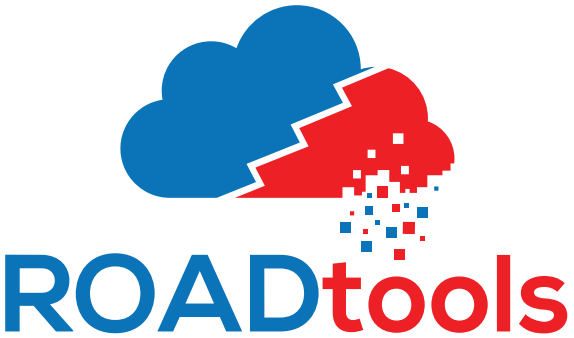
/OUTSIDER SECURITY



Evolving ROADtools

Dirk-jan Mollema @ WWHF Denver

Agenda

- ROADtools 101
- Azure AD graph deprecation update
- Bob is Global Admin
  - Privileged Identity Management
  - Entitlement Management
- Bonus demo?

About me

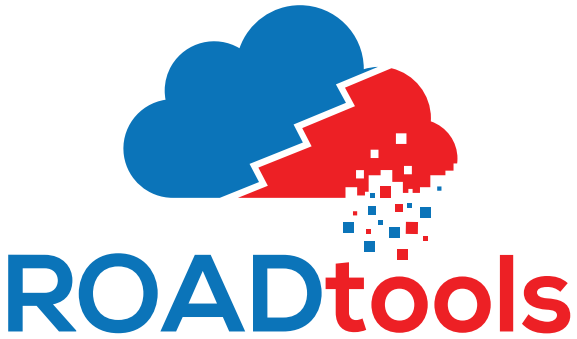
/OUTSIDER SECURITY

- Dirk-jan Mollema
- From The Hague, Netherlands
- Hacker / Researcher / Founder / Trainer @ Outsider Security
- Talks at Black Hat / DEF CON / BlueHat / Troopers / x33fcon
- Author of several Active Directory and Entra ID tools
  - mitm6
  - ldapdomaindump
  - adidnsdump
  - BloodHound.py
  - ntlmrelayx / krbrelayx
  - ROADtools

Socials

Blog/talks:	dirkjanm.io
Twitter/X:	@_dirkjan
BlueSky:	@dirkjanm.io

ROADtools



- Open Source Entra ID toolkit released in 2020
  - ROADlib
    - Authentication logic for all token request and usage flows
    - Azure AD graph schema definitions
  - ROADrecon
    - Entra ID recon tool with GUI, plugins and analysis capabilities
  - roadtx
    - Token eXchange tool supporting many token operations

- Available at https://github.com/dirkjanm/roadtools

ROADrecon and the Azure AD Graph API

Entra ID API’s

- Azure AD Graph API (graph.windows.net)
  - Old school
  - Secret internal versions with interesting insights
- Microsoft Graph API (graph.microsoft.com)
  - Official
  - Documented
  - High level (boring)
  - Restrictions what you can access (boo)

Azure AD Graph deprecation

Key timelines in the retirement of Azure AD Graph are as follows:

- 2019: Initial announcement of the deprecation of Azure AD Graph. Retirement set for June 30, 2023.
- June 30, 2023: End of the three-year notice period for deprecation of Azure AD Graph. Azure AD Graph enters its retirement cycle.
- August 31, 2024: New applications created after this date can't use Azure AD Graph unless they explicitly opt in for extended access. Existing applications continue to work.
- February 1, 2025: **All new and existing apps must** explicitly opt in for extended access to use Azure AD Graph, *including* apps created before August 31, 2024.
- August 31, 2025: End of extended access to Azure AD Graph. Azure AD Graph will be fully retired.

Seems that passed

is today before or after august 31, 2025

Copilot

Today is **February 8, 2026**, which is **after** August 31, 2025.

So the answer: **today is after August 31, 2025.**

If you need help comparing other dates, feel free to ask!

Azure AD Graph deprecation and ROADtools

- Blocked for customer applications since Q3 2025.
- Microsoft apps continue to work.
- Azure AD Graph PowerShell module also deprecated around the same time.
- Client ID blocked from accessing the Azure AD Graph since October 2025.
- ROADrecon defaults to this client ID and thus is blocked by default.

“Fixing” ROADrecon

- In the end, ROADrecon needs a token that is:
  - For graph.windows.net
  - From a Microsoft client
  - With “user_impersonation” permissions
- There are many clients that meet this requirement.
- roadtx findscope -s https://graph.windows.net/user_impersonation gives about 100 client IDs.
- Azure CLI is one of them, which is now the new default client ID in ROADtools.

The long term fix

- Migrate ROADrecon to the Microsoft Graph
- Downsides:
  - Higher level API, less insights than internal API.
  - Missing many settings that internal AAD Graph shows us, but Microsoft Graph does not or requires admin rights for (Global Reader).
  - No insight into Conditional Access Policies without the correct role.
  - API level telemetry making this very noisy (MS Graph activity logs in XDR).
  - No magic scope that allows all enumeration, means changing tokens to get the correct scopes for data access.

Microsoft Graph migration

- A Microsoft Graph implementation was contributed by Thomas Byrne from Reversec
- Still working on merging that in but expect it to be available in a few weeks.

Other major contributions and changes

- Improved UI performance with server side paging.
  - Based on the contributions of Kévin Tellier (@flashlam) and Richard Gomez (@rgmz)
- New UI written in Vue by Kévin Tellier.
- Scoped Conditional Access policies in the UI.

ROADrecon demo 1

New ROADrecon release focus

- Answer the question: What can any individual user access or obtain access to?

Bob is Global Admin

Bob

User

Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request

Edit properties | Delete | Refresh | Reset password | Revoke sessions | Manage view | Got feedback?

Overview | Monitoring | Properties

Basic info

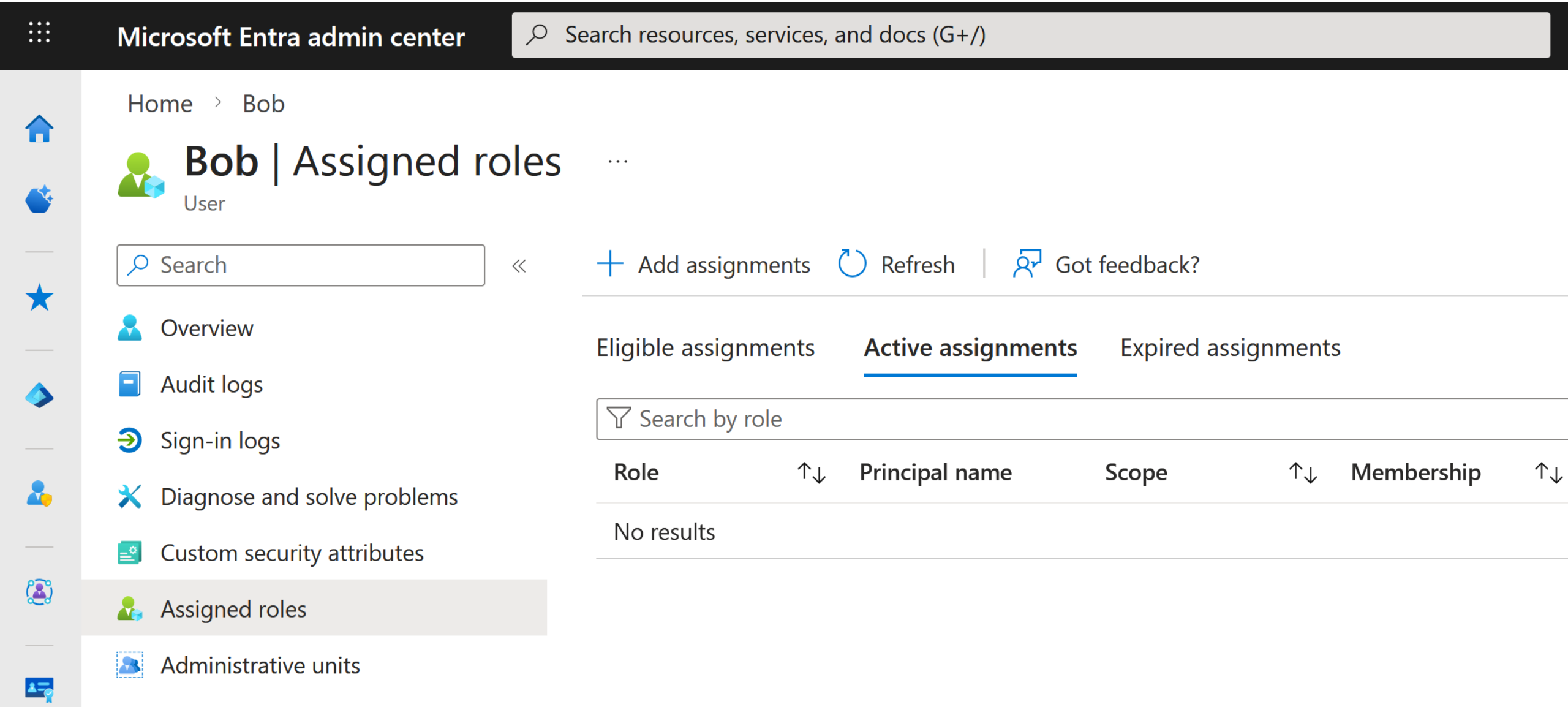
B

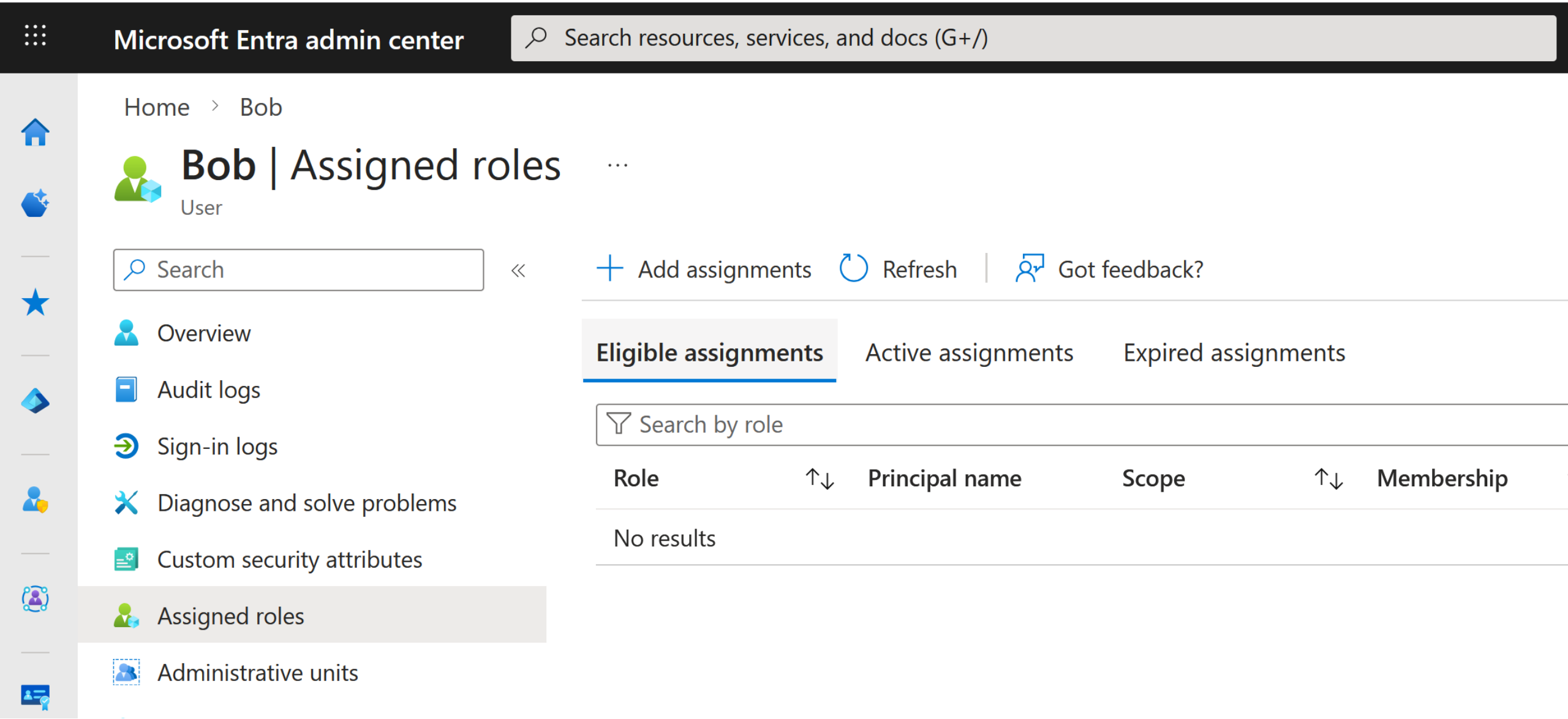
Bob
bob@iminyour.cloud
Member

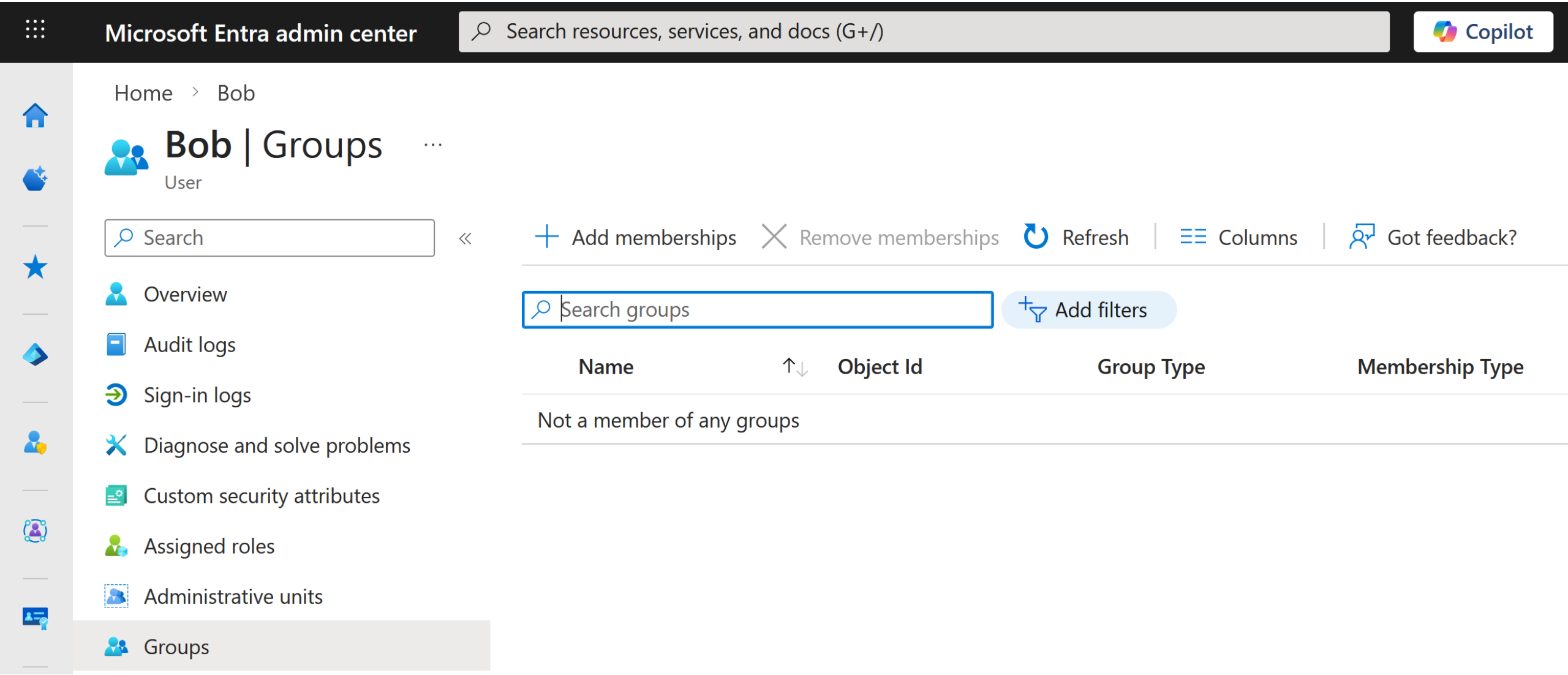
User principal name	bob@iminyour.cloud
Object ID	f84a053c-d050-4c7c-bfce-9a3f95bc80ae
Created date time	Mar 4, 2021, 12:01 PM
User type	Member
Identities	iminyourcloud.onmicrosoft.com

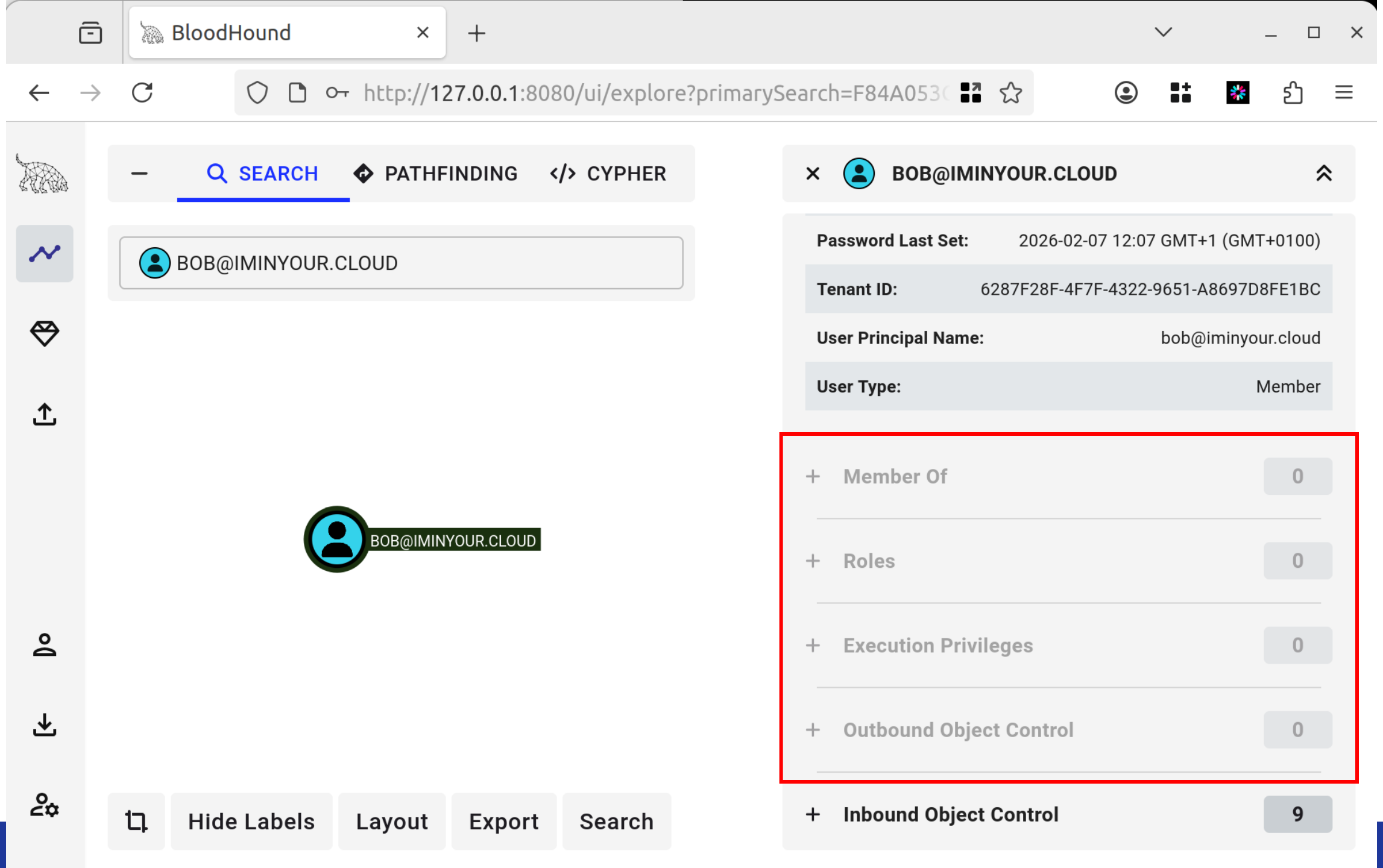
Group memberships	0
Applications	0
Assigned roles	0
Assigned licenses	1

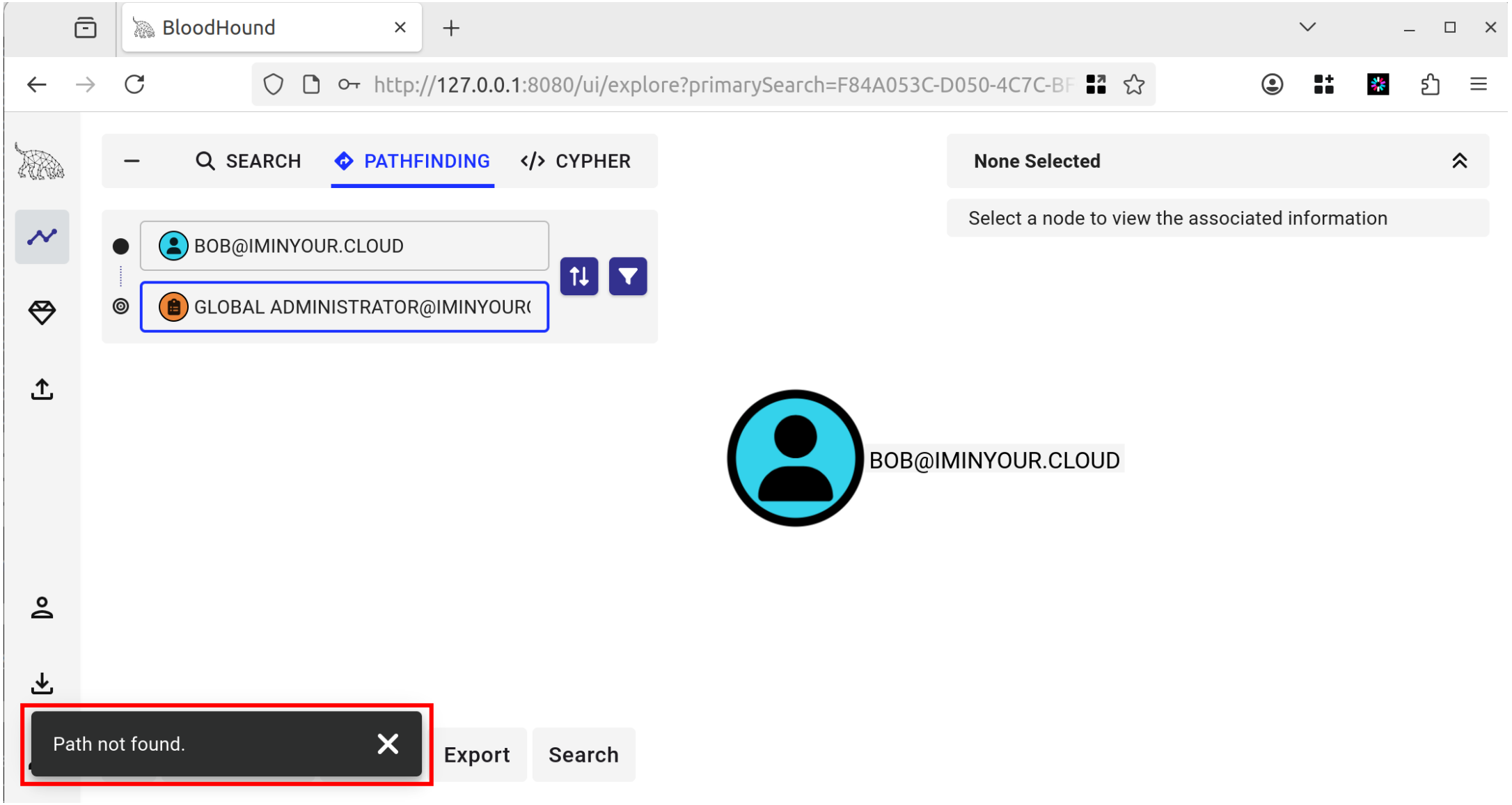
My Feed


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Bob
Bob | Assigned roles
User
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Add assignments
Refresh
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by role
Role
Principal name
Scope
Membership
No results


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Bob
Bob | Assigned roles
User
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Add assignments
Refresh
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by role
Role
Principal name
Scope
Membership
No results


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home
Bob
Bob | Groups
User
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Add memberships
Remove memberships
Refresh
Columns
Got feedback?
Search groups
Add filters
Name
Object Id
Group Type
Membership Type
Not a member of any groups


BloodHound
http://127.0.0.1:8080/ui/explore?primarySearch=F84A053
SEARCH
PATHFINDING
CYPHER
BOB@IMINYOUR.CLOUD
BOB@IMINYOUR.CLOUD
BOB@IMINYOUR.CLOUD
Password Last Set: 2026-02-07 12:07 GMT+1 (GMT+0100)
Tenant ID: 6287F28F-4F7F-4322-9651-A8697D8FE1BC
User Principal Name: bob@iminyour.cloud
User Type: Member
Member Of 0
Roles 0
Execution Privileges 0
Outbound Object Control 0
Inbound Object Control 9
Hide Labels
Layout
Export
Search


BloodHound
http://127.0.0.1:8080/ui/explore?primarySearch=F84A053C-D050-4C7C-BF
SEARCH
PATHFINDING
CYPHER
None Selected
Select a node to view the associated information
BOB@IMINYOUR.CLOUD
GLOBAL ADMINISTRATOR@IMINYOUR(
BOB@IMINYOUR.CLOUD
Path not found.
Export
Search

ROADrecon demo 2 - PIM

Privileged Identity Management

- Entra ID premium P2 feature.
- Supports elevating permissions by activating eligible assignments:
  - Entra ID roles
  - Entra ID groups
  - Azure resources
- PIM is not Entra ID native, which means Entra ID is not always aware of eligible memberships.
- PIM activation can have conditions:
  - Security controls like MFA, CA policies.
  - Approval from other users.

PIM data enumeration

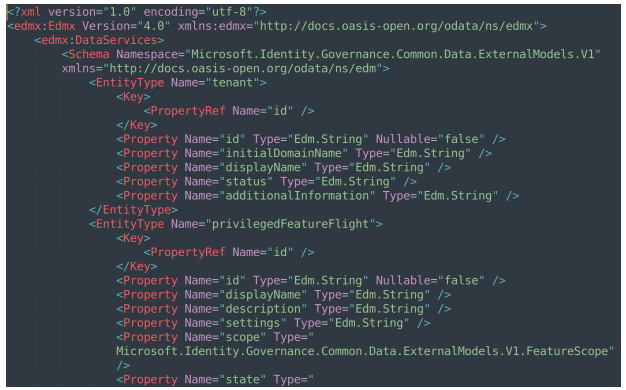
- Exposed via Microsoft Graph
- Microsoft portals will use undocumented internal API:
  - https://api.azrbac.mspim.azure.com
- Azure CLI client has *user_impersonation* rights on this API
- Regular users can query most info
  - Entra roles and eligible assignments
  - Onboarded groups and elevation settings
- Permissions are needed to query some info
  - Entra role elevation settings
  - Azure resource data in PIM limited to current user's Azure access

PIM Metadata – Odata schema

```
<?xml version="1.0" encoding="utf-8"?>
<edmx:Edmx Version="4.0" xmlns:edmx="http://docs.oasis-open.org/odata/ns/edmx">
    <edmx:DataServices>
        <Schema Namespace="Microsoft.Identity.Governance.Common.Data.ExternalModels.V1"
        xmlns="http://docs.oasis-open.org/odata/ns/edm">
            <EntityType Name="tenant">
                <Key>
                    <PropertyRef Name="id" />
                </Key>
                <Property Name="id" Type="Edm.String" Nullable="false" />
                <Property Name="initialDomainName" Type="Edm.String" />
                <Property Name="displayName" Type="Edm.String" />
                <Property Name="status" Type="Edm.String" />
                <Property Name="additionalInformation" Type="Edm.String" />
            </EntityType>
            <EntityType Name="privilegedFeatureFlight">
                <Key>
                    <PropertyRef Name="id" />
                </Key>
                <Property Name="id" Type="Edm.String" Nullable="false" />
                <Property Name="displayName" Type="Edm.String" />
                <Property Name="description" Type="Edm.String" />
                <Property Name="settings" Type="Edm.String" />
                <Property Name="scope" Type="
                Microsoft.Identity.Governance.Common.Data.ExternalModels.V1.FeatureScope"
                />
                <Property Name="state" Type="
```

ROADtools – roadlib schema

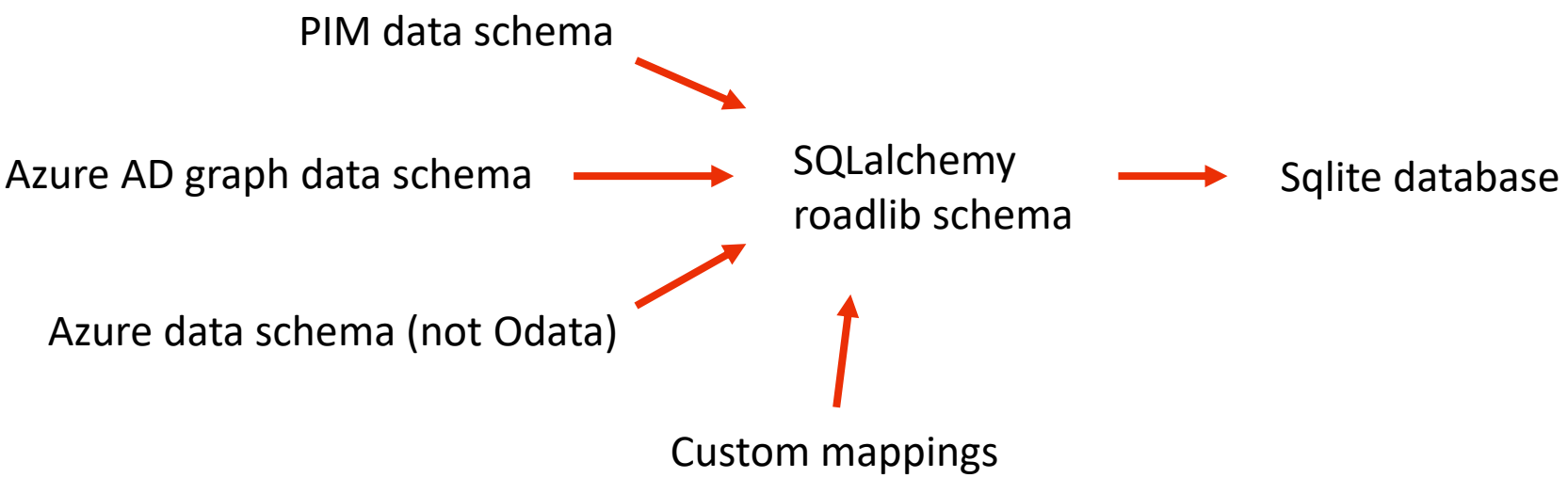
Azure AD Graph data schema



```
<?xml version="1.0" encoding="utf-8"?>
<edmx:Edmx Version="4.0" xmlns:edmx="http://docs.oasis-open.org/odata/ns/edmx">
    <edmx:DataServices>
        <Schema Namespace="Microsoft.Identity.Governance.Common.Data.ExternalModels.V1"
        xmlns="http://docs.oasis-open.org/odata/ns/edm">
            <EntityType Name="tenant">
                <Key>
                    <PropertyRef Name="id" />
                </Key>
                <Property Name="id" Type="Edm.String" Nullable="false" />
                <Property Name="initialDomainName" Type="Edm.String" />
                <Property Name="displayName" Type="Edm.String" />
                <Property Name="status" Type="Edm.String" />
                <Property Name="additionalInformation" Type="Edm.String" />
            </EntityType>
            <EntityType Name="privilegedFeatureFlight">
                <Key>
                    <PropertyRef Name="id" />
                </Key>
                <Property Name="id" Type="Edm.String" Nullable="false" />
                <Property Name="displayName" Type="Edm.String" />
                <Property Name="description" Type="Edm.String" />
                <Property Name="settings" Type="Edm.String" />
                <Property Name="scope" Type="
                Microsoft.Identity.Governance.Common.Data.ExternalModels.V1.FeatureScope"
                />
                <Property Name="state" Type="
```

→ SQLalchemy roadlib schema → Sqlite database

Extending the schema



Calculating relationships with custom mappings

```
{'Conditions': {'Applications': {'Include': [{'Applications': ['All']}]},
                'Users': {'Include': [{'Users': ['2e673139-c815-42dd-86e6-2746a0627b7d']}]}},
 'Controls': [{'AuthStrengthIds': ['00000000-0000-0000-0000-000000000004']}],
 'CreatedDateTime': '2024-06-07T11:25:10.6192774Z',
 'EnforceAllPoliciesForEas': True,
 'IncludeOtherLegacyClientTypeForEvaluation': True,
 'ModifiedDateTime': '2024-07-24T12:42:34.9664604Z',
 'State': 'Enabled',
 'Version': 1}
```

User database class

```
class User(Base, SerializeMixin):
    __tablename__ = "Users"
    objectType = Column(Text)
    objectId = Column(Text, primary_key=True)
    deletionTimestamp = Column(DateTime)
    acceptedAs = Column(Text)
    acceptedOn = Column(DateTime)
    accountEnabled = Column(Boolean)
    ageGroup = Column(Text)
    alternativeSecurityIds = Column(JSON)
    signInNames = Column(JSON)
    signInNamesInfo = Column(JSON)
    appMetadata = Column(JSON)
    assignedLicenses = Column(JSON)
    assignedPlans = Column(JSON)
    city = Column(Text)
```

Establishing links to other schemas

```
ownedGroups = relationship("Group",
    secondary=lnk_group_owner_user,
    back_populates="ownerUsers")

memberOfAu = relationship("AdministrativeUnit",
    secondary=lnk_au_member_user,
    back_populates="memberUsers")

policiesIncluded = relationship("Policy",
    secondary=lnk_policy_user_include,
    back_populates="includedUsers")

policiesExcluded = relationship("Policy",
    secondary=lnk_policy_user_exclude,
    back_populates="excludedUsers")

pimRoleAssignments = relationship("PIMgovernanceRoleAssignment",
    secondary=lnk_pim_roleassignment_subjectuser,
    back_populates="subjectUser")

pimRoleAssignmentRequests = relationship("PIMgovernanceRoleAssignmentRequest",
    secondary=lnk_pim_roleassignmentrequest_subjectuser,
    back_populates="subjectUser")
```

ROADrecon demo 3 – Entitlement Management

Microsoft Entra ID Governance

- Identity Governance
  - Privileged Identity Management
  - Entitlement Management
  - Lifecycle management / access reviews

Licenses

- **Microsoft Entra ID Governance** - Microsoft Entra ID Governance is an advanced set of identity governance capabilities available for Microsoft Entra ID P1 and P2 customers. Microsoft Entra ID Governance is available as six products **Microsoft Entra ID Governance**, **Microsoft Entra ID Governance Step Up for Microsoft Entra ID P2**, **Entra ID Governance Frontline Worker**, **Microsoft Entra ID Governance Step up for Microsoft Entra ID F2**, **Microsoft Entra ID Governance for Government** and **Microsoft Entra ID Governance Add-on for Microsoft Entra ID P2 for Government**. These six products differ only in their prerequisites; they contain both the entitlement management, privileged identity management and access reviews capabilities that were in Microsoft Entra ID P2, and additional advanced identity governance capabilities. The following section goes into more detail on the different prerequisites of these products.

Focus: Entitlement Management

- Entitlement Management allows you to create access packages
- Access Packages contain resources that can be granted to users:
  - Group membership
  - Application access
  - Role access
  - SharePoint sites
  - API permissions
- Can be scoped to internal and guest users, service principals, AI agents

Entitlement Management enumeration

- Unfortunately requires Global Reader or Security Reader to enumerate all packages.
- Your own packages can be listed on https://myaccess.microsoft.com
- Again, the Azure CLI has the *user_impersonation* scope on the required internal API https://elm.iga.azure.com

Access Packages abuse paths

- Entitlement Management is a very privileged service completely outside of the Entra ID control plane.
- Access packages may contain access to roles or groups that grant privileges. Abuse options:
  - Access packages without approval scoped to compromised account.
  - Control over both the account and one of the approver accounts.
  - Social engineer approval from manager or other person.

Access Packages abuse paths

- **EntitlementManagement.ReadWrite.All** Microsoft Graph permission gives full control of EM features. Aka privilege escalation to Global Admin.
- “Identity Governance Administrator” Entra ID role grants the same rights.
  - Privilege escalation to Global Admin possible provided resources with GA rights exist or you have an ID Governance license which allows you to add API rights and Entra ID roles in the packages.

☐	Hybrid Identity Administrator	Can manage AD to Microsoft Entra cloud provisioning, Microsoft Entra Connect, and federation settings.	PRIVILEGED	1	Built-in
☐	Identity Governance Administrator	Manage access using Microsoft Entra ID Governance scenarios.		1	Built-in
☐	Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.	PRIVILEGED	0	Built-in

???

Wrapping it all up – Azure CLI refresh token

```
(ROADtools) → ROADtools git:(master) ✗ roadrecon gatherall --autotoken -d all.db
Enumerating AAD Graph
Starting data gathering phase 1 of 2 (collecting objects)
Starting data gathering phase 2 of 2 (collecting properties and relationships)
ROADrecon gather executed in 55.54 seconds and issued 5876 HTTP requests.
Enumerating IG data
Phase 1 - gather data
Starting data gathering
Phase 2 - calculate access package scopes
ROADrecon gather executed in 4.42 seconds and issued 13 HTTP requests.
Enumerating PIM data
Starting data gathering
ROADrecon gather executed in 28.46 seconds and issued 127 HTTP requests.
Enumerating Azure data
Starting data gathering phase 1 of 2 (collecting objects)
Sleeping because of rate-limit hit
Phase 2 - calculate IAM permissions
ROADrecon gather executed in 15.04 seconds and issued 5 HTTP requests.
```

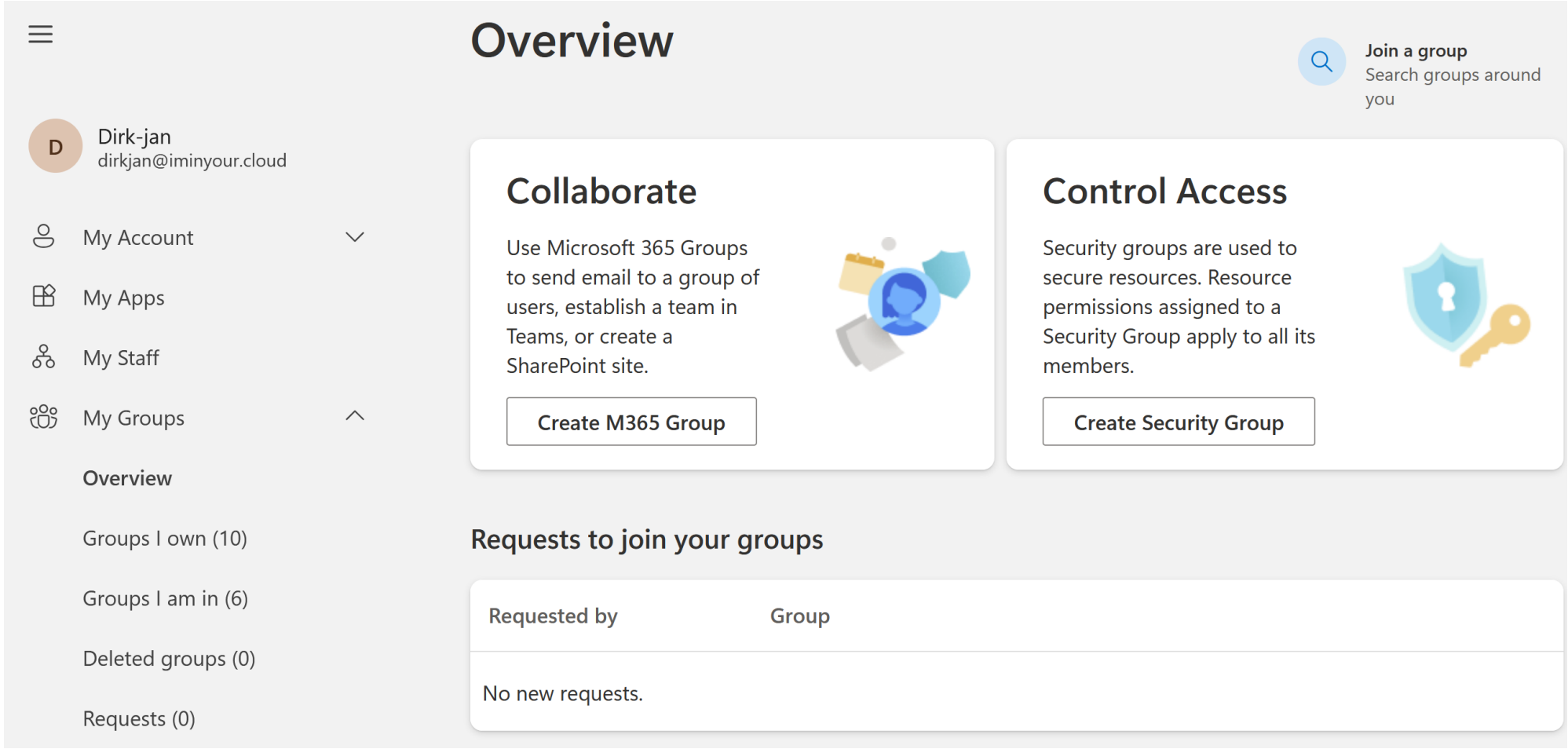
The wrap-up: new ROADrecon features

- Support for CA policies per user in the UI
- Azure permissions support
- PIM support (groups/roles/azure roles)
- Entitlement Management support (access packages)

- Not yet live on GitHub but will be released soon™

Extra stuff

Bonus – Public groups



Overview

Join a group
Search groups around you

D
Dirk-jan
dirkjan@iminyour.cloud

- My Account
- My Apps
- My Staff
- My Groups
  - Overview
  - Groups I own (10)
  - Groups I am in (6)
  - Deleted groups (0)
  - Requests (0)
- My Access

Give feedback

New Security group

Name *

Group name

Description

Tell people the purpose of your group

Policy *

This group is open to join for all users

- Select policy type
- This group is open to join for all users
- This group requires owner approval
- Only the owner of this group and admins can add members

ROADrecon demo 4 – Public Groups and Azure