TRUSTEDSEC

General Housekeeping



This presentation is being recorded.

Please silence your cell phones and devices.

Please hold your questions until the end of the presentation.

We want your feedback! Survey available at the end of this presentation.



10 Ways to Secure Entra ID

Brandon Colley & Sean Metcalf

TRUSTEDSEC



10+ Ways to Secure Entra ID

Brandon Colley & Sean Metcalf

TRUSTEDSEC

About Brandon

- Senior Security Consultant @ TrustedSec
- 15+ years experience administering and securing AD
- Speaker: DEFCON, CypherCon, TEC, BsidesKC, CornCon, Hackers Teaching Hackers, etc.
- Identity Security Research Blogger - Quest, Practical 365, TrustedSec, etc.
- @techBrandon – LinkedIn, Twitter, GitHub



About Sean

- Identity Security Architect @ TrustedSec
- Founder of Trimarc Security
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, Blue Team Con, multiple BSides, DEFCON, DerbyCon, HIPConf, RSAC, TEC, Troopers, etc.
- Enterprise Security Weekly Co-Host
- Former Microsoft MVP
- Security Consultant / Researcher
- Own & Operate ADSecurity.org (Microsoft identity security info)



PyroTek.io/About

10+ Ways to Secure Entra ID

Agenda

1. User Defaults
2. Guest Defaults
3. Application Consent Defaults
4. Entra ID Roles (Tier 0 & 1)
5. Privileged Role Membership (admin accounts, MFA, etc.)
6. Role Assignable Groups
7. Highly Privileged Applications
8. Conditional Access
9. Partner Access
10. Secure Entra Connect
11. Entra ID Attacks



Dangerous Defaults



#1 User Defaults
#2 Guest Defaults

Defaults

Default user role permissions

Learn more

Users can register applications — Yes

Restrict non-admin users from creating tenants — No

Users can create security groups — Yes

Guest user access

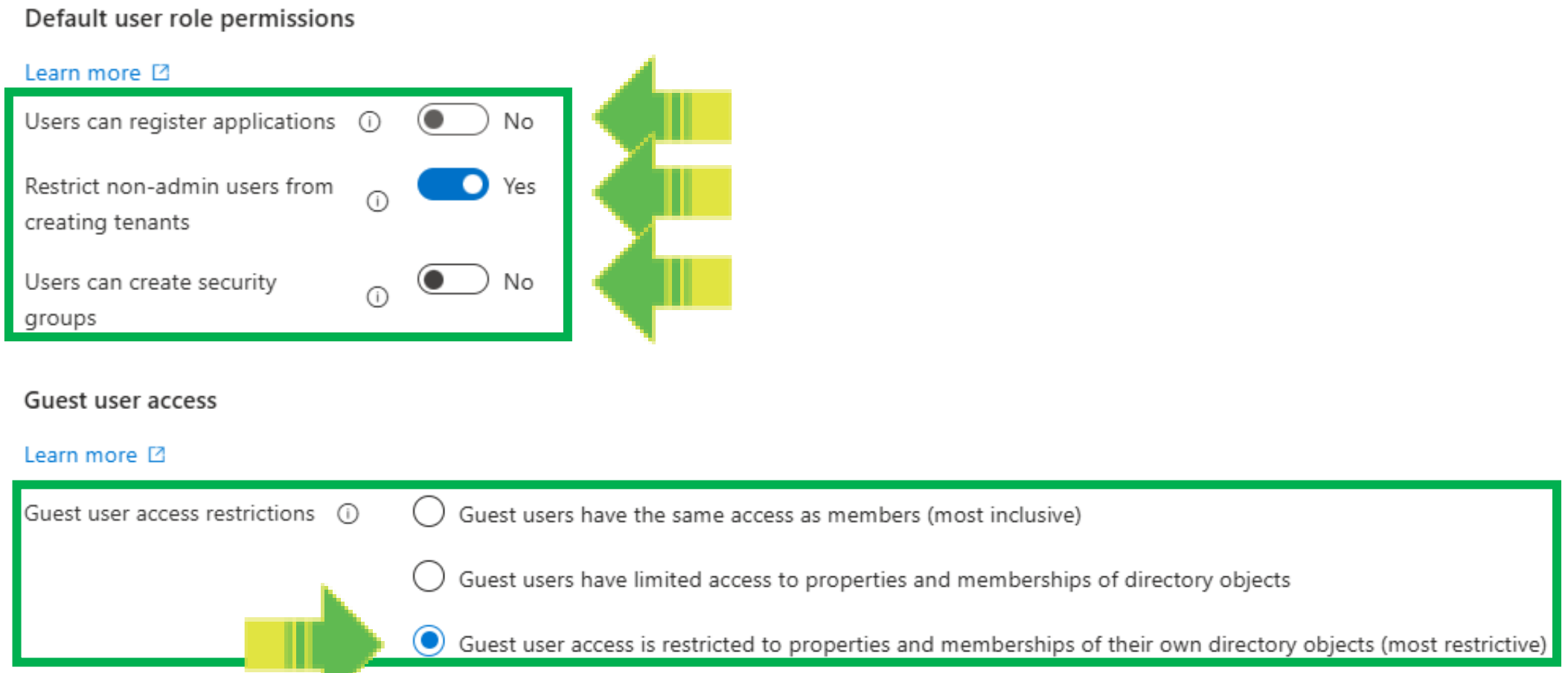
Learn more

Guest user access restrictions

- (●) Guest users have the same access as members (most inclusive)
- ( ) Guest users have limited access to properties and memberships of directory objects
- ( ) Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings

Recommendation



https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings

Defaults

Users may join devices to Microsoft Entra ⓘ

All | Selected | None

Selected

No member selected

Users may register their devices with Microsoft Entra ⓘ

All | None

Learn more on how this setting works

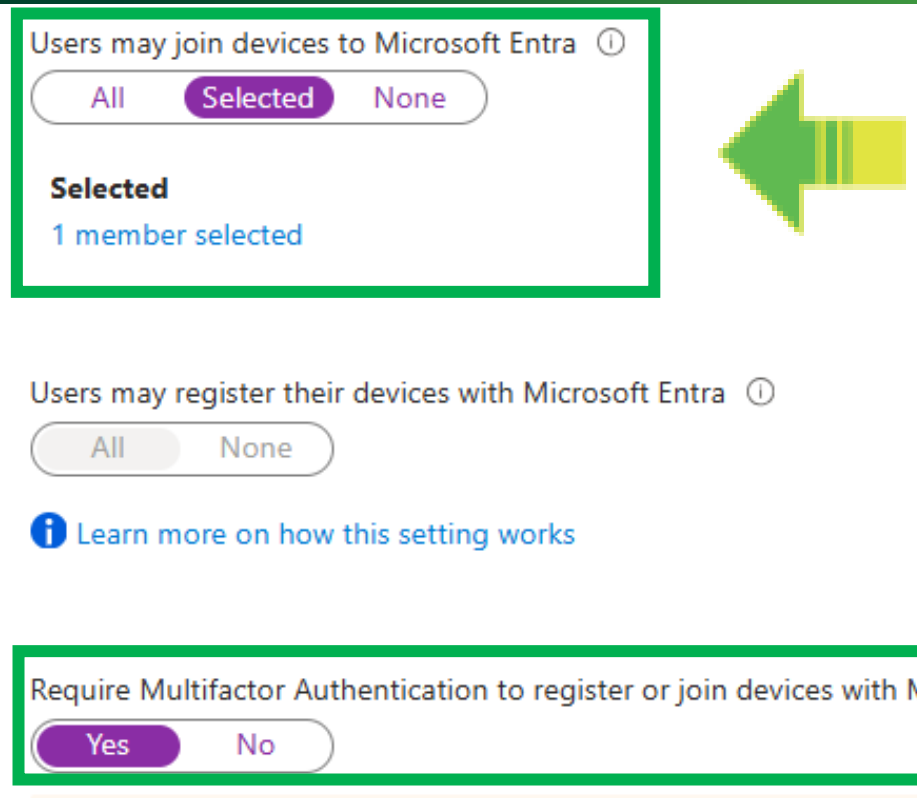
Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

Yes | No

⚠ We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using Conditional Access. Set this device setting to No if you require Multifactor Authentication using Conditional Access.

https://portal.azure.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/DeviceSettings/menuId~/null

Recommendation



https://portal.azure.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/DeviceSettings/menuId~/null

Defaults

Guest invite settings

Guest invite restrictions ⓘ

Learn more

- (•) Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ( ) Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ( ) Only users assigned to specific admin roles can invite guest users
- ( ) No one in the organization can invite guest users including admins (most restrictive)

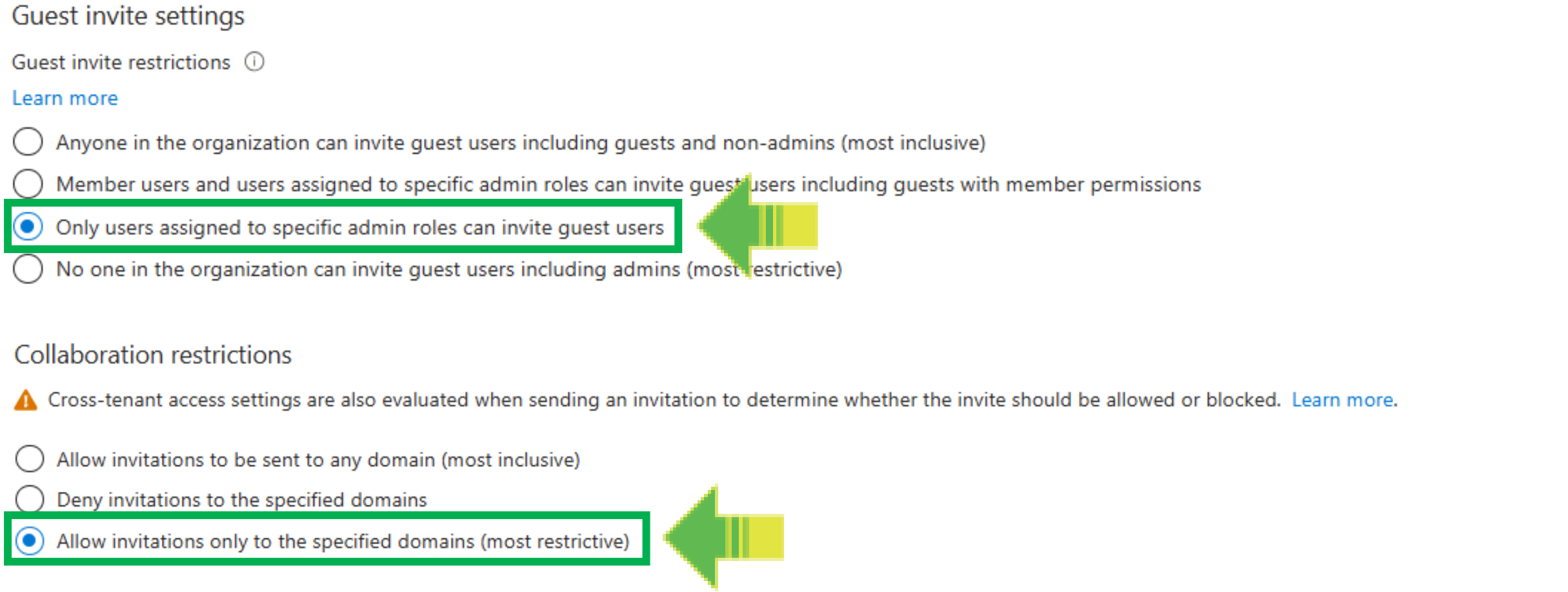
Collaboration restrictions

⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. Learn more.

- (•) Allow invitations to be sent to any domain (most inclusive)
- ( ) Deny invitations to the specified domains
- ( ) Allow invitations only to the specified domains (most restrictive)

https://portal.azure.com/#view/Microsoft_AAD_IAM/AllowlistPolicyBlade

Recommendation



https://portal.azure.com/#view/Microsoft_AAD_IAM/AllowlistPolicyBlade



#3 Secure Entra ID Application Consent Defaults



TRUSTEDSEC

THE FUTURE IS TRUSTEDSEC
SMILEYCON 2026

Once Upon a Time…



Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

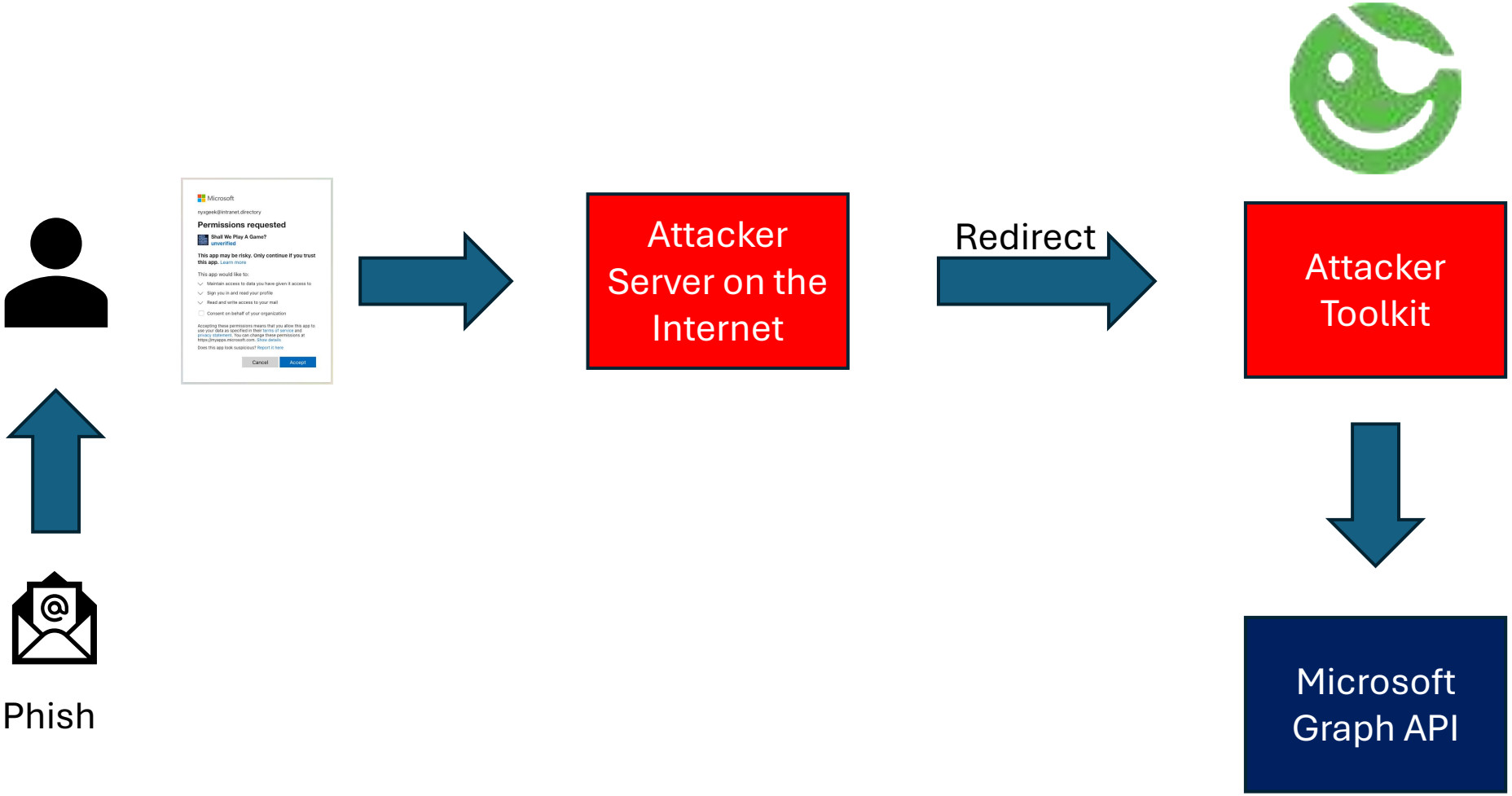
Save | Discard | Got feedback?

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data.
Learn more about consent and permissions

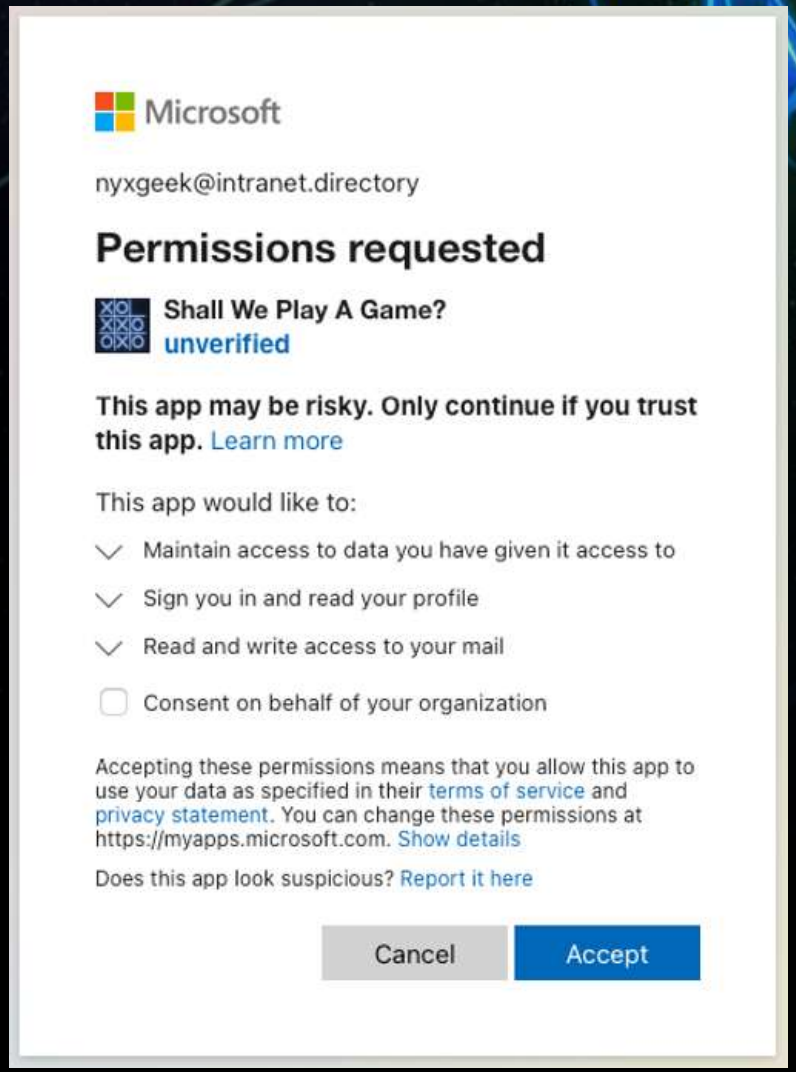
User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- Do not allow user consent
  An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- Allow user consent for apps
  All users can consent for any app to access the organization's data.

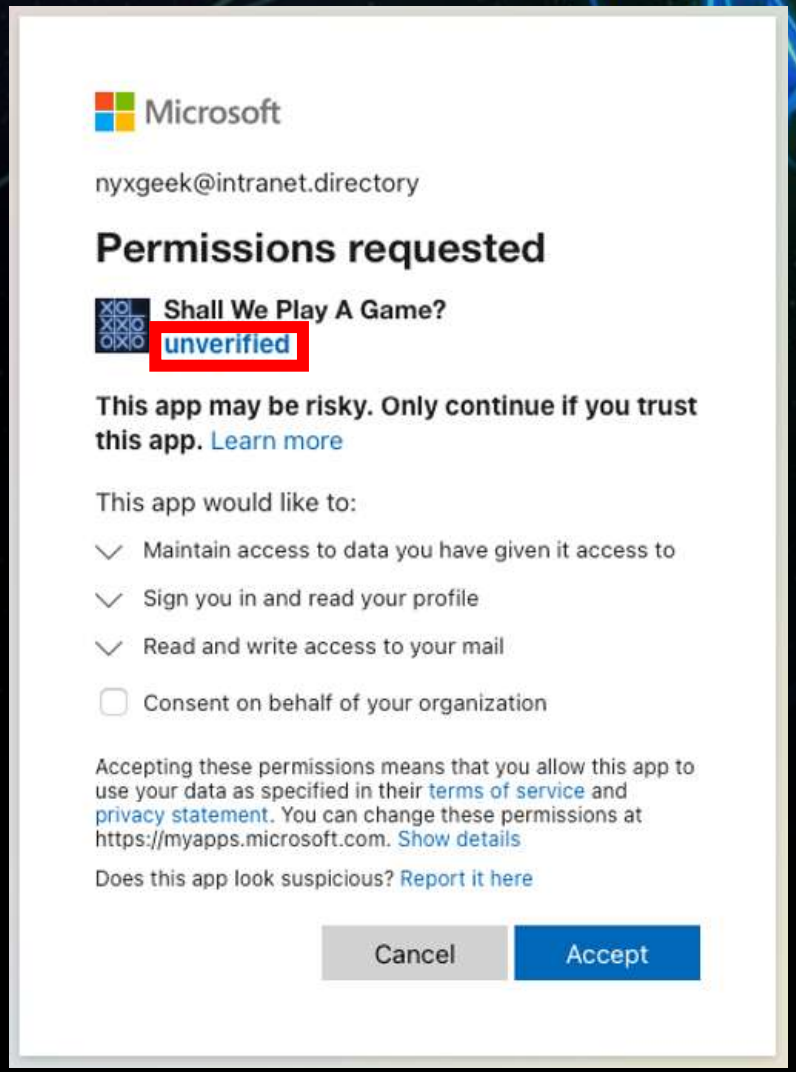
Conceptual Consent Grant Attack Flow



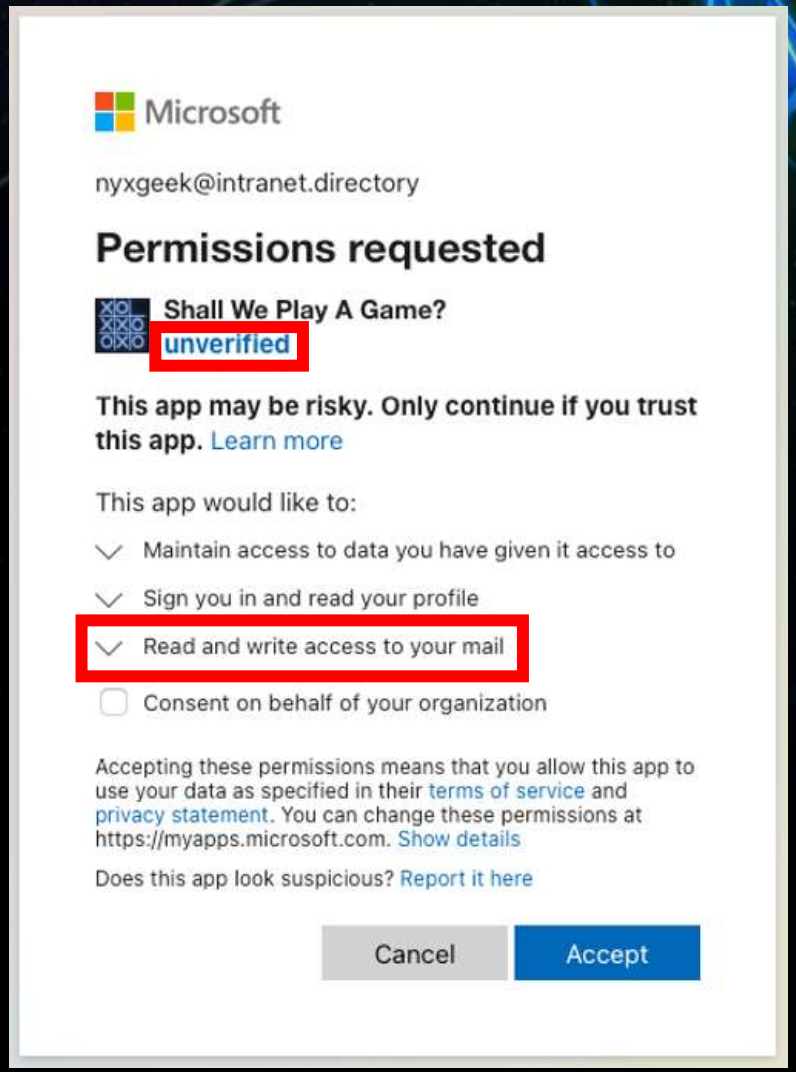
Consent Grant Attack



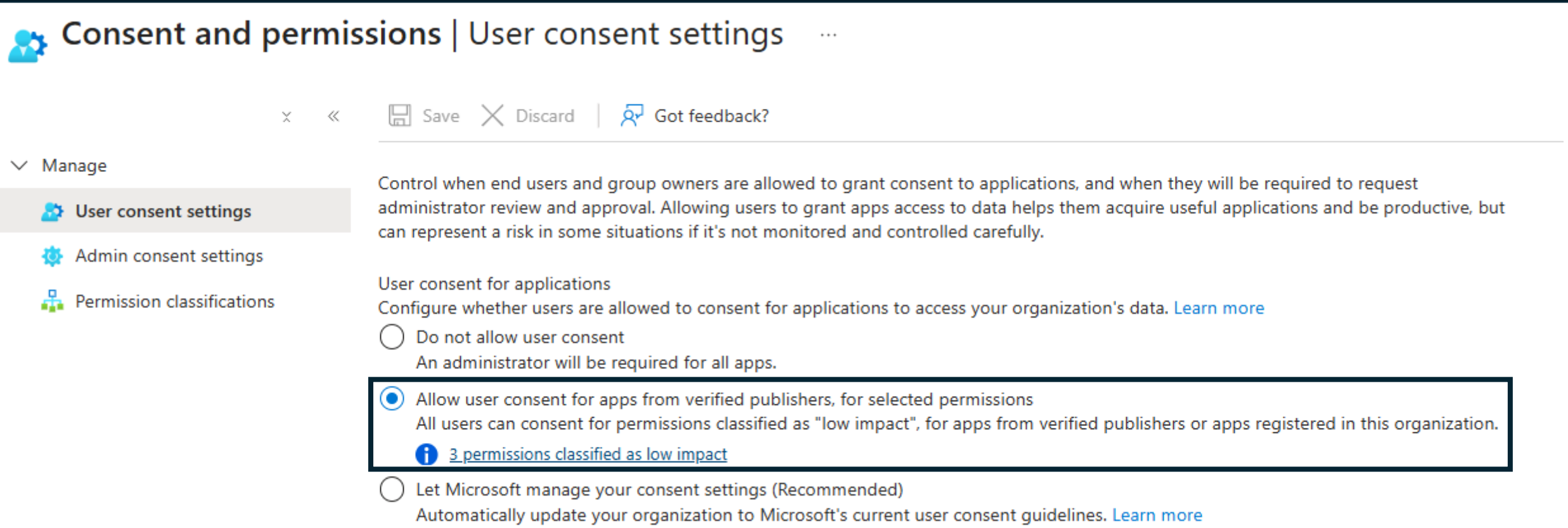
Consent Grant Attack



Consent Grant Attack

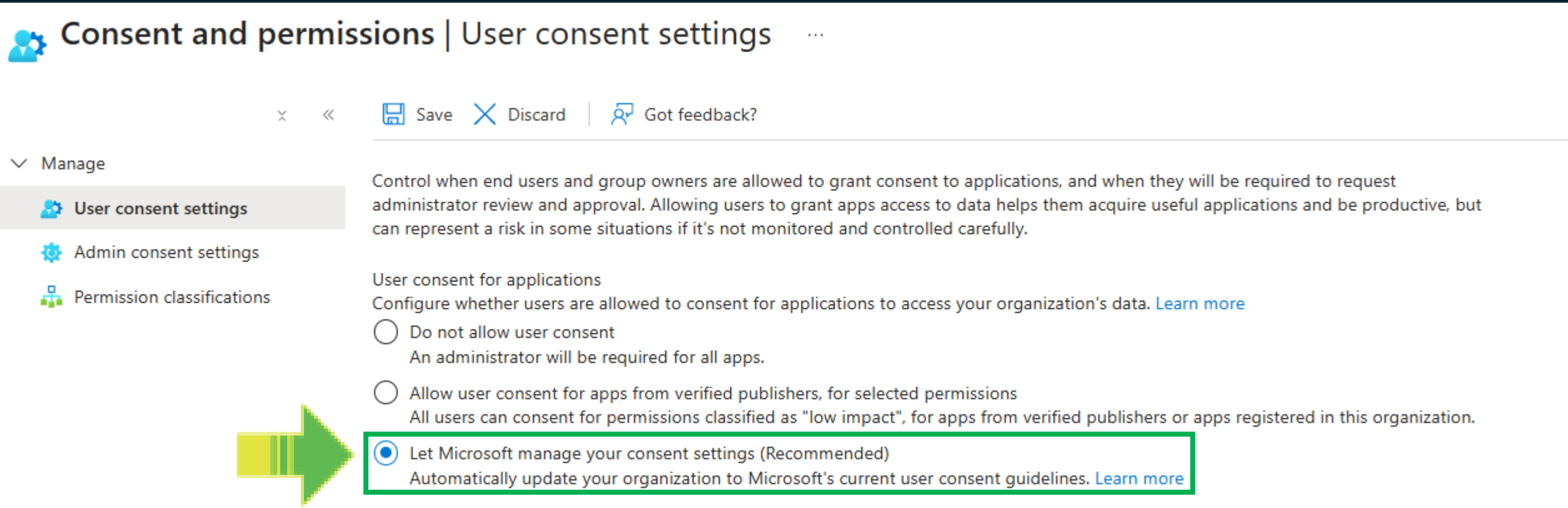


Todays Default



https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings

TrustedSec Recommended Settings



https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings

#4 Secure Entra ID Roles



TRUSTEDSEC

There are >**100** Entra ID Roles!

Administrative roles

Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID not rela

Learn more about Microsoft Entra ID role-based access control

Search by name or description | Add filters

Role	Description	Privileged
Agent ID Administrator	Manage all aspects of agents in a tenant including identity lifecycle operations for agent blueprints, agent service principals, agent identities, and agentic users.	
Agent ID Developer	Create an agent blueprint and its service principal in a tenant. User will be added as an owner of the agent blueprint and its service principal.	
Agent Registry Administrator	Manage all aspects of the Agent Registry service in Microsoft Entra ID	
AI Administrator	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.	
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED
Attack Payload Author	Can create attack payloads that an administrator can	

Microsoft's PRIVILEGED Roles

- Agent ID Administrator
- Application Administrator
- Application Developer
- Attribute Provisioning Administrator
- Attribute Provisioning Reader
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Conditional Access Administrator
- Directory Writers
- Domain Name Administrator
- External Identity Provider Administrator
- Global Administrator
- Global Reader
- Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator
- Lifecycle Workflows Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

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

Microsoft's PRIVILEGED Roles

- Agent ID Administrator
- Security Defaults Application Administrator
- Application Developer
- Attribute Provisioning Administrator
- Attribute Provisioning Reader
- Security Defaults Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Security Defaults Cloud Application Administrator
- Cloud Device Administrator
- Security Defaults Conditional Access Administrator
- Directory Writers
- Domain Name Administrator
- External Identity Provider Administrator
- Security Defaults Global Administrator
- Global Reader
- Security Defaults Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator
- Lifecycle Workflows Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- Security Defaults Password Administrator
- Security Defaults Privileged Authentication Administrator
- Security Defaults Privileged Role Administrator
- Security Defaults Security Administrator
- Security Operator
- Security Reader
- Security Defaults User Administrator

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#require-administrators-to-do-multifactor-authentication

Microsoft's PRIVILEGED Roles

- Agent ID Administrator
- Security Defaults Application Administrator
- Application Developer
- Attribute Provisioning Administrator
- Attribute Provisioning Reader
- Security Defaults Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Security Defaults Cloud Application Administrator
- Cloud Device Administrator
- Security Defaults Conditional Access Administrator
- Directory Writers
- Domain Name Administrator
- External Identity Provider Administrator
- Security Defaults Global Administrator
- Global Reader
- Security Defaults Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator
- Lifecycle Workflows Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- Security Defaults Password Administrator
- Security Defaults Privileged Authentication Administrator
- Security Defaults Privileged Role Administrator
- Security Defaults Security Administrator
- Security Operator
- Security Reader
- Security Defaults User Administrator
- Security Defaults Authentication Policy Administrator
- Security Defaults Billing Administrator
- Security Defaults Exchange Administrator
- Security Defaults Identity Governance Administrator
- Security Defaults SharePoint Administrator

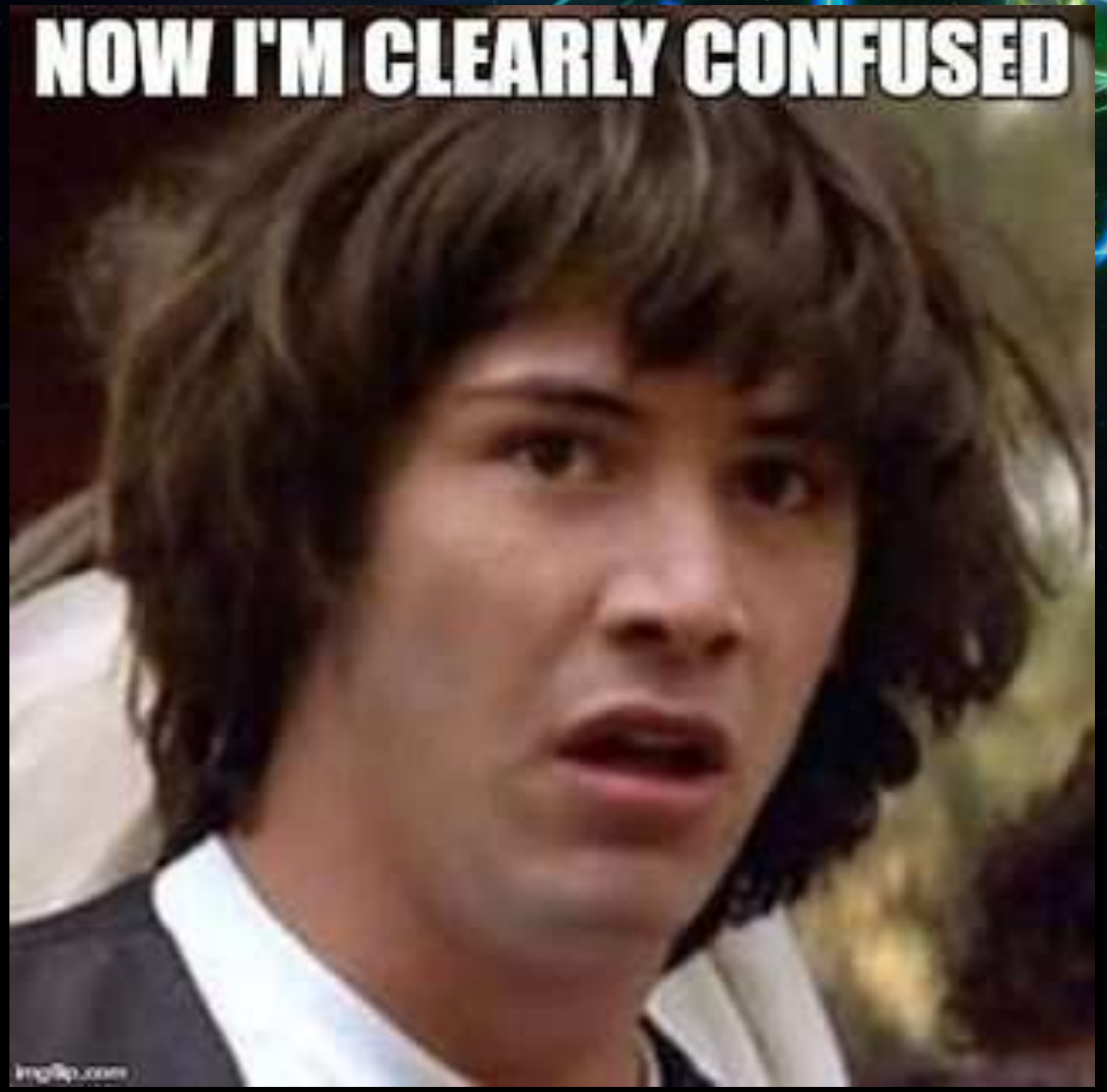
https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#require-administrators-to-do-multifactor-authentication

Microsoft's PRIVILEGED Roles

- Agent ID Administrator
- Application Administrator
- Application Developer
- Attribute Provisioning Administrator
- Attribute Provisioning Reader
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Conditional Access Administrator
- Directory Writers
- Domain Name Administrator
- External Identity Provider Administrator
- Global Administrator
- Global Reader
- Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator
- Lifecycle Workflows Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

- Authentication Policy Administrator
- Billing Administrator
- Exchange Administrator
- Identity Governance Administrator
- SharePoint Administrator

https://learn.microsoft.com/en-us/entra/identity/conditional-access/managed-policies#what-administrator-roles-are-covered-by-these-policies


NOW I'M CLEARLY CONFUSED

TrustedSec's Entra ID Tier 0 List (9)

- Application Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Global Administrator
- Hybrid Identity Administrator
- Partner Tier2 Support
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator

https://trustedsec.com/blog/managing-privileged-roles-in-microsoft-entra-id-a-pragmatic-approach

TrustedSec's Entra ID Tier 1 List (37)

- AI Administrator
- Attribute Assignment Administrator
- Attribute Provisioning Administrator
- Authentication Administrator
- Authentication Extensibility Administrator
- Authentication Policy Administrator
- B2C IEF Keyset Administrator
- Cloud App Security Administrator
- Compliance Administrator
- Directory Synchronization Accounts
- Directory Writers
- Domain Name Administrator
- Dynamics 365 Administrator
- Exchange Administrator
- External ID User Flow Administrator
- External Identity Provider Administrator
- Global Secure Access Administrator
- Groups Administrator
- Helpdesk Administrator
- Identity Governance Administrator
- Intune Administrator
- Knowledge Administrator
- Lifecycle Workflows Administrator
- Microsoft 365 Backup Administrator
- Microsoft 365 Migration Administrator
- On Premises Directory Sync Account
- Partner Tier1 Support
- Password Administrator
- Power Platform Administrator
- Security Operator
- SharePoint Administrator
- Skype for Business Administrator
- Teams Administrator
- Teams Telephony Administrator
- User Administrator
- Windows 365 Administrator
- Yammer Administrator

https://trustedsec.com/blog/managing-privileged-roles-in-microsoft-entra-id-a-pragmatic-approach

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

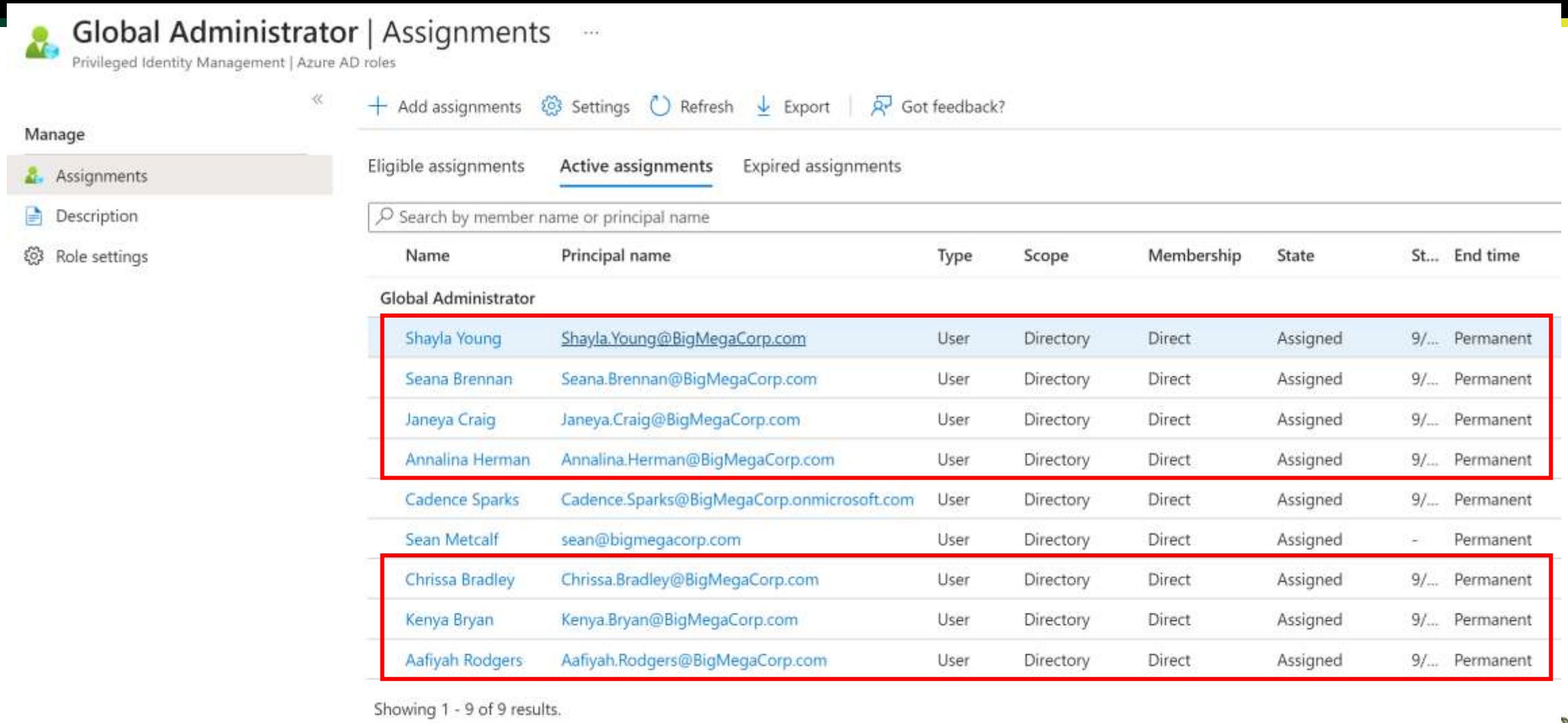


#5 Secure Privileged Role Membership

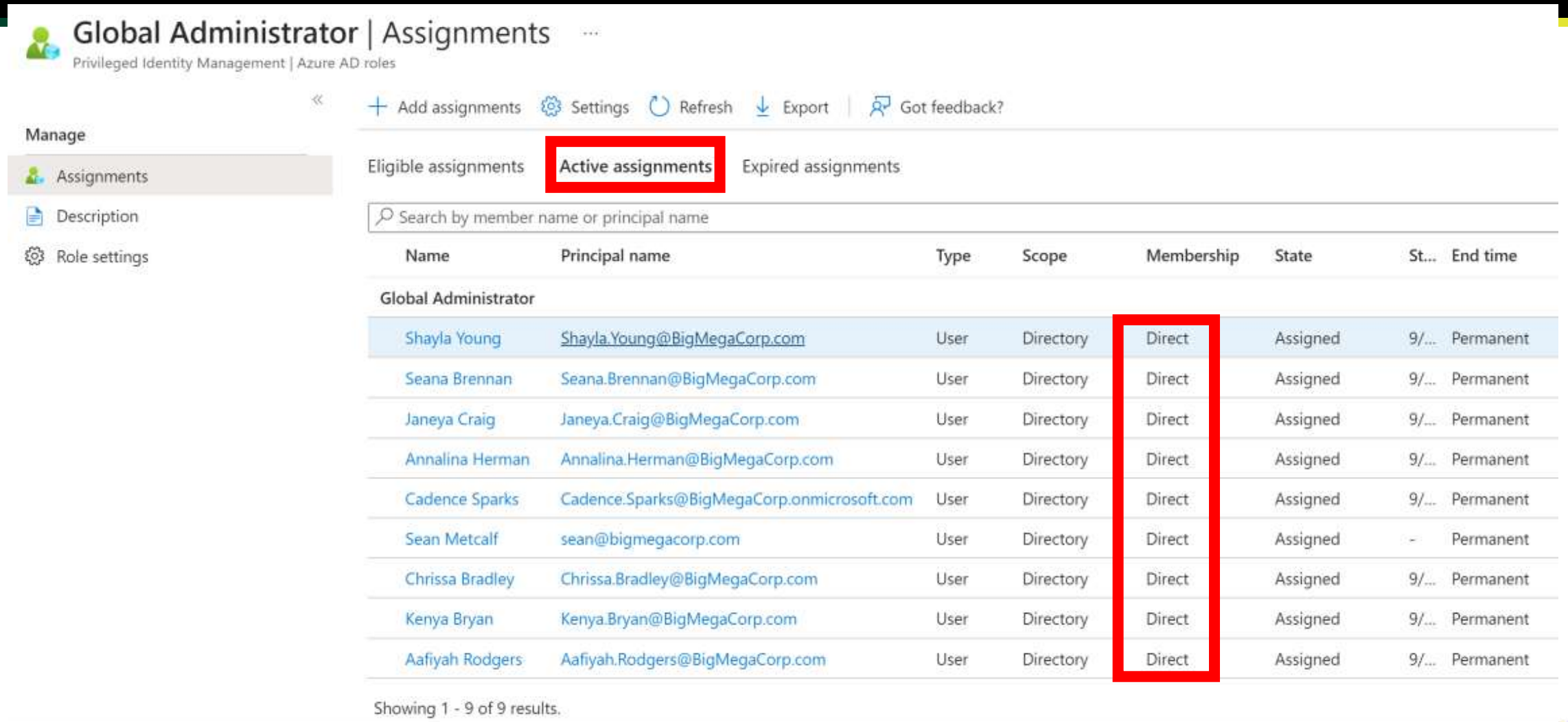


THE FUTURE IS TRUSTED SEC
SMILEYCON 2026

Highly Privileged Standard User Accounts



PIM Members are Active, Not Eligible



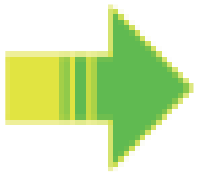
Tier 0 Admin Accounts without MFA

UserDisplayName	UserUPN	MFAPhoneNumber	MFAPhoneType	MFAEmailAddress	MFADeviceDisplayName	MFADeviceTag	MFAPhoneAppVersion	MFASoftwareOathAuthentication	LastPasswordChangeDate
Aabid Rodriguez	Aabid.Rodriguez@BigMegaCorp.com								11/17/2019 11:16:00 PM
Aabidah Nichols	Aabidah.Nichols@BigMegaCorp.com								11/18/2019 1:04:53 AM
Aabir Knapp	Aabir.Knapp@BigMegaCorp.com								11/17/2019 11:15:43 PM
Aadit White	Aadit.White@BigMegaCorp.com								12/5/2019 5:55:55 AM
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com								11/20/2019 11:01:27 PM
Aafiyah Zamora	Aafiyah.Zamora@BigMegaCorp.com								11/17/2019 9:46:55 PM
Aagam Marshall	Aagam.Marshall@BigMegaCorp.com								
Annalina Herman	Annalina.Herman@BigMegaCorp.com								11/17/2019 10:38:11 PM
BigMegaAdmin1	BigMegaAdmin1@bigmegacorp.com								9/18/2023 6:28:52 PM
Brandon Colley	brandon@BigMegaCorp.onmicrosoft.com	+1 [redacted]	mobile		Pixel 6	SoftwareTokenActivated	6.2407.5108		8/1/2024 8:18:32 PM
Cadence Mclean	Cadence.Mclean@BigMegaCorp.com								12/4/2019 8:06:01 PM
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	+1 [redacted]	mobile					SoftwareOathAuthentication	2/6/2026 8:09:09 PM
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com								11/17/2019 11:35:35 PM
Dane Pineda	Dane.Pineda@BigMegaCorp.com								12/5/2019 2:08:43 AM
Dirk Lester	Dirk.Lester@BigMegaCorp.com								12/4/2019 8:42:14 PM
Janeya Craig	Janeya.Craig@BigMegaCorp.com								11/17/2019 10:01:11 PM
Jason Crawford	jasonc@bigmegacorp.com	+1 [redacted]	mobile		iPhone 14 Pro	SoftwareTokenActivated	6.7.12		8/2/2023 3:39:57 PM
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com								11/17/2019 9:59:41 PM
Rachelle Powers	Rachelle.Powers@BigMegaCorp.com								11/20/2019 8:47:37 PM
Sean Metcalf	sean@bigmegacorp.com	+1 [redacted]	mobile	sean@adsecurity.org	iPhone 16 Pro	SoftwareTokenActivated	6.8.40		10/8/2025 4:45:32 PM
Seana Brennan	Seana.Brennan@BigMegaCorp.com								11/17/2019 10:50:13 PM
Shayla Young	Shayla.Young@BigMegaCorp.com								11/18/2019 1:28:22 AM
Stela Noble	Stela.Noble@BigMegaCorp.onmicrosoft.com								11/16/2019 7:27:44 AM
SVC-GA_App	SVC-GA_App@bigmegacorp.com								1/21/2024 10:27:20 PM
Trimarc MCSA	TrimarcMCSA@bigmegacorp.com	+1 [redacted]	office	sean@adsecurity.org	iPhone	SoftwareTokenActivated	6.8.39		5/30/2022 2:39:16 AM
Tyrek Miller	Tyrek.Miller@BigMegaCorp.com								12/5/2019 2:18:34 AM
Wilson Merritt	Wilson.Merritt@BigMegaCorp.com								12/5/2019 2:12:49 AM
Yasmine Briggs	Yasmine.Briggs@BigMegaCorp.com								11/17/2019 11:00:59 PM

Get-EntraUserMFAConfig.ps1

https://github.com/PyroTek3/EntraID

Tier 0 Admin Accounts without MFA



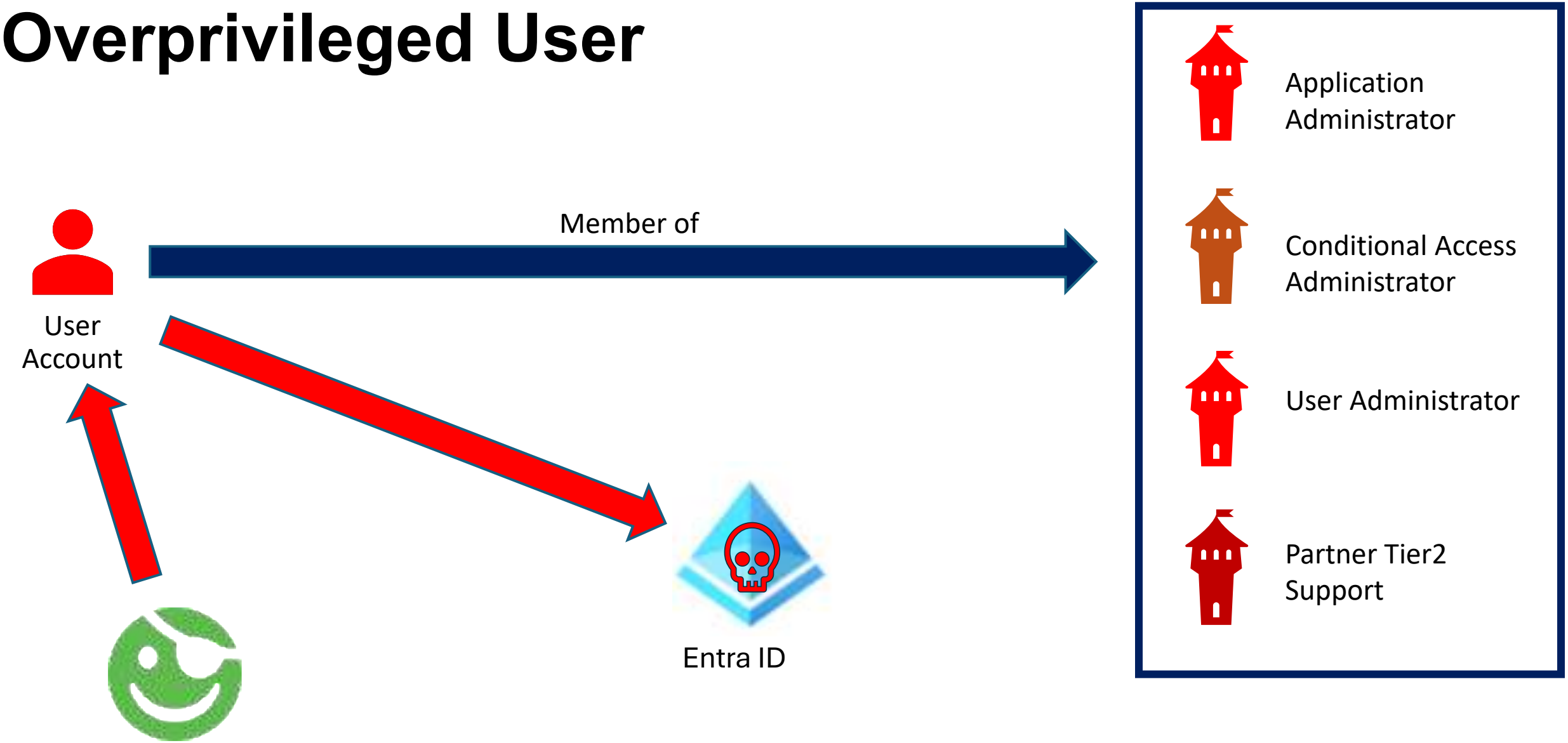
```
Total Tier 0 Admins: 31
  Admins with No MFA: 26
  Admins with Phone Number (Mobile): 4
  SMS is disabled
  Total Admins with Microsoft Authenticator App: 4
  Total Admins with a different Authenticator app: 1

26 Admins with No MFA Configured:
 * Aabid Rodriguez (Aabid.Rodriguez@BigMegaCorp.com)
 * Aabidah Nichols (Aabidah.Nichols@BigMegaCorp.com)
 * Aabir Knapp (Aabir.Knapp@BigMegaCorp.com)
 * Aadit White (Aadit.White@BigMegaCorp.com)
 * Aafiyah Rodgers (Aafiyah.Rodgers@BigMegaCorp.com)
 * Aafiyah Zamora (Aafiyah.Zamora@BigMegaCorp.com)
 * Aagam Marshall (Aagam.Marshall@BigMegaCorp.com)
 * Annalina Herman (Annalina.Herman@BigMegaCorp.com)
 * BigMegaAdmin1 (BigMegaAdmin1@bigmegacorp.com)
 * Cadence Mclean (Cadence.Mclean@BigMegaCorp.com)
 * Chrissa Bradley (Chrissa.Bradley@BigMegaCorp.com)
 * Dane Pineda (Dane.Pineda@BigMegaCorp.com)
 * Dirk Lester (Dirk.Lester@BigMegaCorp.com)
 * Janeya Craig (Janeya.Craig@BigMegaCorp.com)
 * Kenya Bryan (Kenya.Bryan@BigMegaCorp.com)
 * Rachelle Powers (Rachelle.Powers@BigMegaCorp.com)
 * Seana Brennan (Seana.Brennan@BigMegaCorp.com)
 * Shayla Young (Shayla.Young@BigMegaCorp.com)
 * Stela Noble (Stela.Noble@BigMegaCorp.onmicrosoft.com)
 * SVC-GA_App (SVC-GA_App@bigmegacorp.com)
 * Tyrek Miller (Tyrek.Miller@BigMegaCorp.com)
 * Wilson Merritt (Wilson.Merritt@BigMegaCorp.com)
 * Yasmine Briggs (Yasmine.Briggs@BigMegaCorp.com)
```

Get-EntraUserMFAConfig.ps1

https://github.com/PyroTek3/EntraID

Overprivileged User



There's an app (PowerShell) for Tier 0 & 1 Roles!

Current Active Tier 0 Role Membership:

MemberOfRole	accountEnabled	ObjectType	DisplayName	UserPrincipalName	Synced	MemberOfGroup
Application Administrator	True	User	Aabir Knapp	Aabir.Knapp@BigMegaCorp.com	False	BigMegaCorp Application Administrators
Application Administrator	True	User	Aabidah Nichols	Aabidah.Nichols@BigMegaCorp.com	False	BigMegaCorp Application Administrators
Application Administrator	True	User	Rachelle Powers	Rachelle.Powers@BigMegaCorp.com	False	
Application Administrator		Group	BigMegaCorp Application Administrators			
Cloud Application Administrator	True	User	Aadish Lloyd	Aadish.Lloyd@BigMegaCorp.com	False	BMC - RG - Cloud Application Administrator
Cloud Application Administrator	True	User	Aadit Daniel	Aadit.Daniel@BigMegaCorp.com	False	BMC - RG - Cloud Application Administrator
Cloud Application Administrator		Group	BMC - RG - Cloud Application Administrator			
Cloud Application Administrator	True	User	Aadit Roach	Aadit.Roach@BigMegaCorp.onmicrosoft.com	False	BMC - RG - Cloud Application Administrator
Conditional Access Administrator	True	User	Yasmine Briggs	Yasmine.Briggs@BigMegaCorp.com	False	
Conditional Access Administrator	True	User	Stela Noble	Stela.Noble@BigMegaCorp.onmicrosoft.com	False	
Global Administrator	True	User	Dane Pineda	Dane.Pineda@BigMegaCorp.com	False	BigMegaCorp Global Admins
Global Administrator	True	User	Wilson Merritt	Wilson.Merritt@BigMegaCorp.com	False	BigMegaCorp Global Admins
Global Administrator	True	User	Cadence Mclean	Cadence.Mclean@BigMegaCorp.com	False	BigMegaCorp Global Admins
Global Administrator	True	User	Dirk Lester	Dirk.Lester@BigMegaCorp.com	False	BigMegaCorp Global Admins
Global Administrator	True	User	Tyrek Miller	Tyrek.Miller@BigMegaCorp.com	False	BigMegaCorp Global Admins
Global Administrator	True	User	Brandon Colley	brandon@BigMegaCorp.onmicrosoft.com	False	
Global Administrator	True	User	KC Shaw	KCShaw@bigmegacorp.com	False	
Global Administrator	True	User	Aadit White	Aadit.White@BigMegaCorp.com	False	BigMegaCorp Global Admins
Global Administrator	True	User	SVC-GA_App	SVC-GA_App@bigmegacorp.com	False	
Global Administrator	True	User	Janeya Craig	Janeya.Craig@BigMegaCorp.com	False	
Global Administrator	True	User	Annalina Herman	Annalina.Herman@BigMegaCorp.com	False	
Global Administrator	True	User	Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	False	
Global Administrator	True	User	Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	False	
Global Administrator	True	User	Seana Brennan	Seana.Brennan@BigMegaCorp.com	False	
Global Administrator	True	User	BigMegaAdmin1	BigMegaAdmin1@bigmegacorp.com	False	
Global Administrator		Group	BigMegaCorp Global Admins			
Global Administrator	True	User	Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	False	
Global Administrator	True	User	Shayla Young	Shayla.Young@BigMegaCorp.com	False	
Hybrid Identity Administrator	True	User	Aabidah Nichols	Aabidah.Nichols@BigMegaCorp.com	False	
Hybrid Identity Administrator	True	User	Aabir Knapp	Aabir.Knapp@BigMegaCorp.com	False	
Privileged Authentication Administrator		Group	BigMegaCorp Application Administrators			
Privileged Authentication Administrator	True	User	Aabir Knapp	Aabir.Knapp@BigMegaCorp.com	False	BigMegaCorp Application Administrators
Privileged Authentication Administrator	True	User	Aabidah Nichols	Aabidah.Nichols@BigMegaCorp.com	False	BigMegaCorp Application Administrators
Privileged Authentication Administrator	True	User	Aafiyah Zamora	Aafiyah.Zamora@BigMegaCorp.com	False	
Privileged Authentication Administrator	True	User	Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	False	
Privileged Authentication Administrator	True	User	Aagam Marshall	Aagam.Marshall@BigMegaCorp.com	False	
Privileged Role Administrator	True	User	Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	False	
Security Administrator		Group	BMC - RG - Security Administrator			
Security Administrator	True	User	Aabid Rodriguez	Aabid.Rodriguez@BigMegaCorp.com	False	BMC - RG - Security Administrator
Security Administrator	True	User	Trimarc MCSA	TrimarcMCSA@bigmegacorp.com	False	
Security Administrator	True	User	Sean Metcalf	sean@bigmegacorp.com	False	
Security Administrator	True	User	Jason Crawford	jasonc@bigmegacorp.com	False	

There’s an app (PowerShell) for Tier 0 & 1 Roles!

```
Current Active Tier 1 Role Membership:

MemberOfRole            accountEnabled ObjectType DisplayName                    UserPrincipalName                          Synced MemberOfGroup
------------            -------------- ---------- -----------                    -----------------                          ------ -------------
Exchange Administrator            True User       Aabir Knapp                    Aabir.Knapp@BigMegaCorp.com                 False BMC - RG - Exchange Administrator
Exchange Administrator            True User       Aabriella Cortez               Aabriella.Cortez@BigMegaCorp.onmicrosoft.com False BMC - RG - Exchange Administrator
Exchange Administrator                 Group      BMC - RG - Exchange Administrator
Helpdesk Administrator            True User       Aabid Friedman                 Aabid.Friedman@BigMegaCorp.com              False BMC - RG - Helpdesk Administrator
Helpdesk Administrator            True User       Aabid Hanna                    Aabid.Hanna@BigMegaCorp.com                 False BMC - RG - Helpdesk Administrator
Helpdesk Administrator            True User       Aaban Williams                 Aaban.Williams@BigMegaCorp.com              False BMC - RG - Helpdesk Administrator
Helpdesk Administrator                 Group      BMC - RG - Helpdesk Administrator
Helpdesk Administrator            True User       Aabid Pope                     Aabid.Pope@BigMegaCorp.com                  False BMC - RG - Helpdesk Administrator
Intune Administrator              True User       Bobby Mccoy                    Bobby.Mccoy@BigMegaCorp.com                 False
SharePoint Administrator          True User       Aaban Williams                 Aaban.Williams@BigMegaCorp.com              False BMC - RG - SharePoint Administrator
SharePoint Administrator          True User       Aabid Hanna                    Aabid.Hanna@BigMegaCorp.com                 False BMC - RG - SharePoint Administrator
SharePoint Administrator          True User       Aabidah Nichols                Aabidah.Nichols@BigMegaCorp.com             False BMC - RG - SharePoint Administrator
SharePoint Administrator          True User       Aabid Rodriguez                Aabid.Rodriguez@BigMegaCorp.com             False BMC - RG - SharePoint Administrator
SharePoint Administrator               Group      BMC - RG - SharePoint Administrator
SharePoint Administrator          True User       Aabir Harvey                   Aabir.Harvey@BigMegaCorp.com                False BMC - RG - SharePoint Administrator
SharePoint Administrator          True User       Aabir Petersen                 Aabir.Petersen@BigMegaCorp.com              False BMC - RG - SharePoint Administrator
User Administrator                True User       Aafiya Cardenas                Aafiya.Cardenas@BigMegaCorp.com             False BMC - RG - User Administrator
User Administrator                True User       Aagam Rodriguez                Aagam.Rodriguez@BigMegaCorp.com             False BMC - RG - User Administrator
User Administrator                True User       Aagam Marshall                 Aagam.Marshall@BigMegaCorp.com              False BMC - RG - User Administrator
User Administrator                True User       Aafiyah Rodgers                Aafiyah.Rodgers@BigMegaCorp.com             False BMC - RG - User Administrator
User Administrator                True User       Aadyn Strickland               Aadyn.Strickland@BigMegaCorp.onmicrosoft.com False BMC - RG - User Administrator
User Administrator                     Group      BMC - RG - User Administrator
User Administrator                True User       Aafiya Weber                   Aafiya.Weber@BigMegaCorp.com                False BMC - RG - User Administrator
User Administrator                True User       Aafiyah Zamora                 Aafiyah.Zamora@BigMegaCorp.com              False BMC - RG - User Administrator
```

Get-EntraIDAdmins.ps1

https://github.com/PyroTek3/EntraID

#6 Secure Role Assignable Groups

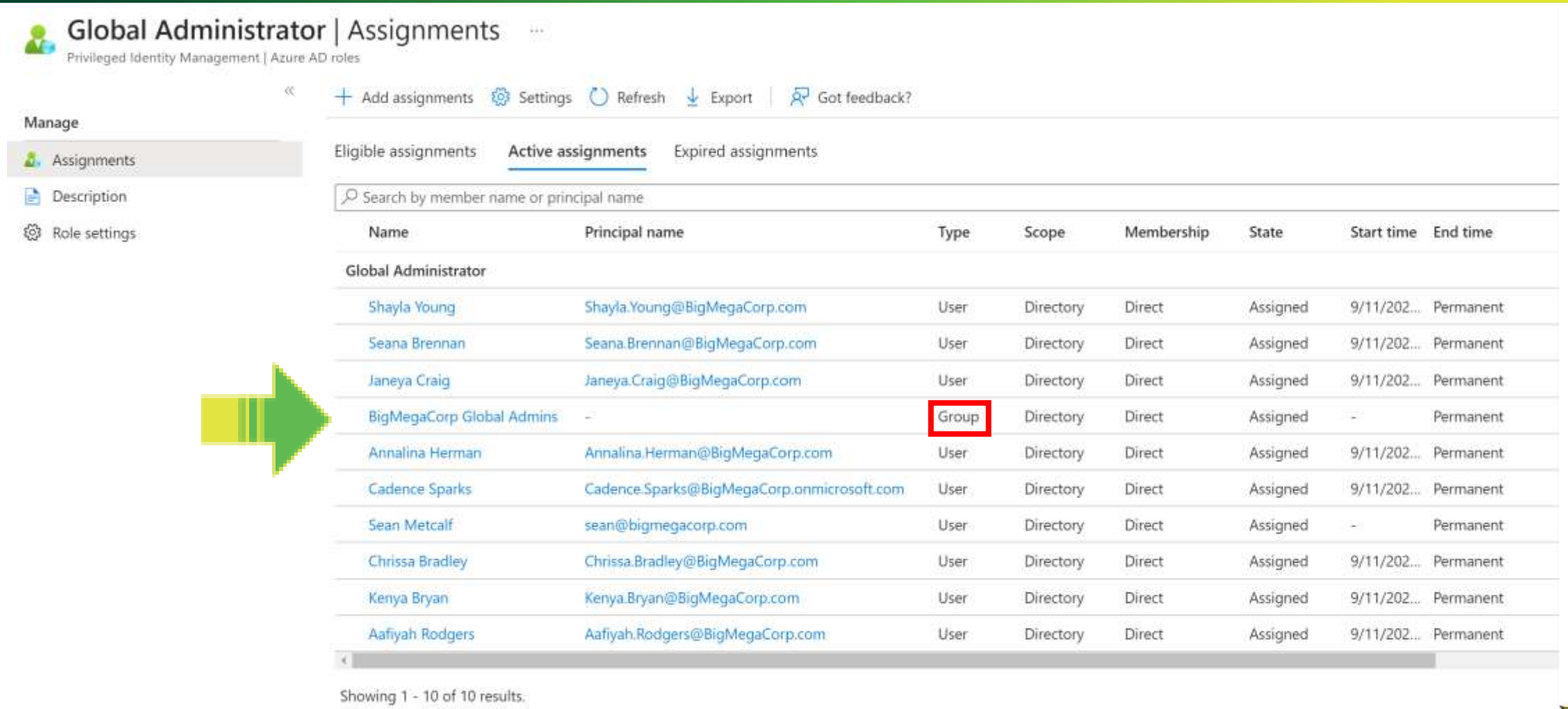


Role Assignable Groups (RAGs)

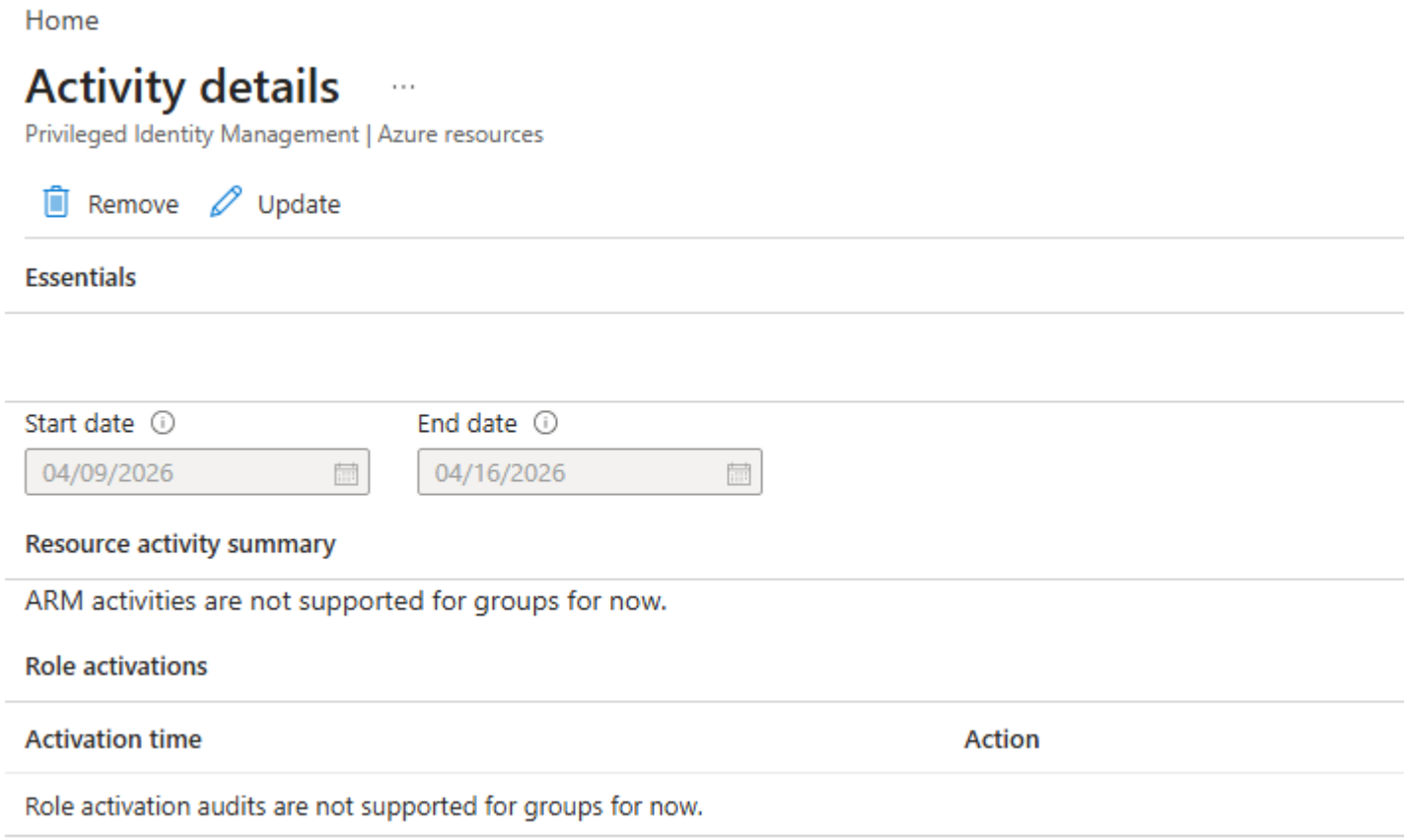
- Role Assignable Groups are Security or Microsoft 365 group with the isAssignableToRole property set to true and cannot be dynamic.
- Created to solve the potential issue where groups are added to an Entra ID role and a group admin could modify membership.
- Only Global Administrators or Privileged 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.

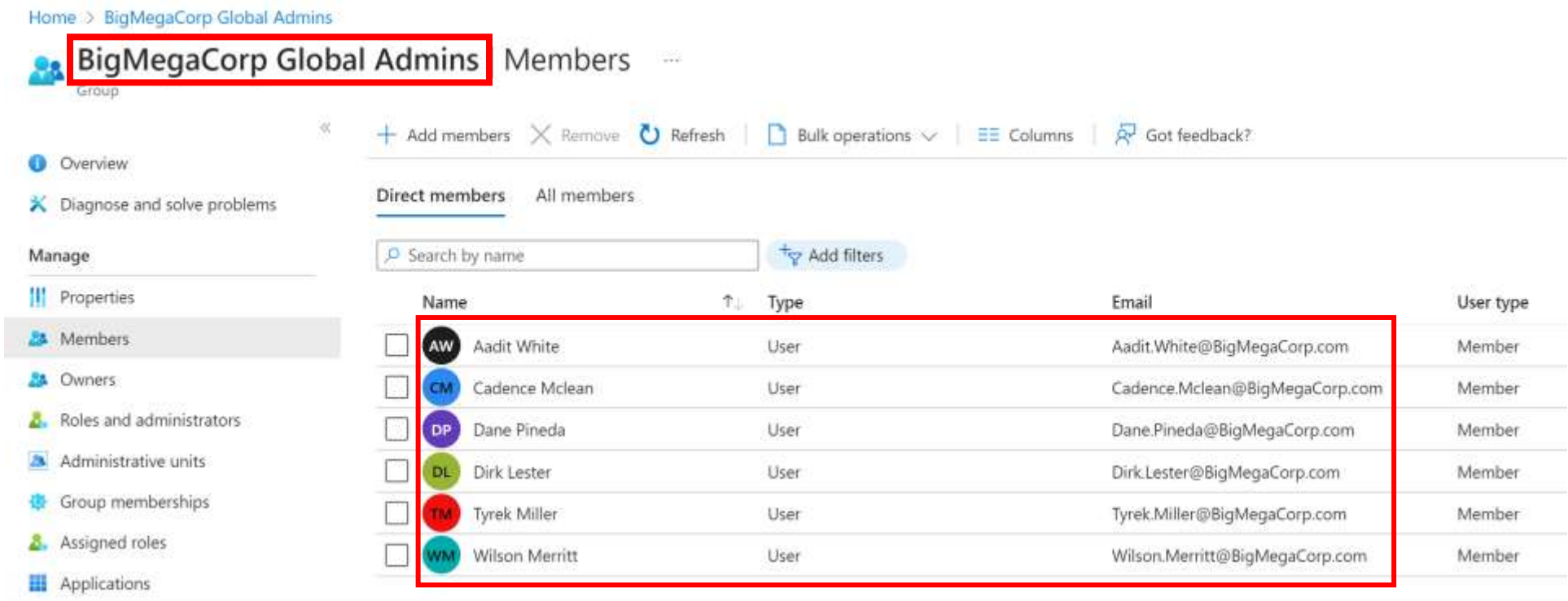
Privileged Roles with Group Nesting



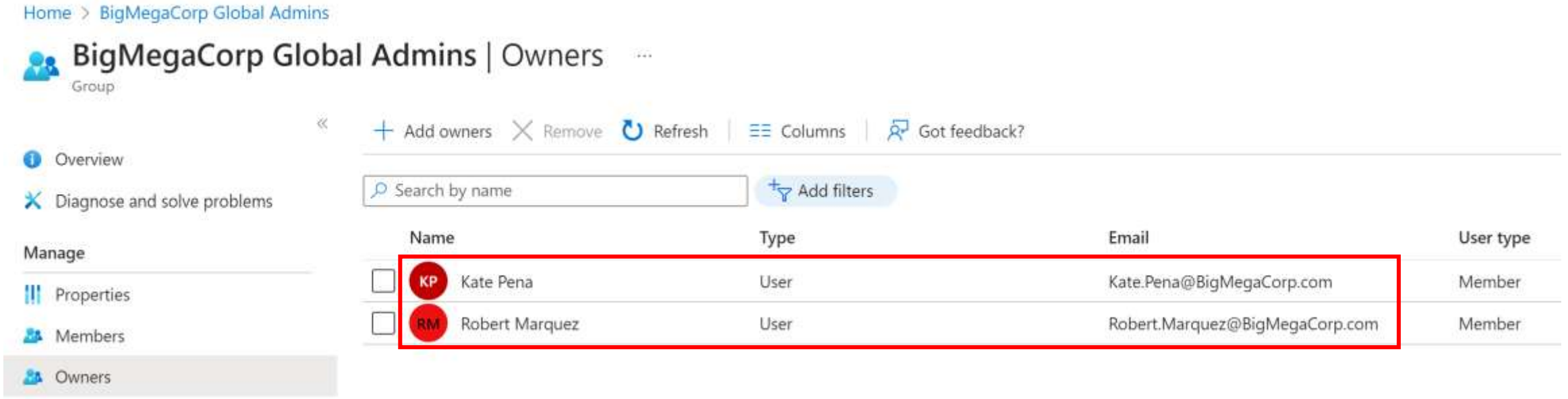
Privileged Roles with Group Nesting



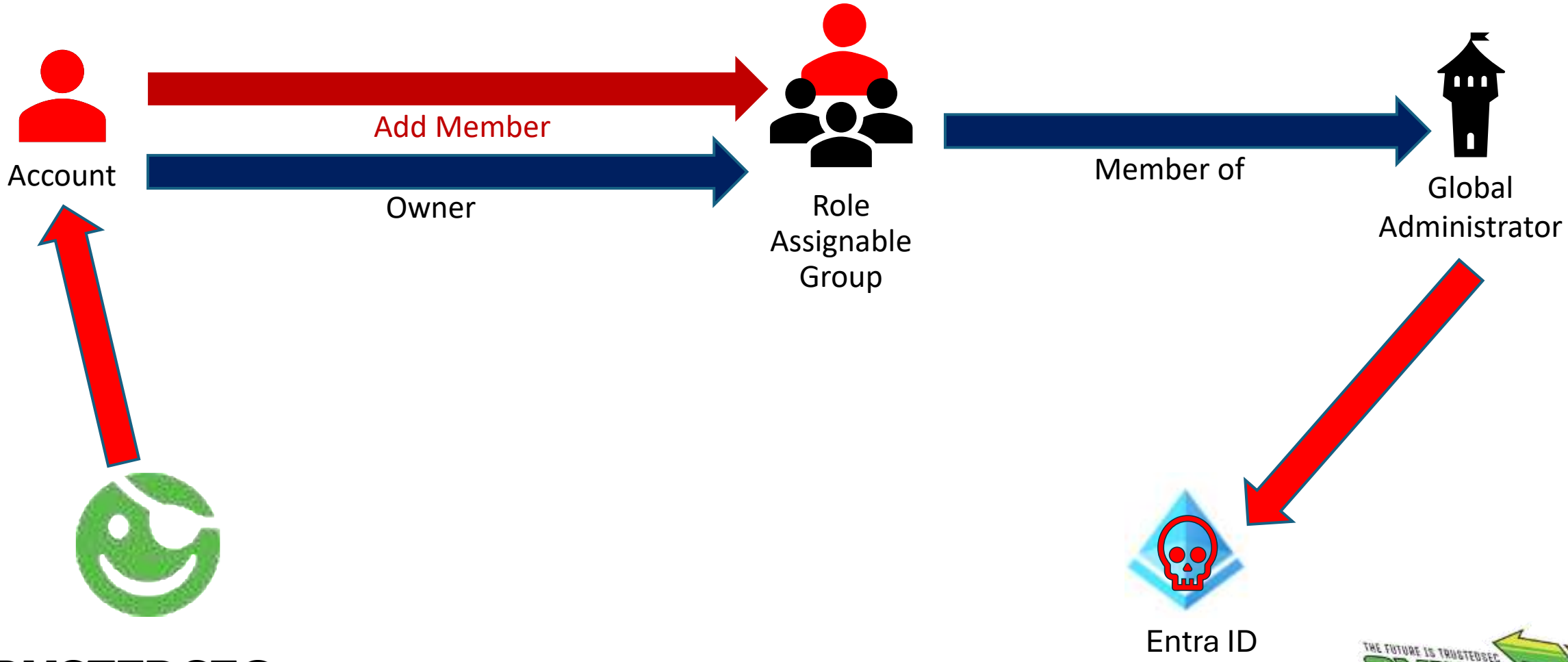
Group Nesting – Have to Open Groups



Role Assignable Group Owners



Compromise Azure AD through Role Assignable Group Owner Rights



There’s an app (PowerShell) for that!

```
Tier 0 Role Assignable Group Owners:

OwnerDisplayName OwnerUPN                                RoleAssignableGroup                    MemberOfRole                          O
---------------- --------                                -------------------                    ------------                          -
Judy Flynn       Judy.Flynn@BigMegaCorp.com              BigMegaCorp Application Administrators Application Administrator             2
Kate Pena        Kate.Pena@BigMegaCorp.com               BigMegaCorp Global Admins              Global Administrator                  e
Robert Marquez   Robert.Marquez@BigMegaCorp.com          BigMegaCorp Global Admins              Global Administrator                  2
Judy Flynn       Judy.Flynn@BigMegaCorp.com              BigMegaCorp Application Administrators Privileged Authentication Administrator 2
Aadhi Haynes     Aadhi.Haynes@BigMegaCorp.onmicrosoft.com BMC - RG - Security Administrator     Security Administrator                d


PIM Eligible Tier 0 Roles:

RoleName            PrincipalObjectType PrincipalDisplayName Status   MemberOfGroup StartDateTime         EndDateTime
--------            ------------------- --------------------- ------   ------------- -------------         -----------
Global Administrator User                Bridgette Ramos       Eligible                1/26/2026 8:04:00 PM
Global Administrator User                Daney Bond            Eligible Global Admins
Global Administrator User                Diana Fletcher        Eligible                1/26/2026 8:12:40 PM
Global Administrator Group               Global Admins         Eligible                1/26/2026 10:10:20 PM
Global Administrator User                Sam Kane              Eligible                1/26/2026 8:05:36 PM  12/31/2026 8:04:03 PM
```

Get-EntraIDAdmins.ps1

https://github.com/PyroTek3/EntraID



#7 Secure Highly Privileged Applications

Permissions Structure

OBJECT . ACCESS . CONSTRAINT

Examples:

Application.ReadWrite.All

Calendars.ReadWrite

Directory.ReadWrite.All

Mail.ReadWrite

Mail.Send

Policy.Read.ConditionalAccess

User.ReadWrite.All

Tier 0 Application Permissions

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

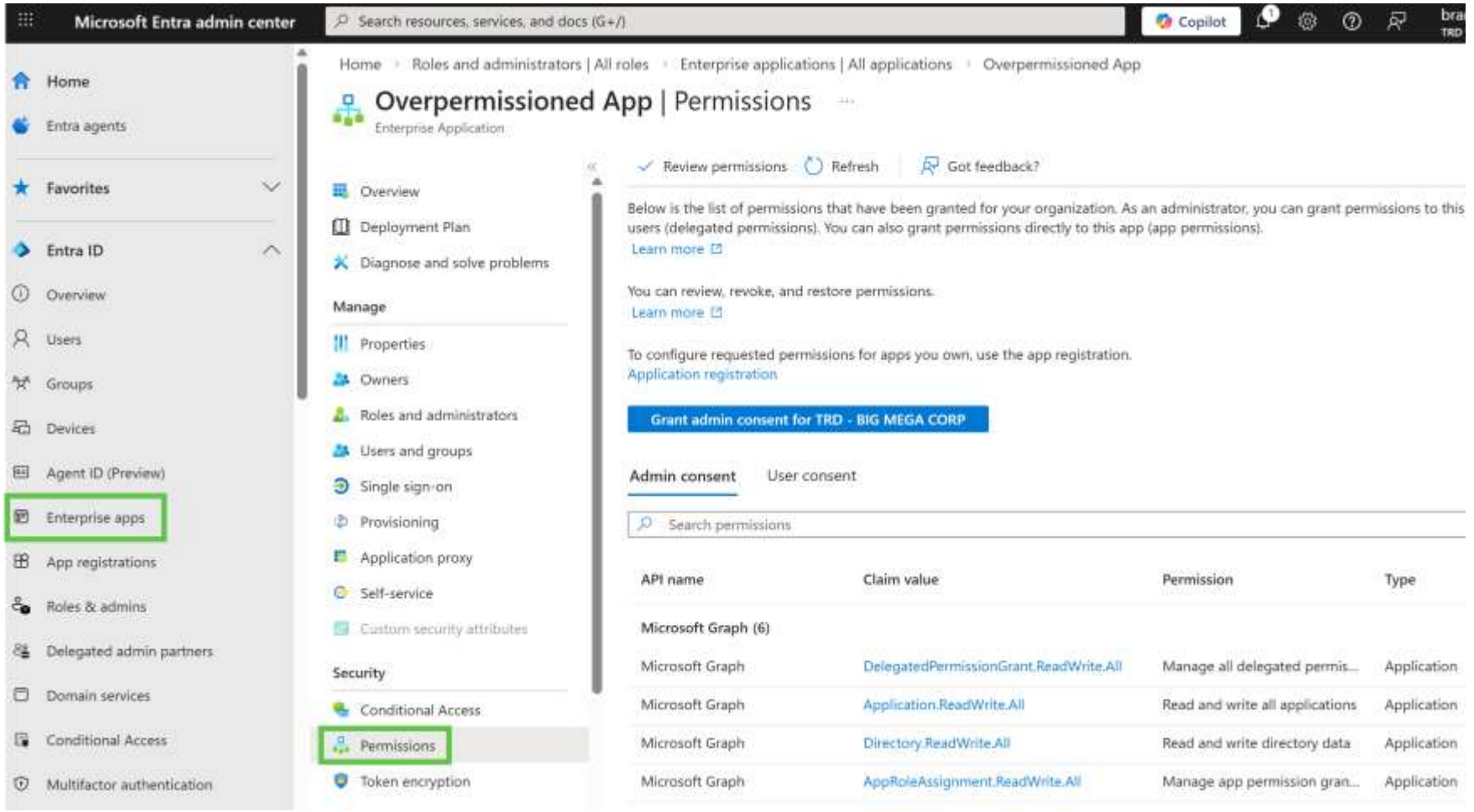
Directory.ReadWrite.All	• “Directory.ReadWrite.All grants access that is broadly equivalent to a global tenant admin.” *
AppRoleAssignment.ReadWrite.All	• Allows the app to manage permission grants for application permissions to any API & application assignments for any app, on behalf of the signed-in 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.

TRUSTEDSEC

**There is published info that this is not entirely true, but Microsoft says it is.*

THE FUTURE IS TRUSTEDSEC SMILEYCON 2026

Application Permissions



Application Permissions

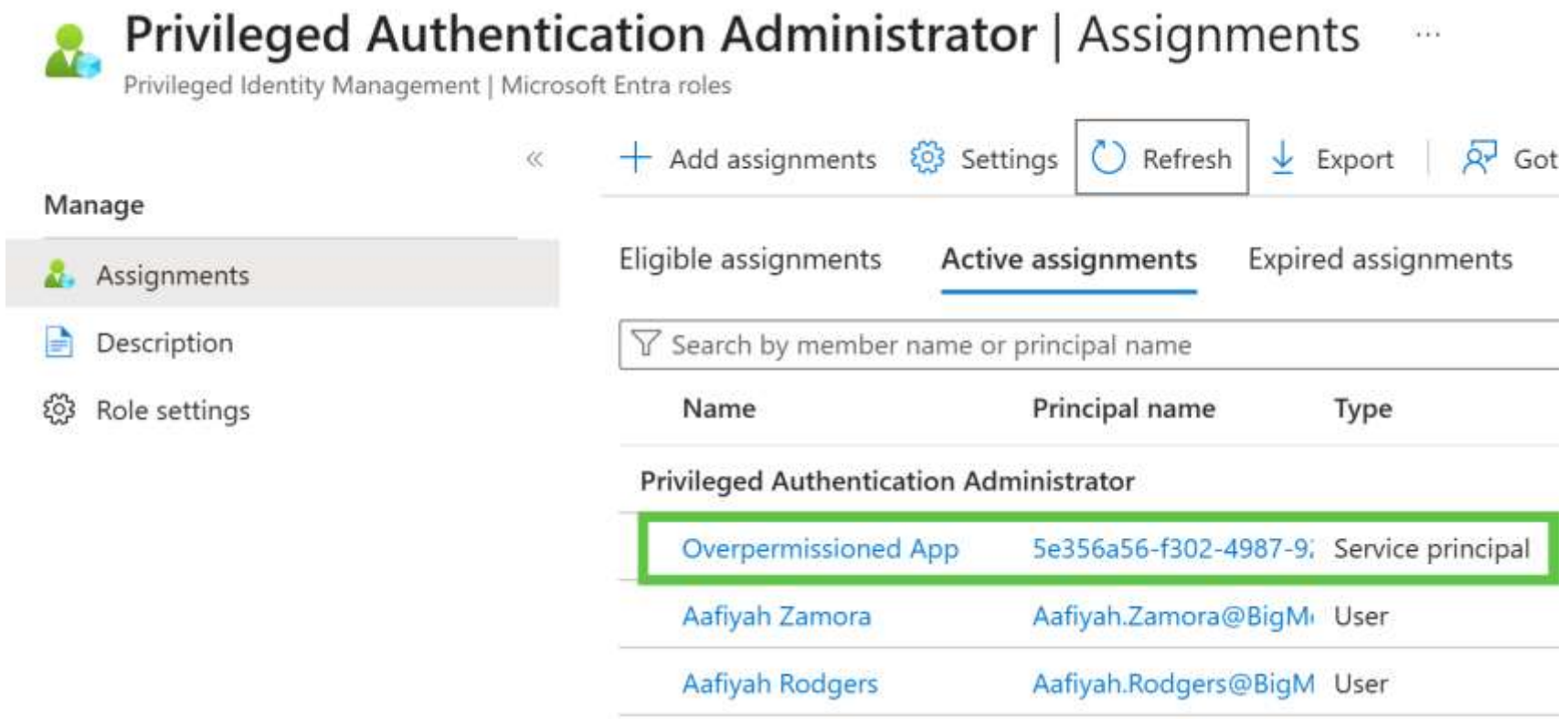
```
Applications with Tier 0 Application Permissions:

AppName                                                 AppPermission
-------                                                 -------------
AAD-Persist                                             AppRoleAssignment.ReadWrite.All
AAD-Persist                                             Directory.ReadWrite.All
ConnectSyncProvisioning_BMCSYNC01_7b13c2e401c6          ADSynchronization.ReadWrite.All
Lots 'o Privs!                                          DelegatedPermissionGrant.ReadWrite.All
Lots 'o Privs!                                          Directory.ReadWrite.All
Overpermissioned App                                    Application.ReadWrite.All
Overpermissioned App                                    AppRoleAssignment.ReadWrite.All
Overpermissioned App                                    DelegatedPermissionGrant.ReadWrite.All
Overpermissioned App                                    Directory.ReadWrite.All
Overpermissioned App                                    RoleManagement.ReadWrite.Directory
Test Privileged L0 App                                  AppRoleAssignment.ReadWrite.All
Test Privileged L0 App                                  RoleManagement.ReadWrite.Directory
Test Privileged L0 App                                  RoleManagement.ReadWrite.Exchange
Test Privileged L0 App                                  RoleManagementPolicy.ReadWrite.Directory
```

Get-EntraIDAppPermissions.ps1

https://github.com/PyroTek3/EntraID

Applications in Privileged Roles



Applications in Privileged Roles

```
PS C:\Users\vagrant> Find-EntraPrivilegedRoleAssignments


Control     : EA-301
Setting     : Service principals assigned to privileged roles
Status      : FINDING
Description : Found 3 assignment(s) to privileged roles
Details     : {@{RoleName=Application Administrator; RoleId=9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3; PrincipalName=BigMegaCorp Application Administrators;
              PrincipalId=7d32a3af-4eff-4914-8dcf-039719300321; PrincipalType=Group; MemberCount=; AssignmentType=GroupMembership; ScopeId=/}, @{RoleName=Global Administrator;
              RoleId=62e90394-69f5-4237-9190-012177145e10; PrincipalName=BigMegaCorp Global Admins; PrincipalId=9f46993a-bdf2-4c79-b9c1-ca59bf1bf5bd; PrincipalType=Group;
              MemberCount=; AssignmentType=GroupMembership; ScopeId=/}, @{RoleName=Cloud Application Administrator; RoleId=158c047a-c907-4556-b7ef-446551a6b5f7; PrincipalName=BMC - RG
              - Cloud Application Administrator; PrincipalId=5b34a4fe-aef0-4533-aad7-d6d59b3aaeea; PrincipalType=Group; MemberCount=; AssignmentType=GroupMembership; ScopeId=/}}
```

https://github.com/techBrandon/Entra-Applications

Application Owners

```
PS C:\Users\vagrant> Get-MgApplication -All -ExpandProperty Owners | Where-Object Owners | Select-Object DisplayName, Owners
Get-MgServicePrincipal -All -ExpandProperty Owners | Where-Object Owners | Select-Object DisplayName, Owners

DisplayName           Owners
-----------           ------
AAD-Persist           {5f78476c-eef1-4284-a8c3-57ee32bdf2e0}
ProofPoint Custom App {70d9a5f5-7190-4452-a743-4f2bede82c06, 7d8afa78-d799-4bdc-8e33-3dff42fbbac3}
BMC Custom App        {9e52b493-140e-45a4-b71d-e9ca27992c9d}
Overpermissioned App  {ab2365a7-24a1-4ac0-9cd0-2d529d759323, 70d9a5f5-7190-4452-a743-4f2bede82c06, 7d8afa78-d799-4bdc-8e33-3dff42fbbac3}
Overpermissioned App  {7f194050-68fe-47d3-a111-5a898ffe7849, 4a2a5140-8b0a-4033-bd94-2781de8d37cc, 70d9a5f5-7190-4452-a743-4f2bede82c06, b4afc993-f1ca-45d7-ab11-7f0605433915...}
Lots o Privs!         {74bc7815-7155-4f42-bc3a-33dc873c6344}
ProofPoint Custom App {70d9a5f5-7190-4452-a743-4f2bede82c06, 7d8afa78-d799-4bdc-8e33-3dff42fbbac3}
Azure Media Service   {5098c760-6d6d-4617-8b34-0492d498e7bc}
```

Application Owners

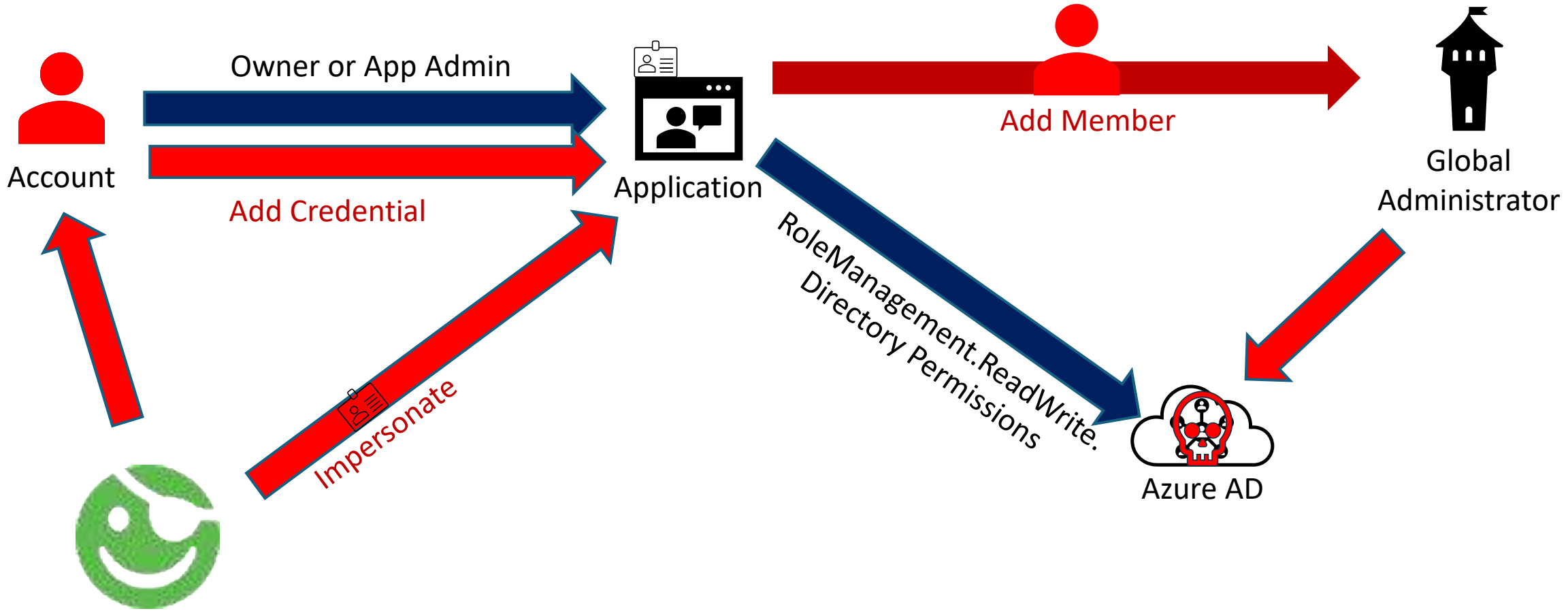
```
Application Owners:

TierLevel ApplicationName       displayName    userPrincipalName                  TierPermissions
--------- ---------------       -----------    -----------------                  ---------------
        0 AAD-Persist           Sean Metcalf   sean@bigmegacorp.com               Directory.ReadWrite.All, AppRoleAssignment.ReadWrite.All
          BMC Custom App        Aadyn Charles  Aadyn.Charles@BigMegaCorp.com
        0 Overpermissioned App  Kenyatta Yoder Kenyatta.Yoder@BigMegaCorp.onmicrosoft.com DelegatedPermissionGrant.ReadWrite.All, Application.ReadWrite.All,
        0 Overpermissioned App  Shayla Santana Shayla.Santana@BigMegaCorp.com      DelegatedPermissionGrant.ReadWrite.All, Application.ReadWrite.All,
        0 Overpermissioned App  Cadence Mclean Cadence.Mclean@BigMegaCorp.com      DelegatedPermissionGrant.ReadWrite.All, Application.ReadWrite.All,
          ProofPoint Custom App Shayla Santana Shayla.Santana@BigMegaCorp.com
          ProofPoint Custom App Cadence Mclean Cadence.Mclean@BigMegaCorp.com
```

Get-EntraIDAppOwners.ps1

https://github.com/PyroTek3/EntraID

Compromise Azure AD through Application Permissions



#8 Secure Entra ID with Conditional Access Policies

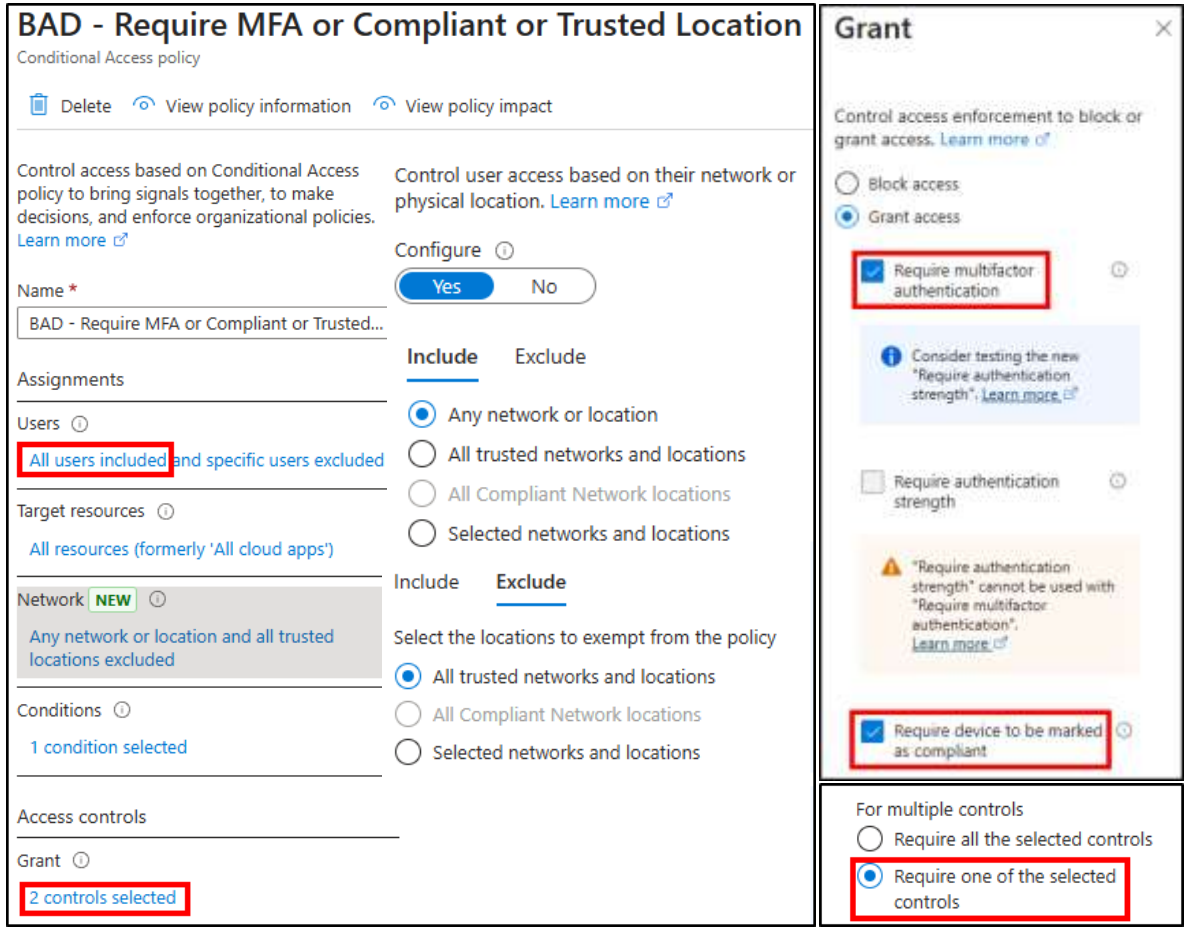


CA Policy Gap #1

- Users Require MFA Outside of Corp Network
- AKA: Exceptions vs. Exclusions

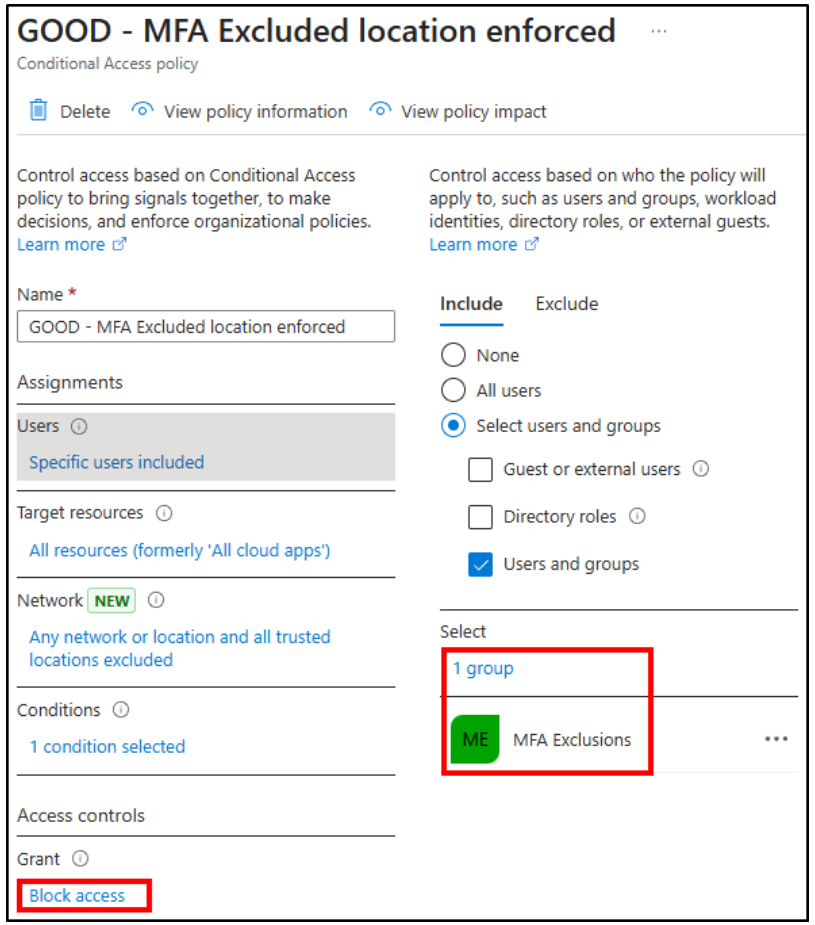
CA Policy Gap #1

- Exceptions
  - All Users
  - Exclude Trusted
  - Grant Control



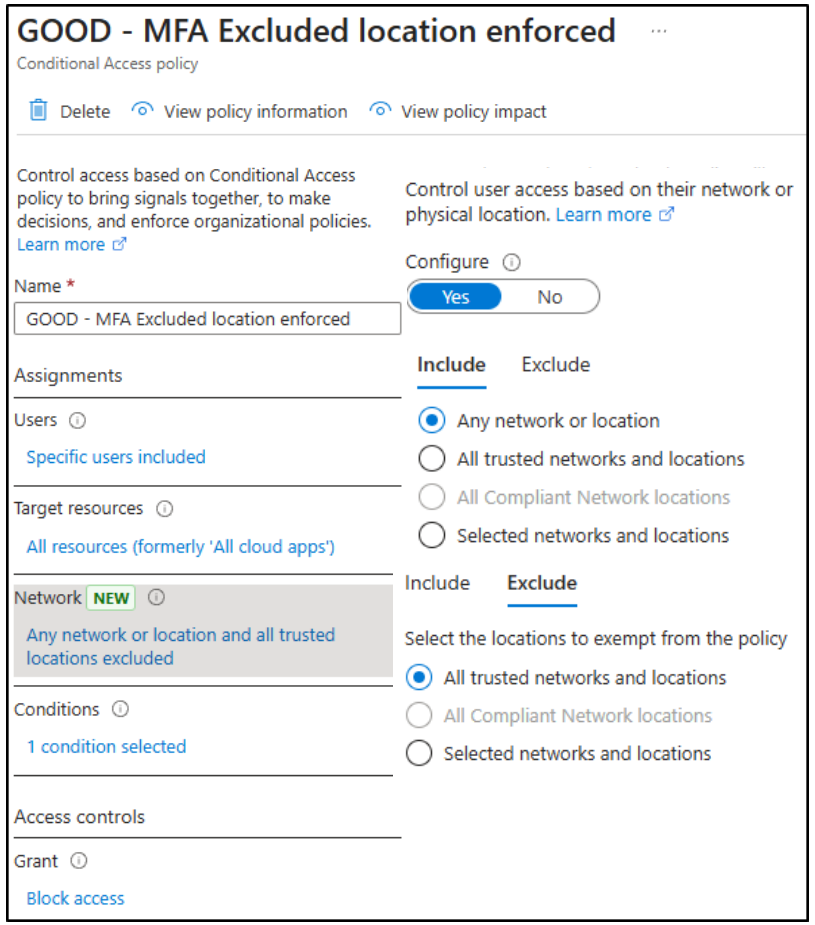
CA Policy Gap #1

- Exclusions
  - Specific Users
  - Block Control



CA Policy Gap #1

- Exclusions
  - Specific Users
  - Block Control
  - Exclude Trusted



CA Policy Gap #2

- Admins require MFA when…
  - accessing certain applications
  - they are a member of certain roles

CA Policy Gap #2

- Application Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Global Administrator
- Hybrid Identity Administrator
- Partner Tier2 Support
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator

https://trustedsec.com/blog/managing-privileged-roles-in-microsoft-entra-id-a-pragmatic-approach

CA Policy Gap #2

- Add (at least) These:
  - Authentication Policy Administrator
  - Directory Writers PRIVILEGED
  - External Identity Provider Administrator PRIVILEGED
  - Hybrid Identity Administrator PRIVILEGED
  - Identity Governance Administrator
  - Intune Administrator PRIVILEGED

All Admins All the Time

```
---------------- Microsoft Graph API ----------------
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! mfasweep1@[redacted] was able to authenticate to https://graph.windows.net - NOTE: The resp
onse indicates MFA (Microsoft) is in use.


---------------- Azure Service Management API ----------------
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! mfasweep1@[redacted] was able to authenticate to the Azure Service Management API - NOTE: T
he response indicates MFA (Microsoft) is in use.
```

```
---------------- Microsoft Graph API ----------------
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! mfasweep2[redacted] was able to authenticate to https://graph.windows.net
[***] NOTE: The "MSOnline" PowerShell module should work here.


---------------- Azure Service Management API ----------------
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! mfasweep2@[redacted] was able to authenticate to the Azure Service Management API
[***] NOTE: The "Az" PowerShell module should work here.
```

Key Conditional Access Policies



Block device code flow	Block legacy authentication (username and password authentication)	Block location by geography	Enforce compliance on all devices
Protect security info registration	Restrict access to apps by location	Require MFA for accounts with administrative roles (preferably FIDO2)	Require MFA for guest users
Require MFA for device registration	Require MFA for risky sign-ins	Require password change for risky users	

Key Conditional Access Policies

```
Categorize Policies:

Policies that Block Legacy Authentication
Block legacy authentication SMTP
Block legacy authentication - 4real

Policies that enforce MFA for Administrators
Require multifactor authentication for admins
Require multifactor authentication for some users
Require multifactor authentication for admins - template

Policies that enforce MFA for Users
Allow Legacy app for Adele - test
Require multifactor authentication for some users
Require multifactor authentication for all users

Policies that enforce MFA for Guests
Require multifactor authentication for guest access

Policies that affect Risky Users
Require multifactor authentication for risky sign-ins
Require password change for high&Med-risk users
Require password change for high-risk users

Policies that require Approved Client or App Protection
Require approved client apps Android iOS
Require approved client apps or app protection policies - Mobile
```

```
Policies that require Approved Client or App Protection
Require approved client apps Android iOS
Require approved client apps or app protection policies - Mobile

Policies that require Device Compliance
Require compliant device for admins
Require compliant or hybrid Azure AD joined device for admins
BAD - Require MFA or Compliant or Trusted Location

Policies that restrict access by Location
Require multifactor authentication for admins
trusted IP test
block Lee from my IP

Policies that restrict access to the Admin Portal
block azure portal

Policies that require MFA for Device Join
register device
Require MFA for Device Registration

Policies that block Authentication Flows
Block Device Code Auth

Policies that target All Resources and All Users
Block legacy authentication - 4real
Require multifactor authentication for all users

Policies that secure Secuirity Info Registration
secure registration
```

https://github.com/techBrandon/CAPs

Key Conditional Access Policies

```
Checking for Misconfigured CAPs

MFA Policies that target Admin roles should include the 14 default roles and any other role the environment deems privileged.

CAP_Name                                          Total_Roles Default_Roles Additional_Roles
--------                                          ----------- ------------- ----------------
Require multifactor authentication for admins              21 14/14                      7
Require multifactor authentication for some users           1 1/14                       0
Require multifactor authentication for admins - template   14 14/14                      0



MFA Policies that utilize Authentication Strength should use passwordless or phishing-resistant methods of MFA.

CAP_Name                                          Total_Methods Status PhishResistant Passwordless Multifactor Singlefactor
--------                                          ------------- ------ -------------- ------------ ----------- ------------
Require multifactor authentication for admins              17 Fail                3            1          13            0
secure registration                                         4 Pass                3            1           0            0
Require multifactor authentication for Azure management    22 Fail                3            1          13            4
BAD - Require MFA or Compliant or Trusted Location         17 Fail                3            1          13            0
```

https://github.com/techBrandon/CAPs

#9 Secure Partner Access

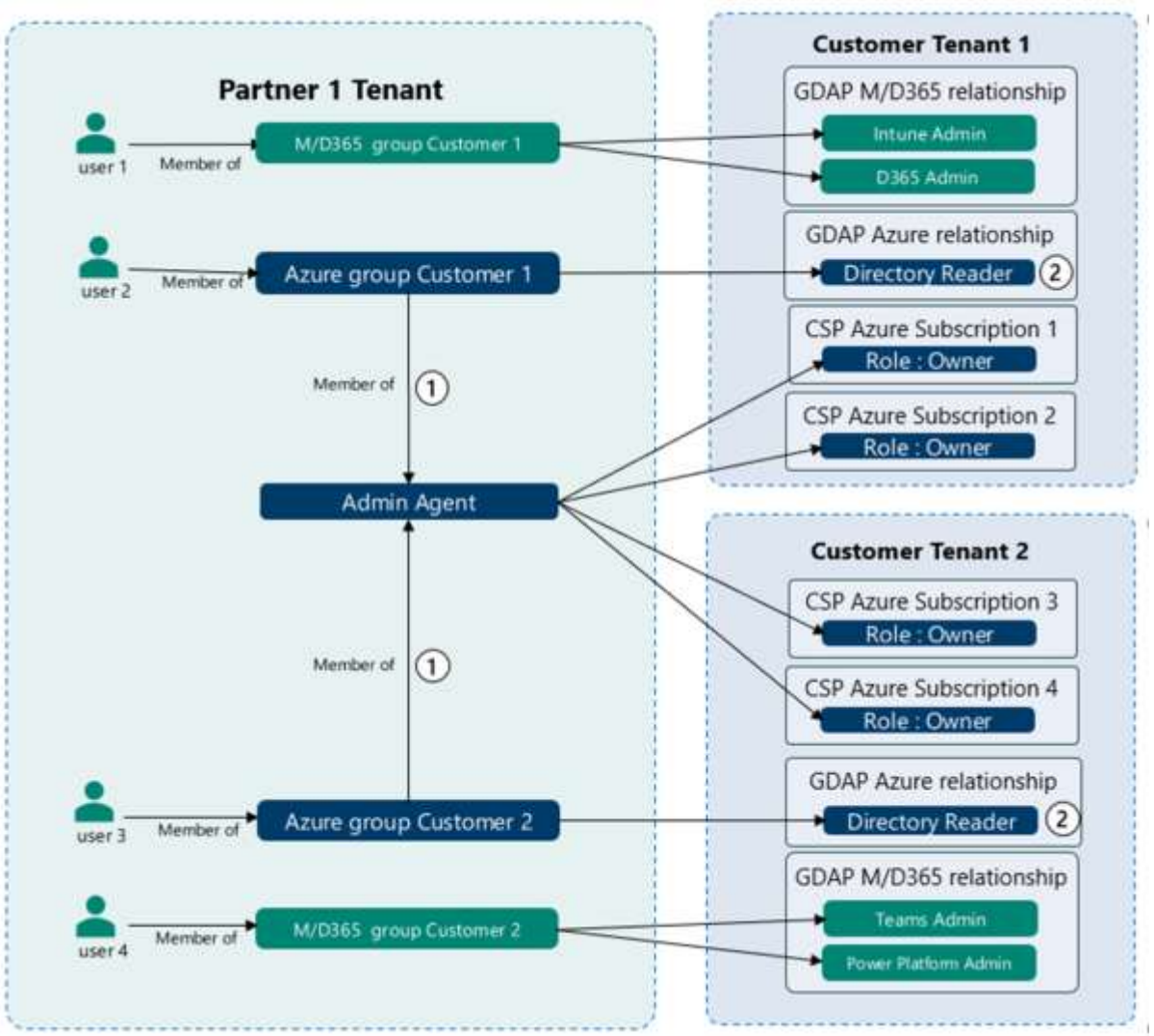


Partner Relationships – aka Delegated Administration

- 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!

Move to Granular Delegated Admin Privileges (GDAP)



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



BIG MEGA CORP | Delegated admin partners ...

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- **Delegated admin partners**

Got feedback?

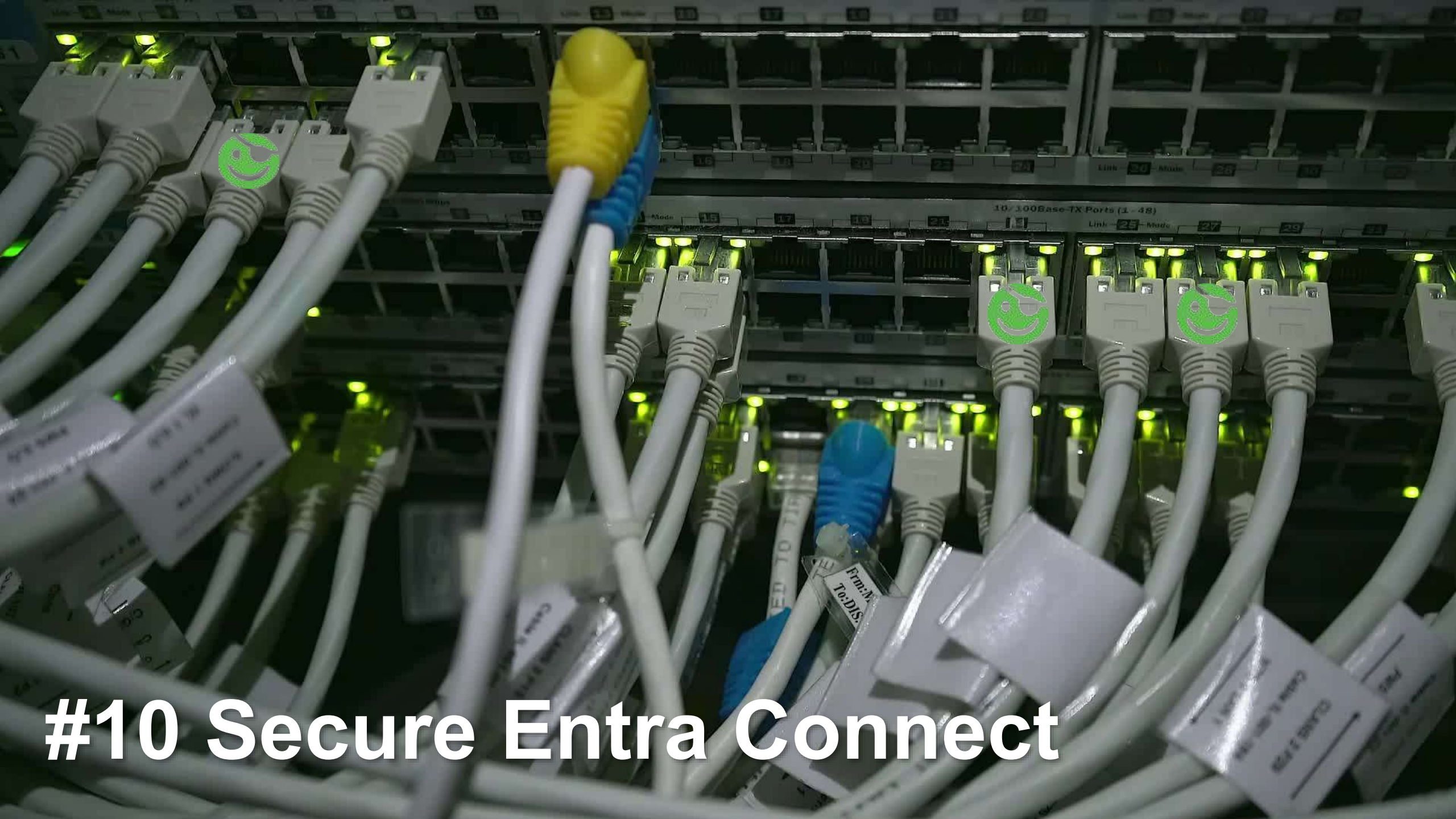
Delegated admin partners are Microsoft partners that you have authorized to administer Microsoft services in your tenant using delegated administration privileges.

Partner Name	Relationship type	Roles

No partner relationships

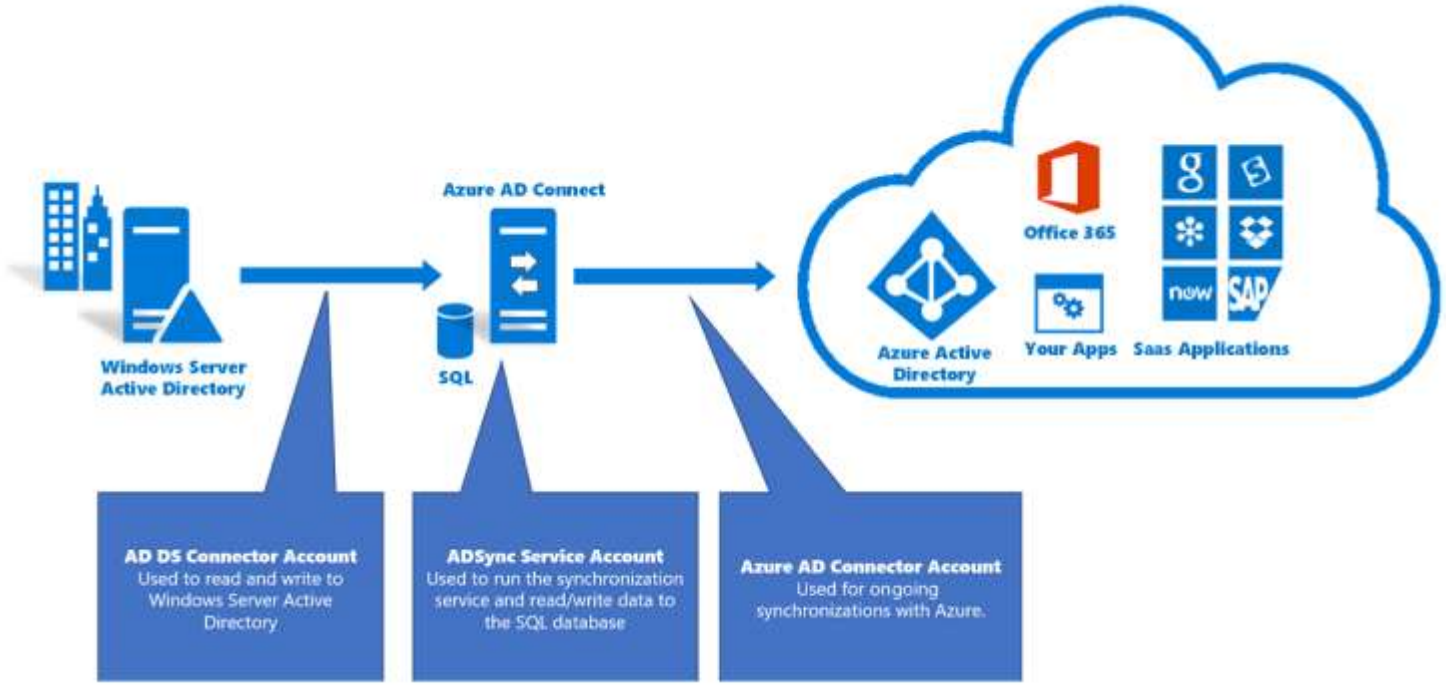


Check Partner Configuration for your tenant here:
https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/PartnerRelationships



#10 Secure Entra Connect

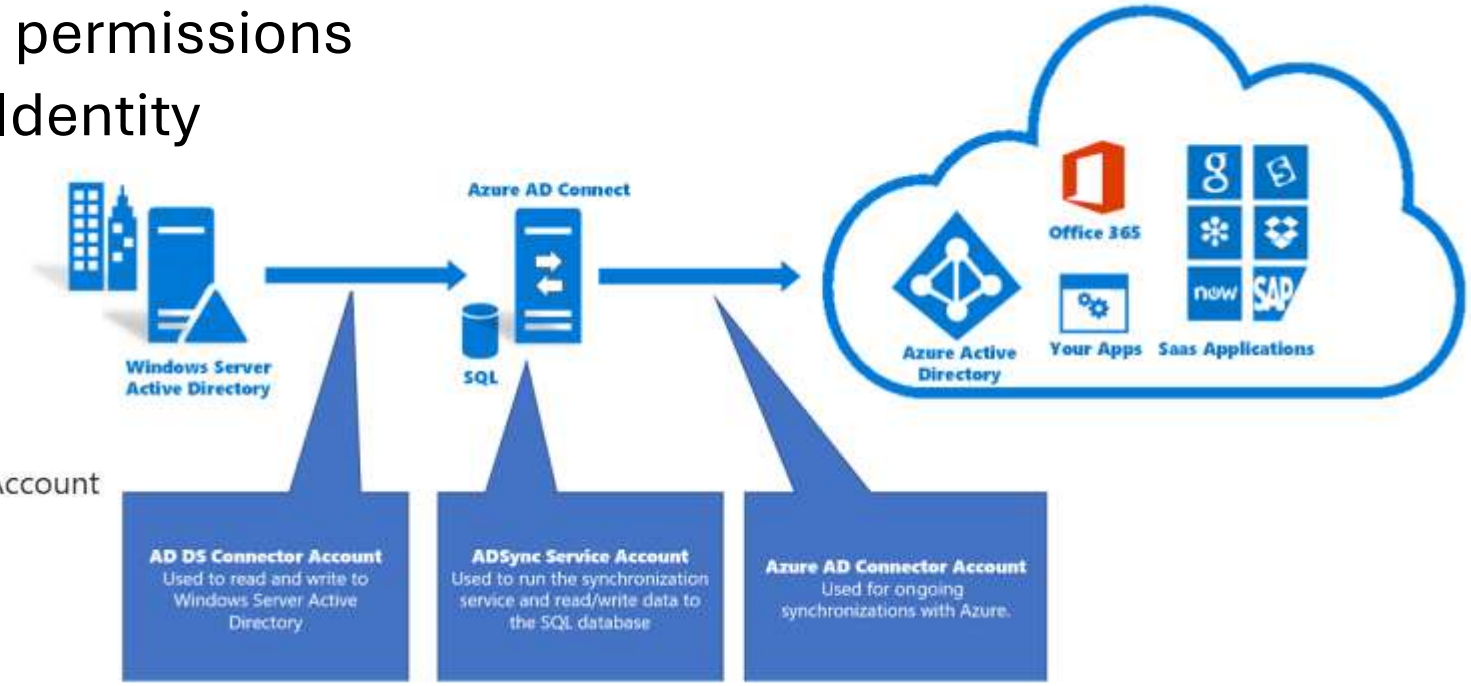
Compromising Entra



https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-accounts-permissions

Compromising Entra

- Entra Connect
  - August 2024 – Reduced permissions
  - July 2025 – Application Identity



Basic info

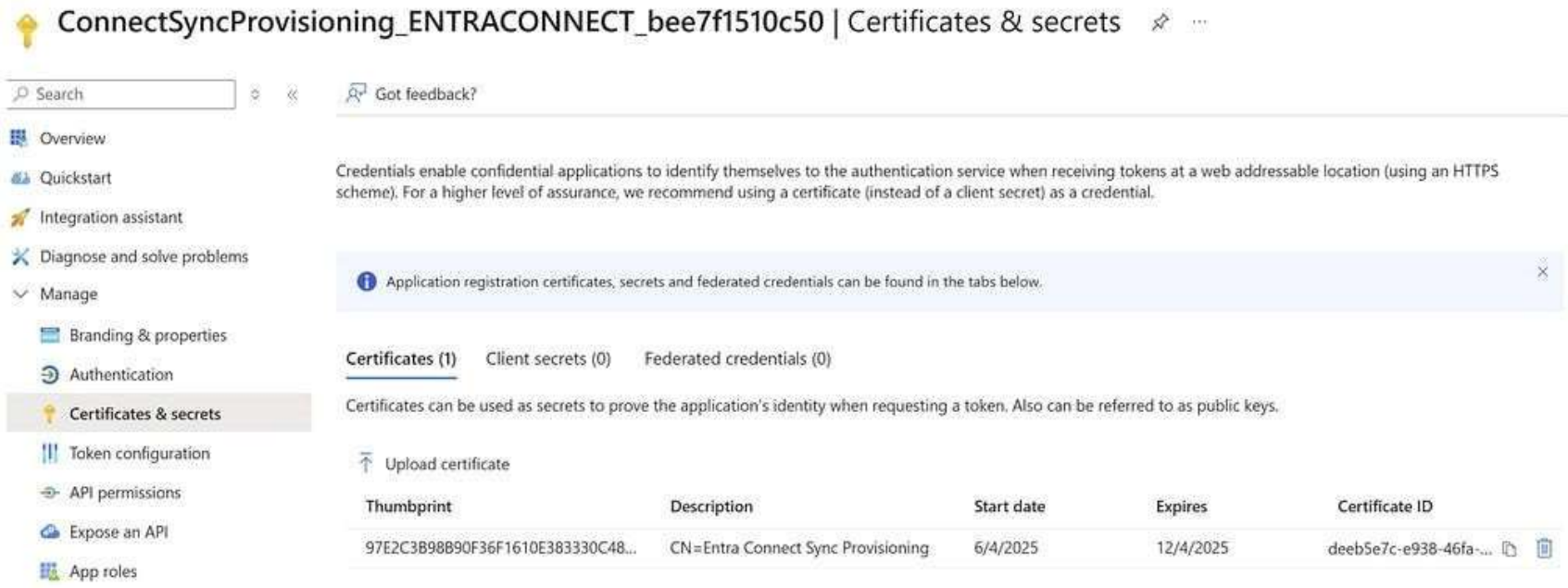
O

On-Premises Directory Synchronization Service Account
Sync_KINGSLANDING_95f0c10db682@6m1nzt.onmicrosoft.com
Member

https://cloudbrothers.info/prem-global-admin-password-reset/
https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/authenticate-application-id?tabs=default

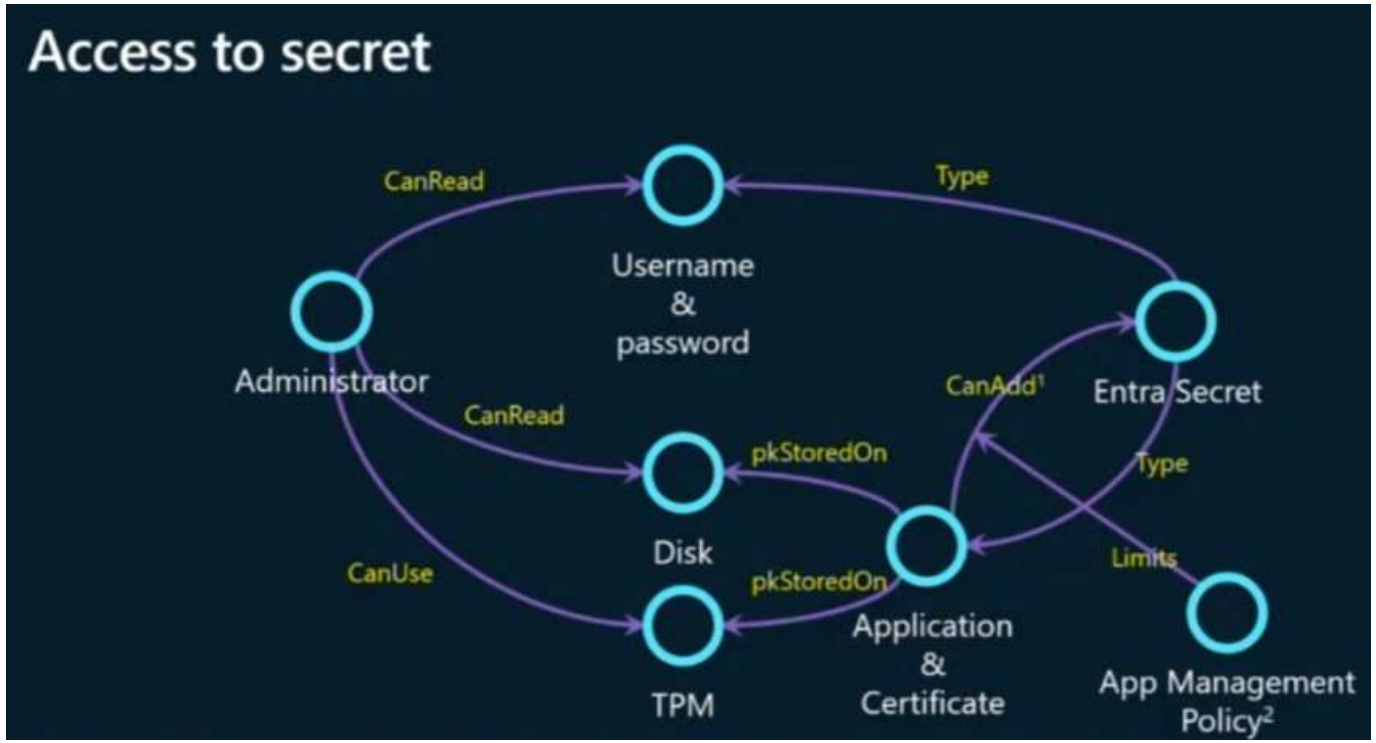
Compromising Entra

- Entra Connect
  - Automatic onboarding in version 2.5.76.0
    - Released 7/31/2025



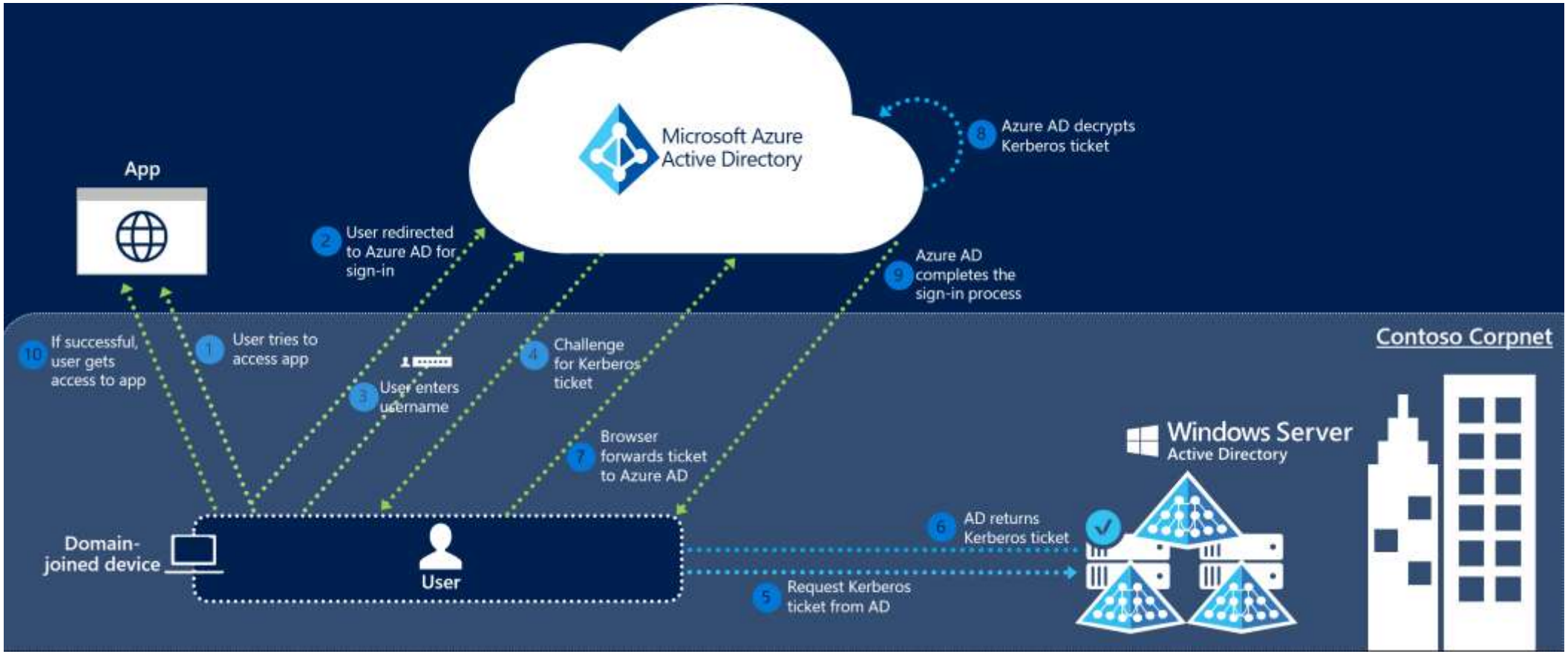
Compromising Entra

- **Entra Connect Security**
  - Update Entra Connect
  - Store credentials using TPM
  - Implement workload identities
  - Treat Entra Connect as Tier 0

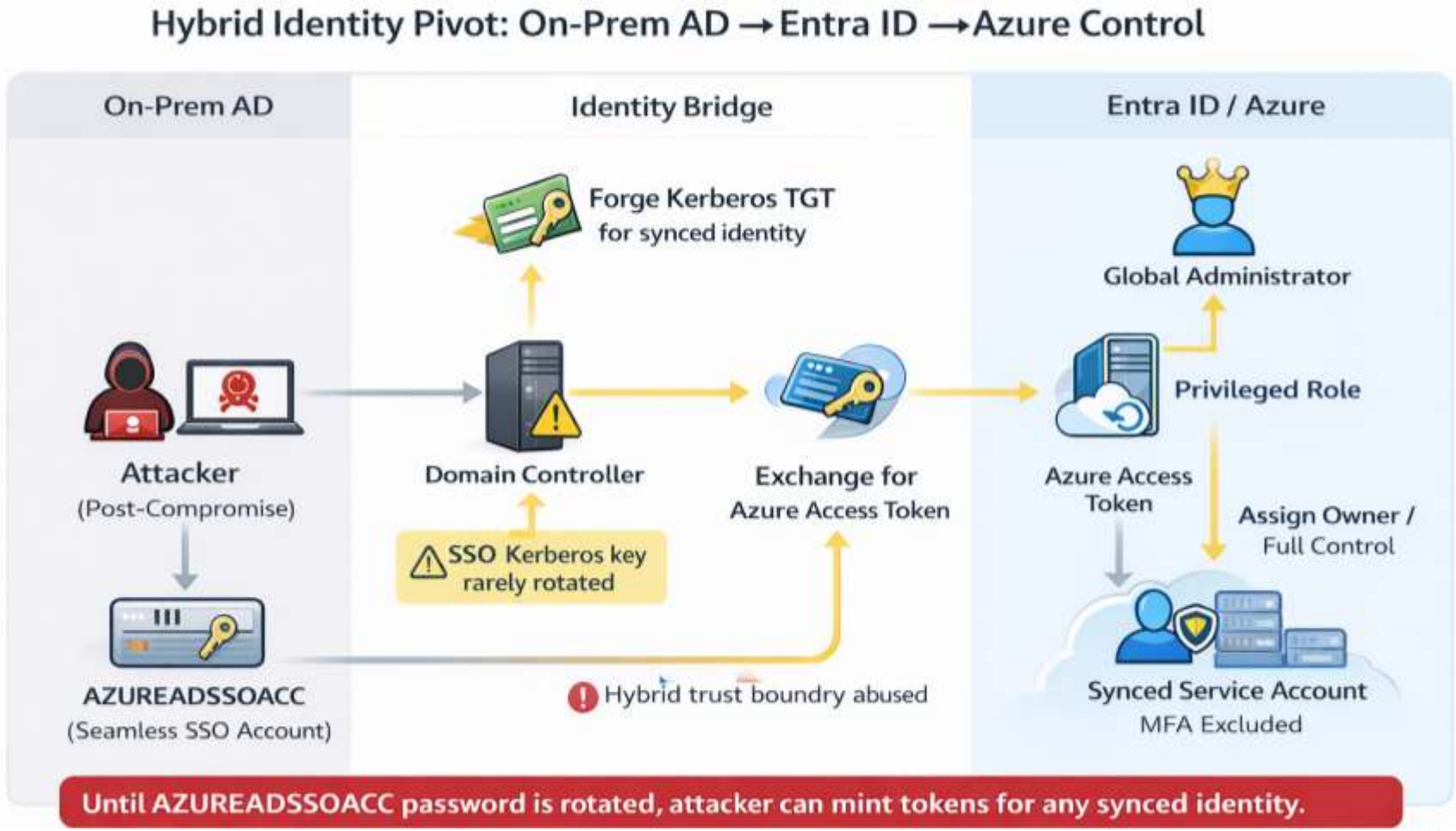


https://specterops.io/blog/2025/06/09/update-dumping-entra-connect-sync-credentials/
https://learn.microsoft.com/en-us/entra/workload-id/workload-identities-overview
https://www.youtube.com/watch?v=6MoV7SEEkJg

Seamless Single Sign-On (SSSO)



Seamless Single Sign-On (SSSO)



https://trustedsec.com/blog/azure-ad-kerberos-tickets-pivoting-to-the-cloud

Securing Entra Connect

- Don’t sync admin accounts
- Modern OS use Primary Refresh Token (PRT)
- Change SSSO key (password) multiple times per year
- Treat Entra Connect & PTA agents as Tier 0
- Tier 0 systems:
  - Treat like Domain Controllers
  - Isolate administration to only AD admins
  - Ensure linked group policy objects are only controlled by AD admins
  - Restrict local admin accounts to AD admins

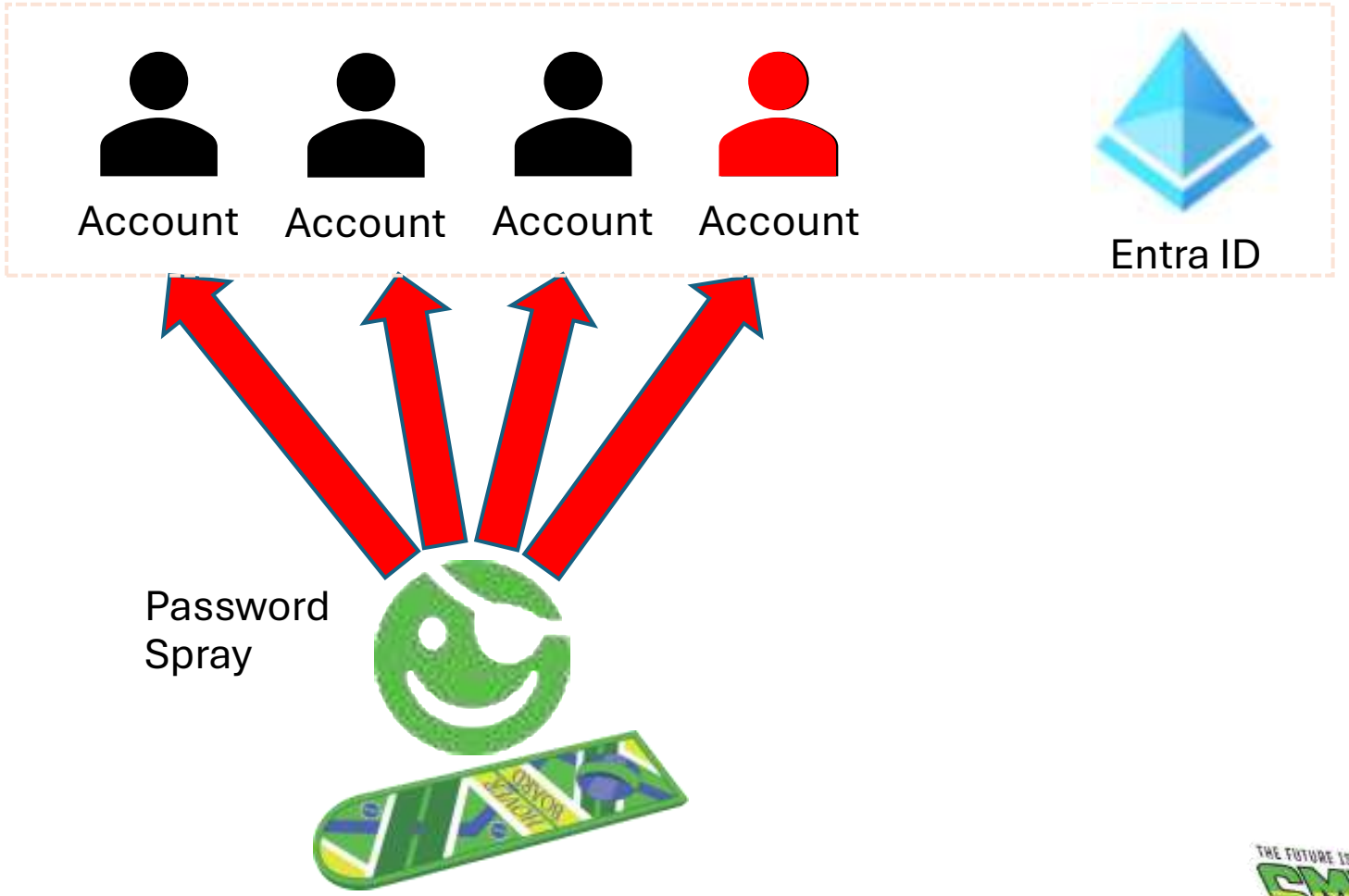
Entra ID Attacks



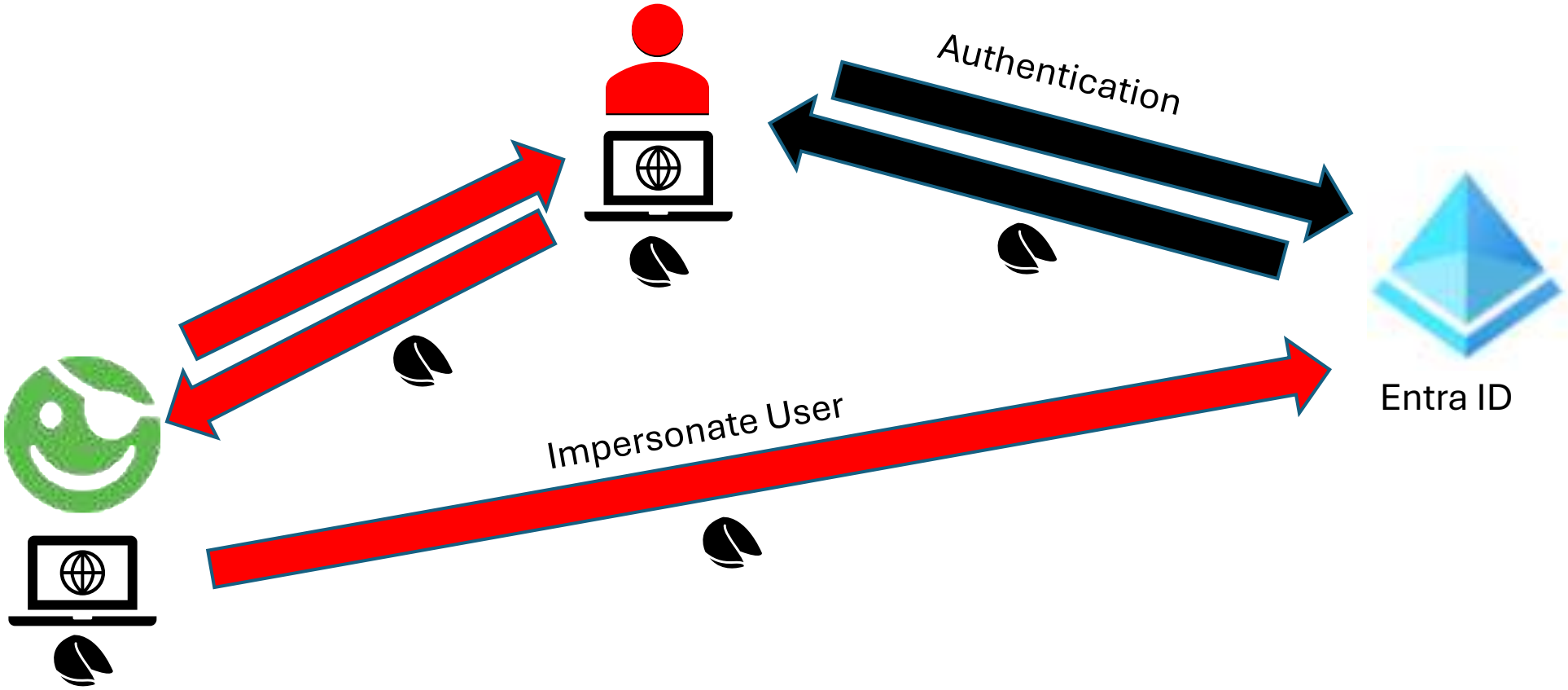
Attack Tools

- AADInternals
- Evilginx2
- GraphRunner
- GraphSpy
- Microburst
- MFASweep
- MSOLSpray
- O365Recon
- Onedrive_user_enum
- ROADTools
- Teamfiltration
- TokenTactics/TokenTactics2

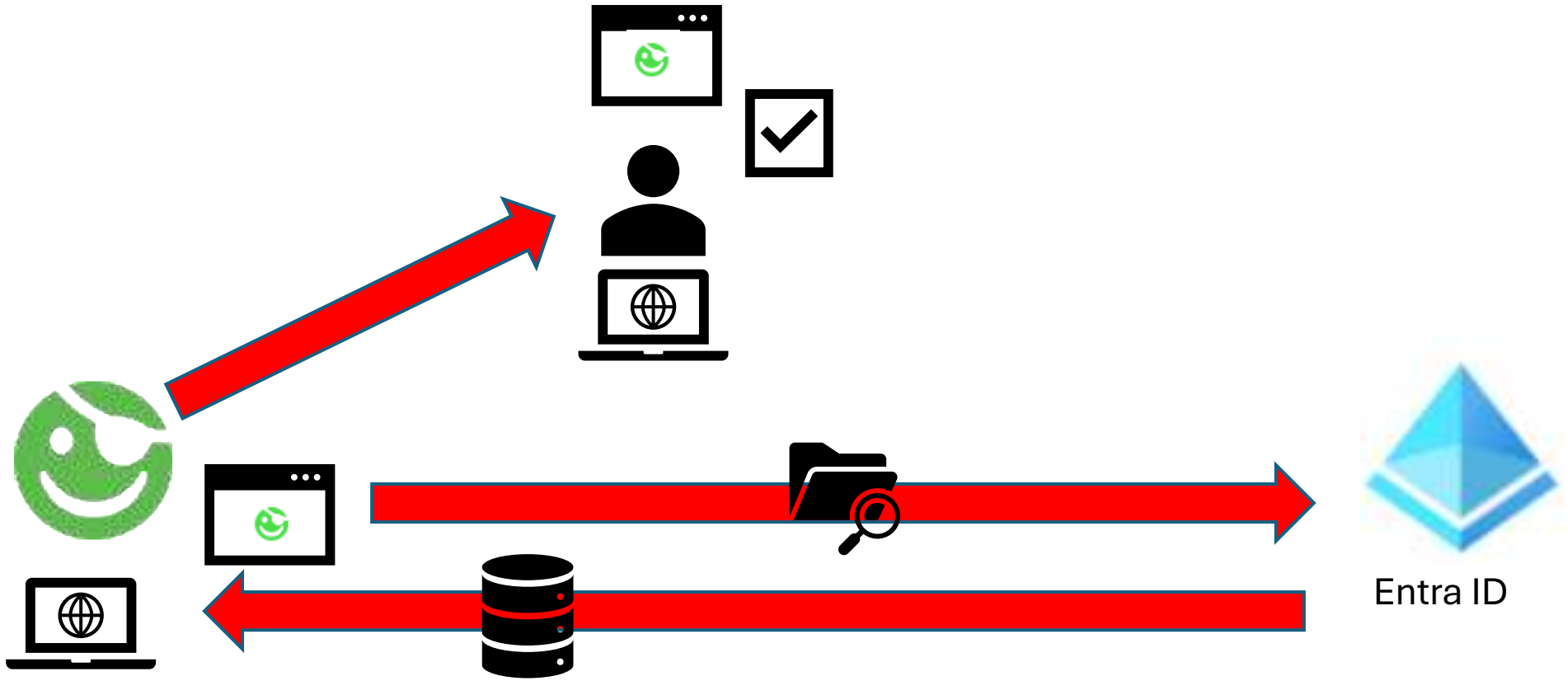
Password Spray Attack



Token Theft & Replay

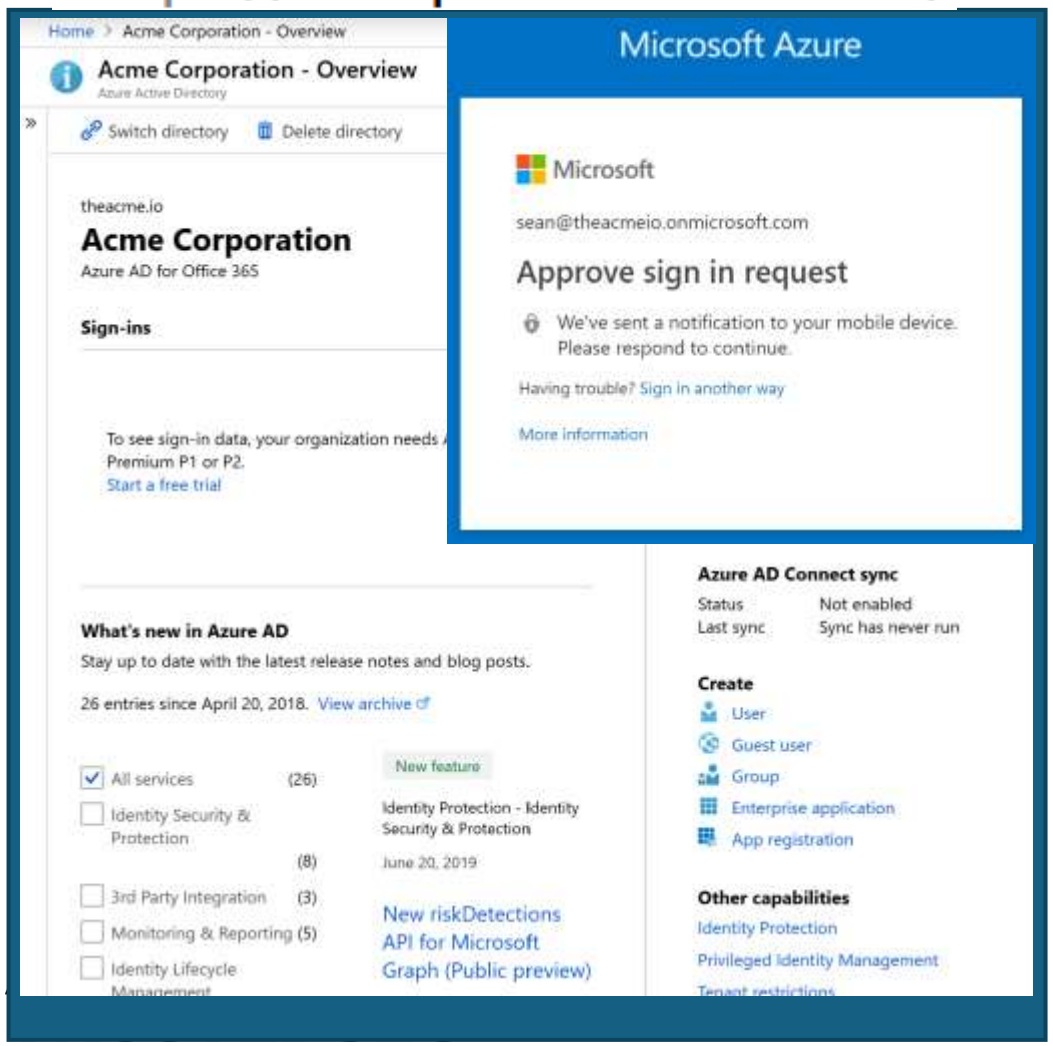


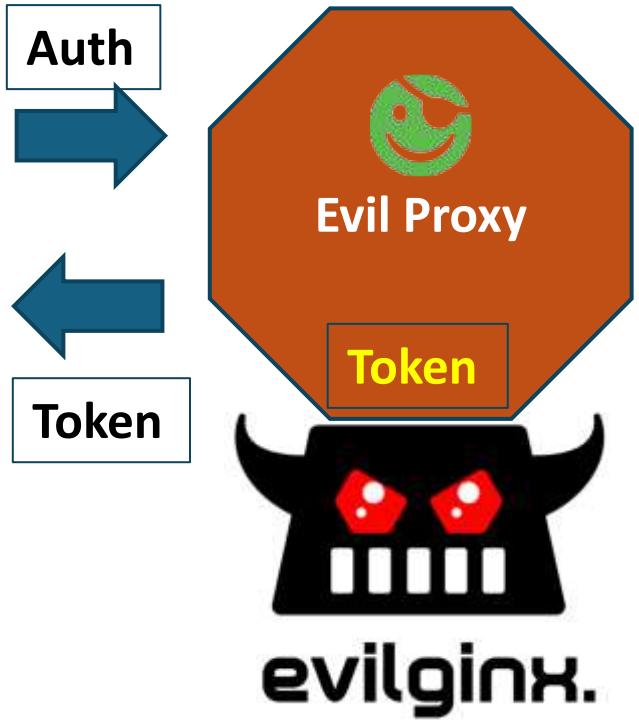
Consent Phishing



Token Theft with evilginx

https://aad.portalazure.com/



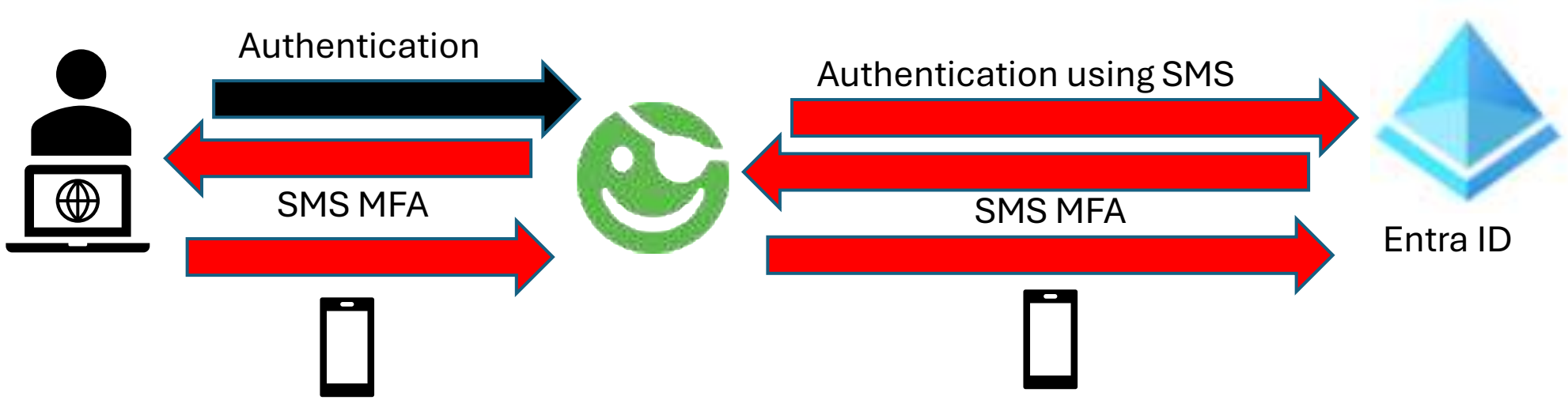


https://aad.portal.azure.com/

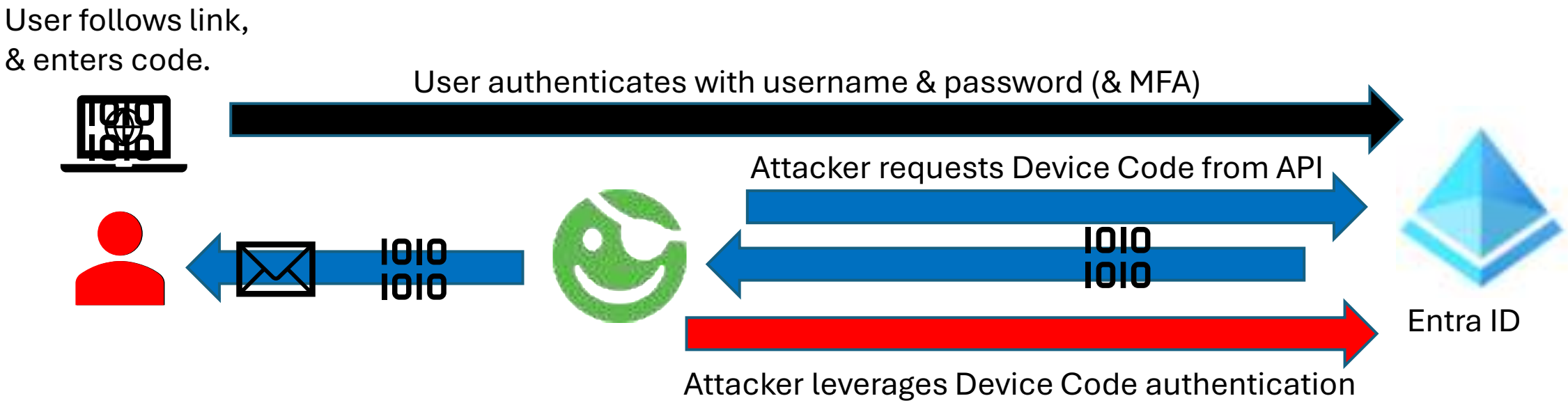


https://github.com/kgretzky/evilginx2

MFA Downgrade Attack



Device Code Flow Attack



Securing Entra ID



Key Mitigations



- Disable Device Code Flow
  https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows
- Leverage the Microsoft Authenticator app for MFA
- Disable Text/SMS as an MFA option
- Ensure cloud admins use a different system from standard web browsing
  - **OK**: Another browser (at a minimum)
  - **Good**: Remote into a cloud admin server
  - **Best**: Use a separate computer for admin actions
- Ensure all Windows computers have VBS backed by a TPM
- Remove local admin rights from standard users on AAD Joined devices
- Do not allow users to join their own devices
- Don’t let users consent to application permissions (or at least use Microsoft recommended)
- Block soft matching & hard matching in Entra ID (Entra Connect)

Secure Entra ID Quickly Checklist



1. Set “Users can register applications” to No
2. Set “Restrict non-admin users from creating tenants” to Yes
3. Set “Users can create security groups” to No
4. Set Guest user access restrictions to “*Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)*”
5. Restrict who can join devices to Microsoft Entra & require MFA
6. Set Guest invite settings to “*Only users assigned to specific admin roles can invite guest users*”
7. Set User consent settings to “*Let Microsoft manage your consent settings (Recommended)”*
8. Review Tier 0 role membership and ensure members are admin accounts, are PIM Eligible, & are not synchronized from on-prem
9. If you’re using Role Assignable Groups, ensure Owners are not set on Tier 0 & 1 roles
10. Scrutinize any applications with Tier 0 Application permissions
11. Ensure that Conditional Access requires MFA for Tier 0 & 1 role members for every authentication, preferably FIDO2/Microsoft Authenticator push (service accounts & service principles excepted).
12. Remove any standard Delegated Administration and shift to Granular Delegated Admin Privileges (GDAP)
13. Treat Entra Connect as a Tier 0 asset (like a Domain Controller)
14. Ensure Cloud Admins are using a separate browser for admin activities (minimum) or connecting to a dedicated cloud admin server (recommended)
15. Ensure there is at least 1 emergency access admin account configured with a FIDO2 key(s).

Stay Up to Date on Entra ID Security

PyroTek.io/EntraIDSecurityList



TRUSTEDSEC

THE FUTURE IS TRUSTEDSEC SMILEYCON 2026

Conclusion



- Attacker cloud capability continues to evolve
- Defender methods need to evolve as well
- There are key mitigations that disrupt multiple attacks

Brandon Colley
@TechBrandon
brandon.colley@trustedsec.com

Sean Metcalf
@PyroTek3
sean.metcalf@trustedsec.com

Slides:
PyroTek.io/SC2026

Questions?



TRUSTEDSEC

We want to hear your Feedback!

Please scan the QR code on this slide to share your feedback regarding this presentation.

Scan To Take Survey

TRUSTEDSEC

FOLLOW US @TRUSTEDSEC

The information security industry is constantly evolving – keep up by following TrustedSec's active social media, blogs, podcasts and webinars.

