Securing Model-Driven Apps 🔐

All-In! A Deep Dive On Model-Driven Apps – Part IV

The Owner-Based Security Model 😺

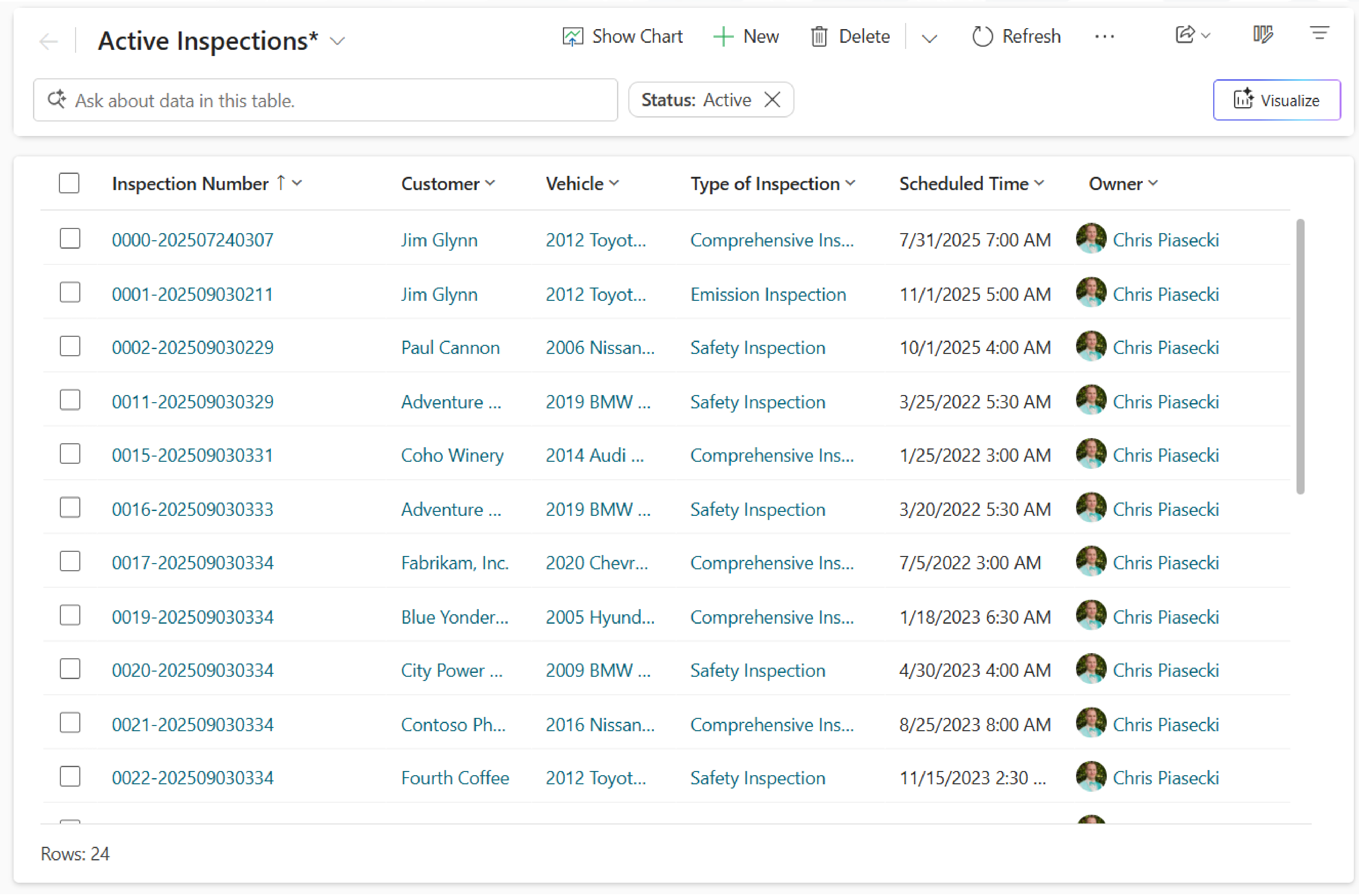
All records in Dataverse have Owner column that determines who has privileges

User

- Defaults to User who created the record
- Can be set to another value on create through automation or manually re-assigned afterwards

Team

- Contains multiple Users from the environment
- Must be set to another value on create through automation or manually re-assigned afterwards



Inspection Number	Customer	Vehicle	Type of Inspection	Scheduled Time	Owner
0000-202507240307	Jim Glynn	2012 Toyot...	Comprehensive Ins...	7/31/2025 7:00 AM	Chris Piasecki
0001-202509030211	Jim Glynn	2012 Toyot...	Emission Inspection	11/1/2025 5:00 AM	Chris Piasecki
0002-202509030229	Paul Cannon	2006 Nissan...	Safety Inspection	10/1/2025 4:00 AM	Chris Piasecki
0011-202509030329	Adventure ...	2019 BMW ...	Safety Inspection	3/25/2022 5:30 AM	Chris Piasecki
0015-202509030331	Coho Winery	2014 Audi ...	Comprehensive Ins...	1/25/2022 3:00 AM	Chris Piasecki
0016-202509030333	Adventure ...	2019 BMW ...	Safety Inspection	3/20/2022 5:30 AM	Chris Piasecki
0017-202509030334	Fabrikam, Inc.	2020 Chevr...	Comprehensive Ins...	7/5/2022 3:00 AM	Chris Piasecki
0019-202509030334	Blue Yonder...	2005 Hyund...	Comprehensive Ins...	1/18/2023 6:30 AM	Chris Piasecki
0020-202509030334	City Power ...	2009 BMW ...	Safety Inspection	4/30/2023 4:00 AM	Chris Piasecki
0021-202509030334	Contoso Ph...	2016 Nissan...	Comprehensive Ins...	8/25/2023 8:00 AM	Chris Piasecki
0022-202509030334	Fourth Coffee	2012 Toyot...	Safety Inspection	11/15/2023 2:30 ...	Chris Piasecki

Rows: 24

Security Roles

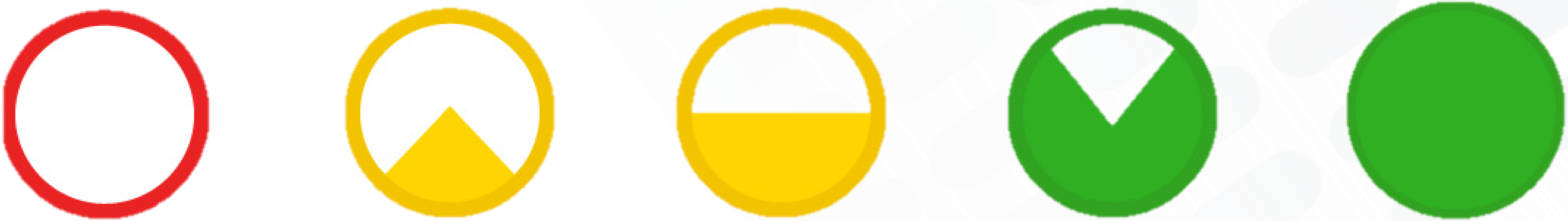
Grant privileges to tables and Dataverse features when assigned to a User

Read	Can I view the record?
Create	Can I create a new record in the table?
Write	Can I update a record?
Delete	Can I remove a record?
Append	Can I relate a record to a Parent record?
Append To	Can I relate a Child record to a record?
Assign	Can I change a record’s Owner?
Share	Can I share a record with another User?

Access-Levels 🪜

Every privilege has an access level assigned to determine who can perform the privilege

I can **UPDATE** a record when... 🤔 💭



None

Actually, I can't

User

I own the record

Business Unit

I belong to the owning business unit

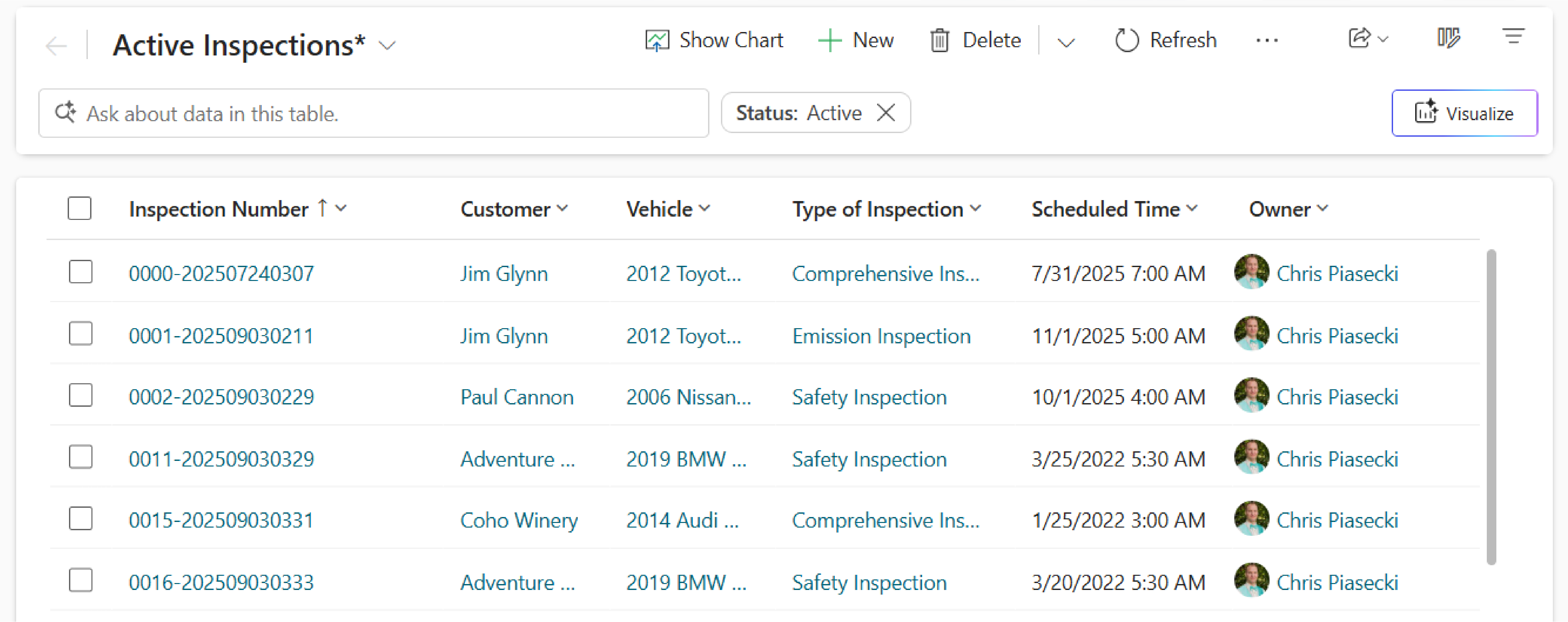
Child B.U.

I belong to a Child B.U. of an owning Parent B.U.

Organization

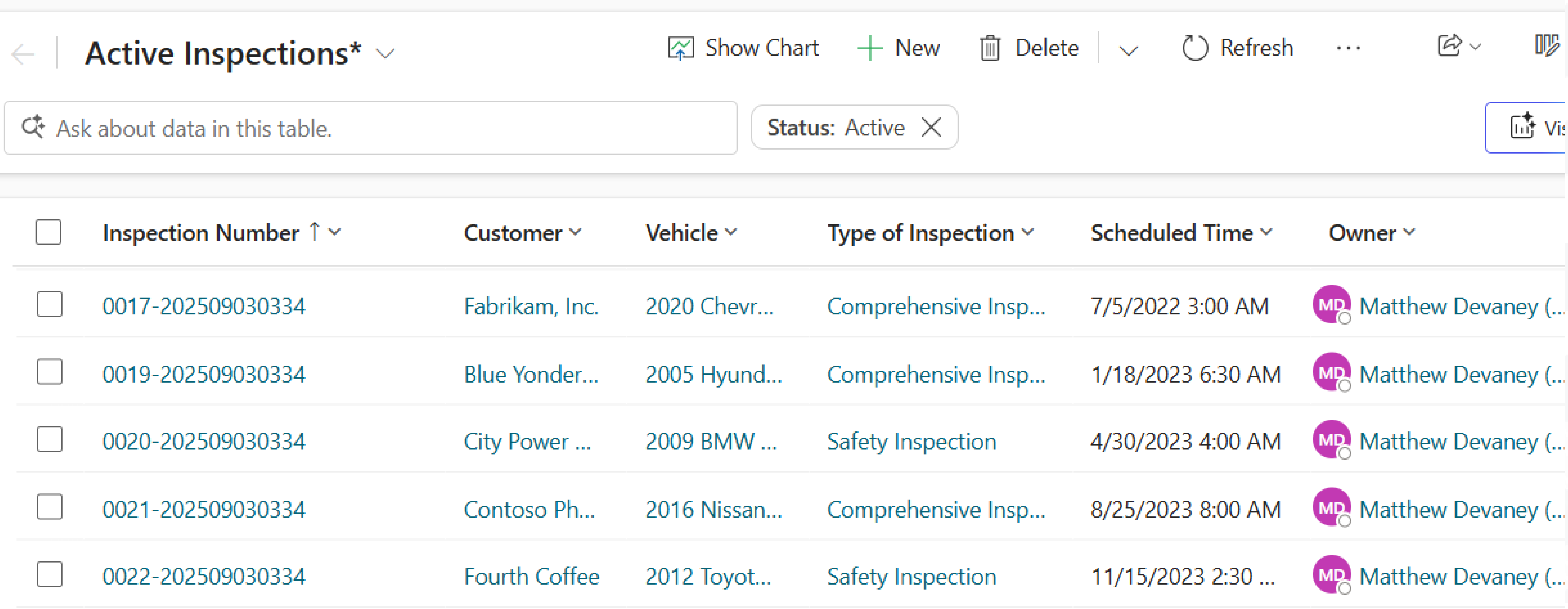
Anyone owns the record

Chris’s security role has **user read permissions** for the Inspections table. He can only see the records he owns.



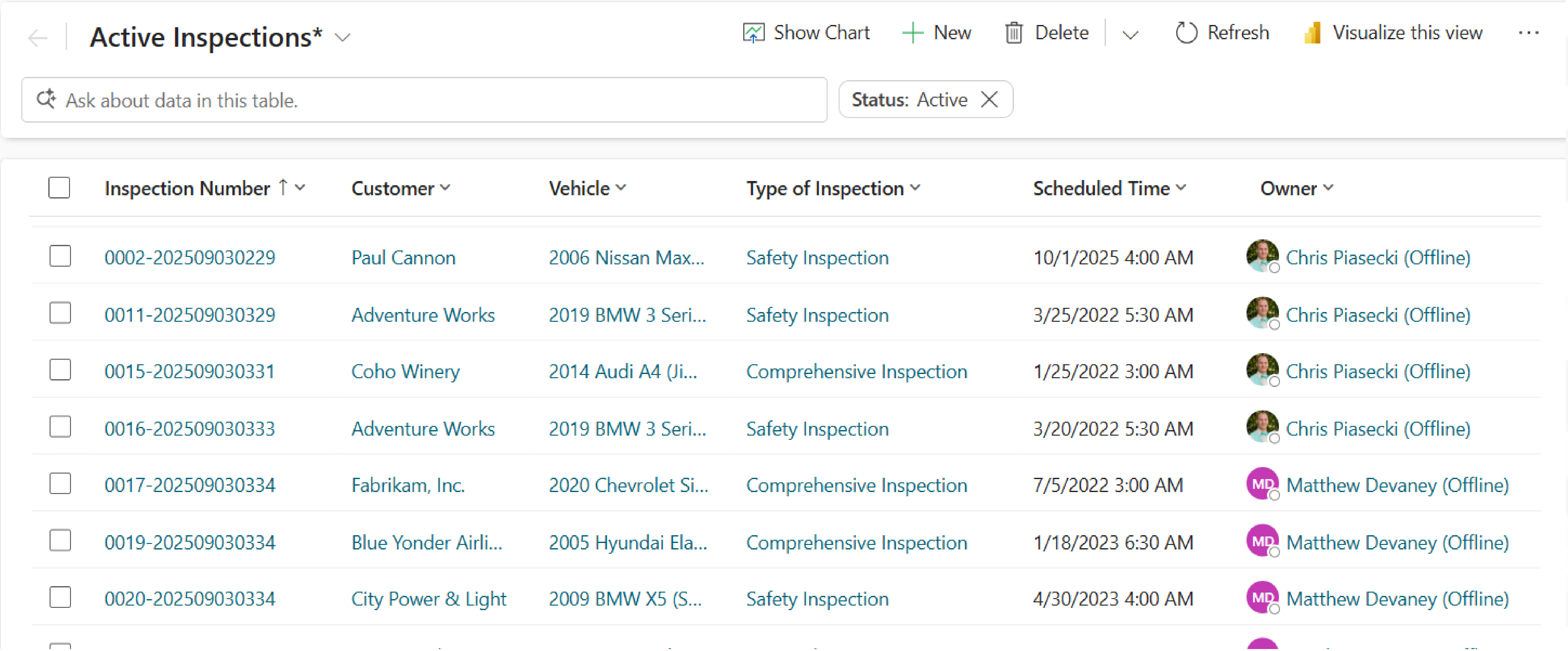
□	Inspection Number ↑	Customer	Vehicle	Type of Inspection	Scheduled Time	Owner
□	0000-202507240307	Jim Glynn	2012 Toyot...	Comprehensive Ins...	7/31/2025 7:00 AM	Chris Piasecki
□	0001-202509030211	Jim Glynn	2012 Toyot...	Emission Inspection	11/1/2025 5:00 AM	Chris Piasecki
□	0002-202509030229	Paul Cannon	2006 Nissan...	Safety Inspection	10/1/2025 4:00 AM	Chris Piasecki
□	0011-202509030329	Adventure ...	2019 BMW ...	Safety Inspection	3/25/2022 5:30 AM	Chris Piasecki
□	0015-202509030331	Coho Winery	2014 Audi ...	Comprehensive Ins...	1/25/2022 3:00 AM	Chris Piasecki
□	0016-202509030333	Adventure ...	2019 BMW ...	Safety Inspection	3/20/2022 5:30 AM	Chris Piasecki

Matthew’s security role has **user read permissions** for the Inspections table. He can only see the records he owns.

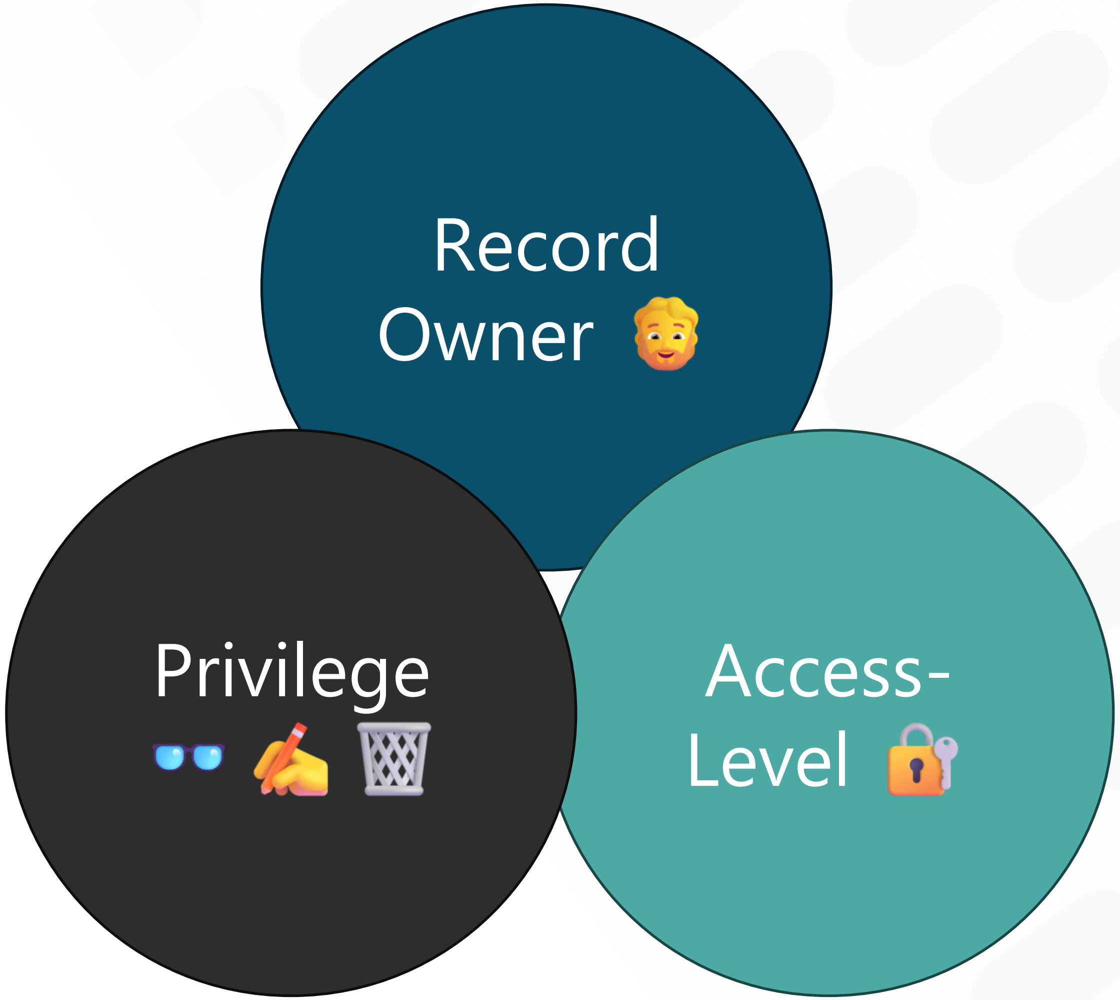


Inspection Number	Customer	Vehicle	Type of Inspection	Scheduled Time	Owner
0017-202509030334	Fabrikam, Inc.	2020 Chevr...	Comprehensive Insp...	7/5/2022 3:00 AM	Matthew Devaney (...
0019-202509030334	Blue Yonder...	2005 Hyund...	Comprehensive Insp...	1/18/2023 6:30 AM	Matthew Devaney (...
0020-202509030334	City Power ...	2009 BMW ...	Safety Inspection	4/30/2023 4:00 AM	Matthew Devaney (...
0021-202509030334	Contoso Ph...	2016 Nissan...	Comprehensive Insp...	8/25/2023 8:00 AM	Matthew Devaney (...
0022-202509030334	Fourth Coffee	2012 Toyot...	Safety Inspection	11/15/2023 2:30 ...	Matthew Devaney (...

Cat boss's security role has **organization read permissions** for the Inspections table. He can see all of records.



□	Inspection Number ↑	Customer	Vehicle	Type of Inspection	Scheduled Time	Owner
□	0002-202509030229	Paul Cannon	2006 Nissan Max...	Safety Inspection	10/1/2025 4:00 AM	Chris Piasecki (Offline)
□	0011-202509030329	Adventure Works	2019 BMW 3 Seri...	Safety Inspection	3/25/2022 5:30 AM	Chris Piasecki (Offline)
□	0015-202509030331	Coho Winery	2014 Audi A4 (Ji...	Comprehensive Inspection	1/25/2022 3:00 AM	Chris Piasecki (Offline)
□	0016-202509030333	Adventure Works	2019 BMW 3 Seri...	Safety Inspection	3/20/2022 5:30 AM	Chris Piasecki (Offline)
□	0017-202509030334	Fabrikam, Inc.	2020 Chevrolet Si...	Comprehensive Inspection	7/5/2022 3:00 AM	MD Matthew Devaney (Offline)
□	0019-202509030334	Blue Yonder Airli...	2005 Hyundai Ela...	Comprehensive Inspection	1/18/2023 6:30 AM	MD Matthew Devaney (Offline)
□	0020-202509030334	City Power & Light	2009 BMW X5 (S...	Safety Inspection	4/30/2023 4:00 AM	MD Matthew Devaney (Offline)



Record Owner 🧔

Privilege 👓 ✍️ 🗑️

Access-Level 🔐

Designing Security Roles

What security roles might be needed for a vehicle inspections solution?

Security Role: Vehicle Inspector Role

Vehicle Inspectors are responsible for conducting inspections on vehicles and recording their findings, but not see other User’s records. They need to access certain data to perform their duties effectively, but should not have unnecessary access to sensitive or administrative information.

Legend

○ None

◒ User

● Organization

Table	Read	Create	Write	Delete	Append	Append To	Assign	Share
Inspection	○	○	○	○	○	○	○	○
Vehicle	○	○	○	○	○	○	○	○
Vehicle Model	○	○	○	○	○	○	○	○
Account	○	○	○	○	○	○	○	○
Contact	○	○	○	○	○	○	○	○

Default Security Roles 🤵

Role Name	Description
App Opener	Has minimum privileges for common tasks. This role is primarily used as a template to create a custom security role for model-driven apps. It doesn't have any privileges to the core business tables, such as Account, Contact, and Activity. However, it has Organization-level read access to system tables, such as Process, to support reading system-supplied workflows. This security role is used when a new, custom security role is created.
Basic User	For out-of-the-box entities only, can run an app in the environment and perform common tasks on the records they own. It has privileges to the core business tables, such as Account, Contact, Activity, and Process.
Environment Maker	Can create new resources associated with an environment, including apps, connections, custom APIs, and flows using Microsoft Power Automate. However, this role doesn't have any privileges to access data in an environment. Environment makers can also distribute the apps they build in an environment to other users in your organization. They can share the app with individual users, security groups, or all users in the organization.
System Administrator	Has full permission to customize or administer the environment, including creating, modifying, and assigning security roles. Can view all data in the environment.
System Customizer	Has full permission to customize the environment. Can view all custom table data in the environment. However, users with this role can only view records that they create in Account, Contact, Activity tables.

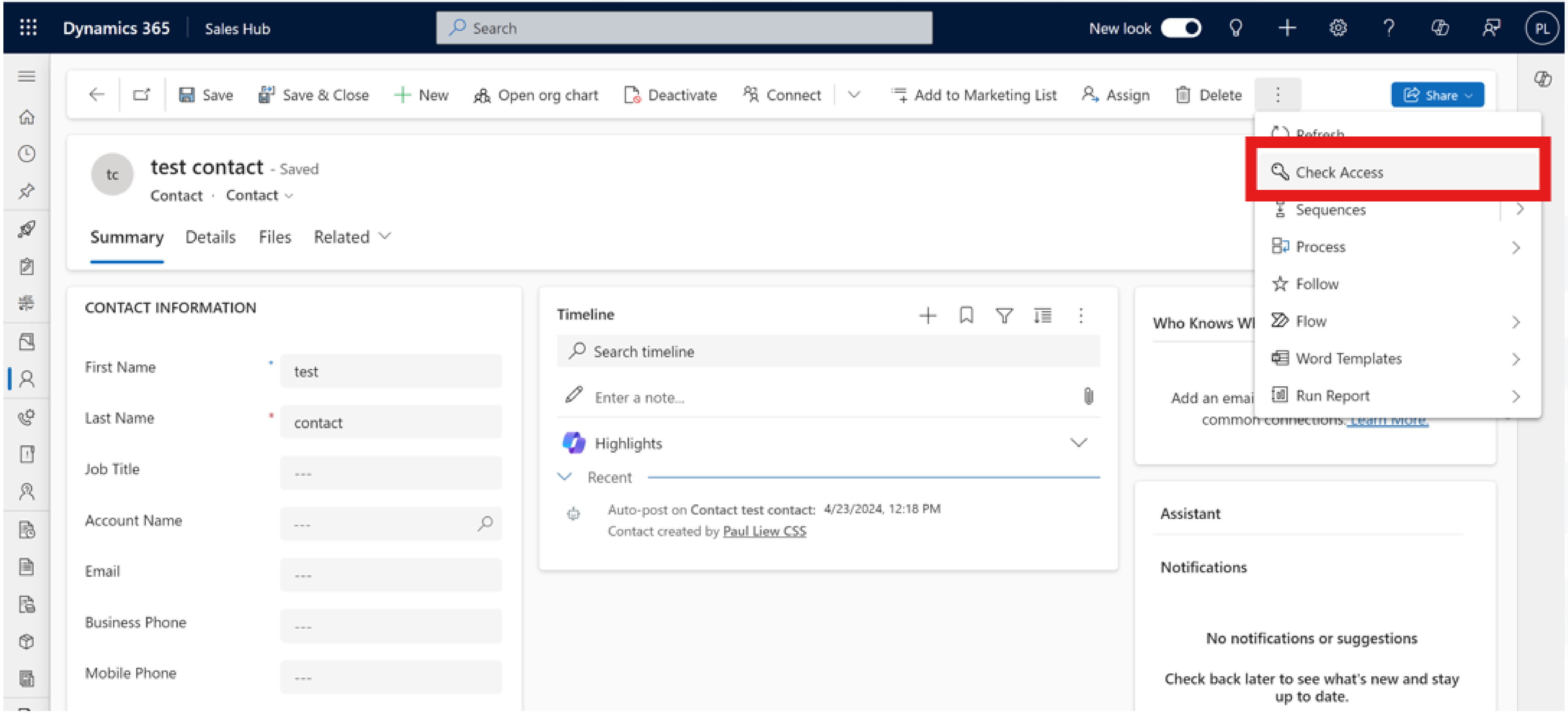
Least Privilege Access:
Grant only minimum permissions needed to perform the job

Cumulative Permissions:
User gets the highest level of permission from multiple assigned roles

Start With App Opener Role:
Use App Opener role as a starting point & customize them to fit your organization's requirements.

Check-Access To Records ☑

Make Forms and Views available based upon the User’s role



test contact - Saved

Contact · Contact

CONTACT INFORMATION

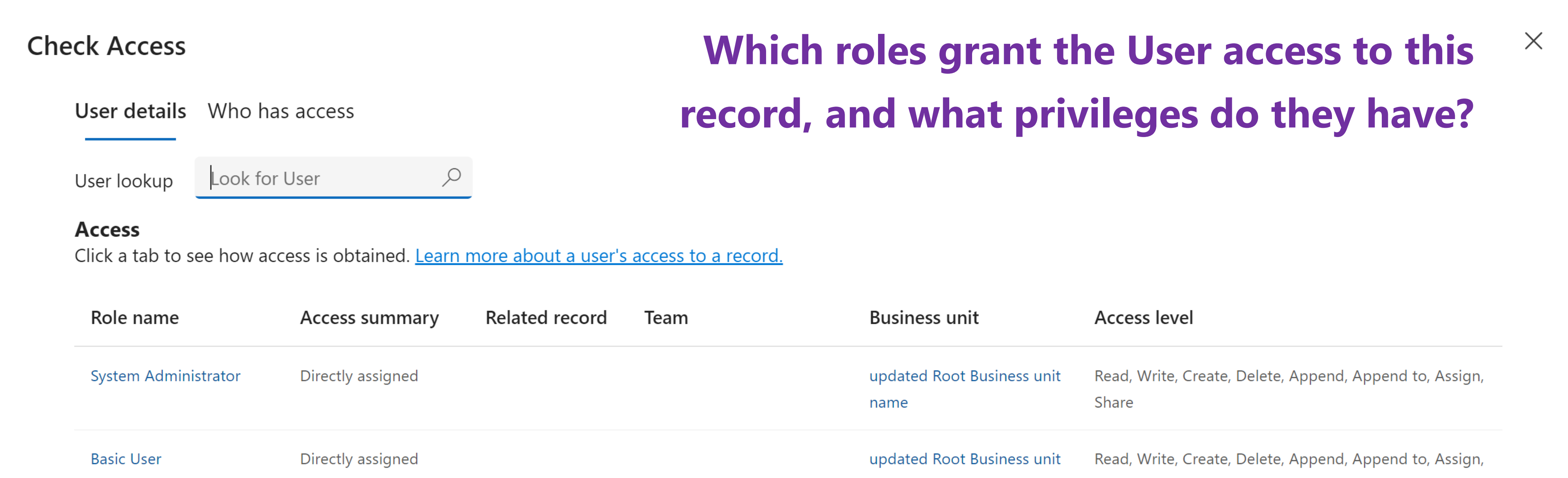
First Name *	test
Last Name *	contact
Job Title	---
Account Name	---
Email	---
Business Phone	---
Mobile Phone	---

Auto-post on Contact test contact: 4/23/2024, 12:18 PM
Contact created by Paul Liew CSS

Add an emai
common connections. Learn More.

No notifications or suggestions

Check back later to see what's new and stay up to date.



Which roles grant the User access to this record, and what privileges do they have?

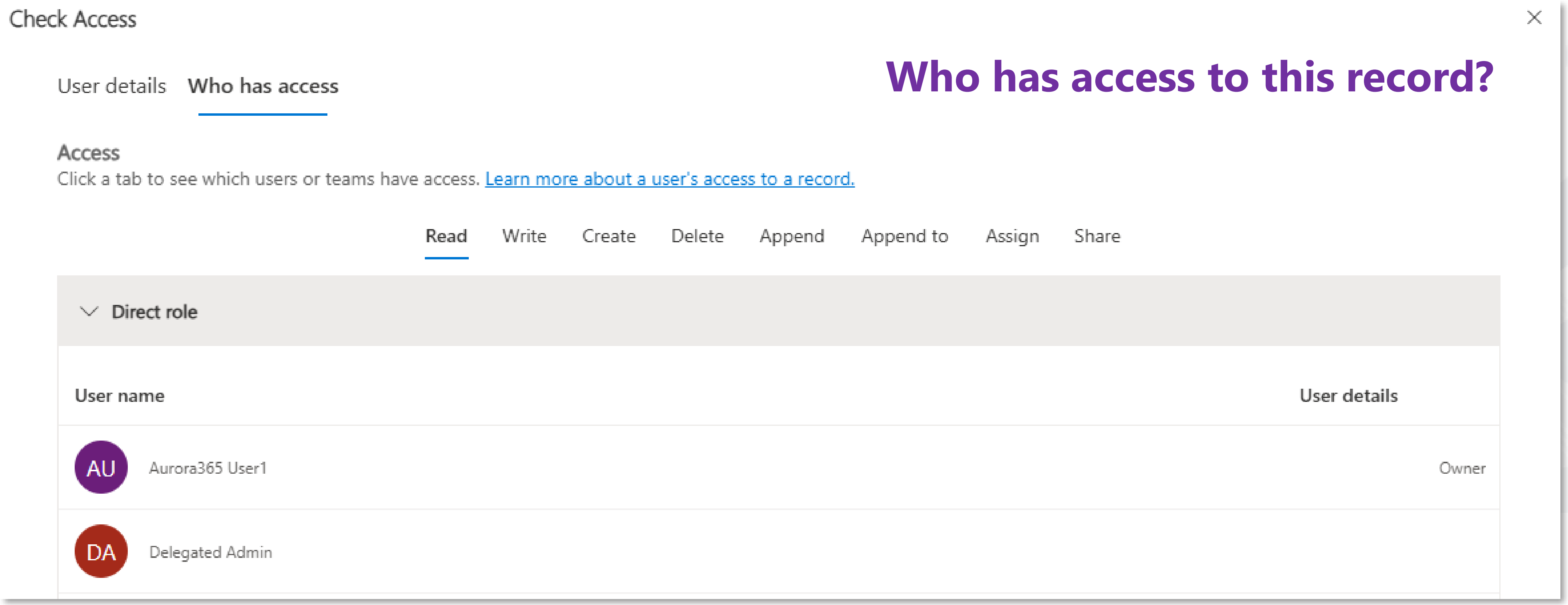
Check Access

User lookup: Look for User

Access

Click a tab to see how access is obtained. Learn more about a user's access to a record.

Role name	Access summary	Related record	Team	Business unit	Access level
System Administrator	Directly assigned			updated Root Business unit name	Read, Write, Create, Delete, Append, Append to, Assign, Share
Basic User	Directly assigned			updated Root Business unit	Read, Write, Create, Delete, Append, Append to, Assign,



Who has access to this record?

Check Access

Access

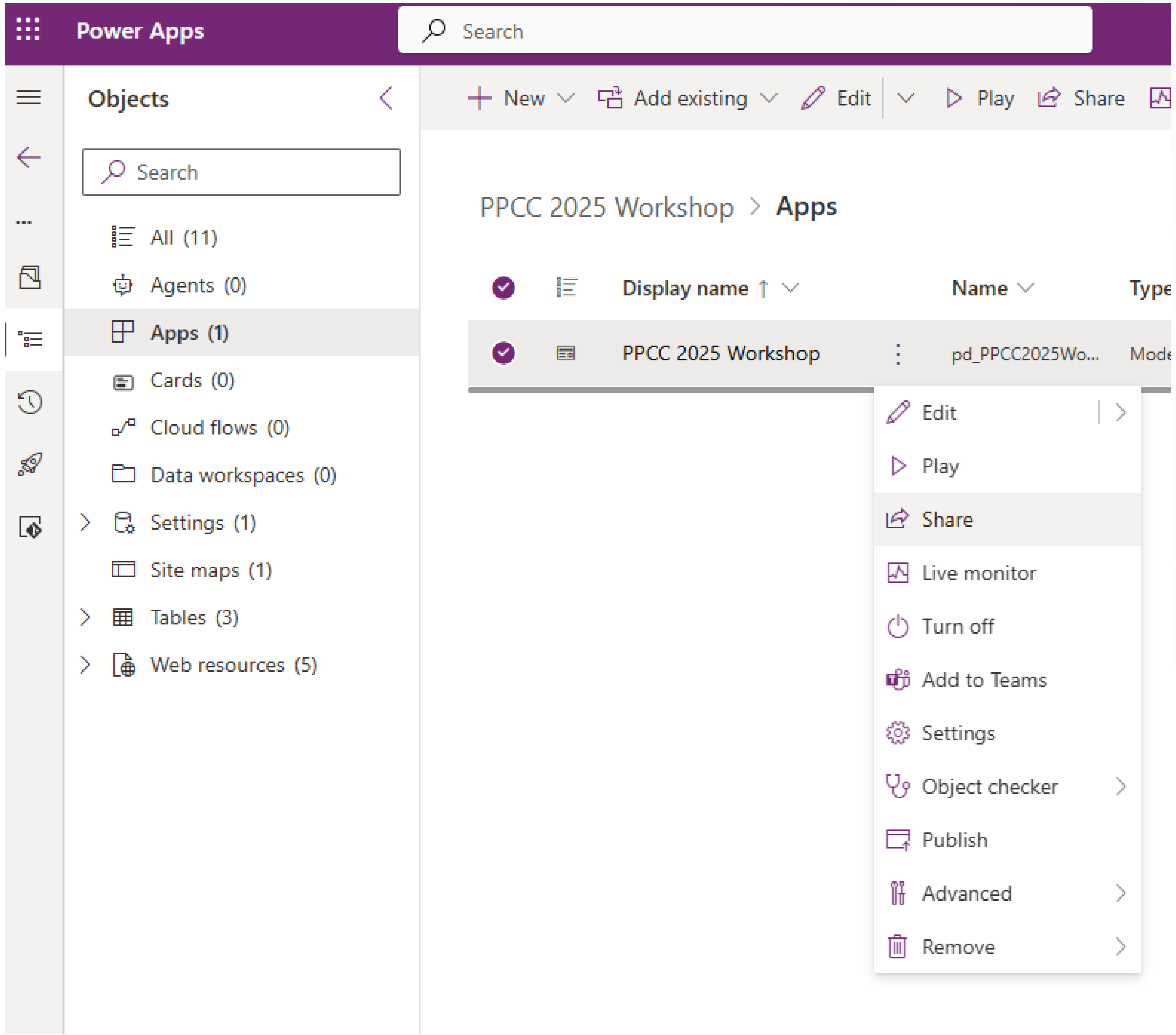
Click a tab to see which users or teams have access. Learn more about a user's access to a record.

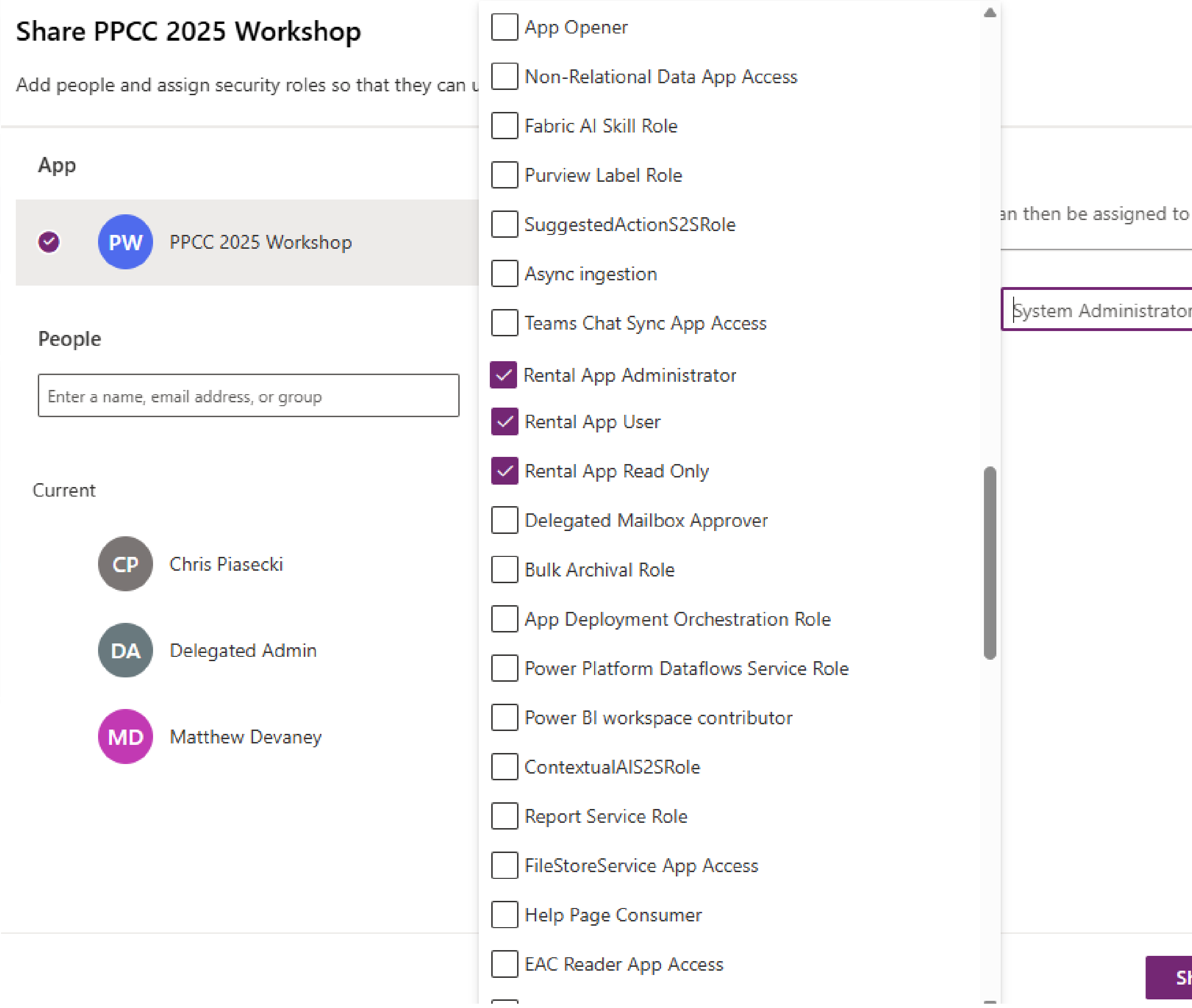
Direct role

User name	User details
AU Aurora365 User1	Owner
DA Delegated Admin	

Sharing Apps

Security roles determine which model driven apps the User has access to





Share PPCC 2025 Workshop

Add people and assign security roles so that they can u

App

● PW PPCC 2025 Workshop

People

Enter a name, email address, or group

Current

CP Chris Piasecki

DA Delegated Admin

MD Matthew Devaney

- □ App Opener
- □ Non-Relational Data App Access
- □ Fabric AI Skill Role
- □ Purview Label Role
- □ SuggestedActionS2SRole
- □ Async ingestion
- □ Teams Chat Sync App Access
- ☑ Rental App Administrator
- ☑ Rental App User
- ☑ Rental App Read Only
- □ Delegated Mailbox Approver
- □ Bulk Archival Role
- □ App Deployment Orchestration Role
- □ Power Platform Dataflows Service Role
- □ Power BI workspace contributor
- □ ContextualAIS2SRole
- □ Report Service Role
- □ FileStoreService App Access
- □ Help Page Consumer
- □ EAC Reader App Access

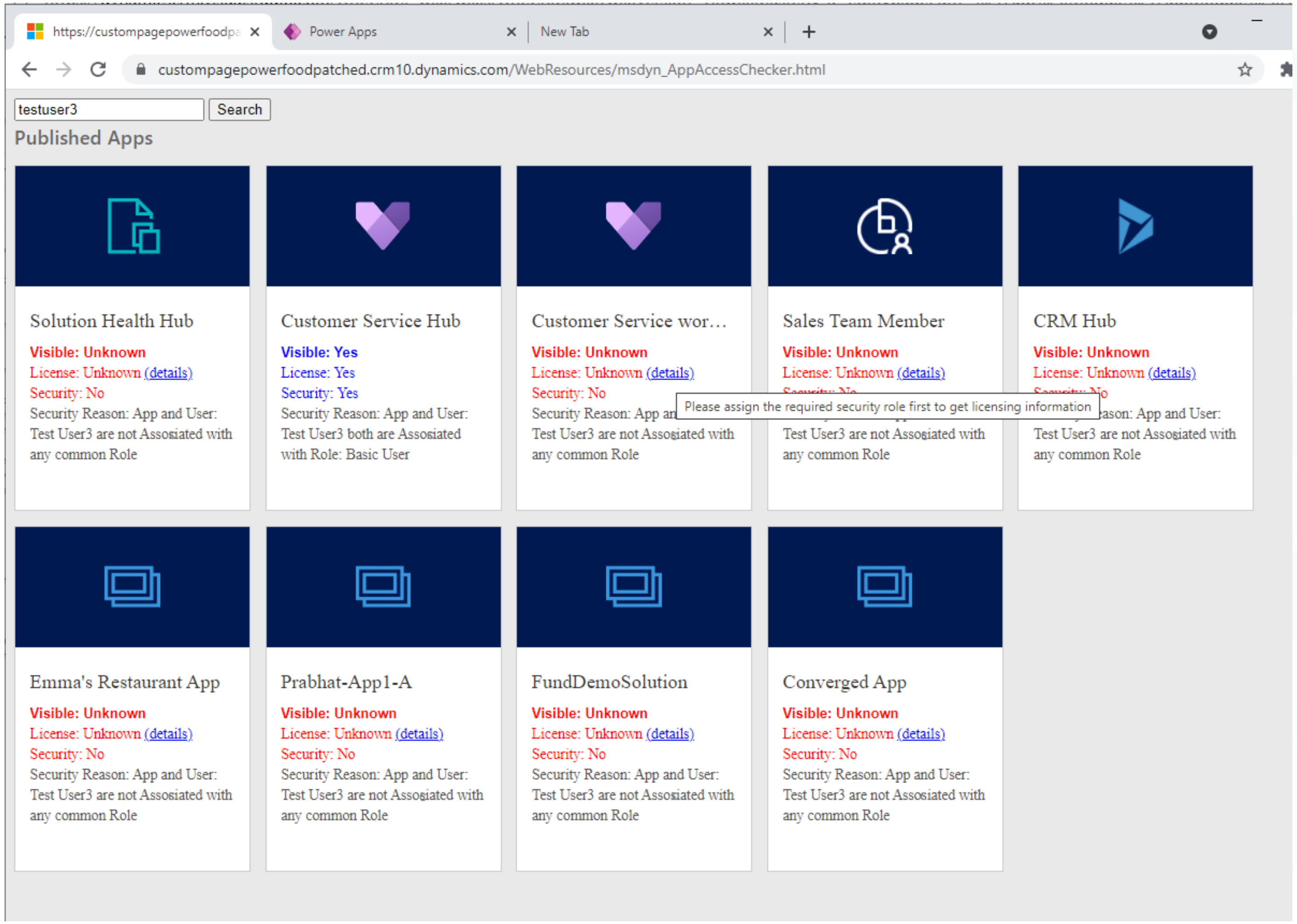
an then be assigned to

System Administrator

Sh

App Access Checker ✅

Which model-driven apps do I have access to?



custompagepowerfoodpatched.crm10.dynamics.com/WebResources/msdyn_AppAccessChecker.html

testuser3 Search

Published Apps

Solution Health Hub
Visible: Unknown
License: Unknown (details)
Security: No
Security Reason: App and User: Test User3 are not Assosiated with any common Role

Customer Service Hub
Visible: Yes
License: Yes
Security: Yes
Security Reason: App and User: Test User3 both are Assosiated with Role: Basic User

Customer Service wor…
Visible: Unknown
License: Unknown (details)
Security: No
Security Reason: App an
Test User3 are not Assosiated with any common Role

Please assign the required security role first to get licensing information

Sales Team Member
Visible: Unknown
License: Unknown (details)
Test User3 are not Assosiated with any common Role

CRM Hub
Visible: Unknown
License: Unknown (details)
ason: App and User: Test User3 are not Assosiated with any common Role

Emma's Restaurant App
Visible: Unknown
License: Unknown (details)
Security: No
Security Reason: App and User: Test User3 are not Assosiated with any common Role

Prabhat-App1-A
Visible: Unknown
License: Unknown (details)
Security: No
Security Reason: App and User: Test User3 are not Assosiated with any common Role

FundDemoSolution
Visible: Unknown
License: Unknown (details)
Security: No
Security Reason: App and User: Test User3 are not Assosiated with any common Role

Converged App
Visible: Unknown
License: Unknown (details)
Security: No
Security Reason: App and User: Test User3 are not Assosiated with any common Role

Add this to your environment URL:

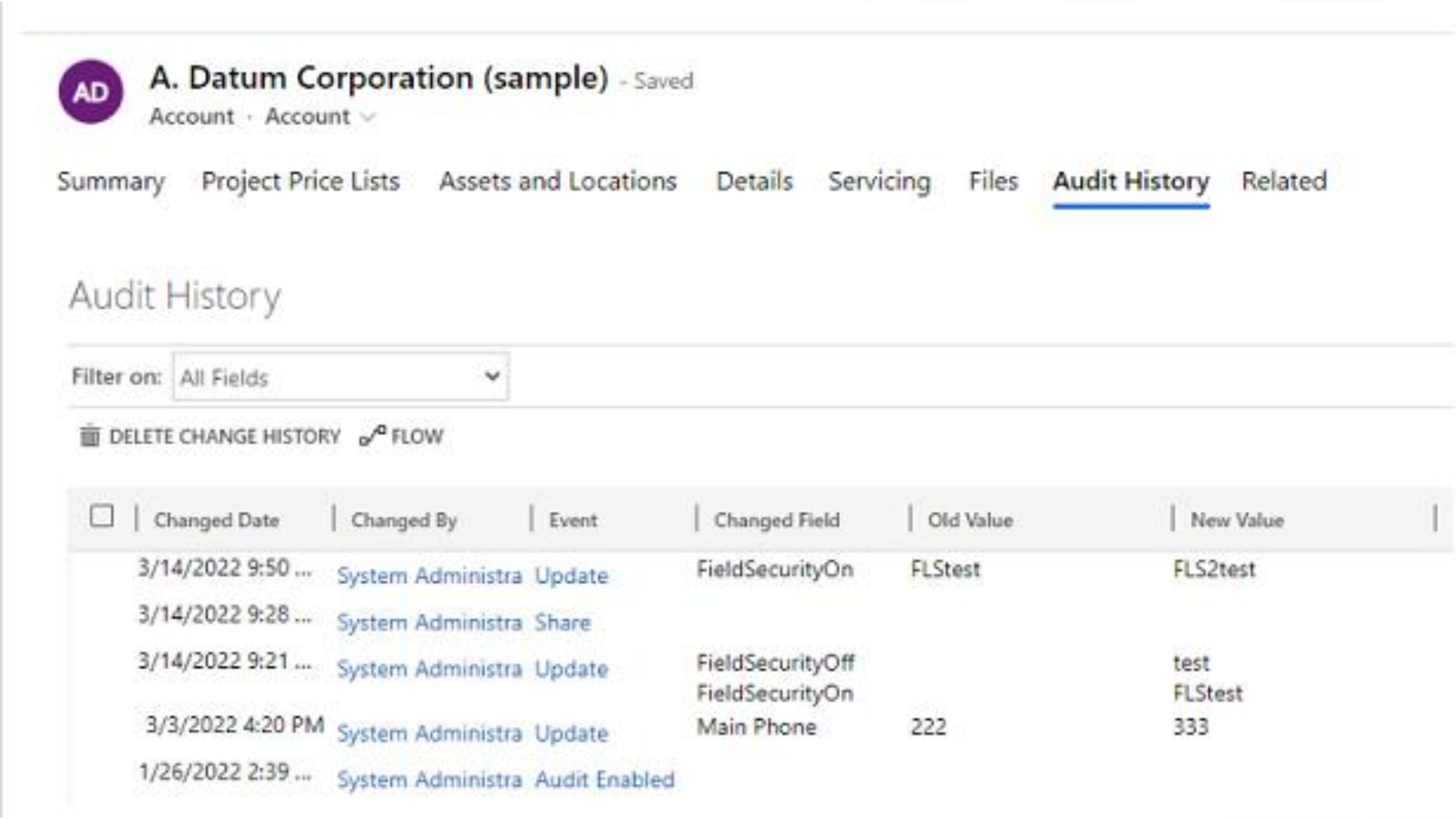
/WebResources/mydsn_AppAccessChecker

Example:

md-rentalsapp.crm.dynamics.com
/WebResources/mydsn_AppAccessChecker

Audit History 🔎

See who created/updated individual fields on a record and when



AD A. Datum Corporation (sample) - Saved

Account · Account

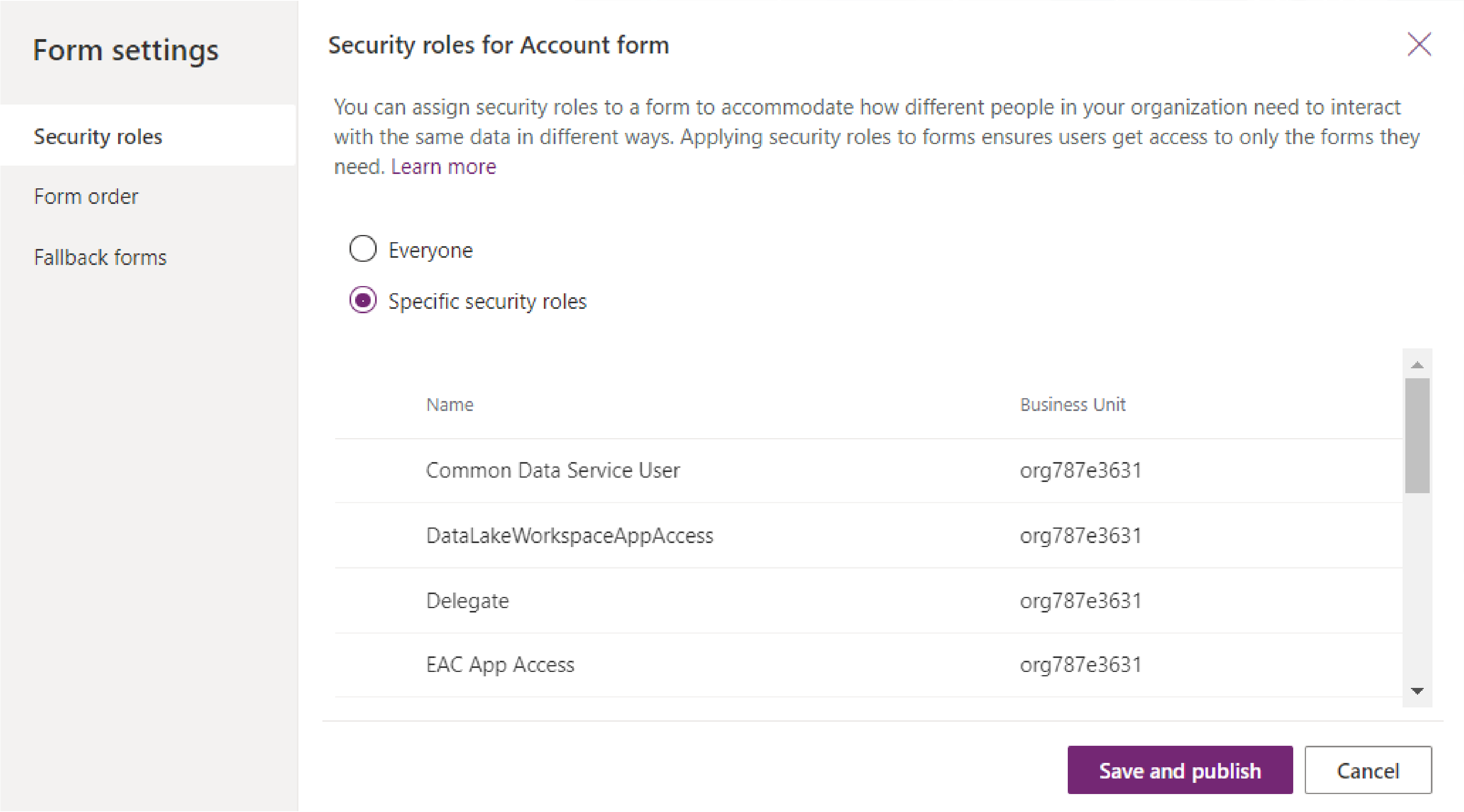
Audit History

Filter on: All Fields

☐	Changed Date	Changed By	Event	Changed Field	Old Value	New Value
	3/14/2022 9:50 ...	System Administra	Update	FieldSecurityOn	FLStest	FLS2test
	3/14/2022 9:28 ...	System Administra	Share			
	3/14/2022 9:21 ...	System Administra	Update	FieldSecurityOff FieldSecurityOn		test FLStest
	3/3/2022 4:20 PM	System Administra	Update	Main Phone	222	333
	1/26/2022 2:39 ...	System Administra	Audit Enabled			

Views & Forms Security

Only show forms and views to specific security roles



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

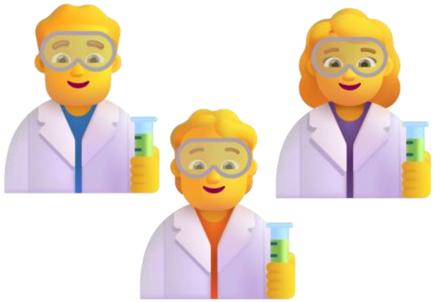
● Specific security roles

Name	Business Unit
Common Data Service User	org787e3631
DataLakeWorkspaceAppAccess	org787e3631
Delegate	org787e3631
EAC App Access	org787e3631

Complex Security Scenarios ☠️

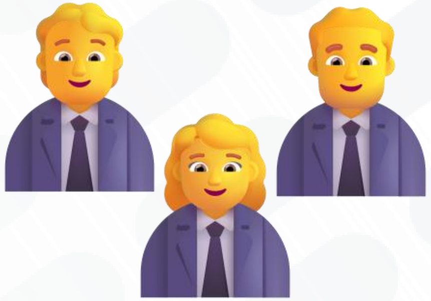
Teams 🐈 🐈‍⬛

A group of Users who collectively own a record



Western US Team

Central US Team



Eastern US Team

Use Owner Teams when…

- There is a clear criteria for forming Teams (Region, Product, Business Function, etc.)
- A set of Users has multiple alike Security Roles and you want to centralize permissions management
- You want to keep Security Roles in sync with an Entra Security Group

Team Types 🐈 🐈‍⬛

- Owner

  Manually assign team members

- Access

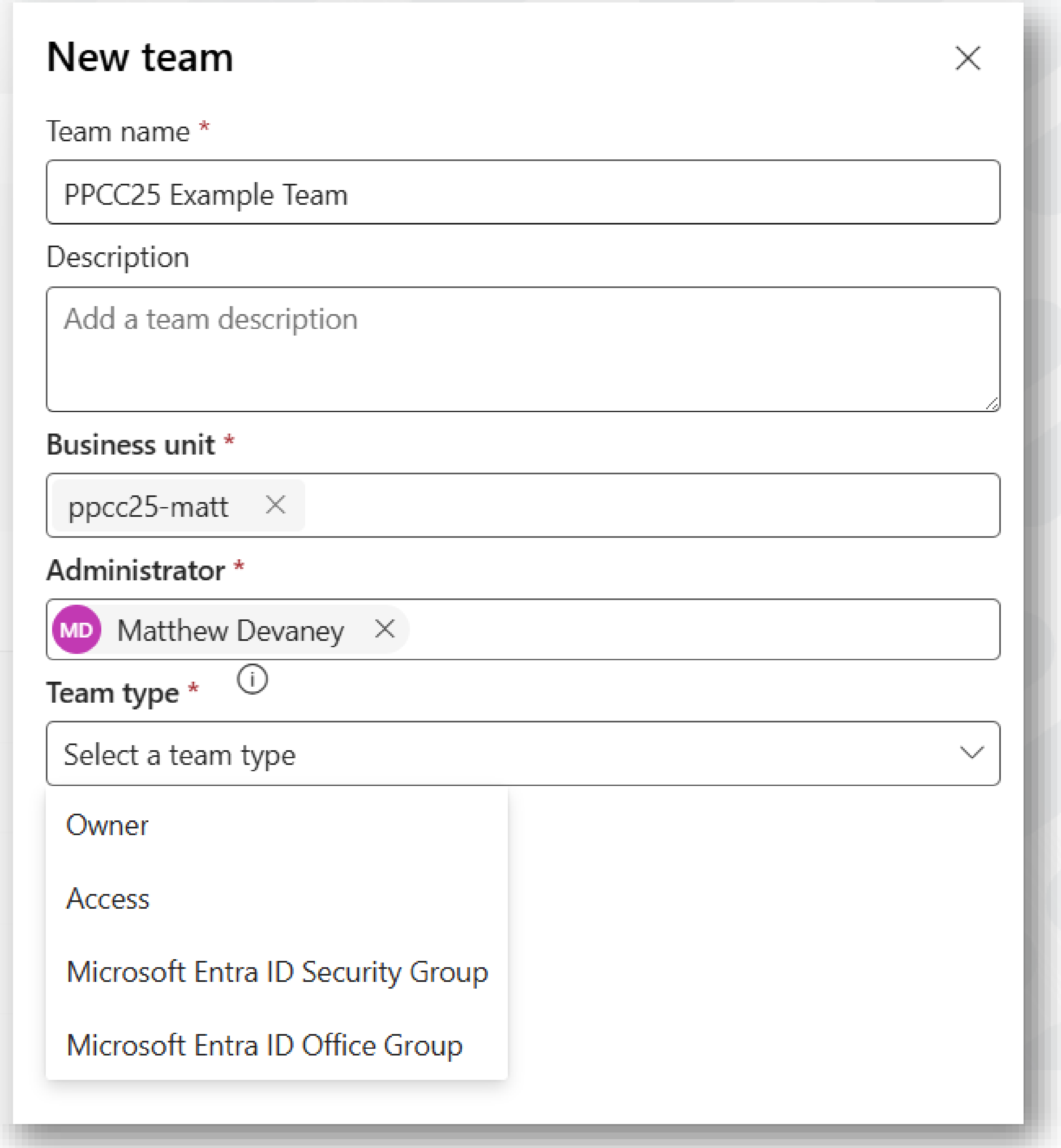
  Assign team members to single record

- Microsoft Entra ID Security Group

  Sync team members to Entra Security Group

- Microsoft Entra ID Office Group

  Sync team members of Office 365 Group



New team

Team name *

PPCC25 Example Team

Description

Add a team description

Business unit *

ppcc25-matt

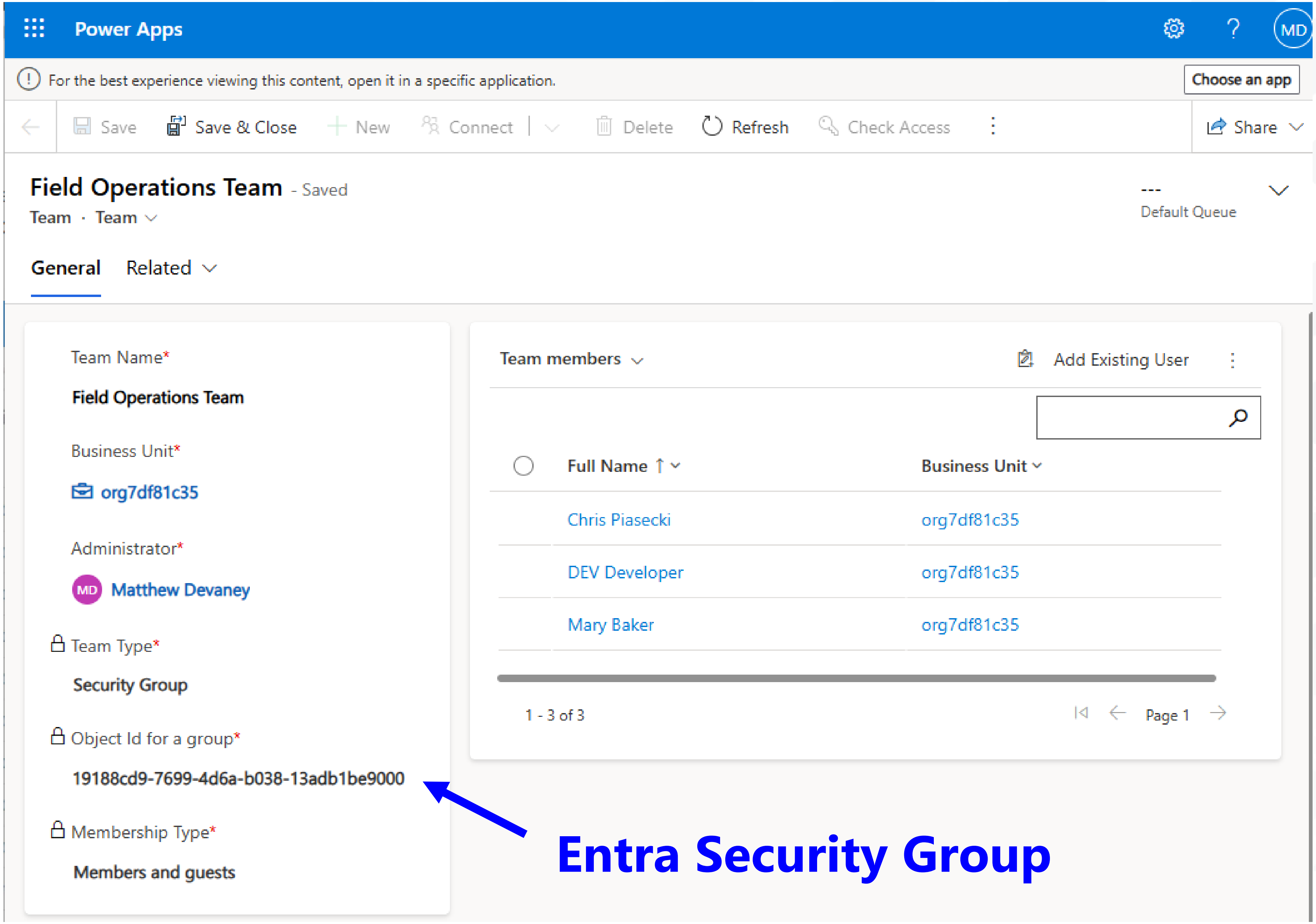
Administrator *

MD Matthew Devaney

Team type *

Select a team type

- Owner
- Access
- Microsoft Entra ID Security Group
- Microsoft Entra ID Office Group



Field Operations Team - Saved

Team · Team

Team Name*
Field Operations Team

Business Unit*
org7df81c35

Administrator*
Matthew Devaney

Team Type*
Security Group

Object Id for a group*
19188cd9-7699-4d6a-b038-13adb1be9000

Membership Type*
Members and guests

Full Name ↑	Business Unit
Chris Piasecki	org7df81c35
DEV Developer	org7df81c35
Mary Baker	org7df81c35

1 - 3 of 3

Entra Security Group

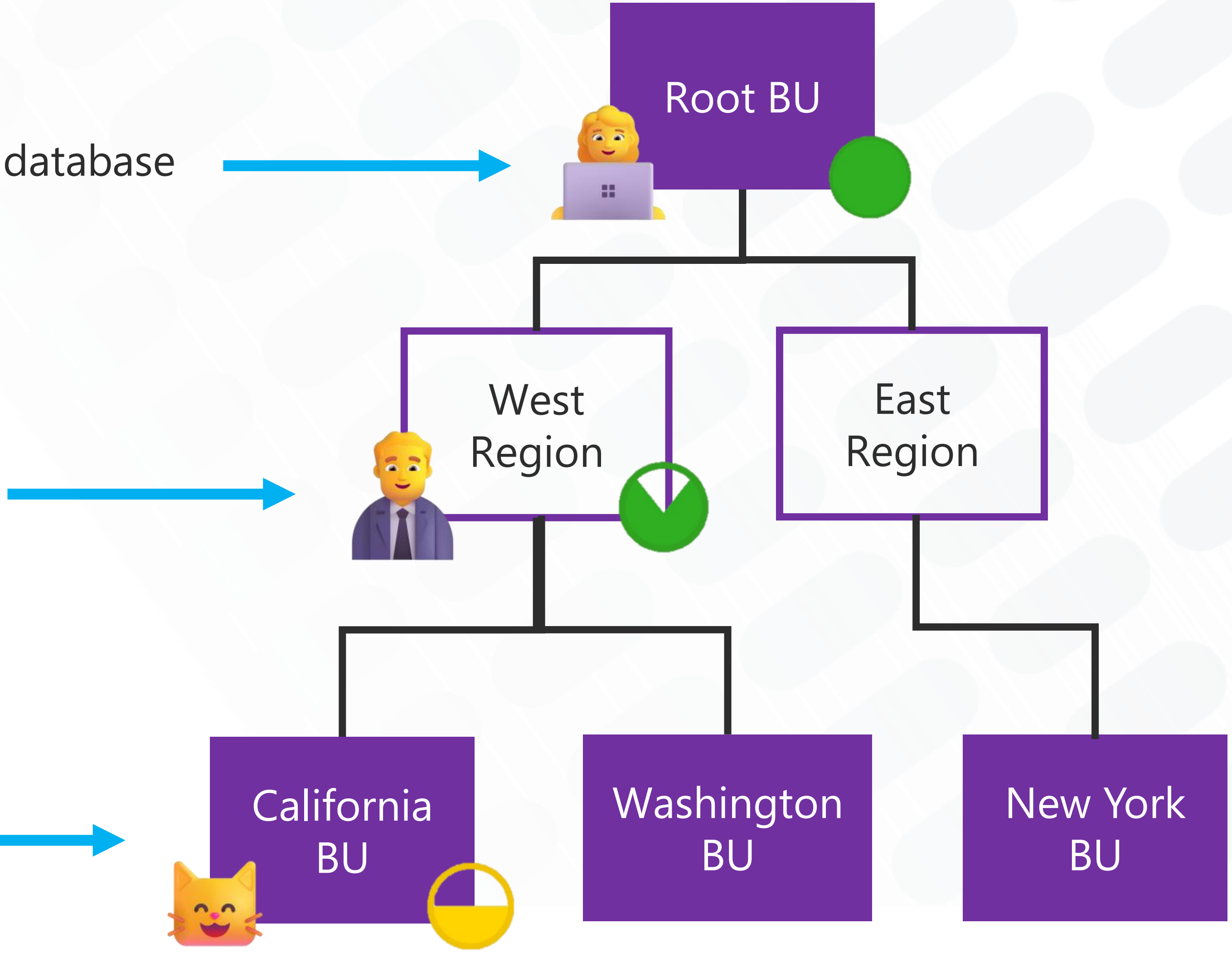
Business Units (Hierarchy) 🪜

“I want access to match the hierarchy of my company”

The Administrator has access all records in the database

Chris the Corporate Vice-President of the West Region and needs access to California and Washington records

Matthew is an individual contributor and should only have privileges to the California records

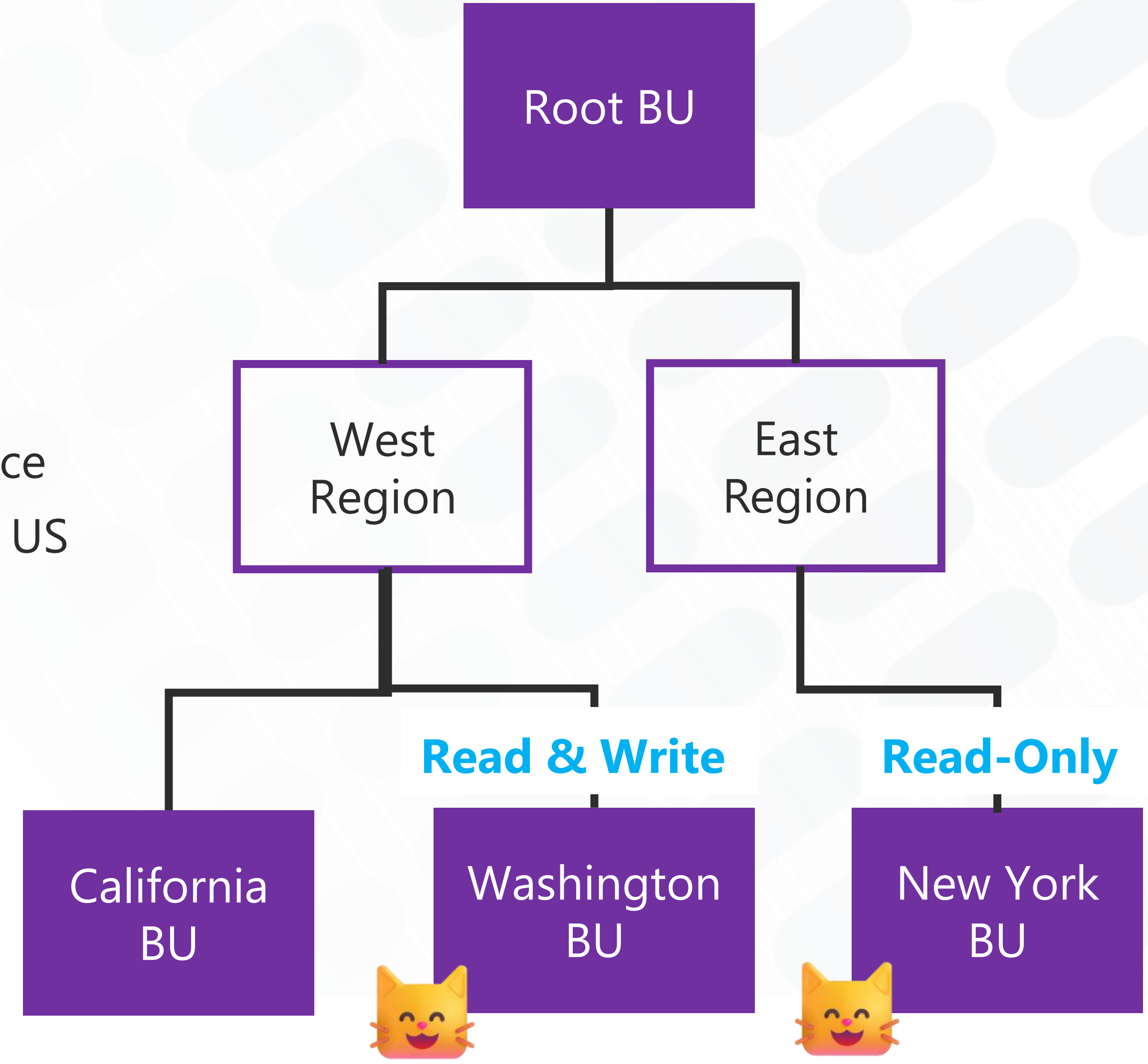


Business Units (Matrix-Style) 😬

“I want to have different privileges in different Business Units”

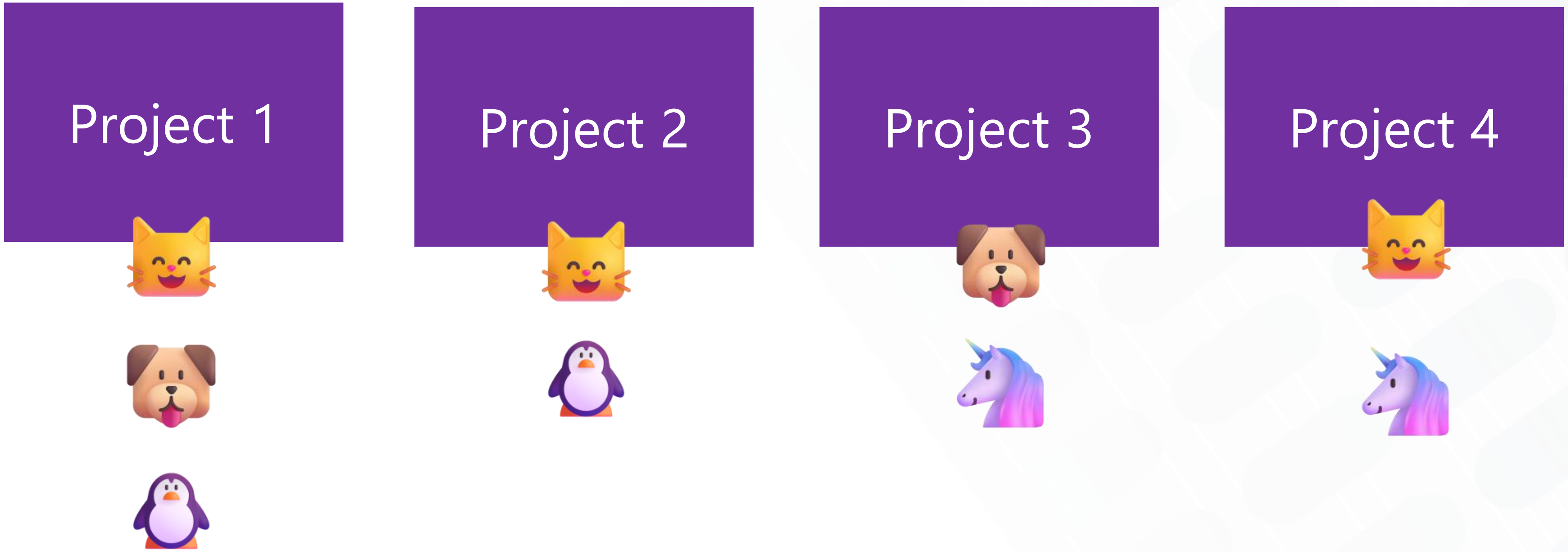
Matthew works in Washington and needs **read & write** access to records belonging to that US location

Matthew also supports the New York region during office holidays and needs **read-only** access to records in that US State



Access Teams

“I want every record in the table to belong to a different set of Owners”



Project 1

Project 2

Project 3

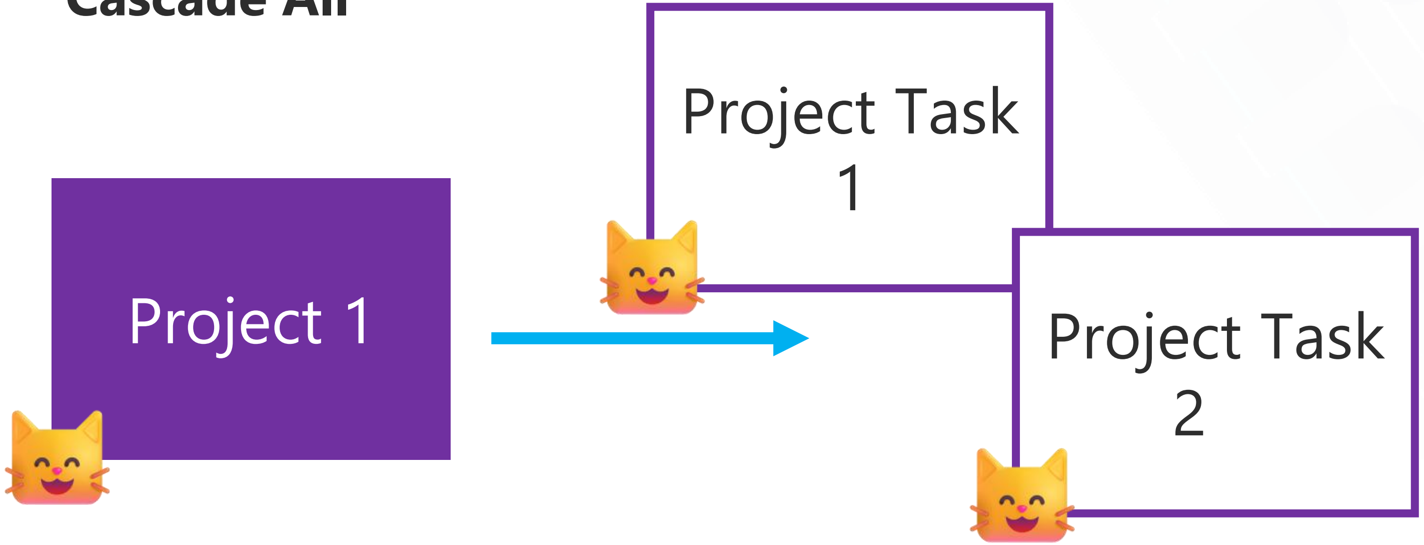
Project 4

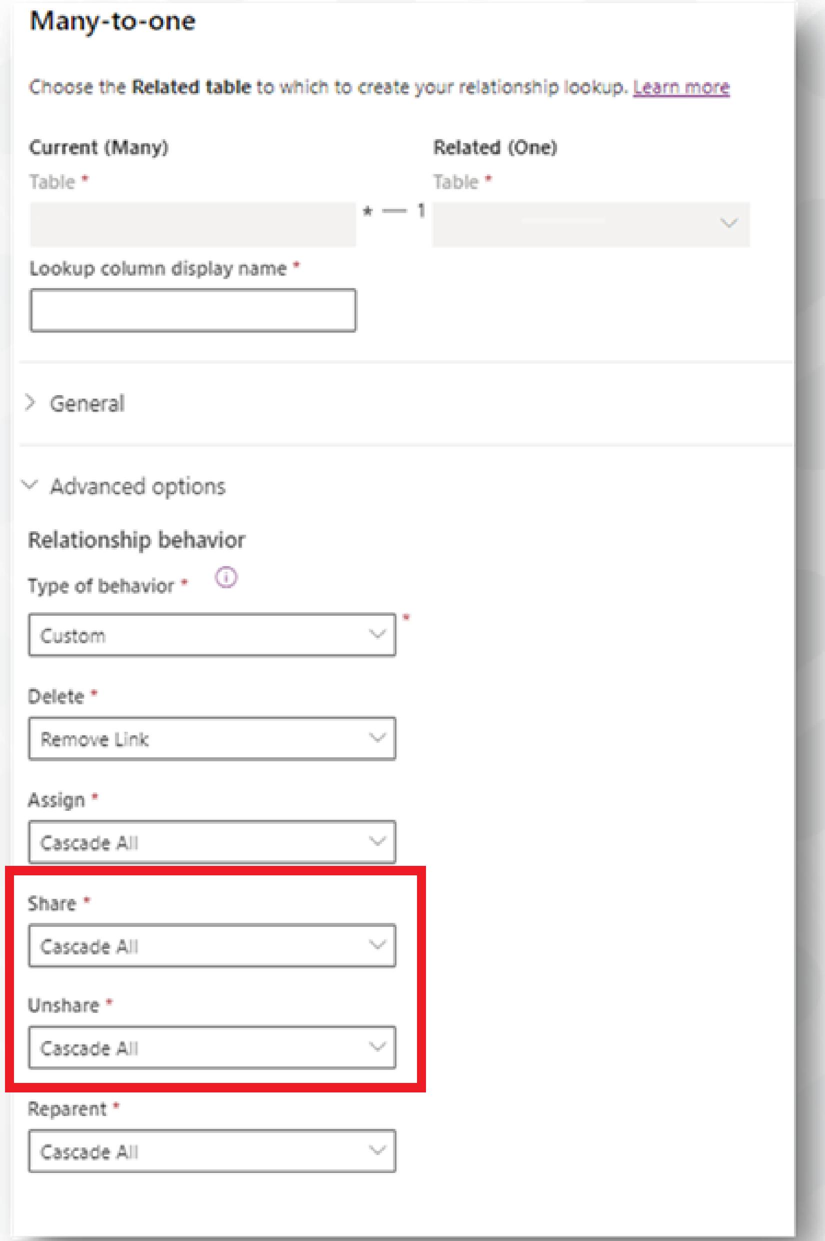
Use Access Teams when…

- Teams are dynamically being formed and dissolved
- The number of teams isn’t known at the design time
- Privileges should be determined by individual security roles

Cascade Sharing Records

- Access Teams grant permission to a record
- Access Teams can also **grant permissions to related records**
- Relationship type must be **a parental relationship** with the cascade option or have Share/Unshare set to **Cascade All**





Many-to-one

Choose the **Related table** to which to create your relationship lookup. Learn more

Current (Many)
Table *

Related (One)
Table *

Lookup column display name *

General

Advanced options

Relationship behavior

Type of behavior *: Custom

Delete *: Remove Link

Assign *: Cascade All

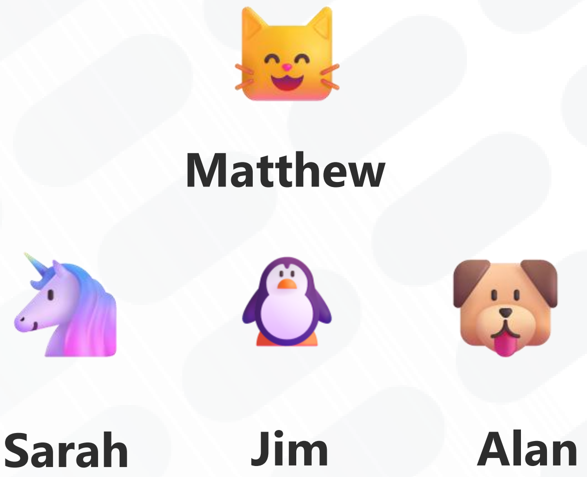
Share *: Cascade All

Unshare *: Cascade All

Reparent *: Cascade All

Manager Hierarchy & Position Hierarchy

Manager Hierarchy is when a Manager is considered to own their direct reports records in the system



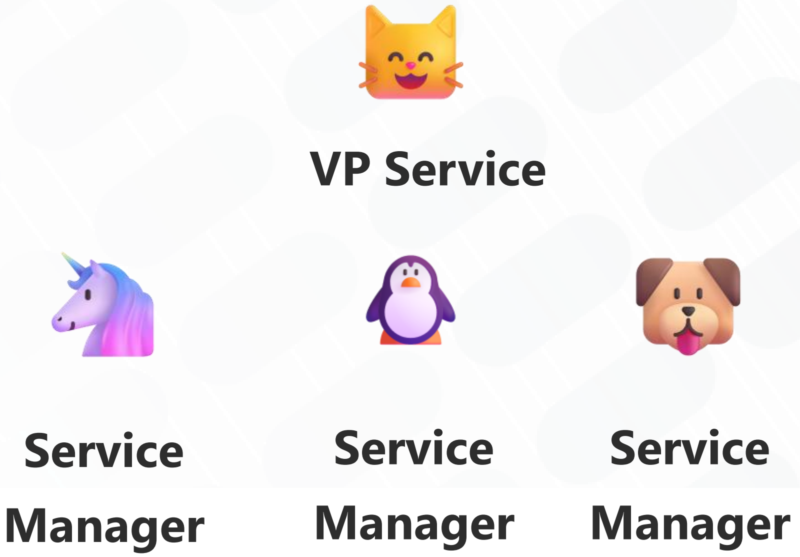
Matthew

Sarah

Jim

Alan

Positional Hierarchy is when a senior position is considered to own the records of direct reports underneath them



VP Service

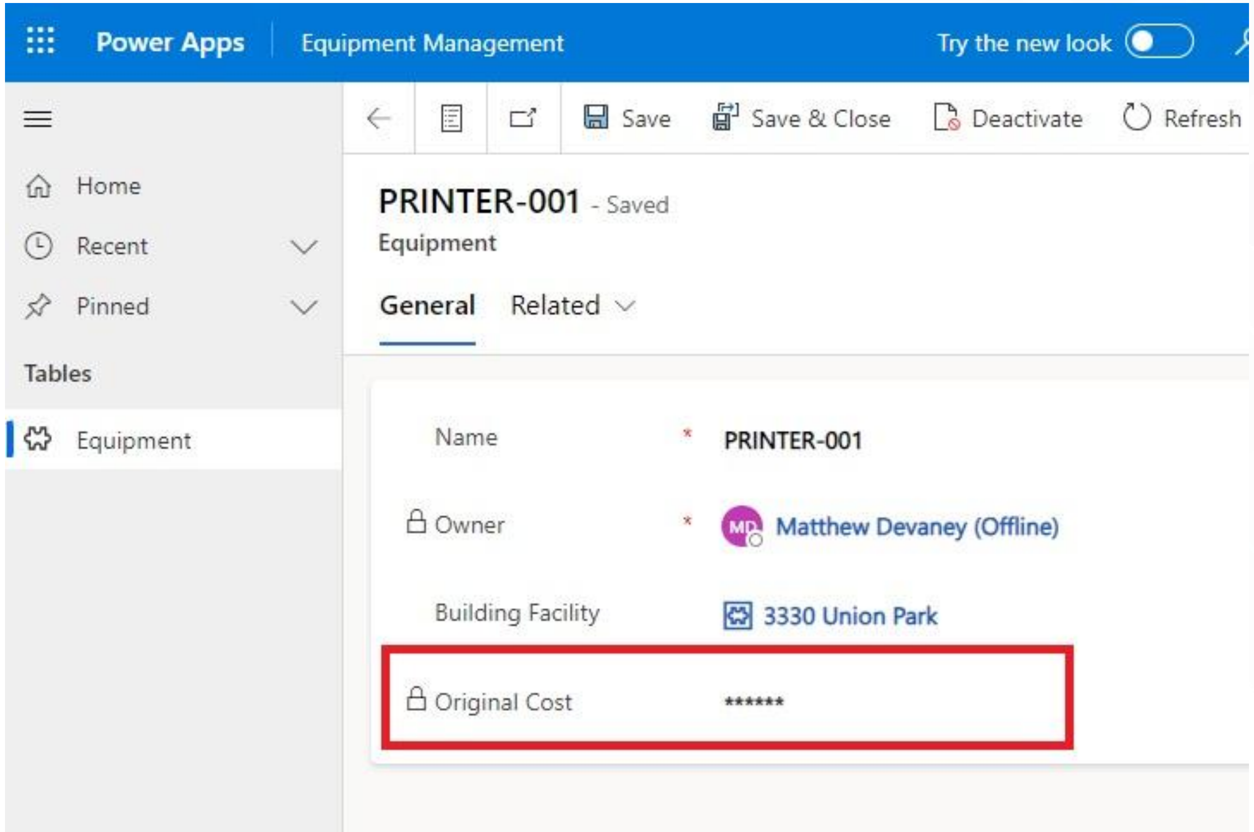
Service Manager

Service Manager

Service Manager

Column-Level Security 👁

Grant privileges for an individual field in a table

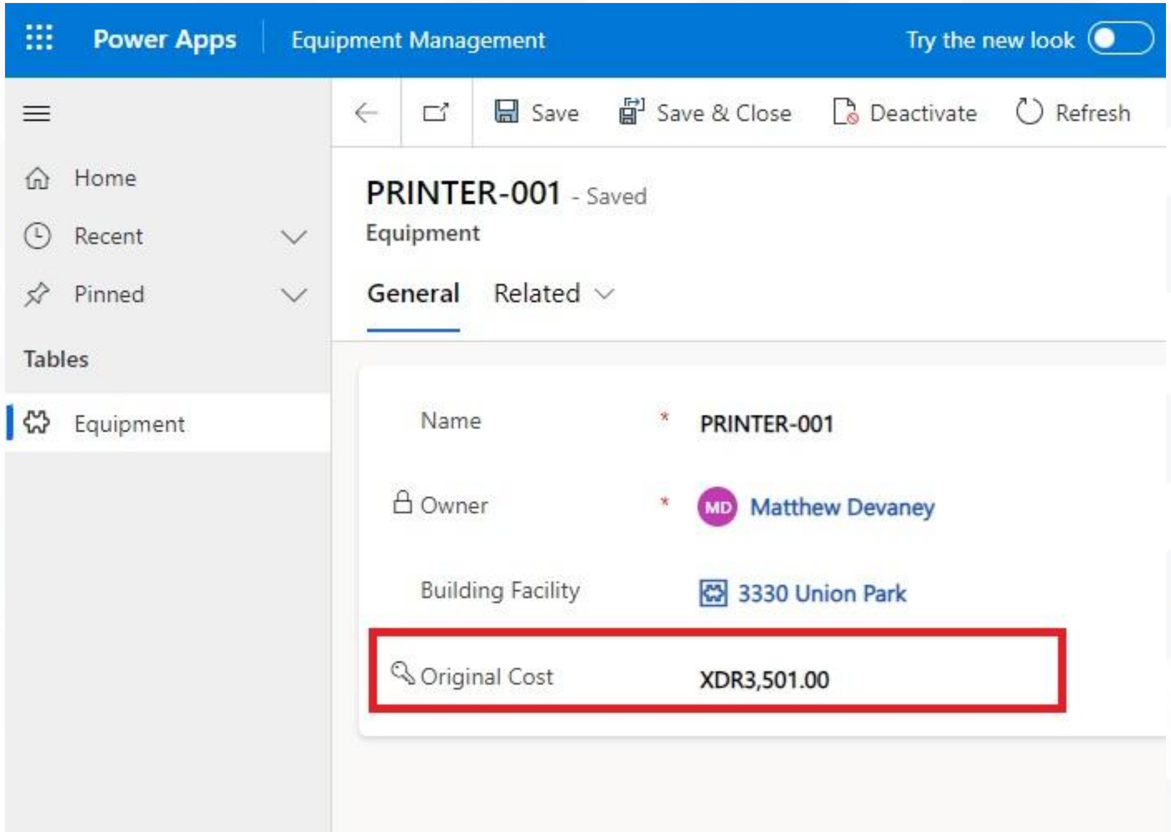


PRINTER-001 - Saved

Equipment

Name *	PRINTER-001
Owner *	Matthew Devaney (Offline)
Building Facility	3330 Union Park
Original Cost	******

Read Privileges Disabled



PRINTER-001 - Saved

Equipment

Name *	PRINTER-001
Owner *	Matthew Devaney
Building Facility	3330 Union Park
Original Cost	XDR3,501.00

Edit Privileges Disabled

What Security Features Should I Choose? 🤔 💭

Requirement	Recommendation
Users have privileges to their own records or the entire organization	User
Two or more groups of users should only have privileges for their own team’s records	Teams
The use case has multiple groups in a hierarchy, and privileges and parent groups should have privileges for child groups	Business units (hierarchy)
Users belong to more than one group and perform different roles in each group	Business units (matrix-style)
Every time a new project is started a unique set of team members is assigned	Access Teams
Specific columns have sensitive data and only some users can read/write	Column-based security

🙋‍♂️ 🙋‍♀️

Q&A Time ⏰

Softball questions only. Unless you have a difficult problem.