OVERLOOKED AND EXOTIC ATTACK SURFACE

SHINING A LIGHT ON HIDDEN VULNERABILITIES IN ENTERPRISE TECHNOLOGIES

8/17/2023

Nick Popovich | Hacker

ROTAS SECURITY

AGENDA

ROTAS SECURITY

- The Technology Ecosystem's Evolution
- Security Assessment & Testing - Two W's and an H
- "New" Threat Landscape - What's Old Is New
- Practical Examples – Teams
- Practical Examples – Conditional Access Policies
- Practical Examples - Azure AD
- Practical Examples –ServiceNow
- ~~Bonus (if we have time) Practical Examples – MacOS~~

whoami

- US Army Veteran - Signal Corps
- Founder and Principal Hacker at Rotas Security – rotassecurity.com
- I have seen many winters as a pentester and red teamer (since '09)
- Former Practice Director of Optiv's Attack & Pen team
- Also spent time as a senior operator for a fortune 500's Red Team

REFERENCED WORK

We Stand on the Shoulders of Giants

ROTAS
SECURITY

REFERENCES

- Beau Bullock - @dafthack from BHIS & BreakForge
  - Extensive training, podcasts
- Mauricio Velazco - @mvelazco from Splunk
  - Created BadZure training resource https://github.com/mvelazc0/BadZure
- Andy Robbins - @_wald0 from SpectreOps
- Cedric Owens - @cedowens from Meta
- Patrick Wardle - @patrickwardle from Objective-See Foundation
- Blogs, podcasts, tweets and amazing research from @fabian_bader, @dirkjan, @DrAzureAD, @Haus3c, @kfosaaen, @inversecos, and too many others to mention on a slide…

THE TECHNOLOGY ECOSYSTEM'S EVOLUTION

Where We've Come from & Where We're Going

ROTAS
SECURITY

THE TECHNOLOGY ECOSYSTEM – This We'll Defend

ROTAS SECURITY

- Ecosystem defined:

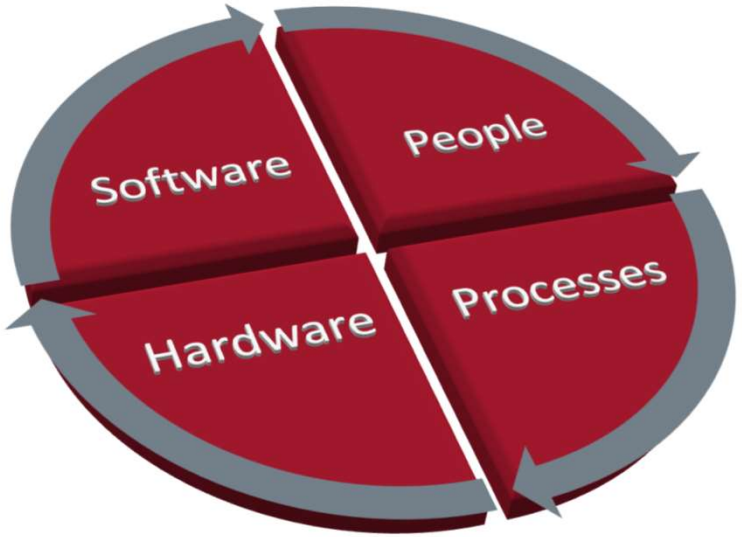
noun, *Ecology.*

1. a system, or a group of interconnected elements, formed by the interaction of a community of organisms with their environment.

2. any system or network of interconnecting and interacting parts, as in business.

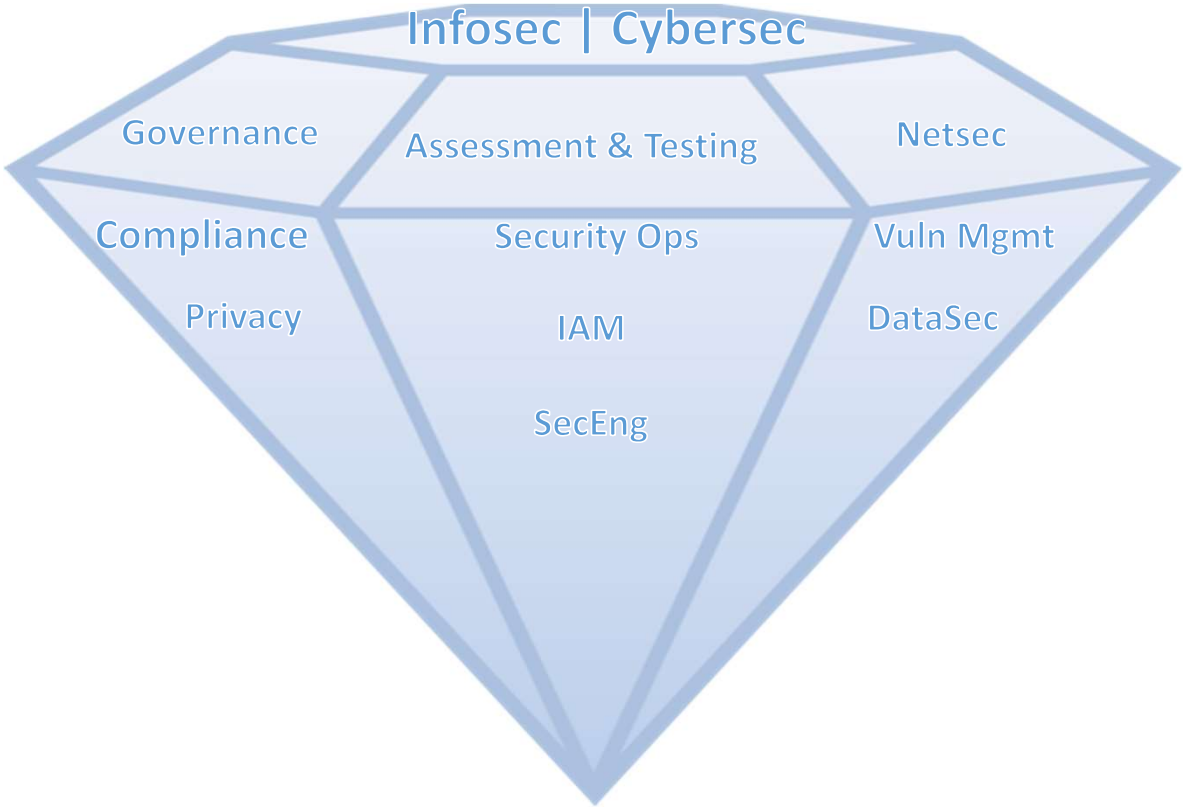
http://www.dictionary.com/browse/ecosystem

THE TECHNOLOGY ECOSYSTEM – This We'll Defend



THE TECHNOLOGY ECOSYSTEM – One Team One Fight

ROTAS SECURITY



HISTORICAL AREAS OF CONCERN

ROTAS SECURITY

Attack Surface

- Not being aware of what attack surface looks like. What systems, people, applications, assets or data is accessible.
- Over reliance on automated tools and systems

Monitoring

- Internal and perimeter network monitors not tuned. Too much noise. Cannot differentiate attack activity from Internet noise.
- Not watching the Internal network, focusing on perimeter.
- No anomalous activity monitoring for users or endpoints.
- SIEM not consuming endpoint event information.

Users and Credentials

- Not using Multi-factor authentication for external access
- Easily guessable passwords
- Default credentials
- Not following concept of least privilege
- Shared credentials
- Administrative services open to the world

Network Access and Egress

- Limited outbound egress control or monitoring
- No central control points (direct connection)
- Lack of internal NAC/802.1x

AREAS OF CONCERN... Evolved

ROTAS SECURITY

AREAS OF CONCERN… Evolved

ROTAS SECURITY

Attack Surface

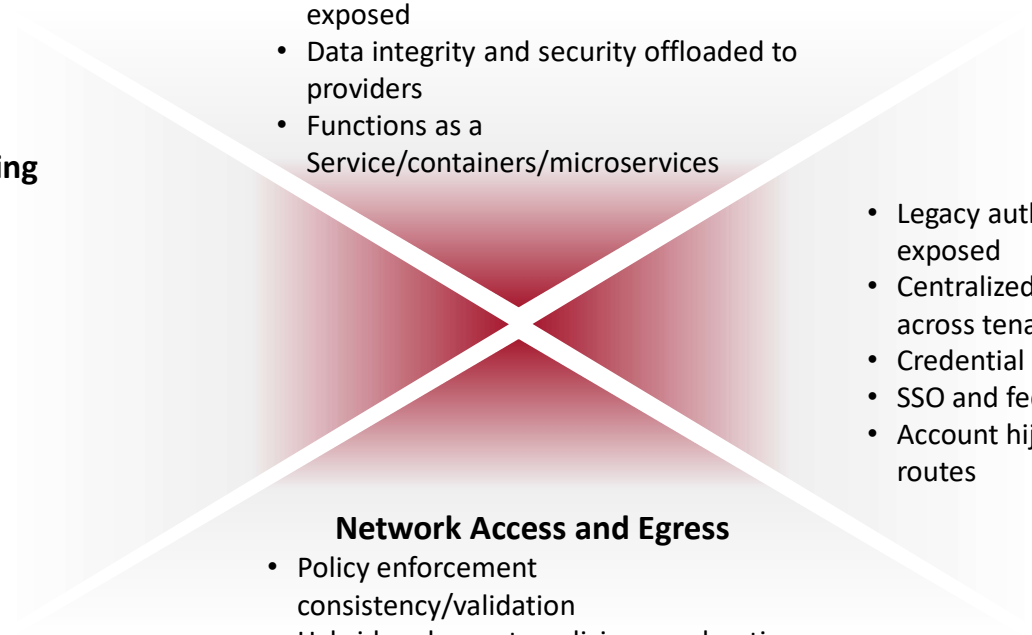
- Multi-tenancy concerns
- Lack of insight into available services exposed
- Data integrity and security offloaded to providers
- Functions as a Service/containers/microservices

Monitoring

- What monitoring?

IAM

- Legacy authentication providers exposed
- Centralized identity management across tenants
- Credential storage
- SSO and federation concerns
- Account hijacking via tokens/web routes



Network Access and Egress

- Policy enforcement consistency/validation
- Hybrid and remote policies are chaotic

SECURITY ASSESSMENT & TESTING

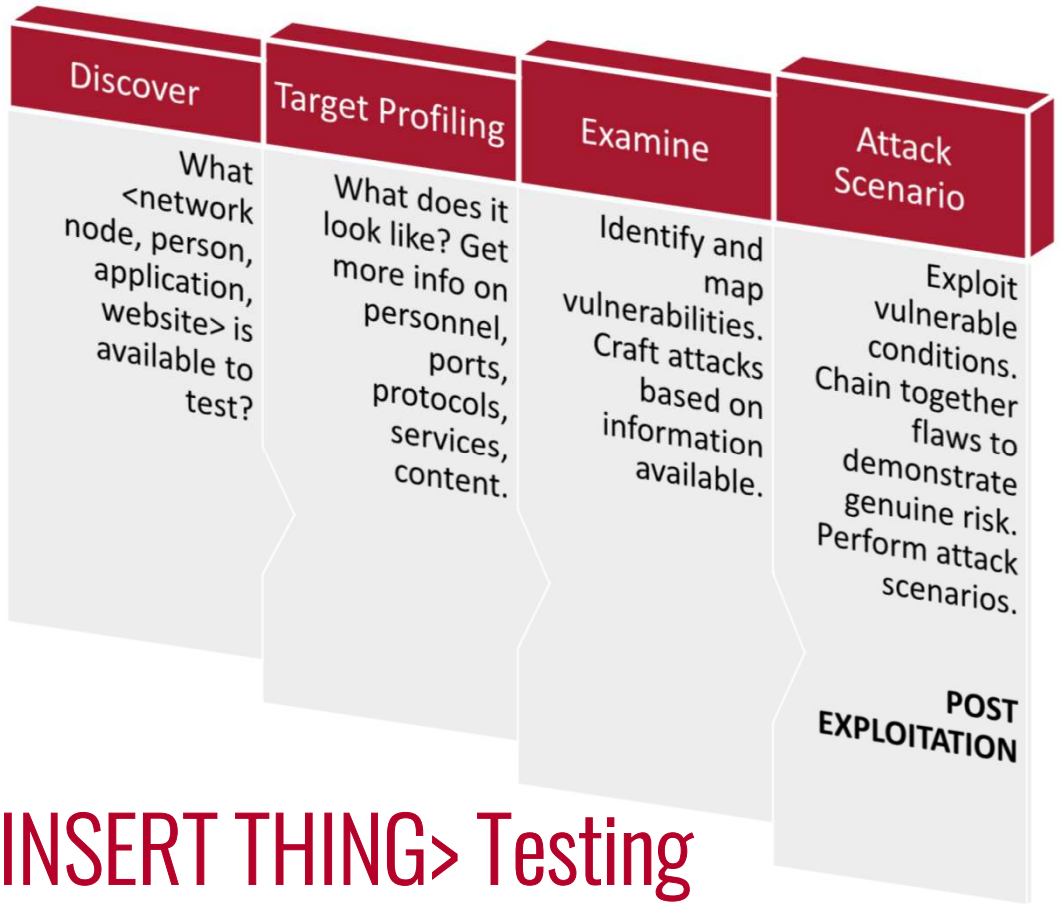
Two W's and an H

HOW IT'S GOING

ROTAS SECURITY

SECURITY ASSESSMENT & TESTING

ROTAS SECURITY



Methodology for <INSERT THING> Testing

TESTING FRAMEWORK- Two W's and an H

- WHAT we're doing is typically going to be static
  - e.g. enumerating endpoints for information, query services for functionality
- WHY we're doing it is also mostly immutable
  - Gain insight
- HOW we do it is going to change
  - Tools, techniques, technologies

WHAT'S OLD IS NEW AGAIN

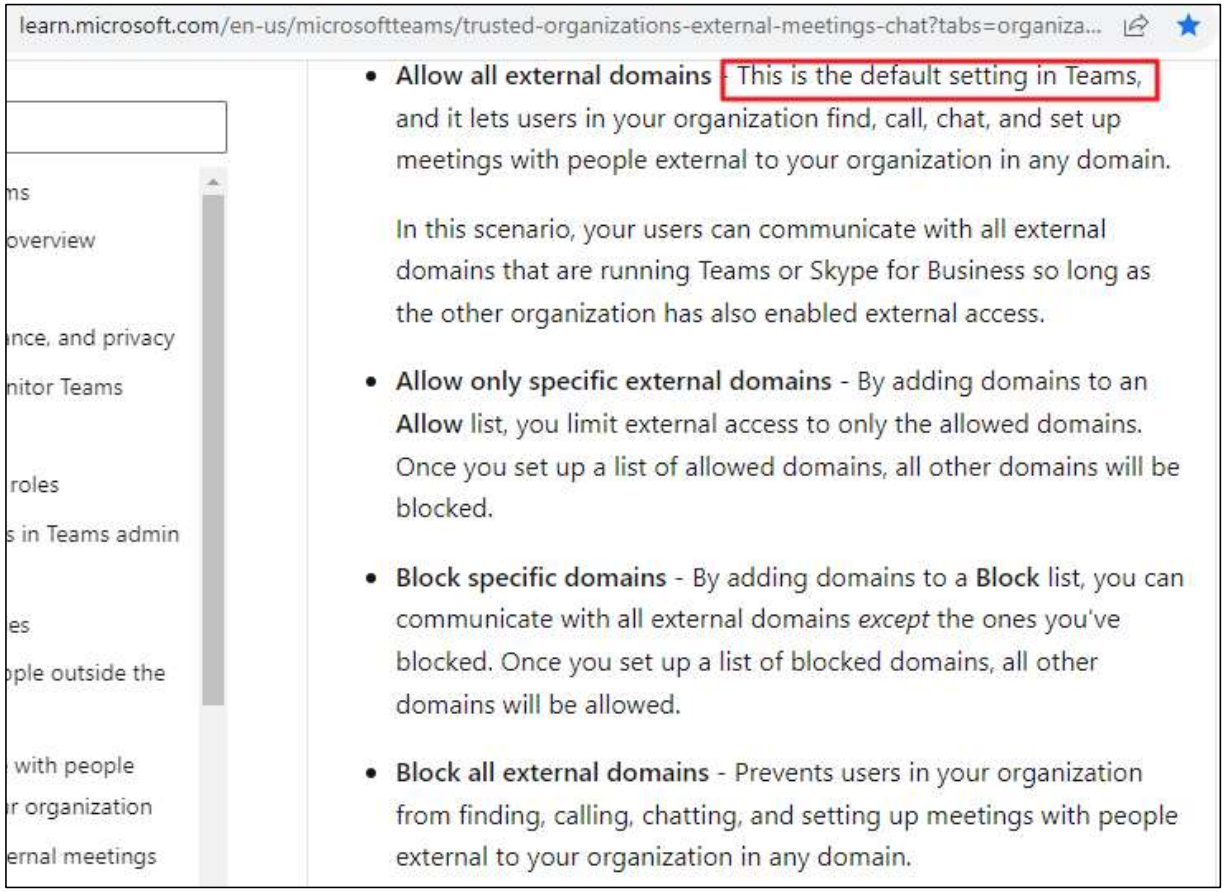
WHAT'S OLD IS NEW AGAIN

ROTAS SECURITY

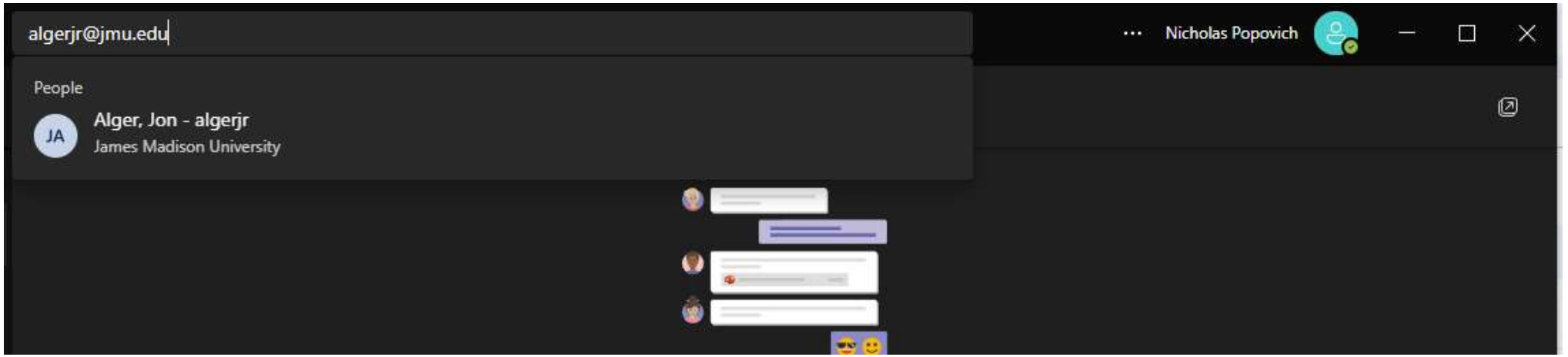
- Introduction of new tech = similar flaws that have been "handled" before
- Examples
  - SQL injection conditions in NoSQL because developers are expecting programmatic use
  - API's that do not sanitize data and result in injection conditions
  - Apps that have overflow conditions due to lack of bounds/input checking
  - Session issues regarding access tokens
  - Conditional Access Policy enforcement is bypassed due to conflicting policies
- As new tech is adopted innovators and implementors focus on usability rather than security (a tale as old as time)

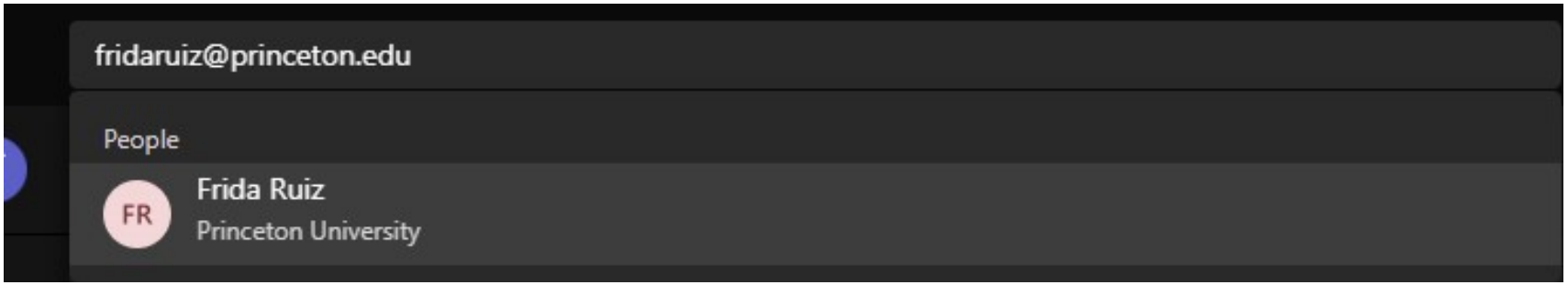
PRACTICAL EXAMPLES

PRACTICAL EXAMPLE – MS Teams

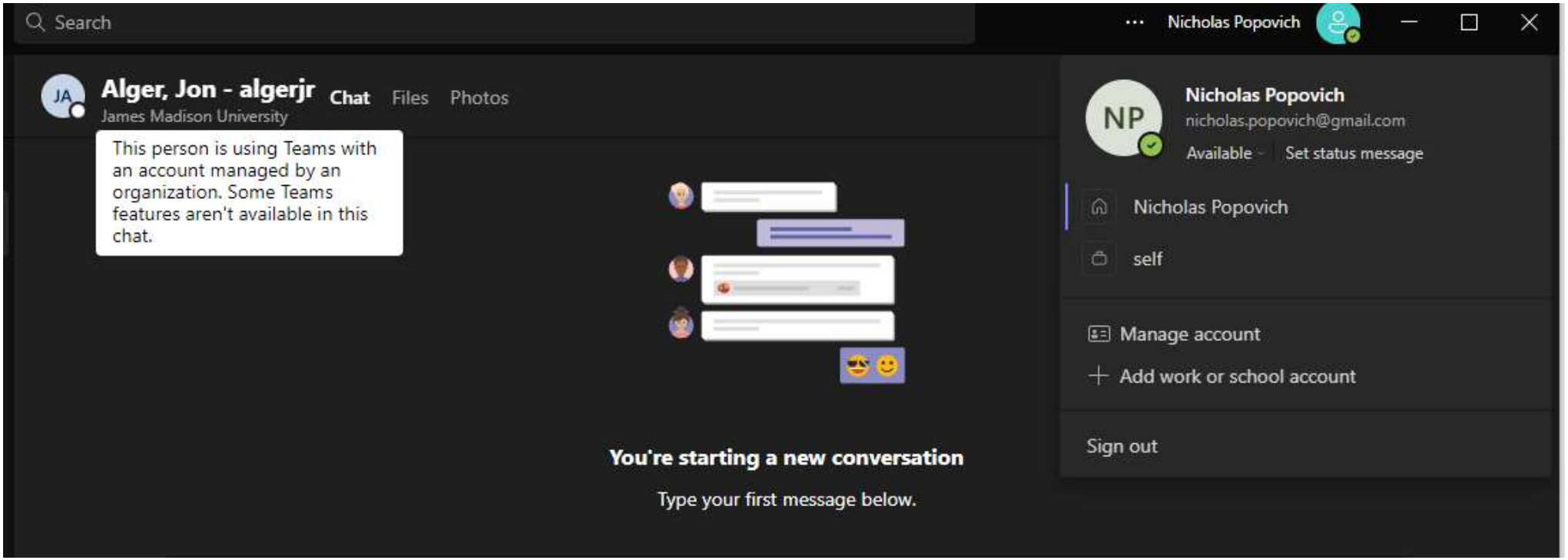


PRACTICAL EXAMPLE – MS Teams



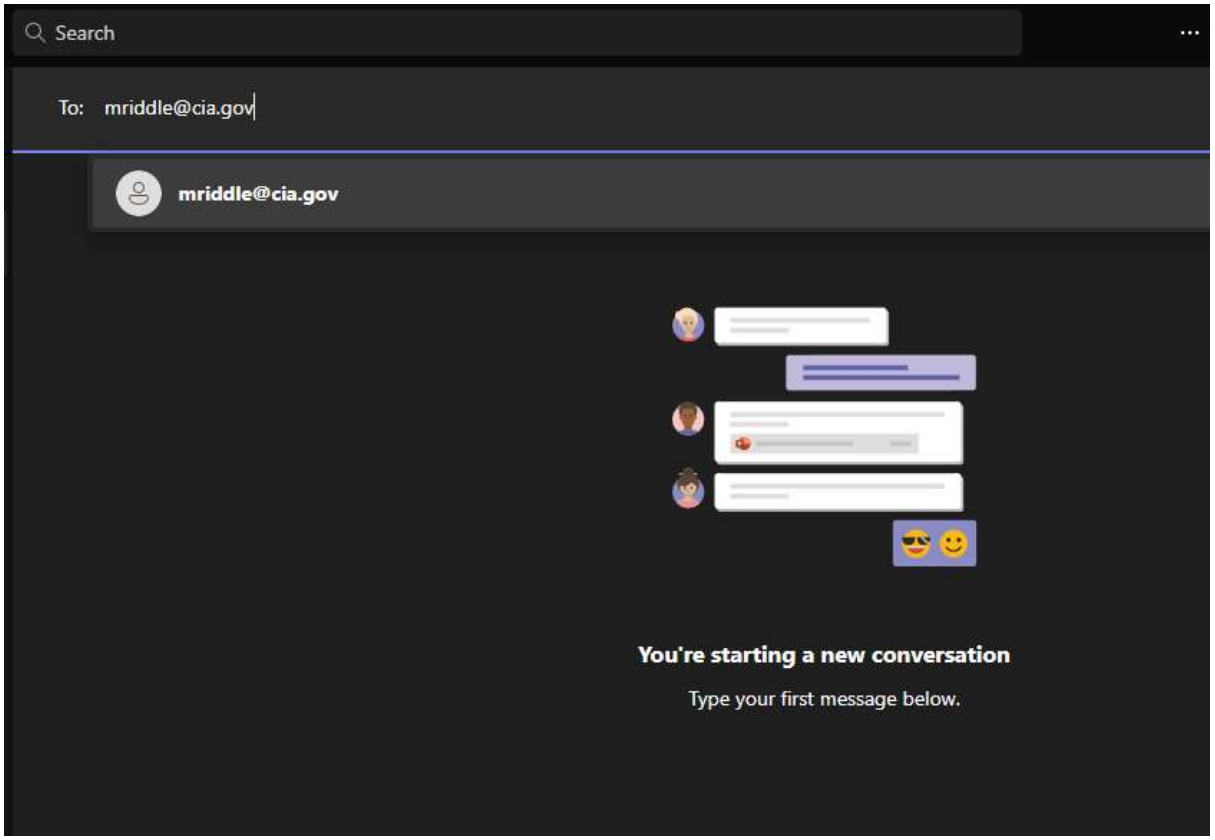


PRACTICAL EXAMPLE – MS Teams

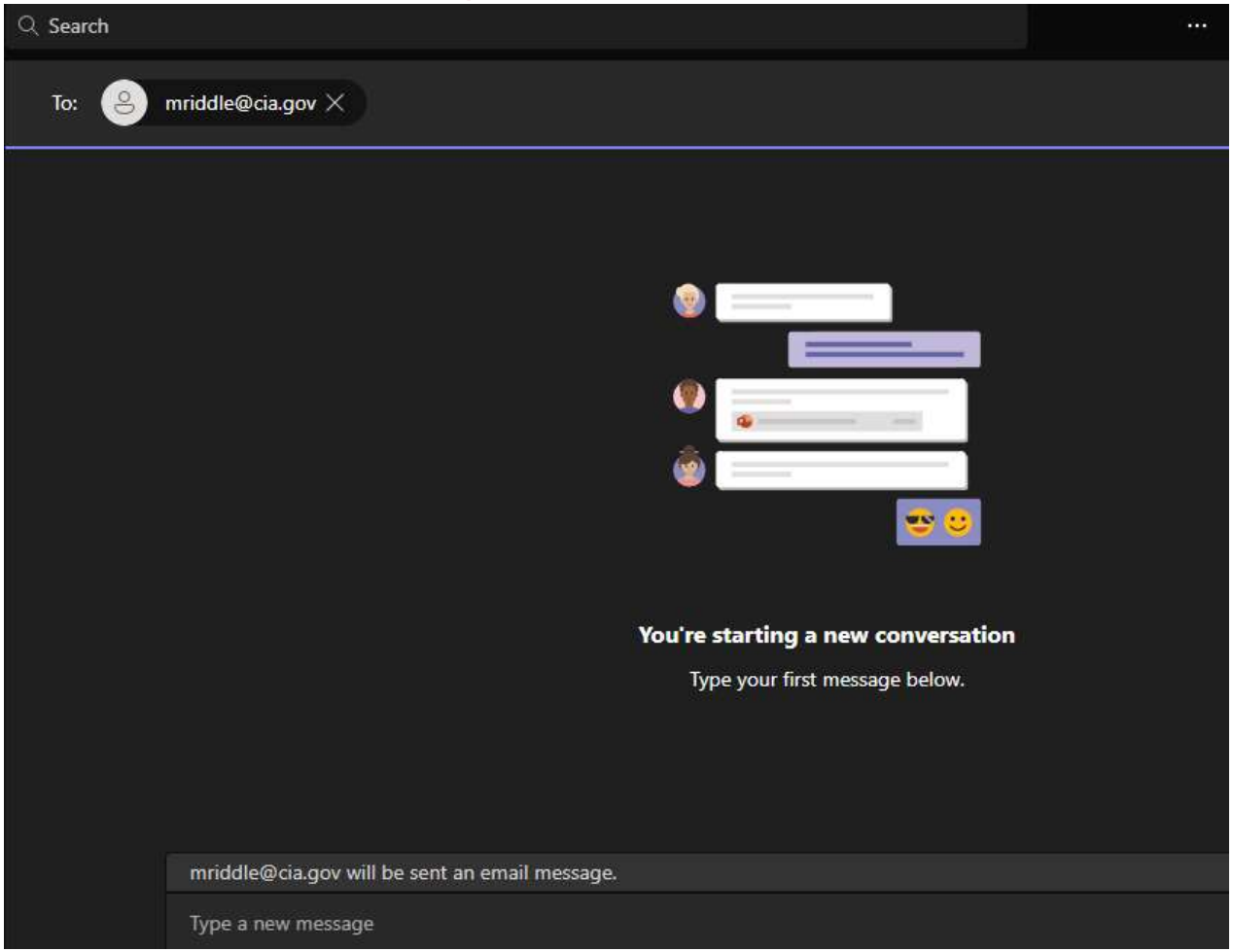


PRACTICAL EXAMPLE – MS Teams

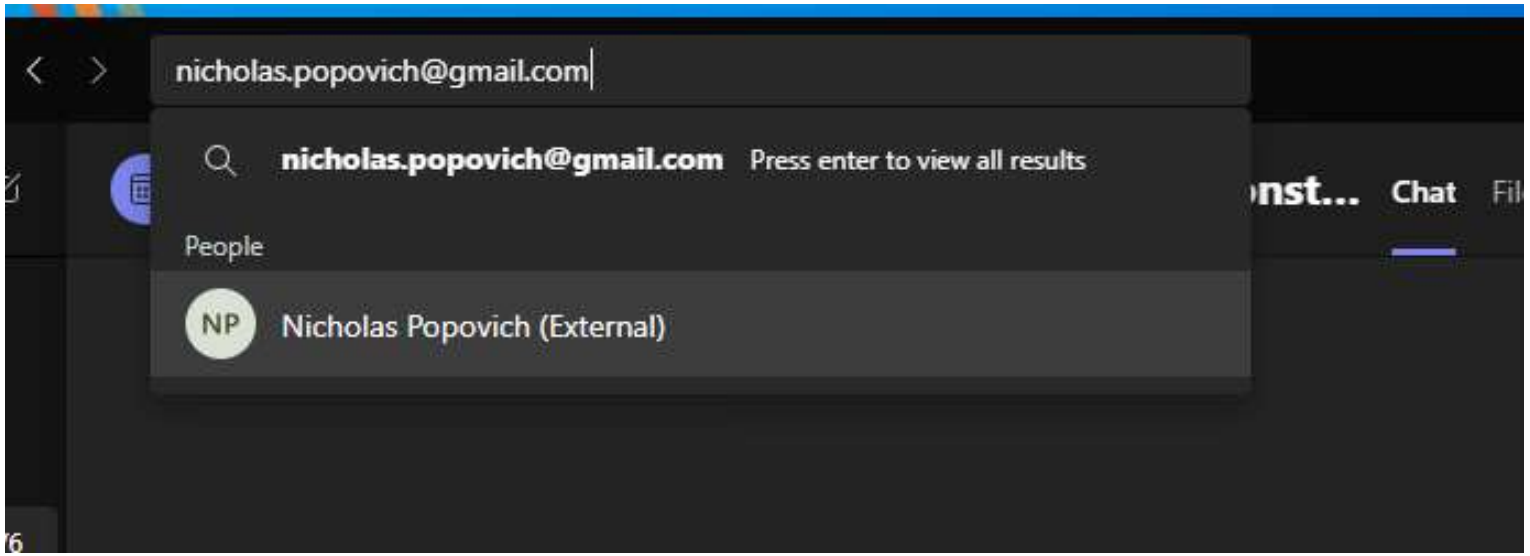
ROTAS SECURITY



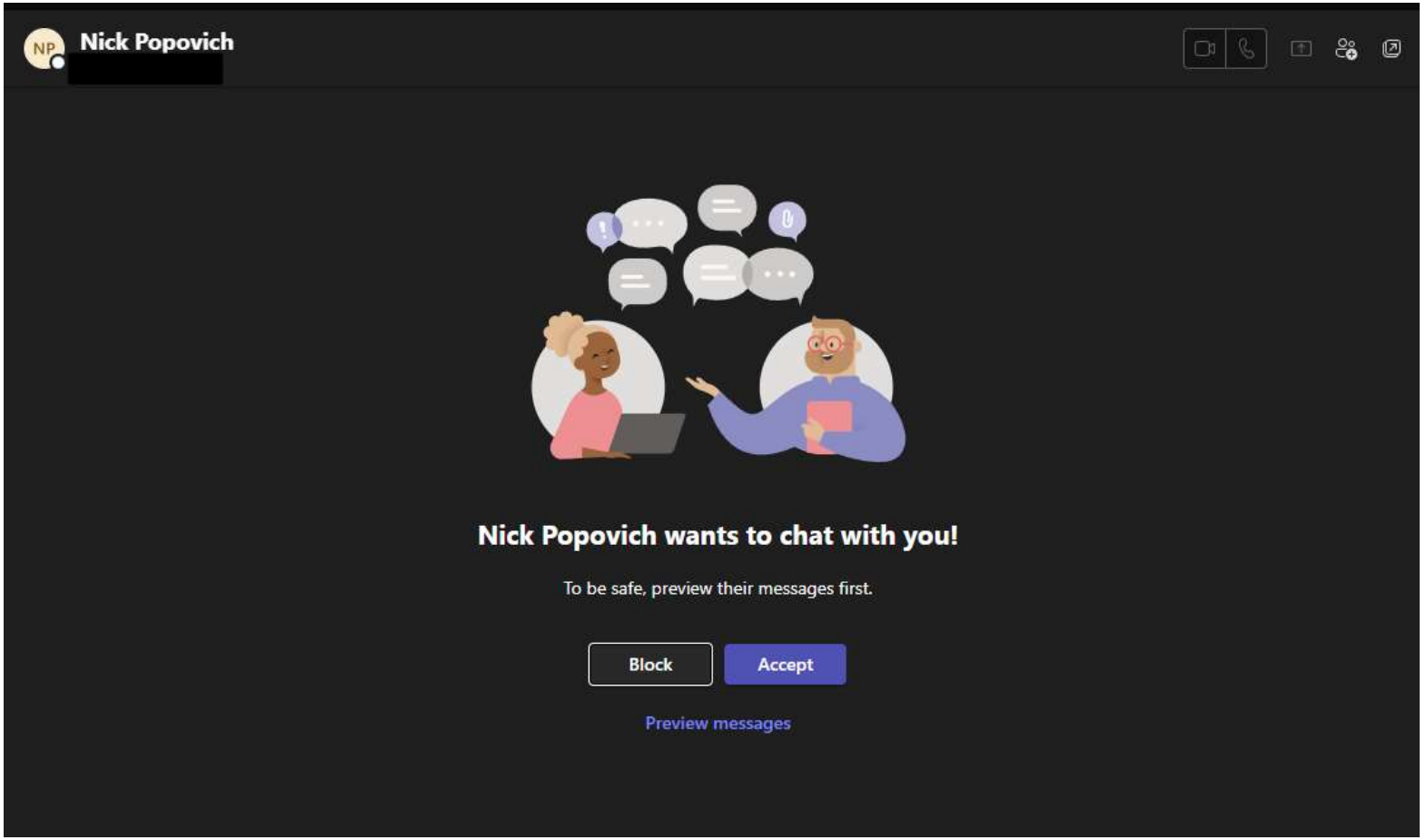
PRACTICAL EXAMPLE – MS Teams



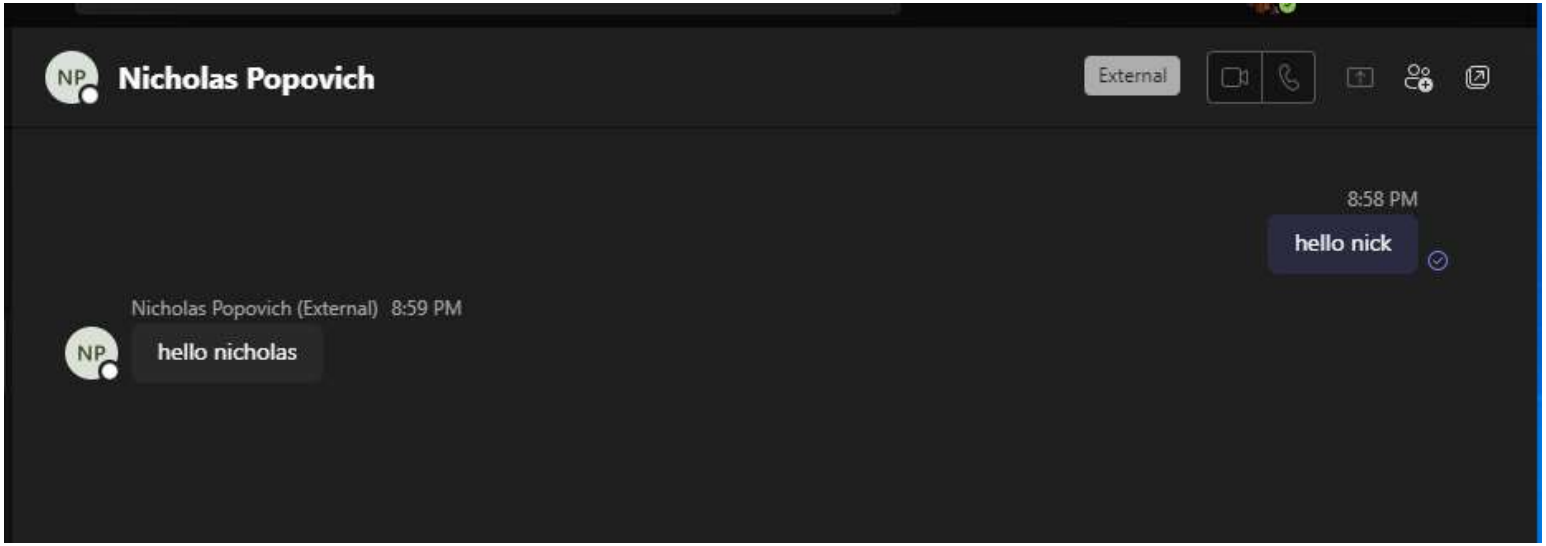
PRACTICAL EXAMPLE – MS Teams



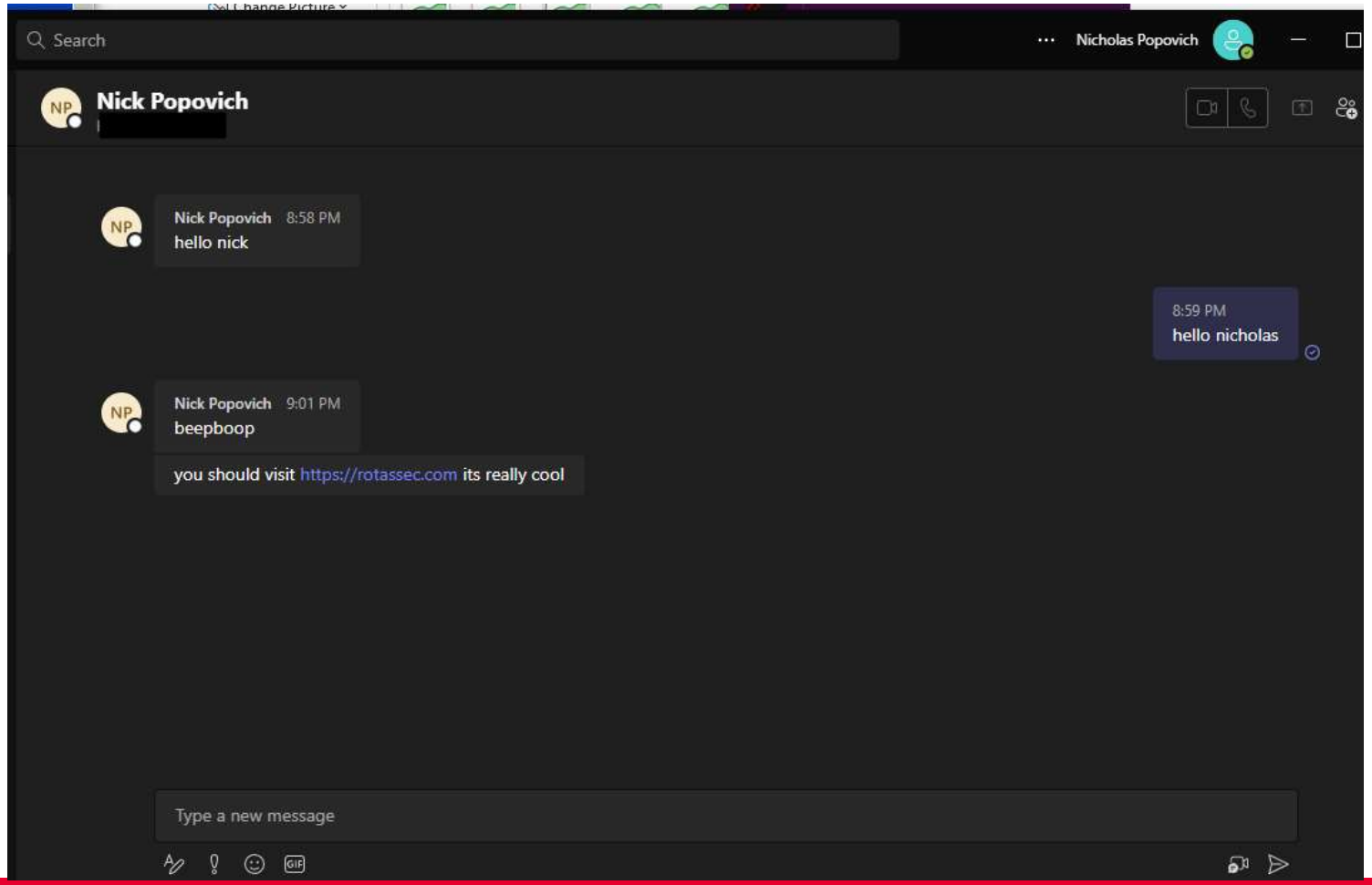
PRACTICAL EXAMPLE – MS Teams



PRACTICAL EXAMPLE – MS Teams



PRACTICAL EXAMPLE – MS Teams



PRACTICAL EXAMPLE – MS Teams

Ok, but at least external users can't attach files…

Oh sweet, sweet child.

Jun 21, 2023

https://labs.jumpsec.com/advisory-idor-in-microsoft-teams-allows-for-external-tenants-to-introduce-malware/

"Max Corbridge (@CorbridgeMax) and Tom Ellson (@tde_sec) of JUMPSEC's Red Team recently discovered a vulnerability in the latest version of Microsoft Teams which allows for the possible introduction of malware into any organisations using Microsoft Teams in its default configuration."

PRACTICAL EXAMPLE – MS Teams

Ok, but at least it requires advanced l33t hax0r skillz…

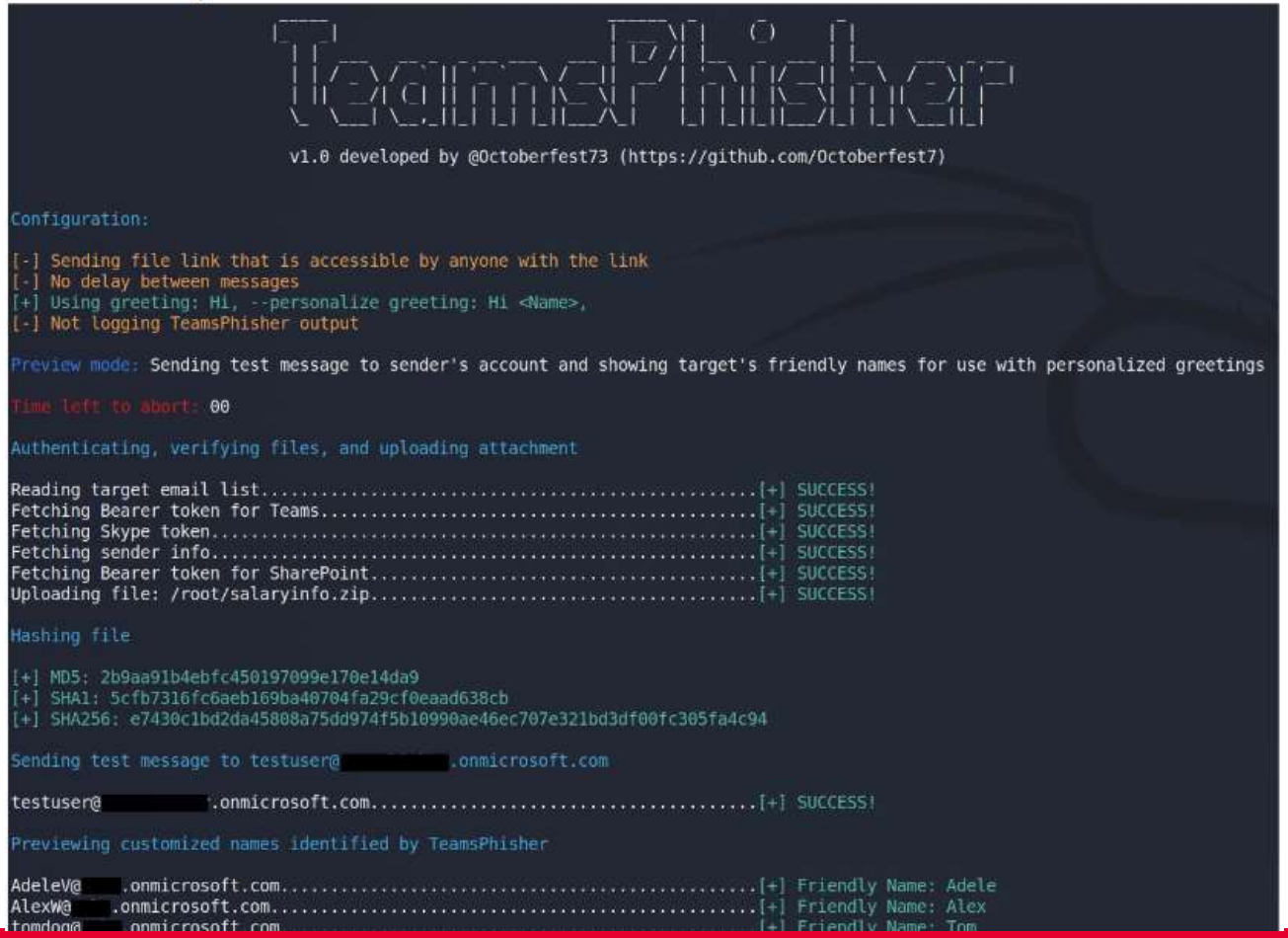
July 5, 2023

https://github.com/Octoberfest7/TeamsPhisher

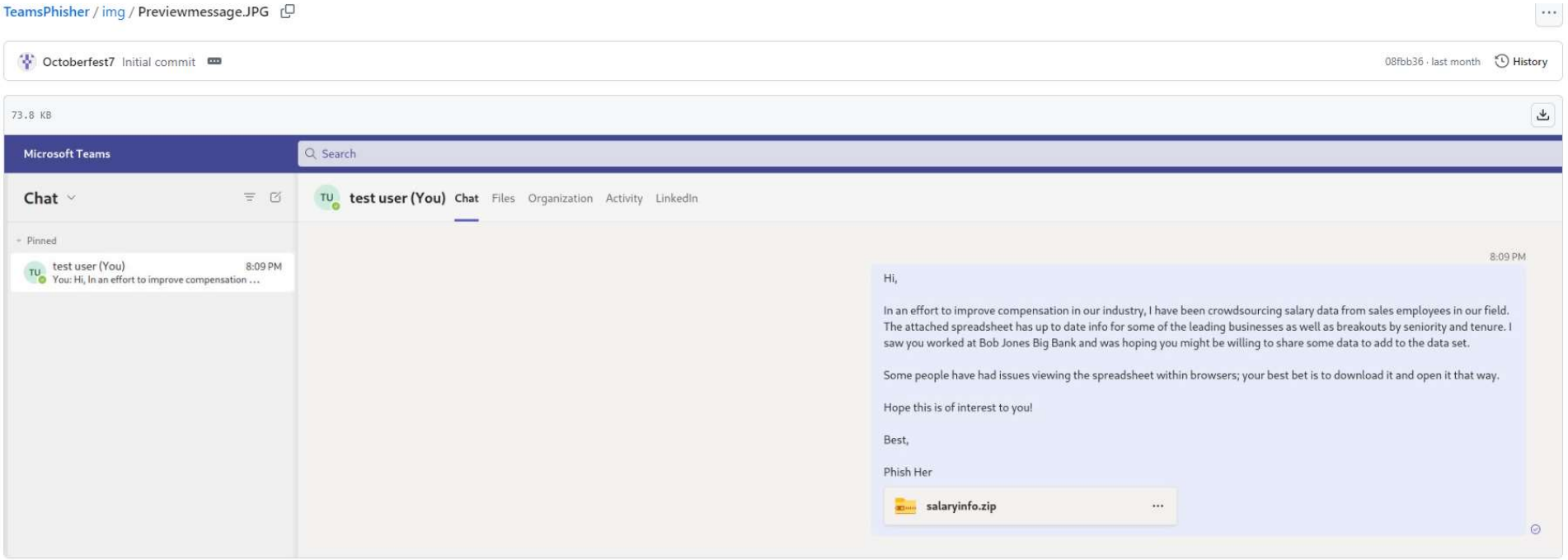
"Give TeamsPhisher an attachment, a message, and a list of target Teams users. It will upload the attachment to the sender's Sharepoint, and then iterate through the list of targets," reads the description from Alex Reid, the developer of the red team utility."

PRACTICAL EXAMPLE – MS Teams

TeamsPhisher output:



PRACTICAL EXAMPLE – MS Teams



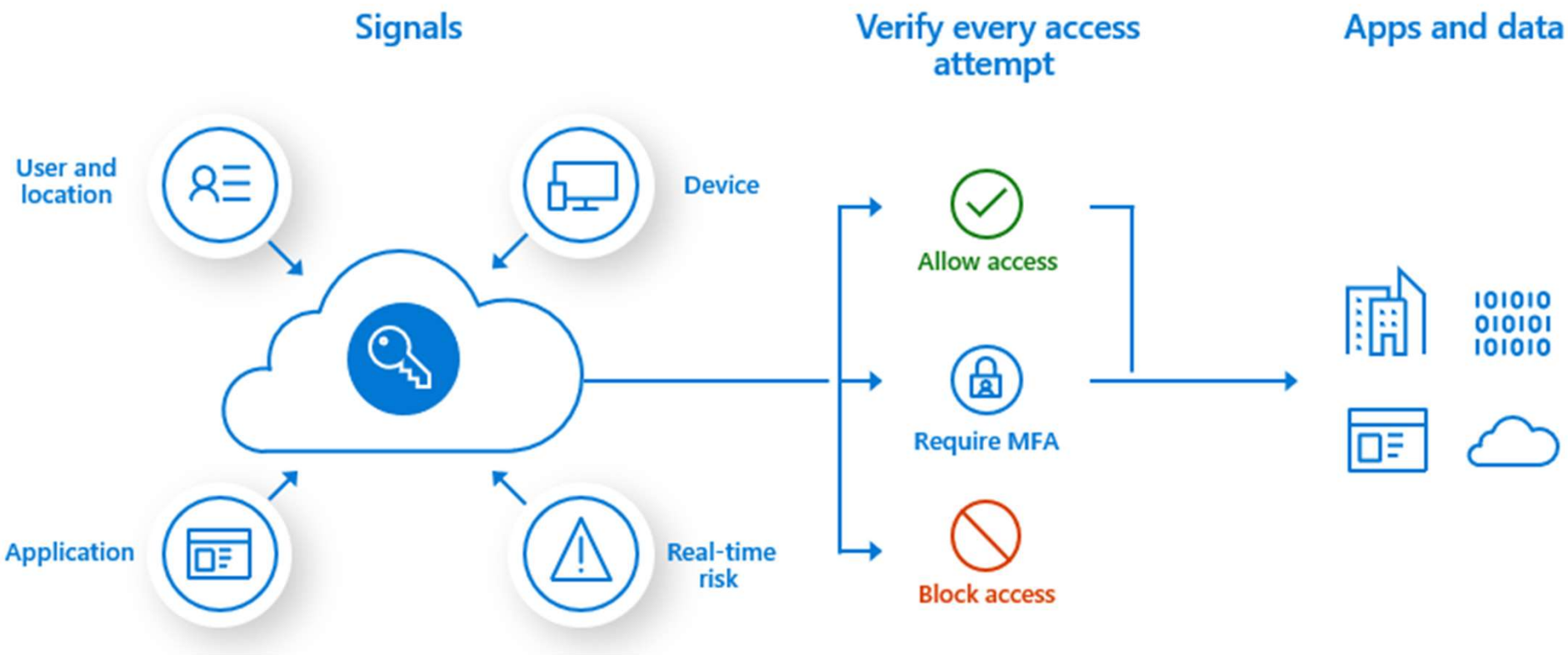
PRACTICAL EXAMPLE – Conditional Access Policies

Azure Conditional Access is a feature of Azure Active Directory (Azure AD) that enables organizations to define and enforce policies that evaluate specific conditions and determine when and how users can access certain resources.

PRACTICAL EXAMPLE – Conditional Access Policies

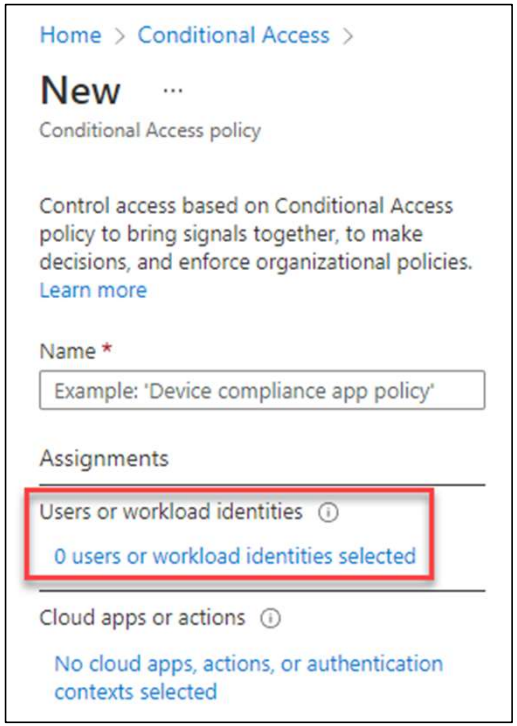
- Assignments:
  - Users and Groups: Specifies which users and groups the policy applies to. You can target all users, specific groups, or exclude certain users/groups.
  - Cloud Apps or Actions: Specifies the applications or actions the policy applies to. This can be any cloud app integrated with Azure AD or specific actions like registering a security information.
- Conditions:
  - Sign-in Risk: Evaluates the risk involved in a sign-in based on Azure AD's real-time and offline risk detection.
  - Device Platform: Specifies conditions based on the platform like Windows, macOS, Android, or iOS.
  - Locations: Defines trusted locations based on IP ranges or named locations.
  - Client Apps: Differentiates between browser, mobile apps and desktop clients, Exchange ActiveSync, etc.
  - Device State: Considers whether a device is marked as compliant or hybrid Azure AD joined.
- Access Controls:
  - Grant: Specifies the requirements to grant access. This can include requiring multi-factor authentication (MFA), requiring the device to be marked as compliant, or requiring Hybrid Azure AD joined device.
  - Session: Allows for enforcing session limitations, like requiring reauthentication after a certain period or making apps read-only.

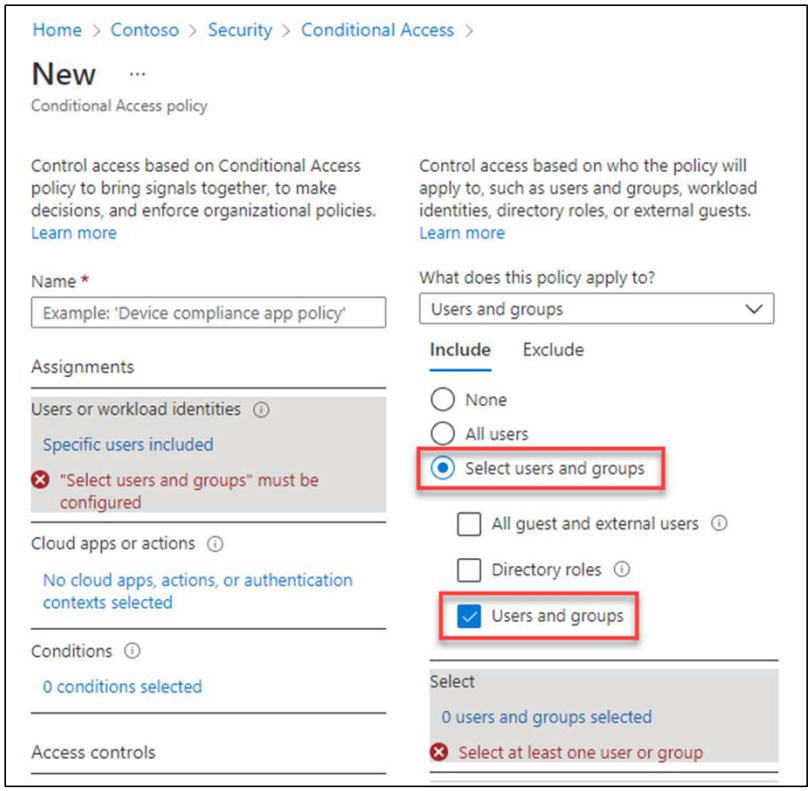
PRACTICAL EXAMPLE – Conditional Access Policies



https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

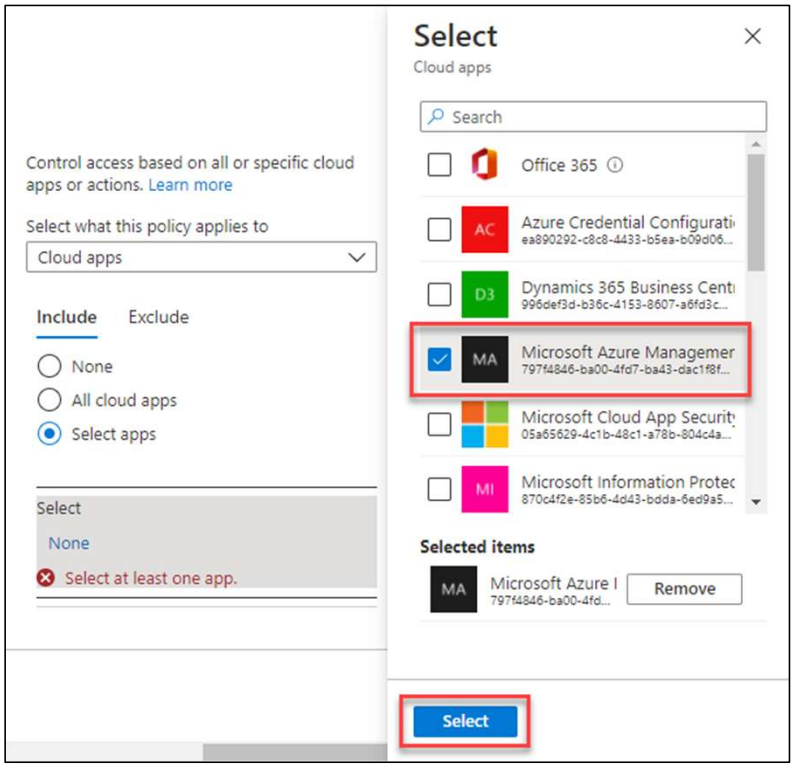
PRACTICAL EXAMPLE – Conditional Access Policies

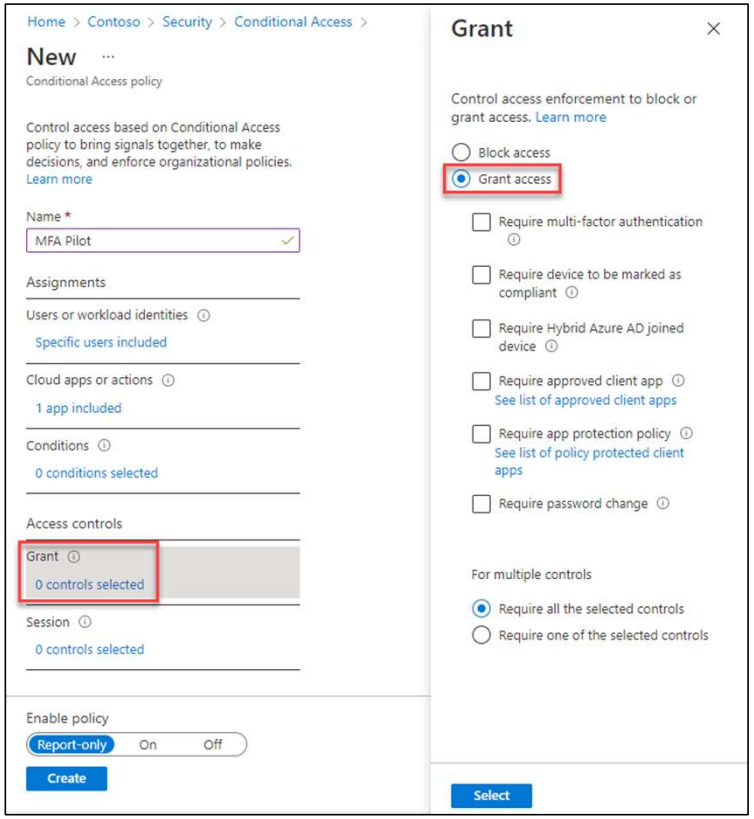




https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

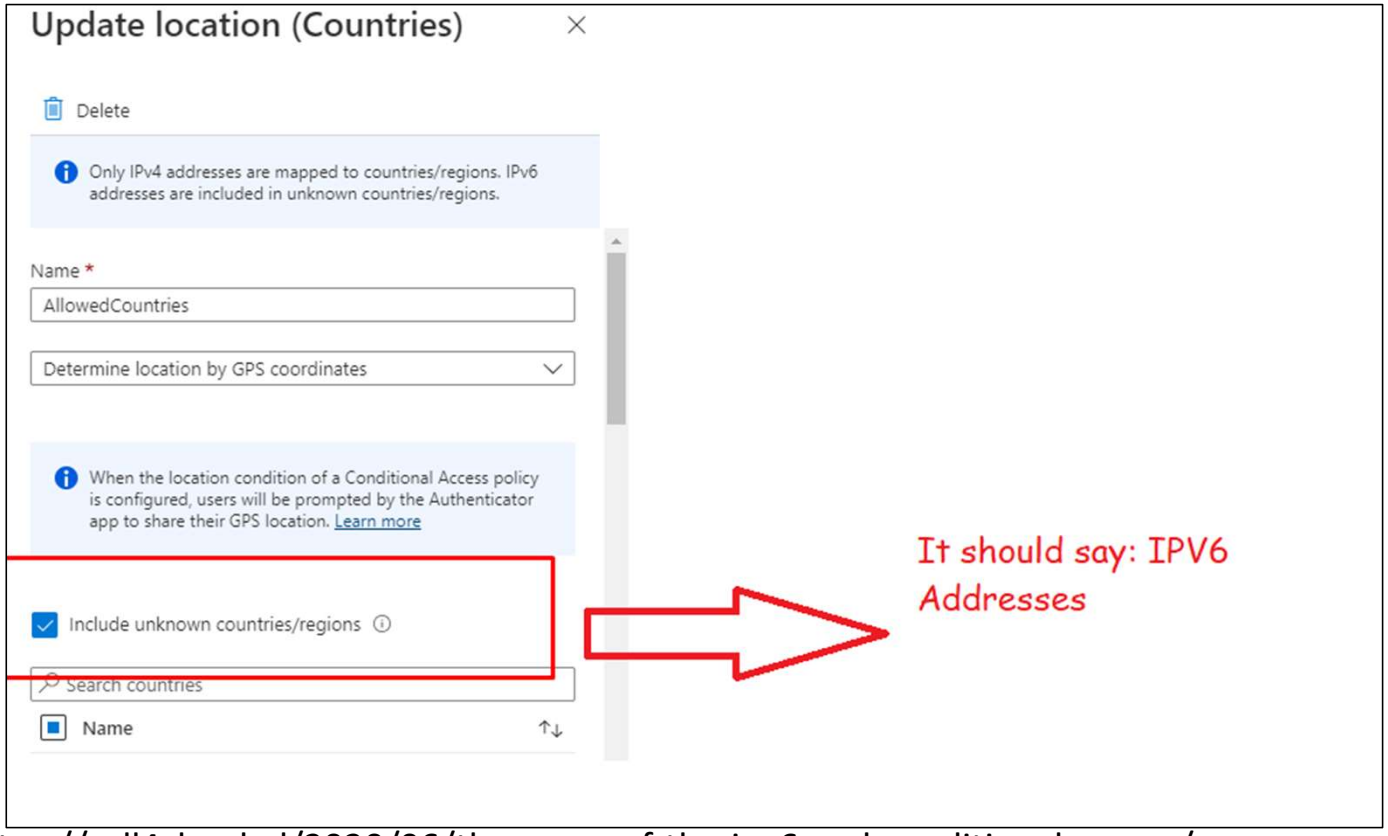
PRACTICAL EXAMPLE – Conditional Access Policies





https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

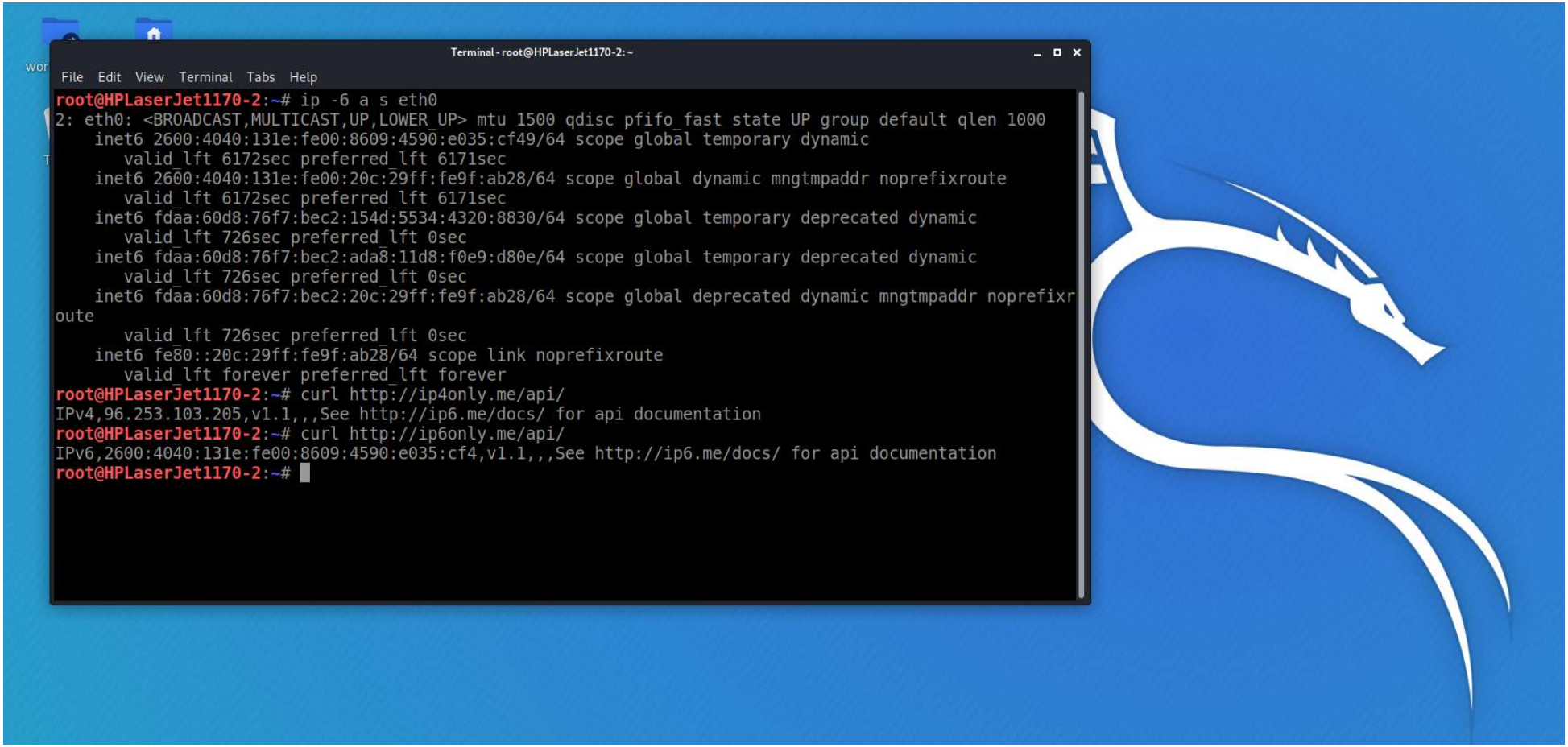
PRACTICAL EXAMPLE – Conditional Access Policies



https://call4cloud.nl/2020/06/the-curse-of-the-ipv6-and-conditional-access/

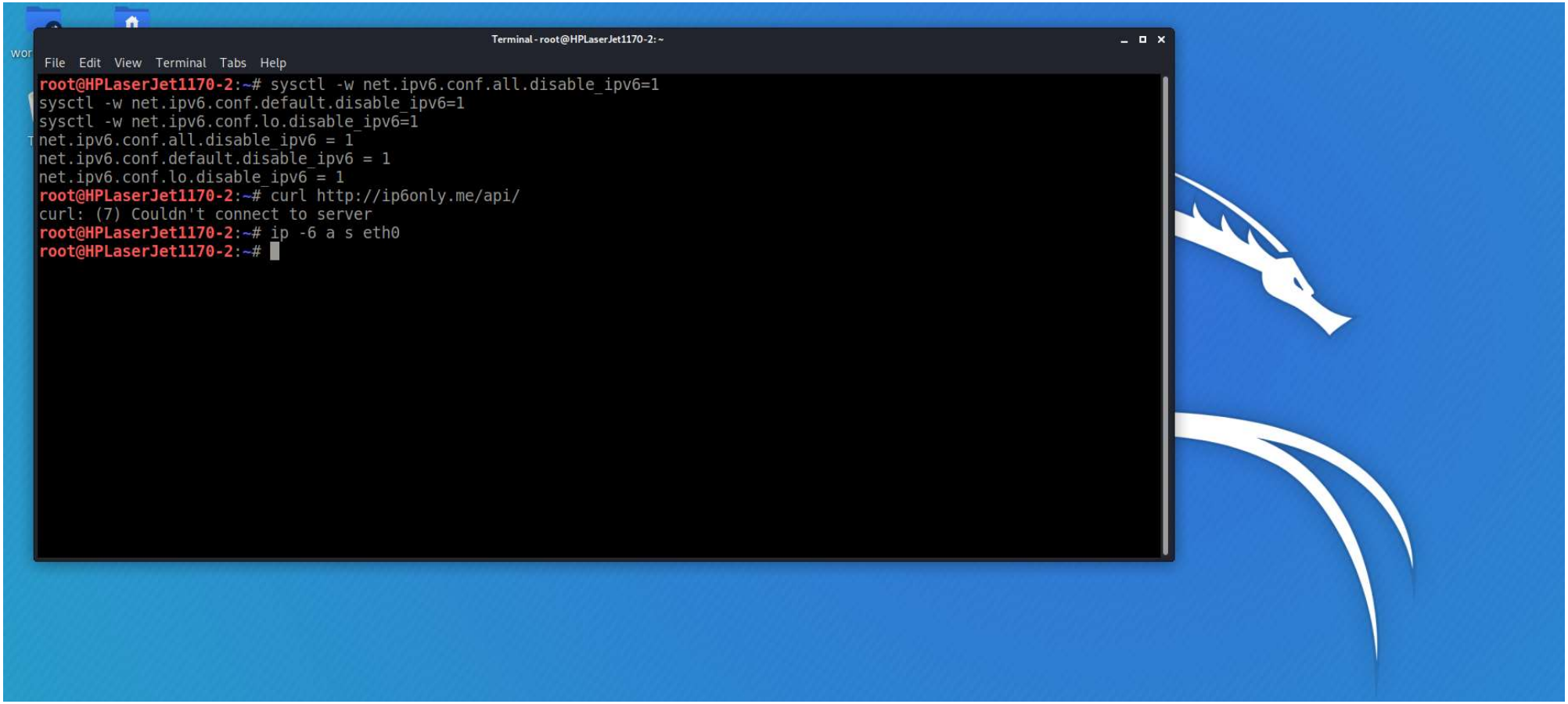
PRACTICAL EXAMPLE – Conditional Access Policies

ROTAS SECURITY

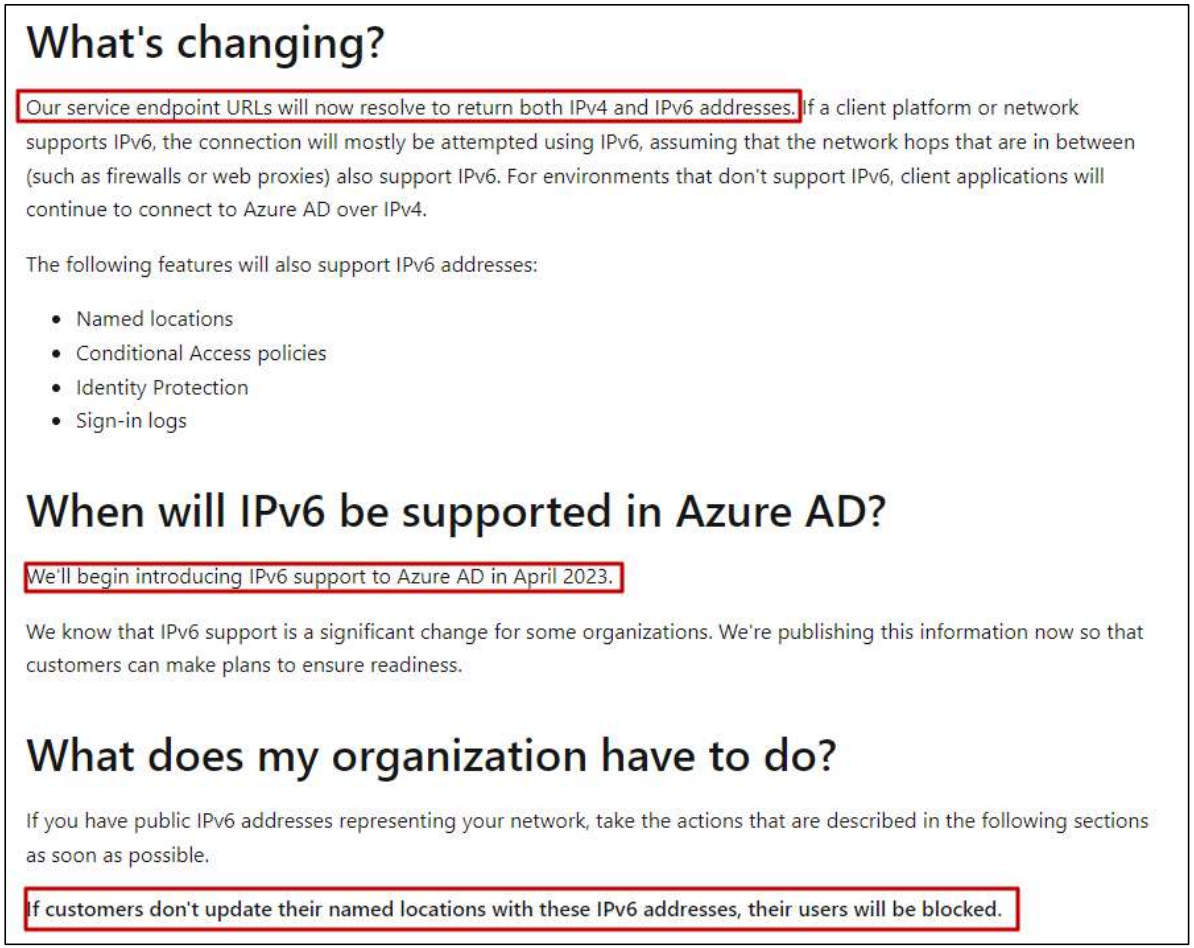


PRACTICAL EXAMPLE – Conditional Access Policies

ROTAS SECURITY



PRACTICAL EXAMPLE – Conditional Access Policies



What's changing?

Our service endpoint URLs will now resolve to return both IPv4 and IPv6 addresses. If a client platform or network supports IPv6, the connection will mostly be attempted using IPv6, assuming that the network hops that are in between (such as firewalls or web proxies) also support IPv6. For environments that don't support IPv6, client applications will continue to connect to Azure AD over IPv4.

The following features will also support IPv6 addresses:

- Named locations
- Conditional Access policies
- Identity Protection
- Sign-in logs

When will IPv6 be supported in Azure AD?

We'll begin introducing IPv6 support to Azure AD in April 2023.

We know that IPv6 support is a significant change for some organizations. We're publishing this information now so that customers can make plans to ensure readiness.

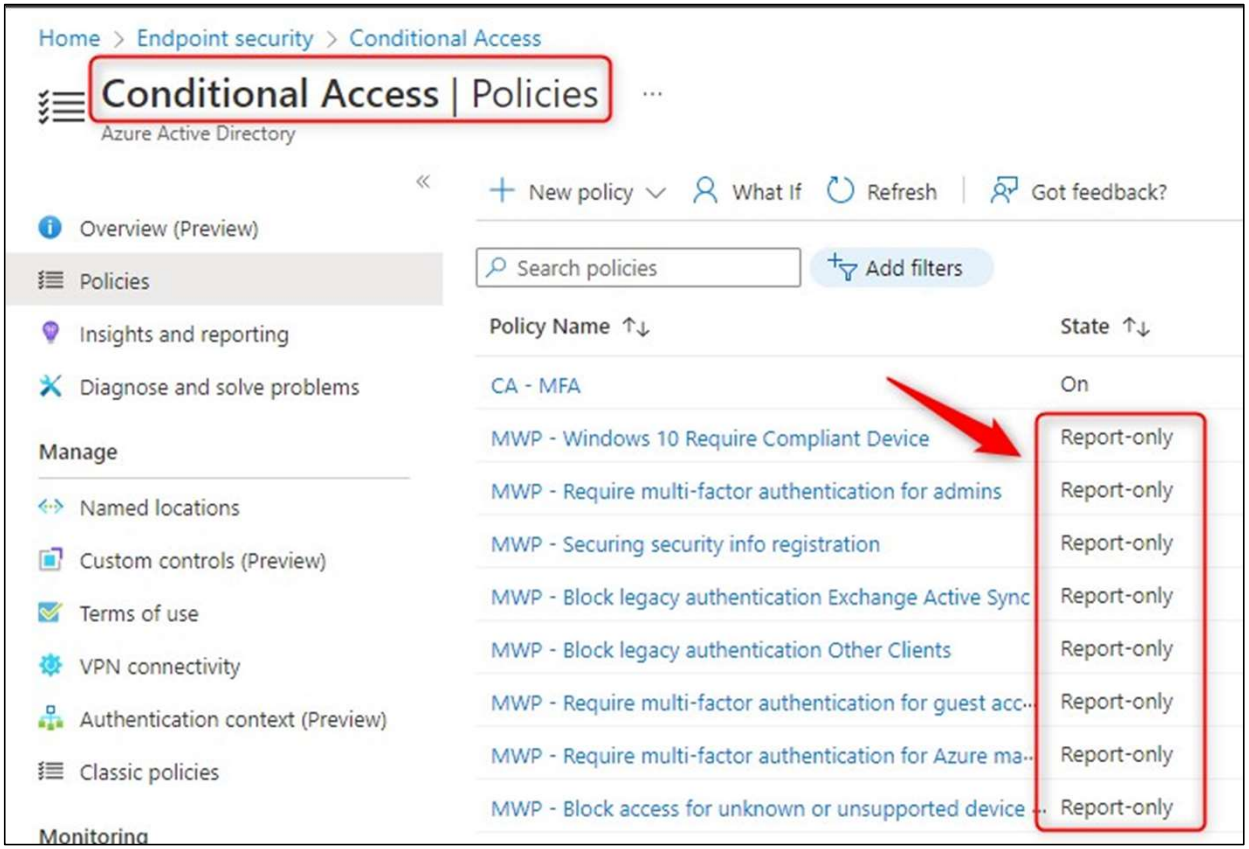
What does my organization have to do?

If you have public IPv6 addresses representing your network, take the actions that are described in the following sections as soon as possible.

If customers don't update their named locations with these IPv6 addresses, their users will be blocked.

PRACTICAL EXAMPLE – Conditional Access Policies

ROTAS SECURITY



PRACTICAL EXAMPLE – Conditional Access Policies

ROTAS SECURITY

Device platforms

Conditional Access identifies the device platform by using information provided by the device, such as user agent strings. Since user agent strings can be modified, this information is unverified. Device platform should be used in concert with Microsoft Intune device compliance policies or as part of a block statement. The default is to apply to all device platforms.

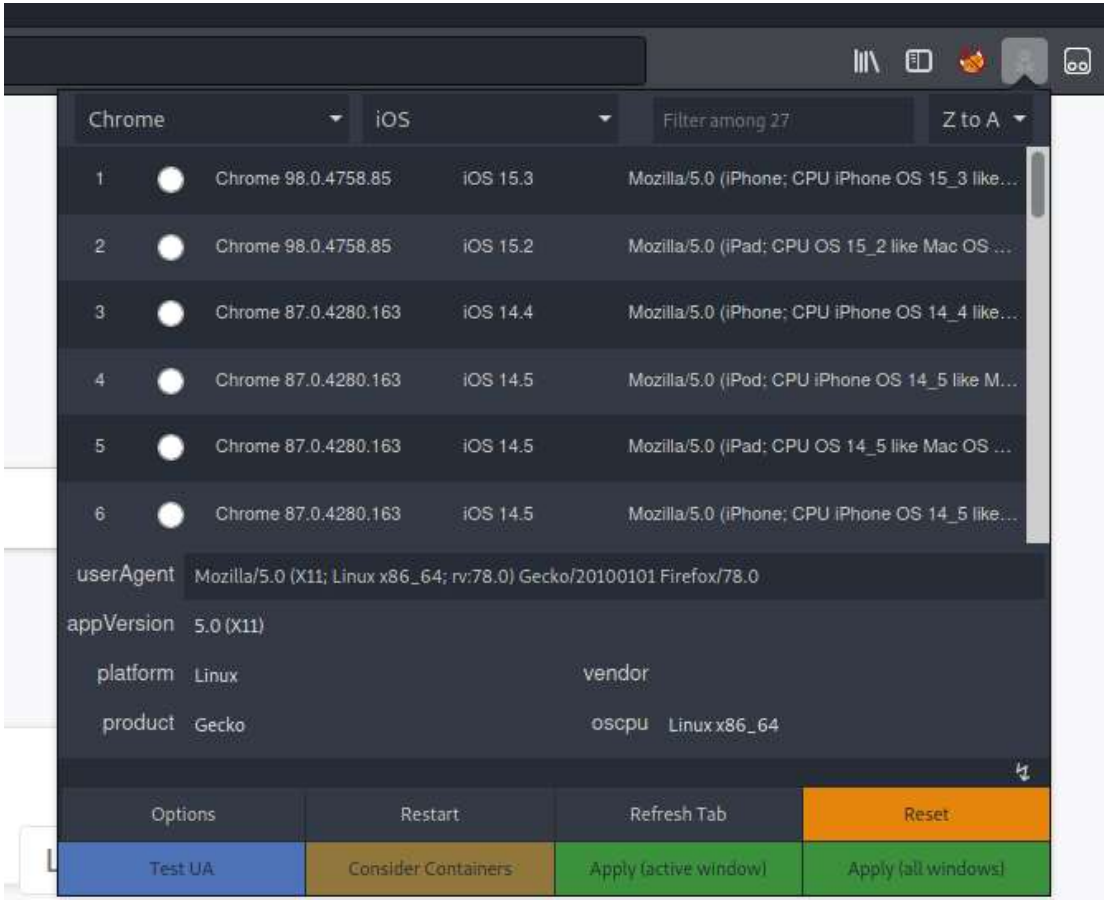
Conditional Access supports the following device platforms:

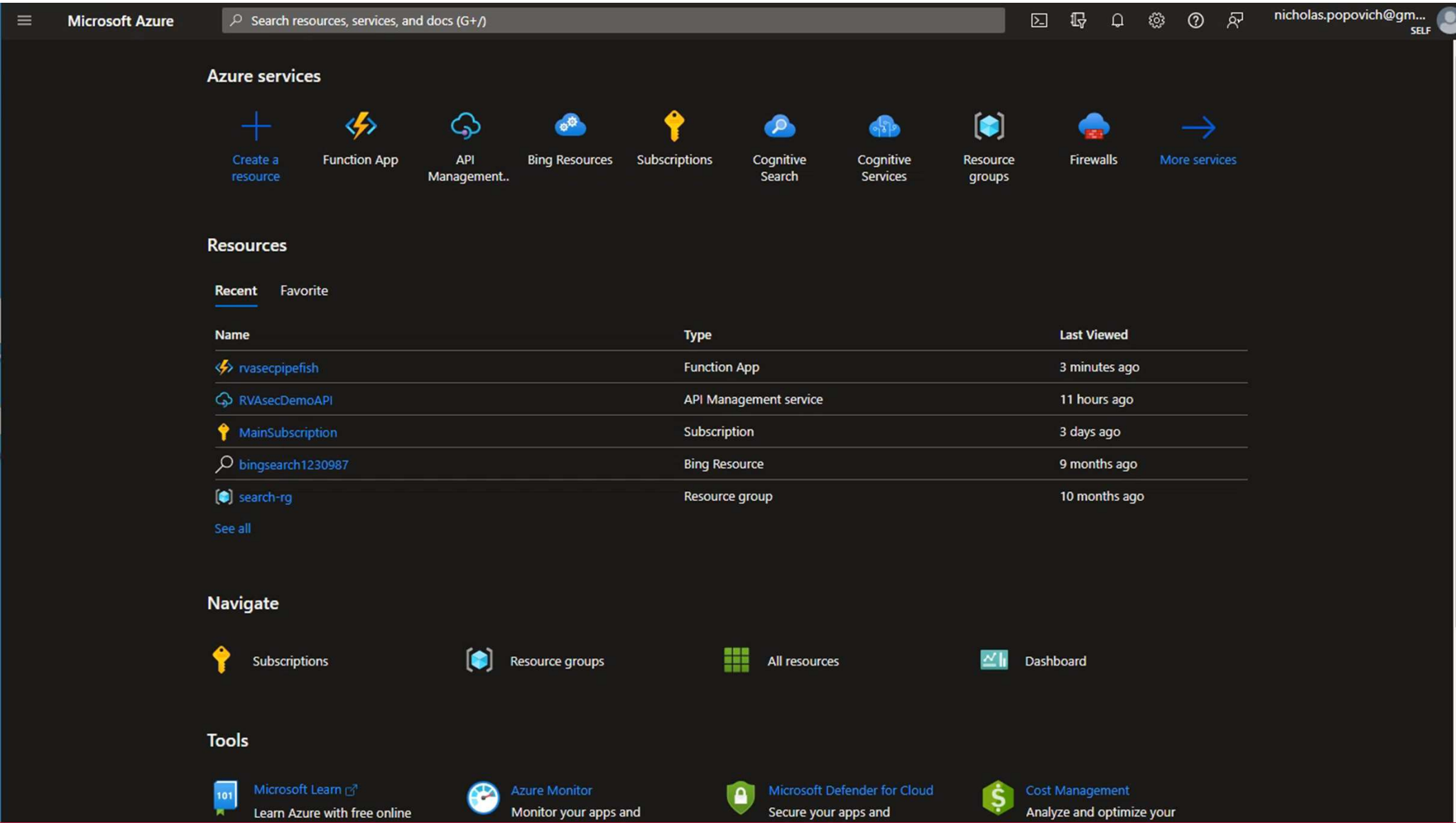
- Android
- iOS
- Windows
- macOS
- Linux

If you block legacy authentication using the **Other clients** condition, you can also set the device platform condition.

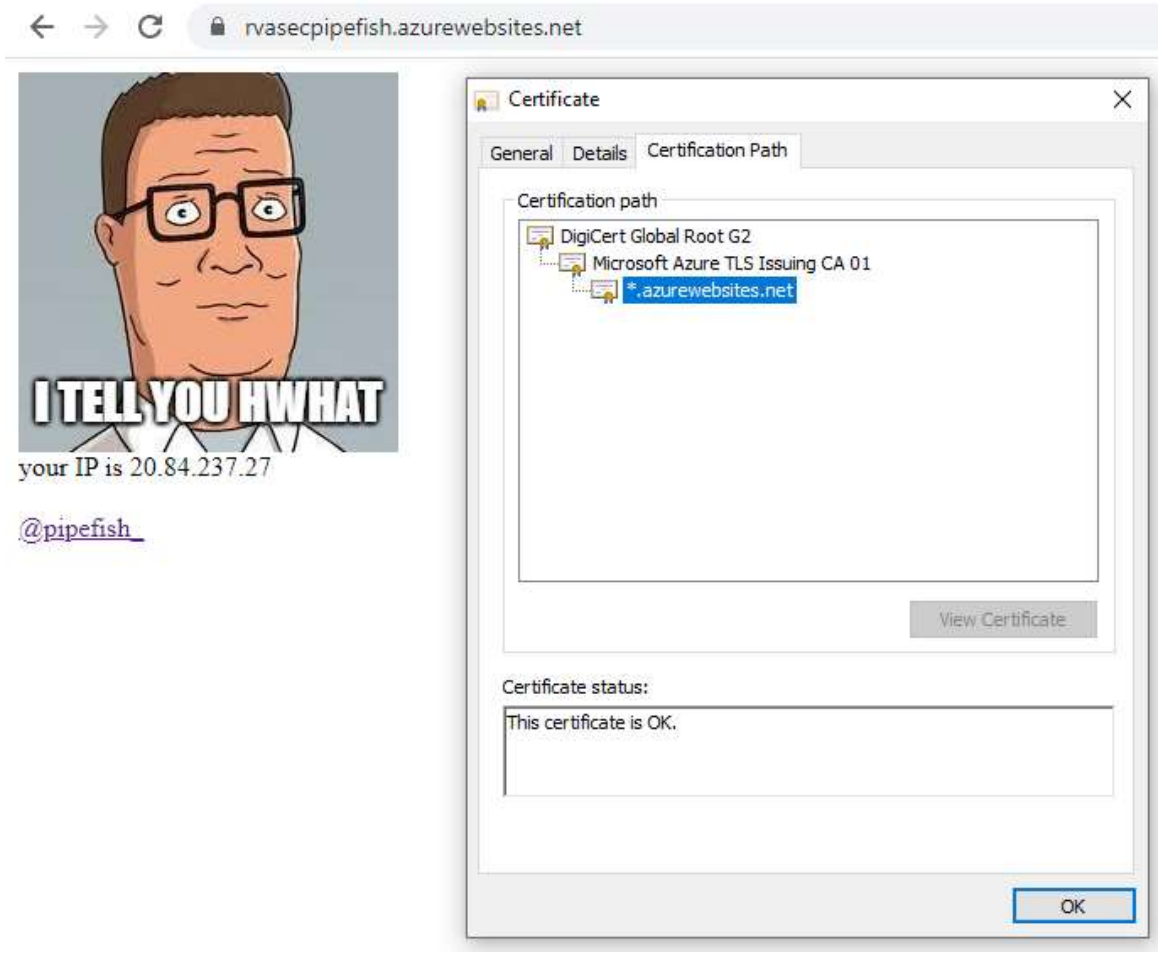
PRACTICAL EXAMPLE – Conditional Access Policies

ROTAS SECURITY




Microsoft Azure
Search resources, services, and docs (G+/)
nicholas.popovich@gm...
SELF
Azure services
Create a resource
Function App
API Management..
Bing Resources
Subscriptions
Cognitive Search
Cognitive Services
Resource groups
Firewalls
More services
Resources
Recent
Favorite
Name
Type
Last Viewed
rvasecpipefish
Function App
3 minutes ago
RVAsecDemoAPI
API Management service
11 hours ago
MainSubscription
Subscription
3 days ago
bingsearch1230987
Bing Resource
9 months ago
search-rg
Resource group
10 months ago
See all
Navigate
Subscriptions
Resource groups
All resources
Dashboard
Tools
Microsoft Learn
Learn Azure with free online
Azure Monitor
Monitor your apps and
Microsoft Defender for Cloud
Secure your apps and
Cost Management
Analyze and optimize your

PRACTICAL EXAMPLE – Conditional Access Policies



PRACTICAL EXAMPLE – Conditional Access Policies

ROTAS SECURITY

Whois IP 20.84.237.27

Updated 1 second ago

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#


NetRange:       20.33.0.0 - 20.128.255.255
CIDR:           20.128.0.0/16, 20.64.0.0/10, 20.48.0.0/12, 20.34.0.0/15, 20.3
NetName:        MSFT
NetHandle:      NET-20-33-0-0-1
Parent:         NET20 (NET-20-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Microsoft Corporation (MSFT)
RegDate:        2017-10-18
Updated:        2021-12-14
Ref:            https://rdap.arin.net/registry/ip/20.33.0.0


OrgName:        Microsoft Corporation
OrgId:          MSFT
Address:        One Microsoft Way
City:           Redmond
```

PRACTICAL EXAMPLE – Azure AD (ok ok Entra ID)

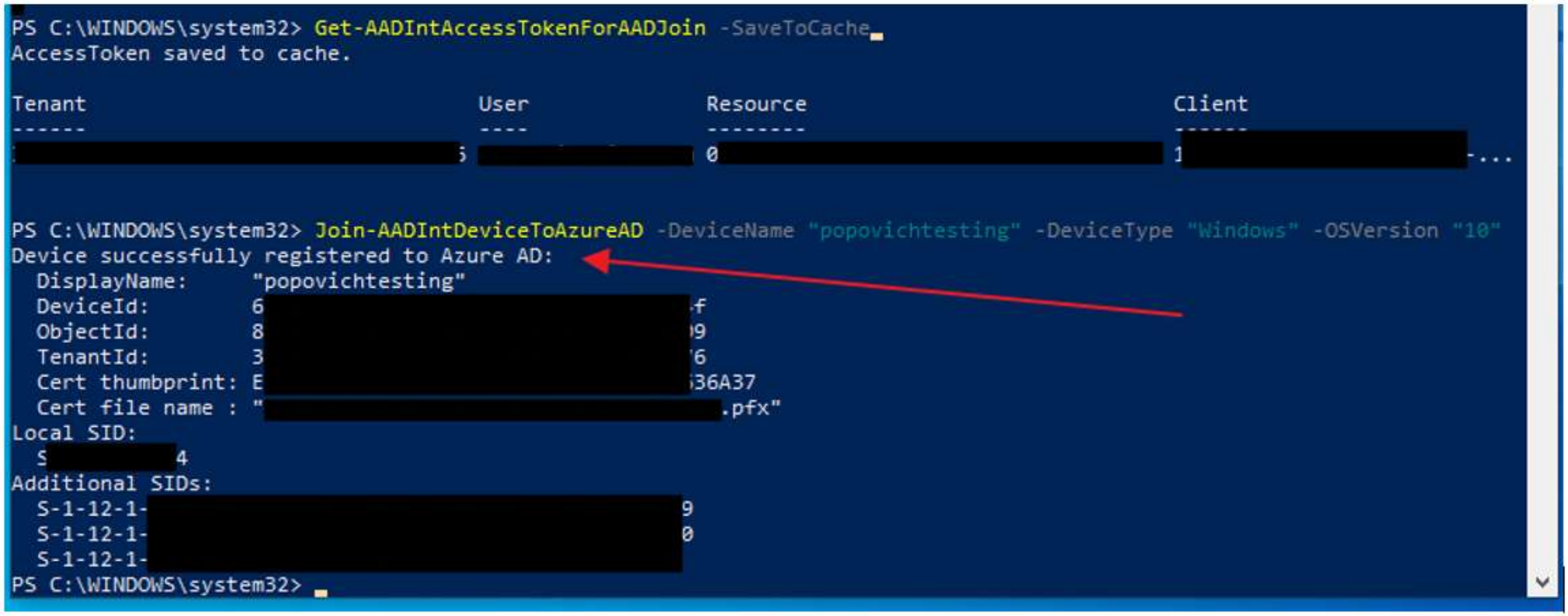
I wasn't sure if this was related to CA Policy before, but it was also related to Azure AD, and combined multiple bypasses. So, here it is...

PRACTICAL EXAMPLE – Azure AD (ok ok Entra ID)

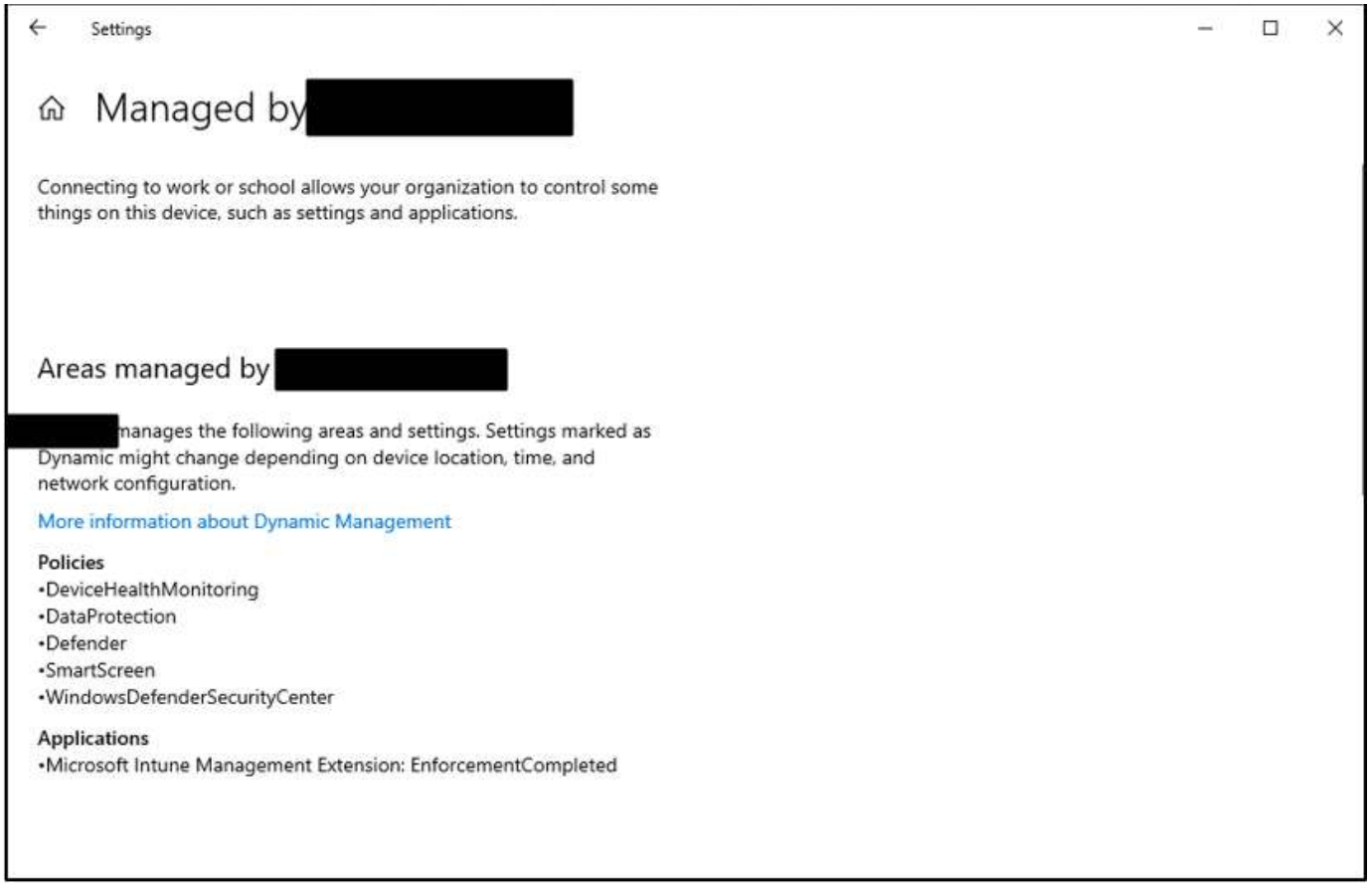
ROTAS SECURITY

- Some quick resource highlights
  - https://msportals.io – amazing list of management portal direct links for o365/azure
  - https://github.com/dafthack/MFASweep - MFASweep is a PowerShell script that attempts to log in to various Microsoft services using a provided set of credentials and will attempt to identify if MFA is enabled.
  - https://github.com/dafthack/MSOLSpray - A password spraying tool for Microsoft Online accounts (Azure/O365).
  - https://github.com/initstring/cloud_enum - Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud.

PRACTICAL EXAMPLE – Azure AD (ok ok Entra ID)

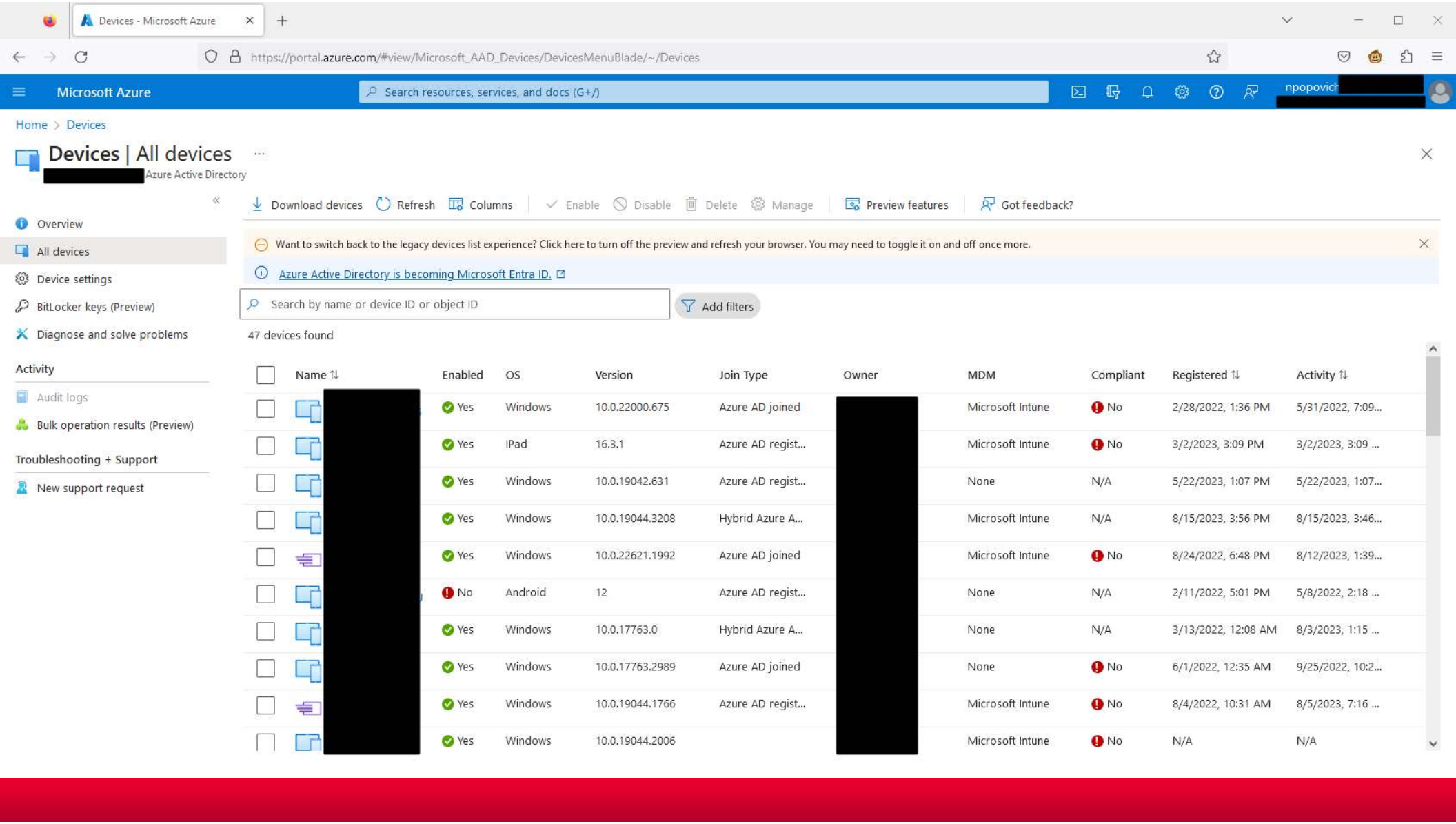


PRACTICAL EXAMPLE – Azure AD (ok ok Entra ID)



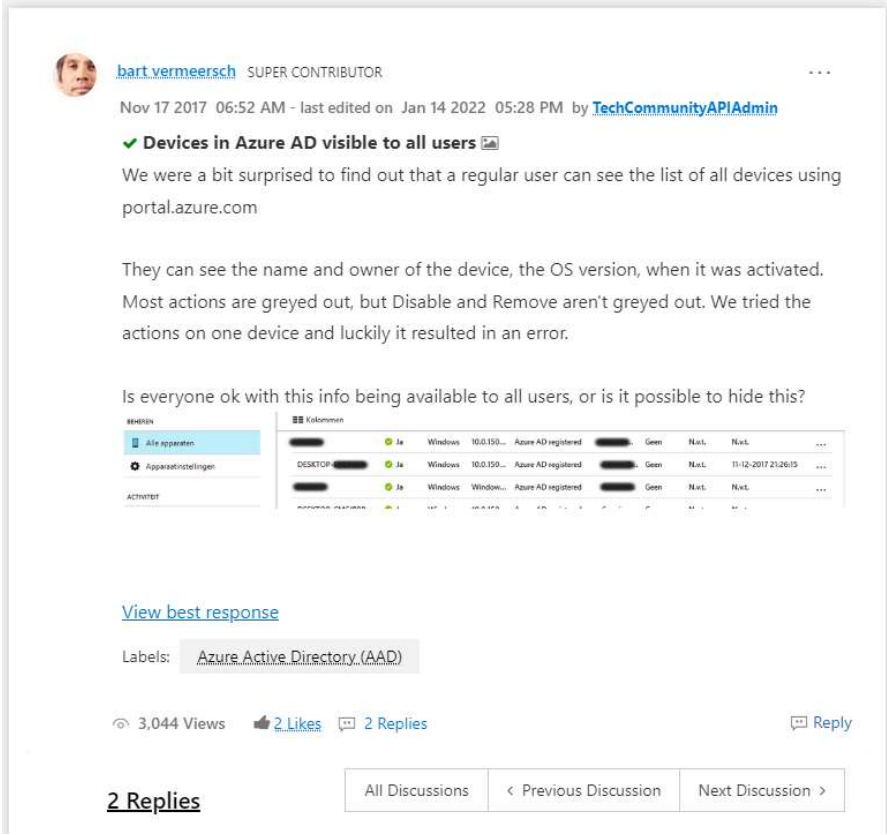
PRACTICAL EXAMPLE – Azure AD (ok ok Entra ID)

Note browsing to this URL directly in Azure Portal lists all domain joined devices, and ignores permissions settings:
https://portal.azure.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/Devices


Devices - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/Devices
Microsoft Azure
Search resources, services, and docs (G+/)
npopovich
Home > Devices
Devices | All devices
Azure Active Directory
Download devices
Refresh
Columns
Enable
Disable
Delete
Manage
Preview features
Got feedback?
Overview
All devices
Device settings
BitLocker keys (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Want to switch back to the legacy devices list experience? Click here to turn off the preview and refresh your browser. You may need to toggle it on and off once more.
Azure Active Directory is becoming Microsoft Entra ID.
Search by name or device ID or object ID
Add filters
47 devices found
Name
Enabled
OS
Version
Join Type
Owner
MDM
Compliant
Registered
Activity
Yes Windows 10.0.22000.675 Azure AD joined Microsoft Intune No 2/28/2022, 1:36 PM 5/31/2022, 7:09...
Yes IPad 16.3.1 Azure AD regist... Microsoft Intune No 3/2/2023, 3:09 PM 3/2/2023, 3:09 ...
Yes Windows 10.0.19042.631 Azure AD regist... None N/A 5/22/2023, 1:07 PM 5/22/2023, 1:07...
Yes Windows 10.0.19044.3208 Hybrid Azure A... Microsoft Intune N/A 8/15/2023, 3:56 PM 8/15/2023, 3:46...
Yes Windows 10.0.22621.1992 Azure AD joined Microsoft Intune No 8/24/2022, 6:48 PM 8/12/2023, 1:39...
No Android 12 Azure AD regist... None N/A 2/11/2022, 5:01 PM 5/8/2022, 2:18 ...
Yes Windows 10.0.17763.0 Hybrid Azure A... None N/A 3/13/2022, 12:08 AM 8/3/2023, 1:15 ...
Yes Windows 10.0.17763.2989 Azure AD joined None No 6/1/2022, 12:35 AM 9/25/2022, 10:2...
Yes Windows 10.0.19044.1766 Azure AD regist... Microsoft Intune No 8/4/2022, 10:31 AM 8/5/2023, 7:16 ...
Yes Windows 10.0.19044.2006 Microsoft Intune No N/A N/A

PRACTICAL EXAMPLE – Azure AD (ok ok Entra ID)

https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad/devices-in-azure-ad-visible-to-all-users/m-p/129033



bart vermeersch SUPER CONTRIBUTOR

Nov 17 2017 06:52 AM - last edited on Jan 14 2022 05:28 PM by TechCommunityAPIAdmin

Devices in Azure AD visible to all users

We were a bit surprised to find out that a regular user can see the list of all devices using portal.azure.com

They can see the name and owner of the device, the OS version, when it was activated. Most actions are greyed out, but Disable and Remove aren't greyed out. We tried the actions on one device and luckily it resulted in an error.

Is everyone ok with this info being available to all users, or is it possible to hide this?

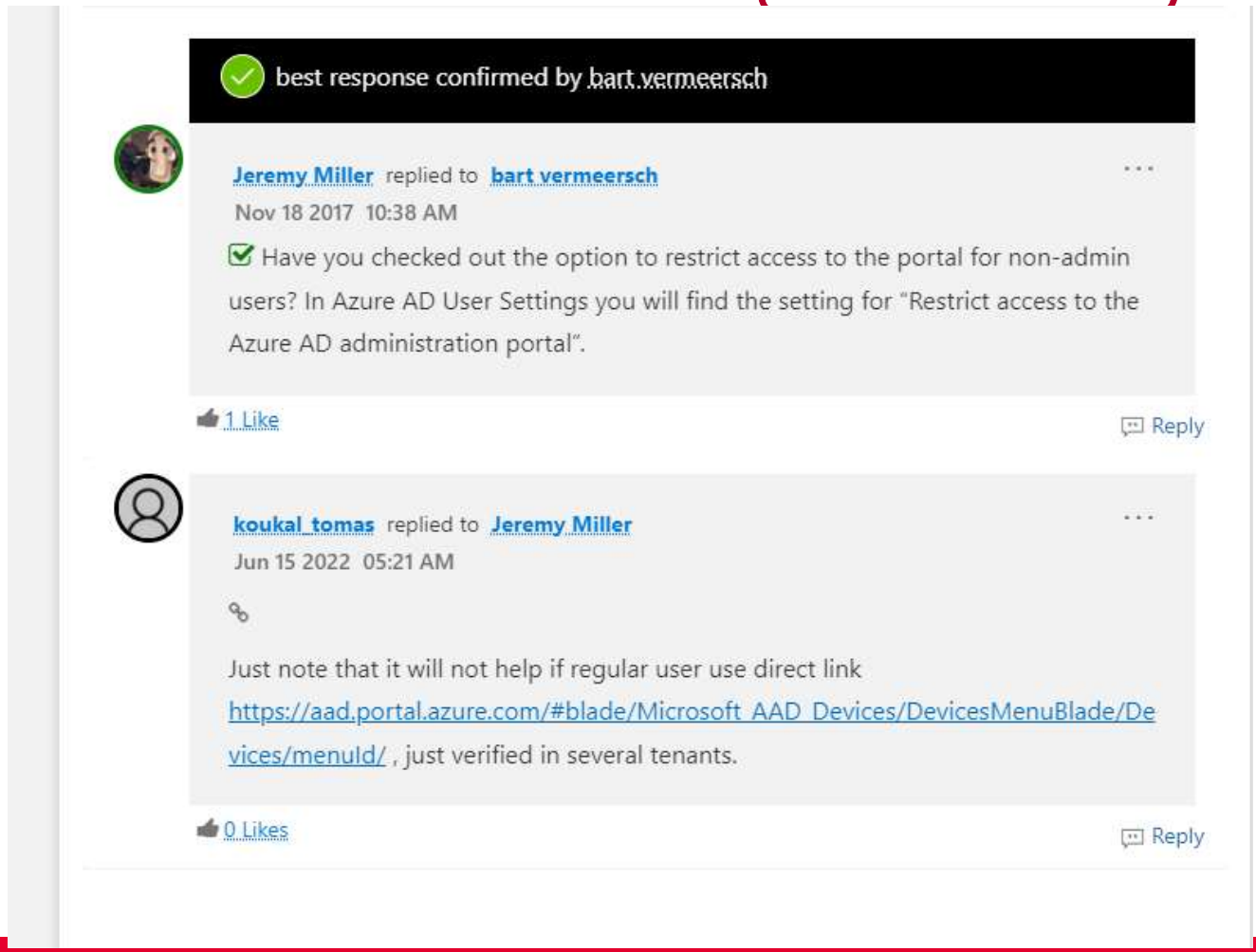
View best response

Labels: Azure Active Directory (AAD)

3,044 Views 2 Likes 2 Replies Reply

2 Replies All Discussions < Previous Discussion Next Discussion >

PRACTICAL EXAMPLE – Azure AD (ok ok Entra ID)



PRACTICAL EXAMPLE – Azure AD (ok ok Entra ID)

https://cmd.ms/portals/azuread/

Microsoft Portals › Azure Active Directory

Azure Active Directory

Search commands...

NAME	COMMAND	ALIAS	URL
Azure Active Directory (Entra)	**ad**.cmd.ms	aad,entra	https://entra.microsoft.com
Azure Active Directory	**azad**.cmd.ms		https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Overview?
App registrations	**adappreg**.cmd.ms		https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade/quickSta...
Enterprise applications	**adentapp**.cmd.ms	adapp,adapps	https://entra.microsoft.com/#view/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/~/App...
Groups	**adgroups**.cmd.ms		https://entra.microsoft.com/#view/Microsoft_AAD_IAM/GroupsManagementMenuBlade/~/AllGro...
Users	**adusers**.cmd.ms		https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade...
Devices	**addevices**.cmd.ms		https://entra.microsoft.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/Devices/menuId...
Device settings	**addevicesettings**.cmd.ms		https://entra.microsoft.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/DeviceSettings/...
External Identities	**adguests**.cmd.ms	adext	https://entra.microsoft.com/#view/Microsoft_AAD_IAM/CompanyRelationshipsMenuBlade/~/Setti...

PRACTICAL EXAMPLE – ServiceNow

servicenow | Product documentation

Home Products Release notes and upgrades PDF library Product accessibility Search documents

ase version

ne

v Platform capabilities

dvanced Work Assignment

orkspace

oud Call Center

onfiguration Management Database

onnect

ontent Management System

onversational Interfaces

purposes only, and will not be updated.

The Management, Instrumentation, and Discovery (MID) Server is a Java application that runs as a Windows service or UNIX daemon on a server in your local network. The ServiceNow® MID Server enables communication and the movement of data between a ServiceNow instance and external applications, data sources, and services.

The MID Server initiates all communications with the ServiceNow® instance. This communication is recorded as records in the ECC Queue, which acts as the communication log between the instance and the MID Server. The MID Server picks up any work it has to do from the ECC Queue and returns the results of that work to the queue.

This video gives you an overview of the MID Server:

MID Server | Overview

On

Se

Up

Re

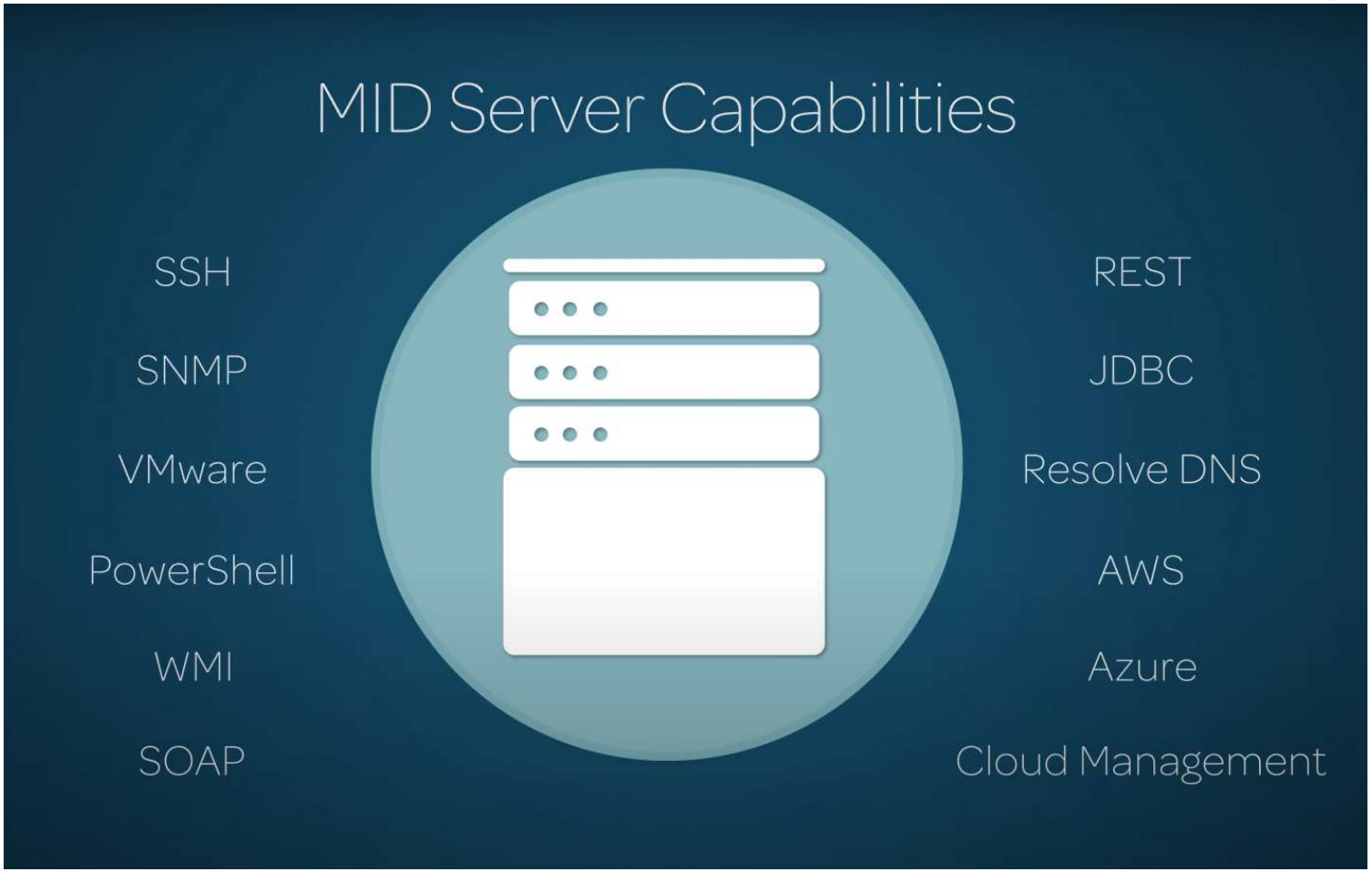
Se

Ex

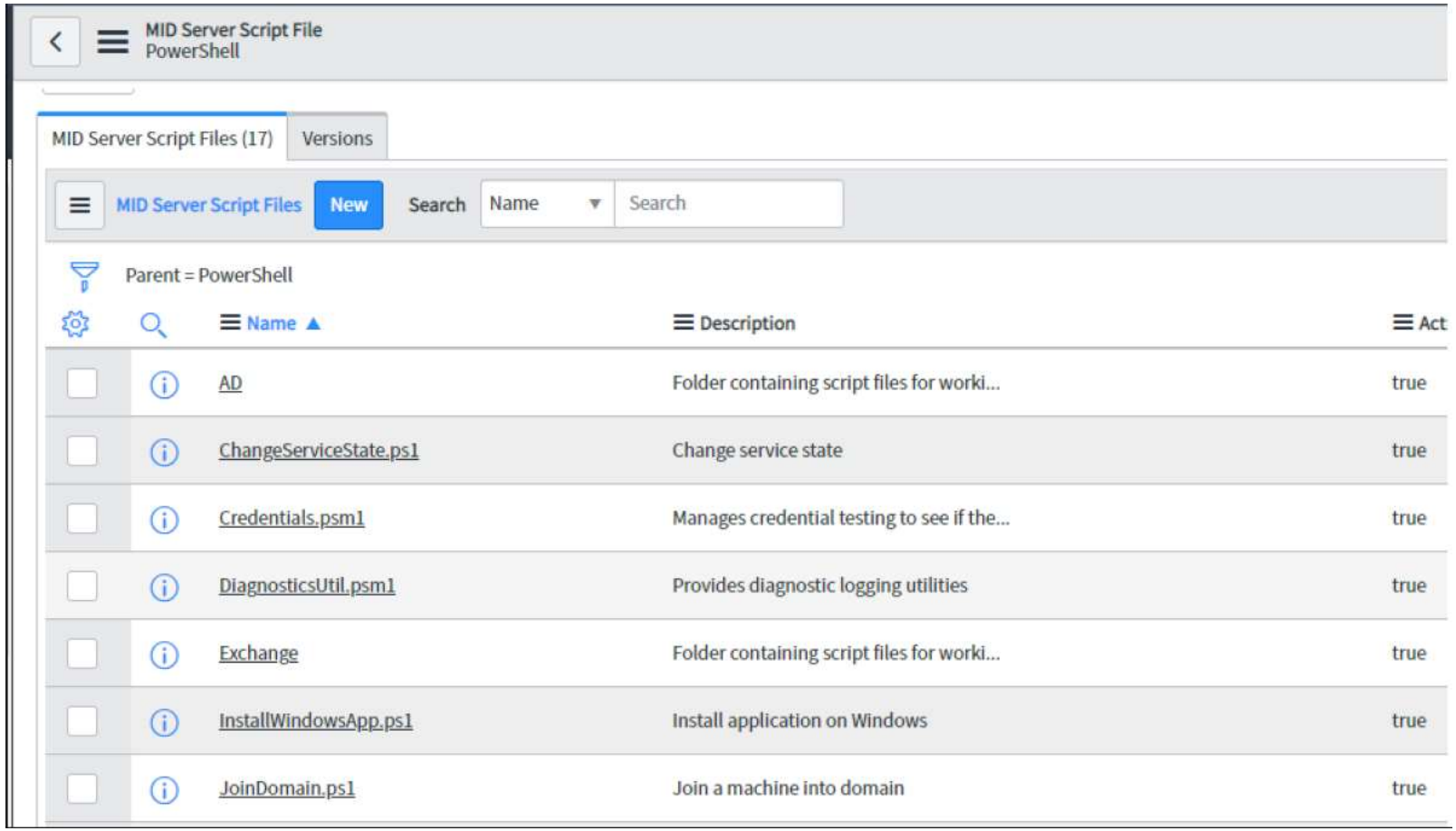
MI

PRACTICAL EXAMPLE – ServiceNow

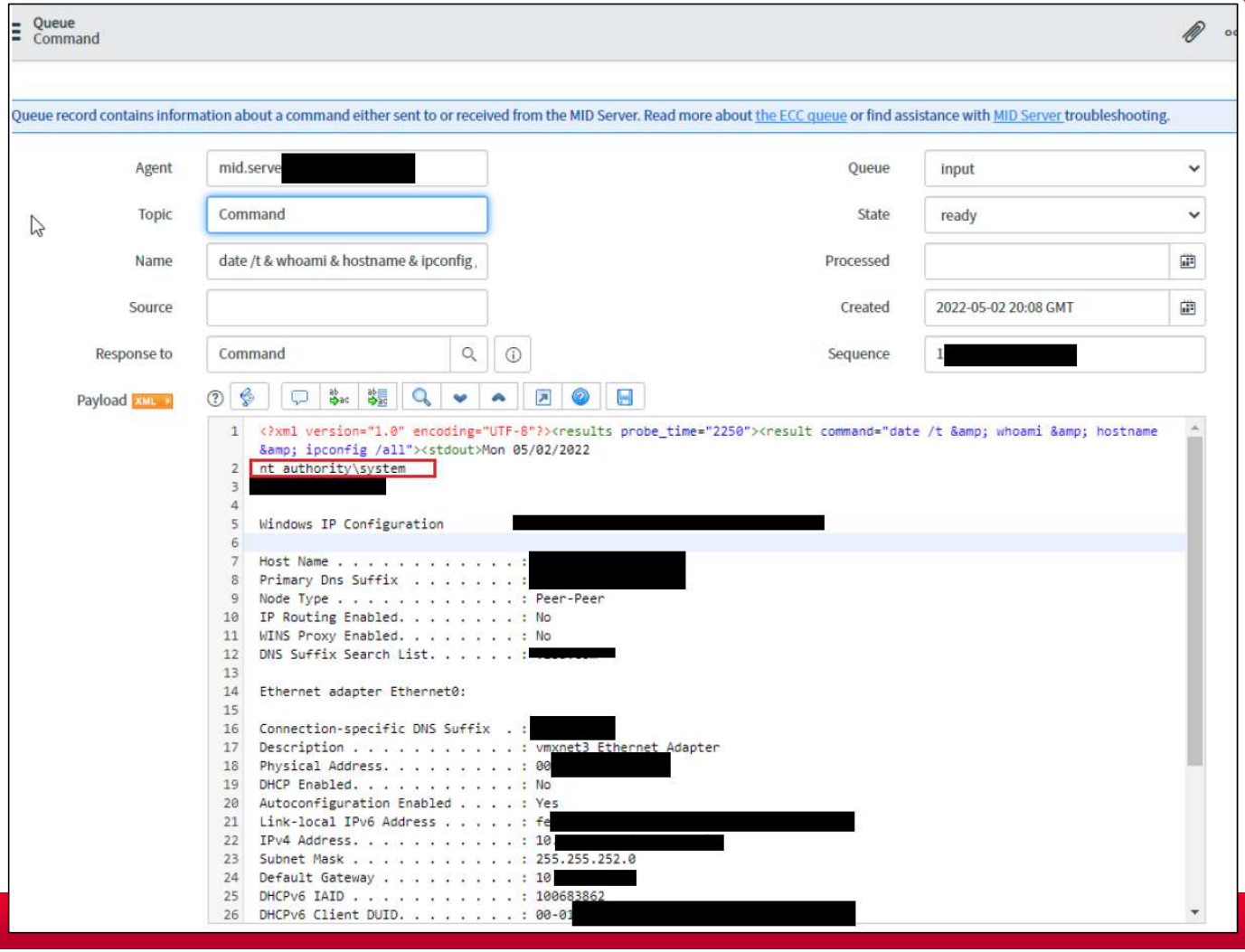
PRACTICAL EXAMPLE – ServiceNow



PRACTICAL EXAMPLE – ServiceNow



PRACTICAL EXAMPLE – ServiceNow

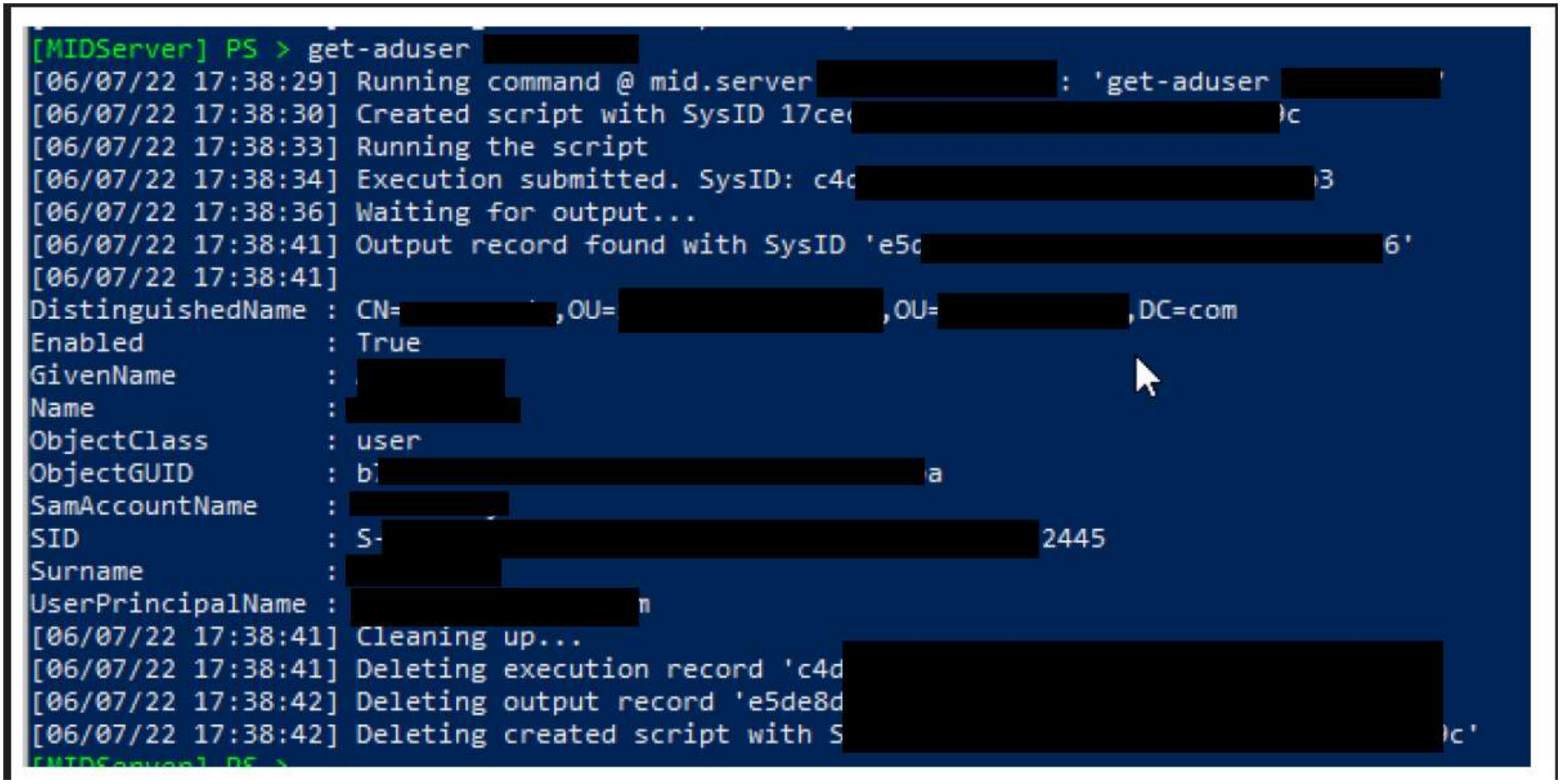


PRACTICAL EXAMPLE – ServiceNow

- 1. Create a PowerShell script that contained the PowerShell to be run. (POST /api/now/table/ecc_agent_script_file)
- 2. Create an ECC Queue task with 'topic' set to 'Powershell', 'agent' set to the name of the MID Server, 'Source' set to '127.0.0.1', and 'payload' referencing the previously created script file. (POST /api/now/table/ecc_queue)
- 3. Retrieve the results in the corresponding ECC input queue task. (GET /api/now/table/ecc_queue)
- 4. Delete the 2 ECC Queue tasks. (DELETE /api/now/table/ecc_queue/<ID>)
- 5. Delete the PowerShell script. (DELETE /api/now/table/ecc_agent_script_file/<ID>)

PRACTICAL EXAMPLE – ServiceNow

ROTAS SECURITY



QUESTIONS AND WRAP-UP

Email: npopovich@rotassec.com
Web: https://rotassecurity.com
Twitter: @pipefish_
Booth: behind you