

From User to Entra ID Admin

Sean Metcalf - @PyroTek3



TRIMARC

About

- Founder & CTO @ Trimarc ([Trimarc.co](https://trimarc.co)), a professional services company that helps organizations better secure their Microsoft Identity systems (Active Directory & Entra ID).
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, Blue Team Con, BSides Charm, BSides DC, BSides PR, DEFCON, DerbyCon, TEC, Troopers
- Former Microsoft MVP
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org (Microsoft identity security info)



Agenda

- Introduction
- Entra ID Highly Privileged Roles & Applications
- Entra ID Security Posture
- Conditional Access Policy & CAP Gaps
- Attacking Entra ID
- Microsoft Blizzard (Midnight Blizzard Attack on Microsoft)
- Securing Entra ID Administration
- Conclusion



Entra ID Level 0

Like Tier 0, but Different!

There are >100 Entra ID Roles!

Role	Description	Template ID
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	3b635d32-2cd3-44c7-3d02-65cc2d5ea5c3
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	c1fc39d5-3621-4004-97cb-879684dced7c
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	3c5-d0192-1a7c-44d3-9c195-66db2d42a58f
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	4c30b336-c635-46cc-36f3-d01b78bb62a
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.	58a13c39-c632-46ae-3ee0-9c0d43cd7f3d
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.	ff452f53-38dc-465c-891d-fc073ab5398f
Attribute Definition Administrator	Define and manage the definition of custom security attributes.	8424-c6f0-1b93-439c-bb40-26c1753c96d4
Attribute Definition Reader	Read the definition of custom security attributes.	1d336d2c-4ae8-42ef-8711-b3604ce3fc2c
Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attributes.	5b784334-f34b-471b-3387-c7219fc43c2d
Attribute Log Reader	Read audit logs related to custom security attributes.	3c95333d-8186-4d04-835f-4d1ef9a2dced
Authentication Administrator	Can access to view, set, and reset authentication method information for any non-admin user.	4c33b3b9-1100-46d0-9d65-fb560da0071f
Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	25a16ed-2f0a-40ca-92d0-12323c21473a
Authentication Policy Administrator	Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and ve	0526716b-113d-4c15-b2c8-68a3c22b3f80
Azure DevOps Administrator	Can manage Azure DevOps policies and settings.	c3373b-df-4387-439c-837a-ba8e231c7286
Azure Information Protection Administrator	Can manage all aspects of the Azure Information Protection product.	7435fd4-34c4-4d15-e269-38788cc339fd
B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	3af43236-0c0d-445f-883a-6355382cc081
B2C IEF Policy Administrator	Can create and manage trust framework policies in the Identity Experience Framework (IEF).	3edaf663-341e-44175-3934-5c339af6c070
Billing Administrator	Can perform common billing related tasks like updating payment method information.	b0f54661-2d74-4c50-af3c-1ec003f12efc
Cloud App Security Administrator	Can manage all aspects of the Defender for Cloud Apps product.	892c5842-936e-463a-8041-72aa08cc3c6e
Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except application proxy.	158c047a-c907-4556-b7af-446551b6b5f7
Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	7636f772-787b-43c8-901f-6046b08affd2
Compliance Administrator	Can read and manage compliance configuration and reports in Microsoft Entra ID and Microsoft 365.	17315797-102d-40b4-33c0-432062ccca18
Compliance Data Administrator	Creates and manages compliance content.	c6f1a23a-d311-4be4-9570-befc86d067a7
Conditional Access Administrator	Can manage Conditional Access capabilities.	b1b61c3c-b65d-4f19-8427-16fa0d97b1c3
Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data.	5c4f93cd-41dc-4d7f-b63a-9c4207bfc39f
Desktop Analytics Administrator	Can manage and manage Desktop management tool and services.	38a3e43f-2bdf-414d-8a6c-5d6db9bace14
Directory Readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	88d8c3c3-8f55-451e-953a-9b3838b8876b
Directory Synchronization Accounts	Only used by Microsoft Entra Connect service.	d2362b05-8046-44ba-8758-162e162cf332
Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	3360fcb5-f418-4b3a-8175-c2a00bac4301
Domain Name Administrator	Can manage domain names in cloud and on-premises.	8329153b-31d0-4727-b345-745eb3bc5f31
Dynamics 365 Administrator	Can manage all aspects of the Dynamics 365 product.	44367163-bba1-44c3-38af-f5787879f96a
Dynamics 365 Business Central Administrator	Can access Dynamics 365 Business Central environments and perform all administrative tasks on the environments.	3653737b-b63b-4cdc-8c63-5878b3f32a3f
Edge Administrator	Manage all aspects of Microsoft Edge.	3f9f6ac-fa04-443e-3b63-10302c854a4f
Exchange Administrator	Can manage all aspects of the Exchange product.	29232cdf-3323-42f4-9dc2-1d079f3c4d4e
Exchange Recipient Administrator	Can create or update Exchange Online recipients within the Exchange Online organization.	31332f7b-586e-42d1-3346-c5345a2cc4e
External ID User Flow Administrator	Can create and manage all aspects of user flows.	6c531065-3bad-43cd-30f3-c9424366d2f0
External ID User Flow Attribute Administrator	Can create and manage the attribute schema available to all user flows.	0f971ee3-41eb-4563-a71c-57bb83ceff1e
External Identity Provider Administrator	Can configure identity providers for use in direct federation.	b62f45a1-457d-42af-a067-6cc1f63bc45
Fabric Administrator	Can manage all aspects of the Fabric and Power BI products.	c3e8339c-122f-4c74-3520-8dcdd192828c
Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	62c30394-69f5-4231-9190-01e11745c10
Global Reader	Can read everything that a Global Administrator can, but not update anything.	3f9c332c-3a0b-483d-bcf7-f126c114c451
Global Secure Access Administrator	Create and manage all aspects of Microsoft Entra Internal Access and Microsoft Entra Private Access, including managin	ac434307-12b3-4f1a-1708-88bf58cabcf1
Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and v	ffdd7a71-b60b-444a-384c-02652f8f8f1c
Guest Inviter	Can invite guest users independent of the 'members can invite guests' setting.	35c73109-35c0-4d8e-aeec-d0faccf2d47b
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	723627c3-3c14-43f7-bb1b-3608f156bbb8
Hybrid Identity Administrator	Can manage Active Directory to Microsoft Entra cloud provisioning, Microsoft Entra Connect, Pass-through Authentica	8ac3fcd4-6cca-42ea-3e63-594c47b60cb2
Identity Governance Administrator	Manage access using Microsoft Entra ID for identity governance scenarios.	4589d3c5-c802-45c6-b32a-1d70b5c186e6
Insights Administrator	Has administrative access in the Microsoft 365 Insights app.	4f44e8d-2d43a-4f09-39b8-fcd65a507e7e
Insights Analyst	Access the analytical capabilities in Microsoft Viva Insights and run custom queries.	25d335f-86cb-4119-b711-0f02d2a207c9
Insights Business Leader	Can view and share dashboards and insights via the Microsoft 365 Insights app.	31c333d-3672-4796-3c2e-873181342d2d
Intune Administrator	Can manage all aspects of the Intune product.	3a2c62db-5318-4204-8d74-23affec5d9d5
Kaizala Administrator	Can manage settings for Microsoft Kaizala.	74cf975b-6605-40af-5d42-b953d836353
Knowledge Administrator	Can configure knowledge, learning, and other intelligent features.	b5a8d3f3-03d5-43a3-a633-8c29cf291470
Knowledge Manager	Can organize, create, manage, and promote topics and knowledge.	744cc460-337c-42ad-a462-8b3f9747a02c
License Administrator	Can manage product licenses on users and groups.	4d6cc14f-3453-4180-bef9-9c0e3917313
Lifecycle Workflows Administrator	Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra ID.	53d4f688-662b-457b-bc4b-5c380945308f
Message Center Privacy Reader	Can read security messages and updates in Office 365 Message Center only.	ac16e43d-7b2d-4d0c-ac05-243f356ab5b
Message Center Reader	Can read messages and updates for their organization in Office 365 Message Center only.	730c1fb3-7f7d-4f88-86a1-cf1f95c05cb
Microsoft 365 Migration Administrator	Perform all migration functionality to migrate content to Microsoft 365 using Migration Manager.	8c8b803f-36c1-4123-9349-20738d3f9652
Microsoft Entra Joined Device Local Administ	Users assigned to this role are added to the local administrators group on Microsoft Entra joined devices.	3f06204d-73c1-4d4c-880a-6cd30606fd8
Microsoft Hardware Warranty Administrator	Create and manage all aspects warranty claims and entitlements for Microsoft manufactured hardware, like Surface and Ho	1501b317-7653-4ff3-94b5-203caf33784f
Microsoft Hardware Warranty Specialist	Create and read warranty claims for Microsoft manufactured hardware, like Surface and HoloLens.	28f1f77f-bb20-4fbb-b7a3-c6c6c5b0439f
Modern Commerce Administrator	Can manage commercial purchases for a company, department or team.	4d4e45f7-156f-4070-844b-2666f266b6e
Network Administrator	Can manage network locations and review enterprise network design insights for Microsoft 365 Software as a Service ap	d37c8bcd-0711-4417-bc38-b4ab66cc4c2
Office Apps Administrator	Can manage Office apps cloud services, including policy and settings management, and manage the ability to select, unsele	2b745bdf-0803-4d80-3a65-822c4433d3ac
Organizational Branding Administrator	Manage all aspects of organizational branding in a tenant.	32cd04bf-c34a-4b82-9723-b739a7a4c178
Organizational Messages Approver	Review, approve, or reject new organizational messages for delivery in the Microsoft 365 admin center before they are se	c48398c2-f4bb-4074-8f31-4586725c205b
Organizational Messages Writer	Write, publish, manage, and review the organizational messages for end-users through Microsoft product surfaces.	507f53c4-4c52-4077-abd3-d2e1558b6ca2
Partner Tier1 Support	Do not use - not intended for general use.	4b639c4d-527c-439b-b33d-d9b432c50246
Partner Tier2 Support	Do not use - not intended for general use.	000c864f-11f5-44ab-3c06-fb35a5b0d49
Password Administrator	Can reset passwords for non-administrators and Password Administrators.	36e707d0-3265-4727-3b2c-8c3a107fb3d4
Permissions Management Administrator	Manage all aspects of Microsoft Entra Permissions Management.	a7f8dc32-cf4d-46f9-ba4c-4428526346b5
Power Platform Administrator	Can create and manage all aspects of Microsoft Dynamics 365, Power Apps and Power Automate.	11648597-326c-4cf3-3c36-bccbb03b8dcc
Printer Administrator	Can manage all aspects of printers and printer connectors.	644cf478-c28f-4e28-b3dc-3fdd63a30bf7
Printer Technician	Can register and unregister printers and update printer status.	8cccf6f1-c4bd-4cc8-bc07-4b8d950f4477
Privileged Authentication Administrator	Can access to view, set, and reset authentication method information for any user (admin or non-admin).	7bc44c8a-9daf-4e2a-84d6-abe2643c08a13
Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.	c8e11b6b-c163-4658-34c1-60213ab1f914
Reports Reader	Can read sign-in and sign-up reports.	4c5d8f65-41de-4d4d-9386-c035e55335cf
Search Administrator	Can create and manage all aspects of Microsoft Search settings.	09c4bb5c-9b3d-4d7b-a239-59a734862a40
Search Editor	Can create and manage the editorial content such as bookmarks, Q and A, locations, floorplan.	8835291a-318c-4fd7-a3ce-faa4390cf7d9
Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.	194ae4cb-b126-40b2-bd5b-603fb38097fd
Security Operator	Creates and manages security events.	5f2222b1-57c3-48ba-8d45-d4753f1d4cf
Security Reader	Can read security information and reports in Microsoft Entra ID and Office 365.	5d6b6bb7-dc71-4623-b4af-9c380a3c52503
Service Support Administrator	Can read service health information and manage support tickets.	1023c481-a637-4b56-39fd-19fbcc0226033
SharePoint Administrator	Can manage all aspects of the SharePoint service.	12b1f50f6a1-4571-818b-6a12f2a5b6c
Slype for Business Administrator	Can manage all aspects of the Slype for Business product.	75341009-315c-4863-ab7-631bf18273e
Teams Administrator	Can manage the Microsoft Teams service.	63031246-20c8-4a56-aa4d-066075b2a7a8
Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.	baf37b3a-610c-45d9-366d-d9d1f5c8314b
Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.	f70338a0-fc10-4177-3a30-2178f8765737
Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.	ref31038-03a3-41a3-b5ba-6f0cc818a12
Teams Device Administrator	Can perform management related tasks on Teams certified devices.	3d762c5a-1b6c-430f-843c-553bc42923d4
Tenant Creator	Create new Microsoft Entra or Azure AD B2C tenants.	11c3ca8d-15ad-4f02-335c-426bca473a6a
Usage Summary Reports Reader	Read Usage reports and Adoption Score, but can't access user details.	7534001a-6c7e-415c-396b-49d4bd49c876c
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	f6300eb7-5a62-47db-91af-98c3a3a338b1
Virtual Visits Administrator	Manage and share Virtual Visits information and metrics from admin centers or the Virtual Visits app.	c300d9c7-4a2b-4235-3eff-f1c78b36cc38
Viva Goals Administrator	Manage and configure all aspects of Microsoft Viva Goals.	32b086b3-c367-4cf2-b863-1dc128fb386e
Viva Pulse Administrator	Can manage all settings for Microsoft Viva Pulse app.	87761b17-1ed2-4af3-3acd-32a150038160
Windows 365 Administrator	Can provision and manage all aspects of Cloud PCs.	11451d60-ccb2-45eb-17d6-43d0f0125c13
Windows Update Deployment Administrator	Can create and manage all aspects of Windows Update deployments through the Windows Update for Business deploym	32636413-001b-469c-378c-cc0f6b3620d2
Yammer Administrator	Manage all aspects of the Yammer service.	810c2642-034-447f-a5c8-41bcaa378541

Microsoft's Privileged Entra ID Roles List [PRIVILEGED]

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

As of:
4/22/2024

Microsoft's Privileged Entra ID Roles List [PRIVILEGED]

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

As of:
4/22/2024

Trimarc 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.”*

Trimarc 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.

Trimarc 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>

From TEC 2022

Background

Highly Sensitive Application Permissions:

- Directory.ReadWrite.All: Effective Global Admin rights to AAD
- RoleManagement.ReadWrite.Directory: Ability to add members to Global Administrator and other roles
- Application.ReadWrite.All: Provides full rights to applications which could result in compromise if there are apps with highly privileged permissions
- AppRoleAssignment.ReadWrite.All: Provides the application the right to grant additional permissions to itself!

<https://learn.microsoft.com/en-us/graph/permissions-reference>

Trimarc 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.

Entra ID Security Posture

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com



Unfortunate Defaults



Users:

- Can register applications
- Can consent to applications
- Can create new tenants
- Can join/hybrid join devices to the tenant & no MFA is required



Guests/External Accounts

- Guests have the same view rights as users
- Guests can invite other guests

Entra ID Common Security Issues

Privileged Account Issues

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

Applications with Highly Privileged Permissions

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


Group Nesting

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

Partner Access - Delegated Access Permissions




- Global Administrator
- Helpdesk Administrator

Highly Privileged User Accounts

 **Global Administrator** | Assignments ...
Privileged Identity Management | Azure AD roles

<< + Add assignments ⚙ Settings 🔄 Refresh ↓ Export 🗨 Got feedback?

Manage


-  Assignments
-  Description
-  Role settings

Eligible assignments **Active assignments** Expired assignments

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

Showing 1 - 9 of 9 results. Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

PIM Members are Permanent, Not Eligible

 **Global Administrator** | Assignments ...
Privileged Identity Management | Azure AD roles

« + Add assignments ⚙ Settings ↻ Refresh ↓ Export | 🗨 Got feedback?

Manage

- Assignments
- Description
- Role settings

Eligible assignments **Active assignments** Expired assignments

🔍 Search by member name or principal name

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

Showing 1 - 9 of 9 results. Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

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.onmicrosoft.com

Kenya.Bryan@BigMegaCorp.com

Janeya.Craig@BigMegaCorp.com

Annalina.Herman@BigMegaCorp.com

Seana.Brennan@BigMegaCorp.com

Chrissa.Bradley@BigMegaCorp.com

Shayla.Young@BigMegaCorp.com


Role Assignable Groups (RAGs)

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

NOTE:




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

Privileged Roles with Group Nesting


 **Global Administrator** | Assignments ...
Privileged Identity Management | Azure AD roles

« [+ Add assignments](#) [Settings](#) [Refresh](#) [Export](#) | [Got feedback?](#)

Manage

-  **Assignments**
-  Description
-  Role settings

Eligible assignments **Active assignments** Expired assignments

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

Showing 1 - 10 of 10 results. Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Group Nesting – Have to Open Groups

Home > BigMegaCorp Global Admins

BigMegaCorp Global Admins Members

Group

+ Add members × Remove ↺ Refresh 📄 Bulk operations Columns 🗨 Got feedback?







Overview
Diagnose and solve problems

Manage

Properties
Members
Owners
Roles and administrators
Administrative units
Group memberships
Assigned roles
Applications

Direct members All members

Search by name Add filters

	Name	Type	Email	User type
<input type="checkbox"/>	 Aadit White	User	Aadit.White@BigMegaCorp.com	Member
<input type="checkbox"/>	 Cadence Mclean	User	Cadence.Mclean@BigMegaCorp.com	Member
<input type="checkbox"/>	 Dane Pineda	User	Dane.Pineda@BigMegaCorp.com	Member
<input type="checkbox"/>	 Dirk Lester	User	Dirk.Lester@BigMegaCorp.com	Member
<input type="checkbox"/>	 Tyrek Miller	User	Tyrek.Miller@BigMegaCorp.com	Member
<input type="checkbox"/>	 Wilson Merritt	User	Wilson.Merritt@BigMegaCorp.com	Member

Role Assignable Group Owners



Home > BigMegaCorp Global Admins

BigMegaCorp Global Admins | Owners

Group

« + Add owners ✕ Remove ↺ Refresh ≡ Columns 🗨 Got feedback?

🔍 Search by name + Add filters

	Name	Type	Email	User type
<input type="checkbox"/>	 Kate Pena	User	Kate.Pena@BigMegaCorp.com	Member
<input type="checkbox"/>	 Robert Marquez	User	Robert.Marquez@BigMegaCorp.com	Member

Manage

- Overview
- Diagnose and solve problems
- Properties
- Members
- Owners

Role Assignable Group Owners can manage group membership

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



Privileged Role Administrator | Assignments ...

Privileged Identity Management | Microsoft Entra roles

Manage

Assignments

Description

Role settings

+ Add assignments ⚙ Settings ↻ Refresh ↓ Export | 🗨 Got feedback?

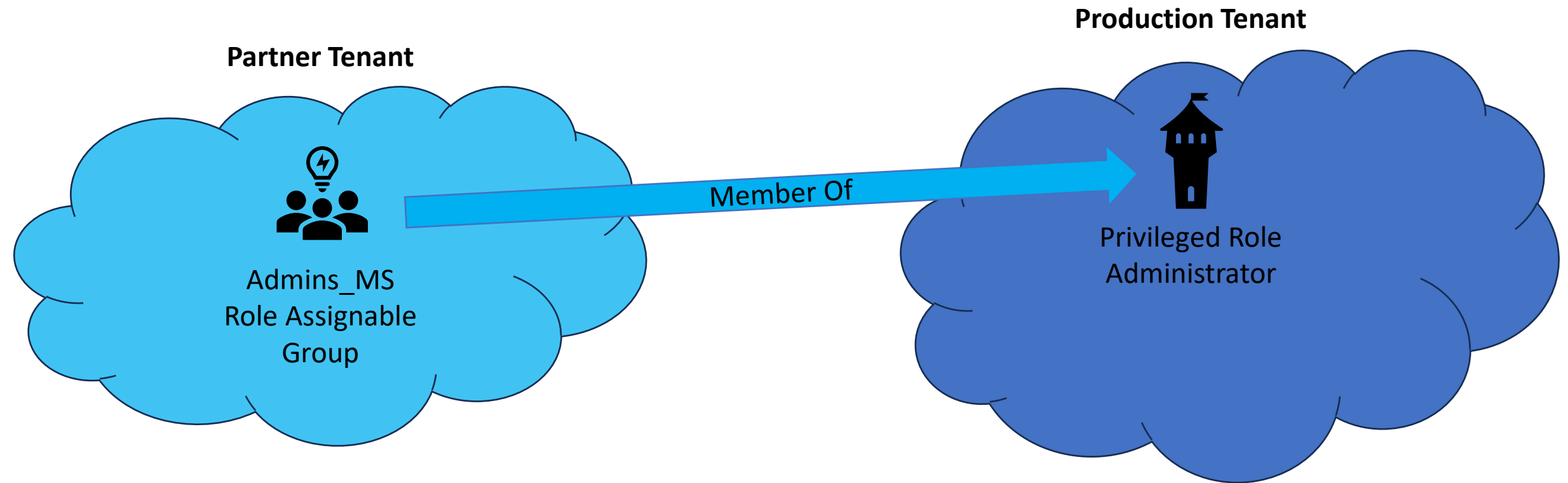
Eligible assignments Active assignments Expired assignments

🔍 Search by member name or principal name

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

Showing 1 - 2 of 2 results.

Privileged Role with Group in another Tenant



Role Group Member Not Shown in PS

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

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

```
PS C:\Data\_MCSA>
```



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?



Signal



Decision



Enforcement

Identities



Microsoft
Entra ID



Microsoft
Defender
for Identity

Endpoints



Microsoft
Defender



Microsoft
Endpoint
Manager

Applications



Microsoft
Defender for
Cloud

Data



Microsoft
Information
Protection

Infrastructure



Microsoft
Cloud App
Security

Network



◊ << + New policy + New policy from template ↑ Upload policy file 👤 What if ↺ Refresh | ⚙️ Preview features | 🗨️ Got feedback?

Overview

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication contexts

Authentication strengths

Classic policies

Monitoring

Troubleshooting + Support

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

All policies

8

Total

Microsoft-managed policies

0

out of 8

Search

Add filter

8 out of 8 policies found

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

Common Conditional Access Policies



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



Require MFA for users with certain administrative roles



Block legacy authentication (username & password auth)



Block/Grant access from specific locations

CA Policy Gap #1:

Users Require MFA Only Outside of Corp Network

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

CA Policy Gap #2:

Admins don't require MFA

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

CA Policy Gap #3:

Exclusions

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

Microsoft Provided Conditional Access Policies



Baseline Policies



Conditional Access Templates



Microsoft Managed Policies



Baseline Policies

Policy Name	State
Baseline policy: Require MFA for admins (Preview)	On
Baseline policy: End user protection (Preview)	On
Baseline policy: Block legacy authentication (Preview)	On
Baseline policy: Require MFA for Service Management (...)	On



Security Defaults

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks.

[Learn more](#) 



Your organization is protected by security defaults.

[Manage security defaults](#)

Microsoft Provided Conditional Access Policies



~~Baseline Policies~~



Conditional Access Templates



Microsoft Managed Policies

Microsoft Managed Policies (MMP)

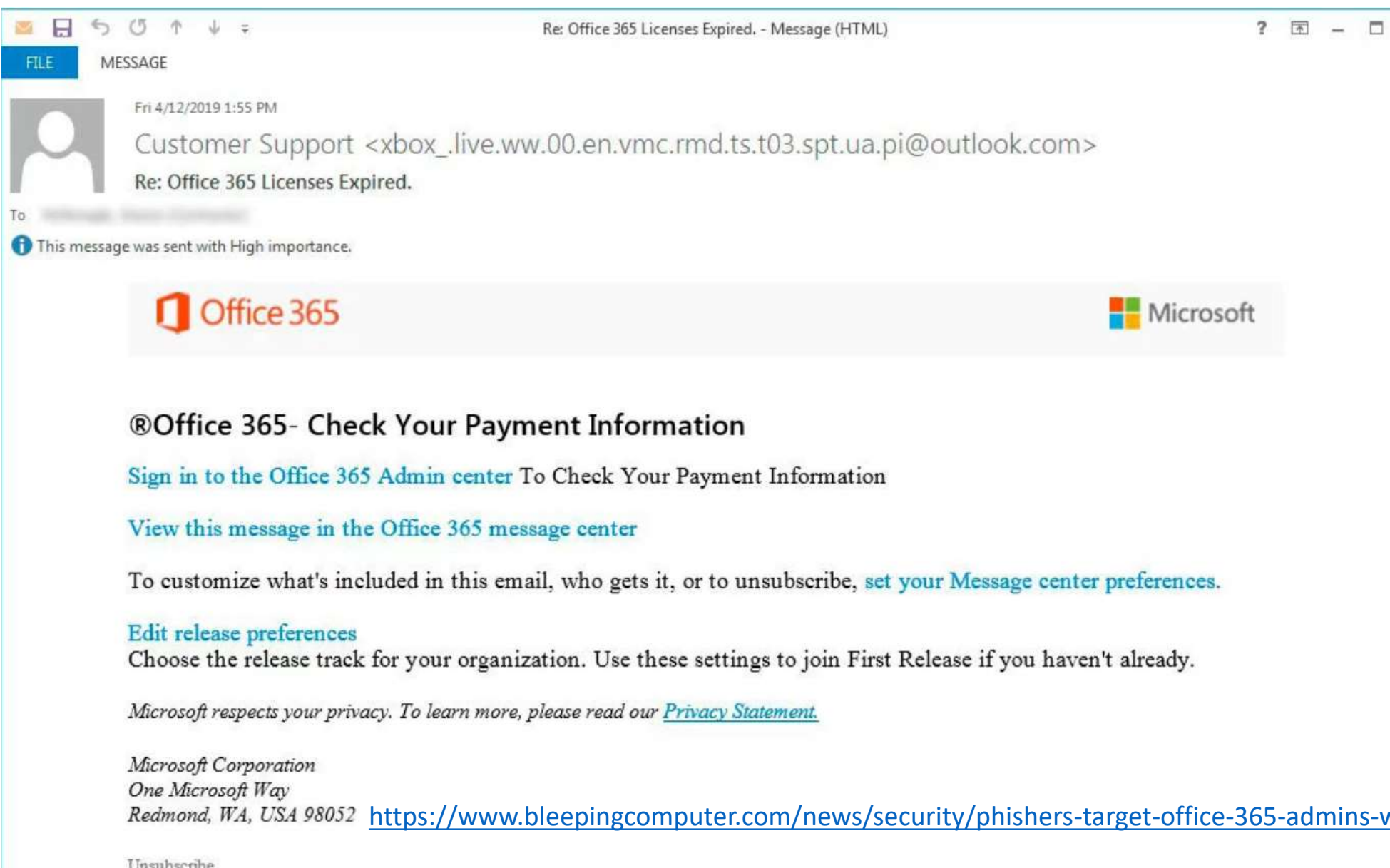
-
- Deployed automatically in reporting mode
 - Modification is limited:
 - Exclude users
 - Turn on or set to Report-only mode
 - Can't rename or delete any Microsoft-managed policies
 - Can duplicate the policy to make custom versions
 - Microsoft might update these policies in the future
 - MMPs turn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

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

Attacking Entra ID



Phishing for Admins



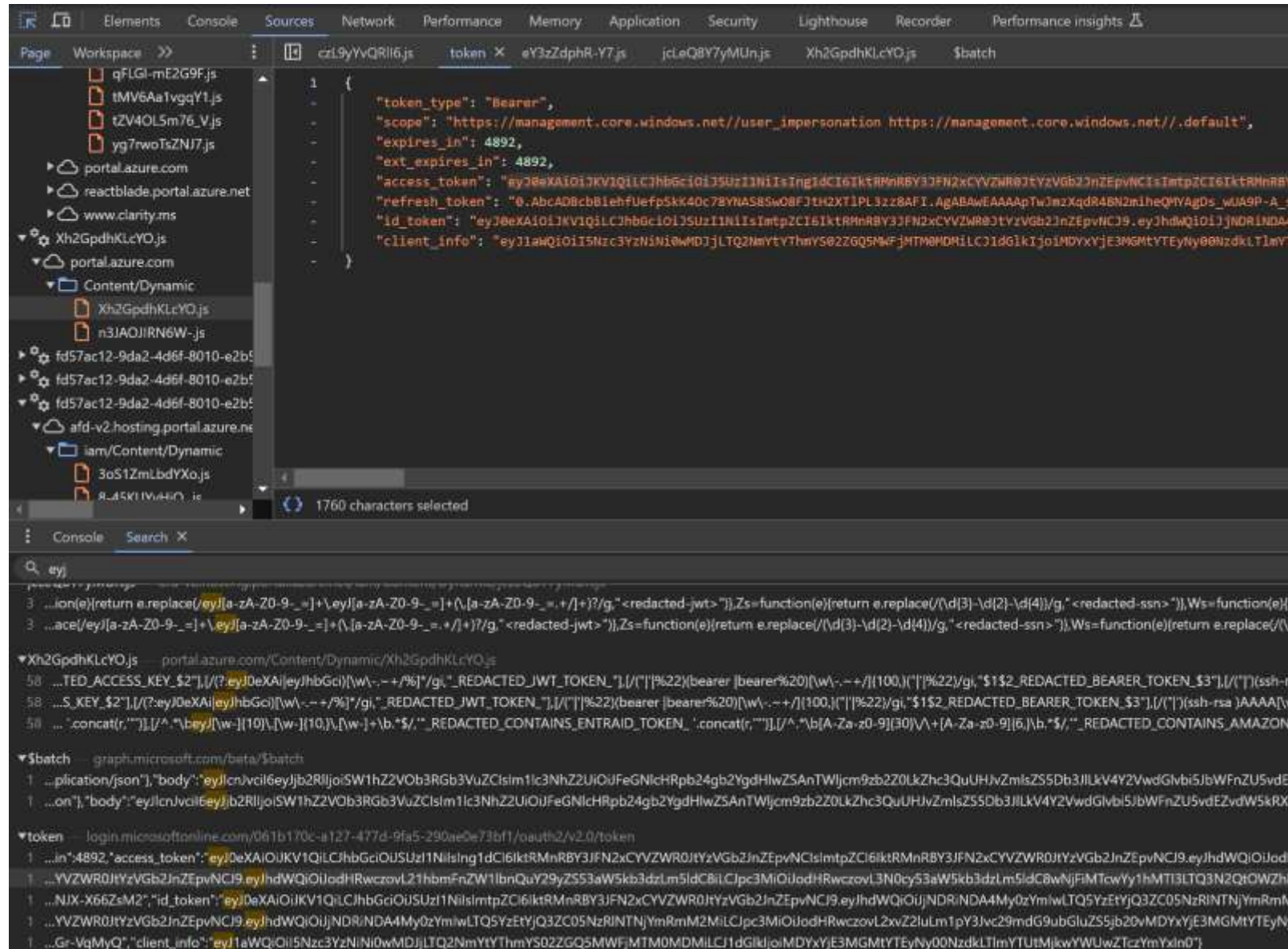
Stealing Tokens from the Web Browser

The image is a composite screenshot. The left portion shows the Microsoft Azure portal interface. At the top, the 'Microsoft Azure' header is visible with a search bar. Below it, the 'Monarch | Overview' page is displayed. The left sidebar contains navigation links: 'Overview', 'Preview features', 'Diagnose and solve problems', and 'Manage'. Under 'Manage', there are links for 'Users', 'Groups', and 'External Identities'. The main content area shows a notification about 'Azure Active Directory is now Microsoft Entra ID' and tabs for 'Overview', 'Monitoring', 'Properties', 'Recommendations', and 'Tutorials'. A search bar for 'Search your tenant' is present. Below this, a 'Basic information' section shows the 'Name' as 'Monarch'.

The right portion of the image shows a browser's developer tools network tab. It displays a list of network requests with columns for Name, Status, Type, Initiator, Size, and Time. The requests include:


Name	Status	Type	Initiator	Size	Time
isDirectoryFeatureEnabled?api...	200	xhr	lvQE5u0JAQOI.js:1	1.3 kB	127 ms
count	204	preflight	Preflight	0 B	625 ms
data:image/svg+xml;...	200	svg+xml	wwgRmzcFQmrg.js (memor...		0 ms
single-file-hooks-frames.js	200	script	VM151 single-file-	9.9 kB	40 ms
Index?reactView=true&retryCo...	200	docum...	(disk ca...		12 ms
\$batch	200	xhr	lvQE5u0JAQOI.js:1	946 B	77 ms
single-file-hooks-frames.js	200	script	single-file-extensi	9.9 kB	8 ms

Stealing Tokens from the Web Browser



Stealing Access Token from the Web Browser

```
jwt.ms
Decoded Token Claims
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "KQ2tAcrE7lBaVVGBmc5FobE",
  "kid": "KQ2tAcrE7lBaVVGBmc5F",
}.{
  "aud": "https://management.core.windows.net/",
  "iss": "https://sts.windows.net/061b170c-a127-477d-9fa5-290ae0e73bf1/",
  "iat": 1723060777,
  "nbf": 1723060777,
  "exp": 1723065970,
  "acr": "1",
  "aio": "AVQAq/8XAAAAIqLZWy2NuIj",
  "amr": [
    "pwd",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-",
  "appidacr": "0",
  "groups": [
    "fe1bc310-"
  ],
  "idtyp": "user",
  "ipaddr": "136.179.21.70",
  "name": "Sean Metcalf",
  "oid": "9777c3b6-002c-46-",
  "puid": "100320037D4!",
  "rh": "0.AbcADBcbBiehfUefpSkK40c7",
  "scp": "user_impersonation",
  "sub": "bT0T7_pKncPMRCvZbs-WtRwC",
  "tid": "061b170c-a127-477d-9fa5-",
  "unique_name": "sean@monarchsciences.org",
  "upn": "sean@monarchsciences.org",
  "uti": "QrkBIwbMpet",
  "ver": "1.0"
}
```

That's It!
Now we have the Access Token

Stealing Tokens from the Web Browser



AADInternals.com

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



v0.9.3 by @DrAzureAD (Nestori Syynimaa)

[AAD KILL CHAIN](#) [DOCUMENTATION](#) [LINKS](#) [OSINT](#) [TALKS](#) [TOOLS](#)

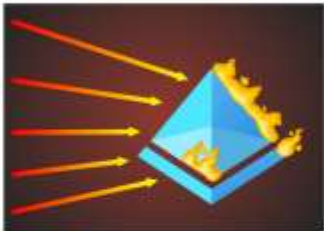


Exfiltrating NTHashes by abusing Microsoft Entra Domain Services

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

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

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



DoSing Azure AD

🕒 July 02, 2023

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



Deploying users with pre-registered MFA

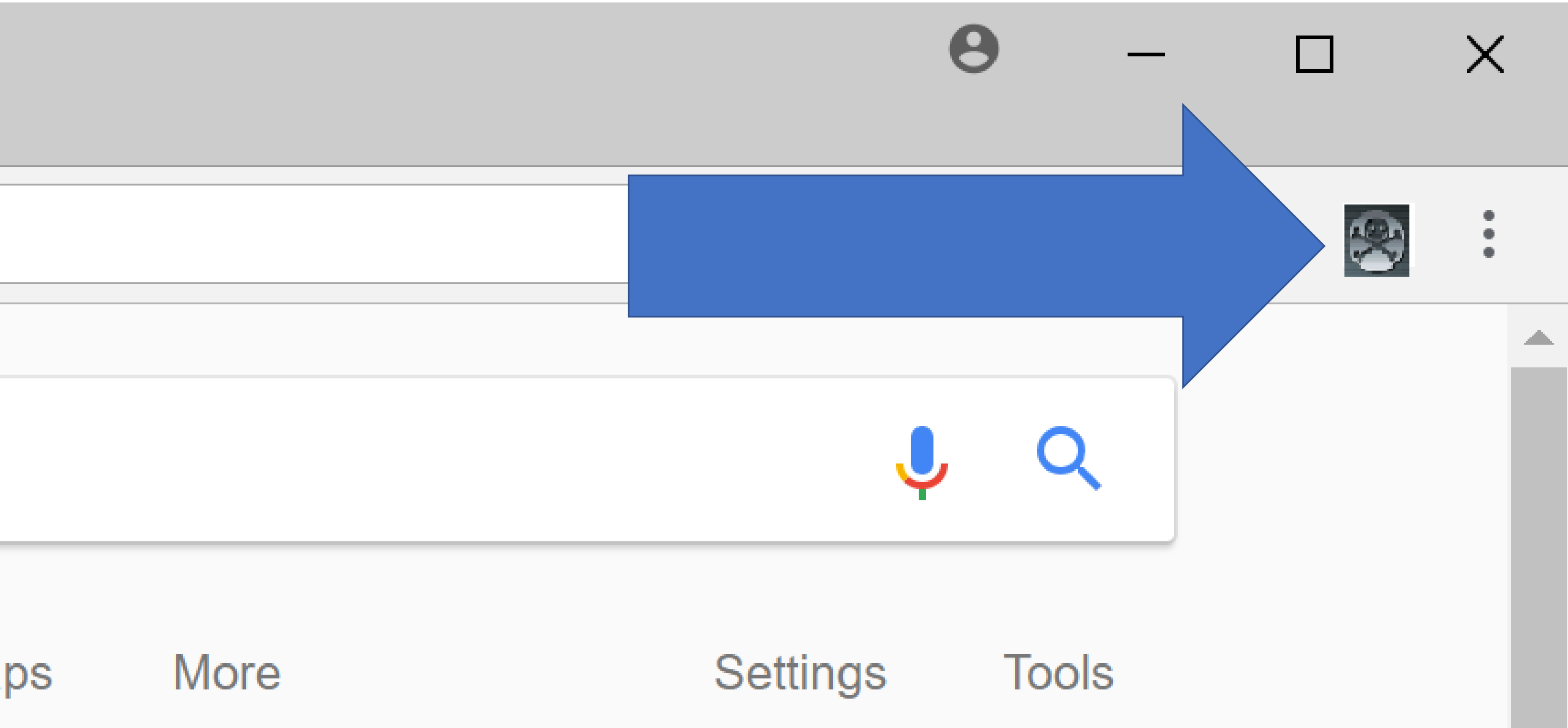
🕒 May 23, 2023 (Last Modified: May 24, 2023)

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

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

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

Token Theft with Browser Extension



Attacks

Sponsored by [LayerX](#)

January 7, 2025

10:02 AM

0



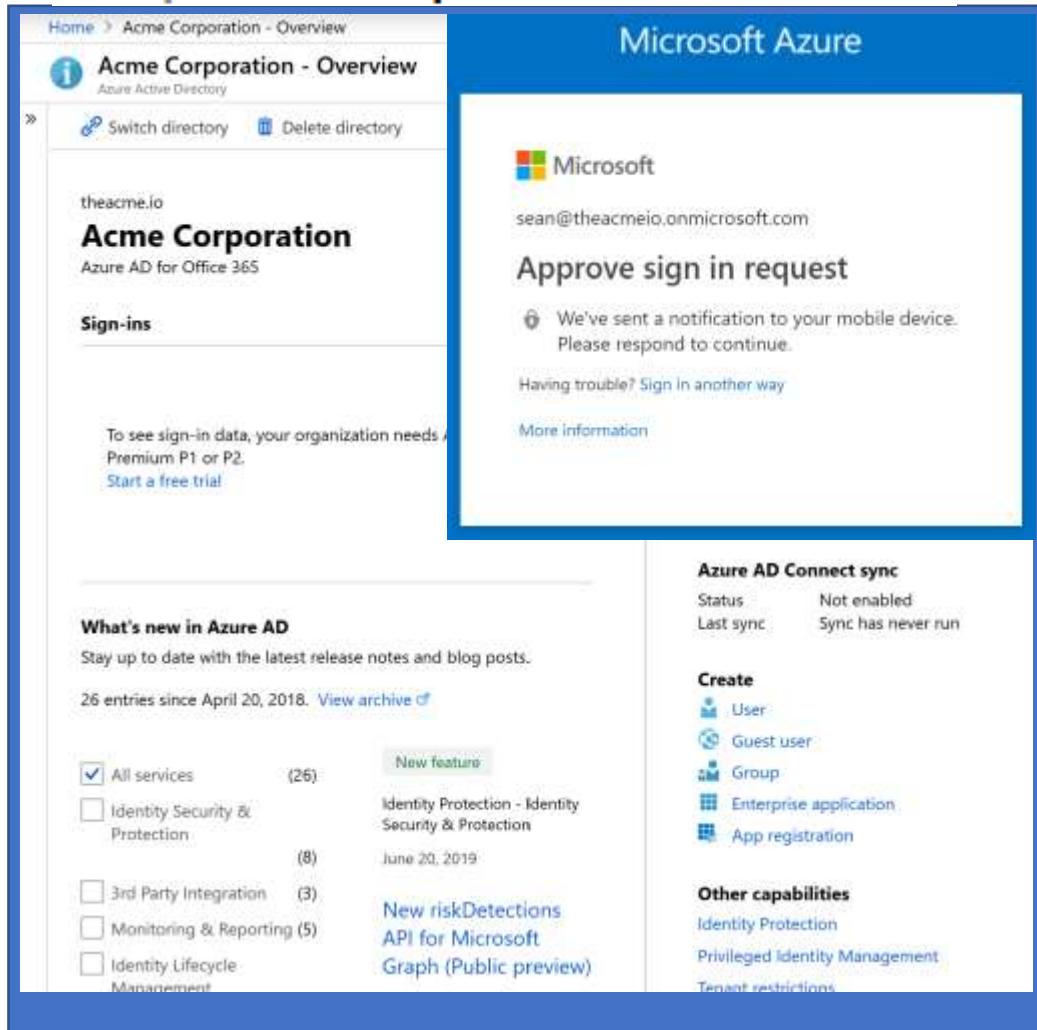
[https://www.bleepingcomputer.com/news/security/malicious-browser-extensions-are-the-next-frontier-for-identity-attacks /](https://www.bleepingcomputer.com/news/security/malicious-browser-extensions-are-the-next-frontier-for-identity-attacks/)

The [recent attack campaign targeting browser extensions](#) shows that malicious browser extensions are the next frontier for identity attacks.

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

Token Theft with evilginx

<https://aad.portalazure.com/>



Home > Acme Corporation - Overview

Acme Corporation - Overview
Azure Active Directory

Switch directory Delete directory

theacme.io

Acme Corporation
Azure AD for Office 365

Sign-ins

To see sign-in data, your organization needs a Premium P1 or P2.
[Start a free trial](#)

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

☒ All services (26) New feature

☐ Identity Security & Protection (8)

☐ 3rd Party Integration (3)

☐ Monitoring & Reporting (5)

☐ Identity Lifecycle Management

Azure AD Connect sync

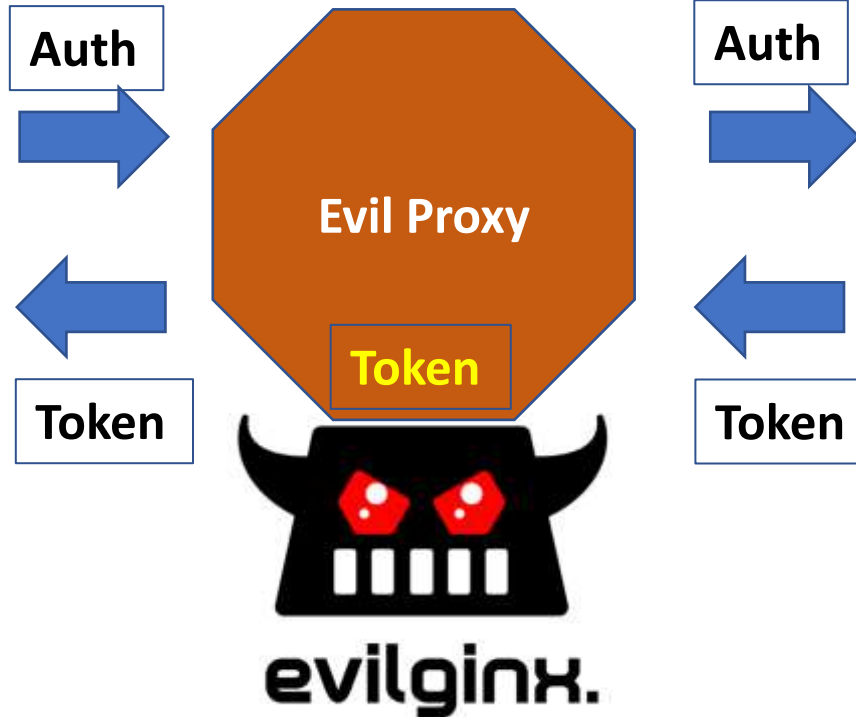
Status	Last sync
Not enabled	Sync has never run

Create

- User
- Guest user
- Group
- Enterprise application
- App registration

Other capabilities

- Identity Protection
- Privileged Identity Management
- Tenant restrictions



<https://github.com/kgretzky/evilginx2>

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



Microsoft Azure

sean@theacmeio.onmicrosoft.com

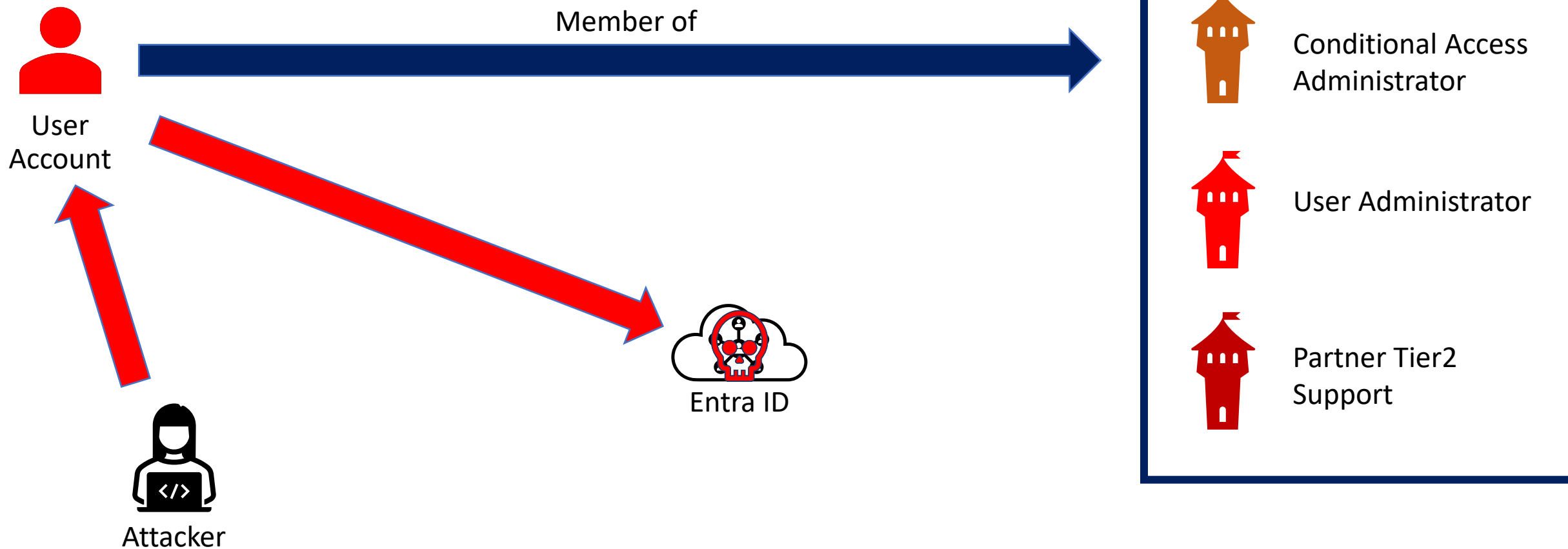
Approve sign in request

We've sent a notification to your mobile device.
Please respond to continue.

Having trouble? [Sign in another way](#)

[More information](#)

Overprivileged User



Application Escalation

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

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

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

Application Escalation: Find the App Owner

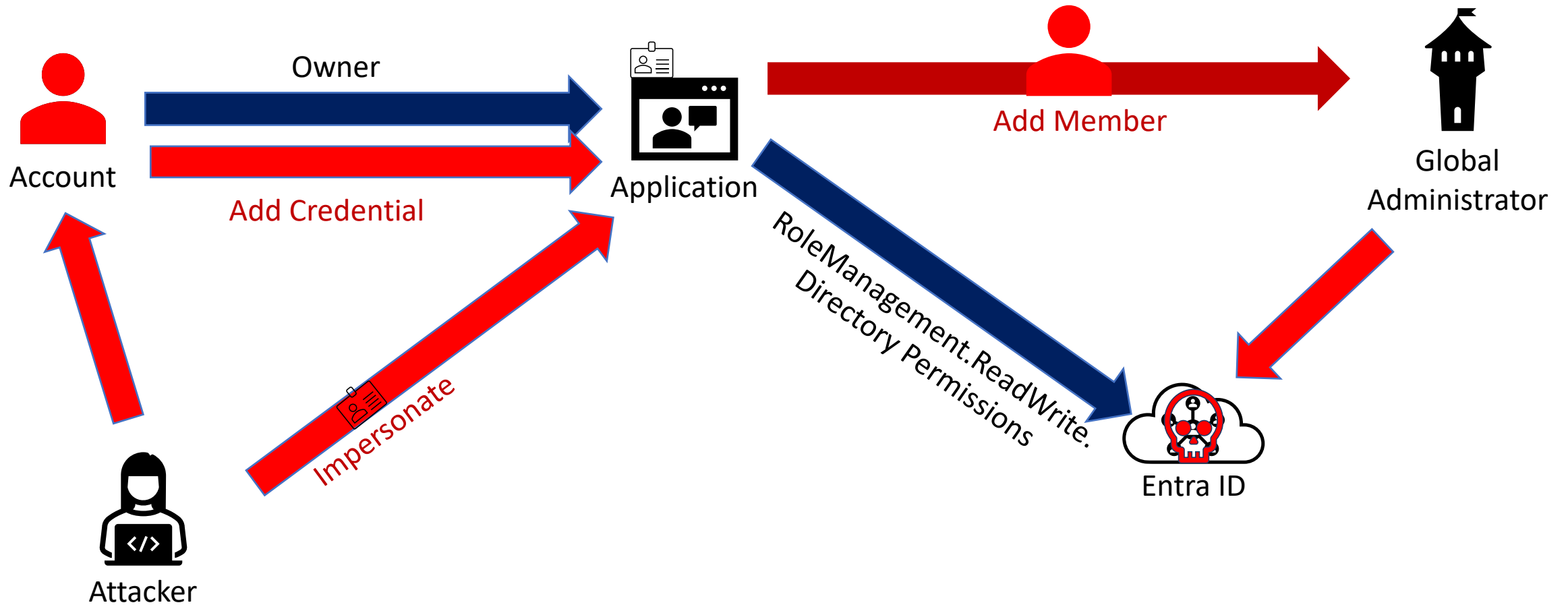
```
PS C:\Data\_MCSA> Get-AzureADApplication -SearchString 'overpermissioned'
```

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

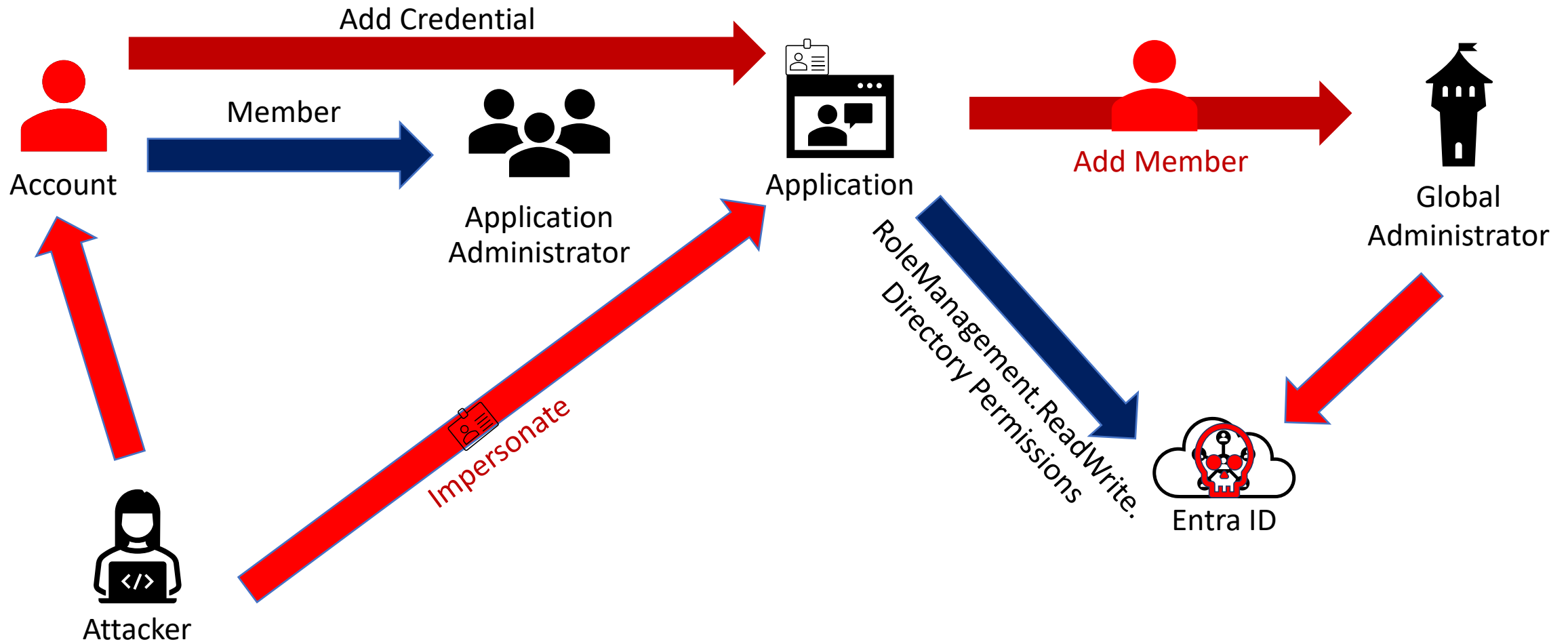
```
PS C:\Data\_MCSA> get-azureadapplicationowner -ObjectId 'fbe4ea6c-0ae4-46b2-a6f0-5f96e3f4858f'
```

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

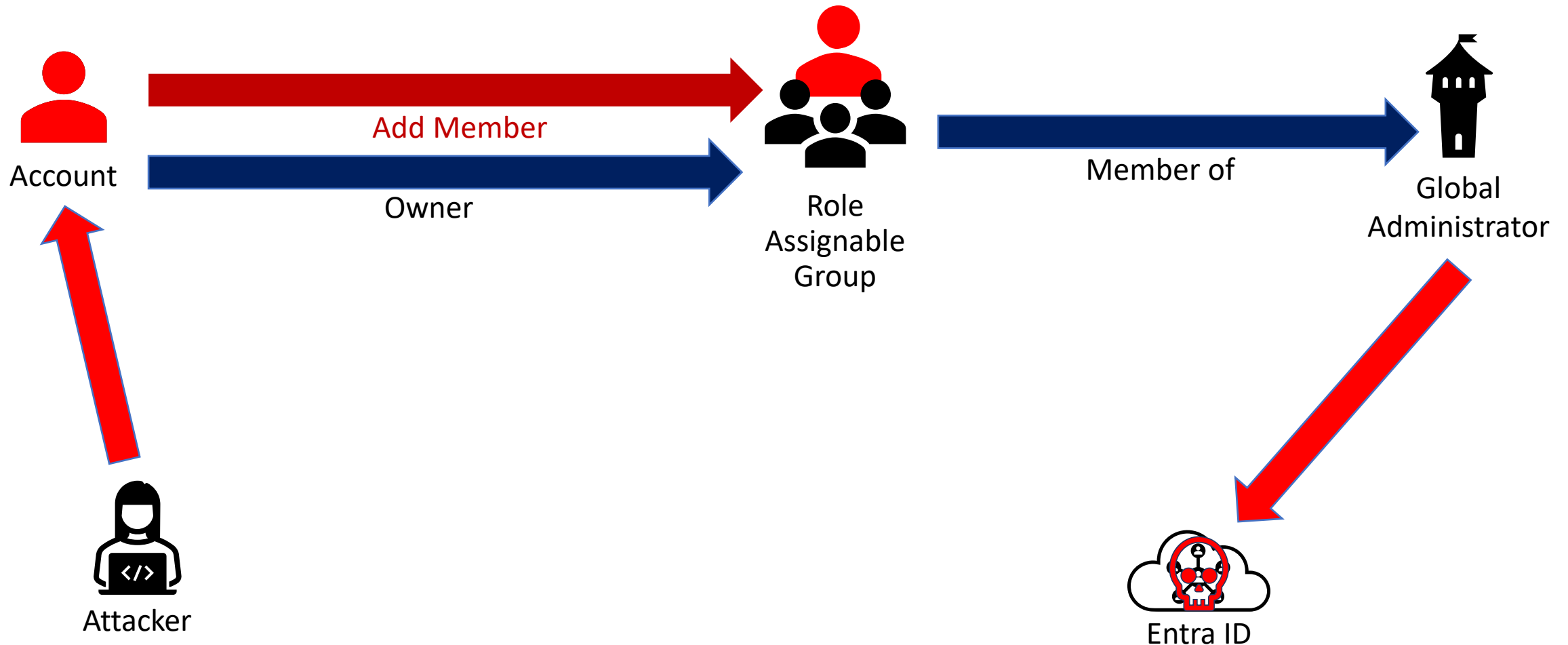
Compromise Entra ID through Application Permissions



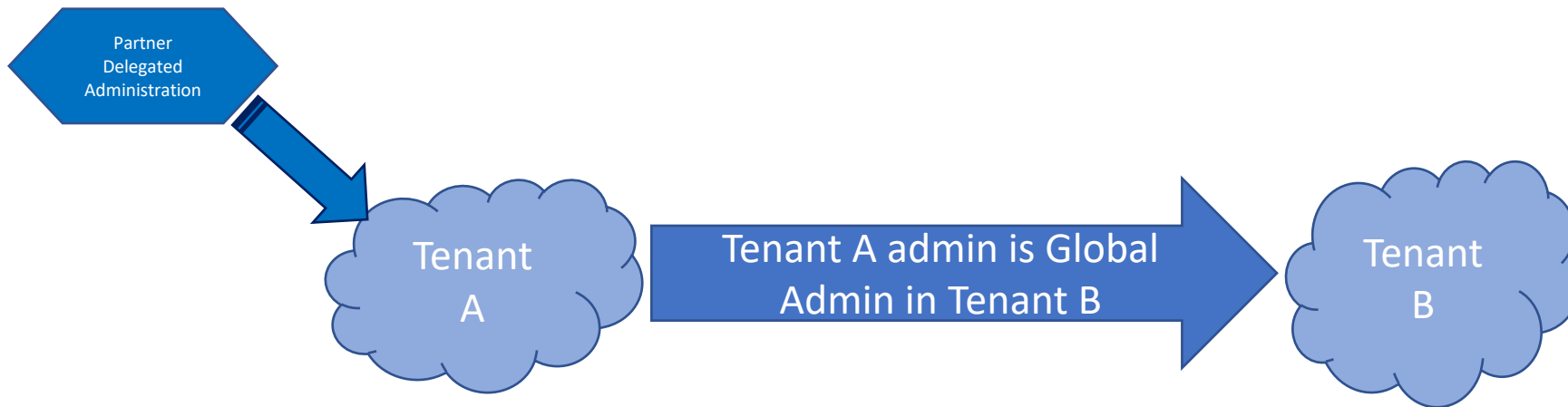
Compromise Azure AD through Application Permissions



Compromise Azure AD through Role Assignable Group Owner Rights



Solarigate “Tenant Hopping”



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

Delegated Admin

Microsoft Entra ID

- Overview
- Preview features
- Diagnose and solve problems
- 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 permission. [Learn about partners.](#)

Partner	Relationship type	Roles	Expiration
None			

Entra ID Menu Item: Delegated admin partners

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

Partner Relationships – aka Delegated Administration

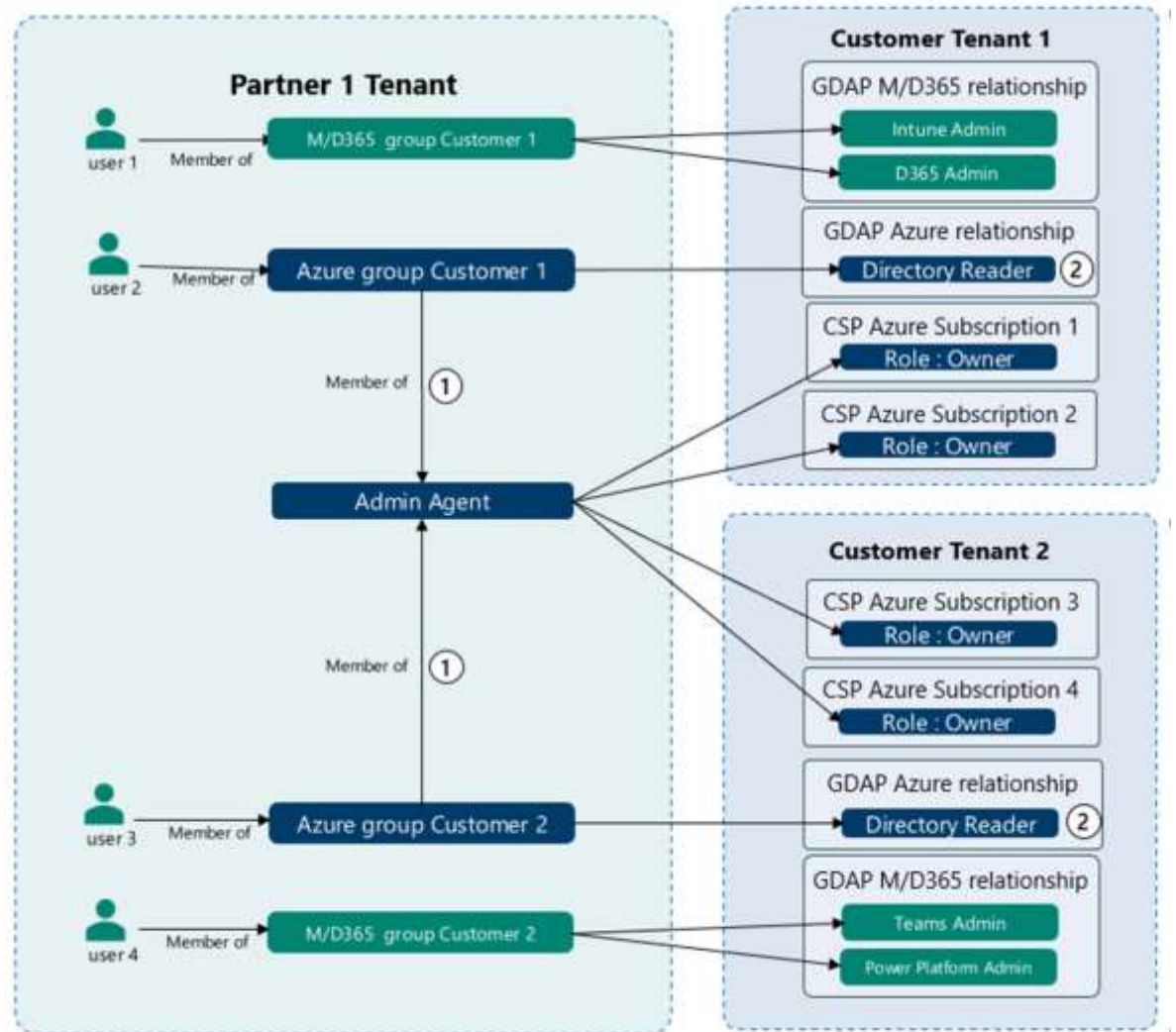
- A configured partner can have admin rights to a customer tenant (“delegated administration”).
- This is provided when the partner requests access to the customer environment.
- When the customer accepts this request:
 - “Admin agent” role in partner tenant is provided effective “Global Administrator”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

Shift to granular delegated admin privileges (GDAP) ASAP!

Check Partner Configuration for your tenant here:

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

Move to Granular Delegated Admin Privileges (GDAP)





What about Admins Synchronized from On-Prem AD?

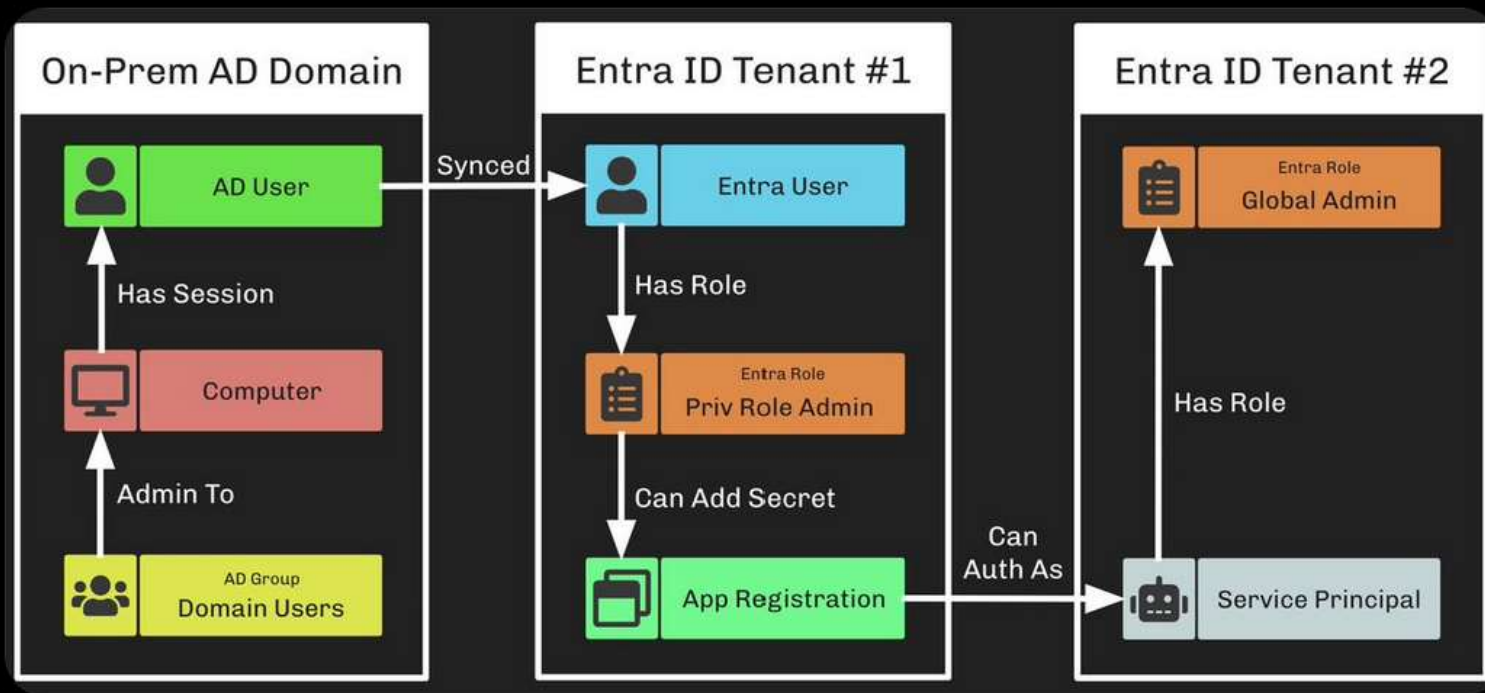


Andy Robbins

@_wald0

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

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



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

Yeah,
don't do that

Midnight Blizzard

January 12, 2024



Microsoft

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

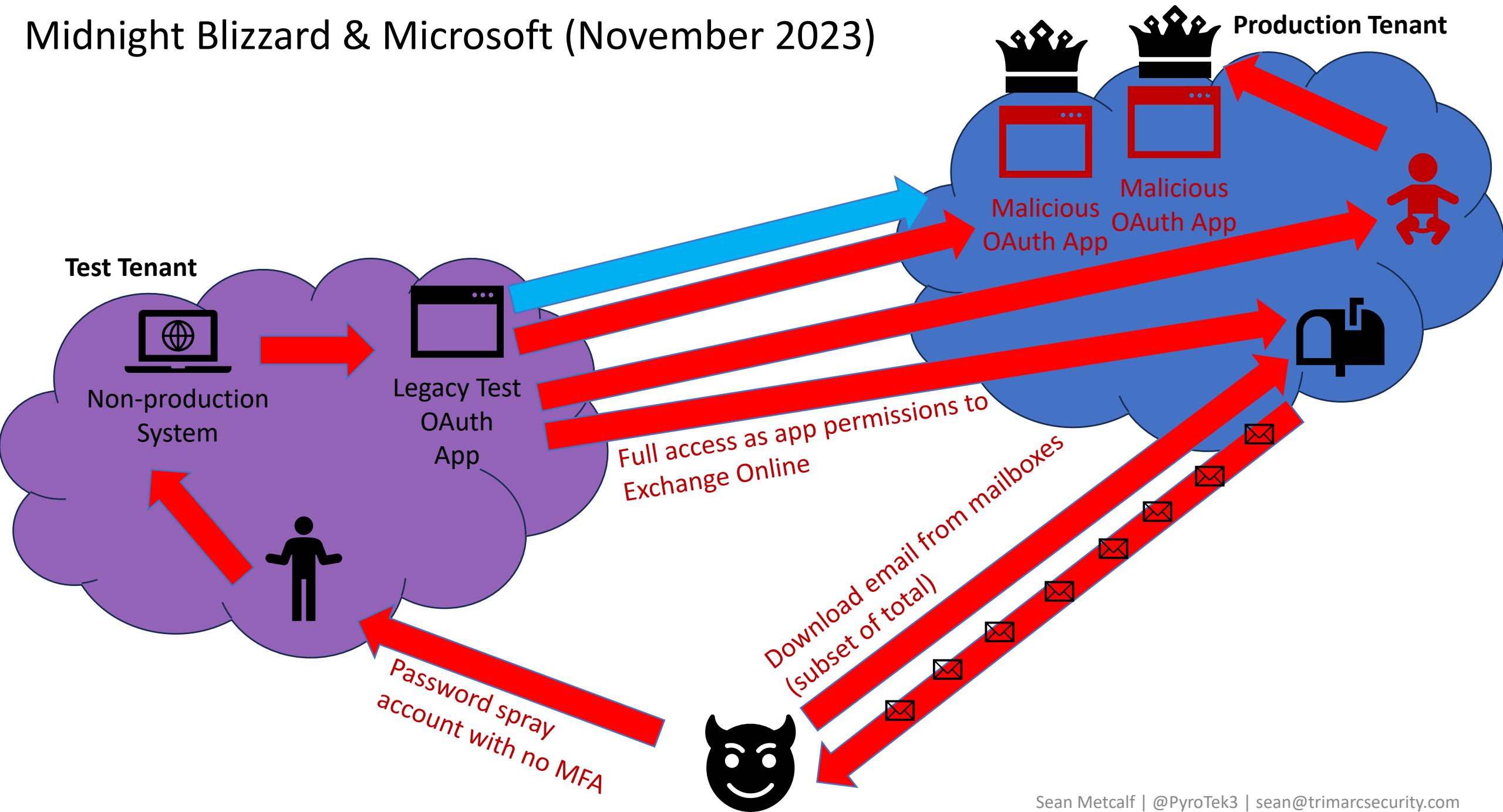
/ By [MSRC](#) / January 19, 2024 / 2 min read

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. Microsoft has identified the threat actor as [Midnight Blizzard](#), the Russian state-sponsored actor also known as Nobelium. As part of our ongoing commitment to responsible transparency as recently affirmed in our [Secure Future Initiative](#) (SFI), we are sharing this update.

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents. The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in the process of notifying employees whose email was accessed.

The attack was not the result of a vulnerability in Microsoft products or services. To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems. We will notify customers if any action is required.

Midnight Blizzard & Microsoft (November 2023)



What We Know

- Midnight Blizzard – a Moscow-supported espionage team also known as APT29 or Cozy Bear – **"utilized password spray attacks that successfully compromised a legacy, non-production test tenant account that did not have multifactor authentication (MFA) enabled."**
- After gaining initial access to a **non-production** Microsoft system, the intruders **compromised a legacy test OAuth application that had access to Microsoft's corporate IT environment.**
- The actor **created additional malicious OAuth applications.**
- **They created a new user account to grant consent in the Microsoft corporate environment to the actor controlled malicious OAuth applications.**
- The threat actor then used the **legacy test OAuth application to grant them the Office 365 Exchange Online full_access_as_app role, which allows access to mailboxes.**
- They then used this access to **steal emails and other files from corporate inboxes belonging to top Microsoft executives and other staff.**
- They used residential broadband networks as proxies to make their traffic look like it was all legitimate traffic from work-from-home staff, since it was coming from seemingly real users' IP addresses.
- This **all happened in late November, Microsoft didn't spot the intrusion until January 12**, and the compromised email accounts included those of senior leadership and cybersecurity and legal employees.
- "If the same team were to deploy the legacy tenant today, mandatory Microsoft policy and workflows would ensure MFA and our active protections are enabled to comply with current policies and guidance, resulting in better protection against these sorts of attacks."

Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

MSRC / By [MSRC](#) / March 08, 2024 / 2 min read

This blog provides an update on the nation-state attack that was detected by the Microsoft Security Team on January 12, 2024. As we [shared](#), on January 19, the security team detected this attack on our corporate email systems and immediately activated our response process. The Microsoft Threat Intelligence investigation identified the threat actor as [Midnight Blizzard](#), the Russian state-sponsored actor also known as NOBELIUM.

As we said at that time, our investigation was ongoing, and we would provide additional details as appropriate.

In recent weeks, we have seen evidence that Midnight Blizzard is using information initially exfiltrated from our corporate email systems to gain, or attempt to gain, unauthorized access. This has included access to some of the company's source code repositories and internal systems. To date we have found no evidence that Microsoft-hosted customer-facing systems have been compromised.

It is apparent that Midnight Blizzard is attempting to use secrets of different types it has found. Some of these secrets were shared between customers and Microsoft in email, and as we discover them in our exfiltrated email, we have been and are reaching out to these customers to assist them in taking mitigating measures. Midnight Blizzard has increased the volume of some aspects of the attack, such as password sprays, by as much as 10-fold in February, compared to the already large volume we saw in January 2024.

Midnight Blizzard's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus. It may be using the information it has obtained to accumulate a picture of areas to attack and enhance its ability to do so. This reflects what has become more broadly an unprecedented global threat landscape, especially in terms of sophisticated nation-state attacks.

Across Microsoft, we have increased our security investments, cross-enterprise coordination and mobilization, and have enhanced our ability to defend ourselves and secure and harden our environment against this advanced persistent threat. We have and will continue to put in place additional enhanced security controls, detections, and monitoring.

Our active investigations of Midnight Blizzard activities are ongoing, and findings of our investigations will continue to evolve. We remain committed to sharing what we learn.

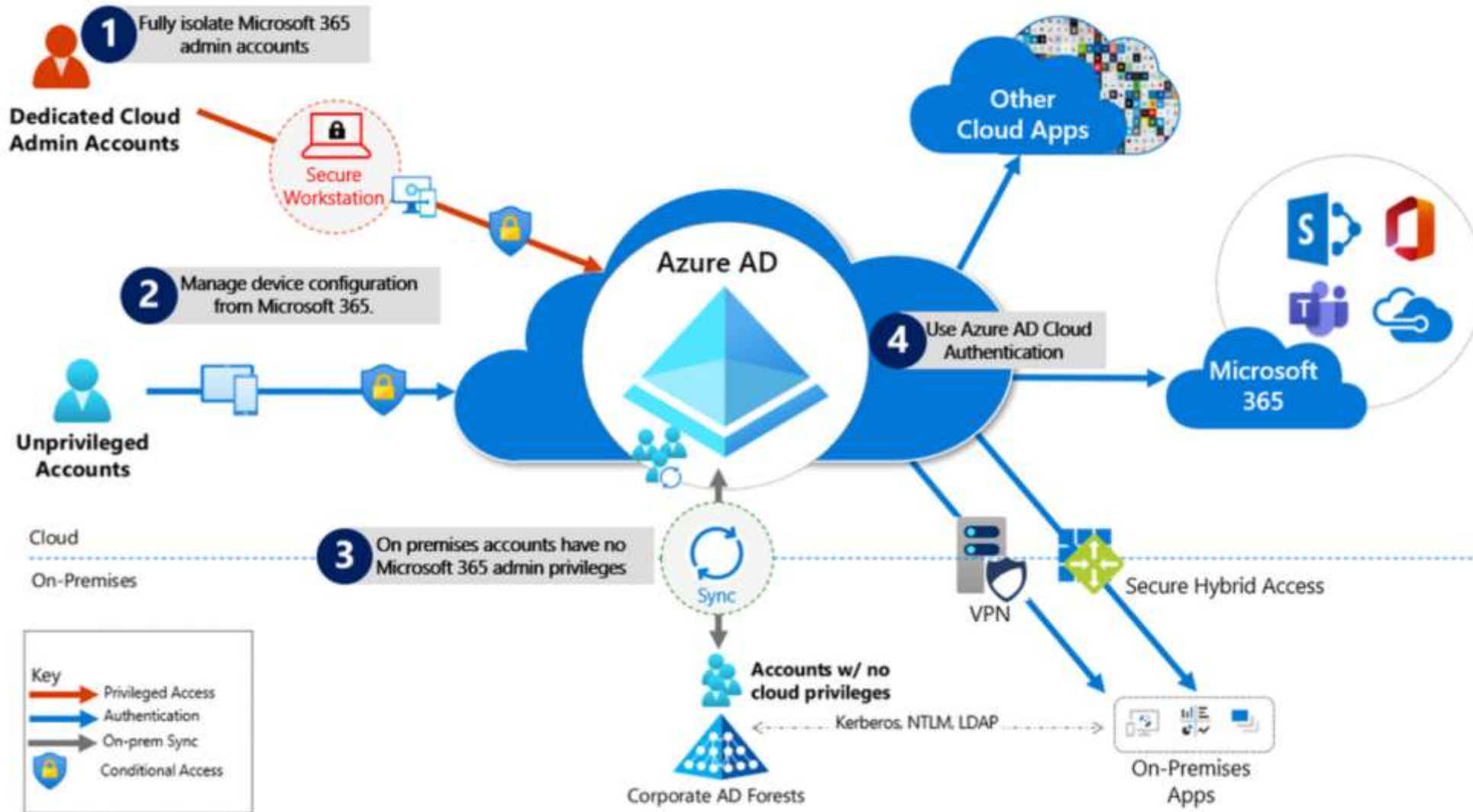
Sean Metcalf | [@PyroTek3](#) | sean@trimarcsecurity.com



Securing Entra ID Administration



Securing Entra ID



<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754> Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Securing Entra ID - Microsoft Summary

Fully Isolate Entra ID & Microsoft 365 admin accounts

They should be:

1. Created in Entra ID.
2. Required to use Multi-factor authentication (MFA).
3. Secured by conditional access.
4. Accessed only by using Azure Managed Workstations.

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

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

Custom smart lockout

Lockout threshold ⓘ

10

Lockout duration in seconds ⓘ

70

Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

seahawks
mariners
sounders
redmond
washington

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

<https://aka.ms/deploypasswordprotection>

Phishing Defensive Layers

Require Users to MFA, preferably FIDO2

- Authenticator App recommended. Better performance and less prompts (behaves as authentication token broker)

Conditional Access Policy

- MFA, Location, App, etc

Risk Based Policy

- Only prompt when Risk 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 Trimarc Level 0 & 1 roles
- FIDO2 keys for Emergency “Break Glass” Accounts
- Leverage Conditional Access policies to enforce MFA for admins from all locations

What are the most resilient MFA methods?

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

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

TLDR: Use FIDO2 security key for emergency accounts

Depends on
Entra Auth Service

1st Place Medal

Certificate based authentication

FIDO2 security key

Windows Hello for Business

Depends on
Entra Auth Service
+
Azure MFA Service

2nd Place Medal

Password
+ Hardware Tokens OTP

Person icon

Password
+ Software Tokens OTP

Depends on
Entra Auth Service
+
Azure MFA Service
+
Phone carrier /
Mobile OS /
Internet

3rd Place Medal

Microsoft Authenticator Passwordless

Password + Microsoft Authenticator Number match

Password + Voice

Password + SMS

<https://x.com/merill/status/1821027962864726249/photo/1>

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.

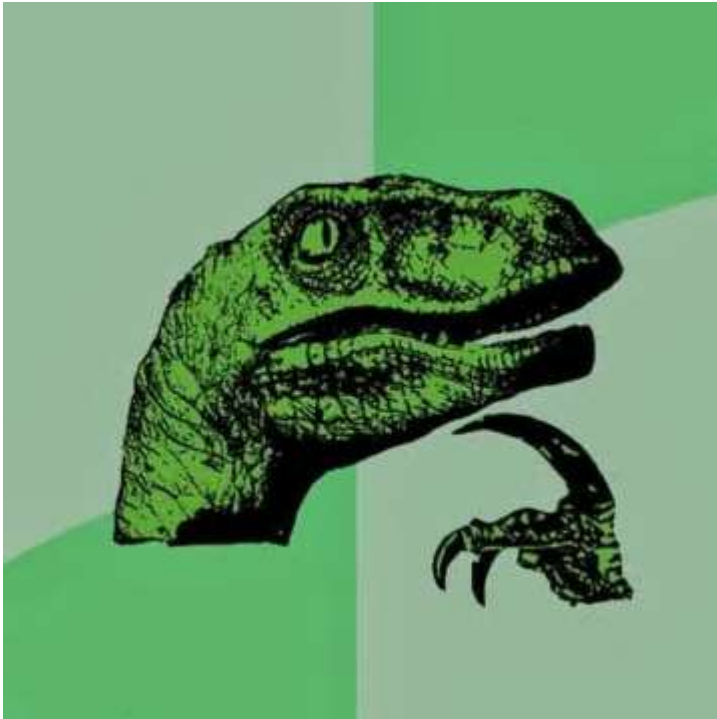
<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide>

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>

Conclusion

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com



Attackers are targeting the cloud

Identifying common security issues and resolving them improves system security.

Fixing these issues provides improved breach resilience.

Slides, Video & Security Articles:
Hub.TrimarcSecurity.com





Questions?