

OVERLOOKED AND EXOTIC ATTACK SURFACE

SHINING A LIGHT ON HIDDEN VULNERABILITIES IN
ENTERPRISE TECHNOLOGIES

8/17/2023

Nick Popovich | Hacker

S A T O R
A R E P O
T E N E T
O P E R A
R O T A S



AGENDA



- 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



REFERENCES



- Beau Bullock - @dafthack from BHIS & BreakForge
 - Extensive training, podcasts
- Mauricio Velazco - @mvelazco from Splunk
 - Created BadZure training resource <https://github.com/mvelazco/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



THE TECHNOLOGY ECOSYSTEM – This We'll Defend



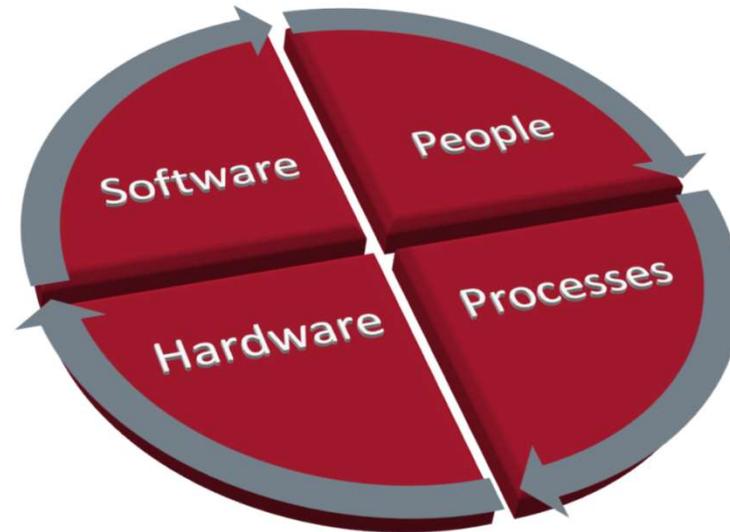
- Ecosystem defined:

noun, *Ecology*.

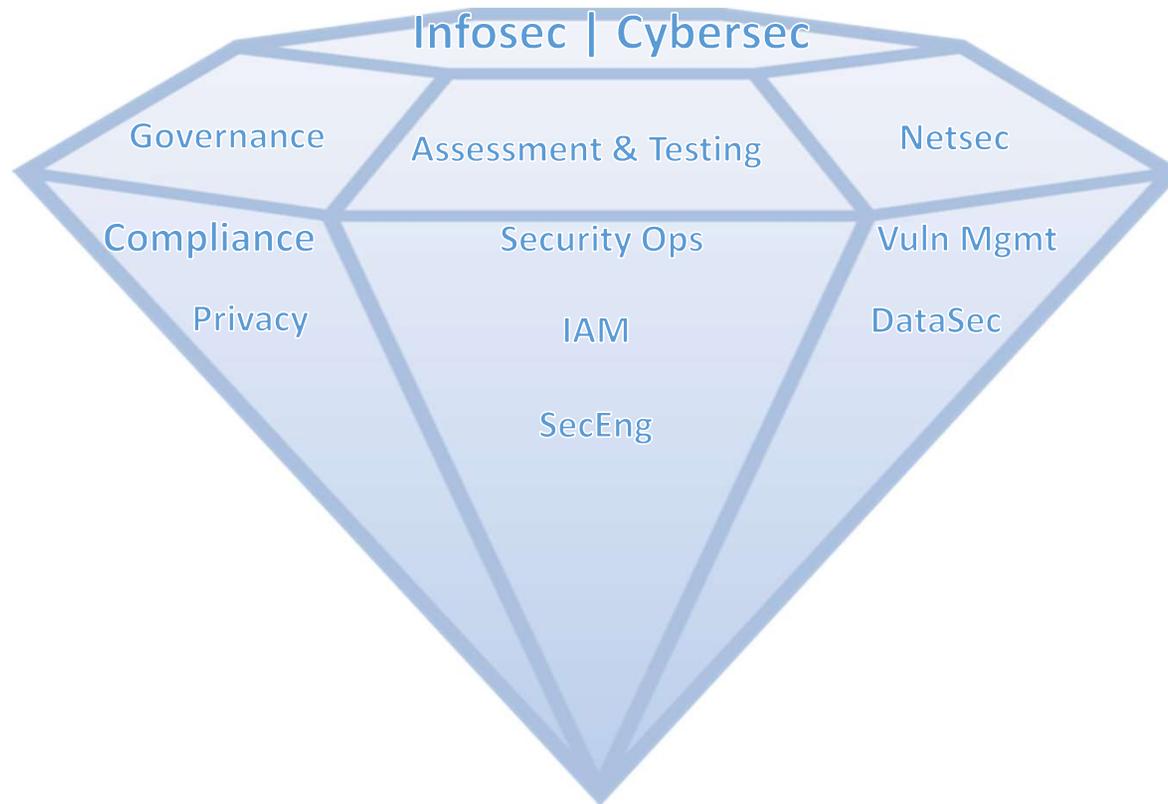
1. a system, or a group of interconnected elements, formed by the interaction of a community of organisms with their environment.
2. any system or network of interconnecting and interacting parts, as in business.

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

THE TECHNOLOGY ECOSYSTEM – This We'll Defend



THE TECHNOLOGY ECOSYSTEM – One Team One Fight



HISTORICAL AREAS OF CONCERN



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



AREAS OF CONCERN... Evolved



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

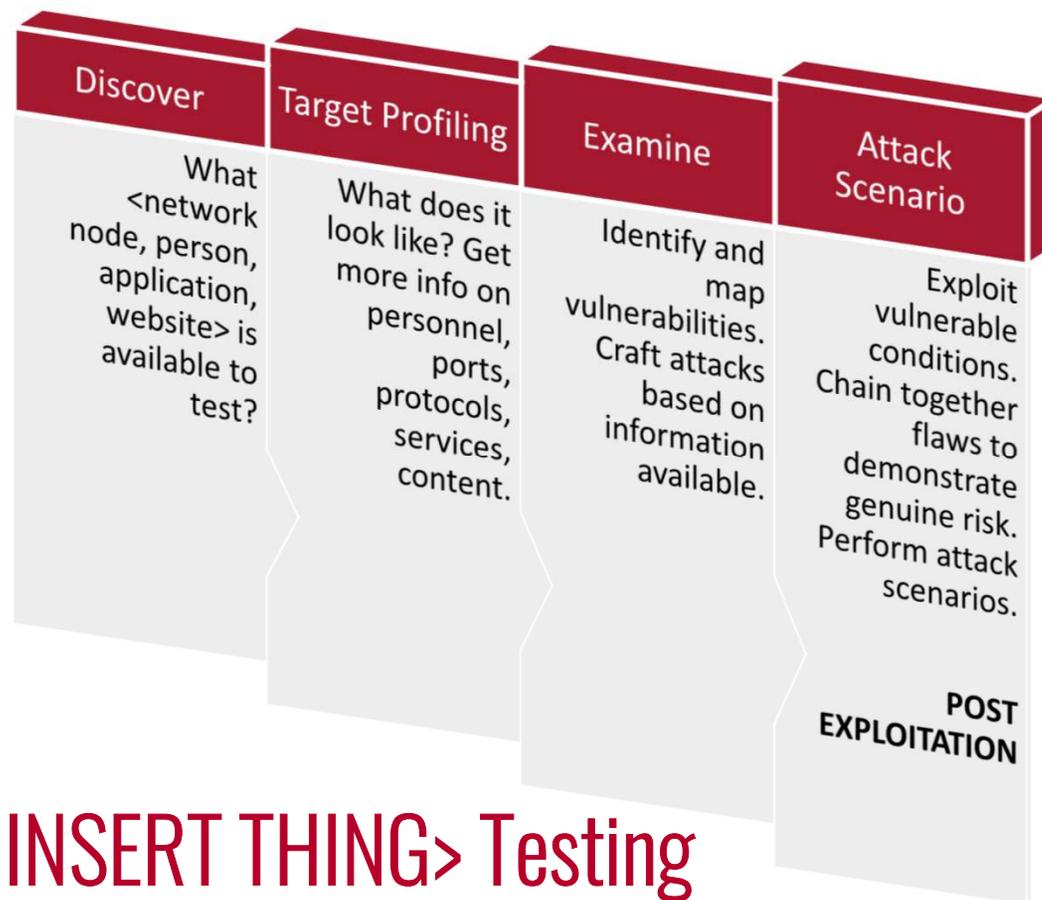
Two W's and an H



HOW IT'S GOING



SECURITY ASSESSMENT & TESTING



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



- 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

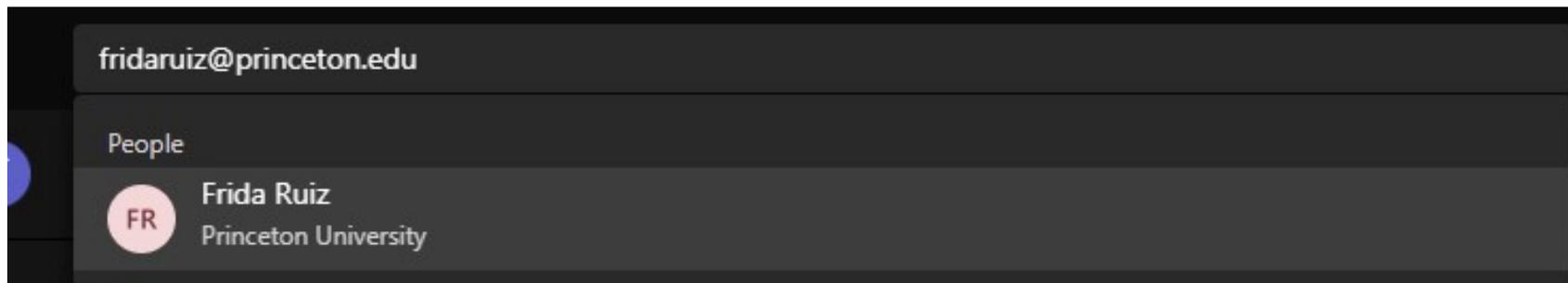
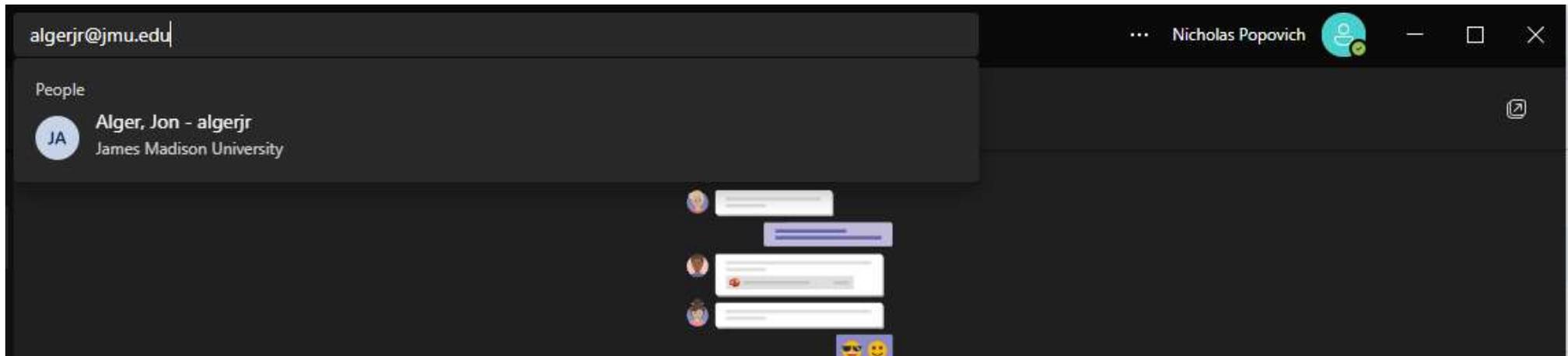


The screenshot shows the Microsoft Teams admin center page for "trusted-organizations-external-meetings-chat". The left sidebar contains a navigation menu with items like "ms", "overview", "nce, and privacy", "onitor Teams", "roles", "s in Teams admin", "es", "ople outside the", "with people", "r organization", and "ernal meetings". The main content area contains the following text:

- **Allow all external domains** This is the default setting in Teams, and it lets users in your organization find, call, chat, and set up meetings with people external to your organization in any domain.

In this scenario, your users can communicate with all external domains that are running Teams or Skype for Business so long as the other organization has also enabled external access.
- **Allow only specific external domains** - By adding domains to an **Allow** list, you limit external access to only the allowed domains. Once you set up a list of allowed domains, all other domains will be blocked.
- **Block specific domains** - By adding domains to a **Block** list, you can communicate with all external domains *except* the ones you've blocked. Once you set up a list of blocked domains, all other domains will be allowed.
- **Block all external domains** - Prevents users in your organization from finding, calling, chatting, and setting up meetings with people external to your organization in any domain.

PRACTICAL EXAMPLE – MS Teams



PRACTICAL EXAMPLE – MS Teams

A screenshot of the Microsoft Teams chat interface. The window title is "Nicholas Popovich". The chat header shows "Alger, Jon - algerjr" with a profile picture and "James Madison University". Below the header is a white notification box that reads: "This person is using Teams with an account managed by an organization. Some Teams features aren't available in this chat." The chat area shows a conversation with three messages and two emojis. At the bottom, it says "You're starting a new conversation" and "Type your first message below." On the right, the user profile for "Nicholas Popovich" is visible, including his email "nicholas.popovich@gmail.com", status "Available", and options like "Manage account" and "Add work or school account".

Search

Nicholas Popovich

Alger, Jon - algerjr Chat Files Photos
James Madison University

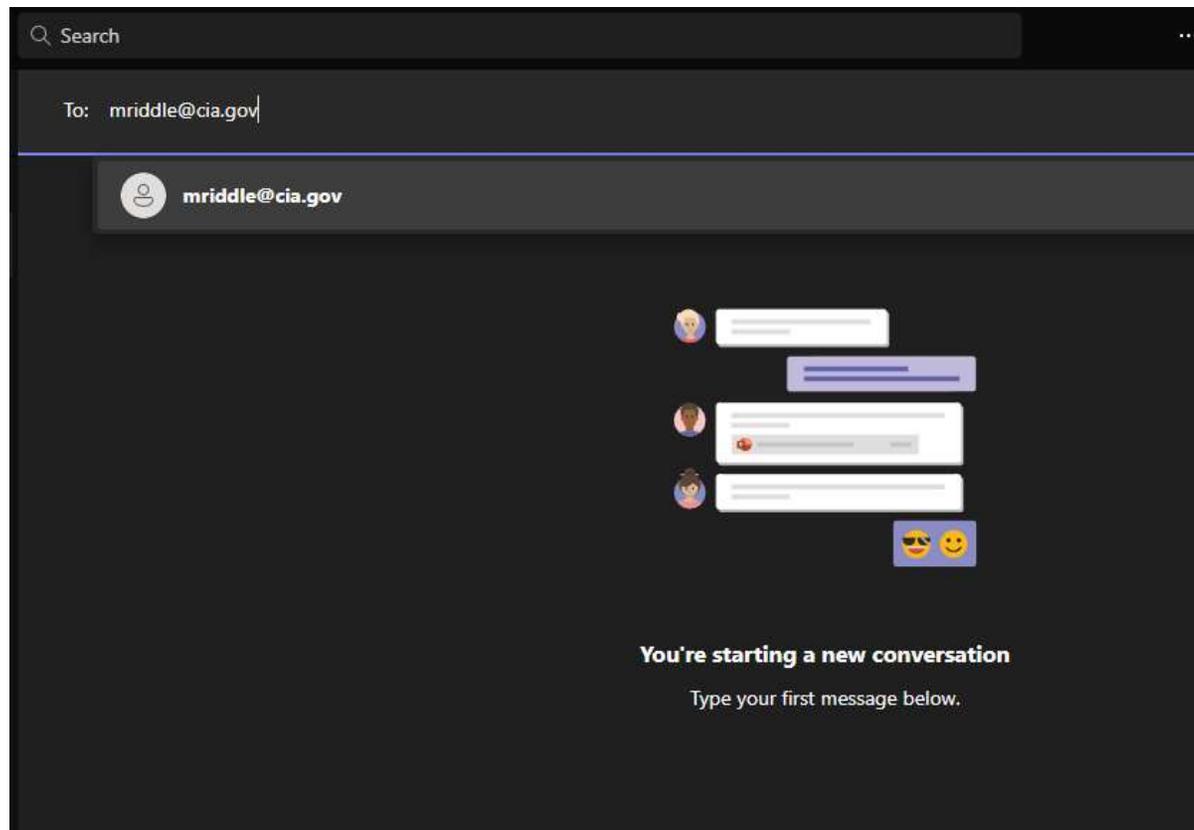
This person is using Teams with an account managed by an organization. Some Teams features aren't available in this chat.

You're starting a new conversation
Type your first message below.

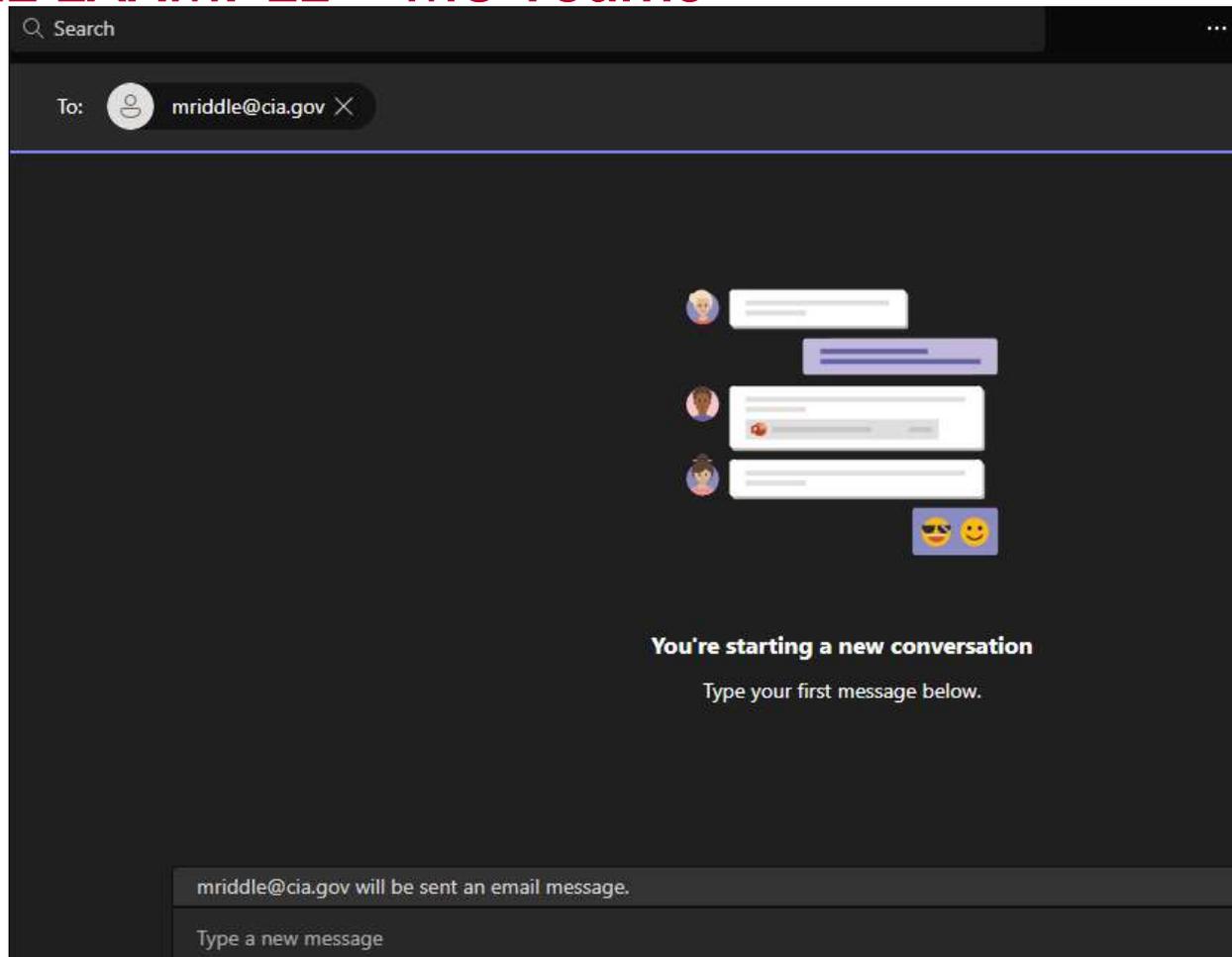
Nicholas Popovich
nicholas.popovich@gmail.com
Available | Set status message

- Nicholas Popovich
- self
- Manage account
- Add work or school account
- Sign out

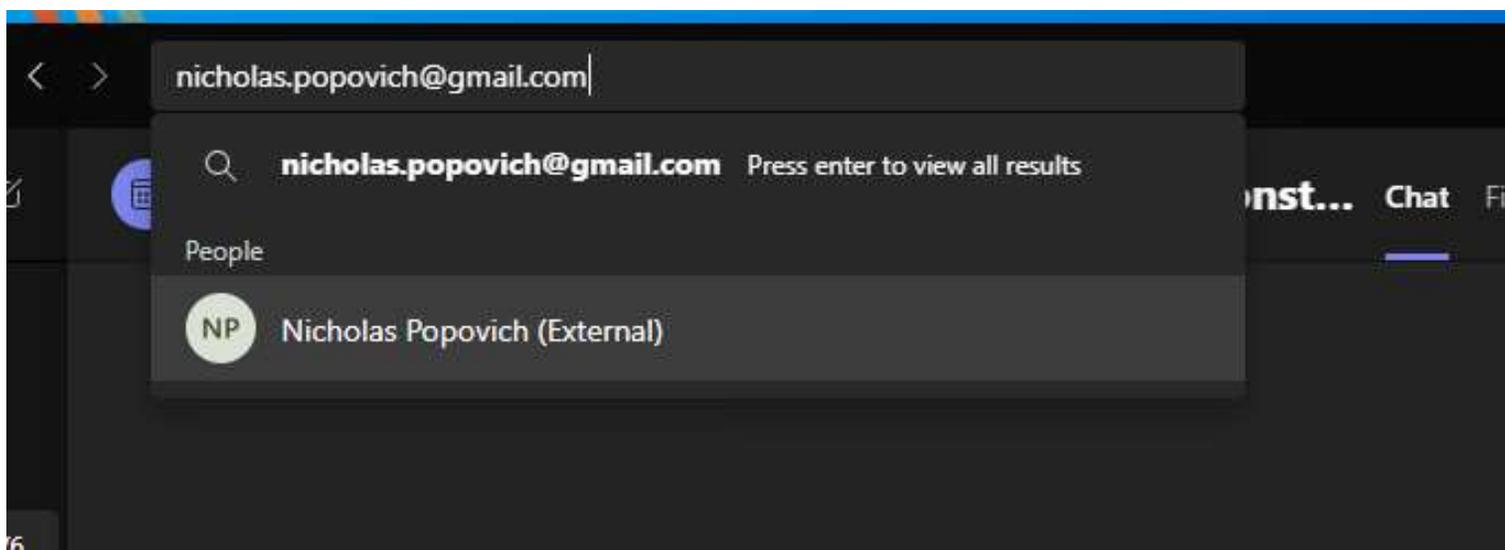
PRACTICAL EXAMPLE – MS Teams



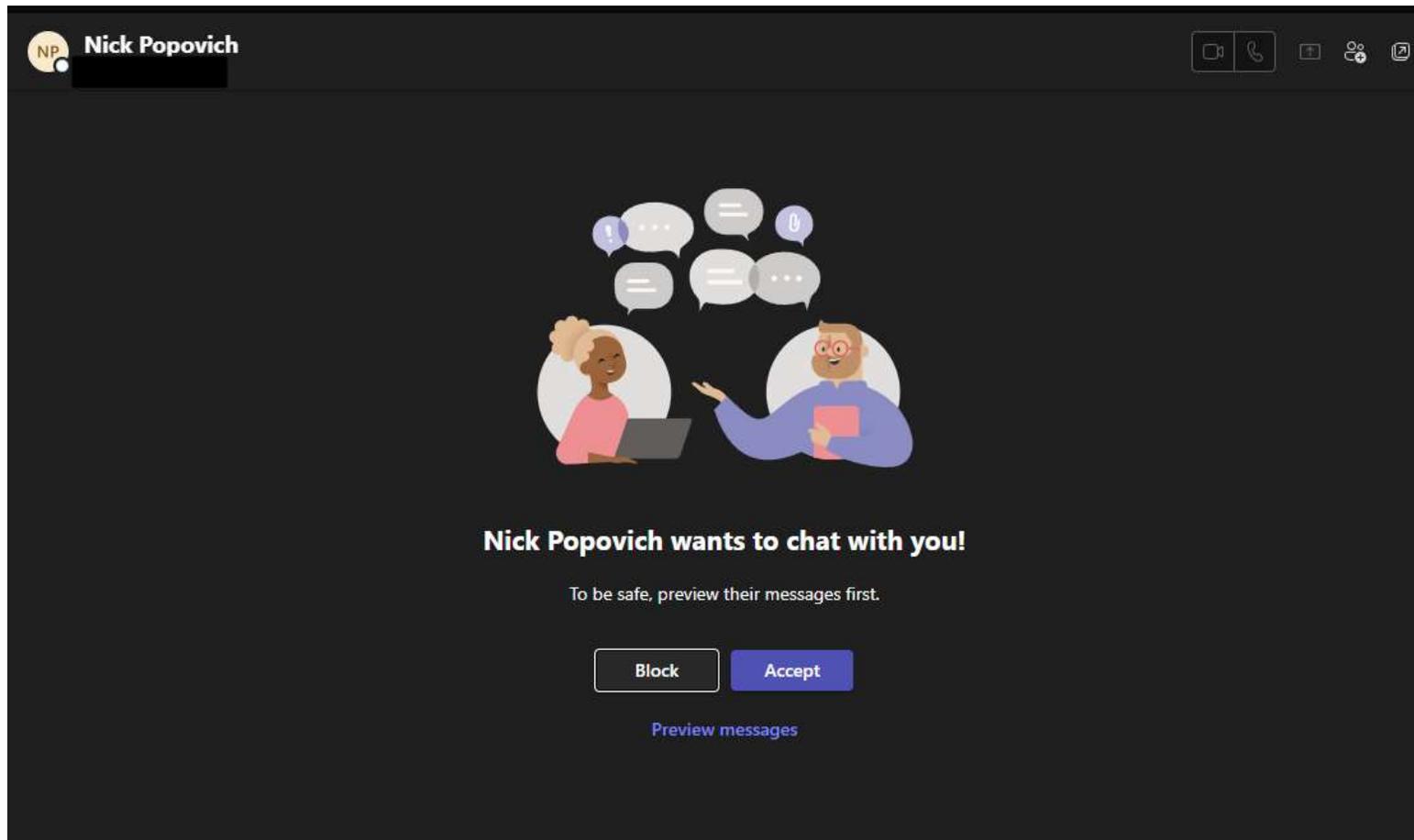
PRACTICAL EXAMPLE – MS Teams



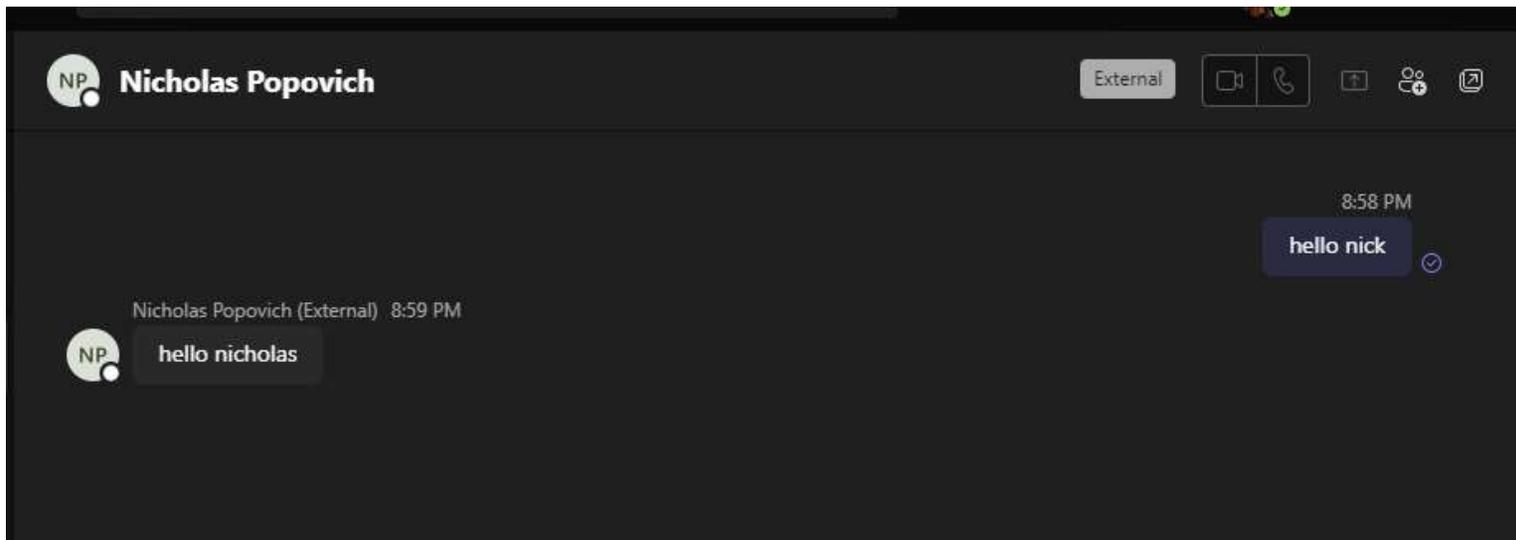
PRACTICAL EXAMPLE – MS Teams



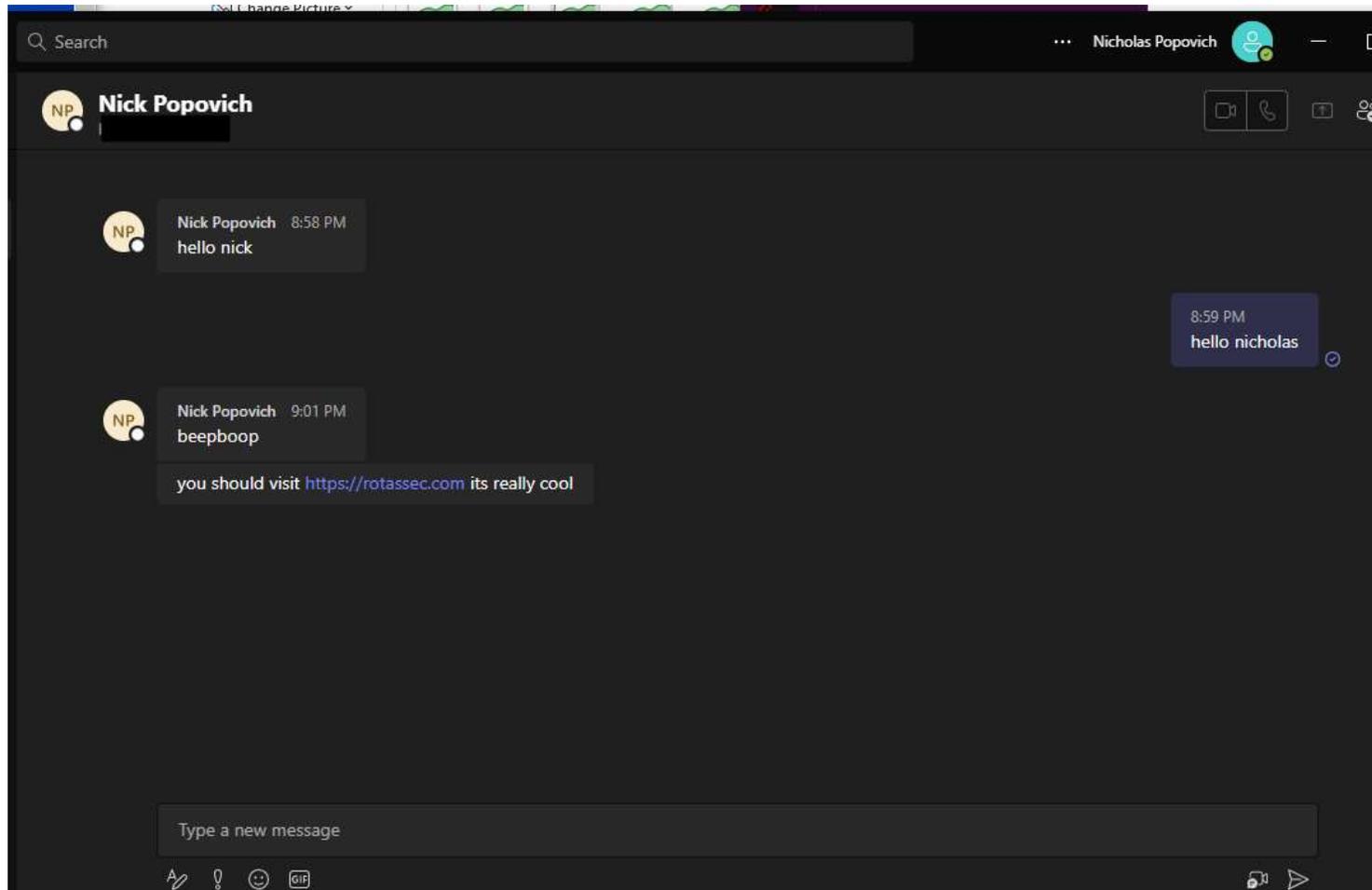
PRACTICAL EXAMPLE – MS Teams



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:

```
TeamsPhisher
v1.0 developed by @Octoberfest73 (https://github.com/Octoberfest7)

Configuration:
[-] Sending file link that is accessible by anyone with the link
[-] No delay between messages
[+] Using greeting: HI, --personalize greeting: HI <Name>,
[-] Not logging TeamsPhisher output

Preview mode: Sending test message to sender's account and showing target's friendly names for use with personalized greetings
Time left to abort: 00

Authenticating, verifying files, and uploading attachment

Reading target email list.....[+] SUCCESS!
Fetching Bearer token for Teams.....[+] SUCCESS!
Fetching Skype token.....[+] SUCCESS!
Fetching sender info.....[+] SUCCESS!
Fetching Bearer token for SharePoint.....[+] SUCCESS!
Uploading file: /root/salaryinfo.zip.....[+] SUCCESS!

Hashing file
[+] MD5: 2b9aa91b4ebfc450197099e170e14da9
[+] SHA1: 5cfb7316fc6aeb169ba40704fa29cf0eaad638cb
[+] SHA256: e7430c1bd2da45808a75dd974f5b10990ae46ec707e321bd3df00fc305fa4c94

Sending test message to testuser@[REDACTED].onmicrosoft.com

testuser@[REDACTED].onmicrosoft.com.....[+] SUCCESS!

Previewing customized names identified by TeamsPhisher

AdeleV@[REDACTED].onmicrosoft.com.....[+] Friendly Name: Adele
AlexW@[REDACTED].onmicrosoft.com.....[+] Friendly Name: Alex
TomDoo@[REDACTED].onmicrosoft.com.....[+] Friendly Name: Tom
```

PRACTICAL EXAMPLE – MS Teams



TeamsPhisher / img / Previewmessage.JPG

Octoberfest7 Initial commit 08fbb36 · last month History

73.8 KB

Microsoft Teams Search

Chat test user (You) Chat Files Organization Activity LinkedIn

- Pinned

test user (You) 8:09 PM
You: Hi, In an effort to improve compensation ...

8:09 PM

Hi,

In an effort to improve compensation in our industry, I have been crowdsourcing salary data from sales employees in our field. The attached spreadsheet has up to date info for some of the leading businesses as well as breakouts by seniority and tenure. I saw you worked at Bob Jones Big Bank and was hoping you might be willing to share some data to add to the data set.

Some people have had issues viewing the spreadsheet within browsers; your best bet is to download it and open it that way.

Hope this is of interest to you!

Best,

Phish Her

salaryinfo.zip

PRACTICAL EXAMPLE – Conditional Access Policies



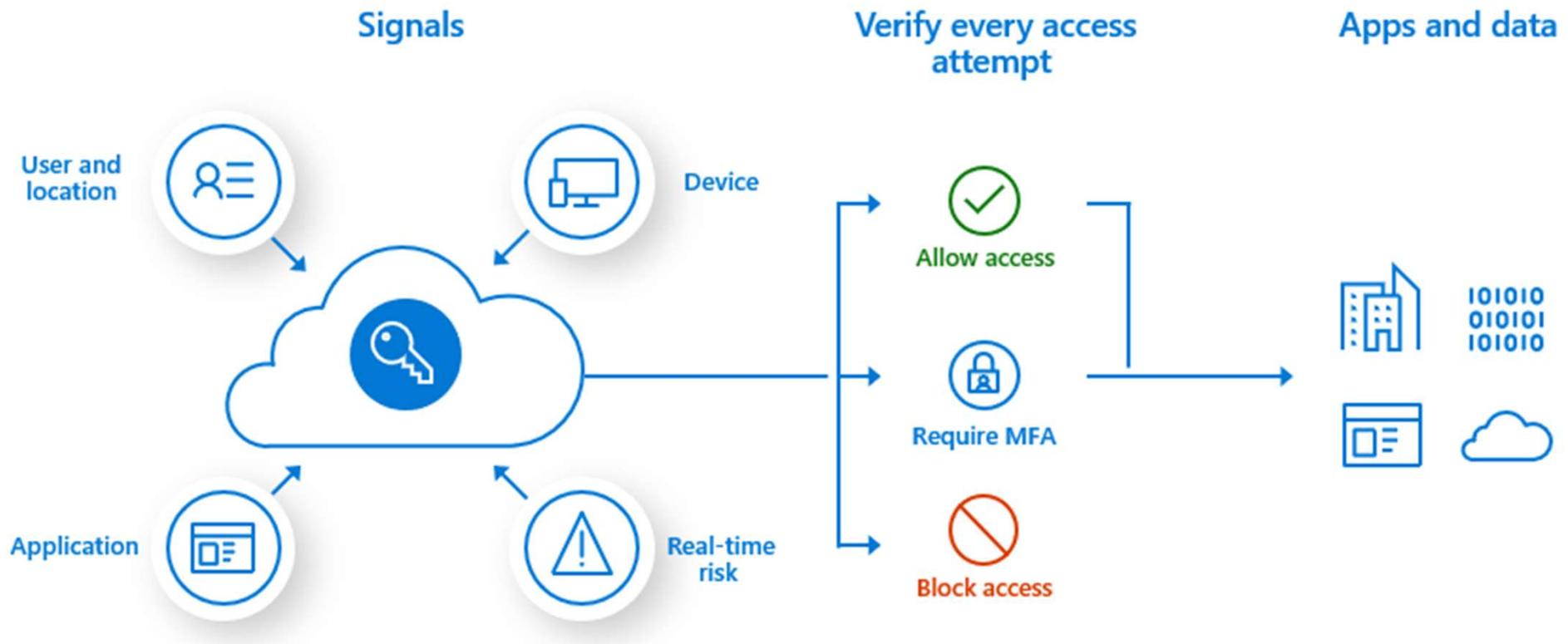
Azure Conditional Access is a feature of Azure Active Directory (Azure AD) that enables organizations to define and enforce policies that evaluate specific conditions and determine when and how users can access certain resources.

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



Home > Conditional Access >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Home > Contoso > Security > Conditional Access >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

Name *

What does this policy apply to?

Users and groups

Include Exclude

None

All users

Select users and groups

All guest and external users ⓘ

Directory roles ⓘ

Users and groups

Select

0 users and groups selected

Select at least one user or group

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

PRACTICAL EXAMPLE – Conditional Access Policies



Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

None

All cloud apps

Select apps

Select

None

Select at least one app.

Select

Cloud apps

Search

- Office 365
- Azure Credential Configurati...
- Dynamics 365 Business Cent...
- MA** Microsoft Azure Manager
- Microsoft Cloud App Security...
- Microsoft Information Protec...

Selected items

- MA** Microsoft Azure I...

Home > Contoso > Security > Conditional Access >

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

MFA Pilot

Assignments

Users or workload identities

Specific users included

Cloud apps or actions

1 app included

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

Report-only On Off

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

- Require multi-factor authentication
- Require device to be marked as compliant
- Require Hybrid Azure AD joined device
- Require approved client app
- Require app protection policy
- Require password change

For multiple controls

Require all the selected controls

Require one of the selected controls

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

PRACTICAL EXAMPLE – Conditional Access Policies



Update location (Countries) ×

Delete

i Only IPv4 addresses are mapped to countries/regions. IPv6 addresses are included in unknown countries/regions.

Name *

AllowedCountries

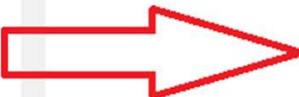
Determine location by GPS coordinates ▾

i When the location condition of a Conditional Access policy is configured, users will be prompted by the Authenticator app to share their GPS location. [Learn more](#)

Include unknown countries/regions ⓘ

Search countries

Name ↑↓



It should say: IPV6 Addresses

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

PRACTICAL EXAMPLE – Conditional Access Policies



```
Terminal - root@HPLaserJet1170-2: ~  
File Edit View Terminal Tabs Help  
root@HPLaserJet1170-2:~# ip -6 a s eth0  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
  inet6 2600:4040:131e:fe00:8609:4590:e035:cf49/64 scope global temporary dynamic  
    valid lft 6172sec preferred_lft 6171sec  
  inet6 2600:4040:131e:fe00:20c:29ff:fe9f:ab28/64 scope global dynamic mngtmpaddr noprefixroute  
    valid lft 6172sec preferred_lft 6171sec  
  inet6 fd0a:60d8:76f7:bec2:154d:5534:4320:8830/64 scope global temporary deprecated dynamic  
    valid lft 726sec preferred_lft 0sec  
  inet6 fd0a:60d8:76f7:bec2:ada8:11d8:f0e9:d80e/64 scope global temporary deprecated dynamic  
    valid lft 726sec preferred_lft 0sec  
  inet6 fd0a:60d8:76f7:bec2:20c:29ff:fe9f:ab28/64 scope global deprecated dynamic mngtmpaddr noprefixroute  
    valid lft 726sec preferred_lft 0sec  
  inet6 fe80::20c:29ff:fe9f:ab28/64 scope link noprefixroute  
    valid lft forever preferred_lft forever  
root@HPLaserJet1170-2:~# curl http://ip4only.me/api/  
IPv4,96.253.103.205,v1.1,,See http://ip6.me/docs/ for api documentation  
root@HPLaserJet1170-2:~# curl http://ip6only.me/api/  
IPv6,2600:4040:131e:fe00:8609:4590:e035:cf4,v1.1,,See http://ip6.me/docs/ for api documentation  
root@HPLaserJet1170-2:~#
```



PRACTICAL EXAMPLE – Conditional Access Policies



```
Terminal - root@HPLaserJet1170-2:~  
File Edit View Terminal Tabs Help  
root@HPLaserJet1170-2:~# sysctl -w net.ipv6.conf.all.disable_ipv6=1  
sysctl -w net.ipv6.conf.default.disable_ipv6=1  
sysctl -w net.ipv6.conf.lo.disable_ipv6=1  
net.ipv6.conf.all.disable_ipv6 = 1  
net.ipv6.conf.default.disable_ipv6 = 1  
net.ipv6.conf.lo.disable_ipv6 = 1  
root@HPLaserJet1170-2:~# curl http://ip6only.me/api/  
curl: (7) Couldn't connect to server  
root@HPLaserJet1170-2:~# ip -6 a s eth0  
root@HPLaserJet1170-2:~#
```



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



The screenshot shows the Azure Active Directory Conditional Access Policies page. The breadcrumb navigation is "Home > Endpoint security > Conditional Access". The page title is "Conditional Access | Policies" with a red box around it. The left sidebar contains navigation options: Overview (Preview), Policies (selected), Insights and reporting, Diagnose and solve problems, Manage (Named locations, Custom controls (Preview), Terms of use, VPN connectivity, Authentication context (Preview), Classic policies), and Monitoring.

The main content area shows a table of policies. The table has columns for "Policy Name" and "State". The "State" column is highlighted with a red box. A red arrow points to the "Report-only" state of the "MWP - Windows 10 Require Compliant Device" policy.

Policy Name ↑↓	State ↑↓
CA - MFA	On
MWP - Windows 10 Require Compliant Device	Report-only
MWP - Require multi-factor authentication for admins	Report-only
MWP - Securing security info registration	Report-only
MWP - Block legacy authentication Exchange Active Sync	Report-only
MWP - Block legacy authentication Other Clients	Report-only
MWP - Require multi-factor authentication for guest acco...	Report-only
MWP - Require multi-factor authentication for Azure ma...	Report-only
MWP - Block access for unknown or unsupported device ...	Report-only

PRACTICAL EXAMPLE – Conditional Access Policies



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



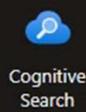
The screenshot shows a mobile device emulation tool interface. At the top, there are dropdown menus for "Chrome" and "iOS", a "Filter among 27" button, and a "Z to A" sort option. Below this is a list of six Chrome instances, each with a radio button, a Chrome version number, an iOS version number, and a user agent string. Below the list, there are fields for "userAgent", "appVersion", "platform", and "product". At the bottom, there are four buttons: "Options", "Restart", "Refresh Tab", and "Reset".

Instance	Chrome Version	iOS Version	User Agent
1	Chrome 98.0.4758.85	iOS 15.3	Mozilla/5.0 (iPhone; CPU iPhone OS 15_3 like...)
2	Chrome 98.0.4758.85	iOS 15.2	Mozilla/5.0 (iPad; CPU OS 15_2 like Mac OS ...)
3	Chrome 87.0.4280.163	iOS 14.4	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4 like...)
4	Chrome 87.0.4280.163	iOS 14.5	Mozilla/5.0 (iPod; CPU iPhone OS 14_5 like M...)
5	Chrome 87.0.4280.163	iOS 14.5	Mozilla/5.0 (iPad; CPU OS 14_5 like Mac OS ...)
6	Chrome 87.0.4280.163	iOS 14.5	Mozilla/5.0 (iPhone; CPU iPhone OS 14_5 like...)

userAgent Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
appVersion 5.0 (X11)
platform Linux vendor
product Gecko ocpu Linux x86_64

Options Restart Refresh Tab Reset
Test UA Consider Containers Apply (active window) Apply (all windows)

Azure services



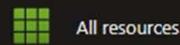
Resources

Recent Favorite

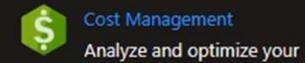
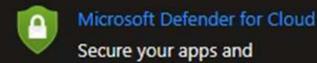
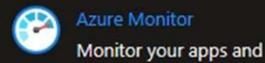
Name	Type	Last Viewed
rvasecpipefish	Function App	3 minutes ago
RVAsecDemoAPI	API Management service	11 hours ago
MainSubscription	Subscription	3 days ago
bingsearch1230987	Bing Resource	9 months ago
search-rg	Resource group	10 months ago

See all

Navigate



Tools



PRACTICAL EXAMPLE – Conditional Access Policies



← → ↻ 🔒 rvasecpipefish.azurewebsites.net



I TELL YOU HWHAT
your IP is 20.84.237.27

[@pipefish](#)

Certificate

General Details Certification Path

Certification path

- DigiCert Global Root G2
 - Microsoft Azure TLS Issuing CA 01
 - *.azurewebsites.net

View Certificate

Certificate status:

This certificate is OK.

OK

PRACTICAL EXAMPLE – Conditional Access Policies



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, 20.33.0.0/16
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)



- 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)



```
PS C:\WINDOWS\system32> Get-AADIntAccessTokenForAADJoin -SaveToCache
AccessToken saved to cache.
```

Tenant	User	Resource	Client
-----	----	-----	-----
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]....

```
PS C:\WINDOWS\system32> Join-AADIntDeviceToAzureAD -DeviceName "popovichtesting" -DeviceType "Windows" -OSVersion "10"
Device successfully registered to Azure AD:
```

```
  DisplayName: "popovichtesting"
  DeviceId:    6 [REDACTED] f
  ObjectId:   8 [REDACTED] 9
  TenantId:   3 [REDACTED] 6
  Cert thumbprint: E [REDACTED] 36A37
  Cert file name : "[REDACTED].pfx"
```

Local SID:

```
S [REDACTED] 4
```

Additional SIDs:

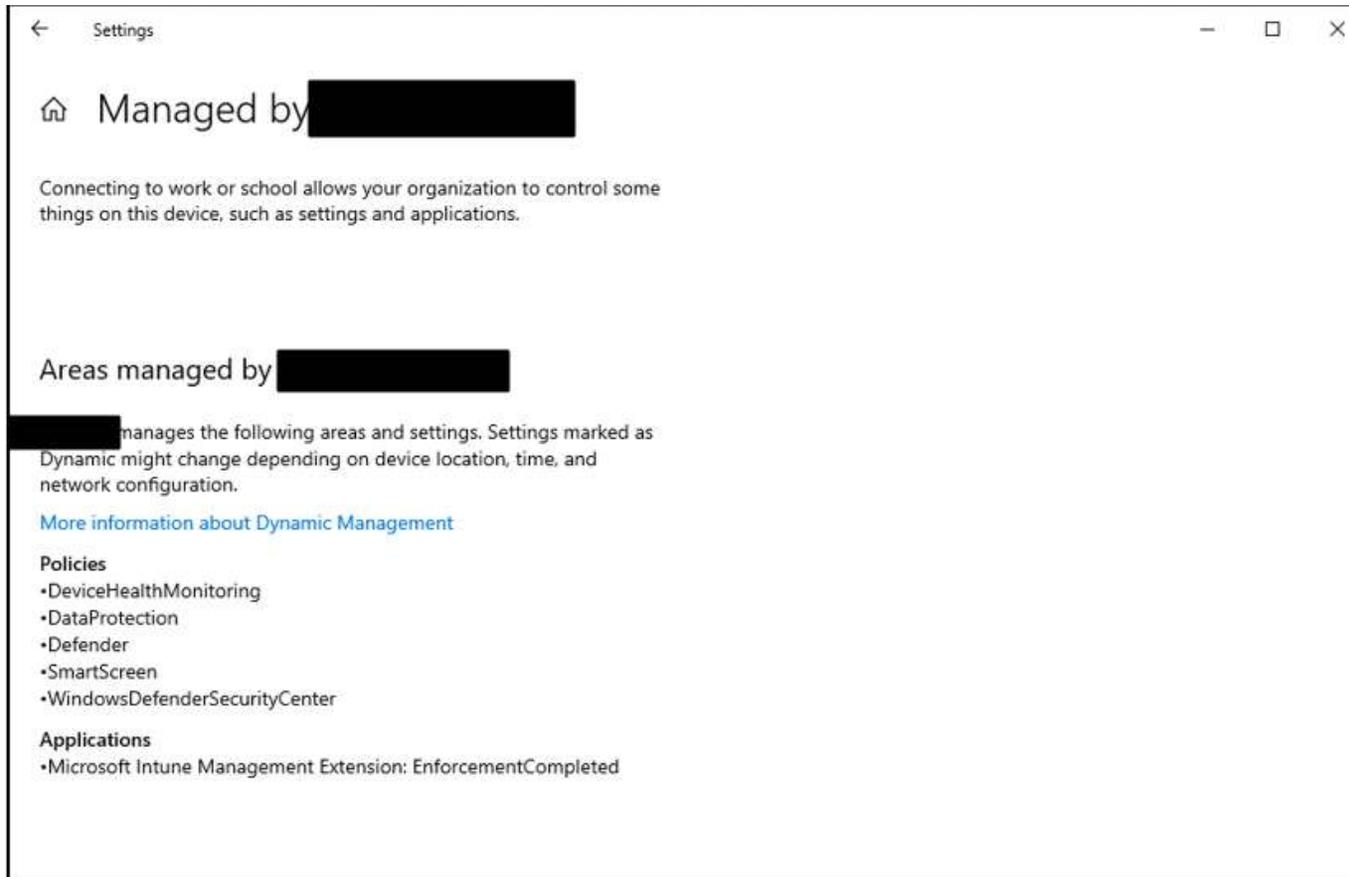
```
S-1-12-1-[REDACTED] 9
```

```
S-1-12-1-[REDACTED] 0
```

```
S-1-12-1-[REDACTED]
```

```
PS C:\WINDOWS\system32>
```

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 | All devices

Download devices Refresh Columns Enable Disable Delete Manage Preview features Got feedback?

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.

Search by name or device ID or object ID

Add filters

47 devices found

- Overview
- All devices
- Device settings
- BitLocker keys (Preview)
- Diagnose and solve problems
- Activity
- Audit logs
- Bulk operation results (Preview)
- Troubleshooting + Support
- New support request

<input type="checkbox"/>	Name ↕	Enabled	OS	Version	Join Type	Owner	MDM	Compliant	Registered ↕	Activity ↕
<input type="checkbox"/>	[Redacted]	Yes	Windows	10.0.22000.675	Azure AD joined	[Redacted]	Microsoft Intune	No	2/28/2022, 1:36 PM	5/31/2022, 7:09...
<input type="checkbox"/>	[Redacted]	Yes	iPad	16.3.1	Azure AD regist...	[Redacted]	Microsoft Intune	No	3/2/2023, 3:09 PM	3/2/2023, 3:09 ...
<input type="checkbox"/>	[Redacted]	Yes	Windows	10.0.19042.631	Azure AD regist...	[Redacted]	None	N/A	5/22/2023, 1:07 PM	5/22/2023, 1:07...
<input type="checkbox"/>	[Redacted]	Yes	Windows	10.0.19044.3208	Hybrid Azure A...	[Redacted]	Microsoft Intune	N/A	8/15/2023, 3:56 PM	8/15/2023, 3:46...
<input type="checkbox"/>	[Redacted]	Yes	Windows	10.0.22621.1992	Azure AD joined	[Redacted]	Microsoft Intune	No	8/24/2022, 6:48 PM	8/12/2023, 1:39...
<input type="checkbox"/>	[Redacted]	No	Android	12	Azure AD regist...	[Redacted]	None	N/A	2/11/2022, 5:01 PM	5/8/2022, 2:18 ...
<input type="checkbox"/>	[Redacted]	Yes	Windows	10.0.17763.0	Hybrid Azure A...	[Redacted]	None	N/A	3/13/2022, 12:08 AM	8/3/2023, 1:15 ...
<input type="checkbox"/>	[Redacted]	Yes	Windows	10.0.17763.2989	Azure AD joined	[Redacted]	None	No	6/1/2022, 12:35 AM	9/25/2022, 10:2...
<input type="checkbox"/>	[Redacted]	Yes	Windows	10.0.19044.1766	Azure AD regist...	[Redacted]	Microsoft Intune	No	8/4/2022, 10:31 AM	8/5/2023, 7:16 ...
<input type="checkbox"/>	[Redacted]	Yes	Windows	10.0.19044.2006		[Redacted]	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?

Naam	Kolommen	Ja	Windows	10.0.150...	Azure AD registered	Geen	Nat.L.	Nat.L.	...
DESKTOP		Ja	Windows	10.0.150...	Azure AD registered	Geen	Nat.L.	11-12-2017 21:26:15	...
		Ja	Windows	Window...	Azure AD registered	Geen	Nat.L.	Nat.L.	...

[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)



✓ best response confirmed by [bart.vermeersch](#)



[Jeremy Miller](#) replied to [bart.vermeersch](#)

Nov 18 2017 10:38 AM

✓ Have you checked out the option to restrict access to the portal for non-admin users? In Azure AD User Settings you will find the setting for "Restrict access to the Azure AD administration portal".

👍 1 Like

🗨 Reply



[koukal tomas](#) replied to [Jeremy Miller](#)

Jun 15 2022 05:21 AM



Just note that it will not help if regular user use direct link

https://aad.portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/Devices/menuld/, just verified in several tenants.

👍 0 Likes

🗨 Reply

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/menul...
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

Release version

Home ▾

Platform capabilities ▾

Advanced Work Assignment >

Workspace >

Cloud Call Center >

Configuration Management Database >

Connect >

Content Management System >

Conversational Interfaces >

purpose only, and will not be updated.

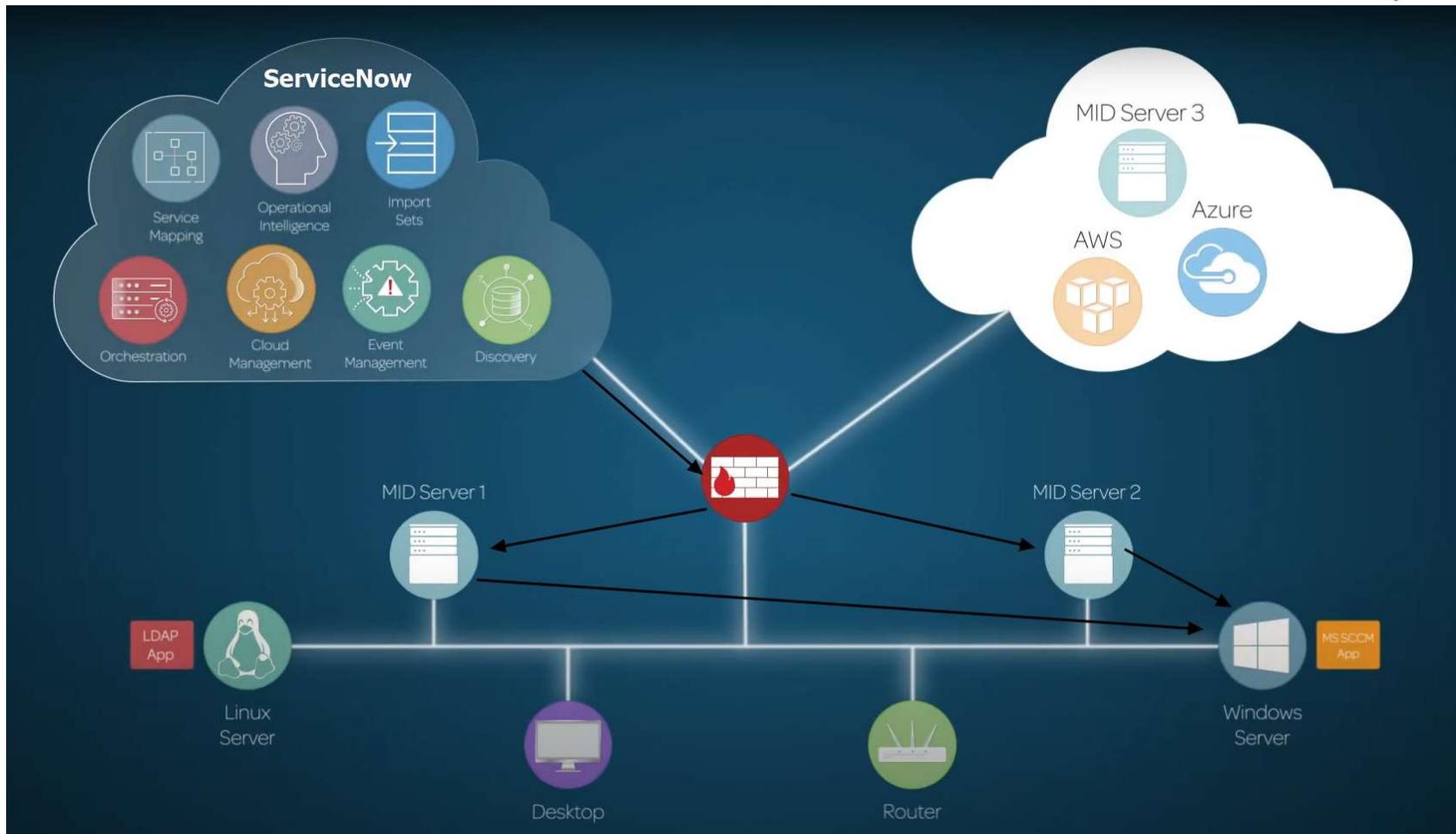
The Management, Instrumentation, and Discovery (MID) Server is a Java application that runs as a Windows service or UNIX daemon on a server in your local network. The ServiceNow® MID Server enables communication and the movement of data between a ServiceNow instance and external applications, data sources,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



PRACTICAL EXAMPLE – ServiceNow



PRACTICAL EXAMPLE – ServiceNow



MID Server Capabilities



SSH

SNMP

VMware

PowerShell

WMI

SOAP

REST

JDBC

Resolve DNS

AWS

Azure

Cloud Management

PRACTICAL EXAMPLE – ServiceNow



MID Server Script File PowerShell

MID Server Script Files (17) Versions

MID Server Script Files **New** Search Name Search

Parent = PowerShell

	Name	Description	Act
<input type="checkbox"/>	AD	Folder containing script files for worki...	true
<input type="checkbox"/>	ChangeServiceState.ps1	Change service state	true
<input type="checkbox"/>	Credentials.psm1	Manages credential testing to see if the...	true
<input type="checkbox"/>	DiagnosticsUtil.psm1	Provides diagnostic logging utilities	true
<input type="checkbox"/>	Exchange	Folder containing script files for worki...	true
<input type="checkbox"/>	InstallWindowsApp.ps1	Install application on Windows	true
<input type="checkbox"/>	JoinDomain.ps1	Join a machine into domain	true

PRACTICAL EXAMPLE – ServiceNow



Queue Command

Queue record contains information about a command either sent to or received from the MID Server. Read more about [the ECC queue](#) or find assistance with [MID Server troubleshooting](#).

Agent	mid.serv[REDACTED]	Queue	input
Topic	Command	State	ready
Name	date /t & whoami & hostname & ipconfig	Processed	<input type="checkbox"/>
Source		Created	2022-05-02 20:08 GMT
Response to	Command	Sequence	1 [REDACTED]

Payload **XML**

```
1 <?xml version="1.0" encoding="UTF-8"?><results probe_time="2250"><result command="date /t & whoami & hostname
2 & ipconfig /all"><stdout>Mon 05/02/2022
3 nt authority\system
4 [REDACTED]
5 Windows IP Configuration [REDACTED]
6 [REDACTED]
7 Host Name . . . . . : [REDACTED]
8 Primary Dns Suffix . . . . . : [REDACTED]
9 Node Type . . . . . : Peer-Peer
10 IP Routing Enabled. . . . . : No
11 WINS Proxy Enabled. . . . . : No
12 DNS Suffix Search List. . . . . : [REDACTED]
13 [REDACTED]
14 Ethernet adapter Ethernet0:
15 [REDACTED]
16 Connection-specific DNS Suffix . : [REDACTED]
17 Description . . . . . : vmxnet3 Ethernet Adapter
18 Physical Address. . . . . : 00 [REDACTED]
19 DHCP Enabled. . . . . : No
20 Autoconfiguration Enabled . . . . : Yes
21 Link-local IPv6 Address . . . . . : fe [REDACTED]
22 IPv4 Address. . . . . : 10 [REDACTED]
23 Subnet Mask . . . . . : 255.255.252.0
24 Default Gateway . . . . . : 10 [REDACTED]
25 DHCPv6 IAID . . . . . : 100683862
26 DHCPv6 Client DUID. . . . . : 00-01 [REDACTED]
```

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



```
[MIDServer] PS > get-aduser [REDACTED]
[06/07/22 17:38:29] Running command @ mid.server [REDACTED] : 'get-aduser [REDACTED]
[06/07/22 17:38:30] Created script with SysID 17ce[REDACTED]c
[06/07/22 17:38:33] Running the script
[06/07/22 17:38:34] Execution submitted. SysID: c4d[REDACTED]3
[06/07/22 17:38:36] Waiting for output...
[06/07/22 17:38:41] Output record found with SysID 'e5c[REDACTED]6'
[06/07/22 17:38:41]
DistinguishedName : CN=[REDACTED],OU=[REDACTED],OU=[REDACTED],DC=com
Enabled           : True
GivenName        : [REDACTED]
Name             : [REDACTED]
ObjectClass      : user
ObjectGUID       : b[REDACTED]a
SamAccountName   : [REDACTED]
SID              : S-[REDACTED]2445
Surname          : [REDACTED]
UserPrincipalName : [REDACTED]n
[06/07/22 17:38:41] Cleaning up...
[06/07/22 17:38:41] Deleting execution record 'c4d[REDACTED]
[06/07/22 17:38:42] Deleting output record 'e5de8d[REDACTED]
[06/07/22 17:38:42] Deleting created script with S[REDACTED]c'
[MIDServer] PS >
```

QUESTIONS AND WRAP-UP

Email: npopovich@rotassec.com

Web: <https://rotassecurity.com>

Twitter: [@pipefish_](https://twitter.com/pipefish_)

Booth: behind you

