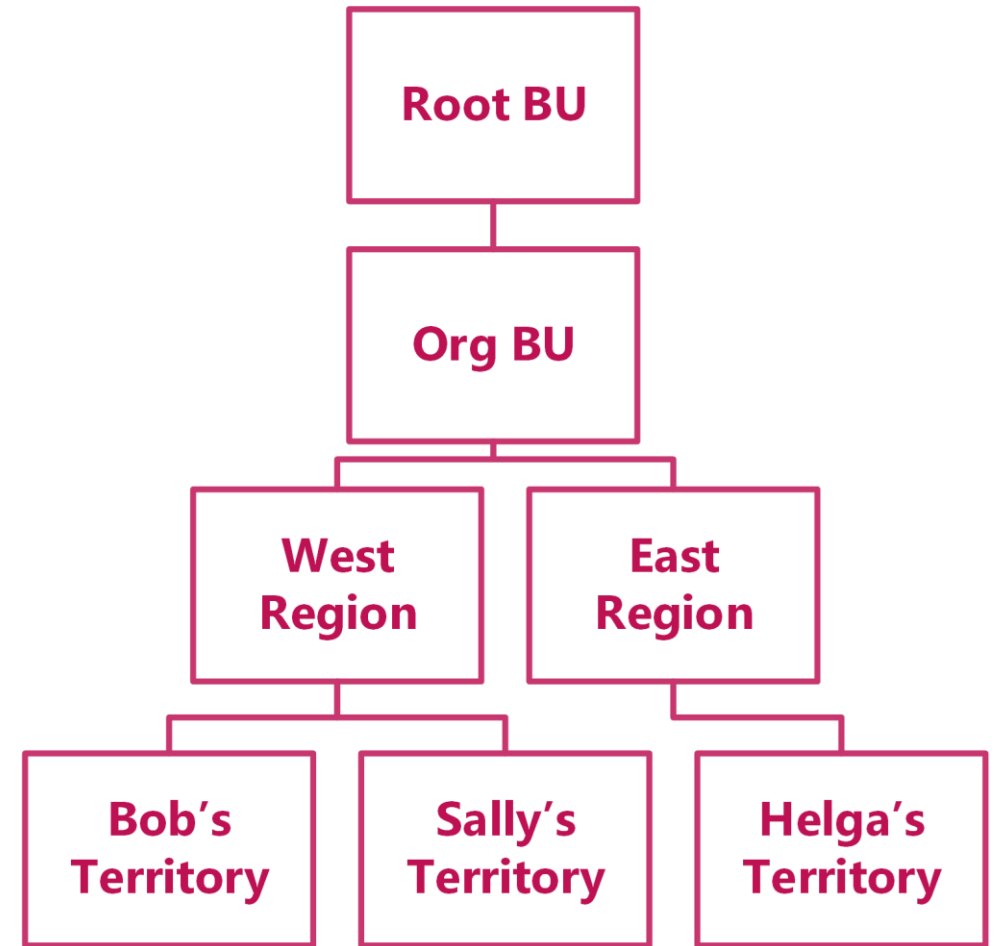


Example Business Unit Structure

Where should Marketing live?

How do we configure management?

What about support staff? Are they dedicated to a territory or region? All the time?



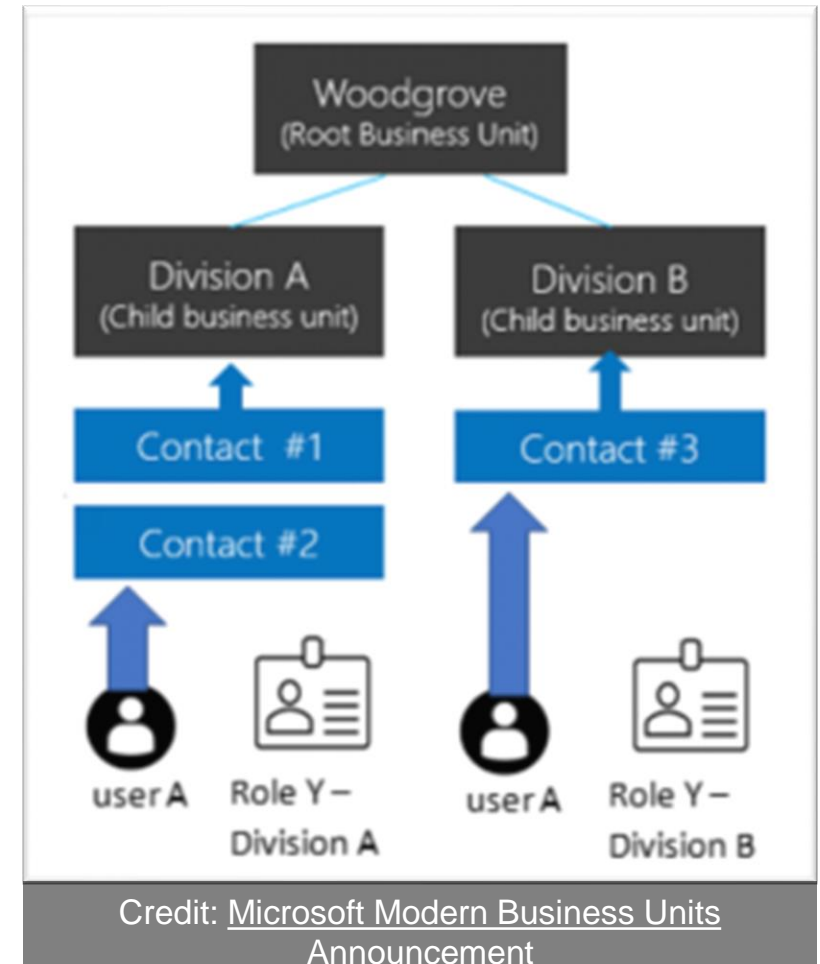
Modern Business Units

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



The screenshot shows the 'West Region Team' configuration page. It has tabs for 'General' and 'Related'. Under 'General', there are fields for 'Team Name*' (set to 'West Region Team'), 'Business Unit*' (set to 'West Region'), 'Administrator*' (set to 'Kylie Kiser'), 'Team Type*' (set to 'Owner'), and 'Azure AD Object Id for a group' (set to '---').

The screenshot shows the 'Team Type*' dropdown menu. The current selection is 'Owner'. The dropdown list includes the following options: '--Select--', 'Owner' (highlighted), 'Access', 'AAD Security Group', and 'AAD Office Group'.

Team Roles and Inheritance

Easy to manage security for a group

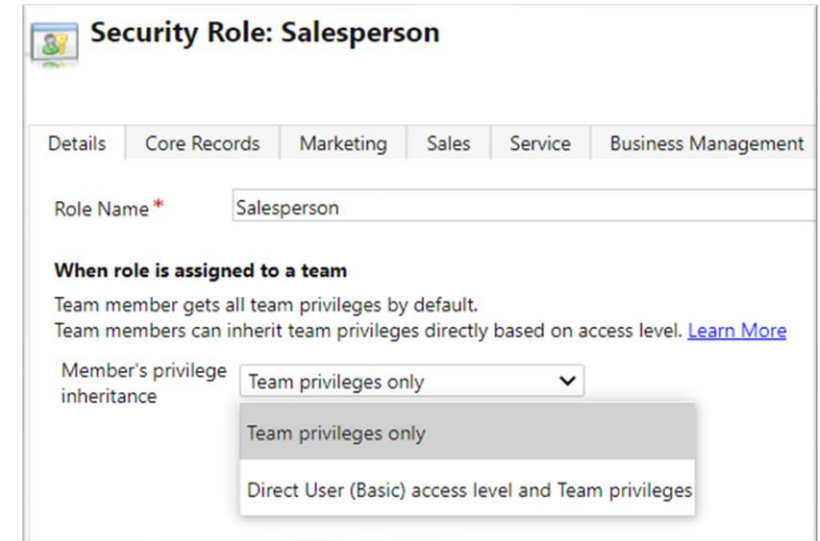
Settings may grant the team roles to the user

- 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)

Documentation:

<https://link.kyliekiser.com/SecurityRoles>



Security Role: Salesperson

Details Core Records Marketing Sales Service Business Management

Role Name * Salesperson

When role is assigned to a team

Team member gets all team privileges by default.
Team members can inherit team privileges directly based on access level. [Learn More](#)

Member's privilege inheritance Team privileges only

- Team privileges only
- Direct User (Basic) access level and Team privileges



Additional Security

Field Level Security

If this isn't enough, we can lock specific Columns down with Field Level Security

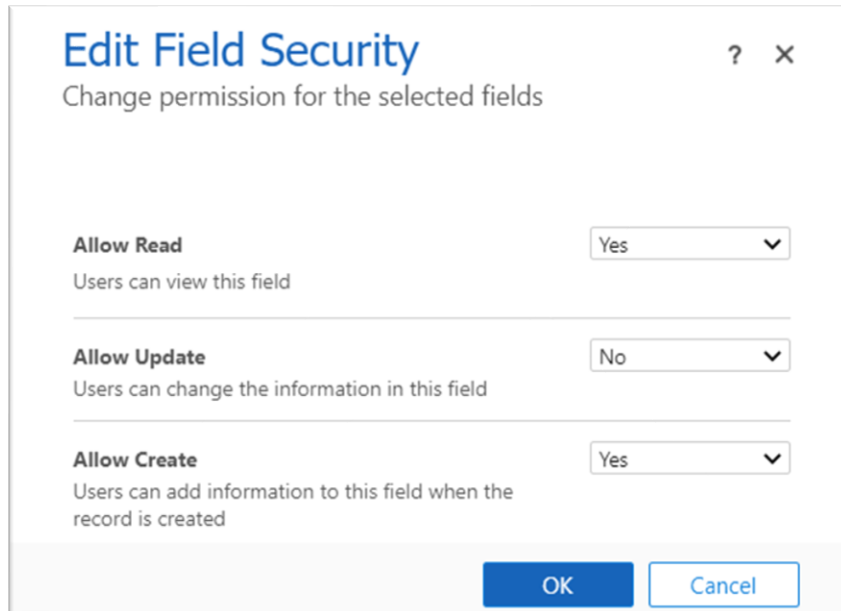
Steps:

- Enable Field Level Security on the Column
- Create/Modify Field Security Profile (classic interface)
- Add 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



Edit Field Security ? x

Change permission for the selected fields

Allow Read Yes ▼
Users can view this field

Allow Update No ▼
Users can change the information in this field

Allow Create Yes ▼
Users can add information to this field when the record is created

OK Cancel

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

Form settings

Security roles

Form order

Fallback forms

Security roles for Account form

You can assign security roles to a form to accommodate how different people in your organization need to interact with the same data in different ways. Applying security roles to forms ensures users get access to only the forms they need. [Learn more](#)

☐ Everyone

☒ Specific security roles

| Name | Business Unit |
|---|---------------|
| <input checked="" type="checkbox"/> Account Manager | kyliekiser |
| Activity Feeds | kyliekiser |
| ... | |

Save and publish | v

Cancel

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

Share Sales trial

Add people and assign security roles so that they can use your app.

App

✓


ST

Sales trial

People

Manage security roles

Define which security roles your app will use. These roles can then be assigned to people. [Learn more](#)

 Dataverse

System Administrator, System Cust... ▼




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.

Overview documentation: <https://link.kyliekiser.com/BPF>

|  Security Role: Salesperson | | | | | | | | |
|---|--------------|-----------|-------|---------|---------------------|--------------------|---------------|------------------|
| Details | Core Records | Marketing | Sales | Service | Business Management | Service Management | Customization | Missing Entities |
| Entity | Create | Read | Write | Delete | Append | Append To | Assign | Share |
| Expired Process | ● | ● | ● | ● | ● | ● | | |
| Lead To Opportunity Sales Process | ● | ● | ● | ● | ● | ● | | |
| Purchase Order Business Process | ○ | ○ | ○ | ○ | ○ | ○ | | |
| CFS - IoT Alert Process Flow | ○ | ○ | ○ | ○ | ○ | ○ | | |



Other Stuff

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

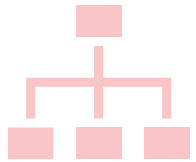
Access Teams are a method of sharing specific permissions quickly

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

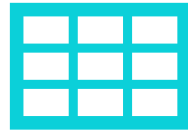


Hierarchical Security



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.



Additional documentation:
<https://link.kyliekiser.com/PositionSecurity>



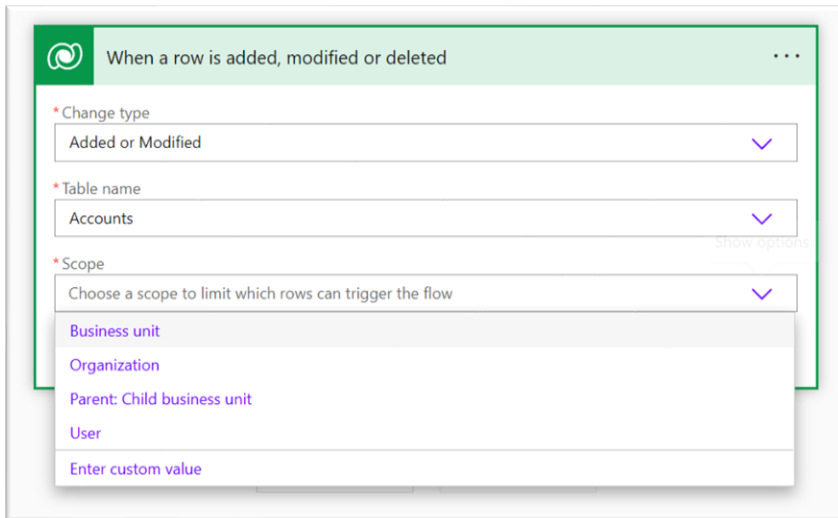
Process Security

Workflows, Business Rules, Plugins, and Power Automate all introduce automation that can affect your entire organization.

- Current user vs Specific user

Recommendation: Unless there's a specific need, processes should run as the current user to enforce security roles restrictions.

Use scope to determine which rows are impacted by the processes.



The screenshot shows the configuration interface for a trigger in Power Automate. The title bar reads "When a row is added, modified or deleted". The configuration is divided into three sections:

- * Change type:** A dropdown menu with "Added or Modified" selected.
- * Table name:** A dropdown menu with "Accounts" selected. A "Show options" link is visible to the right.
- * Scope:** A dropdown menu with the text "Choose a scope to limit which rows can trigger the flow". The dropdown is open, showing the following options:
 - Business unit
 - Organization
 - Parent: Child business unit
 - User
 - Enter custom value

Next Steps

Resources

Overview of Dataverse Security: <https://link.kyliekiser.com/Overview>

Security Concepts: <https://link.kyliekiser.com/SecurityConcepts>

Security Roles: <https://link.kyliekiser.com/SecurityRoles>

Field Level Security: <https://link.kyliekiser.com/FLS>

Model Driven App Security: <https://link.kyliekiser.com/MDA>

Environment Security: <https://link.kyliekiser.com/EnvRoles>

Security Groups and Licenses: <https://link.kyliekiser.com/SecurityGroups>

Hierarchy and Position Security: <https://link.kyliekiser.com/PositionSecurity>

CoE Starter Kit: <https://link.kyliekiser.com/CoE>

Deep Dive into Security mechanisms and performance impacts with Marco Amoedo:
<https://link.kyliekiser.com/Marco>

DynamicsCon Best Practices for Dynamics 365 CE Security Design with Kelsey Carrier:
<https://link.kyliekiser.com/Kelsey>



Connect with Me!

Kylie Kiser



RSM Booth #201



[LinkedIn.com/KylieKiser](https://www.linkedin.com/KylieKiser)



KylieKiser.com

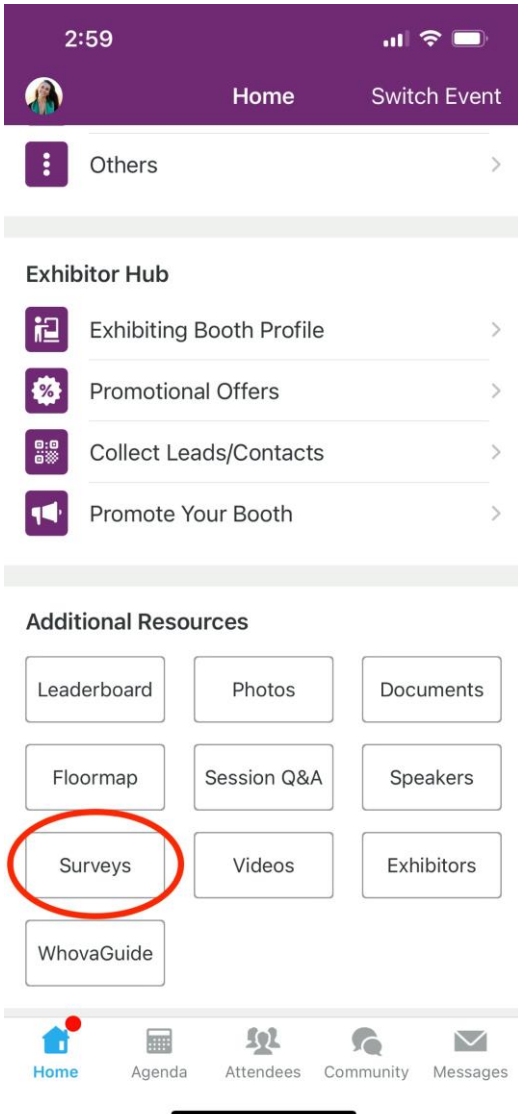


[@KylieKiser](https://twitter.com/KylieKiser)



Youtube.com/KylieKiserPowerPlatform





Session Feedback Surveys

We really want to hear from YOU!

In the pursuit of making next year's Microsoft Power Platform Conference even better, we want to hear your feedback about this session.

Here's How -

- *Simply go to the Whova App on your smartphone*
- *Scroll down on the Microsoft Power Platform Conference Homepage to 'Additional Resources' to click "Surveys".*
- *Click Session Feedback.*
- *Scroll down to find this session title.*
- *Complete the session feedback survey.*
- *Finally, click 'Submit'*

It's just that easy!



Microsoft 365 CONFERENCE

ORLANDO, FLORIDA

APRIL 30, MAY 1 & 2, 2024

Workshops: April 28, 29 & May 3

WALT DISNEY WORLD

Swan & Dolphin Resort

FEATURING:



JEFF TEPER

*President – Microsoft
Collaborative Apps and
Platforms, Microsoft*



KARUANA GATIMU

*Principal Manager, Customer
Advocacy Group Microsoft
Teams Engineering, Microsoft*



ADAM HARMETZ

*Vice President of Product
Management, Microsoft
365, Microsoft*



NAOMI MONEYPENNY

*Director of Product
Development, Viva, Microsoft*

AND MANY MORE!

Microsoft Data & AI CONFERENCE

Join us in
LAS VEGAS

December 12-14, 2023
Workshops 10, 11 & 15

REGISTER TODAY

 MSDataAIconf.com

 [@MSDataAIconf](https://twitter.com/MSDataAIconf)



ARUN ULAGARATCHAGAN

*Corporate Vice President,
Azure Data, Microsoft*



AMIR NETZ

*Technical Fellow and CTO of
Microsoft Fabric, Microsoft*



JESSICA HAWK

*Corporate Vice President Data,
AI, MR Product Marketing,
Microsoft*



ERIC BOYD

*Corporate Vice President AI
Platform, Microsoft*