



10 Ways to Improve Entra ID Security Quickly







Sean Metcalf @PyroTek3



About

- Identity Security Architect @ TrustedSec
- Microsoft Certified Master (MCM)
 Directory Services
- Speaker: Black Hat, Blue Hat, Blue Team Con, multiple BSides, DEFCON, DerbyCon, RSA, TEC, Troopers, etc.
- Former Microsoft MVP
- Security Consultant / Researcher
- Own & Operate <u>ADSecurity.org</u> (Microsoft identity security info)

PyroTek.io/About



C

Agenda

- 1. User Defaults
- 2. Guest User Defaults
- 3. Application Consent Defaults
- 4. Entra ID Roles (Level 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. Bonus Content

Attackers Target Cloud



Suttons Law:

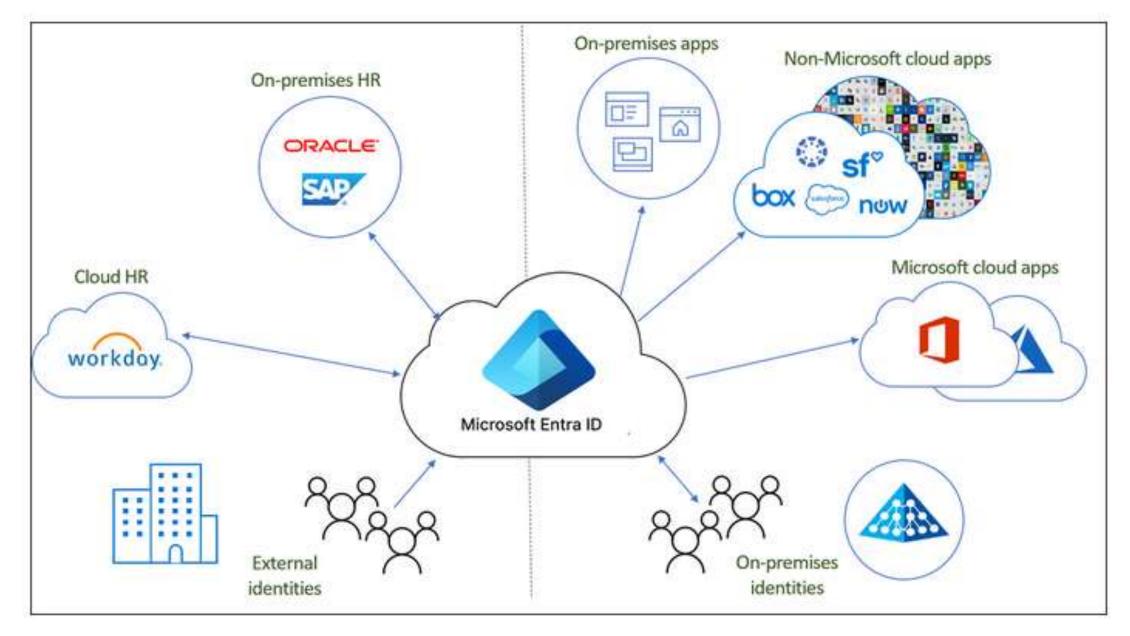
When diagnosing, one should first consider the obvious.

See also Occam's Razor ("entities should not be multiplied without necessity")



What does this mean?

Cloud security often misunderstood
Cloud is where the data is



https://learn.microsoft.com/en-us/entra/identity/hybrid/what-is-provisioning



#1 & #2 Secure Entra ID User & Guest Defaults

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

Default user role permissions

Defaults

Learn more 2

Users can register applications



Yes

Restrict non-admin users from





creating tenants

Users can create security







Yes

Guest user access

Learn more 2

Guest user access restrictions



Guest users have the same access as members (most inclusive)

 \bigcirc

Guest users have limited access to properties and memberships of directory objects

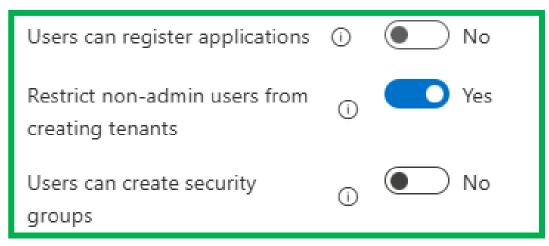
 \bigcirc

Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Default user role permissions

Recommended Settings

Learn more



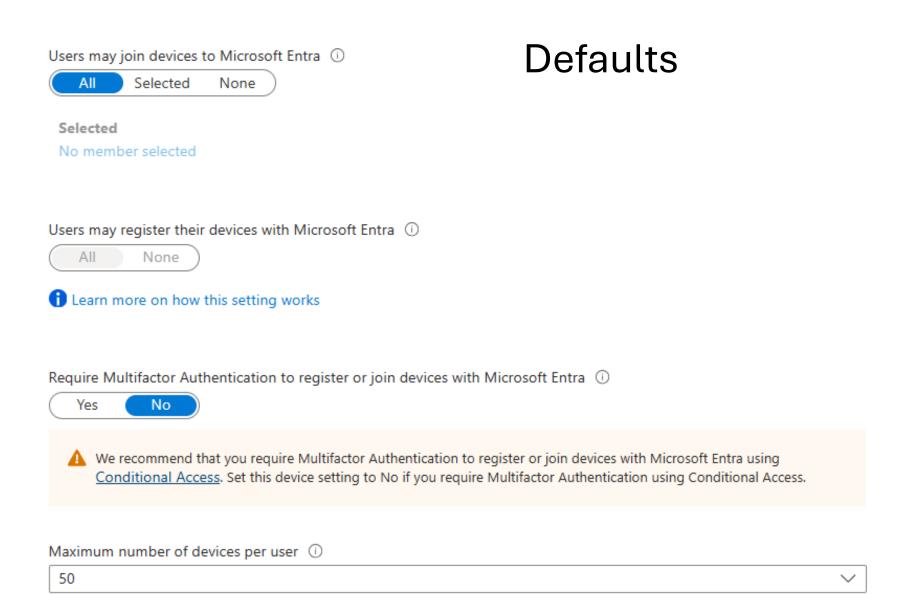
Guest user access

Learn more 🛚

Guest user access restrictions (i) Guest users have the same access as members (most inclusive)

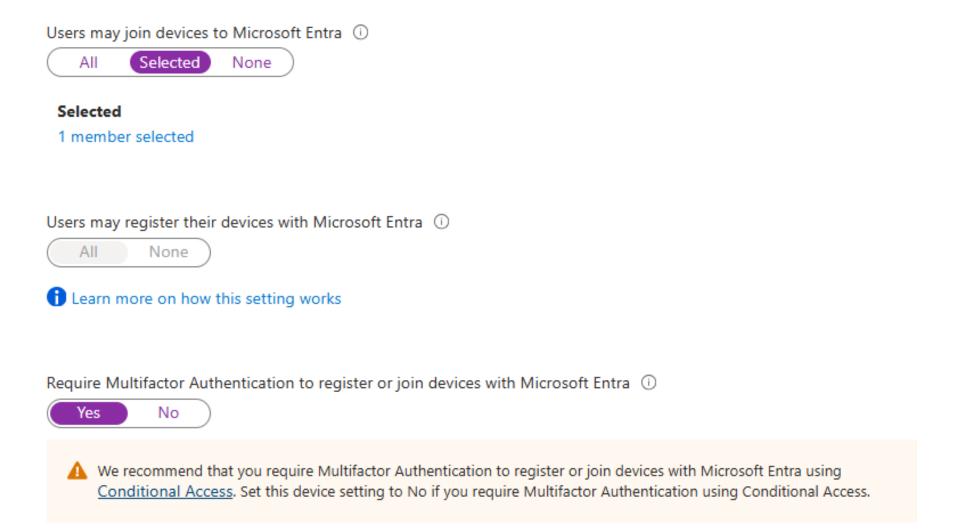
Guest users have limited access to properties and memberships of directory objects

Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)



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

Recommended



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

Defaults

Guest invite settings

Guest	invite	restrictions	(I)
Oucse	HIVICE	restrictions	

Learn more

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

Collaboration restrictions

•	Cross-tenant access settings are also	vovaluatod whon c	conding an invitation	to dotorming whather the	a invita chould ba allow	ad ar blackad. Laarn m	LORG
43	Cross-teriant access settings are also	evaluateu wileii s	senung an invitation	to determine whether the	e ilivite siloulu be allow	eu of blockeu. Leaffi fil	iore

- 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

Recommended Settings

Guest invite settings
Guest invite restrictions ①
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

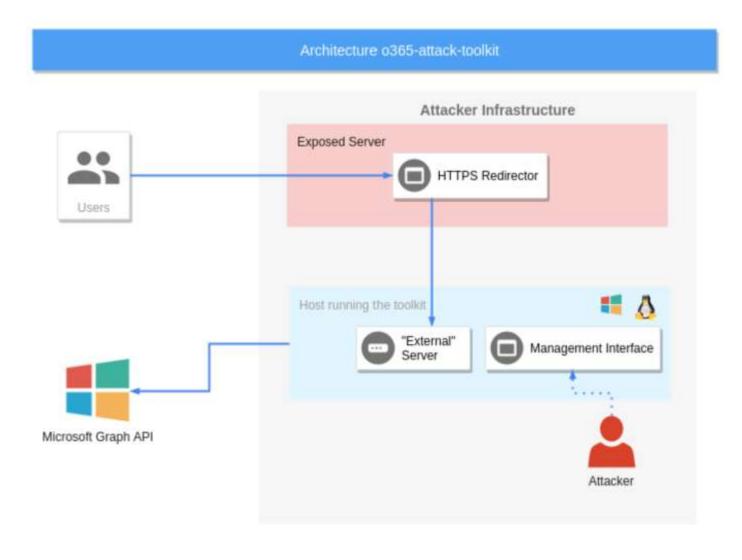
https://portal.azure.com/#view/Microsoft_AAD_IAM/AllowlistPolicyBlade

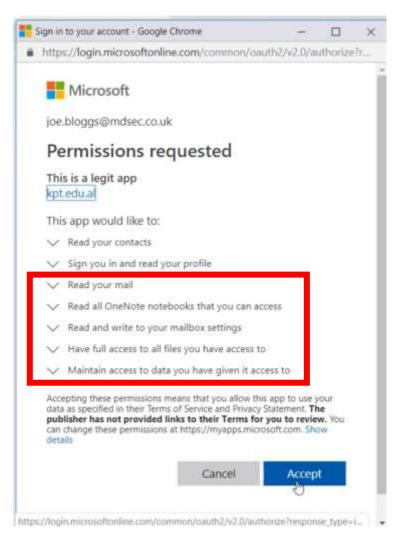
Allow invitations only to the specified domains (most restrictive)

```
peration == "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
#Irror_mod.use_z = False
 operation == "MIRROR Y"
irror_mod.use_x = False
mirror_mod.use_y = True
 irror mod.use z = False
  operation = "MIRROR Z"
  irror_mod.use_x = False
 lrror_mod.use_y = False
 Irror_mod.use_z = True
 melection at the end -add
  ob.select= 1
  er ob.select=1
   ntext.scene.objects.action
  "Selected" + str(modifier
  irror ob.select = 0
 bpy.context.selected_ob_
lata.objects[one.name].sel
 int("please select exaction
 -- OPERATOR CLASSES ----
    ext.active_obje
```

#3 Secure Entra ID Application Consent Defaults

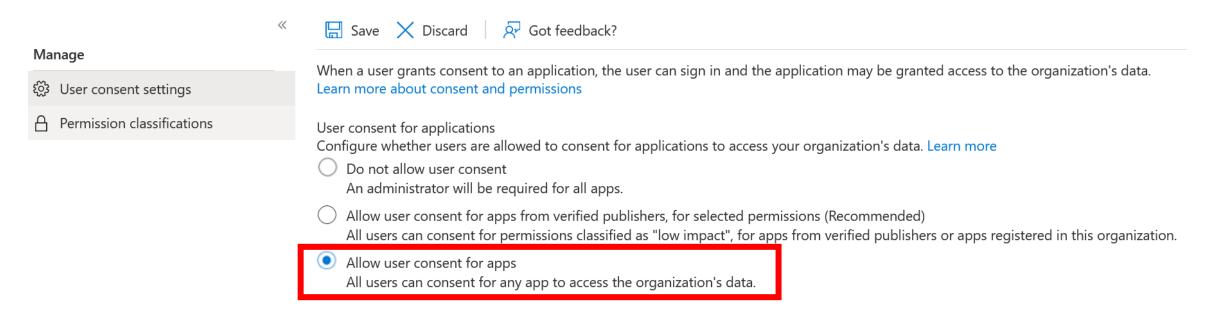
Illicit Consent Grant Attack: MDSec O365 Attack Toolkit





Once Upon a Time...

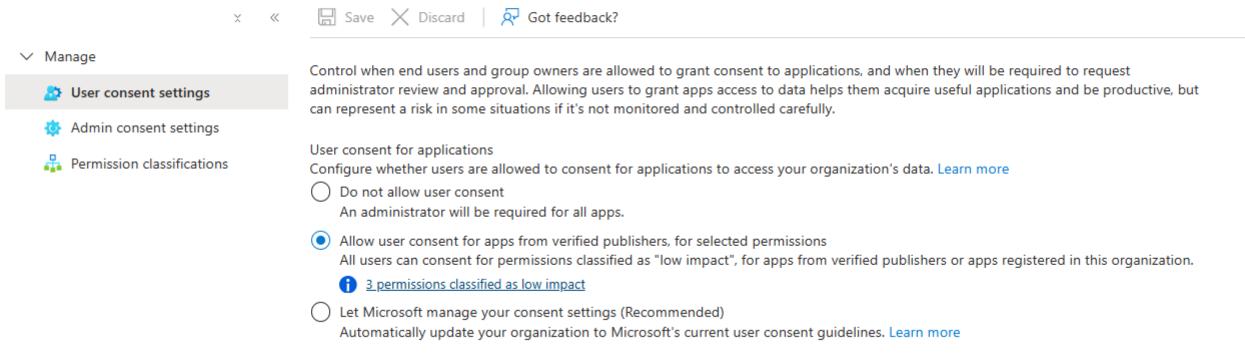
Consent and permissions | User consent settings



Defaults

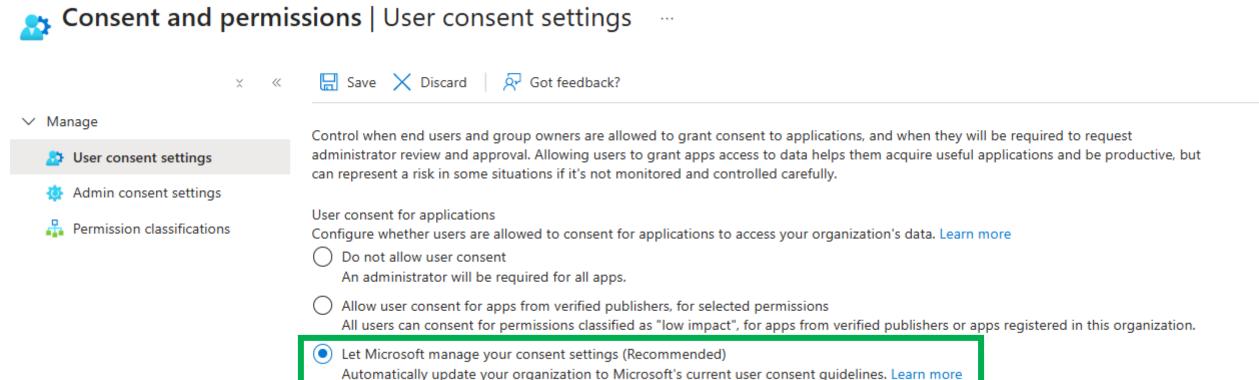


Consent and permissions | User consent settings -



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

Recommended Settings



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

#4 Secure Entra ID Roles



There are >100 Entra ID Roles!

t-i-	Description	Templale ID
Al Administrator	Hanage all appeals of Hiseasoft 365 Capital and Alvertated enterprise accessors in Hiseasoft 365	42562-47446-457766-544-236
Application Administrator	Can arrale and manage all appeals of appregialealisms and colorprine apps.	36832435-5-43-44-7-5482-46-4245
Application Developee Allanh Pagland Author	Can needle application expinited inno independent of the 'Uneen nan expinite applications' nelling. Can needle allanh pagloadu that an adminintealne nan initiale talee.	3.646862-1-7-444-3-6135-664644
Allank Simulation Administrator	Can arrair and manage all appeals of allank simulation nampaigns.	.431.535533-453563-41.6466
Alleikale Ausigament Administratur Alleikale Ausigament Reader	Ausign annlam neuerilg alleihale begn and naluen la nappaeled Mineumél Eulea uhjeulu. Read unulum neuerilg alleihale begn and naluen for unppueled Mineumél Eulea uhjeulu.	58,43,43-4592-464-3-8-8-94849. 66452645-3844-4654-3314-64879-1
Alleibale Definition Administrator	Define and manage the definition of modum nemerity atteibuten.	1424-668-2483-455-4448-26-4755
Alleikale Definition Reader	Read the definition of annual according atteitutes.	1455542
Alleikale Lag Adminialealae Alleikale Lag Readee	Read and il lugu and modiquee diaquoolin nellingu for encolure laled lu noolun neuveilg alleikulen Read and il lugu celaled lu noolun neuveilg alleikulen.	56784334-6346-474,-,387-,72436, 3,335334-8486-484-8356-6454-63
Alleibale Provincesing Administrator	Read and edit the provincing nunfiguration of all aution nuntum neutrity attributes for an applic	
Alleibale Pennininning Reader	Read the province in a sufficient of all aution under country alleibates for an application.	422248-4-4645-4-69-66-8-66445
Authentication Administrator Authentication Enterophisting Administrator	Can annen la nieu, nel and ernel anlbenlinalinn melbod informalion for any non-admin nore. Contonior niqu in and niqu op enperiencen for noren by needling and managing nonlon anlbenlinali	#4-55645-1100-4645-0-65-661604. 25-546-4-26-0-40240-42525-2
Authoritation Poling Administrator	Can arrale and manage the authentication wellands policy, tenant-wide MFA wellings, password pro	85267466-4494-4-45-62-8-68-9-22
Auer-Dra0pa Administrator	Can manage Annee DenOpn polinies and nellings.	+5575646-4587-452+-8572-628+251
Auer Information Protestion Administrator DZC IEF Kryort Administrator	Can manage all appeals of the Asser Information Protestion product. Can manage procedures for federation and conception in the Identity Experience Features (IEF).	74356444-3444-4445-4213-317184 44643236-8484-4456-8134-6355383
PZC IEF Paling Administrator	Can arrain and manage front framework policies in the Identity Engreises of Framework (IEF).	3-4-6663-3414475-3634-5-338-6
Pilling Administrator	Campreform numme killing related tasks like updating pagerel information.	18654664-2474-4458-4645-464886 18245842-4546-4654-1844-724484
Cloud App Scoorilg Administrator Cloud Application Administrator	Can manage all augents of the Defender for Cloud Apps pendunt. Can needle and manage all augents of app registerlinon and enterprine appn encept App Penng.	158-147317-4555-47-6-445551
Cloud Desire Administrator	Limited assess to manage desires in Hiseassett Entra ID.	7698-772-7876-6-48-9846-6846688
Compliance Administrator Compliance Data Administrator	Convended was agree unplicate and figuralism and reports in Microsoft Entry ID and Microsoft S	17315797-1824-4864-35-8-432862. -641-254-11-46-4-3578-6-6-864
Conditional Assess Administrator	Cerales and manages sumplianes unsteal. Can manage Conditional Assess napabilities.	hth-1-3654-4613-8427-656-842
Caulaner LaubBan Raueran Approver	Can approve Hisraroff support requests to assess unabserv organizational data.	54653444-4744-4467-8454-5-4287-
Droklop Analylina Adminintrator Discolary Readers	Can annon and manage Deublop management looks and need need to come of the Can read basis directory information. Commonly used to grant directory read annous to application	31.35434-21.46-414-415-53331.4
Directory Squabrasicalian Assessals	Only and by Hisraroft Entry Coursel arrains.	22312115-1146-441 ₂ -1751-4-26412
DirectorsWriters	Can read and write basis directory information. For granting annexs to applications, not introded	33686+65-6418-46-a-8175-+2-886-
Denzie Haue Administrator Desgue Administrator	Con manage domain names in aland and an permisers. Hanage all appeals of the Hisensoft Deagan admin sealer.	#9294596-9448-4727-6945-745-696 +99+9797-6485-4744-4+4-7496686
Danamina SES Administrator	Can manage all appeals of the Discountil Designs admin senter.	44357453-6644-4463-3866-6578787
Danamina 565 Paniaran Crafral Administrator	Asserts and prefere all administration tasks as Desamins 165 Designes Crateal resignments.	36373766636-4-483-5878636
Edge Administrator Enskange Administrator	Hanage all appeals of Hiseassell Edge. Can manage all appeals of the Eusbauge product.	361de-1-84-4663663-68382 23232d6-3323-4264de2-14837
Ennhange Renipient Administrator	Can arrair or optair Euchauge Online centpiculu within the Euchauge Online organication.	31332666-586a-4241-3346-+53415.
Entraded Directory Unce Administrator	Hanage all appeals of colornal over profiles in the colouded discolory for Teams.	4413831-6287-6648-826-3561-83
Enternal ID Uner Flow Administrator Enternal ID Uner Flow Attribute Administrator	Can needle and manage all appeals of once flows. Can needle and manage the alleibule unbema anailable to all once flows.	E-5318ES-3644-43-4-3863342436 B637441-6-45E3-4715766843
Enternal Identity Provider Administrator	Can annéignes identify pennides a for one in dissal federalism.	6-264521-4574-4226-2867-6-41626
Pakris Administrator	Can manage all appends of the Pabrin and Power DI products.	J3-J355-1226-4-74-5528-8-J-J-J1
Glabal Administrator Glabal Reader	Con manage all augmels of Microsoft Eulea ID and Microsoft according that our Microsoft Eulea id Con cood correlating that a Global Administrator was, but not update anglising.	62+58594-6565-4257-5458-8424774 62+65524-5466-4665-6746-4126++1
Global Sensor Annous Administrator	Create and manage all appeals of Global Senses Internet Assess and Microsoft Global Senses Peir	Ja494917-1269-46-1711-116651-
Global Scoore Assess Log Reader	Prusides designated sesseils personnel with read-only assess to setwork leaffin logs in Hisrons	10331061-73.4-0161-3-66-2-3.470
Graspa Administrator Garat Insiler	Membera of this cale was needle/manage groups, needle/manage groups nellings like naming and e Can insite goest succes independent of the members was insite goests' nelling.	5347-751-666-664-584-826526, 35-73183-35-8-6483-481
Helpdrah Administrator	Can rearl pannuarda for una-administratura and Helpdrok Administratura.	725827-5-5-14-4567-6646-5688645
Habrid Idealila Administrator	Hanage Antine Directory to Hineman's Entrantum provinceing, Hineman's Entra Consent, page	Bandfall4-Erna-42-a-5-63-5364-76
Mealily Goorenzoor Administrator Innights Administrator	Manage annen uning Minemenfi Entra ID for identify government normation. Nan administration annen in the Minemenft SES tonights app.	45383545-4882-4546-4582-437865 +6464-83-2452-4468-3663-474865
leniqhla Analqui	Assess the analytical magabilities in Hisraroff Vina benights and can under garries.	25469956-86-4-4149-4747-866824
Innights Danisess Leader	Can nieu and abare daubhuards and innights sia the Hisronnét SES lunights app.	31-333-4-3672-4736-3-28731813
Inter Administrator Int Design Administrator	Can manage all appents of the Inter-pendual. Penninian new toT denines, manage their lifengule, nunfigure neelifinales, and manage denine les	5.2.6246-5548-4284-8474-25.66** 2546248-4668-6484-9688-42
Kaisala Administrator	Can manage wellings for History of Kainala.	74-69756-6685-48-6-2542-6959941
Kunuledge Administratur	Can nonfigure boundedge, learning, and other intelligent featuren.	15.84.69-8945-4929-4599-8-29-62
Kanuledge Hanager Lineaue Administratur	Can arganiar, arrale, manage, and genuale lapins and basuledge. Can manage pendual liseaura on narra and genupa.	744-4468-557-4224-2462-8656574
LifengaleWarkflaus Administrator	Create and manage all appeals of worldflows and lauks associated with Lifengele Worldflows in Hi	594466911-6621-4571-11-5-9119-
Hennage Center Prinang Reader	Can read aroundly meanagen and updalen in Office 365 Hennage Center only.	an16+454-7624-48+8-an85-2456655
Hennage Center Reader Hinemosti 365 Dankop Administrator	Can read mennagen and updalen for libric organisalism in Office SES Hennage Center uniq. Dank up and centure united anemu unppueled new inco [ShacePoint, OneDeine, and Eunhauge Ont	758-1665-7674-1688-86-161655-
Hierenefi SES Higralies Administrator	Perform all migralion foundinuality to migrate number to Hinrounft SSS uning Higratius Hanager	8-81-836-36-4-4423-3343-2873843
Hierandi Entra Jaiord Draine Land Administra	Unrea anniqued to thin cute are added to the local administrature group on Hincourft Eutrajoined.	36862844-7344-4444-8884-6-46386 674434-5548-4753-6386-227885
Misrosofi Graph Dala Conseel Administrator Misrosofi Hardware Warranty Administrator	Manage augusts of Microsoft Graph Data Consent service in a tenant. Cerate and manage all augusts wave and polation and entitlements for Microsoft manufactured base.	
Hieranell Hardware Warranty Specialist	Create and read warranty ntains for Hisesouft wansfautured hardware, libe Surfaur and Hutute	2816-777-6628-4666-67-5-44-64-5
Helwerk Administrator Office Appa Administrator	Can manage nelwork localisms and centeu enterprine nelwork denign innights for Mineaus (1955). Can manage Office appointed occurrency including poling and nellings management, and manage the	257-86-2-8711-4417-6-58-64-6-6
Organizational Pranding Administrator	Manage all appeals of organizational branding in a trouble.	32-4146-434-4612-3723-6733-7
Organizational Data Source Administrator		\$478768a-8a4a-464a-a-a5-2-42462
Organizational Henrygen Appender	Sering and manage the ingrelian of requainational data into Microscott SSS. Renirus, appears, arrejest are organizational menagen for delivery in the Microscott SSS admin.	+48338+2-6464-4874-8634-4586725
Organizational Mennagen Weiler Partner Tiert Support	Weile, publish, manage, and review the organizational mennagen for end-onces through Hisconnell Do not one - and intended for general one.	46.55.4.527.455.6554.456452.
Parlace Tire2 Support	Do not non- and introduct for general non.	+11+16-C-47+5-C-G-5+16-65145-1
Passaged Administrator Propte Administrator	Can rearl passuards for use administrature and Passuard Administrature. Hanage profile photos of users and people wellings for all users in the organization.	56678748-5265-4727-56-2-8-5-486 8245864-64-5-45-8-8572-485564
Premiunium Management Administrator	Hanage all aspents of Historia February Permissions Hanagement.	.6784.52-664-4565-6-4-4428525
Planes Administrator	Hanage all appeals of the Hiseassell Planes service.	7868-021-2602-4692-5116-6412-26 11648597-9260-4669-5096-60-668
Power Platform Administrator Printer Administrator	Can needle and manage all appeals of Minesouf! Desamins 365, Power Appe and Power Antonale. Can manage all appeals of printers and printer nonnealnes.	\$44,6478-2286-4-28-6544-5644-5.
Printer Trabainian	Can register and unregister printers and update printer status.	-1
Prinileged Authentication Administrator Prinileged Rule Administrator	Can assess in sires, and and event authorities line without information for any core judgic or served	
Prinileged Role Administrator Reports Reader	Can manage enter anniquements in Minemont I Enter ID, and all appeals of Peiniteged Identity Manage Can read sign in and andit reports.	4.518665-4117-41-4-130813286
Search Administrator	Can arrair and manage all appeals of Hisrosoft Search wellings.	856665-5646-6476-3425-58-756
Srareb Edilor Sraerilg Administrator	Can arrain and manage the editorial number took as knobmarks, Q and An, tonations, Storeplan. Can erad around it information and exports, and manage configuration in Microsoft Eutra 10 and Q	1855251a-518a-4647-a5ar-6aa4561
Security Operator	Creates and manages prescrit proceds.	56222264-5745-4864-8445-4475561
Senneily Reader	Can read according information and reports in History Flavor ID and Office \$65.	54666647-4-74-4629-64-6-96986-5
Servior Support Administrator SharePoint Administrator	Can read arraine health information and manage appport linkels. Can manage all appeals of the Share Point presine.	68256481-1697-4656-5564-751-182 628-1658-66-7-4571-8186-6-1262
SharePoint Embedded Administrator	Hanage all appeals of SharePoint Embedded soulainees.	1,747816-0256-0761-18-1-3561745
Shape for Donineon Administrator	Can manage all appeals of the Shape for Positions product.	75341883-3152-4863-26-7-6316661
Trans Administrator Trans Communications Administrator	Can manage the Hinemonth Teams need inc. Can manage nulling and meetings features within the Hinemonth Teams need inc.	65854246-28+8-4-5644-8668751 6-4577656484565-62-4544-5-
Trans Communications Support Engineer	Can brookleshed summericalism issues wilkin Teams using advanced bads.	678338.4-6.48-4177-3-38-2178687
Trans Communications Support Specialist	Can breakbrokent annunciaalisen innern vilkin Trans oning kanin bede.	6.691111-11-1-11-11-15156111
Trans Draines Administrator Trans Reader	Can preform management related tasks on Trans overlifted desires. Read correptions in the Trans admin order, but out update anything.	34762454-1664-4396-8494-5549647 18764491-6949-4147-4999-4446564
Trans Telephong Administrator	Hanage union and belephong features and brookleshool nonmonicalise issues wilkin the Hisraroft	
Treasl Crealer	Creale and Historia Estea or Asser AD DZC Ireasts.	112-112-15-4-4182-55545686-4
Unage Summary Reports Reader Uner Administrator	Read Unage repuels and Adaptios Soure, but not't assens over delaits. Cas manage all aspents of overe and geosps, including ceartling passwords for limited admiss.	75334834-6+7+-4454-3347-4846445 6+3386+7-5+62-4746-3446-384345
Uner Emperieur Sauaren Hanager	View product feedback, accorderantle, and reports to find training and accommission apportunit	27468883-1461-4631-6832-3673643
Yirlad Yisila Administrator Yisa Glist Tracal Administrator	Hanage and abase Vielaal Visila information and meleion from admin or olers or the Vielaal Visila Hanage and monitore Himmonft Visa Glint wellings in the Himmonft SES admin or oler.	+38845+7-4-26-4255-5+66-6447865 8+456532-5846-4444-5+65-8577-47
Yina Gliel Tread Administrator Yina Guale Administrator	Manage and nonfigure Minemont! Yina Glin! nellings in the Minemont! 365 admin wester. Manage and nonfigure all appeals of Minemont! Yina Goals.	3248843-387-4-62-4863-14-1286
Yina Polor Administrator	Can manage all nellings for Hisesouff Vina Polor app.	87754647-4-42-4-63-5-44-32-4588
Windows SES Administrator	Can premision and manage all approle of Cloud PCs.	11451268-2262-45-6-2726-4528681
Windows Updale Deployment Administrator Yammer Administrator	Can arrain and manage all angents of Windows Update deployments through the Windows Update fo Hanage all angents of the Yammer arraine.	14175645-1134-4424-2241-4414-72

Microsoft's Privileged Azure AD Roles List (28) [PRIVILEGED]

- 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

Microsoft's Privileged Azure AD Roles List (28) [PRIVILEGED]

- 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

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. Sean Metcalf @PyroTek3 sean.metcalf@trustedsec.com

Level 1 Entra ID Roles (2 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
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.

Azure Privilege Escalation via Service Principal Abuse



Andy Robbins · Follow

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

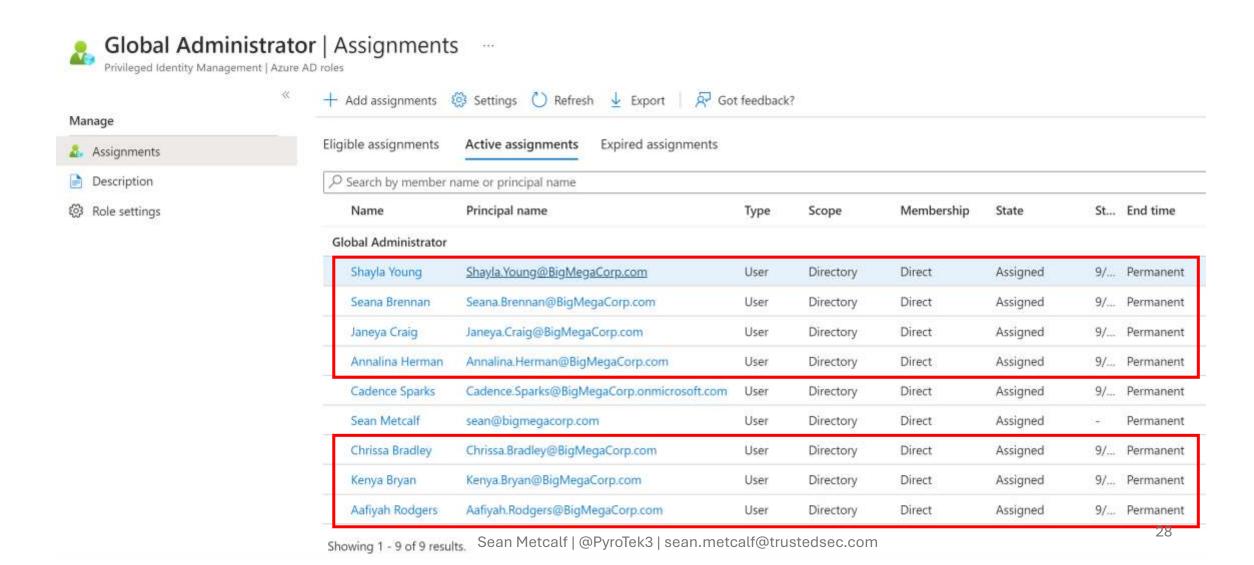
	Can a User with Role in Column A reset a password for a user with a Role in Row 2?													
	(No Role)	Global Administrator	Privileged Authentication Administrator	Helpdesk Administrator	Authentication Administrator	User Administrator	Password Administrator	Directory Readers	Guest Inviter	Message 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

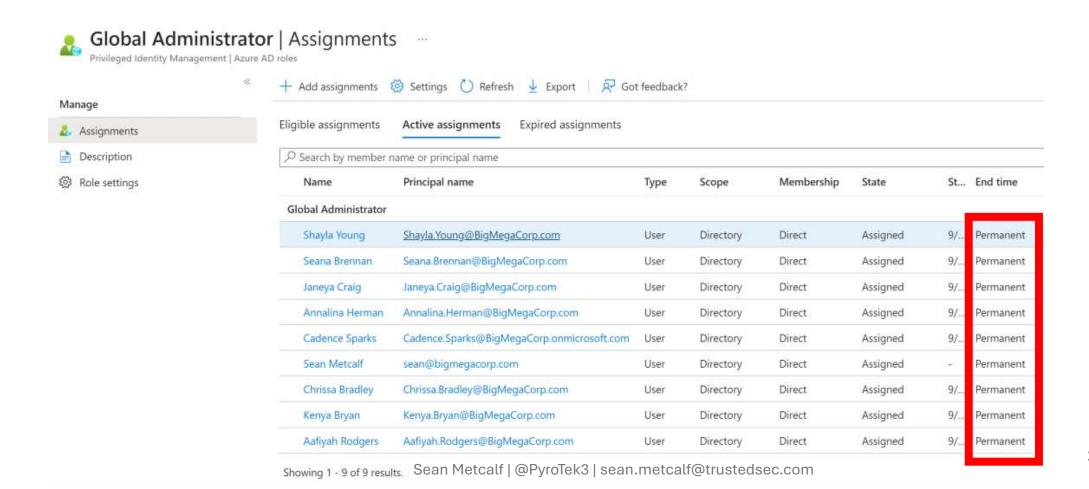


#5 Secure Privileged Role Membership

Highly Privileged User Accounts



PIM Members are Permanent, Not Eligible



Admin Accounts without MFA

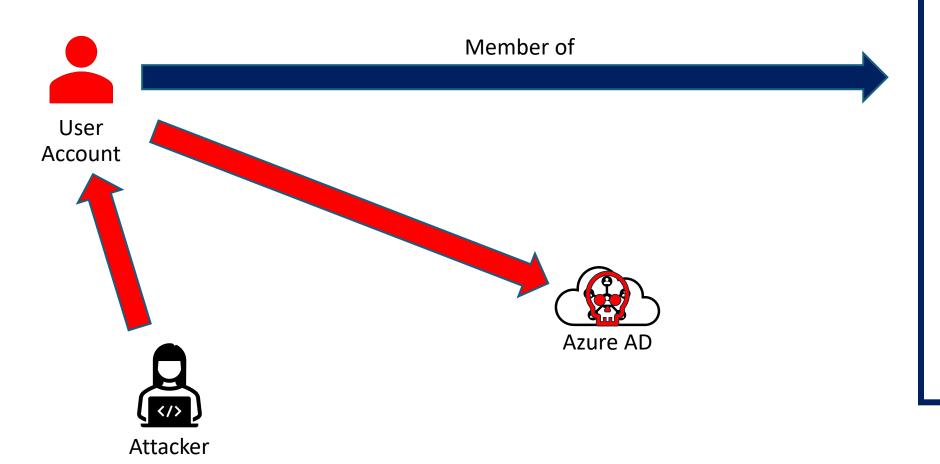
```
The Following Global Admin Account(s) have MFA Successfully Configured:

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.com
Kenya.Bryan@BigMegaCorp.com
Janeya.Craig@BigMegaCorp.com
Janeya.Craig@BigMegaCorp.com
Seana.Brennan@BigMegaCorp.com
Chrissa.Bradley@BigMegaCorp.com
Shayla.Young@BigMegaCorp.com
```

Overprivileged User





#6 Secure Role Assignable Groups



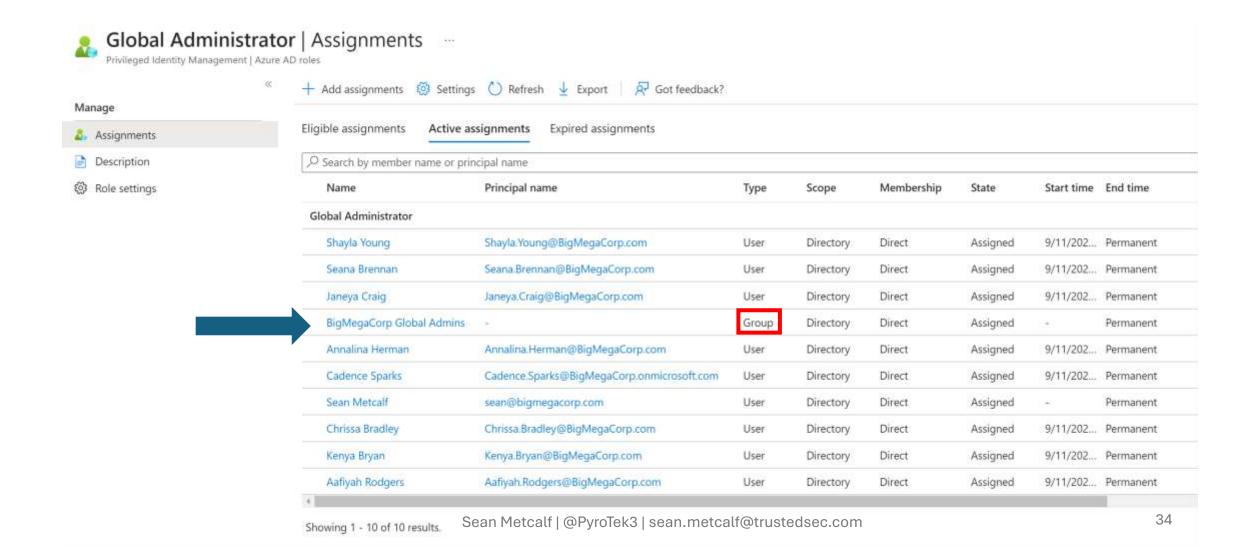
Role Assignable Groups (RAGs)

- Role Assignable Groups are Security or Microsoft 365 group with the is Assignable To Role 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).

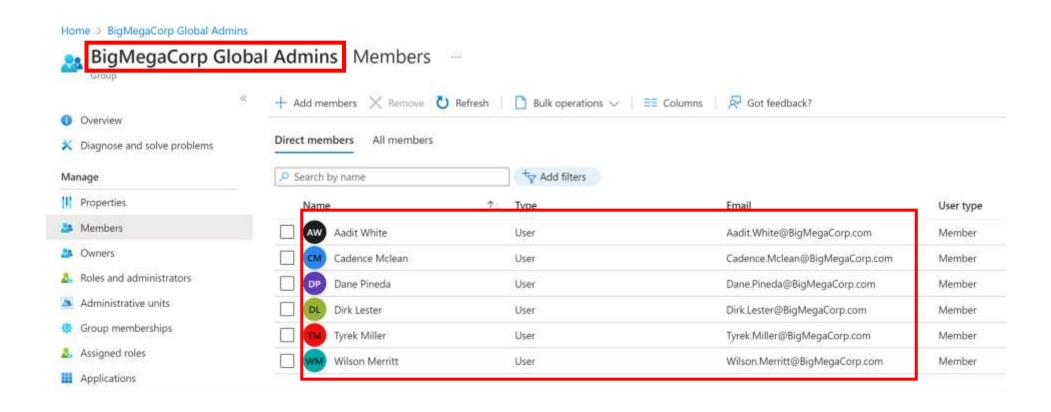
NOTE:

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.

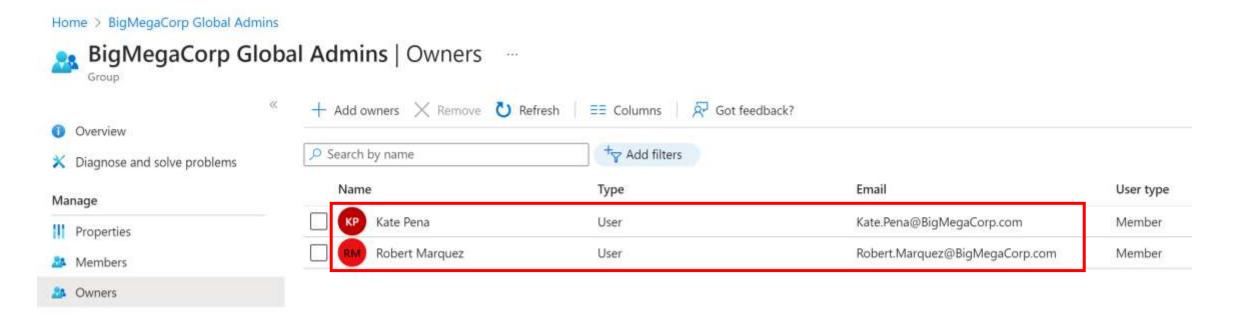
Privileged Roles with Group Nesting



Group Nesting – Have to Open Groups

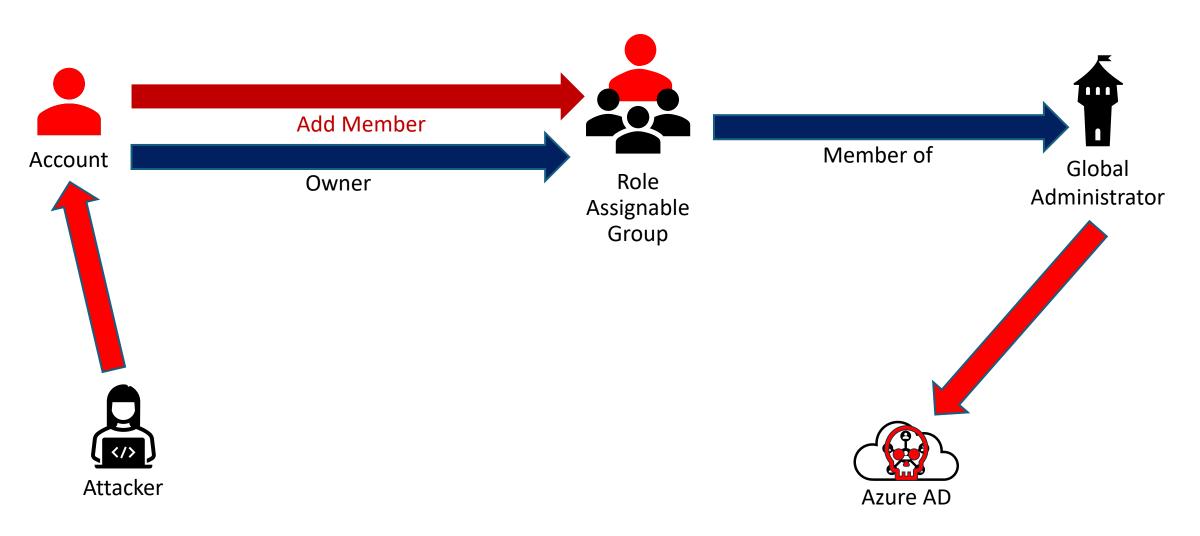


Role Assignable Group Owners



Role Assignable Group Owners can manage group membership

Compromise Azure AD through Role Assignable Group Owner Rights





Permissions Structure

OBJECT. ACCESS. CONSTRAINT

Examples:

Application.ReadWrite.All

Calendars.ReadWrite

Calendars.ReadWrite.All

Directory.ReadWrite.All

Mail.ReadWrite

Mail.Send

User.ReadWrite.All

Permissions Structure: Constraint

All

grants permission for the app to perform the operations on all of the resources of the specified type in a directory.

Shared

grants permission for the app to perform the operations on resources that other users have shared with the signed-in user. This constraint is mainly used with Outlook resources like mail, calendars, and contacts.

AppFolder

grants permission for the app to read and write files in a dedicated folder in OneDrive. This constraint is only exposed on Files permissions and is only valid for Microsoft accounts.

No constraint

the app is limited to performing the operations on the resources owned by the signed-in user.

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.

Reviewing Azure AD Permissions with PowerShell

```
PS C:\> Get-AzureADPSPermissions -ApplicationPermissions | Select ClientDisplayName,ResourceDisplayName,Permission
ClientDisplayName ResourceDisplayName
                                                  Permission
Trimarc RD TestApp Windows Azure Active Directory Device.ReadWrite.All
Trimarc RD TestApp Windows Azure Active Directory Member.Read.Hidden
Trimarc RD TestApp Windows Azure Active Directory Directory.ReadWrite.All
Trimarc RD TestApp Windows Azure Active Directory Domain.ReadWrite.All
Trimarc RD TestApp Windows Azure Active Directory Application.ReadWrite.OwnedBy
Trimarc RD TestApp Windows Azure Active Directory Application.ReadWrite.All
Trimarc KD TestApp Office 365 Exchange Unline
                                                  User.Kead.All
Trimarc RD TestApp Office 365 Exchange Online
                                                  Mail.ReadWrite
Trimarc RD TestApp Office 365 Exchange Online
                                                  MailboxSettings.ReadWrite
Trimarc RD TestApp Office 365 Exchange Online
                                                  Contacts.ReadWrite
Trimarc RD TestApp Office 365 Exchange Online
                                                  Mailbox.Migration
Trimarc RD TestApp Office 365 Exchange Online
                                                  Calendars.ReadWrite.All
Trimarc RD TestApp Office 365 Exchange Online
                                                  Mail.Send
Office 365 ASI App Office 365 Management APIs
                                                  ServiceHealth.Read
Office 365 ASI App Office 365 Management APIs
                                                  ActivityFeed.Read
```

Who are the Application Owners for TestApp?

```
PS C:\> Get-AzureADApplication -Objectid $appid | Select displayname,Objectid,appid
DisplayName
               ObjectId
                                                        AppId
Trimarc RD TestApp c8e9b6fe-cc98-4e90-8b7b-15fba500d49c 2f337e5f-8414-45a4-b48f-e0ec2014a1d4
PS C:\> Get-AzureADApplicationOwner -ObjectId $AppId
ObjectId
                                     DisplayName UserPrincipalName
                                                                           UserType
71575fad-39b2-475a-b519-314dde65e7cf Sean Metcalf sean@trimarcrd.com
                                                                           Member
13cf788e-baf0-4b1e-b9fa-46128a6468d0 Joe User
                                                  JoeUser@TrimarcRD.com
                                                                           Member
f4d30f9e-0837-4e3f-974e-ef282a2fcefe Darth Vader
                                                  DarthVader@TrimarcRD.com Member
f2a0fb99-bdaf-49ce-9192-9488ea5d3dae Boba Fett
                                                  BobaFett@TrimarcRD.com
                                                                           Member
```

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

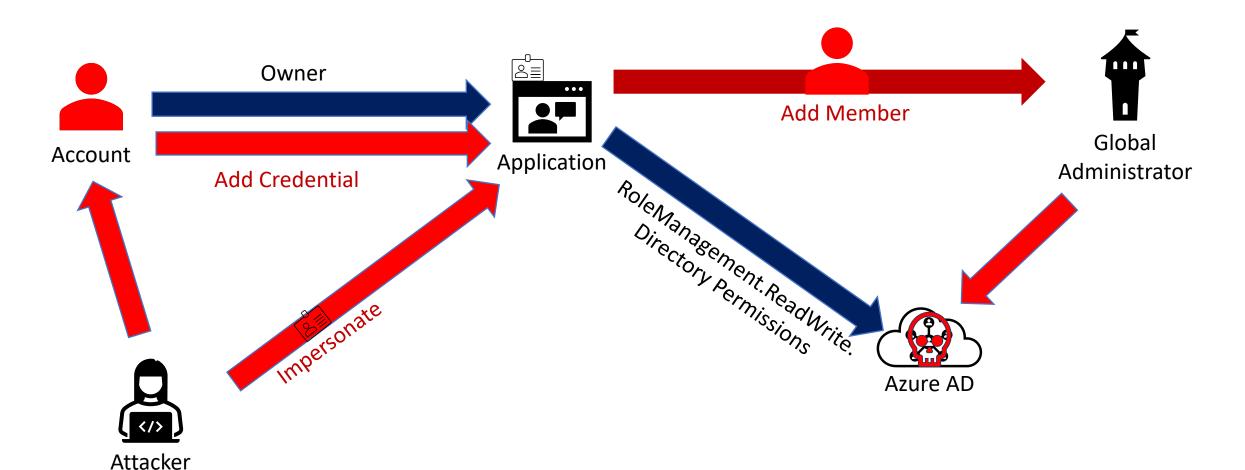


https://gist.github.com/psignoret/9d73b00b377002456b24fcb808265c23

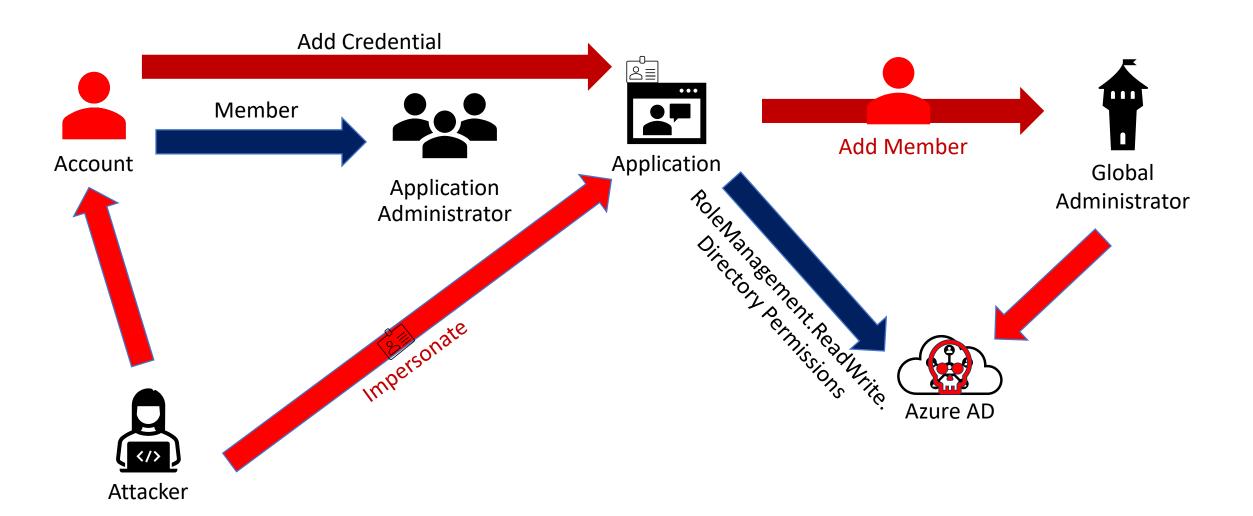
Application Escalation: Find the App Owner



Compromise Azure AD through Application Permissions



Compromise Azure AD through Application Permissions





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?



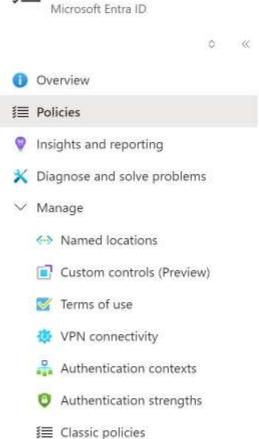






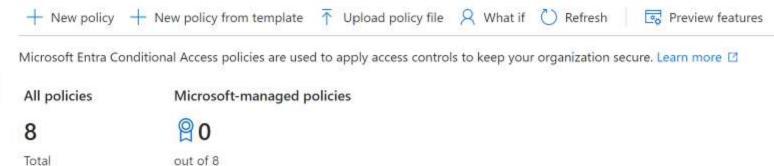


Conditional Access | Policies



Monitoring

> Troubleshooting + Support





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	

Got feedback?

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 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

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 <u>admins</u> accessing Microsoft <u>Admin Portals</u>
 - MFA for <u>per-user MFA</u> configured on users
 - MFA and reauthentication for <u>risky sign-ins</u>

Key Conditional Access Policies

Require	Require MFA for accounts with administrative roles (preferably FIDO2)
Block	Block legacy authentication (username & password authentication)
Block	Block location by geography
Block	Block device code flow*
Enforce	Enforce device compliance on all devices
Restrict	Restrict access to apps by location
Require	Require MFA for guest users

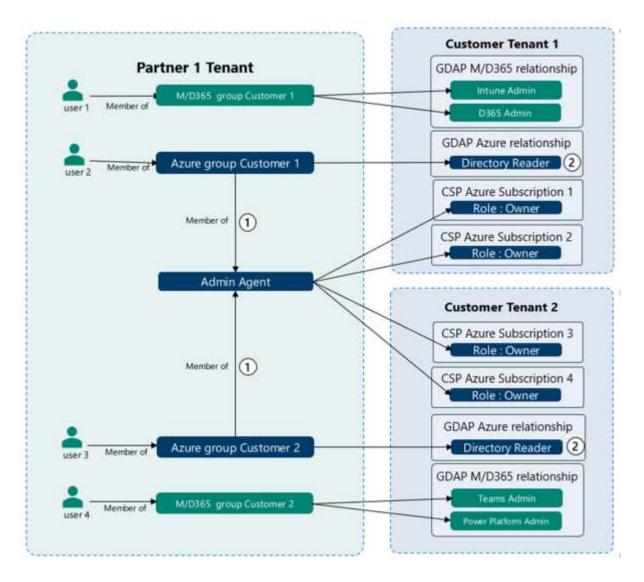


Partner Relationships – aka Delegated Administration

- 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 <u>only options</u>.
 - 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.

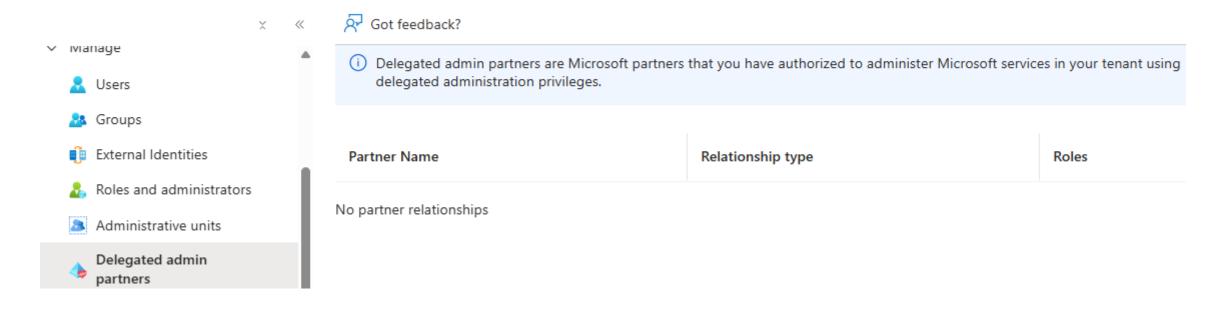
Shift to granular delegated admin privileges (GDAP) ASAP!

Move to Granular Delegated Admin Privileges (GDAP)

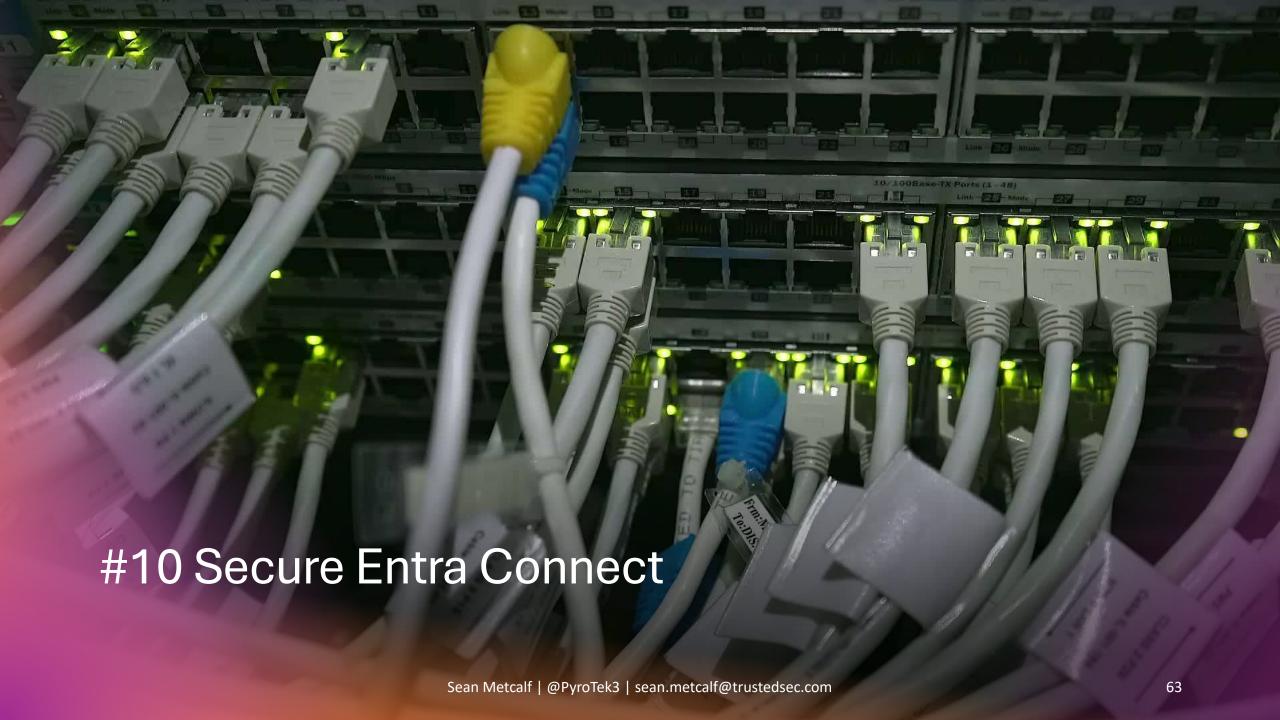


https://learn.microsoft.com/en-us/partner-center/gdap-introduction

Trimarc RD - BIG MEGA CORP | Delegated admin partners



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



Compromising Entra Connect (on-prem)



Compromise Active Directory



Get admin rights on Entra Connect server (or SQL db) OU admin rights
Local admin rights
GPO modify rights
Get local admin password on other systems (when not unique)



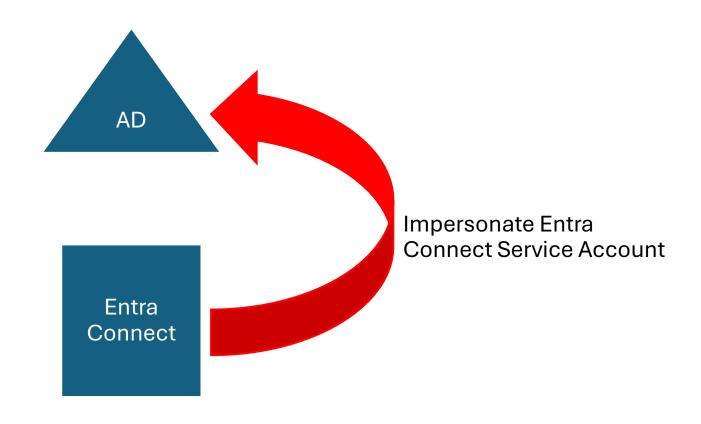
Gain control of management system

Microsoft SCCM (or similar) Vulnerability scanner

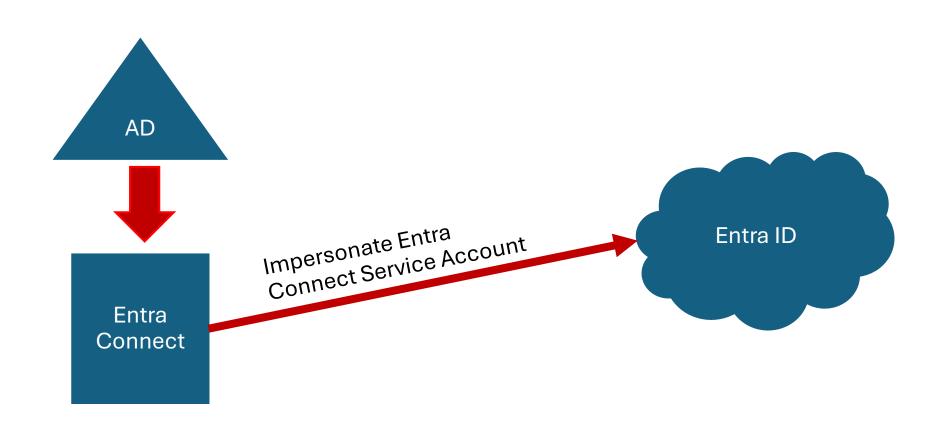


Compromise VMware (or other virtual platform)

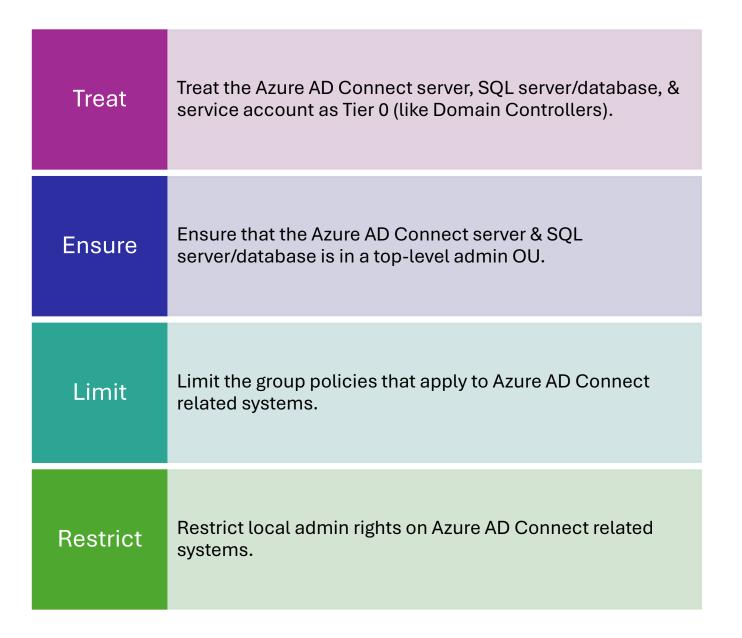
From Entra Connect to Active Directory



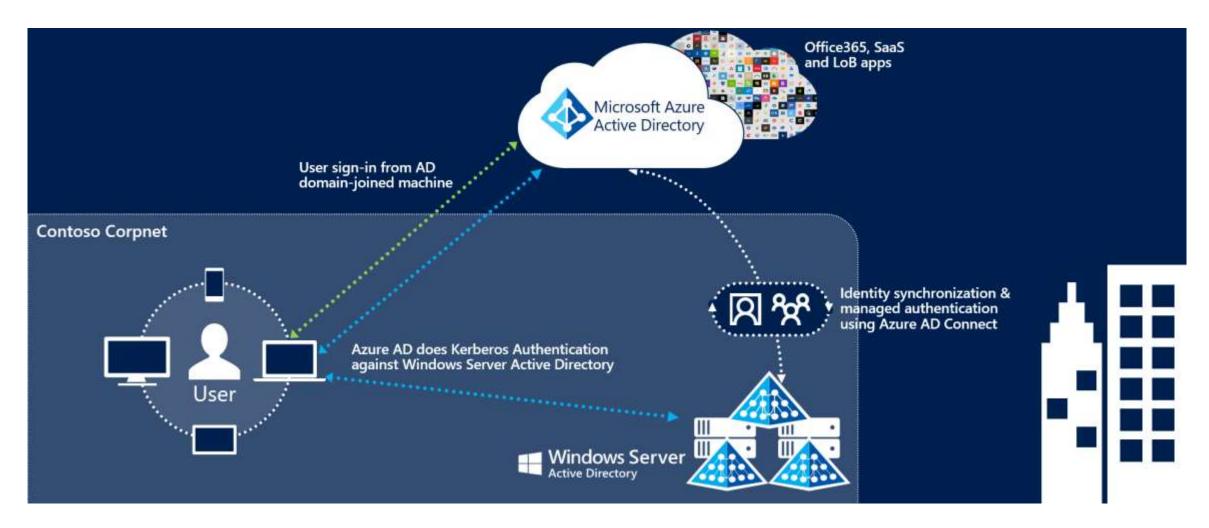
From Entra Connect to Entra ID



Defending Azure AD Connect



Securing Seamless Single Sign-On (SSSO)



Attacking Azure AD Seamless Single Sign-On

- Managed by Azure AD Connect
- "Azure AD exposes a publicly available endpoint that accepts Kerberos tickets and translates them into SAML and JWT tokens"
- Compromise the Azure AD Seamless SSO Computer Account password hash ("AZUREADSSOACC")
- Generate a Silver Ticket for the user you want to impersonate and the service 'aadg.windows.net.nsatc.net'
- Inject this ticket into the local Kerberos cache
- Azure AD Seamless SSO computer account password doesn't change

Securing
Seamless
Single Sign-On
(SSSO)



For Windows 10, Windows Server 2016, and later versions, it's recommended to use SSO via primary refresh token (PRT).

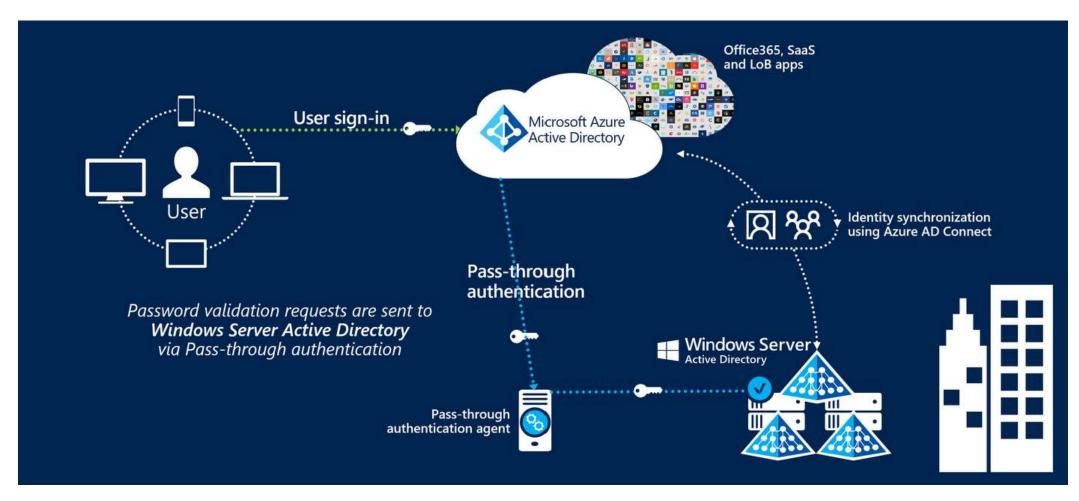


For Windows 7 and Windows 8.1, it's recommended to use Seamless SSO



Ensure the Azure AD Seamless Single Sign-On key (password) changes several times a year.

Microsoft Pass-Through Authentication (PTA)



https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Attacking Microsoft PTA



Managed by Azure AD Connect



Compromise server hosting PTA (typically Azure AD Connect server)



Azure AD sends the clear-text password (not hashed!) to authenticate the user.

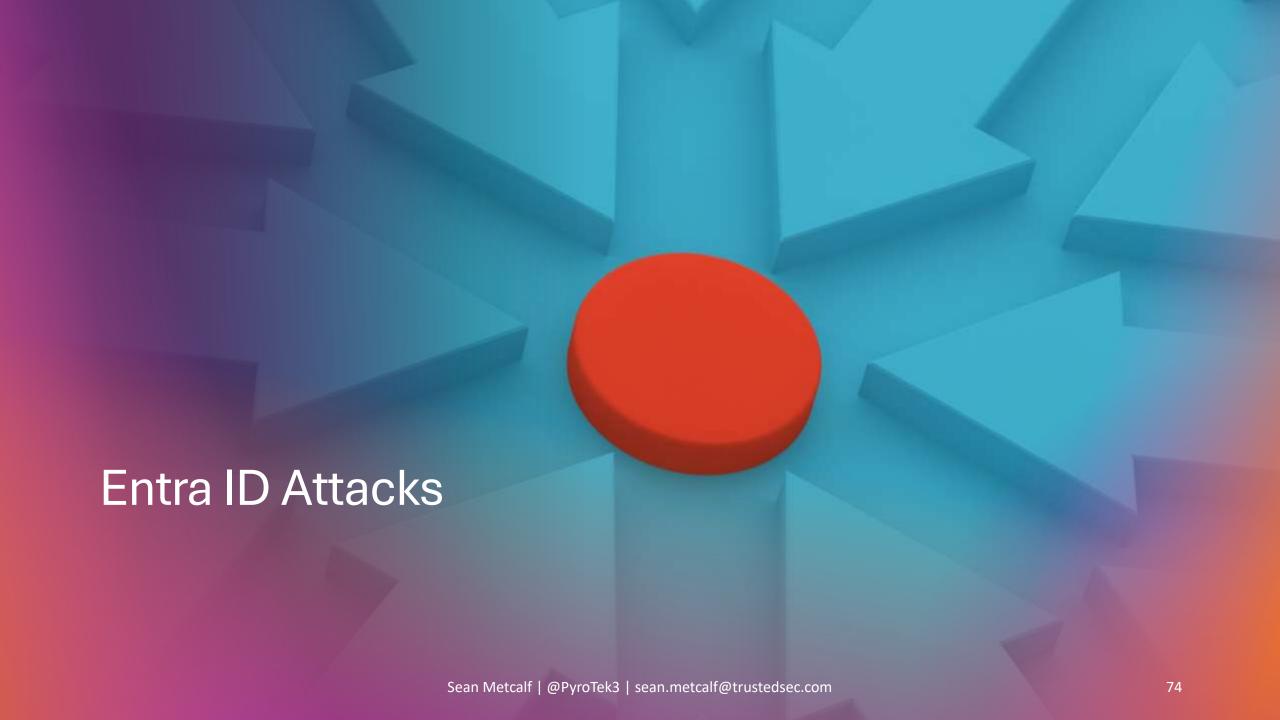


Inject DLL to compromise credentials used for PTA

Securing Pass Through Authentication (PTA)

 Treat Azure AD Connect as a Tier 0 asset (like a Domain Controller)

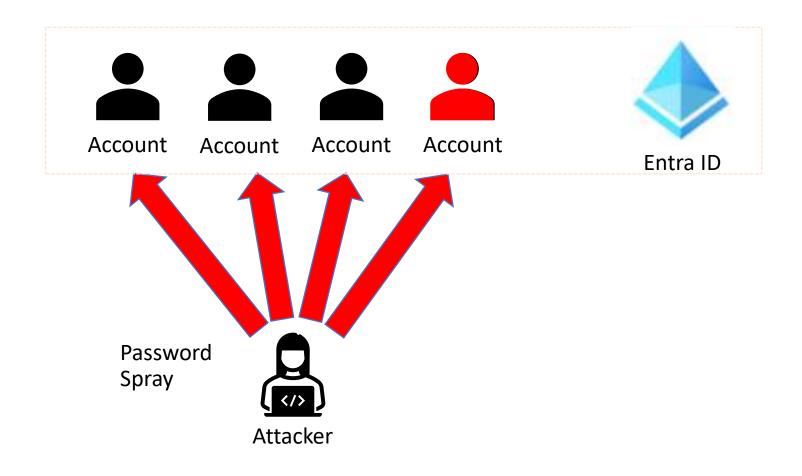




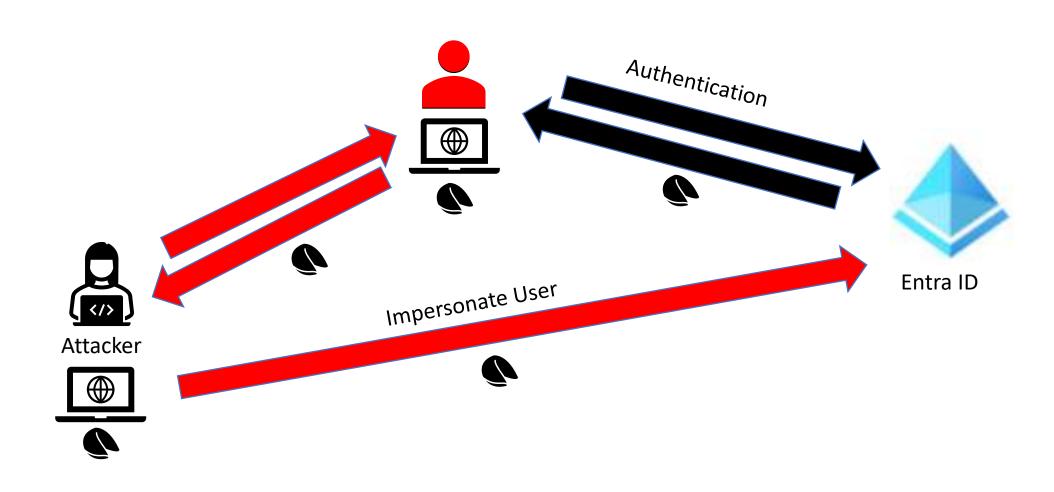
Attack Tools

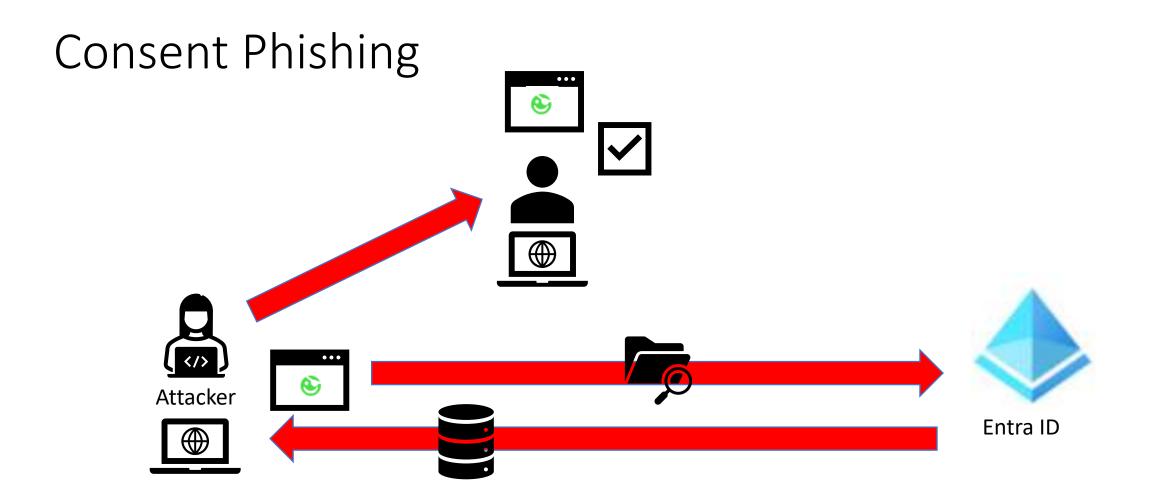
- AADInternals
- Evilginx2
- GraphRunner
- GraphSpy
- <u>Microburst</u>
- MFASweep
- MSOLSpray
- O365Recon
- Onedrive_user_enum
- ROADTools
- <u>Teamfiltration</u>
- <u>TokenTactics/TokenTactics2</u>

Password Spray Attack



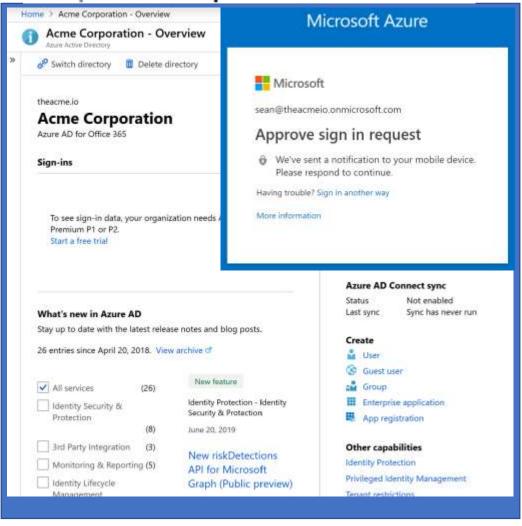
Token Theft & Replay

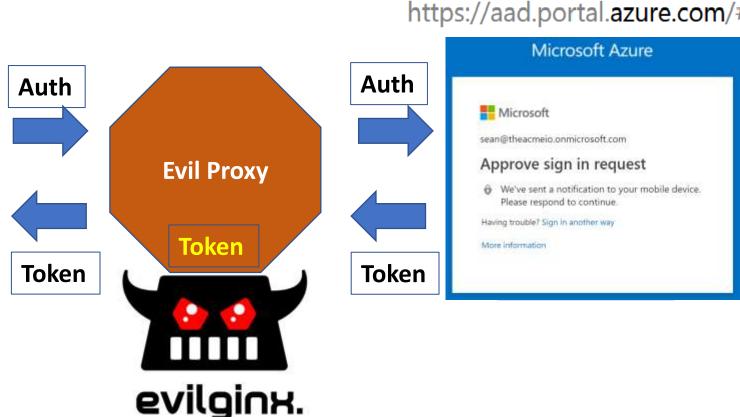




Token Theft with evilginx

https://aad.portalazure.com/

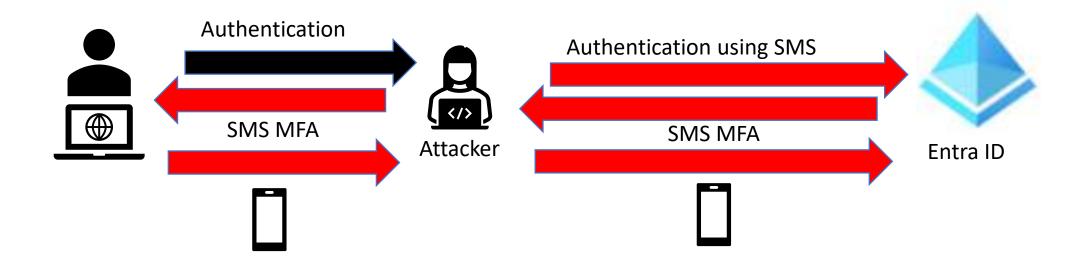




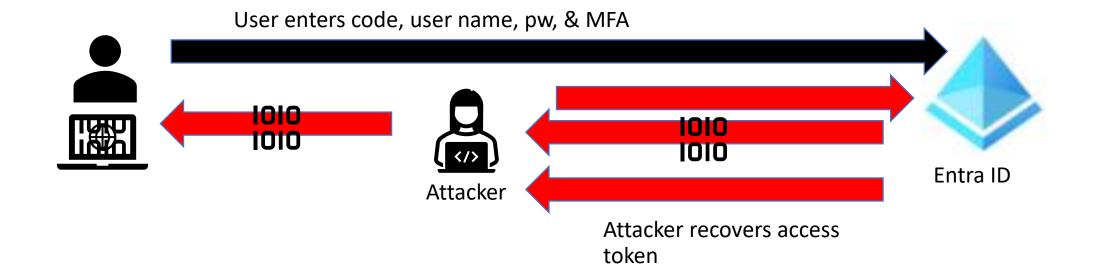
https://github.com/kgretzky/evilginx2

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

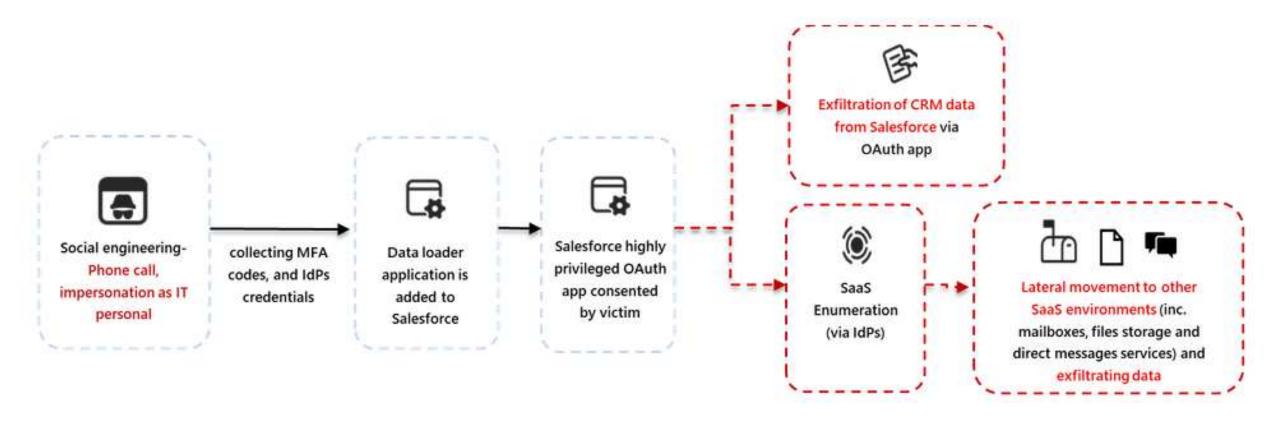
MFA Downgrade Attack



Device Code Flow Attack



Salesforce Oauth Attack



https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/protect-against-oauth-attacks-in-salesforce-with-microsoft-defender/4450584



Securing Entra ID - Microsoft Summary



Manage from Cloud controlled Devices

Use Azure AD Join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure, which can compromise device and security controls.



No on-prem account has Azure AD / Microsoft Office 365 privileges

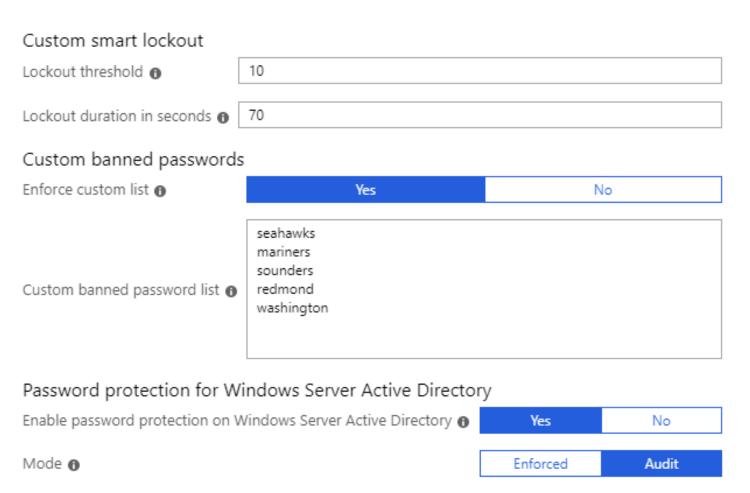
Privileged on-premises software must not be capable of impacting Azure AD privileged accounts or roles.



Use Azure AD cloud authentication to eliminate on-prem credential dependencies. Always use strong authentication, such as Windows Hello, FIDO, the Microsoft Authenticator, or Azure AD MFA.

On-Prem: Entra Password Protection

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



https://aka.ms/deploypasswordprotection

Phishing Defensive Layers

Require Users to MFA, preferably FIDO2

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
 People will fall to Phishing no matter what so we must monitor...

Key Cloud Administration Security Controls

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



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

Common Persistence Method Checks

Review Illicit Consent Grants
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

Key Mitigations

- Disable Device Code Flow <u>https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows</u>
- 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
 - Another browser (at a minimum)
 - Remote into a cloud admin server
 - 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)

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 Level 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 Level 0 & 1 roles
- 10. Scrutinize any applications with Level 0 Application permissions
- 11. Ensure that Conditional Access requires MFA for Level 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

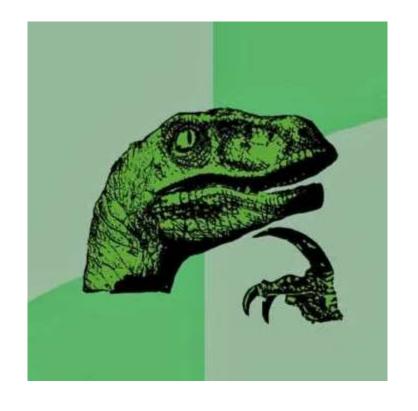


- <u>@TechBrandon</u> Brandon
- <u>@_dirkjan</u> Dirk-Jan
- <u>@EricaZellic</u> Erica Zellic
- @inversecos Inversecos
- @ITGuySoCal Joe Stocker
- <u>@Merill</u> Merill Fernando
- <u>ONathanMcNulty</u> Nathan McNulty



Sean's Entra ID Security List: <u>PyroTek.io/EntralDSecurityList</u>

Conclusion



Attacker cloud capability continues to evolve

Defender methods need to evolve as well

There are key mitigations that disrupt multiple attacks



Slides:

PyroTek.io/BSNoVa2025

Sean Metcalf

@PyroTek3

sean.metcalf@trustedsec.com

Security Articles, Slides, & Video:

ADSecurity.org



Questions?