#RSAC

RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: CLS-R02

Your Microsoft Cloud Is the Attacker's Computer

Sean Metcalf

Identity Security Architect
TrustedSec
https://www.linkedin.com/in/seanmmetcalf/
@PyroTek3

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

About Me

- Identity Security Architect at TrustedSec
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, Blue Team Con, BSides Charm, BSides DC, BSides PR, DEFCON, DerbyCon, TEC, & Troopers
- Former Microsoft MVP
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org (Microsoft identity security info)

Agenda

- Introduction
- Entra ID Highly Privileged Roles & Applications
- Entra ID Security Posture
- Conditional Access Policy & CAP Gaps
- Attacking Entra ID
- From Entra ID to Azure to Active Directory
- Securing Entra ID Administration
- Conclusion

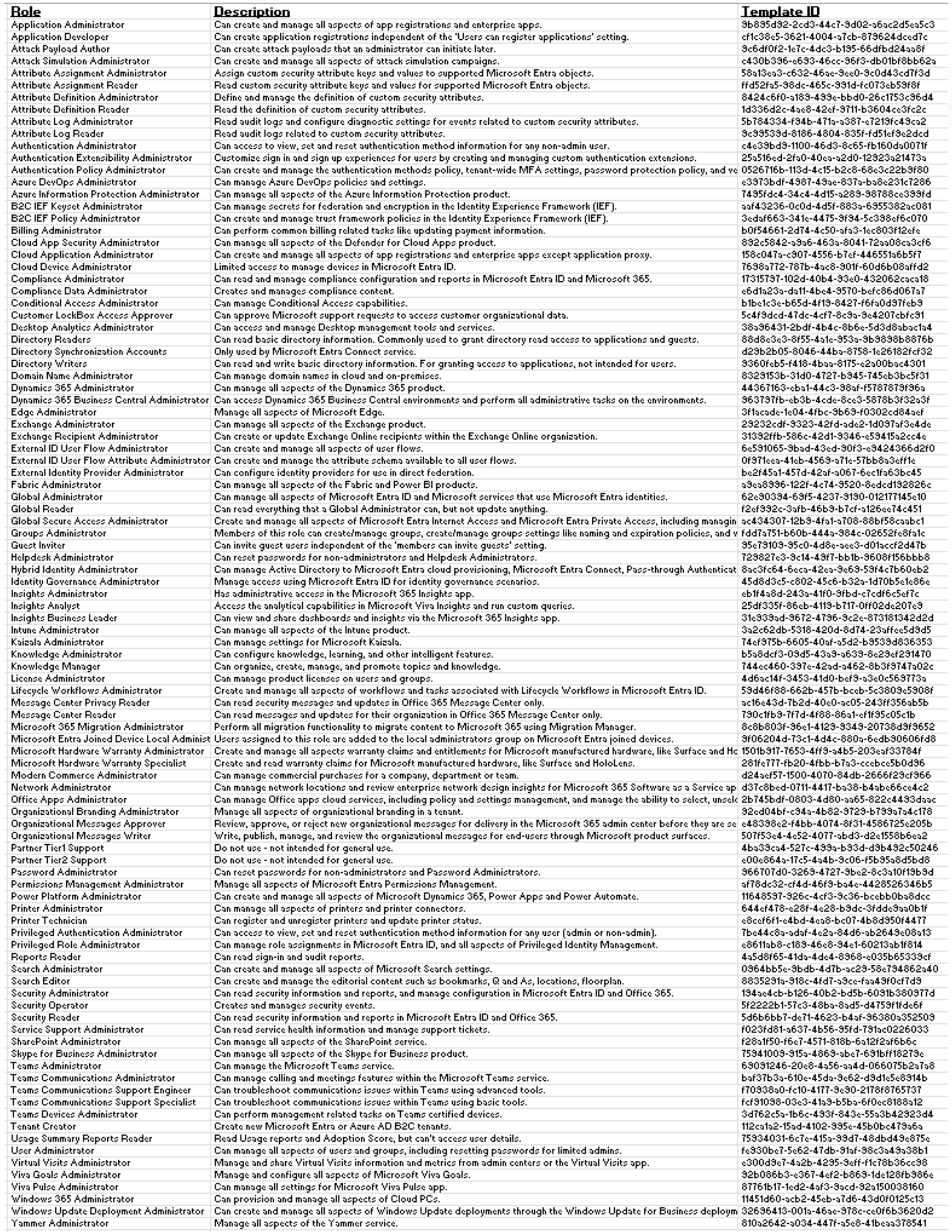
RSAC | 2025 Conference

Entra ID Level 0

Like Tier 0, but Different!

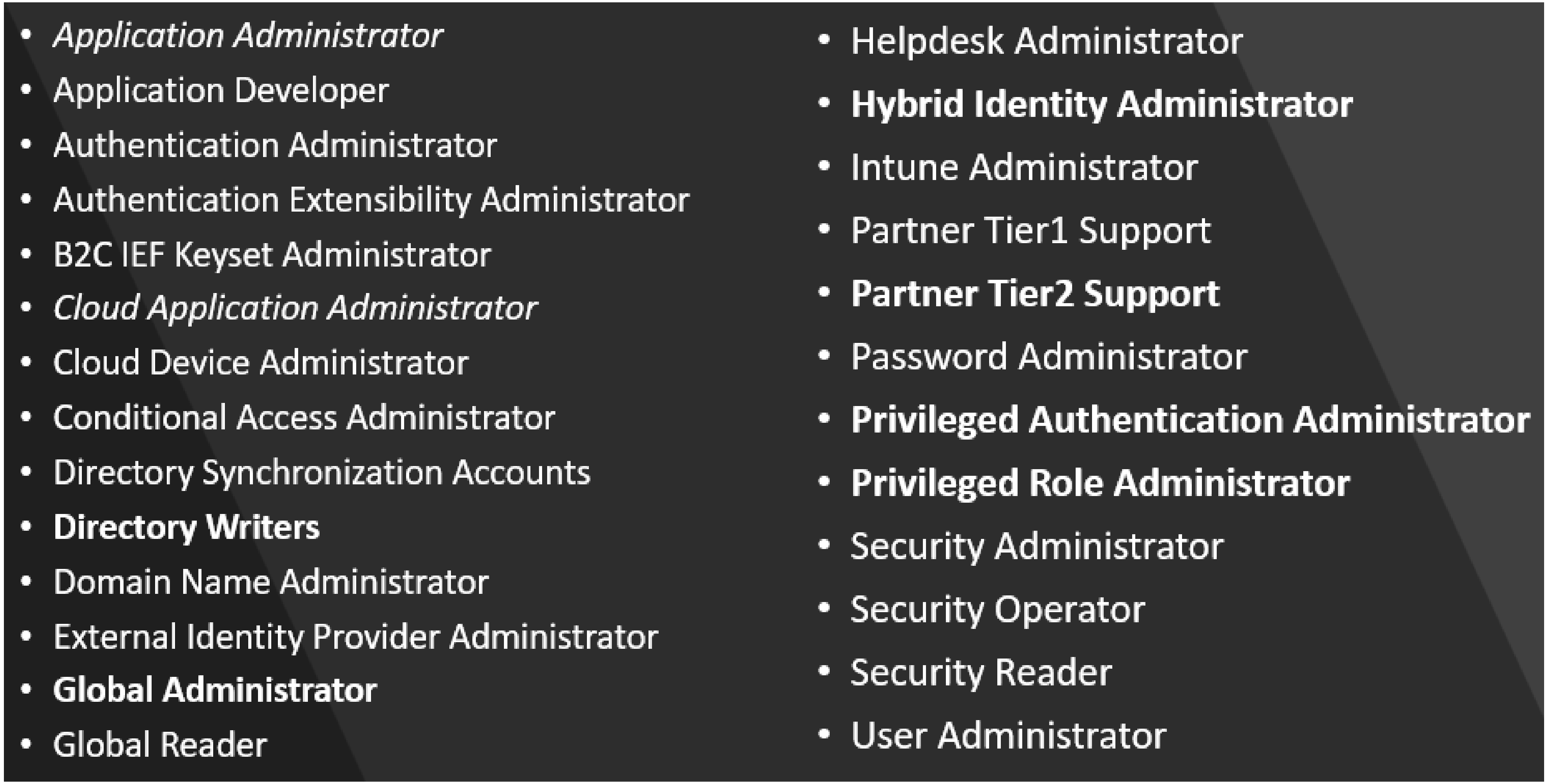
Many Voices.
One Community.

There are >100 Entra ID Roles!



Role	Description	Template ID
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	cf1c38e5-3621-4004-a7cb-879624dced7c
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	9c6df0f2-1e7c-4dc3-b195-66dfbd24aa8f
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	c430b396-e693-46cc-96f3-db01bf8bb62a
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.	58a13ea3-c632-46ae-9ee0-9c0d43cd7f3d
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.	ffd52fa5-98dc-465c-991d-fc073eb59f8f
Attribute Definition Administrator	Define and manage the definition of custom security attributes.	8424c6f0-a189-499e-bbd0-26c1753c96d4
Attribute Definition Reader	Read the definition of custom security attributes.	1d336d2c-4ae8-42ef-9711-b3604ce3fc2c
Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attributes.	5b784334-f94b-471a-a387-e7219fc49ca2
Attribute Log Reader	Read audit logs related to custom security attributes.	9c99539d-8186-4804-835f-fd51ef9e2dcd
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	c4e39bd9-1100-46d3-8c65-fb160da0071f
Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	25a516ed-2fa0-40ea-a2d0-12923a21473a
Authentication Policy Administrator	Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and ve	0526716b-113d-4c15-b2c8-68e3c22b9f80
Azure DevOps Administrator	Can manage Azure DevOps policies and settings.	e3973bdf-4987-49ae-837a-ba8e231c7286
Azure Information Protection Administrator	Can manage all aspects of the Azure Information Protection product.	7495fdc4-34c4-4d15-a289-98788ce399fd
B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	aaf43236-0c0d-4d5f-883a-6955382ac081
B2C IEF Policy Administrator	Can create and manage trust framework policies in the Identity Experience Framework (IEF).	3edaf663-341e-4475-9f94-5c398ef6c070
Billing Administrator	Can perform common billing related tasks like updating payment information.	b0f54661-2d74-4c50-afa3-1ec803f12efe
Cloud App Security Administrator	Can manage all aspects of the Defender for Cloud Apps product.	892c5842-a9a6-463a-8041-72aa08ca3cf6
Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except application proxy.	158c047a-c907-4556-b7ef-446551a6b5f7
Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	7698a772-787b-4ac8-901f-60d6b08affd2
Compliance Administrator	Can read and manage compliance configuration and reports in Microsoft Entra ID and Microsoft 365.	17315797-102d-40b4-93e0-432062caca18
Compliance Data Administrator	Creates and manages compliance content.	e6d1a23a-da11-4be4-9570-befc86d067a7
Conditional Access Administrator	Can manage Conditional Access capabilities.	b1be1c3e-b65d-4f19-8427-f6fa0d97feb9
Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data.	5c4f9dcd-47dc-4cf7-8c9a-9e4207cbfc91
Desktop Analytics Administrator	Can access and manage Desktop management tools and services.	38a96431-2bdf-4b4c-8b6e-5d3d8abac1a4
Directory Readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	88d8e3e3-8f55-4a1e-953a-9b9898b8876b
Directory Synchronization Accounts	Only used by Microsoft Entra Connect service.	d29b2b05-8046-44ba-8758-1e26182fcf32
Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	9360feb5-f418-4baa-8175-e2a00bac4301
Domain Name Administrator	Can manage domain names in cloud and on-premises.	8329153b-31d0-4727-b945-745eb3bc5f31
Dynamics 365 Administrator	Can manage all aspects of the Dynamics 365 product.	44367163-eba1-44c3-98af-f5787879f96a
Dynamics 365 Business Central Administrator	Can access Dynamics 365 Business Central environments and perform all administrative tasks on the environments.	963797fb-eb3b-4cde-8ce3-5878b3f32a3f
Edge Administrator	Manage all aspects of Microsoft Edge.	3f1acade-1e04-4fbc-9b69-f0302cd84aef
Exchange Administrator	Can manage all aspects of the Exchange product.	29232cdf-9323-42fd-ade2-1d097af3e4de
Exchange Recipient Administrator	Can create or update Exchange Online recipients within the Exchange Online organization.	31392ffb-586c-42d1-9346-e59415a2cc4e
External ID User Flow Administrator	Can create and manage all aspects of user flows.	6e591065-9bad-43ed-90f3-e9424366d2f0
External ID User Flow Attribute Administrator	Can create and manage the attribute schema available to all user flows.	0f971eea-41eb-4569-a71e-57bb8a3eff1e
External Identity Provider Administrator	Can configure identity providers for use in direct federation.	be2f45a1-457d-42af-a067-6ec1fa63bc45
Fabric Administrator	Can manage all aspects of the Fabric and Power BI products.	a9ea8996-122f-4c74-9520-8edcd192826c
Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	62e90394-69f5-4237-9190-012177145e10
Global Reader	Can read everything that a Global Administrator can, but not update anything.	f2ef992c-3afb-46b9-b7cf-a126ee74c451
Global Secure Access Administrator	Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managin	ac434307-12b9-4fa1-a708-88bf58caabc1
Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and v	fdd7a751-b60b-444a-984c-02652fe8fa1c
Guest Inviter	Can invite guest users independent of the 'members can invite guests' setting.	95e79109-95c0-4d8e-aee3-d01accf2d47b
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	729827e3-9c14-49f7-bb1b-9608f156bbb8
Hybrid Identity Administrator	Can manage Active Directory to Microsoft Entra cloud provisioning, Microsoft Entra Connect, Pass-through Authenticat	8ac3fc64-6eca-42ea-9e69-59f4c7b60eb2
Identity Governance Administrator	Manage access using Microsoft Entra ID for identity governance scenarios.	45d8d3c5-c802-45c6-b32a-1d70b5e1e86e
Insights Administrator	Has administrative access in the Microsoft 365 Insights app.	eb1f4a8d-243a-41f0-9fbd-c7cdf6c5ef7c
Insights Analyst	Access the analytical capabilities in Microsoft Viva Insights and run custom queries.	25df335f-86eb-4119-b717-0ff02de207e9
Insights Business Leader	Can view and share dashboards and insights via the Microsoft 365 Insights app.	31e939ad-9672-4796-9c2e-873181342d2d
Intune Administrator	Can manage all aspects of the Intune product.	3a2c62db-5318-420d-8d74-23affee5d9d5
Kaizala Administrator	Can manage settings for Microsoft Kaizala.	74ef975b-6605-40af-a5d2-b9539d836353
Knowledge Administrator	Can configure knowledge, learning, and other intelligent features.	b5a8dcf3-09d5-43a9-a639-8e29ef291470
Knowledge Manager	Can organize, create, manage, and promote topics and knowledge.	744ec460-397e-42ad-a462-8b3f9747a02c
License Administrator	Can manage product licenses on users and groups.	4d6ac14f-3453-41d0-bef9-a3e0c569773a
Lifecycle Workflows Administrator	Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra ID.	59d46f88-662b-457b-bceb-5c3809e5908f
Message Center Privacy Reader	Can read security messages and updates in Office 365 Message Center only.	ac16e43d-7b2d-40e0-ac05-243ff356ab5b
Message Center Reader	Can read messages and updates for their organization in Office 365 Message Center only.	790c1fb9-7f7d-4f88-86a1-ef1f95c05c1b
Microsoft 365 Migration Administrator	Perform all migration functionality to migrate content to Microsoft 365 using Migration Manager.	8c8b803f-96e1-4129-9349-20738d9f9652
Microsoft Entra Joined Device Local Administ	Users assigned to this role are added to the local administrators group on Microsoft Entra joined devices.	9f06204d-73c1-4d4c-880a-6edb90606fd8
Microsoft Hardware Warranty Administrator	Create and manage all aspects warranty claims and entitlements for Microsoft manufactured hardware, like Surface and Hc	1501b917-7653-4ff9-a4b5-203eaf33784f
Microsoft Hardware Warranty Specialist	Create and read warranty claims for Microsoft manufactured hardware, like Surface and HoloLens.	281fe777-fb20-4fbb-b7a3-ccebce5b0d96
Modern Commerce Administrator	Can manage commercial purchases for a company, department or team.	d24aef57-1500-4070-84db-2666f29cf966
Network Administrator	Can manage network locations and review enterprise network design insights for Microsoft 365 Software as a Service ap	d37c8bed-0711-4417-ba38-b4abe66ce4c2
Office Apps Administrator	Can manage Office apps cloud services, including policy and settings management, and manage the ability to select, unsele	2b745bdf-0803-4d80-aa65-822c4493daac
Organizational Branding Administrator	Manage all aspects of organizational branding in a tenant.	92ed04bf-c94a-4b82-9729-b799a7a4c178
Organizational Messages Approver	Review, approve, or reject new organizational messages for delivery in the Microsoft 365 admin center before they are se	e48398e2-f4bb-4074-8f31-4586725e205b
Organizational Messages Writer	Write, publish, manage, and review the organizational messages for end-users through Microsoft product surfaces.	507f53e4-4e52-4077-abd3-d2e1558b6ea2
Partner Tier1 Support	Do not use - not intended for general use.	4ba39ca4-527c-499a-b93d-d9b492c50246
Partner Tier2 Support	Do not use - not intended for general use.	e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8
Password Administrator	Can reset passwords for non-administrators and Password Administrators.	966707d0-3269-4727-9be2-8c3a10f19b9d
Permissions Management Administrator	Manage all aspects of Microsoft Entra Permissions Management.	af78dc32-cf4d-46f9-ba4e-4428526346b5
Power Platform Administrator	Can create and manage all aspects of Microsoft Dynamics 365, Power Apps and Power Automate.	11648597-926c-4cf3-9c36-bcebb0ba8dcc
Printer Administrator	Can manage all aspects of printers and printer connectors.	644ef478-e28f-4e28-b9dc-3fdde9aa0b1f
Printer Technician	Can register and unregister printers and update printer status.	e8cef6f1-e4bd-4ea8-bc07-4b8d950f4477
Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).	7be44c8a-adaf-4e2a-84d6-ab2649e08a13
Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.	e8611ab8-c189-46e8-94e1-60213ab1f814
Reports Reader	Can read sign-in and audit reports.	4a5d8f65-41da-4de4-8968-e035b65339cf
Search Administrator	Can create and manage all aspects of Microsoft Search settings.	0964bb5e-9bdb-4d7b-ac29-58e794862a40
Search Editor	Can create and manage the editorial content such as bookmarks, Q and As, locations, floorplan.	8835291a-918c-4fd7-a9ce-faa49f0cf7d9
Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.	194ae4cb-b126-40b2-bd5b-6091b380977d
Security Operator	Creates and manages security events.	5f2222b1-57c3-48ba-8ad5-d4759f1fde6f
Security Reader	Can read security information and reports in Microsoft Entra ID and Office 365.	5d6b6bb7-de71-4623-b4af-96380a352509
Service Support Administrator	Can read service health information and manage support tickets.	f023fd81-a637-4b56-95fd-791ac0226033
SharePoint Administrator	Can manage all aspects of the SharePoint service.	f28a1f50-f6e7-4571-818b-6a12f2af6b6c
Skype for Business Administrator	Can manage all aspects of the Skype for Business product.	75941009-915a-4869-abe7-691bff18279e
Teams Administrator	Can manage the Microsoft Teams service.	69091246-20e8-4a56-aa4d-066075b2a7a8
Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.	baf37b3a-610e-45da-9e62-d9d1e5e8914b
Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.	f70938a0-fc10-4177-9e90-2178f8765737
Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.	fcf91098-03e3-41a9-b5ba-6f0ec8188a12
Teams Devices Administrator	Can perform management related tasks on Teams certified devices.	3d762c5a-1b6c-493f-843e-55a3b42923d4
Tenant Creator	Create new Microsoft Entra or Azure AD B2C tenants.	112ca1a2-15ad-4102-995e-45b0bc479a6a
Usage Summary Reports Reader	Read Usage reports and Adoption Score, but can't access user details.	75934031-6c7e-415a-99d7-48dbd49e875e
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	fe930be7-5e62-47db-91af-98c3a49a38b1
Virtual Visits Administrator	Manage and share Virtual Visits information and metrics from admin centers or the Virtual Visits app.	e300d9e7-4a2b-4295-9eff-f1c78b36cc98
Viva Goals Administrator	Manage and configure all aspects of Microsoft Viva Goals.	92b086b3-e367-4ef2-b869-1de128fb986e
Viva Pulse Administrator	Can manage all settings for Microsoft Viva Pulse app.	87761b17-1ed2-4af3-9acd-92a150038160
Windows 365 Administrator	Can provision and manage all aspects of Cloud PCs.	11451d60-acb2-45eb-a7d6-43d0f0125c13
Windows Update Deployment Administrator	Can create and manage all aspects of Windows Update deployments through the Windows Update for Business deploym	32696413-001a-46ae-978c-ce0f6b3620d2
Yammer Administrator	Manage all aspects of the Yammer service.	810a2642-a034-447f-a5e8-41beaa378541

Microsoft’s Privileged Entra ID Roles List [PRIVILEGED]



- *Application Administrator*
- Application Developer
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- *Cloud Application Administrator*
- Cloud Device Administrator
- Conditional Access Administrator
- Directory Synchronization Accounts
- **Directory Writers**
- Domain Name Administrator
- External Identity Provider Administrator
- **Global Administrator**
- Global Reader
- Helpdesk Administrator
- **Hybrid Identity Administrator**
- Intune Administrator
- Partner Tier1 Support
- **Partner Tier2 Support**
- Password Administrator
- **Privileged Authentication Administrator**
- **Privileged Role Administrator**
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

26 roles: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Level 0 Entra ID Roles (5)

Effective Full Admin Rights or Capability to Gain Full Admin to Entra ID

- **Global Administrator**
  - Full admin rights to the Entra ID, Microsoft 365, and 1-click full control of all Azure subscriptions
    From Azure AD to Active Directory (via Azure) – An Unanticipated Attack Path (2020)

- **Hybrid Identity Administrator**
  - *"Can create, manage and deploy provisioning configuration setup from Active Directory to Microsoft Entra ID using Cloud Provisioning as well as manage Microsoft Entra Connect, Pass-through Authentication (PTA), Password hash synchronization (PHS), Seamless Single Sign-On (Seamless SSO), and **federation settings**."*
    https://medium.com/tenable-techblog/roles-allowing-to-abuse-entra-id-federation-for-persistence-and-privilege-escalation-df9ca6e58360

- **Partner Tier2 Support**
  - *"The Partner Tier2 Support role can reset passwords and invalidate refresh tokens for all non-administrators and administrators (including Global Administrators). "*

    "not quite as powerful as Global Admin, but the role does allow a principal with the role to promote themselves or any other principal to Global Admin."
    The Most Dangerous Entra Role You've (Probably) Never Heard Of

- **Privileged Authentication Administrator**
  - *Microsoft: "do not use."*
    "Set or reset any authentication method (including passwords) for any user, including Global Administrators. …
    Force users to re-register against existing non-password credential (such as MFA or FIDO) and revoke remember MFA on the device, prompting for MFA on the next sign-in of all users."

- **Privileged Role Administrator**
  - *"Users with this role can manage role assignments in Microsoft Entra ID, as well as within Microsoft Entra Privileged Identity Management. …*
    This role grants the ability to manage assignments for all Microsoft Entra roles including the Global Administrator role. "

Level 1 Entra ID Roles (1 of 2)

Highly Privileged Rights that have Privilege Escalation Potential Depending on Tenant Configuration or ability to reconfigure the security posture of the tenant

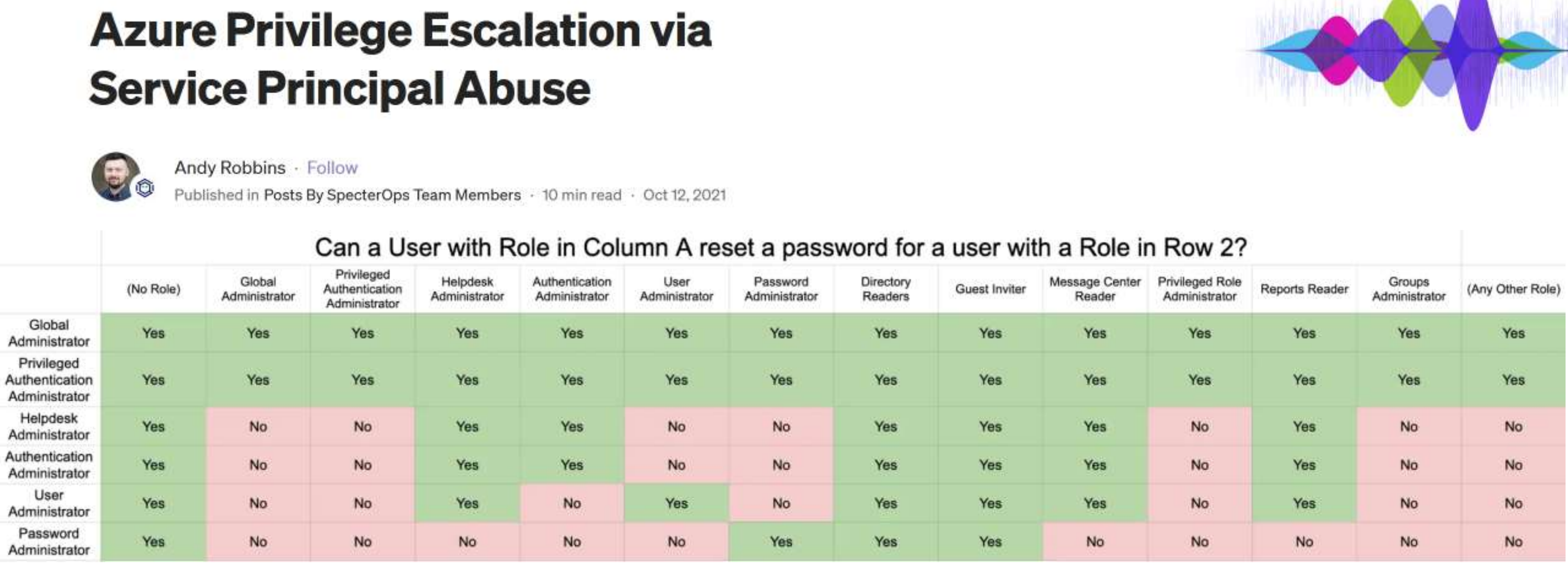
Role	Microsoft Description
Application Administrator	This is a privileged role. Users in this role can create and manage all aspects of enterprise applications, application registrations, and application proxy settings.
Authentication Administrator	This is a privileged role. Set or reset any authentication method (including passwords) for non-administrators and some roles. Require users who are non-administrators or assigned to some roles to re-register against existing non-password credentials (for example, MFA or FIDO), and can also revoke remember MFA on the device, which prompts for MFA on the next sign-in. Perform sensitive actions for some users.
Domain Name Administrator	This is a privileged role. Users with this role can manage (read, add, verify, update, and delete) domain names. Can be used in federation attacks.
Microsoft Entra Joined Device Local Administrator	During Microsoft Entra join, this group is added to the local Administrators group on the device.
Cloud Application Administrator	This is a privileged role. Users in this role have the same permissions as the Application Administrator role, excluding the ability to manage application proxy. This role grants the ability to create and manage all aspects of enterprise applications and application registrations.
Conditional Access Administrator	This is a privileged role. Users with this role have the ability to manage Microsoft Entra Conditional Access settings.
Directory Synchronization Accounts	This is a privileged role. Do not use. This role is automatically assigned to the Microsoft Entra Connect service, and is not intended or supported for any other use. Privileged rights: Update application credentials, Manage hybrid authentication policy in Microsoft Entra ID, Update basic properties on policies, & Update credentials of service principals
Directory Writers	This is a privileged role. Users in this role can read and update basic information of users, groups, and service principals. Privileged rights: Create & update OAuth 2.0 permission grants, add/disable/enable users, Force sign-out by invalidating user refresh tokens, & Update User Principal Name of users.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Level 1 Entra ID Roles (2 of 2)

Role	Microsoft Description
Exchange Administrator	Users with this role have global permissions within Microsoft Exchange Online. Trimarc flags this role since it is a role that threat actors target.
External Identity Provider Administrator	This is a privileged role. This administrator manages federation between Microsoft Entra organizations and external identity providers. With this role, users can add new identity providers and configure all available settings (e.g. authentication path, service ID, assigned key containers). This user can enable the Microsoft Entra organization to trust authentications from external identity providers.
Helpdesk Administrator	This is a privileged role. Users with this role can change passwords, & invalidate refresh tokens, Invalidating a refresh token forces the user to sign in again.
Intune Administrator	This is a privileged role. Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups. Privileged rights: Read Bitlocker metadata and key on devices
Password Administrator	This is a privileged role. Users with this role have limited ability to manage passwords.
Partner Tier1 Support	This is a privileged role. Do not use. The Partner Tier1 Support role can reset passwords and invalidate refresh tokens for only non-administrators. Privileged rights: Update application credentials, Create and delete OAuth 2.0 permission grants, & read and update all properties
Security Administrator	This is a privileged role. Users with this role have permissions to manage security-related features in the Microsoft 365 Defender portal, Microsoft Entra ID Protection, Microsoft Entra Authentication, Azure Information Protection, and Microsoft Purview compliance portal.
User Administrator	This is a privileged role. Can reset passwords for users.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference



Azure Privilege Escalation via Service Principal Abuse

Andy Robbins · Follow

Published in Posts By SpecterOps Team Members · 10 min read · Oct 12, 2021

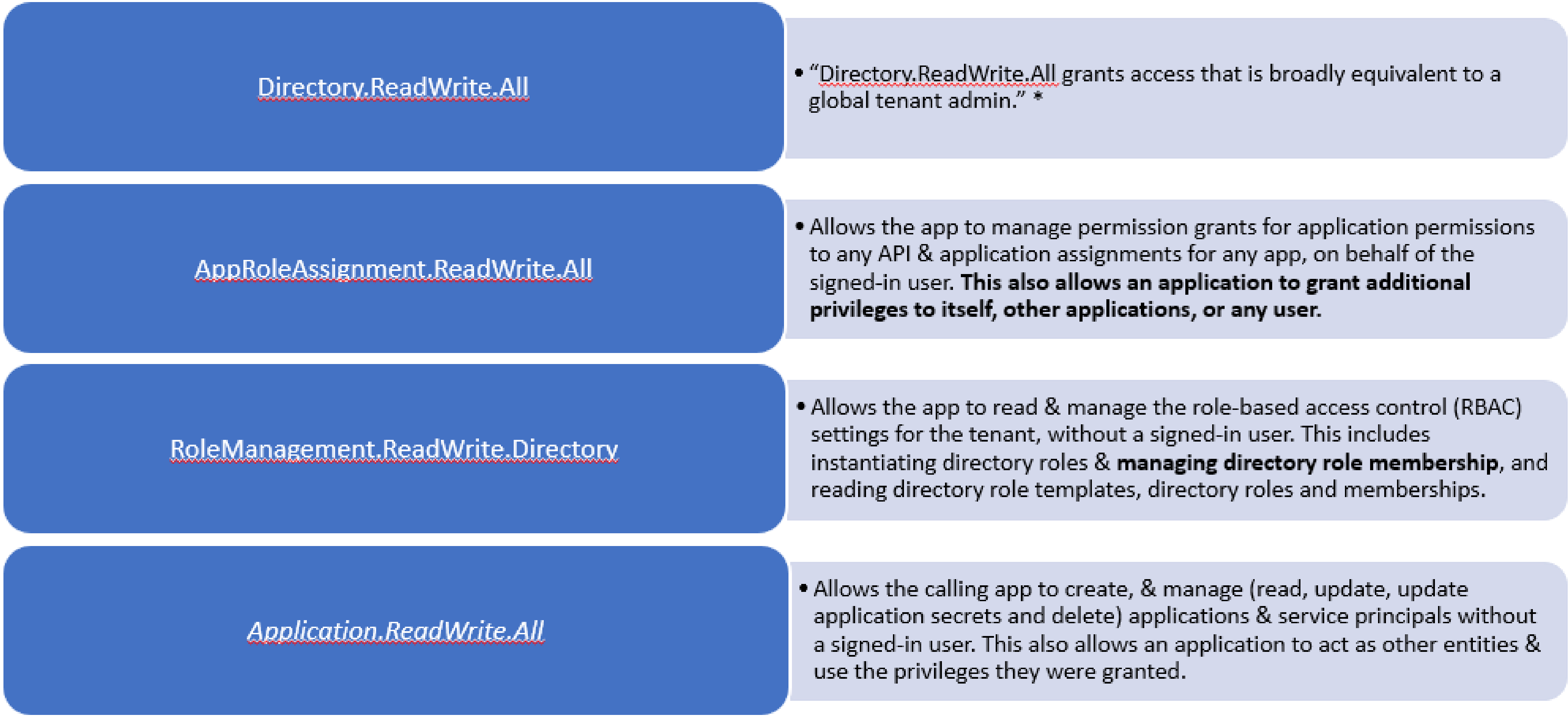
Can a User with Role in Column A reset a password for a user with a Role in Row 2?

	(No Role)	Global Administrator	Privileged Authentication Administrator	Helpdesk Administrator	Authentication Administrator	User Administrator	Password Administrator	Directory Readers	Guest Inviter	Message Center Reader	Privileged Role Administrator	Reports Reader	Groups Administrator	(Any Other Role)
Global Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Privileged Authentication Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Helpdesk Administrator	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	No	No
Authentication Administrator	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	No	No
User Administrator	Yes	No	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	No
Password Administrator	Yes	No	No	No	No	No	Yes	Yes	Yes	No	No	No	No	No

https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5

Level 0 Applications

Effective Full Admin Rights or Capability to Gain Full Admin to Entra ID



Directory.ReadWrite.All

- “Directory.ReadWrite.All grants access that is broadly equivalent to a global tenant admin.” *

AppRoleAssignment.ReadWrite.All

- Allows the app to manage permission grants for application permissions to any API & application assignments for any app, on behalf of the signed-in user. **This also allows an application to grant additional privileges to itself, other applications, or any user.**

RoleManagement.ReadWrite.Directory

- Allows the app to read & manage the role-based access control (RBAC) settings for the tenant, without a signed-in user. This includes instantiating directory roles & **managing directory role membership**, and reading directory role templates, directory roles and memberships.

Application.ReadWrite.All

- Allows the calling app to create, & manage (read, update, update application secrets and delete) applications & service principals without a signed-in user. This also allows an application to act as other entities & use the privileges they were granted.

RSAC 2025 Conference

Entra ID Security Posture

Many Voices.
One Community.

Unfortunate Defaults

Users:

Can register applications

Can consent to applications

Can create new tenants

Can join/hybrid join devices to the tenant & no MFA is required

Guests/External Accounts

Guests have the same view rights as users

Guests can invite other guests

Entra ID Common Security Issues

Privileged Account Issues

- Standard user accounts are members
- Service Accounts / Service Principals are members
- Account(s) authenticate from user workstations
- Using PIM, but all/most are permanently active, not eligible.
- MFA not configured on highly privileged role members

Applications with Highly Privileged Permissions

- Highly privileged applications (Trimarc Level 0) with standard user account as owner
- Standard user account in Application Administrator and/or Cloud Application Administration role(s).

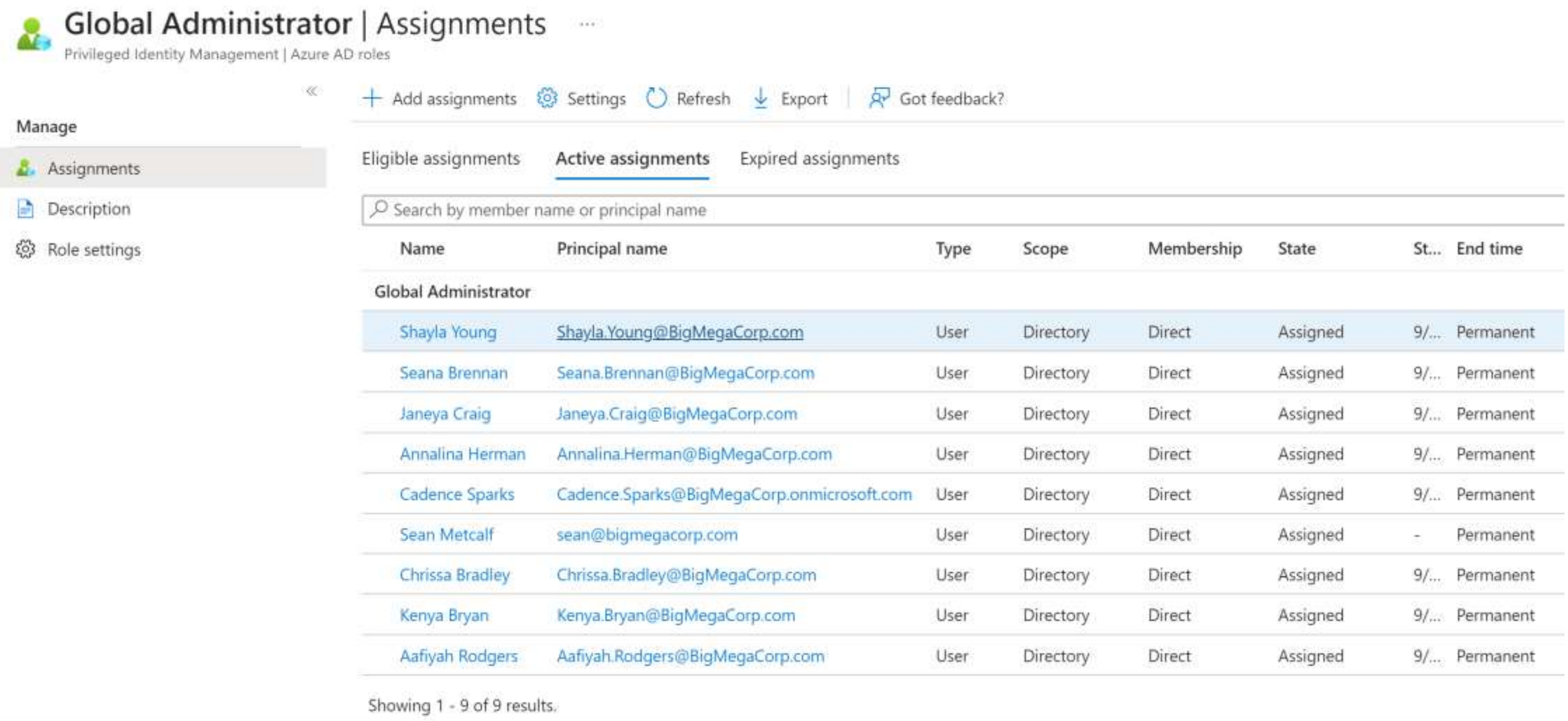
Group Nesting

- Role Assignable Groups in highly privileged roles (Trimarc Level 0)

Partner Access - Delegated Access Permissions

- Global Administrator
- Helpdesk Administrator

Highly Privileged User Accounts



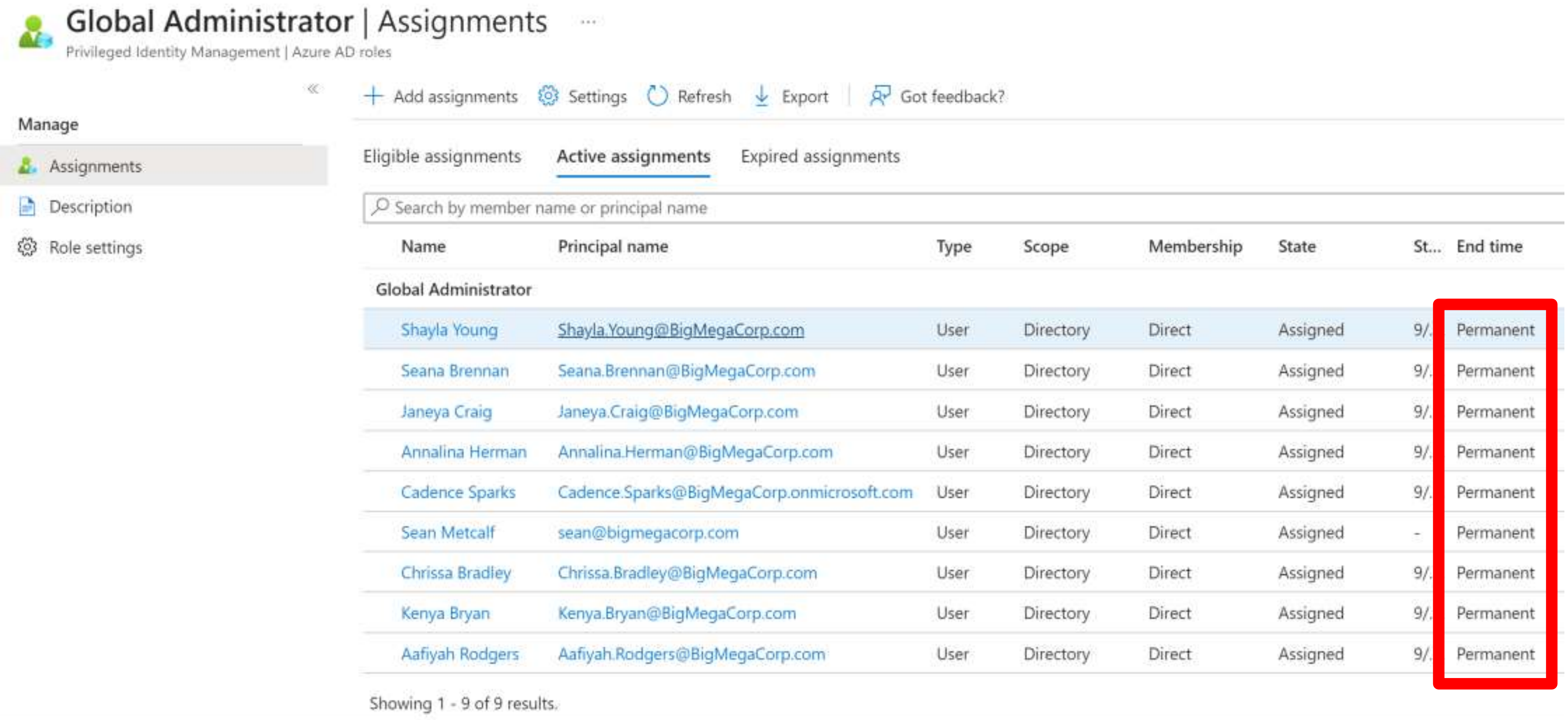
Global Administrator | Assignments

Privileged Identity Management | Azure AD roles

Name	Principal name	Type	Scope	Membership	State	St...	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/...	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent

Showing 1 - 9 of 9 results.

PIM Members are Permanent, Not Eligible



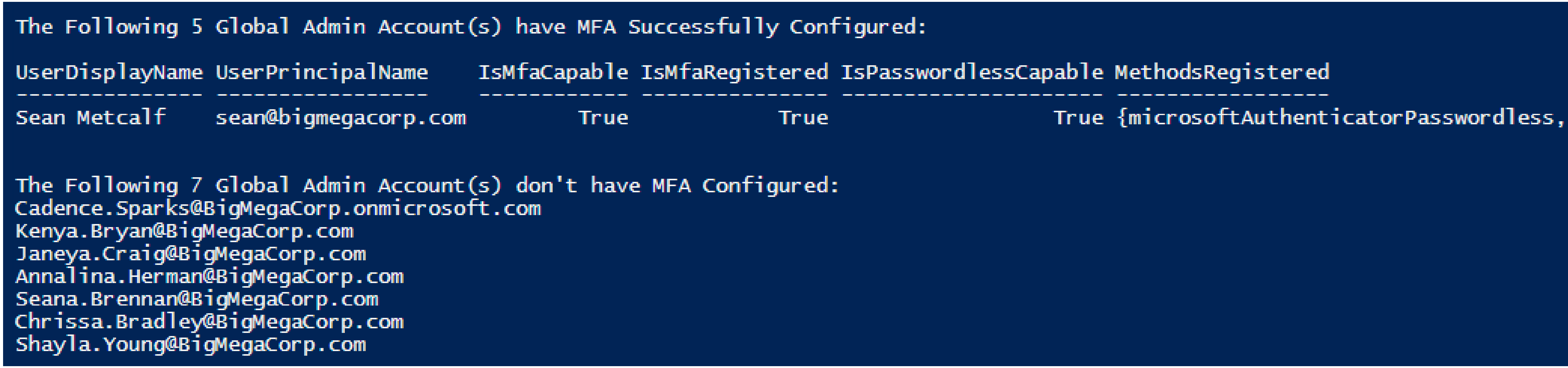
Global Administrator | Assignments

Privileged Identity Management | Azure AD roles

Name	Principal name	Type	Scope	Membership	State	St...	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/.	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/.	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/.	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/.	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/.	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/.	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/.	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/.	Permanent

Showing 1 - 9 of 9 results.

Admin Accounts without MFA



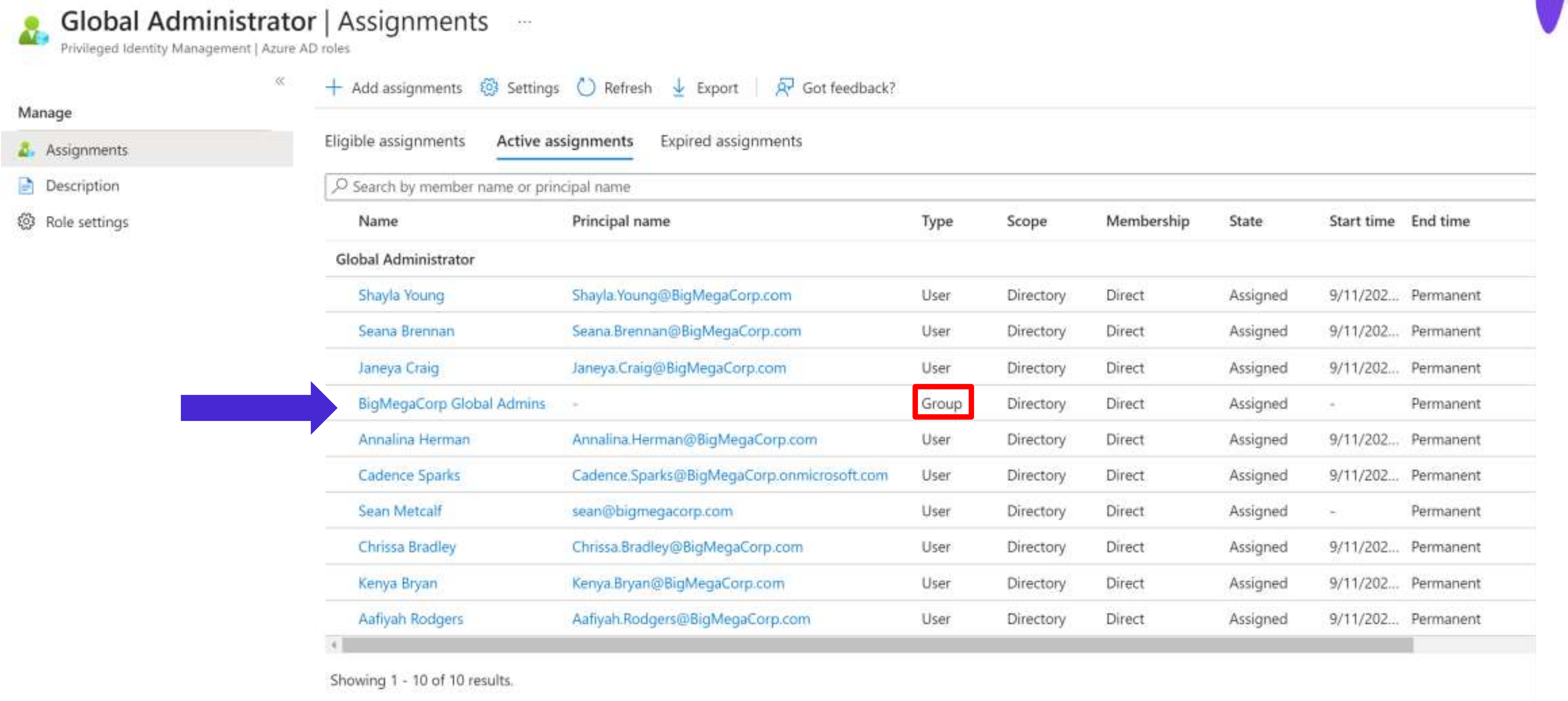
```
The Following 5 Global Admin Account(s) have MFA Successfully Configured:

UserDisplayName UserPrincipalName    IsMfaCapable IsMfaRegistered IsPasswordlessCapable MethodsRegistered
--------------- -----------------    ------------ --------------- --------------------- -----------------
Sean Metcalf    sean@bigmegacorp.com         True            True                  True {microsoftAuthenticatorPasswordless,


The Following 7 Global Admin Account(s) don't have MFA Configured:
Cadence.Sparks@BigMegaCorp.onmicrosoft.com
Kenya.Bryan@BigMegaCorp.com
Janeya.Craig@BigMegaCorp.com
Annalina.Herman@BigMegaCorp.com
Seana.Brennan@BigMegaCorp.com
Chrissa.Bradley@BigMegaCorp.com
Shayla.Young@BigMegaCorp.com
```

Role Assignable Groups (RAGs)

- Role Assignable Groups are Security or Microsoft 365 group with the isAssignableToRole property set to true and cannot be dynamic.
- Created to solve the potential issue where groups are added to an Entra ID role and a group admin could modify membership.
- Only Global Administrators or Privileged Role Administrators can create Role Assignable Groups and manage them (membership).
- Role Assignable Group owners can manage them.
- There is an application permission (Graph:RoleManagement.ReadWrite.Directory) that provides management rights as well.
- 500 role-assignable groups maximum in an Entra ID tenant (creation maximum).

NOTE: Only a Privileged Authentication Administrator or a Global Administrator can change the credentials or reset MFA or modify sensitive attributes for members & owners of a role-assignable group.

Privileged Roles with Group Nesting



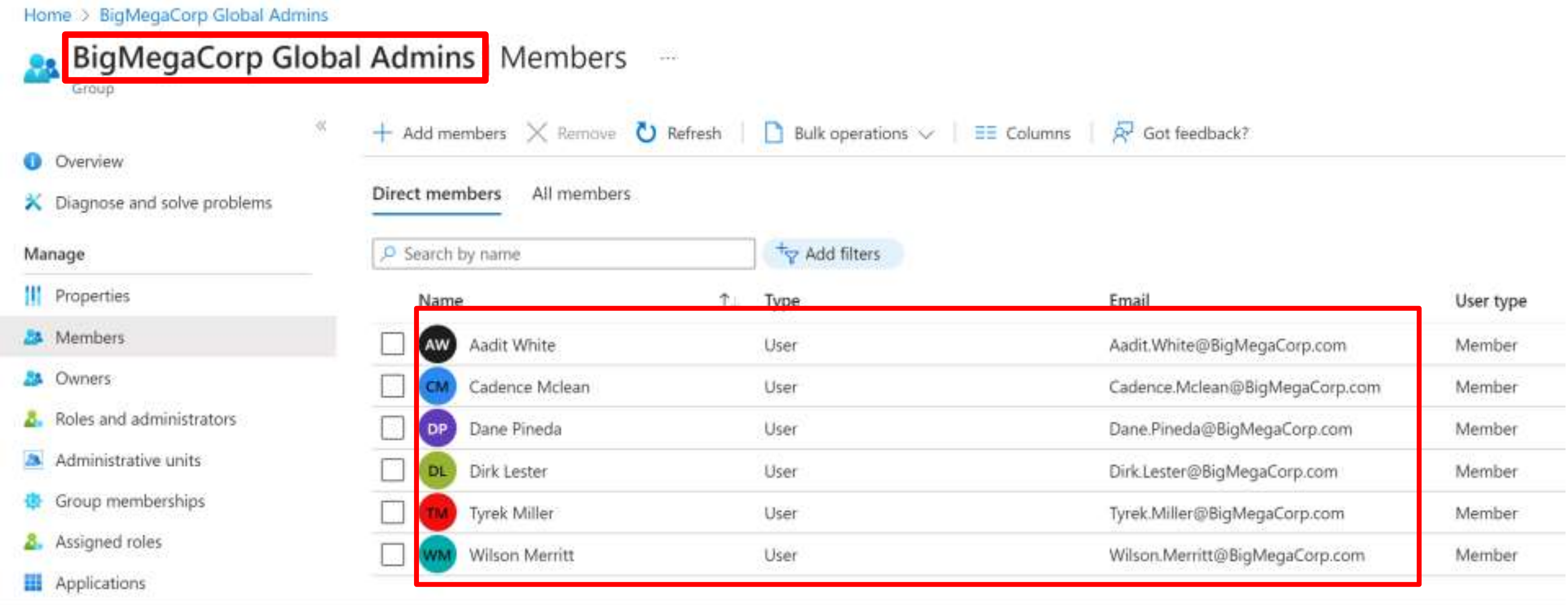
Global Administrator | Assignments ...

Privileged Identity Management | Azure AD roles

Name	Principal name	Type	Scope	Membership	State	Start time	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
BigMegaCorp Global Admins	-	Group	Directory	Direct	Assigned	-	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent

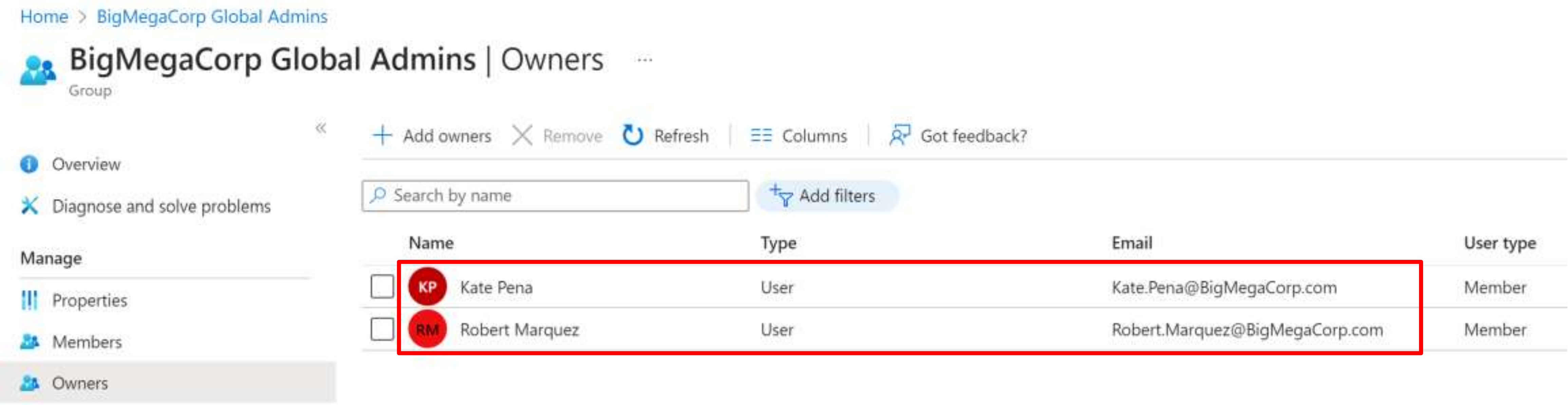
Showing 1 - 10 of 10 results.

Group Nesting – Have to Open Groups



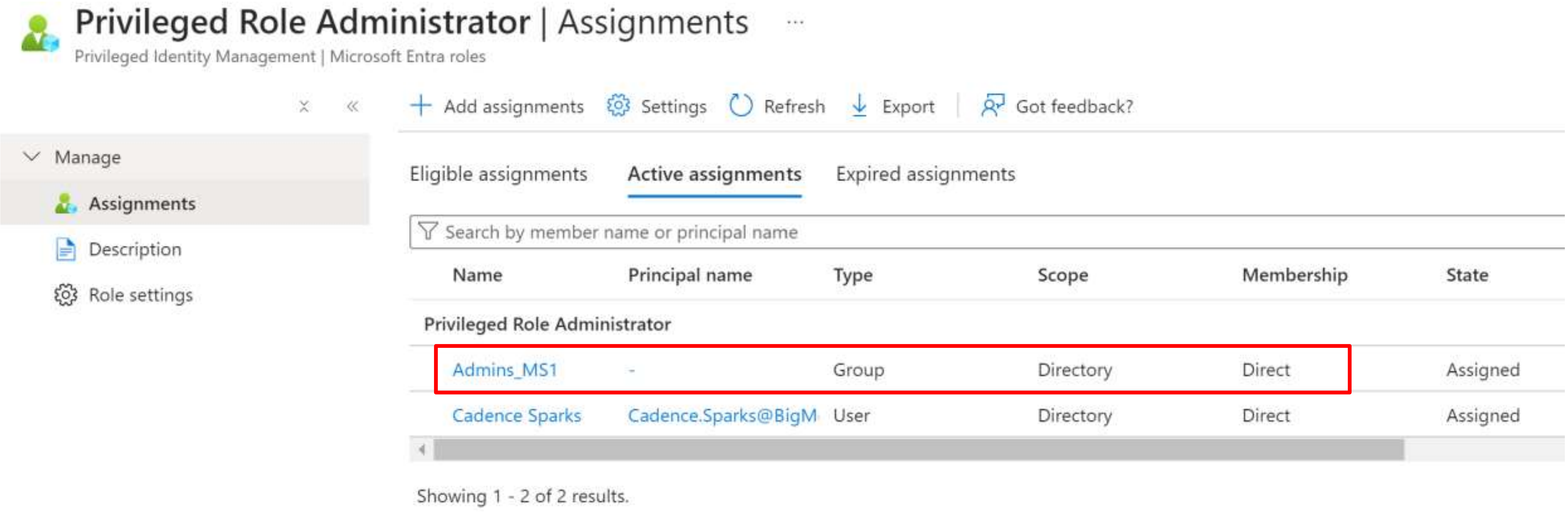
	Name	Type	Email	User type
□	AW Aadit White	User	Aadit.White@BigMegaCorp.com	Member
□	CM Cadence Mclean	User	Cadence.Mclean@BigMegaCorp.com	Member
□	DP Dane Pineda	User	Dane.Pineda@BigMegaCorp.com	Member
□	DL Dirk Lester	User	Dirk.Lester@BigMegaCorp.com	Member
□	TM Tyrek Miller	User	Tyrek.Miller@BigMegaCorp.com	Member
□	WM Wilson Merritt	User	Wilson.Merritt@BigMegaCorp.com	Member

Role Assignable Group Owners



	Name	Type	Email	User type
□	KP Kate Pena	User	Kate.Pena@BigMegaCorp.com	Member
□	RM Robert Marquez	User	Robert.Marquez@BigMegaCorp.com	Member

What if the Role Assignable Group is in a Different Tenant?



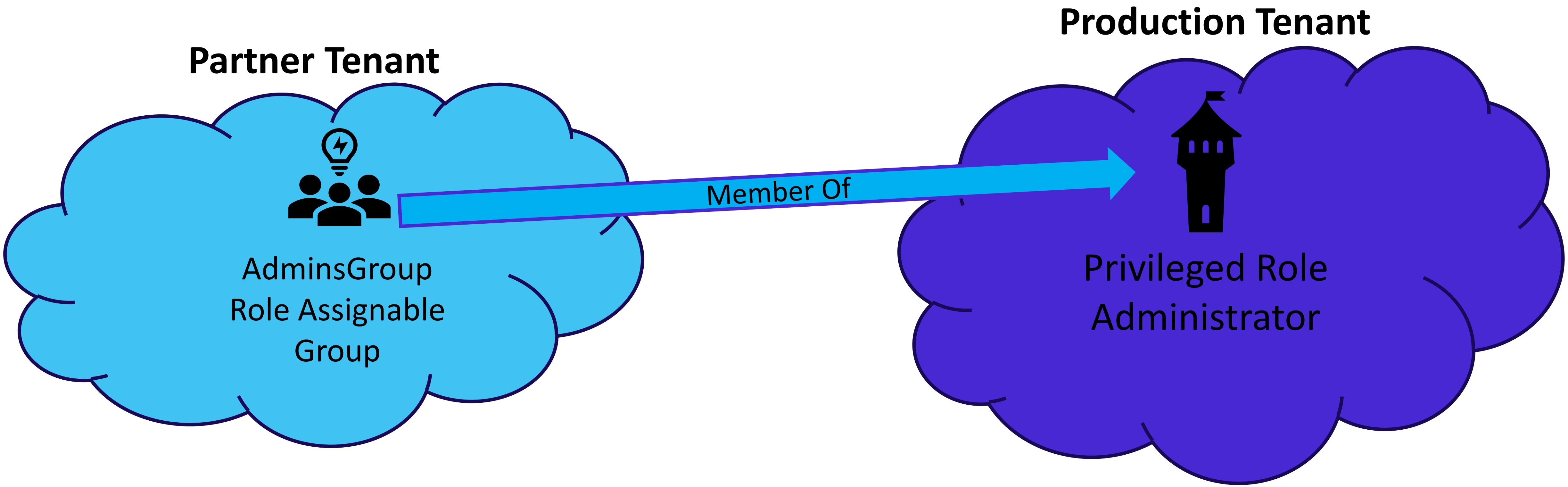
Privileged Role Administrator | Assignments

Privileged Identity Management | Microsoft Entra roles

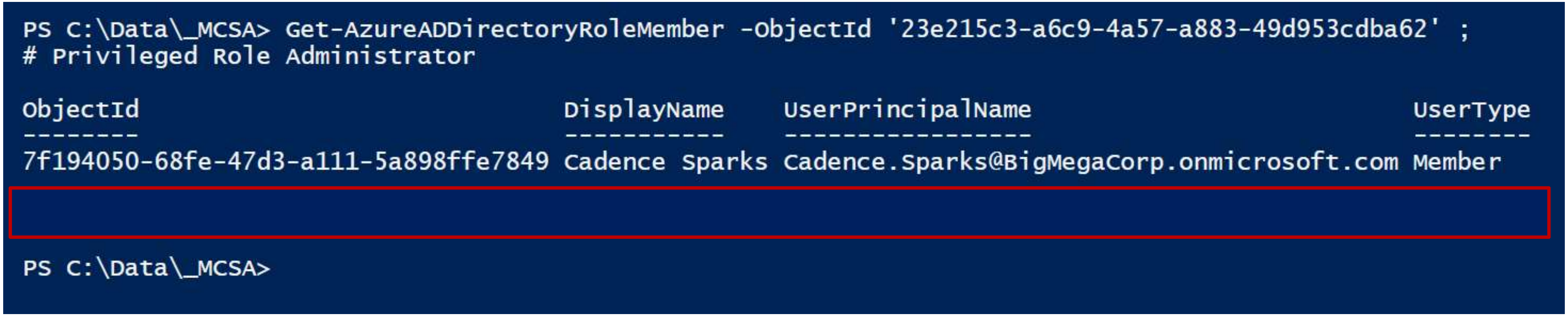
Name	Principal name	Type	Scope	Membership	State
Privileged Role Administrator					
Admins_MS1	-	Group	Directory	Direct	Assigned
Cadence Sparks	Cadence.Sparks@BigM	User	Directory	Direct	Assigned

Showing 1 - 2 of 2 results.

Privileged Role with Group in another Tenant



Role Group Member Not Shown in PowerShell



```
PS C:\Data\_MCSA> Get-AzureADDirectoryRoleMember -ObjectId '23e215c3-a6c9-4a57-a883-49d953cdba62' ;
# Privileged Role Administrator

ObjectId                             DisplayName     UserPrincipalName                         UserType
--------                             -----------     -----------------                         --------
7f194050-68fe-47d3-a111-5a898ffe7849 Cadence Sparks  Cadence.Sparks@BigMegaCorp.onmicrosoft.com Member


PS C:\Data\_MCSA>
```

RSAC | 2025 Conference

Conditional Access Policies

… and the Gaps therein

Many Voices.
One Community.

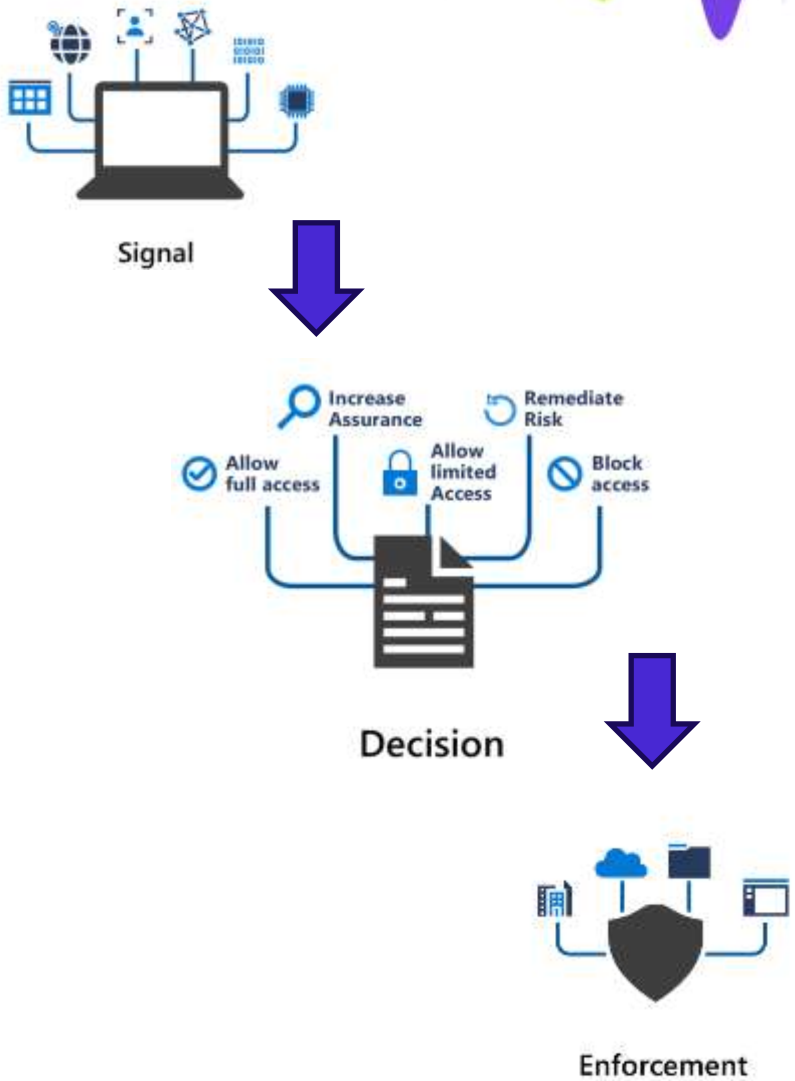
Conditional Access Policies

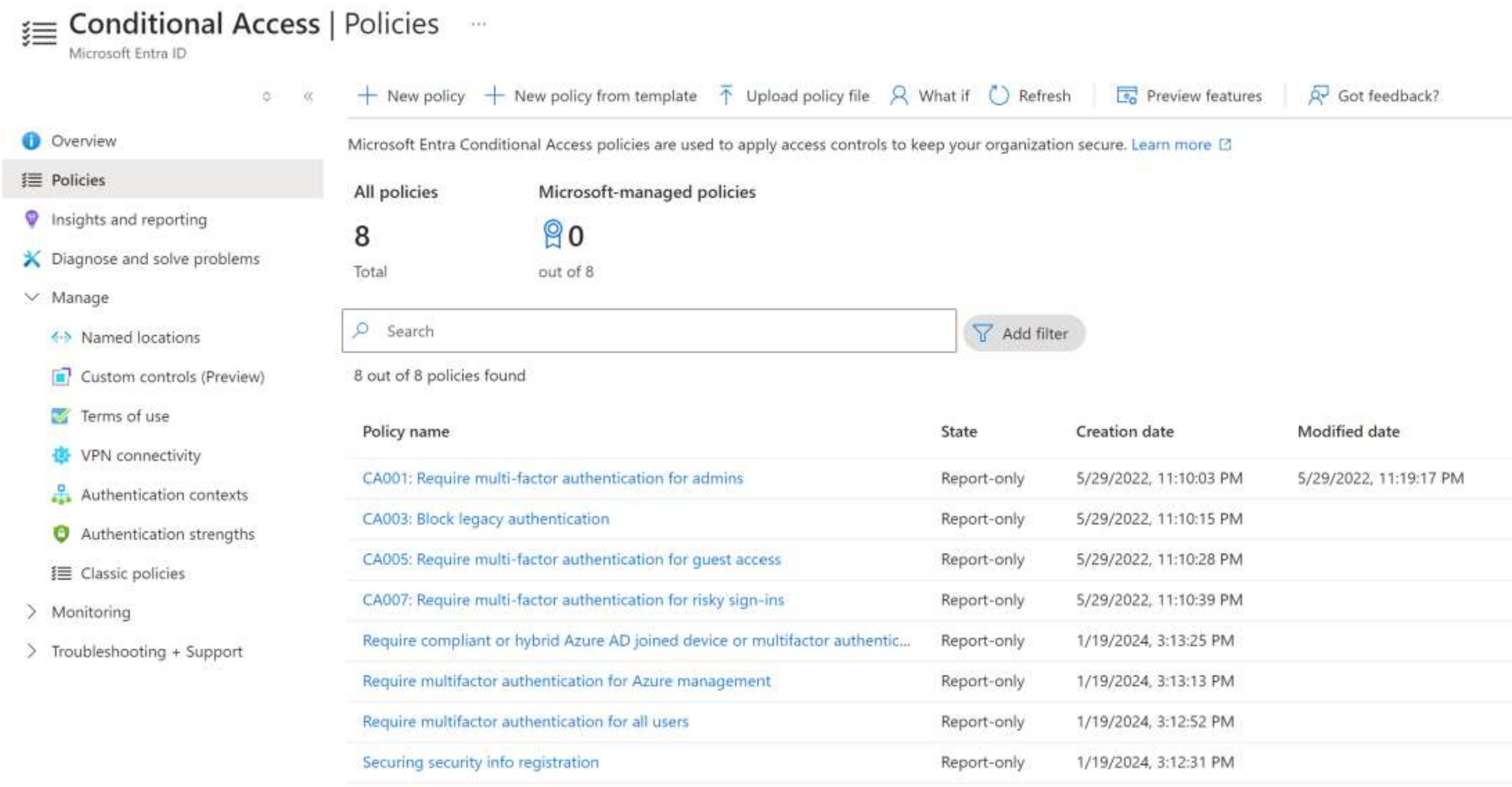
Policies apply after (first-factor) authentication

Requires P1 licensing

Rules based on:

- Who is connecting?
- Where are they connecting (from)?
- What app and/or device is connecting?
- When does this apply?





Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies
8
Total

Microsoft-managed policies
0
out of 8

8 out of 8 policies found

Policy name	State	Creation date	Modified date
CA001: Require multi-factor authentication for admins	Report-only	5/29/2022, 11:10:03 PM	5/29/2022, 11:19:17 PM
CA003: Block legacy authentication	Report-only	5/29/2022, 11:10:15 PM	
CA005: Require multi-factor authentication for guest access	Report-only	5/29/2022, 11:10:28 PM	
CA007: Require multi-factor authentication for risky sign-ins	Report-only	5/29/2022, 11:10:39 PM	
Require compliant or hybrid Azure AD joined device or multifactor authentic...	Report-only	1/19/2024, 3:13:25 PM	
Require multifactor authentication for Azure management	Report-only	1/19/2024, 3:13:13 PM	
Require multifactor authentication for all users	Report-only	1/19/2024, 3:12:52 PM	
Securing security info registration	Report-only	1/19/2024, 3:12:31 PM	

Common Conditional Access Policies

Require users to use MFA when connecting outside of the corporate network

Require MFA for users with certain administrative roles

Block legacy authentication (username & password auth)

Block/Grant access from specific locations

CA Policy Gap #1:
Users Require MFA Only Outside of Corp Network

- CAP requires users to MFA when they are working remotely (not on the corporate network or connected via VPN)
- Assumes no attacker would be on the corporate network
- Attacker can use username/password without having to MFA
- Fun Fact: Attackers love SSO!

CA Policy Gap #2:
Admins don’t require MFA

- MFA is required for certain users to access specific applications
- However, there is no CAP that requires MFA for Admins
- Or… CAP only requires members of a few roles use MFA
- Attacker can use username/password without having to MFA
- Fun Fact: Attackers love SSO!

CA Policy Gap #3: Exclusions

- CAP includes several security controls
  - MFA required
  - AAD Joined &Compliant device
  - Location based access
- However, there are exclusions:
  - Admins
  - VIPs
  - Executives
  - HR
  - Etc
- This creates a significant gap in security posture
- Attackers love being excluded from security controls!

Microsoft Provided Conditional Access Policies

- Baseline Policies
- Conditional Access Templates
- Microsoft Managed Policies

Baseline Policies
Security Defaults

Microsoft Provided Conditional Access Policies

- ✓ ~~Baseline Policies~~
- Conditional Access Templates
- Microsoft Managed Policies

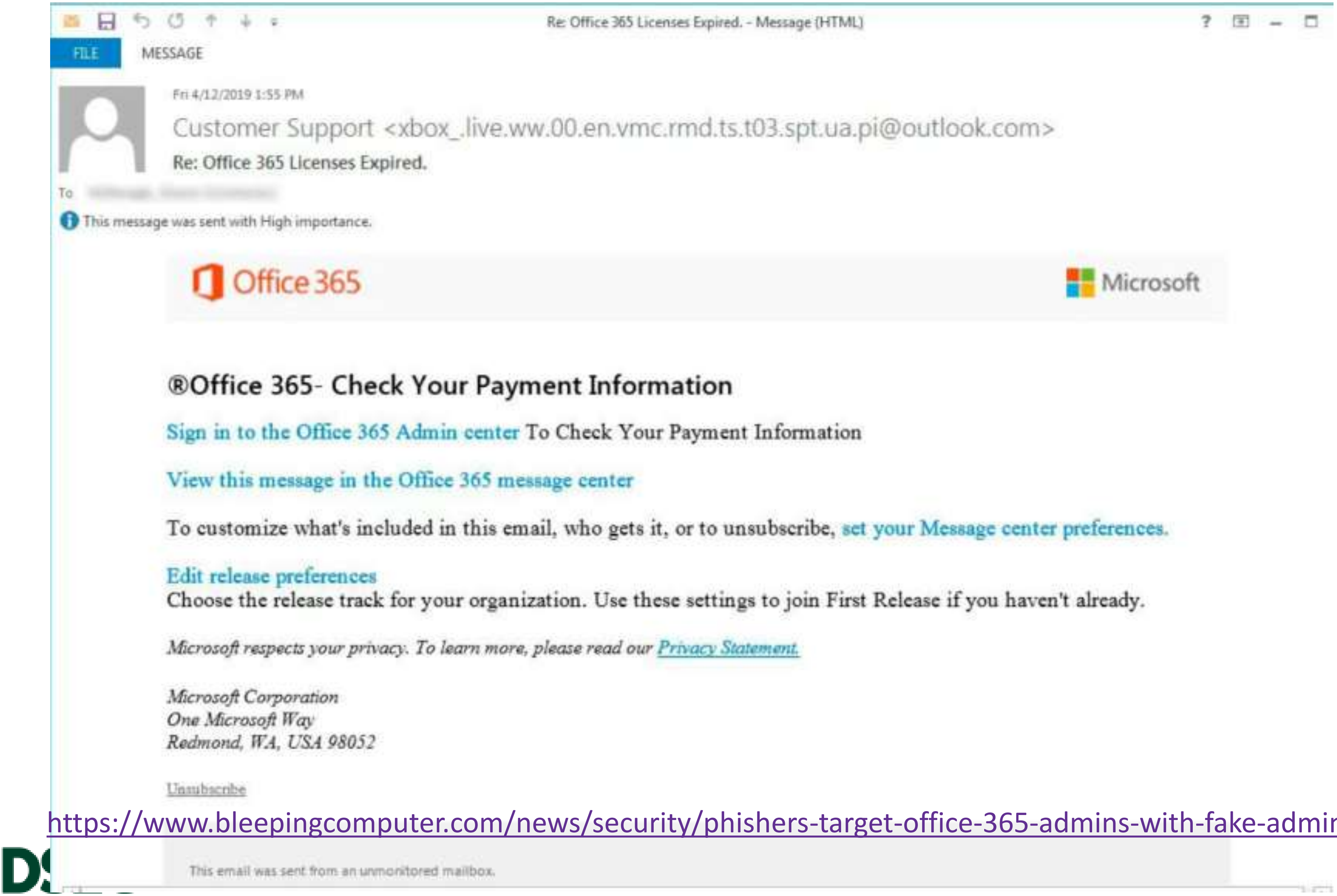
Microsoft Managed Policies (MMP)

- Deployed automatically in reporting mode
- Modification is limited:
  - Exclude users
  - Turn on or set to Report-only mode
  - Can't rename or delete any Microsoft-managed policies
  - Can duplicate the policy to make custom versions
- Microsoft might update these policies in the future
- MMPs turn on (set to enabled) 90 days after introduced to the tenant
- Currently focuses on 3 areas:
  - MFA for admins accessing Microsoft Admin Portals
  - MFA for per-user MFA configured on users
  - MFA and reauthentication for risky sign-ins

https://learn.microsoft.com/en-us/entra/identity/conditional-access/managed-policies

Attacking Entra ID

Phishing for Admins



Fri 4/12/2019 1:55 PM

Customer Support <xbox_.live.ww.00.en.vmc.rmd.ts.t03.spt.ua.pi@outlook.com>

Re: Office 365 Licenses Expired.

To [redacted]

This message was sent with High importance.

Office 365 Microsoft

®Office 365- Check Your Payment Information

Sign in to the Office 365 Admin center To Check Your Payment Information

View this message in the Office 365 message center

To customize what's included in this email, who gets it, or to unsubscribe, set your Message center preferences.

Edit release preferences
Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

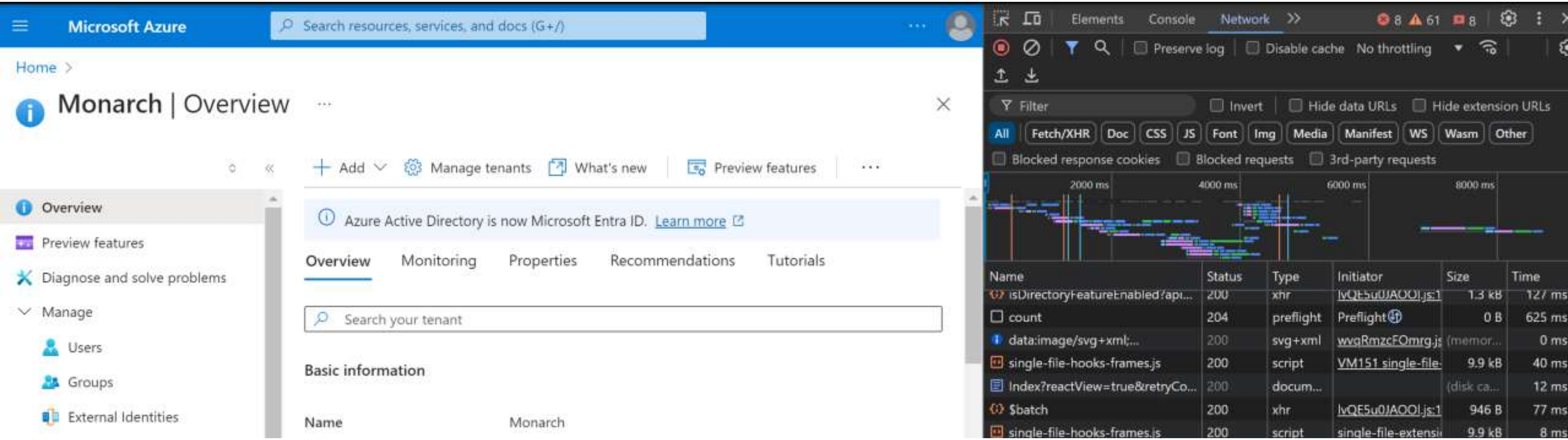
Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

Unsubscribe

This email was sent from an unmonitored mailbox.

https://www.bleepingcomputer.com/news/security/phishers-target-office-365-admins-with-fake-admin-alerts/

Stealing Tokens from the Web Browser



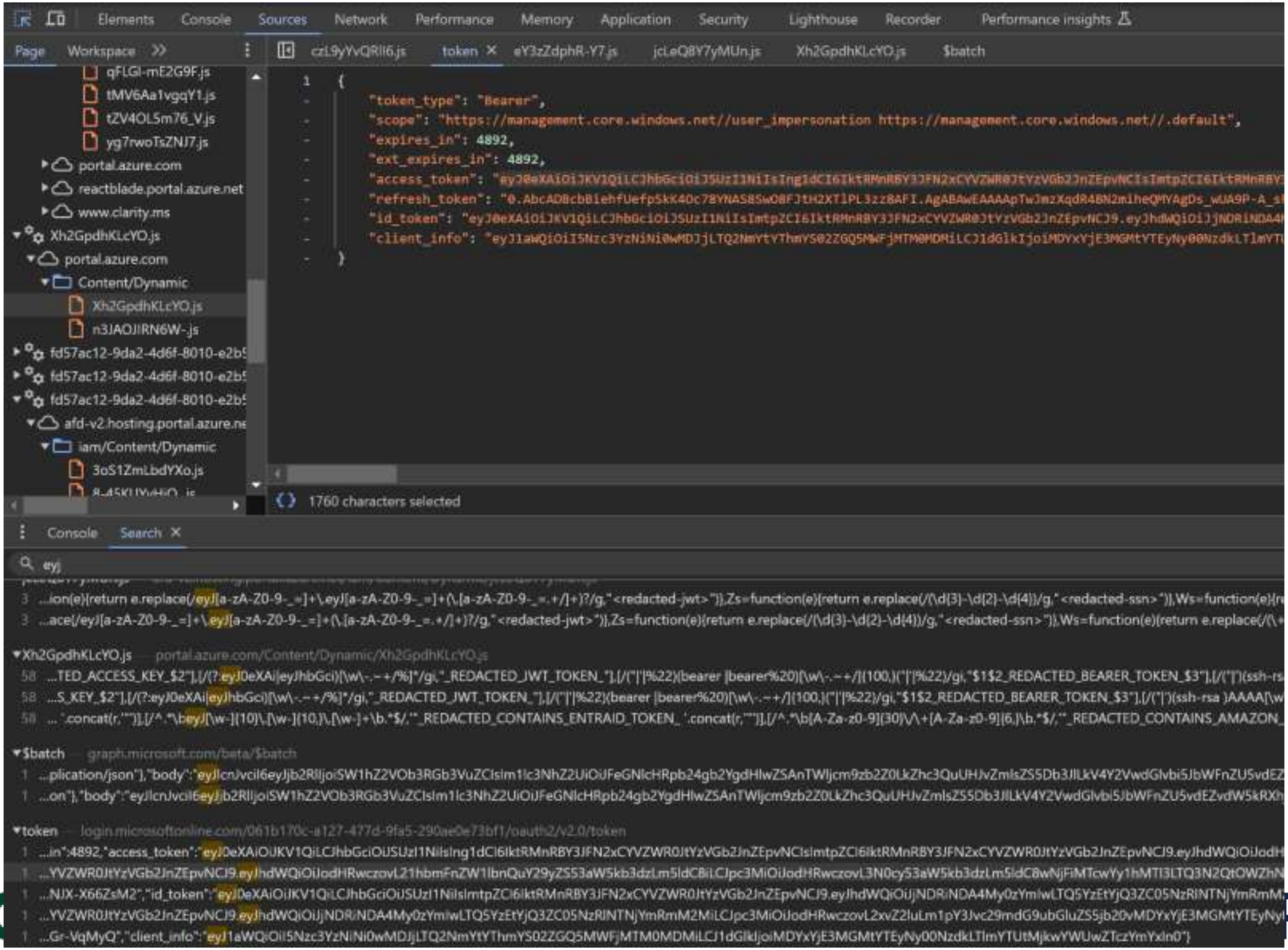
Azure Active Directory is now Microsoft Entra ID. Learn more

Basic information

Name Monarch

Name	Status	Type	Initiator	Size	Time
isDirectoryFeatureEnabled?api...	200	xhr	lvQE5u0JAOOl.js:1	1.3 kB	127 ms
count	204	preflight	Preflight	0 B	625 ms
data:image/svg+xml;...	200	svg+xml	wvqRmzcFOmrg.js	(memor...	0 ms
single-file-hooks-frames.js	200	script	VM151 single-file-	9.9 kB	40 ms
Index?reactView=true&retryCo...	200	docum...		(disk ca...	12 ms
$batch	200	xhr	lvQE5u0JAOOl.js:1	946 B	77 ms
single-file-hooks-frames.js	200	script	single-file-extensi	9.9 kB	8 ms

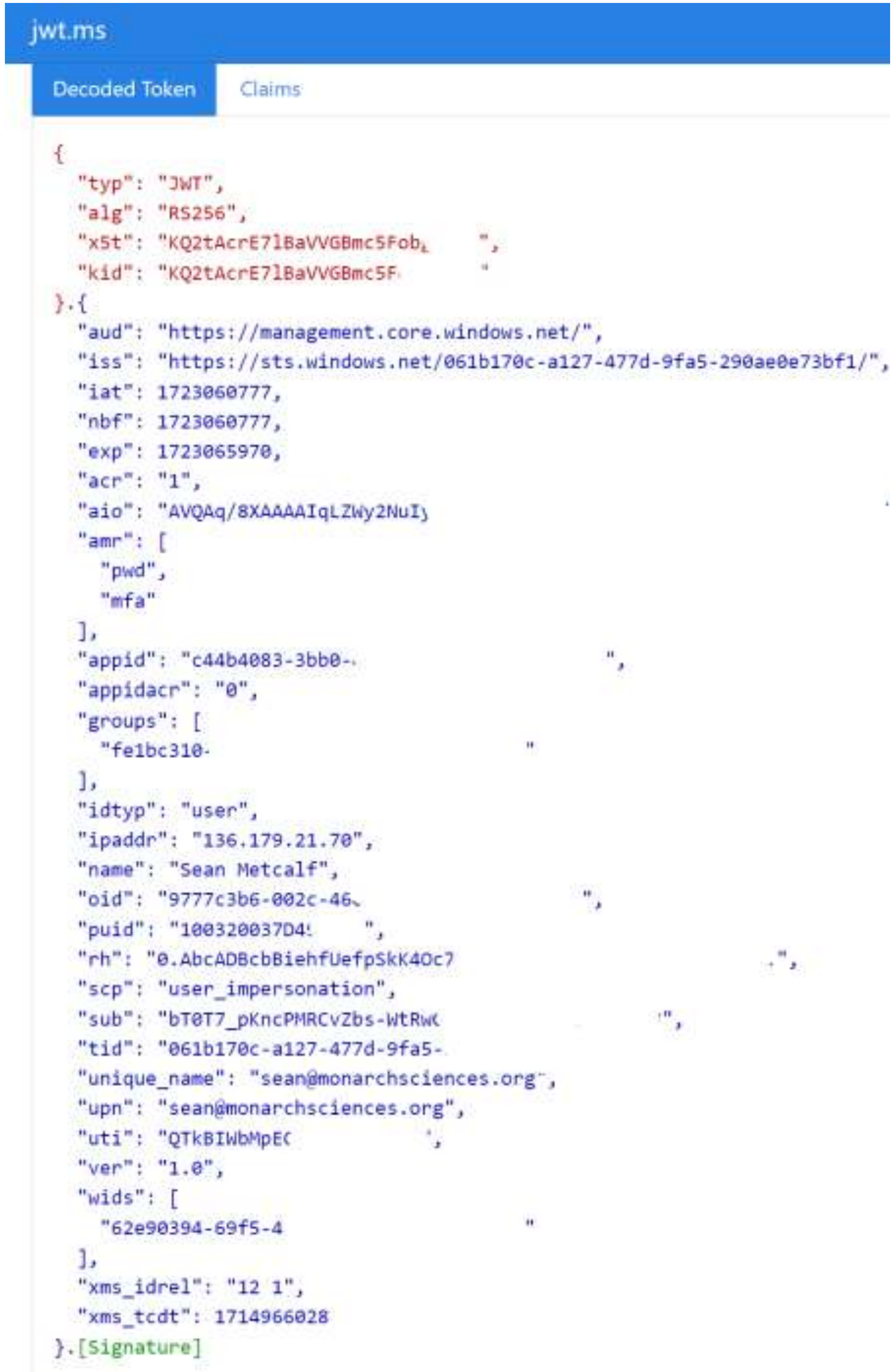
Stealing Tokens from the Web Browser



```
{
    "token_type": "Bearer",
    "scope": "https://management.core.windows.net//user_impersonation https://management.core.windows.net//.default",
    "expires_in": 4892,
    "ext_expires_in": 4892,
    "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IktRMnRBY3JFN2xCYVZWR0JtYzVGb2JnZEpvNCIsImtpZCI6IktRMnRBY3
    "refresh_token": "0.AbcADBcbBiehfUefpSkK40c78YNAS8SwO8FJtH2XTlPL3zz8AFI.AgABAwEAAAApTwJmzXqdR4BN2miheQMYAgDs_wUA9P-A_s
    "id_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IktRMnRBY3JFN2xCYVZWR0JtYzVGb2JnZEpvNCJ9.eyJhdWQiOiJjNDRiNDA4
    "client_info": "eyJ1aWQiOiI5Nzc3YzNiNi0wMDJjLTQ2NmYtYThmYS02ZGQ5MWFjMTM0MDMiLCJ1dGlkIjoiMDYxYjE3MGMtYTEyNy00NzdkLTlmYT
}
```

```
eyj
3  ...ion(e){return e.replace(/eyJ[a-zA-Z0-9-_=]+\.eyJ[a-zA-Z0-9-_=]+(\.[a-zA-Z0-9-_=.+/]+)?/g,"<redacted-jwt>")},Zs=function(e){return e.replace(/(\d{3}-\d{2}-\d{4})/g,"<redacted-ssn>")},Ws=function(e){re
3  ...ace(/eyJ[a-zA-Z0-9-_=]+\.eyJ[a-zA-Z0-9-_=]+(\.[a-zA-Z0-9-_=.+/]+)?/g,"<redacted-jwt>")},Zs=function(e){return e.replace(/(\d{3}-\d{2}-\d{4})/g,"<redacted-ssn>")},Ws=function(e){return e.replace(/(\+

▾Xh2GpdhKLcYO.js — portal.azure.com/Content/Dynamic/Xh2GpdhKLcYO.js
58  ...TED_ACCESS_KEY_$2"],[/(?:eyJ0eXAi|eyJhbGci)[\w\-.~+/%]*/gi,"_REDACTED_JWT_TOKEN_"],[/("|'|%22)(bearer |bearer%20)[\w\-.~+/]{100,}("|'|%22)/gi,"$1$2_REDACTED_BEARER_TOKEN_$3"],[/("|')(ssh-rs
58  ...S_KEY_$2"],[/(?:eyJ0eXAi|eyJhbGci)[\w\-.~+/%]*/gi,"_REDACTED_JWT_TOKEN_"],[/("|'|%22)(bearer |bearer%20)[\w\-.~+/]{100,}("|'|%22)/gi,"$1$2_REDACTED_BEARER_TOKEN_$3"],[/("|')(ssh-rsa )AAAA[\w
58  ... ".concat(r,"")],[/^.*\beyJ[\w-]{10}\.[\w-]{10,}\.[\w-]+\b.*$/,"_REDACTED_CONTAINS_ENTRAID_TOKEN_".concat(r,"")],[/^.*\b[A-Za-z0-9]{30}\/\+[A-Za-z0-9]{6,}\b.*$/,"_REDACTED_CONTAINS_AMAZON_

▾$batch — graph.microsoft.com/beta/$batch
1  ...plication/json"},"body":"eyJlcnJvcil6eyJjb2RlIjoiSW1hZ2VOb3RGb3VuZCIsIm1lc3NhZ2UiOiJFeGNlcHRpb24gb2YgdHlwZSAnTWljcm9zb2Z0LkZhc3QuUHJvZmlsZS5Db3JlLkV4Y2VwdGlvbi5JbWFnZU5vdEZ
1  ...on"},"body":"eyJlcnJvcil6eyJjb2RlIjoiSW1hZ2VOb3RGb3VuZCIsIm1lc3NhZ2UiOiJFeGNlcHRpb24gb2YgdHlwZSAnTWljcm9zb2Z0LkZhc3QuUHJvZmlsZS5Db3JlLkV4Y2VwdGlvbi5JbWFnZU5vdEZvdW5kRXh

▾token — login.microsoftonline.com/061b170c-a127-477d-9fa5-290ae0e73bf1/oauth2/v2.0/token
1  ...in":4892,"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IktRMnRBY3JFN2xCYVZWR0JtYzVGb2JnZEpvNCIsImtpZCI6IktRMnRBY3JFN2xCYVZWR0JtYzVGb2JnZEpvNCJ9.eyJhdWQiOiJodH
1  ...YVZWR0JtYzVGb2JnZEpvNCJ9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuY29yZS53aW5kb3dzLm5ldC8iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC8wNjFiMTcwYy1hMTI3LTQ3N2QtOWZhN
1  ...NJX-X66ZsM2","id_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IktRMnRBY3JFN2xCYVZWR0JtYzVGb2JnZEpvNCJ9.eyJhdWQiOiJjNDRiNDA4My0zYmIwLTQ5YzEtYjQ3ZC05NzRlNTNjYmRmM
1  ...YVZWR0JtYzVGb2JnZEpvNCJ9.eyJhdWQiOiJjNDRiNDA4My0zYmIwLTQ5YzEtYjQ3ZC05NzRlNTNjYmRmM2MiLCJpc3MiOiJodHRwczovL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb20vMDYxYjE3MGMtYTEyNy
1  ...Gr-VqMyQ","client_info":"eyJ1aWQiOiI5Nzc3YzNiNi0wMDJjLTQ2NmYtYThmYS02ZGQ5MWFjMTM0MDMiLCJ1dGlkIjoiMDYxYjE3MGMtYTEyNy00NzdkLTlmYTUtMjkwYWUwZTczYmYxIn0"}
```

Stealing Access Token from the Web Browser

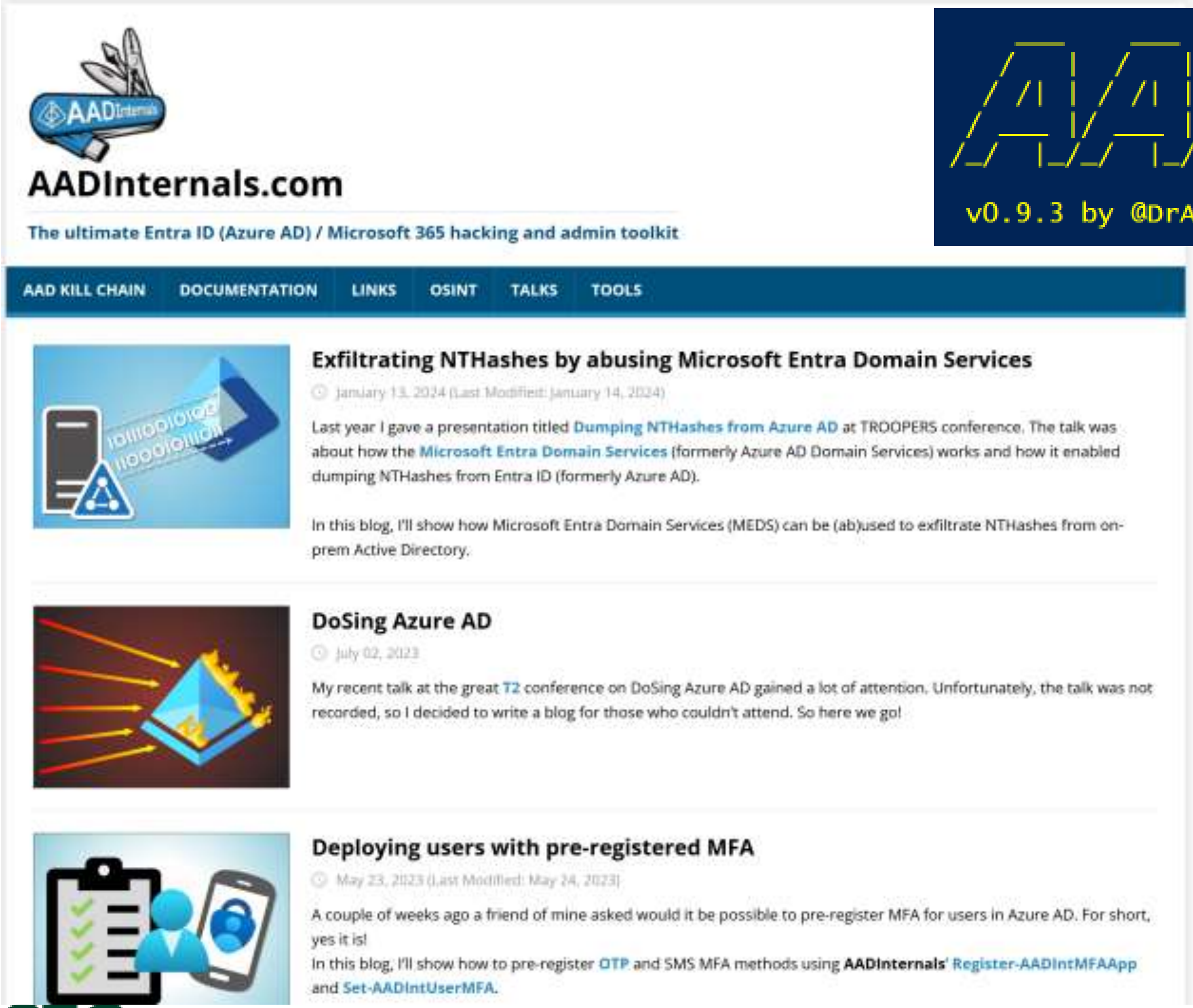


```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "KQ2tAcrE71BaVVGBmc5Fob[redacted]",
  "kid": "KQ2tAcrE71BaVVGBmc5F[redacted]"
}.{
  "aud": "https://management.core.windows.net/",
  "iss": "https://sts.windows.net/061b170c-a127-477d-9fa5-290ae0e73bf1/",
  "iat": 1723060777,
  "nbf": 1723060777,
  "exp": 1723065970,
  "acr": "1",
  "aio": "AVQAq/8XAAAAIqLZWy2NuI[redacted]
  "amr": [
    "pwd",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-[redacted]",
  "appidacr": "0",
  "groups": [
    "fe1bc310-[redacted]"
  ],
  "idtyp": "user",
  "ipaddr": "136.179.21.70",
  "name": "Sean Metcalf",
  "oid": "9777c3b6-002c-46[redacted]",
  "puid": "100320037D4[redacted]",
  "rh": "0.AbcADBcbBiehfUefpSkK4Oc7[redacted]",
  "scp": "user_impersonation",
  "sub": "bT0T7_pKncPMRCvZbs-WtRw[redacted]",
  "tid": "061b170c-a127-477d-9fa5-[redacted]
  "unique_name": "sean@monarchsciences.org",
  "upn": "sean@monarchsciences.org",
  "uti": "QTkBIWbMpE[redacted]",
  "ver": "1.0",
  "wids": [
    "62e90394-69f5-4[redacted]"
  ],
  "xms_idrel": "12 1",
  "xms_tcdt": 1714966028
}.[Signature]
```

That's It!

Now we have the Access Token

Stealing Tokens from the Web Browser



AADInternals.com

The ultimate Entra ID (Azure AD) / Microsoft 365 hacking and admin toolkit

Exfiltrating NTHashes by abusing Microsoft Entra Domain Services

January 13, 2024 (Last Modified: January 14, 2024)

Last year I gave a presentation titled Dumping NTHashes from Azure AD at TROOPERS conference. The talk was about how the Microsoft Entra Domain Services (formerly Azure AD Domain Services) works and how it enabled dumping NTHashes from Entra ID (formerly Azure AD).

In this blog, I'll show how Microsoft Entra Domain Services (MEDS) can be (ab)used to exfiltrate NTHashes from on-prem Active Directory.

DoSing Azure AD

July 02, 2023

My recent talk at the great T2 conference on DoSing Azure AD gained a lot of attention. Unfortunately, the talk was not recorded, so I decided to write a blog for those who couldn't attend. So here we go!

Deploying users with pre-registered MFA

May 23, 2023 (Last Modified: May 24, 2023)

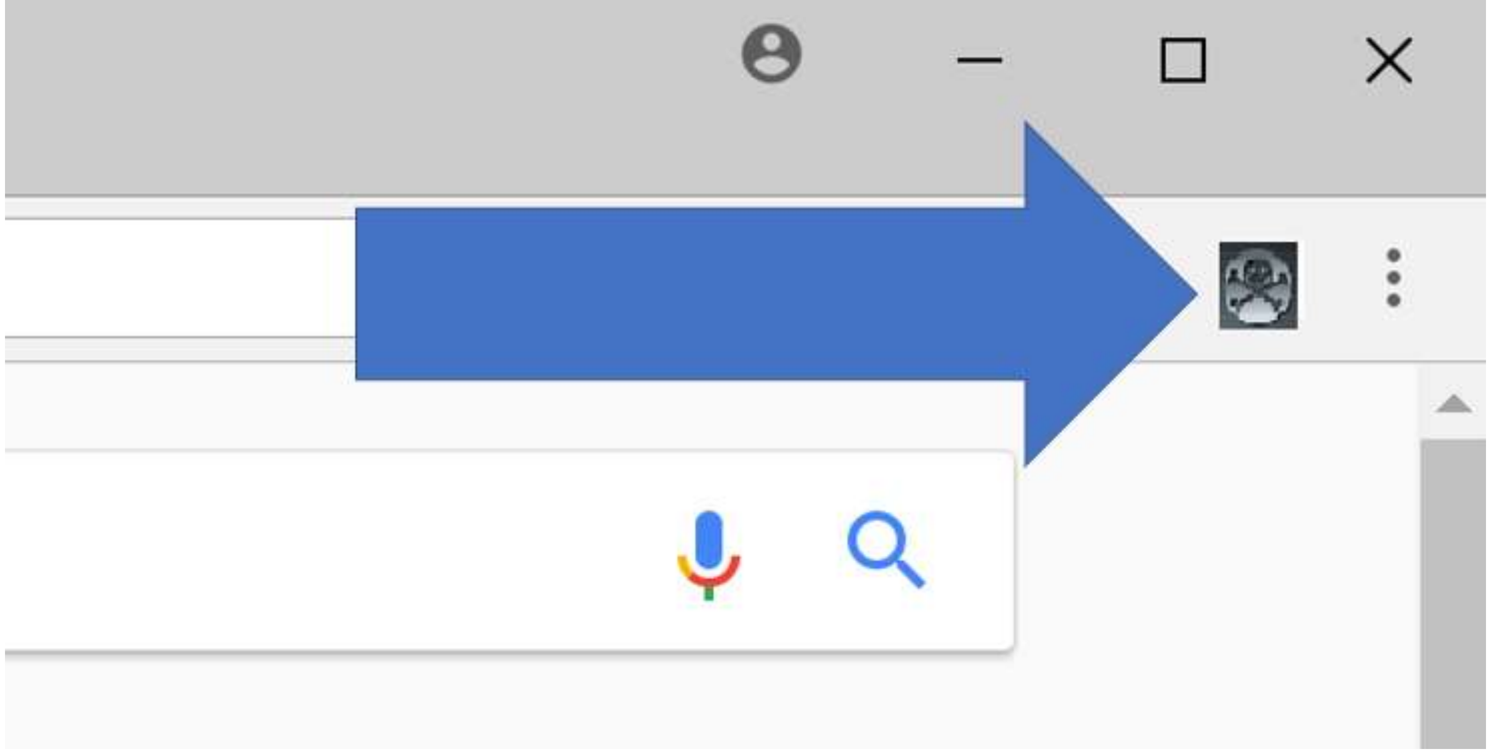
A couple of weeks ago a friend of mine asked would it be possible to pre-register MFA for users in Azure AD. For short, yes it is!

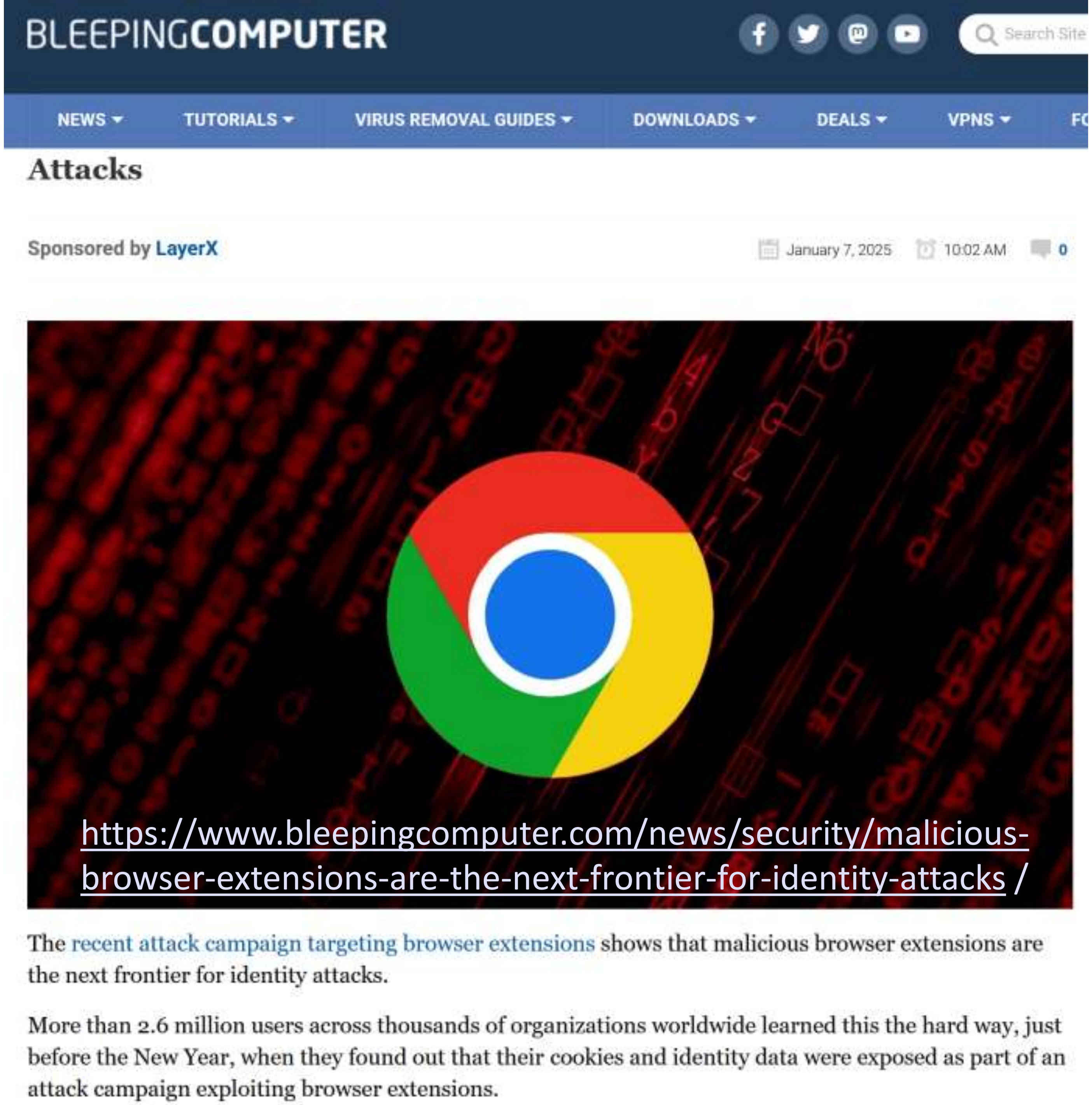
In this blog, I'll show how to pre-register OTP and SMS MFA methods using **AADInternals**' Register-AADIntMFAApp and Set-AADIntUserMFA.

v0.9.3 by @DrAzureAD (Nestori Syynimaa)

Special THANK YOU to Dr AzureAD himself, Dr. Nestori Syynimaa for his help with this section!

Token Theft with Browser Extension





Attacks

Sponsored by LayerX

January 7, 2025 10:02 AM 0

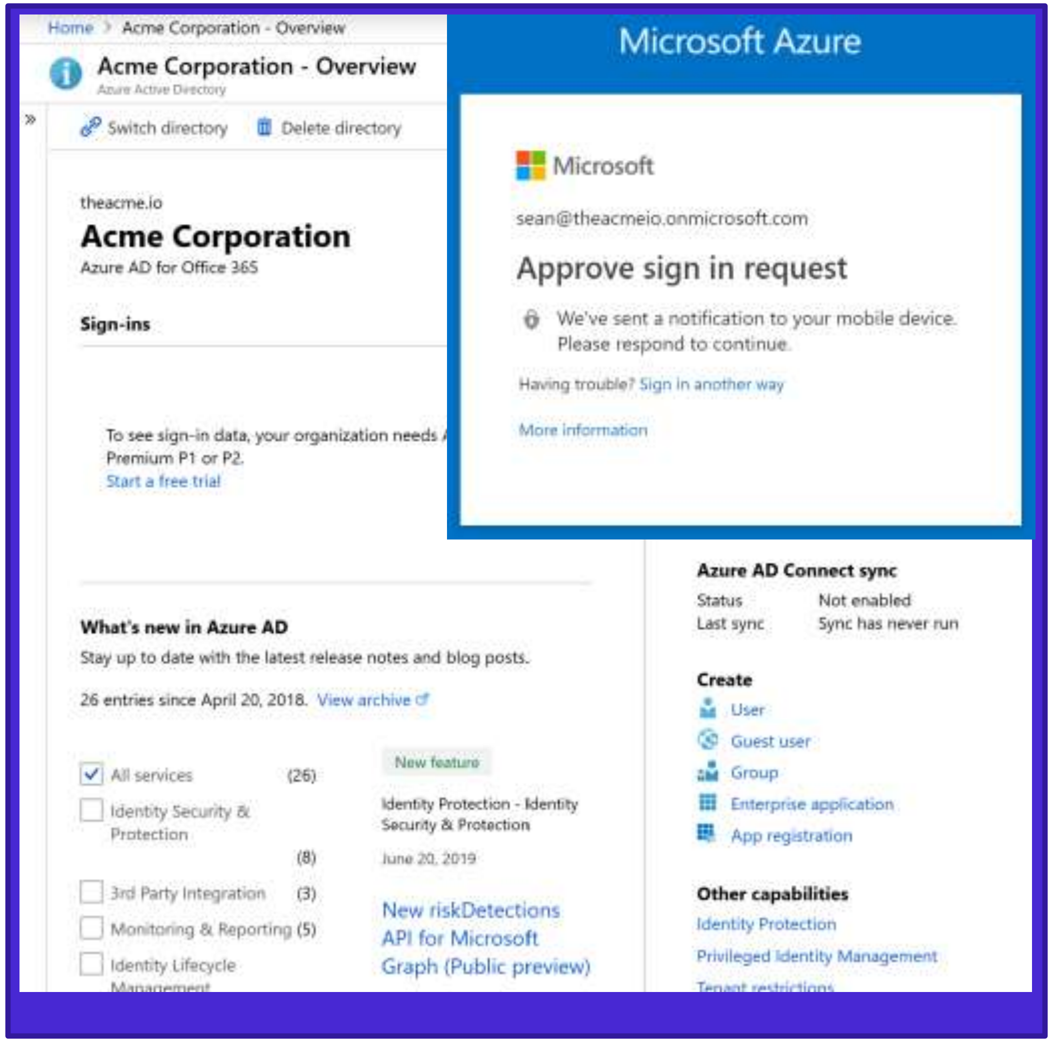
https://www.bleepingcomputer.com/news/security/malicious-browser-extensions-are-the-next-frontier-for-identity-attacks /

The recent attack campaign targeting browser extensions shows that malicious browser extensions are the next frontier for identity attacks.

More than 2.6 million users across thousands of organizations worldwide learned this the hard way, just before the New Year, when they found out that their cookies and identity data were exposed as part of an attack campaign exploiting browser extensions.

Token Theft with evilginx

https://aad.portalazure.com/



Home > Acme Corporation - Overview

Acme Corporation - Overview
Azure Active Directory

Switch directory   Delete directory

theacme.io
Acme Corporation
Azure AD for Office 365

Sign-ins

To see sign-in data, your organization needs
Premium P1 or P2.
Start a free trial

What's new in Azure AD
Stay up to date with the latest release notes and blog posts.
26 entries since April 20, 2018. View archive

☑ All services (26)
□ Identity Security & Protection (8)
□ 3rd Party Integration (3)
□ Monitoring & Reporting (5)
□ Identity Lifecycle Management

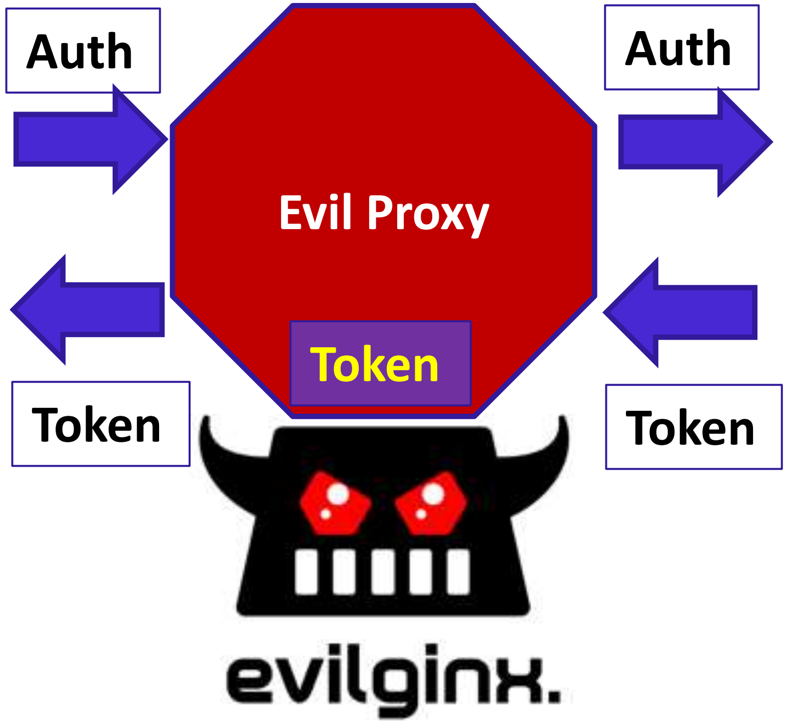
New feature
Identity Protection - Identity Security & Protection
June 20, 2019
New riskDetections API for Microsoft Graph (Public preview)

Azure AD Connect sync
Status Not enabled
Last sync Sync has never run

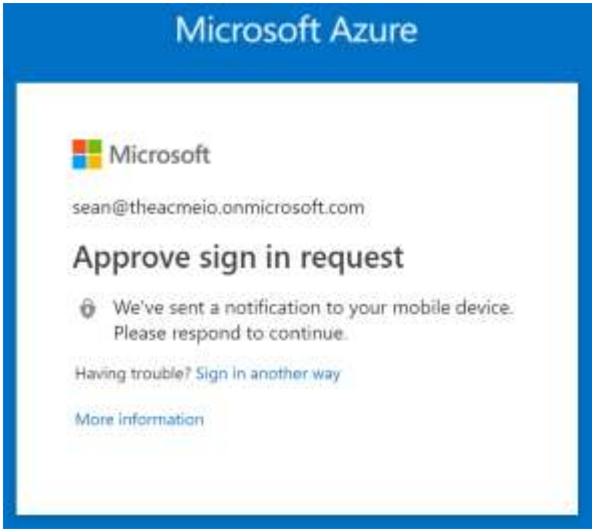
Create
User
Guest user
Group
Enterprise application
App registration

Other capabilities
Identity Protection
Privileged Identity Management
Tenant restrictions

Microsoft Azure
Microsoft
sean@theacmeio.onmicrosoft.com
Approve sign in request
We've sent a notification to your mobile device. Please respond to continue.
Having trouble? Sign in another way
More information



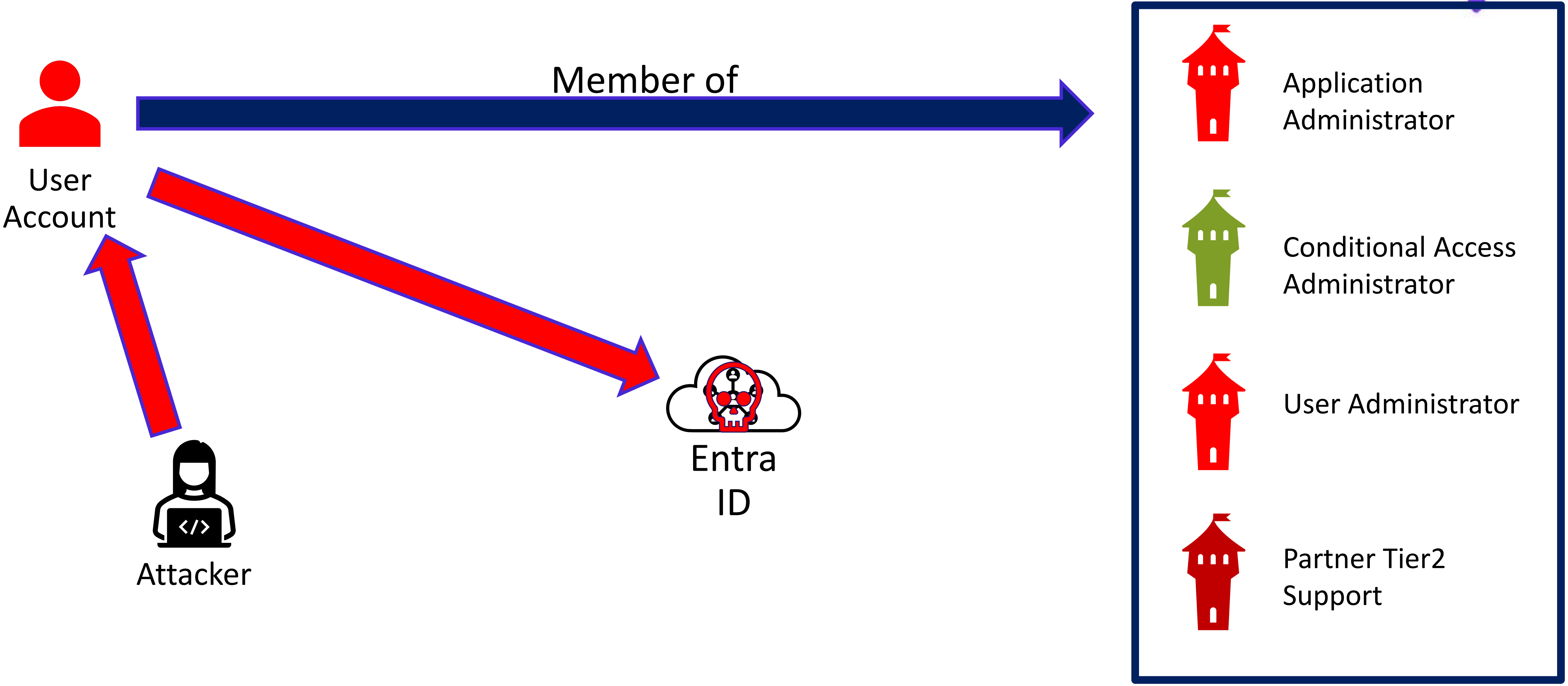
https://aad.portal.azure.com/



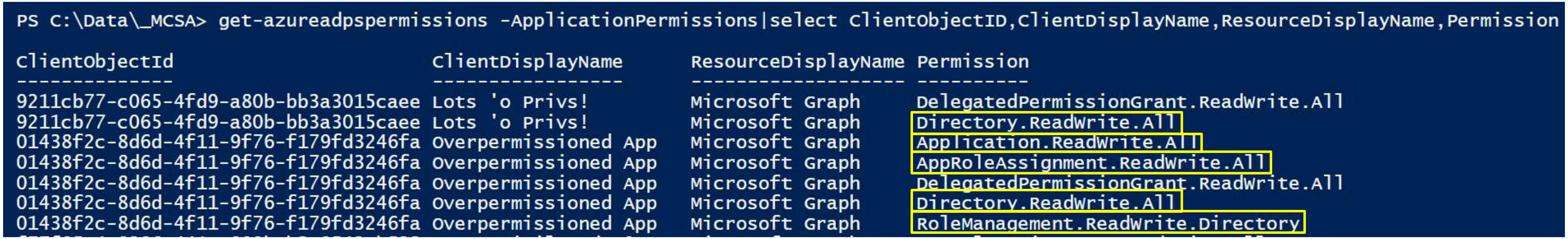
Microsoft Azure
Microsoft
sean@theacmeio.onmicrosoft.com
Approve sign in request
We've sent a notification to your mobile device. Please respond to continue.
Having trouble? Sign in another way
More information

https://github.com/kgretzky/evilginx2

Overprivileged User

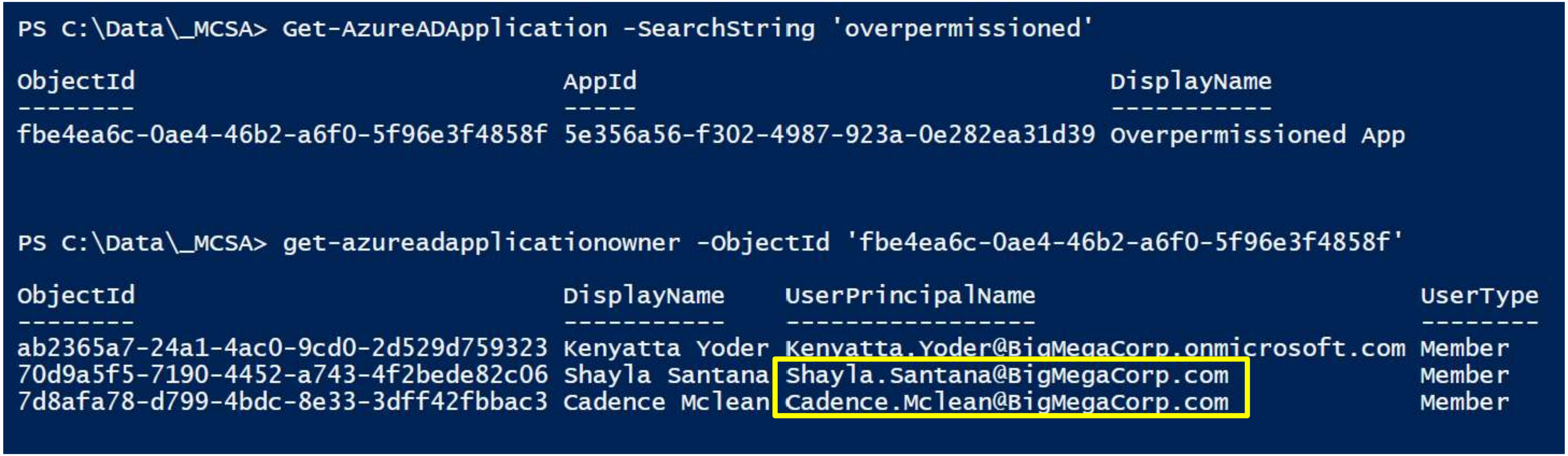


Application Escalation



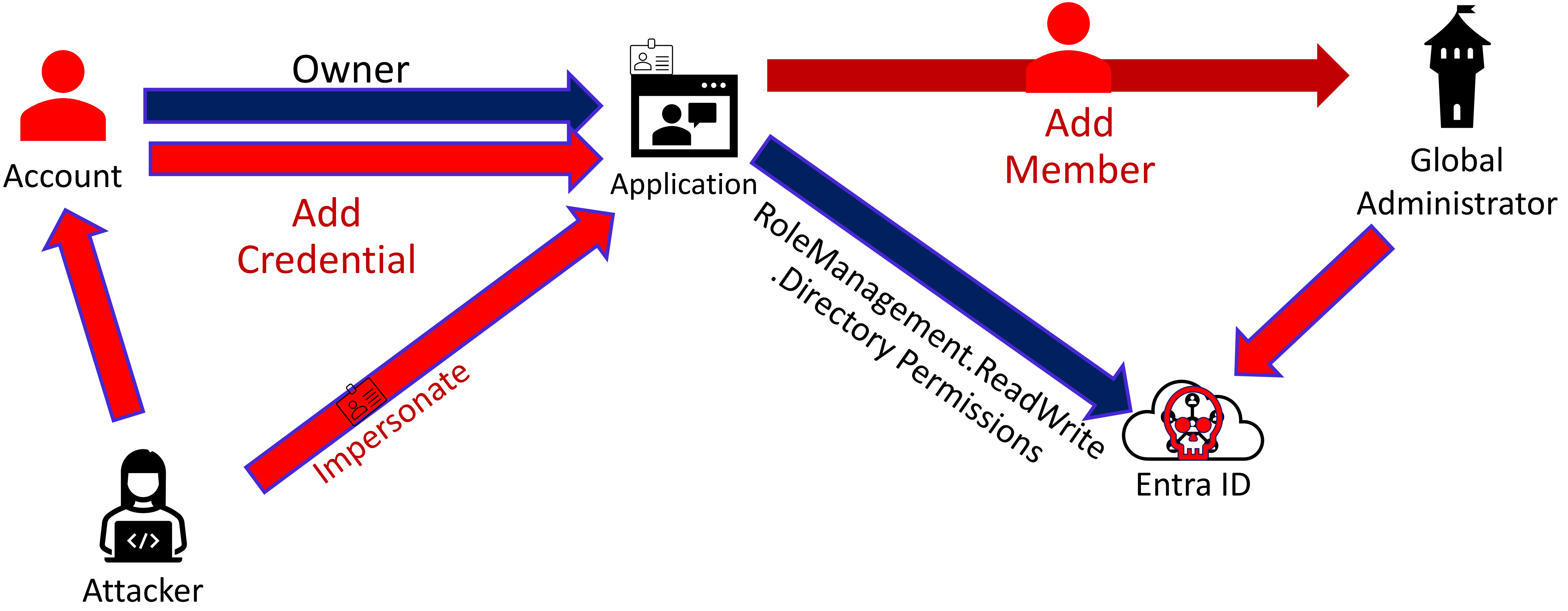
```
PS C:\Data\_MCSA> get-azureadpspermissions -ApplicationPermissions|select ClientObjectID,ClientDisplayName,ResourceDisplayName,Permission

ClientObjectId                       ClientDisplayName      ResourceDisplayName Permission
--------------                       -----------------      ------------------- ----------
9211cb77-c065-4fd9-a80b-bb3a3015caee Lots 'o Privs!         Microsoft Graph     DelegatedPermissionGrant.ReadWrite.All
9211cb77-c065-4fd9-a80b-bb3a3015caee Lots 'o Privs!         Microsoft Graph     Directory.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     Application.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     AppRoleAssignment.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     DelegatedPermissionGrant.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     Directory.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     RoleManagement.ReadWrite.Directory
```

Application Escalation: Find the App Owner

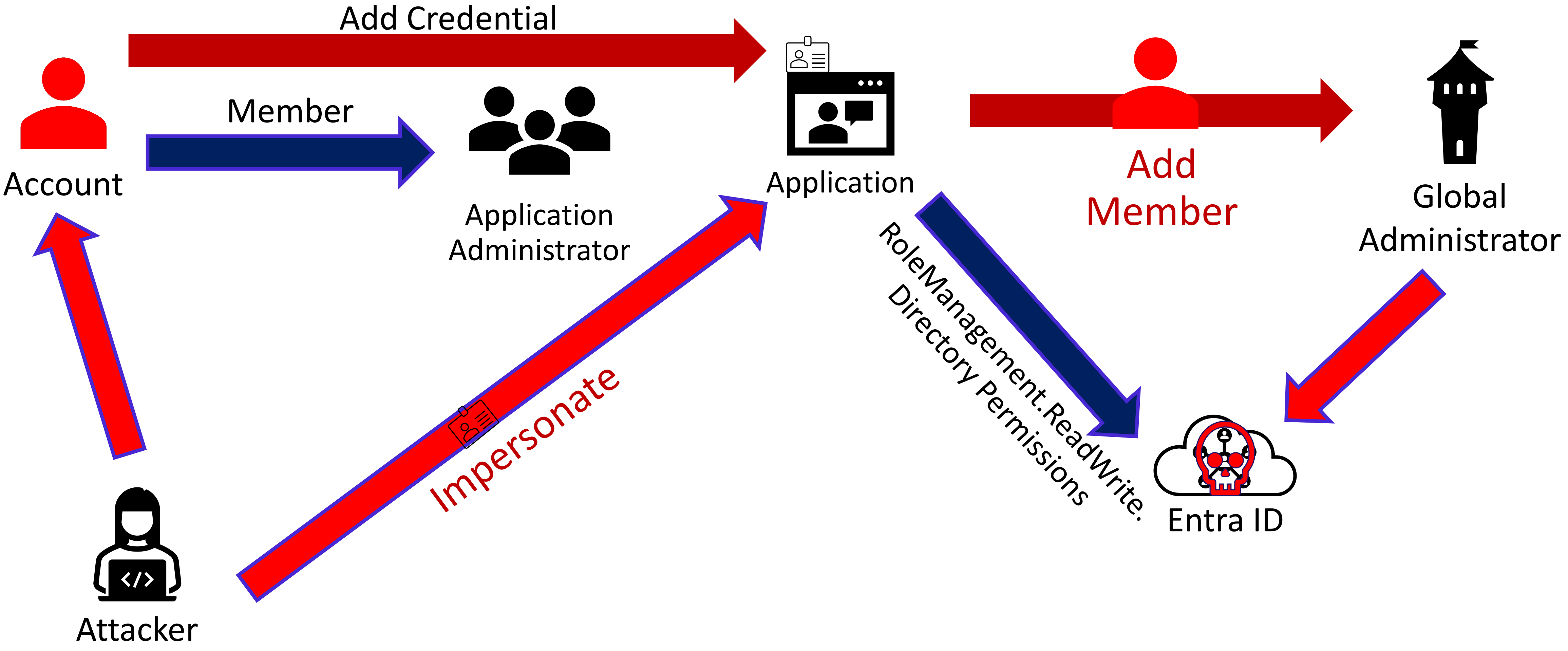


```
PS C:\Data\_MCSA> Get-AzureADApplication -SearchString 'overpermissioned'

ObjectId                             AppId                                DisplayName
--------                             -----                                -----------
fbe4ea6c-0ae4-46b2-a6f0-5f96e3f4858f 5e356a56-f302-4987-923a-0e282ea31d39 Overpermissioned App



PS C:\Data\_MCSA> get-azureadapplicationowner -ObjectId 'fbe4ea6c-0ae4-46b2-a6f0-5f96e3f4858f'

ObjectId                             DisplayName    UserPrincipalName                          UserType
--------                             -----------    -----------------                          --------
ab2365a7-24a1-4ac0-9cd0-2d529d759323 Kenyatta Yoder Kenyatta.Yoder@BigMegaCorp.onmicrosoft.com Member
70d9a5f5-7190-4452-a743-4f2bede82c06 Shayla Santana Shayla.Santana@BigMegaCorp.com             Member
7d8afa78-d799-4bdc-8e33-3dff42fbbac3 Cadence Mclean Cadence.Mclean@BigMegaCorp.com             Member
```

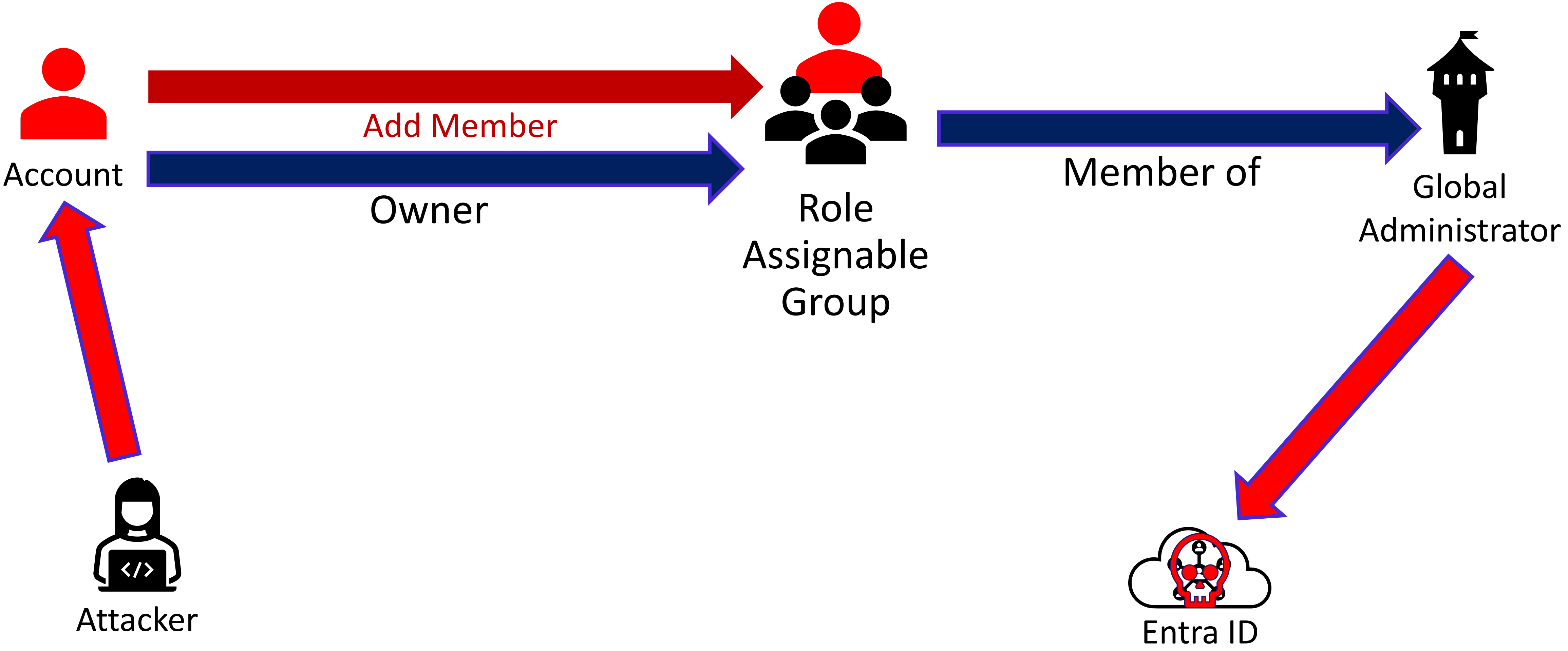
Compromise Entra ID through Application Permissions



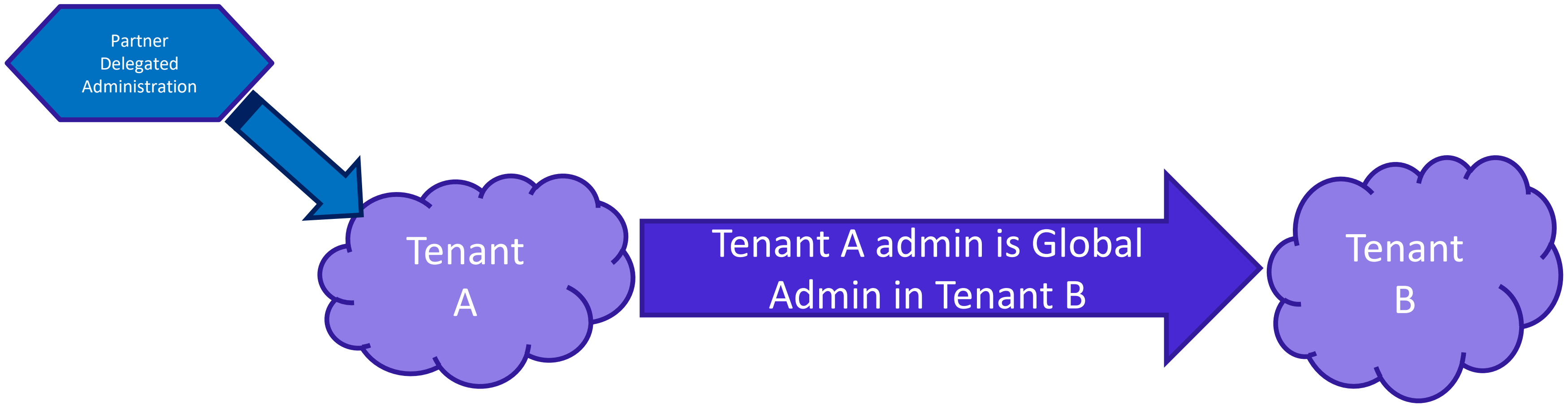
Compromise Azure AD through Application Permissions



Compromise Azure AD through Role Assignable Group Owner Rights



Solarigate “Tenant Hopping”


Partner Delegated Administration
Tenant A
Tenant A admin is Global Admin in Tenant B
Tenant B

- Tenant Hopping (patent pending 😉) is when an attacker compromises one tenant to jump to another, often with privileged rights.
- Similar to trust hopping in Active Directory.
- Solarigate attackers leveraged partner connections.

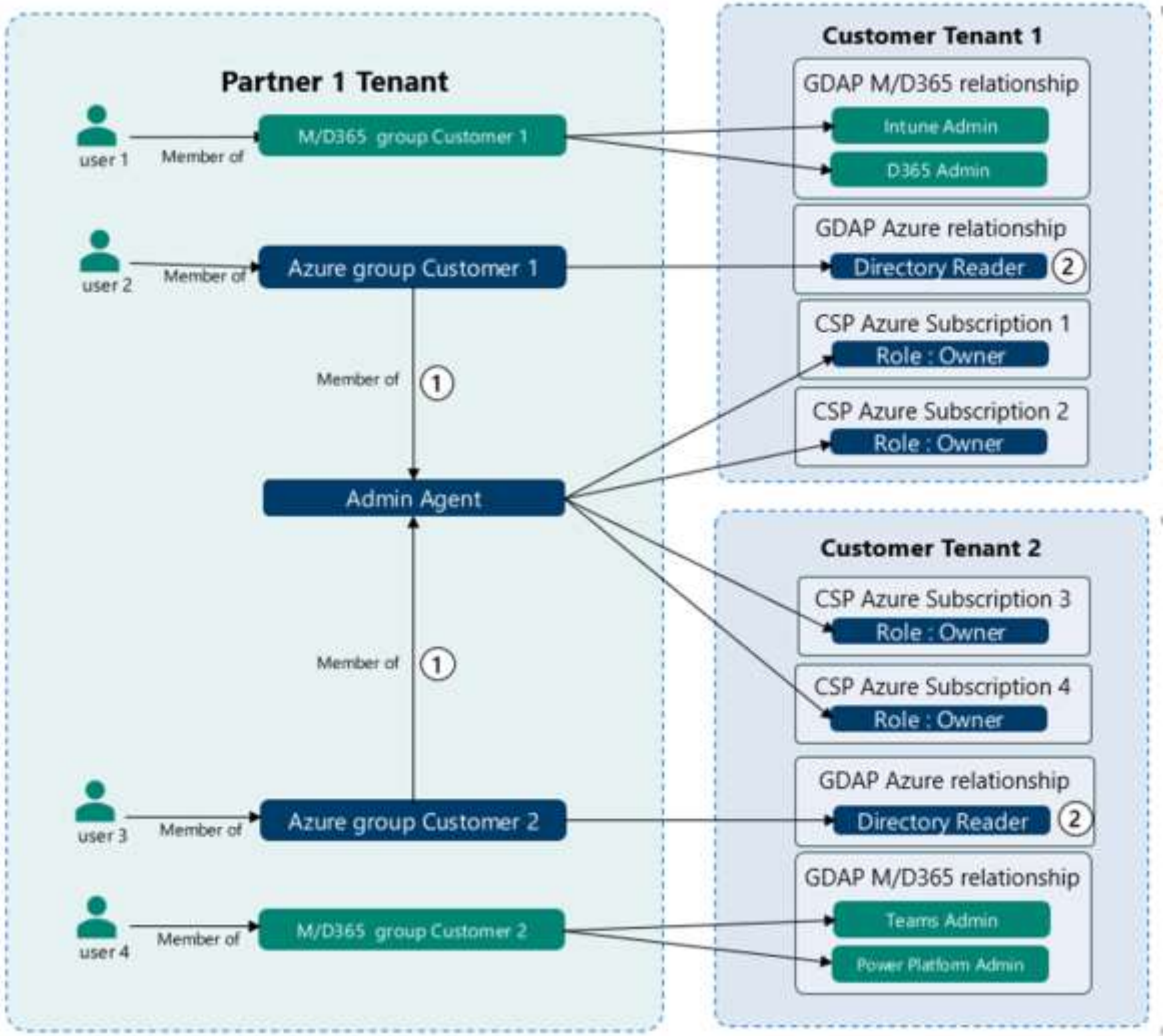
Partner Relationships – aka Delegated Administration

- A configured partner can have admin rights to a customer tenant (“delegated administration”).
- This is provided when the partner requests access to the customer environment.
- When the customer accepts this request:
  - “Admin agent” role in partner tenant is provided effective “Global Administrator” rights to customer tenant.
  - “Helpdesk Agent" role in partner tenant is provided effective "Helpdesk Administrator" (Password Administrator) rights to customer tenant.
  - These are the only options.
  - They **apply to all customer environments** – there is no granular configuration.
- A partner with dozens of customers will result in all partner accounts in these groups having elevated rights in all customer environments.

Shift to granular delegated admin privileges (GDAP) ASAP!

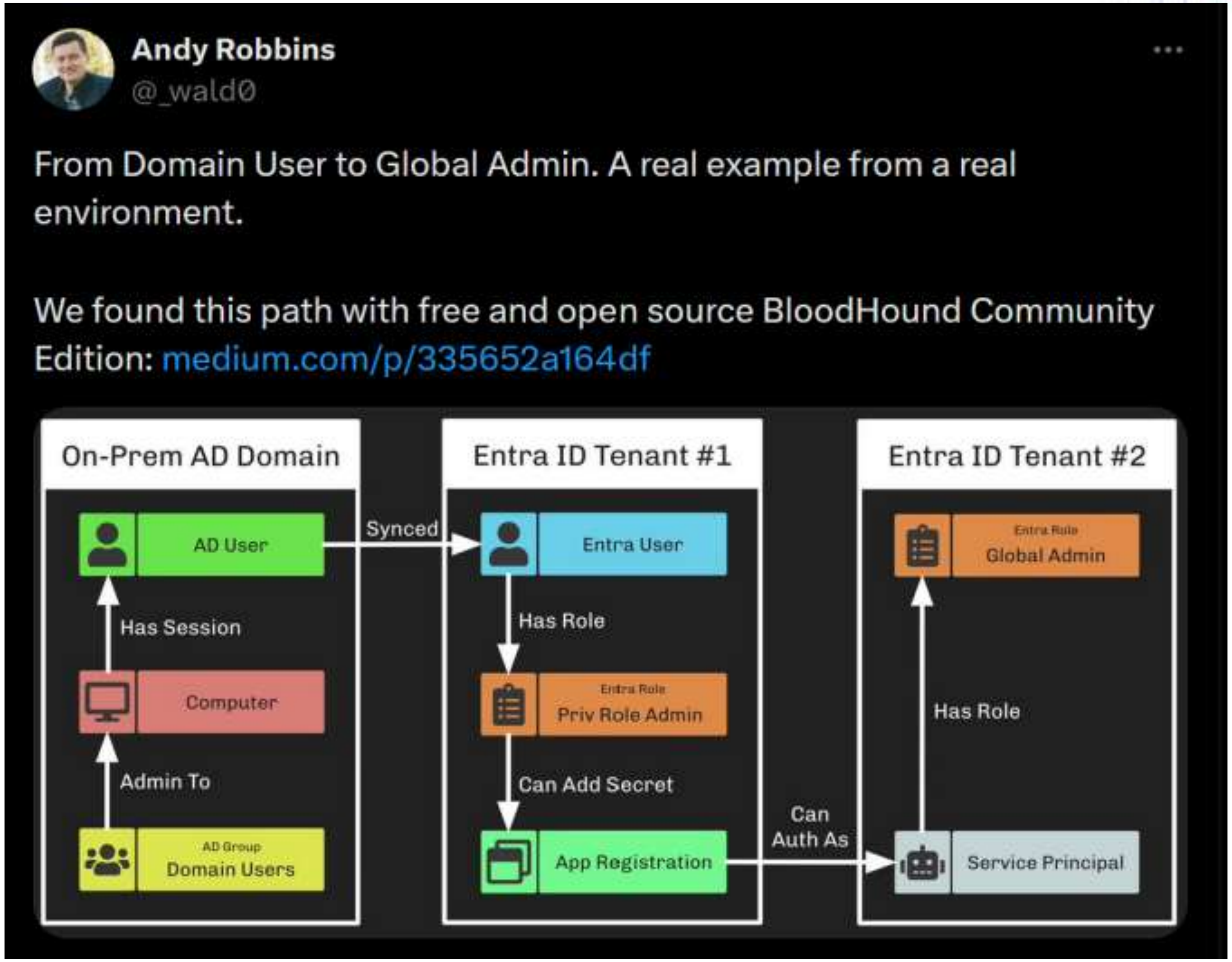
Check Partner Configuration for your tenant here:
https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/PartnerRelationships

Move to Granular Delegated Admin Privileges (GDAP)



https://learn.microsoft.com/en-us/partner-center/gdap-introduction

What about Admins Synchronized from On-Prem AD?



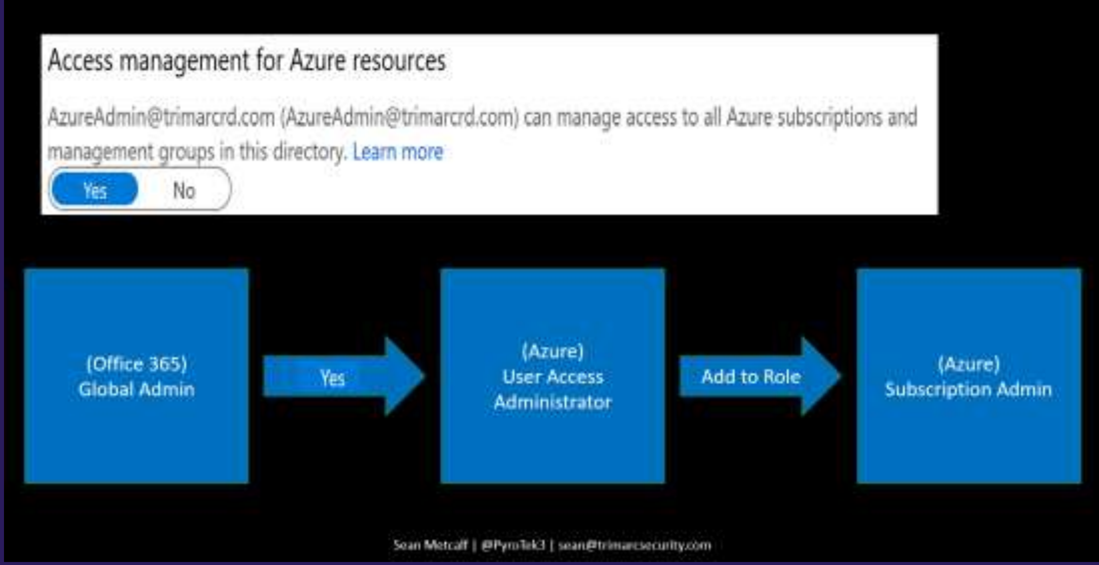
Andy Robbins
@_wald0

From Domain User to Global Admin. A real example from a real environment.

We found this path with free and open source BloodHound Community Edition: medium.com/p/335652a164df

https://posts.specterops.io/hybrid-attack-paths-new-views-and-your-favorite-dog-learns-an-old-trick-335652a164df?gi=543e6e7a310d

RSAC 2025 Conference



Access management for Azure resources

AzureAdmin@trimarcrd.com (AzureAdmin@trimarcrd.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more

[✓ Yes] No

(Office 365) Global Admin → Yes → (Azure) User Access Administrator → Add to Role → (Azure) Subscription Admin

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

From Entra ID to Azure to AD

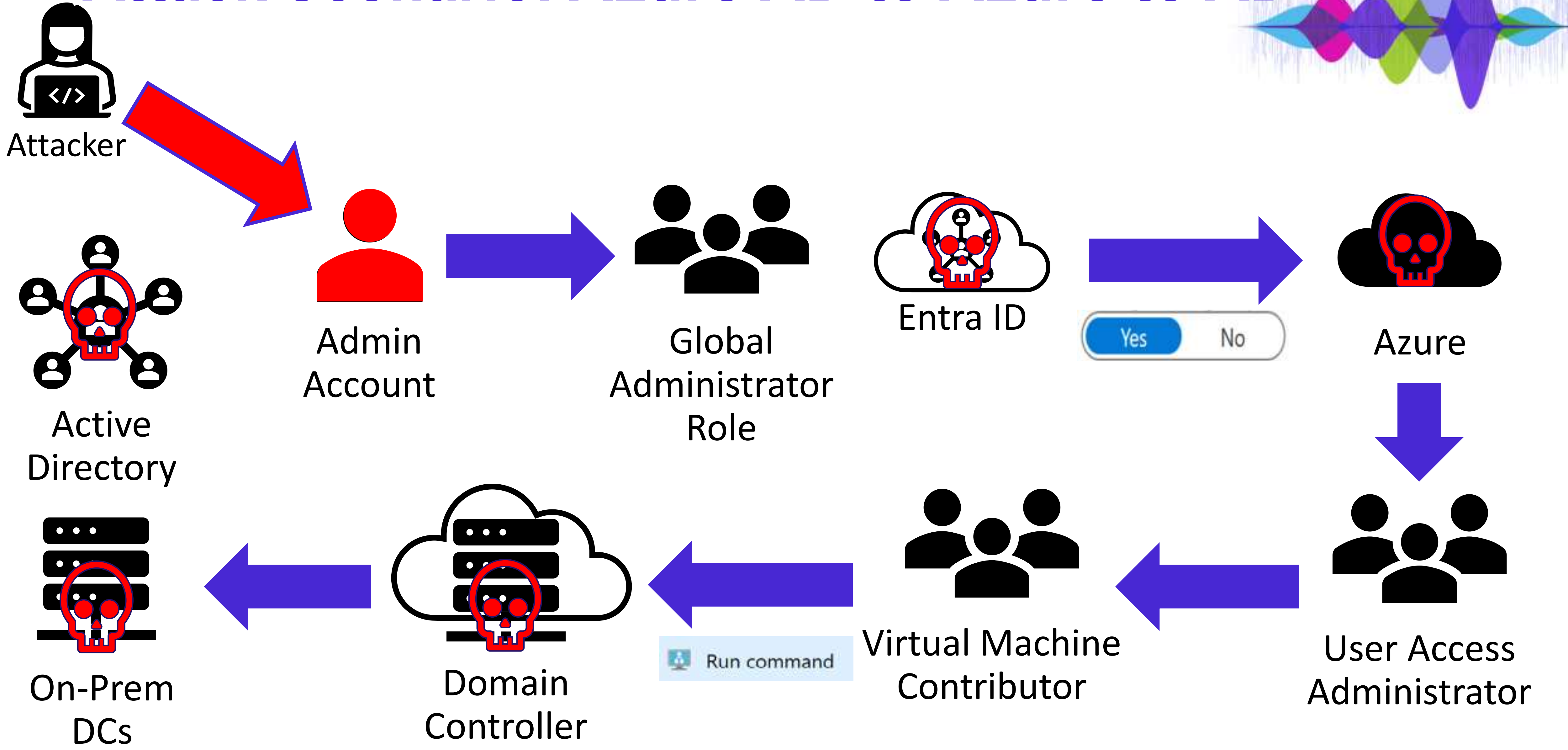
Hacking the Hybrid Cloud

VIRUS ALERT

```
Please select an option:

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt
```

Many Voices.
One Community.

Attack Scenario: Azure AD to Azure to AD



Attacker

Admin Account

Global Administrator Role

Entra ID

Yes No

Azure

User Access Administrator

Virtual Machine Contributor

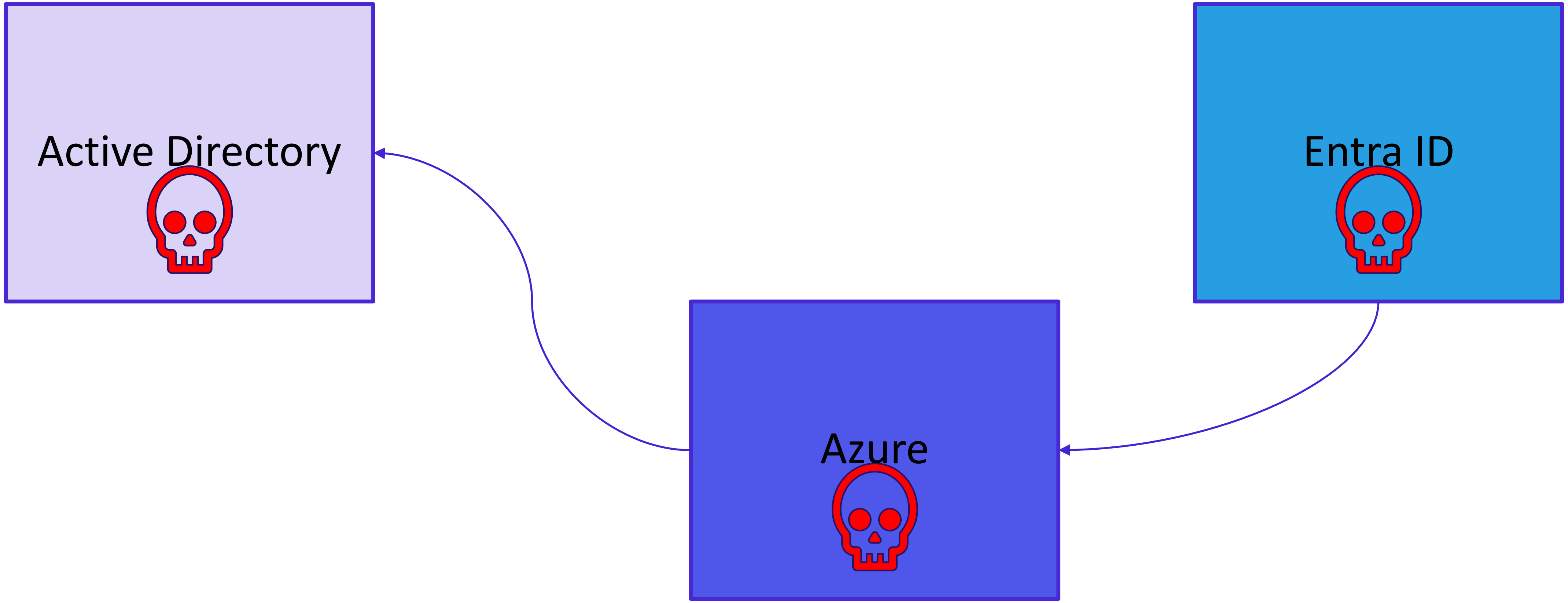
Run command

Domain Controller

On-Prem DCs

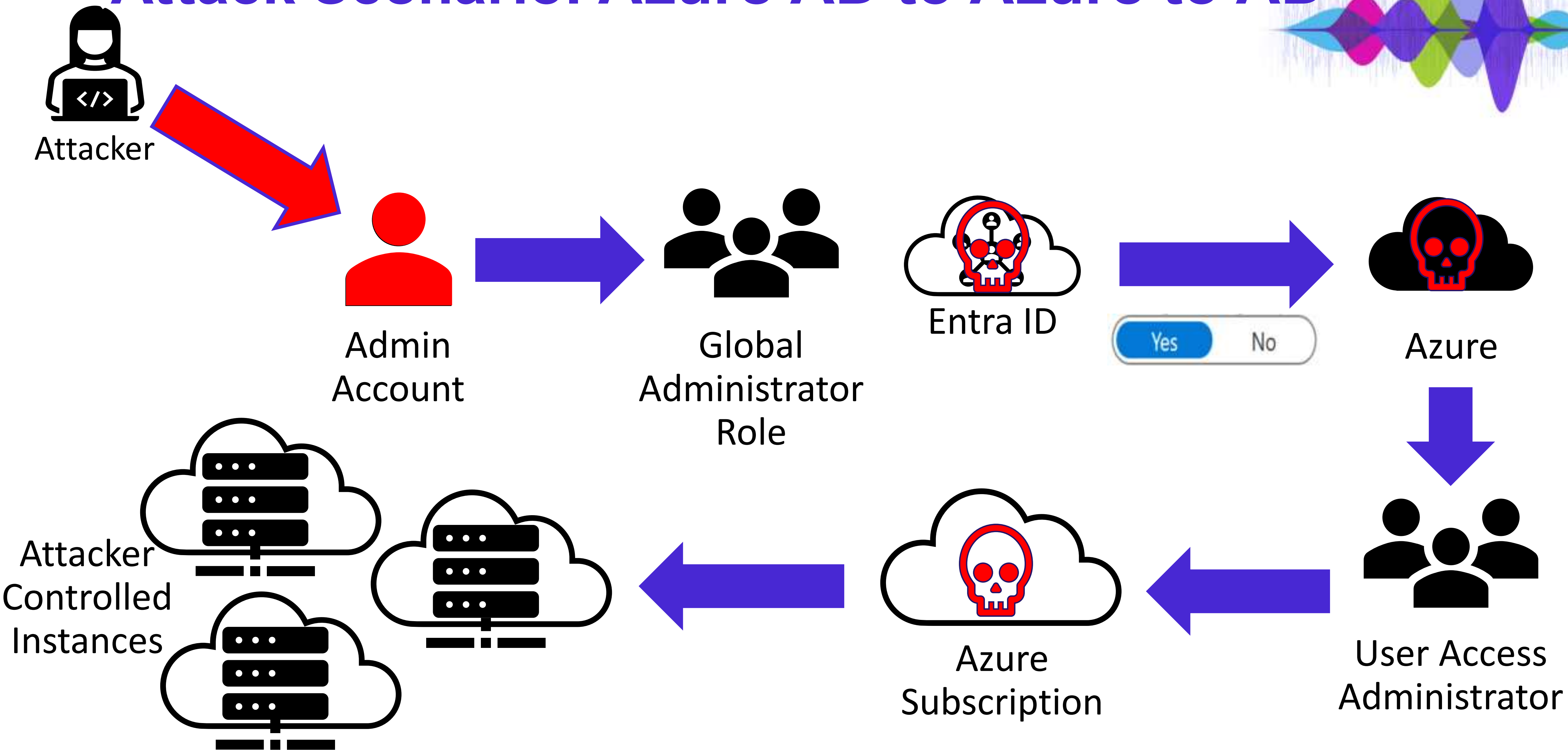
Active Directory

Attack Scenario: Entra ID to Azure to AD



Compromise AD (& Azure & Entra ID) by getting Global Admin rights in Entra ID

Attack Scenario: Azure AD to Azure to AD



Attacker

Admin Account

Global Administrator Role

Entra ID

[✓ Yes] No

Azure

User Access Administrator

Azure Subscription

Attacker Controlled Instances

Attack Scenario Key Takeaways

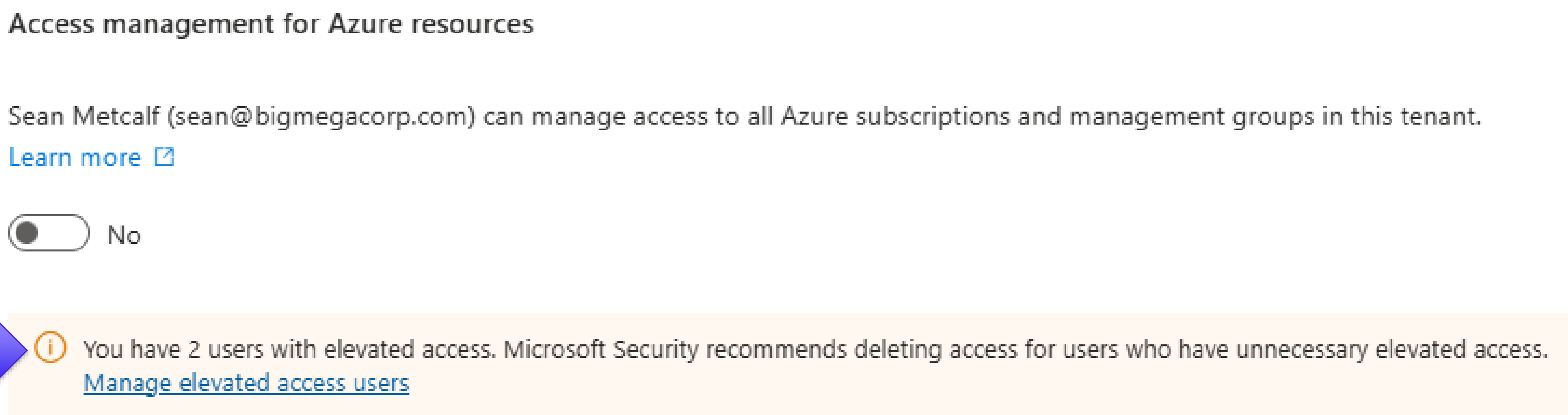
- An attacker that can gain admin rights to one environment can often pivot to another.
- Hosting Domain Controllers on virtual infrastructure such as cloud requires trust in that platform as well as additional protections around compromised accounts & monitoring.
- Jumping from Entra ID to Azure to on-prem Active Directory is possible given how many enterprises are configured and if the Global Admins group isn’t well protected or standard user accounts have the ability to elevate.
- The attacker could also use resources in your subscriptions for their purposes such as spinning up new virtual instances for attacker systems or bitcoin mining.
- Control of subscription access enables the attacker to launch ransomware against virtual instances.

Attack Scenario Key Mitigation

- Severely restrict membership in Global Admins.
- Use PIM (eligible) for Global Admins & require MFA.
- Once Elevated Access is applied to an account, removing role membership has no impact. Elevated Access must be removed separately.
- Monitor the Entra ID Audit Log for Azure RBAC (Elevated Access) activity.
- Closely monitor membership of the “User Access Administrator” Azure role (root level).
- Remove any account with Elevated Access that doesn’t require it.
- Place Domain Controllers and other sensitive systems in another Azure tenant.

https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

Managing Elevated Access



Access management for Azure resources

Sean Metcalf (sean@bigmegacorp.com) can manage access to all Azure subscriptions and management groups in this tenant.

Learn more

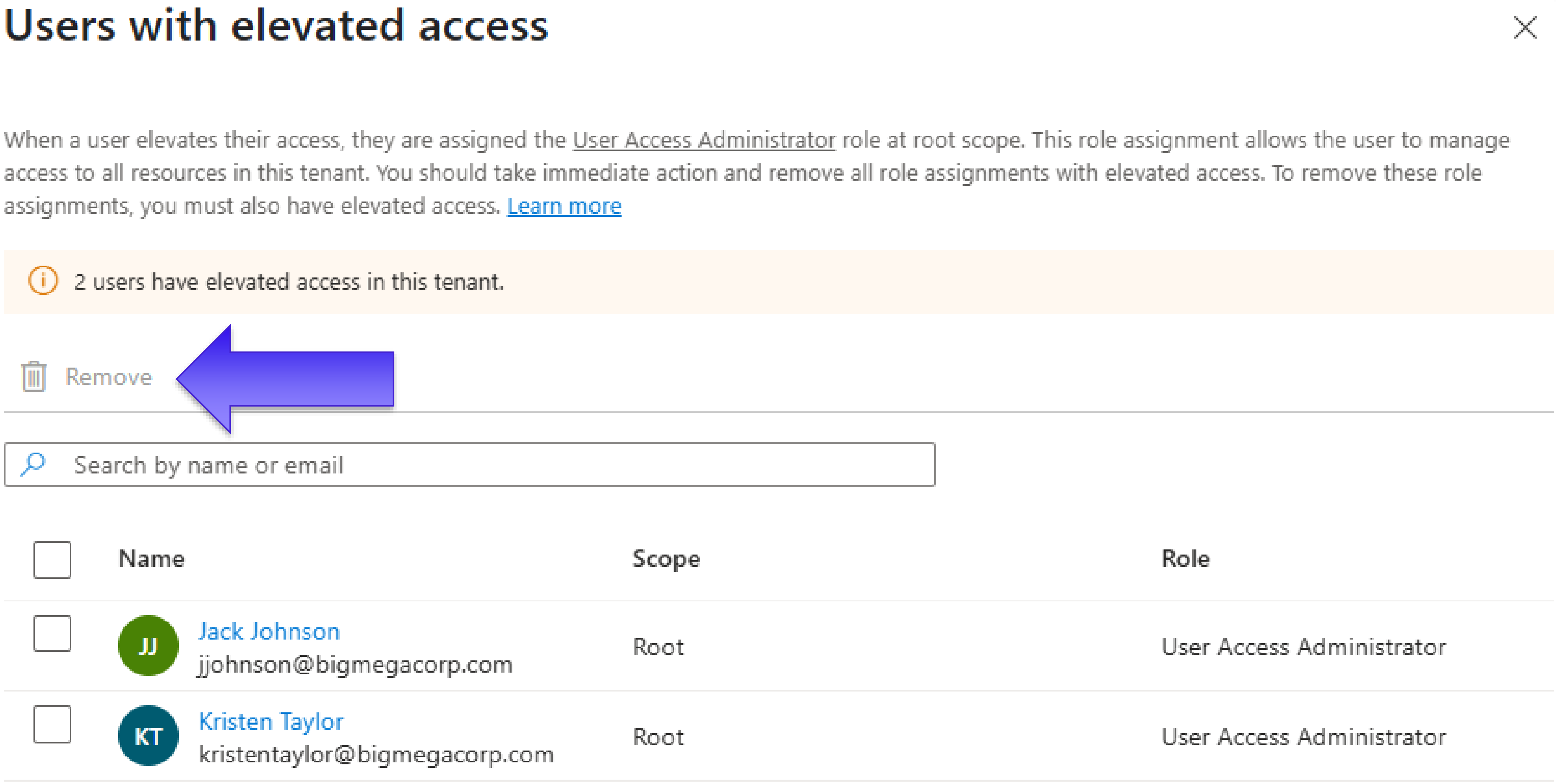
○ No

ⓘ You have 2 users with elevated access. Microsoft Security recommends deleting access for users who have unnecessary elevated access.

Manage elevated access users

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Properties

Managing Elevated Access



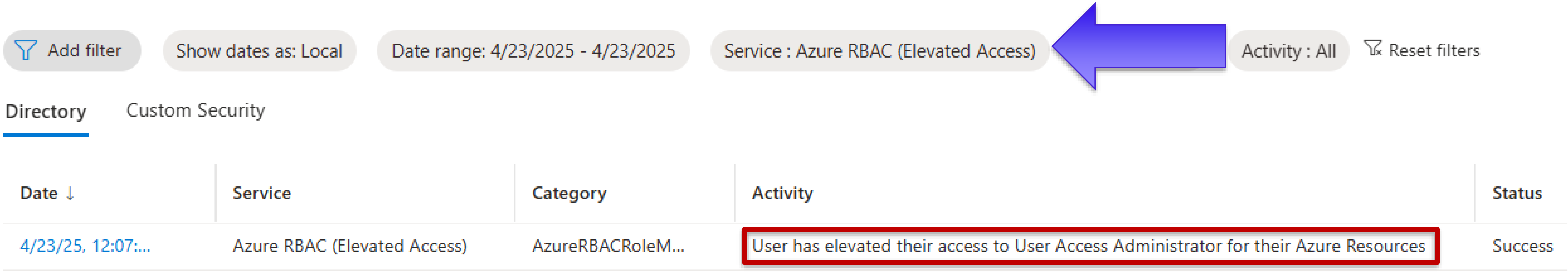
Users with elevated access

When a user elevates their access, they are assigned the User Access Administrator role at root scope. This role assignment allows the user to manage access to all resources in this tenant. You should take immediate action and remove all role assignments with elevated access. To remove these role assignments, you must also have elevated access. Learn more

ⓘ 2 users have elevated access in this tenant.

□	Name	Scope	Role
□	JJ Jack Johnson jjohnson@bigmegacorp.com	Root	User Access Administrator
□	KT Kristen Taylor kristentaylor@bigmegacorp.com	Root	User Access Administrator

Elevated Access Audit Logs (preview)



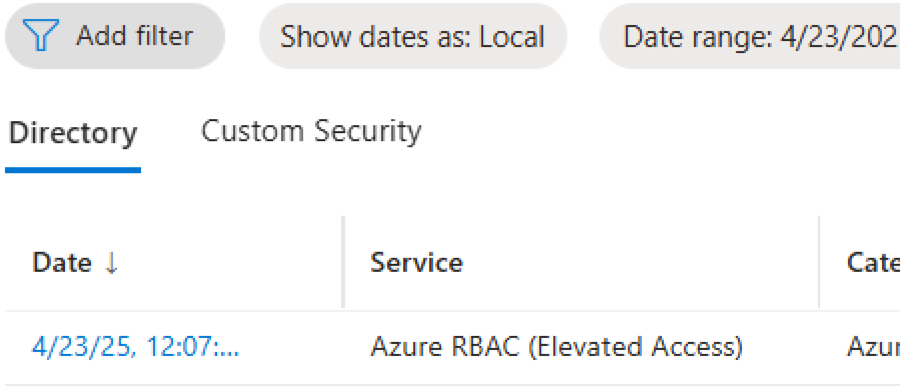
Add filter | Show dates as: Local | Date range: 4/23/2025 - 4/23/2025 | Service : Azure RBAC (Elevated Access) | Activity : All | Reset filters

Directory | Custom Security

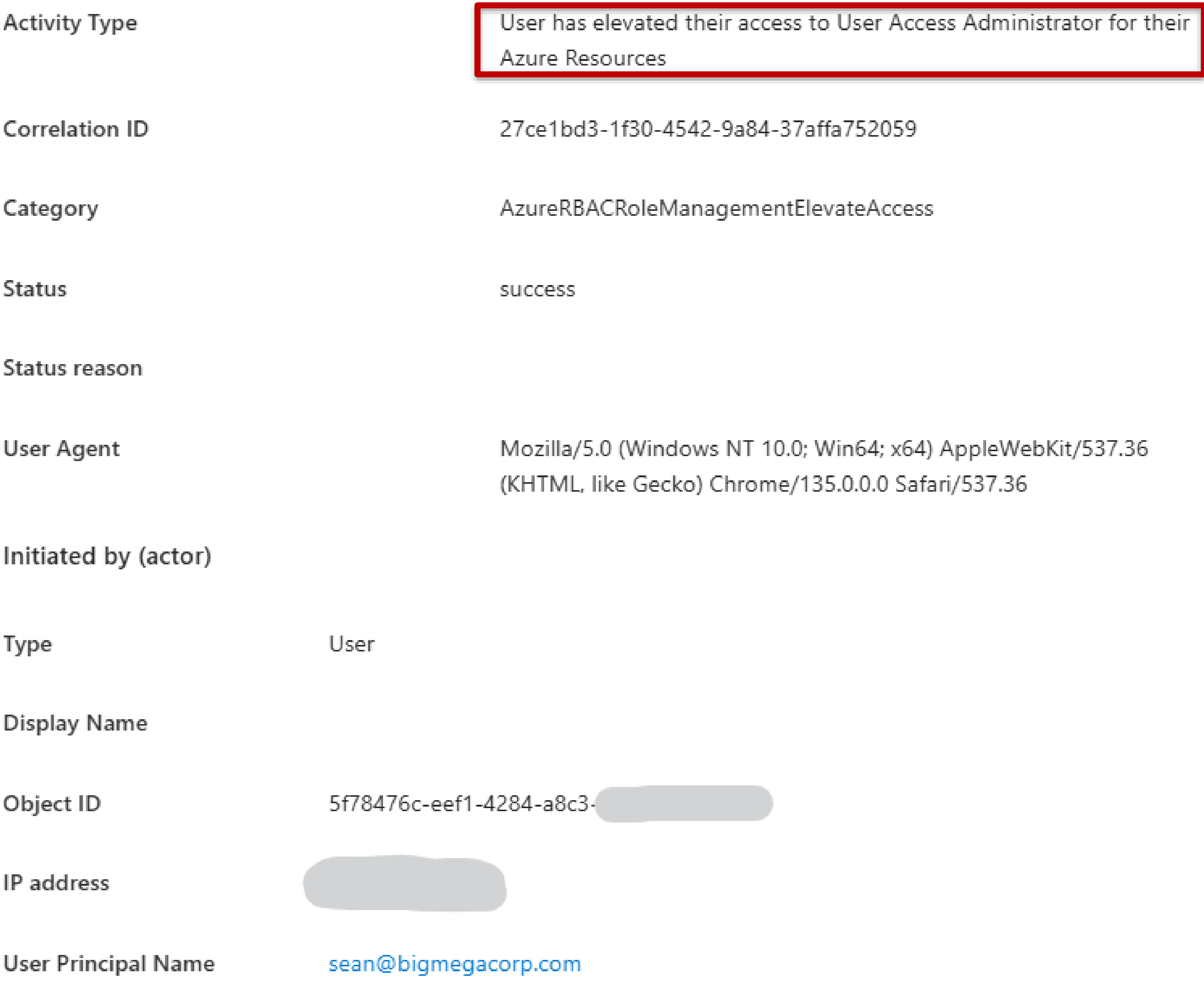
Date ↓	Service	Category	Activity	Status
4/23/25, 12:07:...	Azure RBAC (Elevated Access)	AzureRBACRoleM...	User has elevated their access to User Access Administrator for their Azure Resources	Success

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Audit

Elevated Access Audit Logs (preview)



Date ↓	Service	Cate
4/23/25, 12:07:...	Azure RBAC (Elevated Access)	Azur

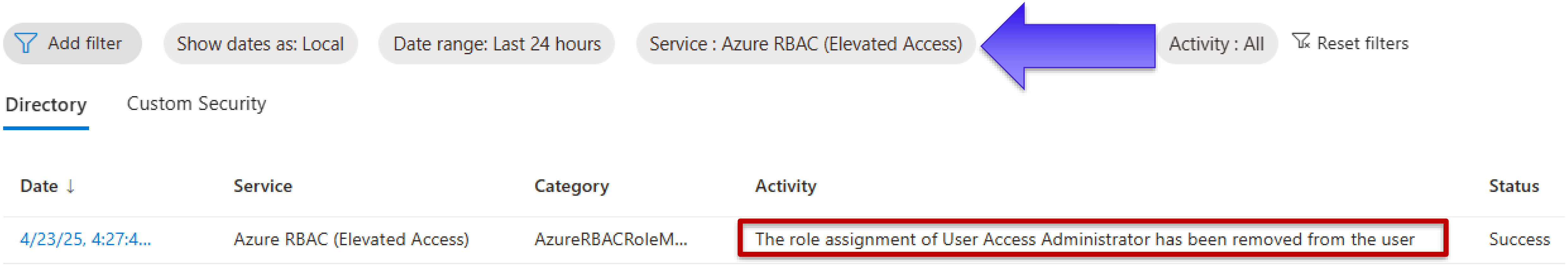


Activity Type	User has elevated their access to User Access Administrator for their Azure Resources
Correlation ID	27ce1bd3-1f30-4542-9a84-37affa752059
Category	AzureRBACRoleManagementElevateAccess
Status	success
Status reason	
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36

Initiated by (actor)

Type	User
Display Name	
Object ID	5f78476c-eef1-4284-a8c3-[redacted]
IP address	[redacted]
User Principal Name	sean@bigmegacorp.com

Elevated Access Audit Logs (preview)



Show dates as: Local

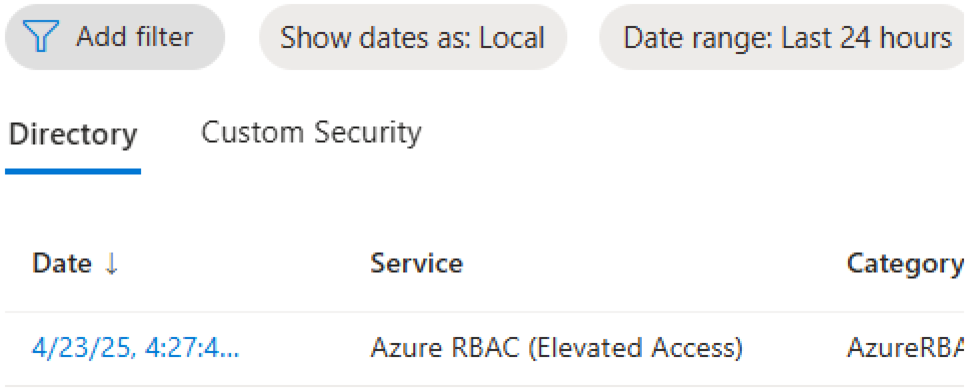
Date range: Last 24 hours

Service : Azure RBAC (Elevated Access)

Activity : All

Date ↓	Service	Category	Activity	Status
4/23/25, 4:27:4...	Azure RBAC (Elevated Access)	AzureRBACRoleM...	The role assignment of User Access Administrator has been removed from the user	Success

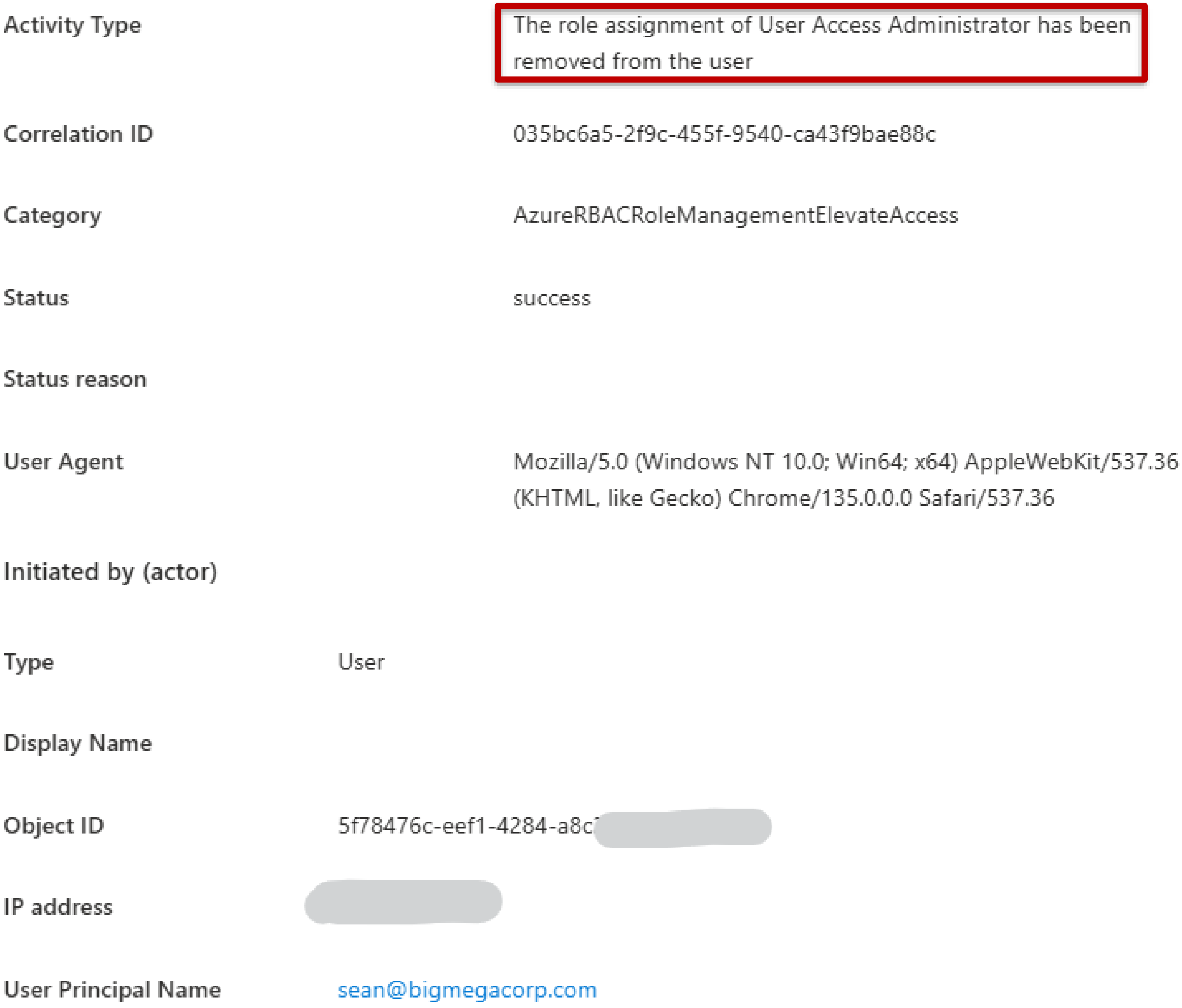
Elevated Access Audit Logs (preview)



Add filter | Show dates as: Local | Date range: Last 24 hours

Directory | Custom Security

Date ↓	Service	Category
4/23/25, 4:27:4...	Azure RBAC (Elevated Access)	AzureRBA



Activity Type	The role assignment of User Access Administrator has been removed from the user
Correlation ID	035bc6a5-2f9c-455f-9540-ca43f9bae88c
Category	AzureRBACRoleManagementElevateAccess
Status	success
Status reason	
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36

Initiated by (actor)

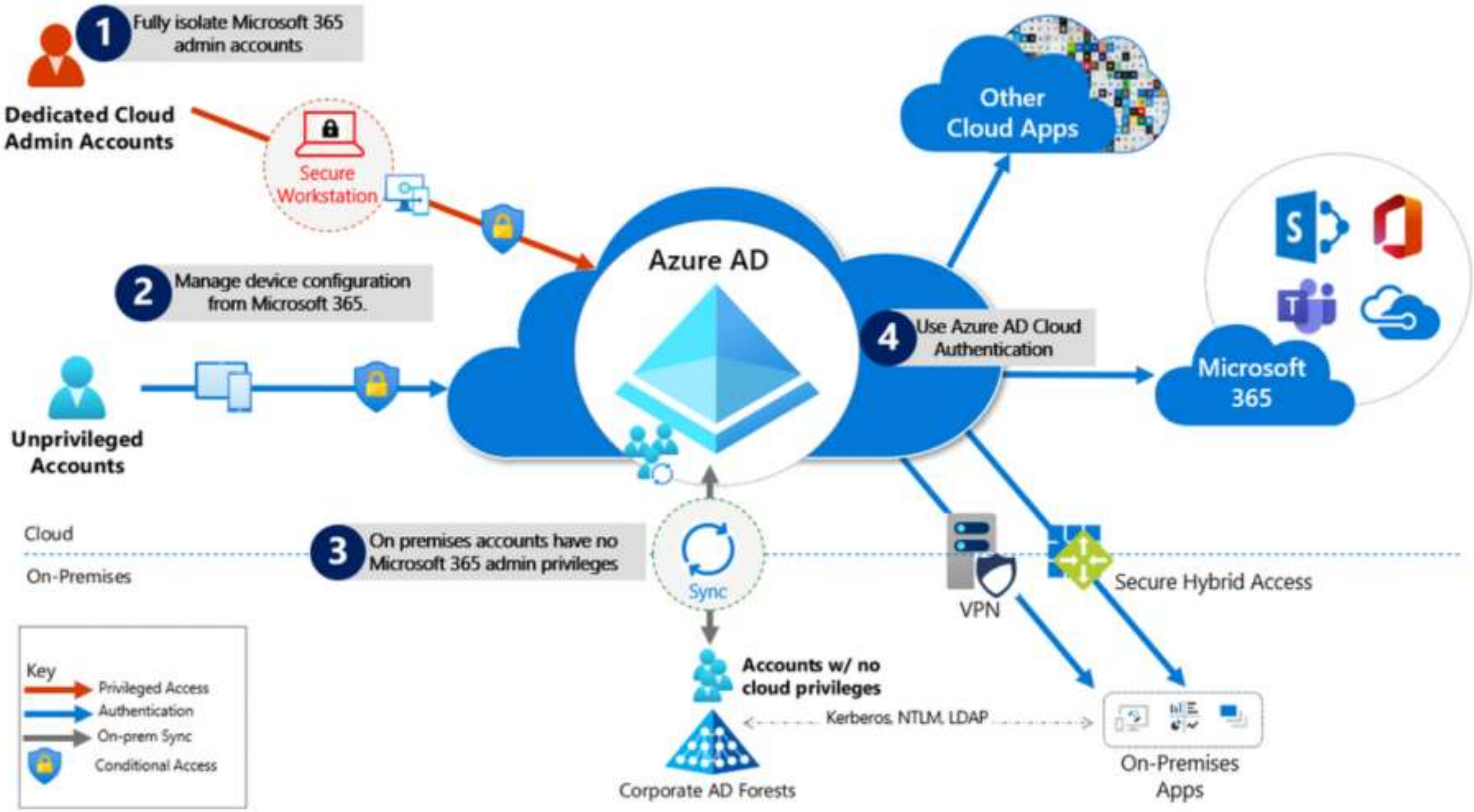
Type	User
Display Name	
Object ID	5f78476c-eef1-4284-a8c[redacted]
IP address	[redacted]
User Principal Name	sean@bigmegacorp.com

RSAC™ | 2025 Conference

Securing Entra ID Administration

Many Voices.
One Community.

Securing Entra ID



1 Fully isolate Microsoft 365 admin accounts

2 Manage device configuration from Microsoft 365.

3 On premises accounts have no Microsoft 365 admin privileges

4 Use Azure AD Cloud Authentication

Dedicated Cloud Admin Accounts

Secure Workstation

Unprivileged Accounts

Azure AD

Other Cloud Apps

Microsoft 365

Cloud

On-Premises

Sync

VPN

Secure Hybrid Access

Accounts w/ no cloud privileges

Kerberos, NTLM, LDAP

Corporate AD Forests

On-Premises Apps

Key

Privileged Access

Authentication

On-prem Sync

Conditional Access

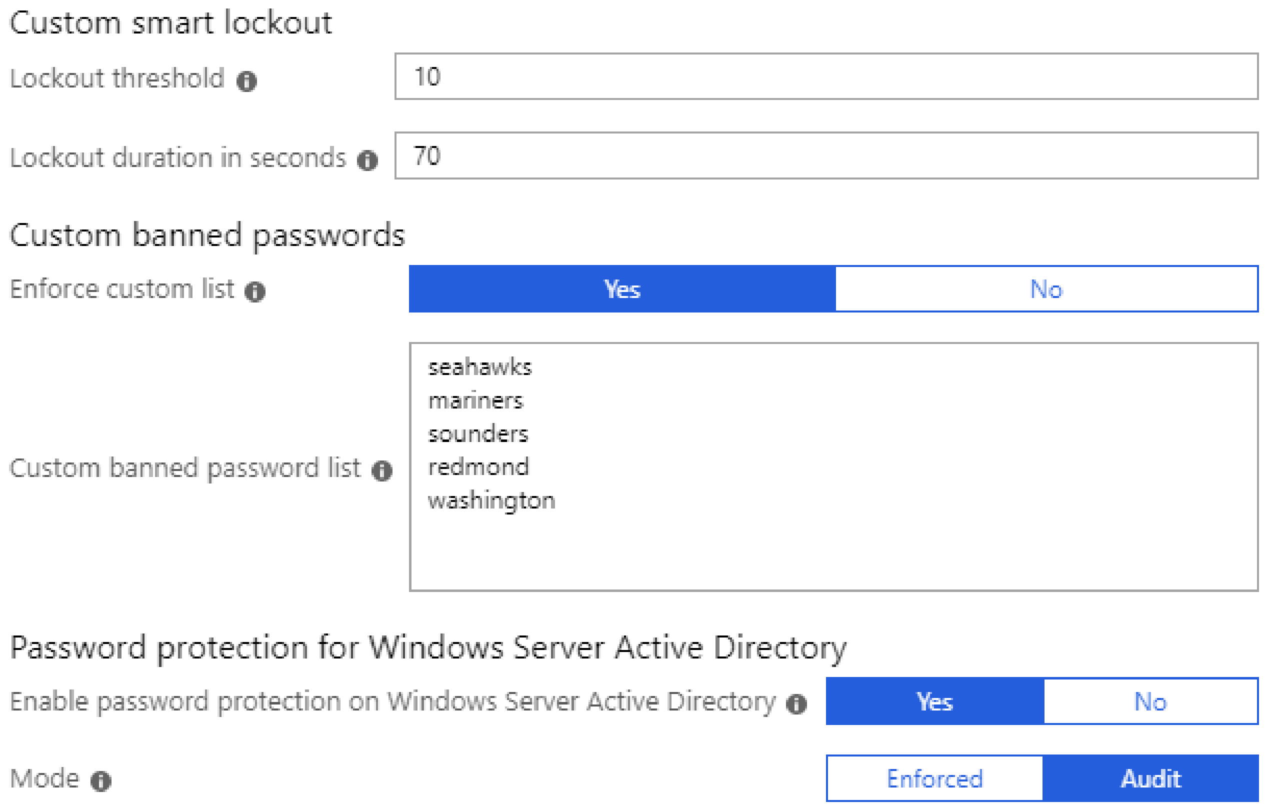
Securing Entra ID - Microsoft Summary

- Fully Isolate Entra ID & Microsoft 365 admin accounts
  They should be:
  - Created in Entra ID.
  - Required to use Multi-factor authentication (MFA).
  - Secured by conditional access.
  - Accessed only by using Azure Managed Workstations.

There should be no on-prem accounts with highly privileged Entra ID rights.

On-Prem: Entra Password Protection

- Prevent users from selecting known bad passwords
- Start in audit mode to get an idea how bad it is



Custom smart lockout

Lockout threshold ⓘ	10
Lockout duration in seconds ⓘ	70

Custom banned passwords

Enforce custom list ⓘ	[✓ Yes] No
Custom banned password list ⓘ	seahawks mariners sounders redmond washington

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ	[✓ Yes] No
Mode ⓘ	Enforced [✓ Audit]

https://aka.ms/deploypasswordprotection

Phishing Defensive Layers

Require Users to MFA (FIDO2 preferred)

- Microsoft Authenticator app recommended

Conditional Access Policy

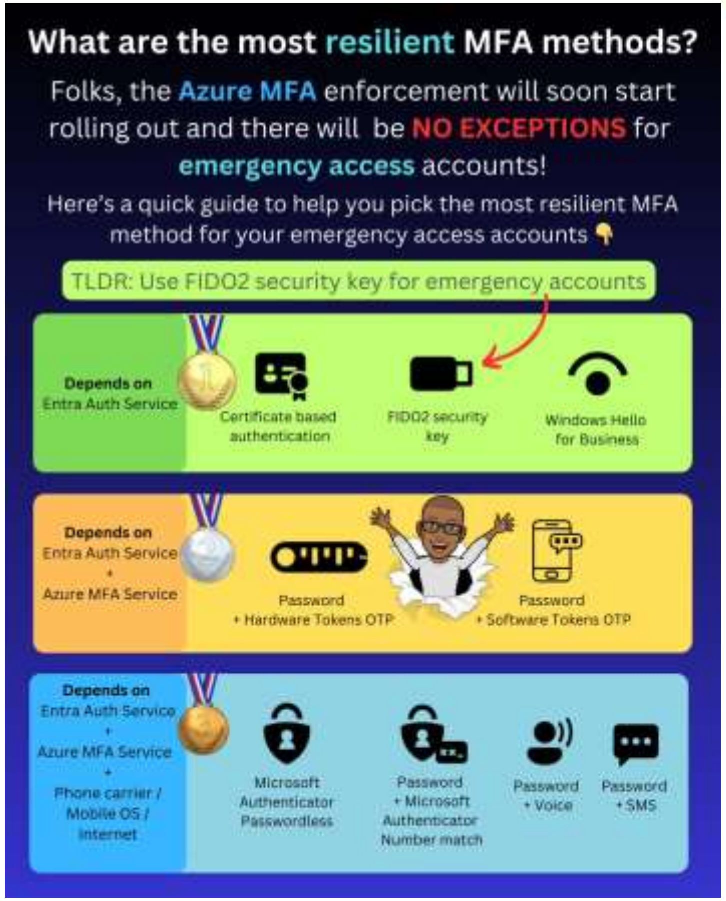
- Enforce MFA
- For specific apps
- Location based grant/block rules

Risk Based Policy

- Only prompt the user to take action when risk is detected

Key Cloud Administration Security Controls

- Use admin systems for cloud administration
- Enforce FIDO2 for Trimarc Level 0 & 1 roles
- FIDO2 keys for Emergency “Break Glass” Accounts
- Leverage Conditional Access policies to enforce MFA for admins from all locations



What are the most resilient MFA methods?

Folks, the Azure MFA enforcement will soon start rolling out and there will be NO EXCEPTIONS for emergency access accounts!

Here’s a quick guide to help you pick the most resilient MFA method for your emergency access accounts 👇

TLDR: Use FIDO2 security key for emergency accounts

Depends on
Entra Auth Service
Certificate based authentication
FIDO2 security key
Windows Hello for Business
Depends on
Entra Auth Service
+
Azure MFA Service
Password + Hardware Tokens OTP
Password + Software Tokens OTP
Depends on
Entra Auth Service
+
Azure MFA Service
+
Phone carrier / Mobile OS / internet
Microsoft Authenticator Passwordless
Password + Microsoft Authenticator Number match
Password + Voice
Password + SMS

https://x.com/merill/status/1821027962864726249/

Key Points for Securing Entra ID

- Review Level 0 & Level 1 roles and ensure they are not synchronized from on-prem Active Directory.
- Ensure no standard user accounts have privileged role membership (Level 0 & Level 1) which includes PIM eligible.
- Review Level 0 & Level 1 membership on a regular basis, including PIM eligible.
- Ensure all Level 0 & Level 1 members are PIM eligible (service accounts & service principles excepted).
- Review role assignable group membership and owner rights on a regular basis.
- Review Application Administrator & Cloud Application Administrator members when there are applications with Level 0 & Level 1 application permissions.
- Ensure that Conditional Access requires MFA for Level 0 & Level 1 role members for every authentication, preferably FIDO2/Microsoft Authenticator push (service accounts & service principles excepted).
- Ensure there is at least 1 emergency access admin account configured with a FIDO2 key(s).

Common Persistence Method Checks

- Review Illicit Consent Grants (OAUTH)
  https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide

- Review Exchange Forms/Rules for potentially malicious settings.
  https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide

- Review Exchange Online mailbox permissions for unusual/unintended configuration (Get-ExoMailboxPermission)
  https://docs.microsoft.com/en-us/powershell/module/exchange/powershell-v2-module/get-exomailboxpermission?view=exchange-ps

Apply What You Have Learned Today

- Next week you should:
  - Identify the Level 0 & Level 1 accounts and Level 0 applications
- In the first three months following this presentation you should:
  - Implement PIM with eligible conditions for all Level 0 & Level 1 accounts.
  - Configure auditing around Elevated Access.
- Within six months you should:
  - Implement Microsoft Authenticator MFA for all admin accounts
  - Remove text/SMS as an MFA option

Conclusion

Attackers are targeting the cloud

Identifying common security issues and resolving them improves system security.

Fixing these issues provides improved breach resilience.

RSAC™ | 2025 Conference

Thank You!