



Exploring 3rd party apps in Entra ID: Utilizing Free and Built-In Tools for Risk Assessment Process



Who am I

Lead Security Architect @
Storebrand

Education

Master of Science in
Information Security

Consultant

10+ Years as
consultant

MSUG

Part of Microsoft
Security User Group
Organizers

Hobbies

Gaming in winter and
disc golf during
summer

Security MVP



Agenda

- Landscape and current state
- Demo MFA
- Entra ID Applications overview
- Detection and protection options
- 3rd party consent app demo
- Where do I start?
- Demo on how to get insight and conduct risk analysis



Threat Landscape: identity

Russia

Nation state threat actor activity

Targeting by region



Sector	Percentage
1 Europe & Central Asia	68%
2 North America	20%
3 Middle East & North Africa	5%
4 East Asia & Pacific	3%
5 Latin America & Caribbean	3%
6 South Asia	1%
7 Sub-Saharan Africa	1%

Most targeted sectors



Sector	Percentage
1 Government	33%
2 IT	15%
3 Think tanks and NGOs	15%
4 Education and Research	9%
5 Inter-governmental organization	4%
6 Defense Industry	4%
7 Transportation	3%
8 Energy	2%
9 Media	2%
10 All others	13%

600 million identity attacks per day. As multifactor authentication blocks most password-based attacks, threat actors are shifting their focus

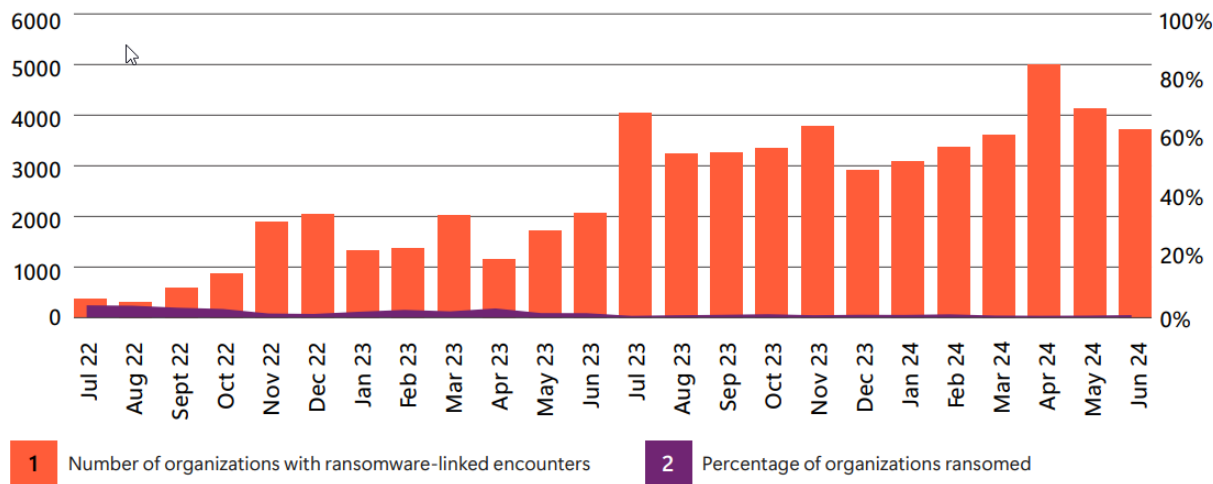
2.6% of workload identity permissions were used and 51% of workload identities were completely inactive.

2.75x increase in human-operated ransomware-linked encounters



Ransomware statistics

Organizations with ransom-linked encounters continues to increase while the percentage of those ransomed is decreasing (July 2022–June 2024)



Although organizations with ransom-linked encounters continues to increase, the percentage that are ultimately ransomed (reaching encryption stage) decreased more than threefold over the past two years.

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.


More than
99% of identity
attacks are
password attacks

Breach replay

Password spray

Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1%
of attacks



MFA attacks

SIM swapping

MFA fatigue

AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.



Post-authentication attacks

Token theft

Consent phishing

Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.



Infrastructure compromise

Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Case Study: Octo Tempest (aka Scattered Spider)

- Octo Tempest is a financially motivated cybercriminal group known for wide-ranging campaigns that feature adversary-in-the-middle (AiTM)
- Octo Tempest uses extensive social engineering techniques, including researching an organization to identify targets and then impersonating employees or members on phone calls to trick technical administrators into performing password resets or resetting multifactor authentication (MFA) methods.
- Exfiltrates data with native tools (Data factory automated pipelines)

TTP: Octo Tempest (aka Scattered Spider)

Tactics, techniques, and procedures used by Octo Tempest

Initial access

Social engineering
Masquerading and impersonation

Discovery

Enumerating internal documentation
Continuing environmental reconnaissance

Credential access, lateral movement

Identifying high-value assets
Accessing enterprise environments via VPN
Collecting additional credentials

Defense evasion, execution

Leveraging EDR and management tooling
Circumventing Conditional Access

Persistence

Installing a trusted backdoor
Manipulating existing accounts
Establishing access to resources

Actions on objective

Staging and exfiltrating stolen data
Deploying BlackCat ransomware

BRUCE WAYNE/BATMAN'S THREAT MODEL



ASSETS



BAT CAVE



ALFRED



EMAILS



TEXTS

PROTECTION



SECURITY SYSTEM



HIDE LOCATION



ENCRYPTION

THREATS



POLICE



THE JOKER



JOURNALISTS

--- LOW RISK
— MED RISK
= HIGH RISK





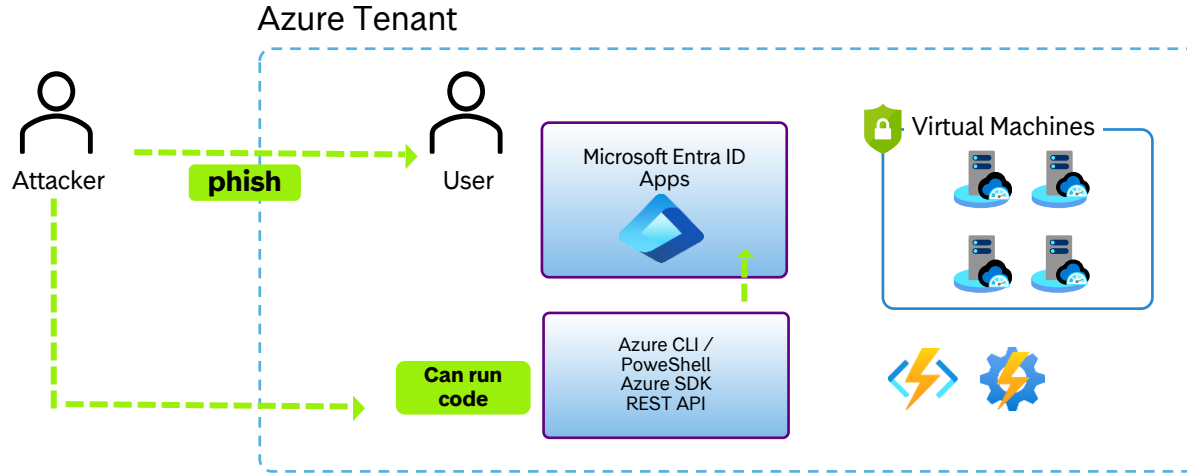
Understand your attack paths

Attack path insights for threat-informed defense (June 2024)



Attack path MFA - Reconnaissance

Passwords are strong enough?



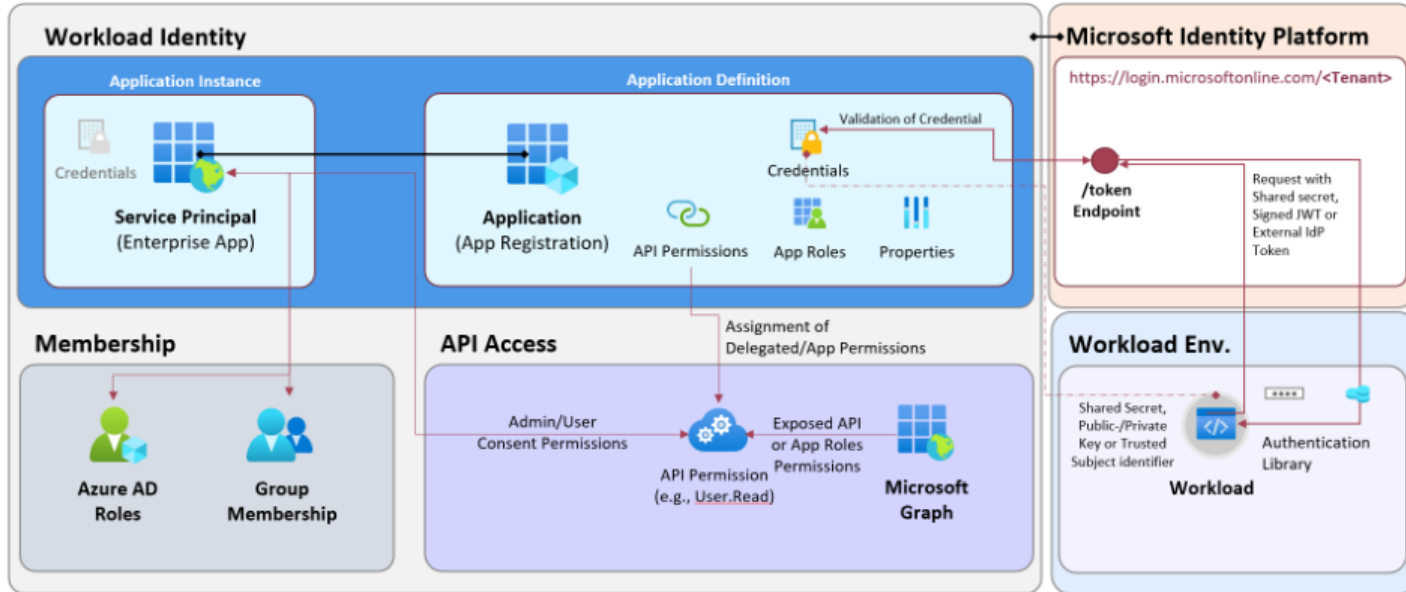
✓ Your organization is protected by security defaults.

[Manage security defaults](#)



Demo MFA

Entra ID Objects of Application Identities



Source: cloud-architekt.net/



Application types

1st party apps

- Developed by Microsoft and are designed to work seamlessly with the Microsoft Ecosystem
- These apps tend to be forgotten but can have a quite large attack surface.
- These apps don't always result in a service principal being created in your tenant. This can lead to confusion.

Own applications

- Developed or created by the organization
- Typical misconfiguration issues with broad access (owners)
- Poor credential management
- Conditional Access
- Lack of monitoring of these apps

3rd party apps

- Managing access can be more complex than 1st party.
- Supply chain review of 3rd party apps is rarely conducted. (NSM Report)
- Conditional Access policy misconfigurations.
- Too broad access
- Lack of risk detection and monitoring

Application type == Microsoft Applications X



Apps we might want to limit or have control of.

**Microsoft Graph
PowerShell /
Microsoft Graph
Command Line
Tools**

(14d82eec-204b-4c2f-
b7e8-296a70dab67e)

Microsoft Graph
PowerShell (Recommended)

**Azure Active
Directory
PowerShell
(1b730954-1685-
4b74-9bfd-
dac224a7b894)**

Planned for deprecation March 30!
STILL HERE!

**Microsoft Azure
PowerShell
(1950a258-227b-
4e31-a9cf-
717495945fc2)**

Planned for deprecation March 30!
STILL HERE!

**Graph Explorer
(de8bc8b5-d9f9-
48b1-a8ad-
b748da725064)**

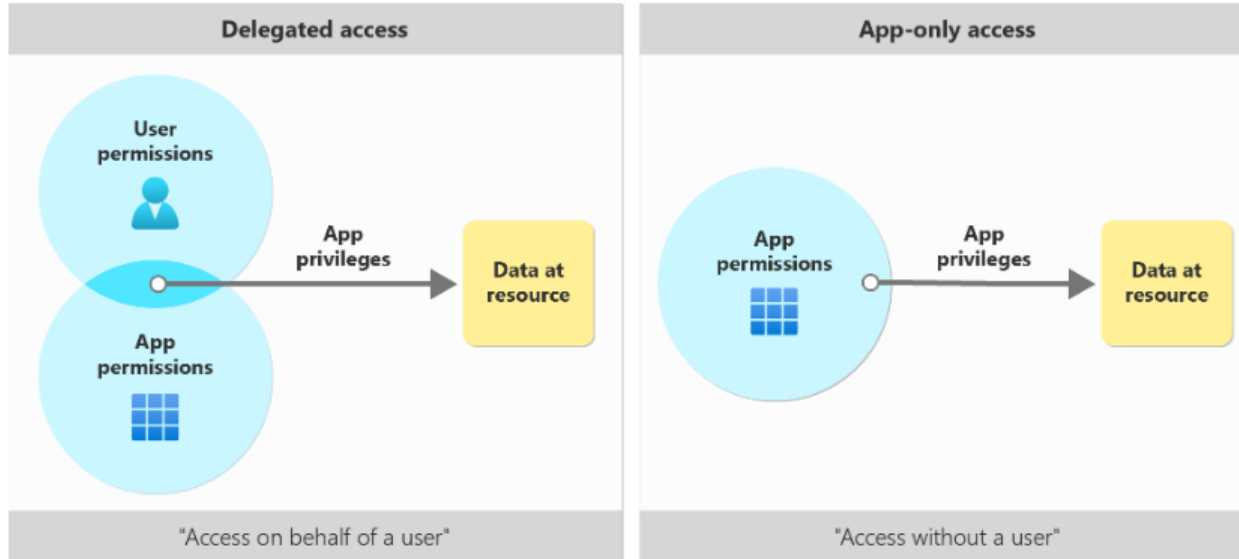
Powerful tool that allows you to make
requests and see responses against
Microsoft Graph

Verify first-party Microsoft applications



Navigating Entra ID: Consents

Delegated vs application



Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (demotroll only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

[Help me decide...](#)



Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)



Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

Yes

No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock ⓘ

Configure the application instance modification lock. [Learn more](#)

[Configure](#)

Resource lock on 3rd party apps:

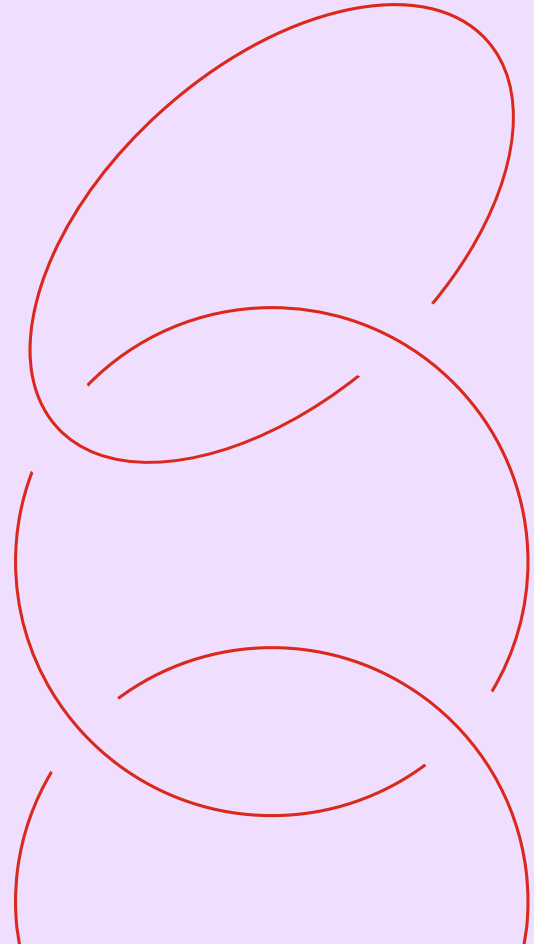
- Application instance lock is a feature in Microsoft Entra ID that allows sensitive properties of a multitenant application object to be locked for modification after the application is provisioned in another tenant.

Enable property lock	Specifies if the property locks are enabled.
All properties	Locks all sensitive properties without needing to select each property scenario.
Credentials used for verification	Locks the ability to add or update credential properties used for verification.
Credentials used for signing tokens	Locks the ability to add or update credential properties used for signing tokens.
Token Encryption KeyId	Locks the ability to change the tokenEncryptionKeyId property.



“

Demo 3rd party app
rights



Permissions requested

Review for your organization



This application is not published by Microsoft or your organization.

This app would like to:

✓ Sign in and read user profile

^ Read mail in all mailboxes

Allows the app to read mail in all mailboxes without a signed-in user.

This is a permission requested to access your data in demotroll.

^ Read all users' full profiles

Allows the app to read user profiles without a signed in user.

This is a permission requested to access your data in demotroll.

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept



Where do I start?

- Inventory off applications is key
- Legal obligations to Dora
- Start with tier 0 rights
- Check if you have broad email send rights
- Use Role based access for application in Exchange online.
- When creating apps, use least privileged scopes
- Create gallery applications if possible

Demo: Insights in apps and risk process

Setup basic application governance

Setup Entra ID User settings

- **Only administrators are Allowed to register applications.**
- **Only administrators are allowed to consent to applications.**
- **An admin consent workflow be configured for applications.**
- **Group owners should not be allowed to consent to applications.**

⊗ Caution

Using the Restrict access to Microsoft Entra administration portal switch is **NOT** a security measure. For more information on the functionality, see the table below.



App governance

Get in-depth visibility and control over OAuth apps integrated with Microsoft 365, Google, and Salesforce.

[What's new](#) [Learn more](#)

[Overview](#) [Microsoft 365](#) [Alerts](#) [Policies](#)

Apps

549 apps found [ⓘ](#)
57 overprivileged apps [ⓘ](#)
208 unused apps [ⓘ](#)
86 highly privileged apps [ⓘ](#)

[View all apps](#)

Incidents

13 unresolved incidents
9 threat incidents
4 policy incidents

[View all incidents](#)

Latest incidents

Last Act...	Severity	Incident name	Source
9/17/2024	Medium	Increase in data ...	Policy
9/6/2024	Medium	Increase in data ...	Policy
8/20/2024	Medium	Dormant OAuth ...	Detection
8/16/2024	Medium	Dormant OAuth ...	Detection
8/14/2024	High	App accessed fr...	Detection
8/8/2024	Medium	Dormant OAuth ...	Detection
8/8/2024	Medium	Dormant OAuth ...	Detection
7/29/2024	Medium	App accessed se...	Policy
7/21/2024	Medium	Dormant OAuth ...	Detection
7/10/2024	Medium	Dormant OAuth ...	Detection

[View all incidents](#)

Predefined policies

Your predefined policies are active

Receive alerts from default policies that identify risky apps, such as apps with excessive privileges, unusual characteristics, or suspicious activities.

Active predefined policies 12 / 12

[View predefined policies](#)

App categories

All apps	Highly privileged	Overprivileged	Unused	Unverified publisher	...
App name	App status	Permission	Consent type	Publis...	Last modified
Cloudockit	Disabled by user	Delegated	Admin	N/A	Sep 10, 2024 1...
Customer Client SPP Dev	Disabled by user	Delegated	Admin	N/A	Jun 6, 2024 8:5...
Secure Practice	Enabled	Delegated	Admin	N/A	

[View all apps](#)

Apps that accessed Microsoft 365 services

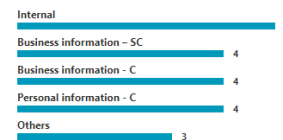
Last 30 days



[View apps](#)

Sensitive data accessed

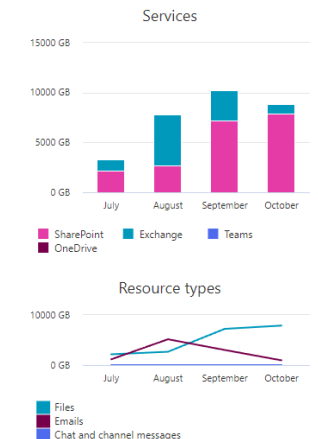
Last 30 days



[View apps](#)

Data usage

Data usage for various services and resources that were accessed using Graph API



Security portal – must be turned on



Navigating Entra ID: Detection and OPS

Detection with log analytics -> Monitor alert, Sentinel incident or hunting

Costs graph activity of this log?

Corp A 200 users

Corp B 40K users

Corp Finance

Table	↑↓	Ingestion Volume	↑↓
MicrosoftGraphActivityLogs		38.27MB	
MicrosoftGraphActivityLogs		1.12GB	
MicrosoftGraphActivityLogs		2.69GB	

Diagnostic setting name

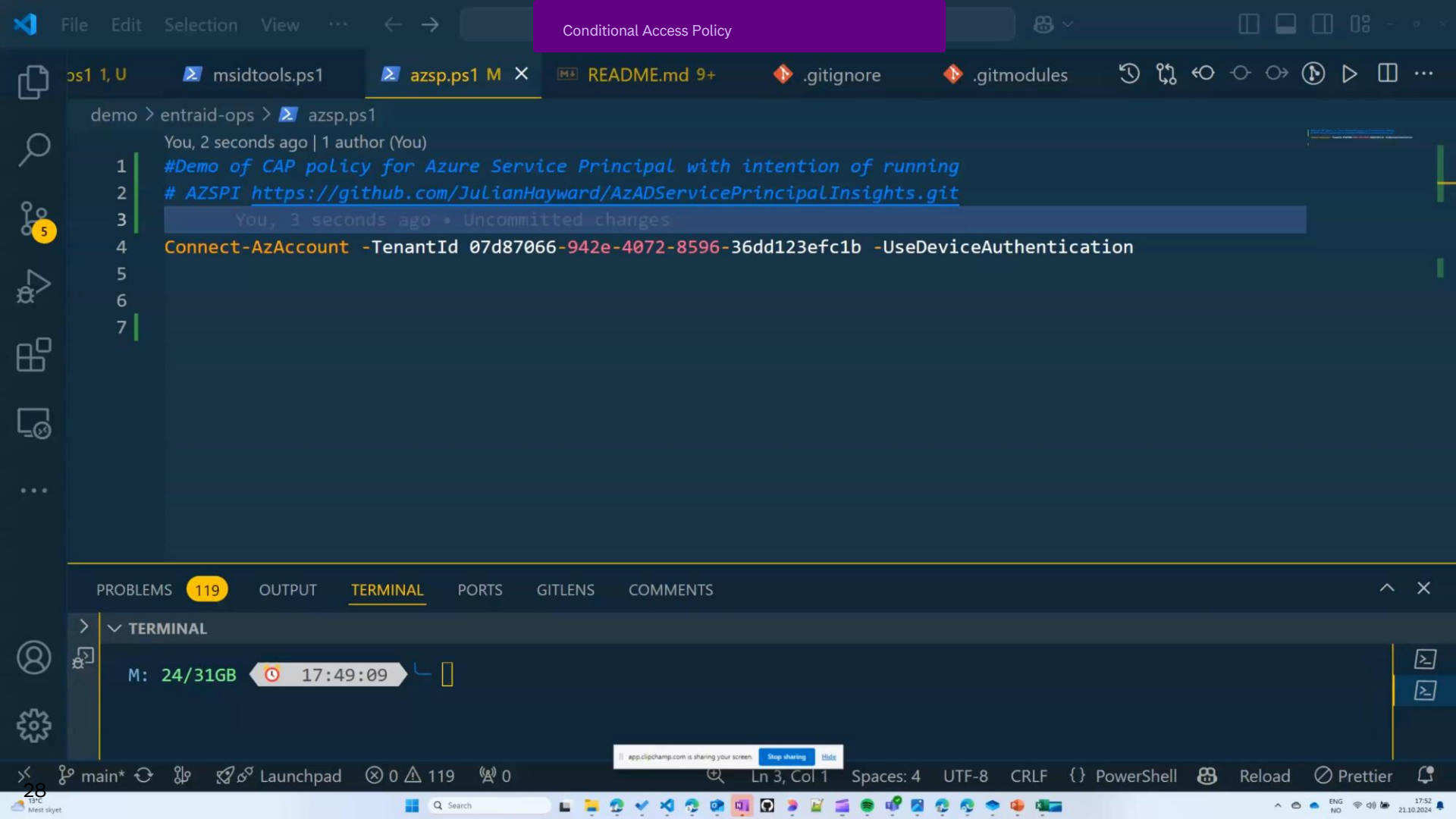
Logs

Categories

☒ AuditLogs

☒ SignInLogs







References / Tools

[AzureAD/MSIdentityTools](#): PowerShell modules Entra ID

<https://graphpermissions.merill.net/>

[MFA Sweep: A tool for checking if MFA status](#)

[Microsoft Digital Defense Report 2024](#)

aka.ms/AzADSPI - Insights and change tracking on Microsoft Entra ID Service Principals

[AppConsent](#)

APPS EVERYWHERE



**DO YOU HAVE ANY
QUESTIONS?**

