www.wpninjas.eu
#WPNinjaS

Security misconfigurations in the wild: What We See, What You Should Fix

Nicola Suter & Loris Ambrozzo

Workplace Ninja Summit 2025

About Us

	Loris Ambrozzo	Nicola Suter
Focus	Security	Security, ITDR
Location	Switzerland	Switzerland
Certifications	Microsoft, SANS	Microsoft Security MVP
Hobbies	Running, Hiking	Cycling, Running, Mountaineering
Contact	in	in
Blog	lorisambrozzo.medium.com	tech.nicolonsky.ch

Our Motivation

Most common critical assessment findings (exploited in the wild)

Technical depth, legacy and simply overlooked

Remediation is often possible with built-in options

Our Assumption

- Cloud-Only Admin Accounts
- MFA Enforcement
- Legacy and Insecure Authentication Protocols Disabled
- App Consent
- Privileged Identity Management (PIM)
- Microsoft Managed CA Policies Adopted

Microsoft Motivation

“Microsoft Incident Response (IR) is often engaged in cases where organizations have lost control of their Microsoft Entra ID tenant due to a combination of **misconfiguration**, administrative **oversight**, **exclusions** to security policies, or **insufficient protection for identities**.”

Source: https://www.microsoft.com/en-us/security/blog/2023/12/05/microsoft-incident-response-lessons-on-preventing-cloud-identity-compromise/

Agenda

Key takeaways:

- Learn about the most common security misconfigurations and how attackers can exploit them.
- Discover practical mitigation steps to close these gaps and strengthen your security posture.

The why of this session

Why is resolving misconfiguration so important?

Insufficient Identity Hardening

How do we improve the security of our Identities?

Unsecured External User Access

How can we protect partner access in our tenant?

Incomplete XDR Deployments

How to we improve our XDR deployment?

Wrap up

Recap of the session

How We Approach Today’s Session

Sections

Summary after each section

In Detail

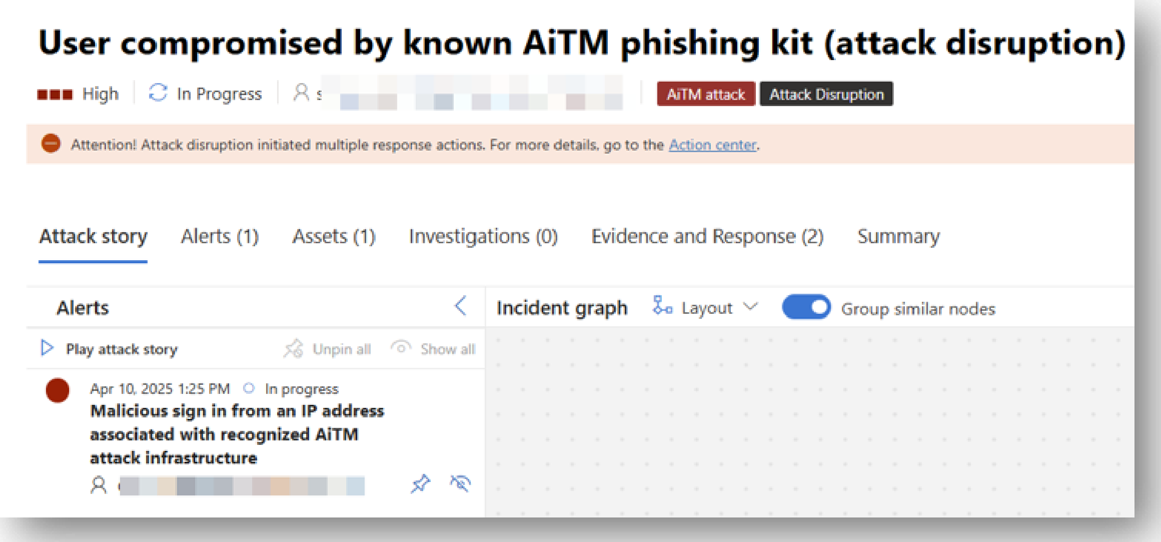
Misconfiguration	Real-world-environment-distribution	Exploitation	Remediation
<>	Based on our assessments and consulting engagements.		

Check the updated handout on sched. We will included links with additional information!

Insufficient protection for identities

Misconfiguration	Real-world-environment-distribution
Missing ID Protection Policies	8 out of 10 tenants have either the policies not active or enabled the policy in the legacy blade

Missing Entra ID Protection Policies

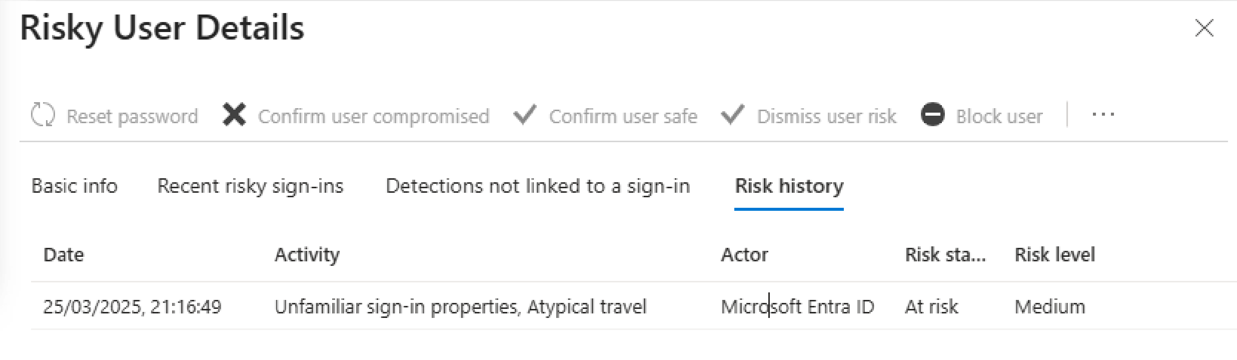


User compromised by known AiTM phishing kit (attack disruption)

High | In Progress | [redacted] | AiTM attack | Attack Disruption

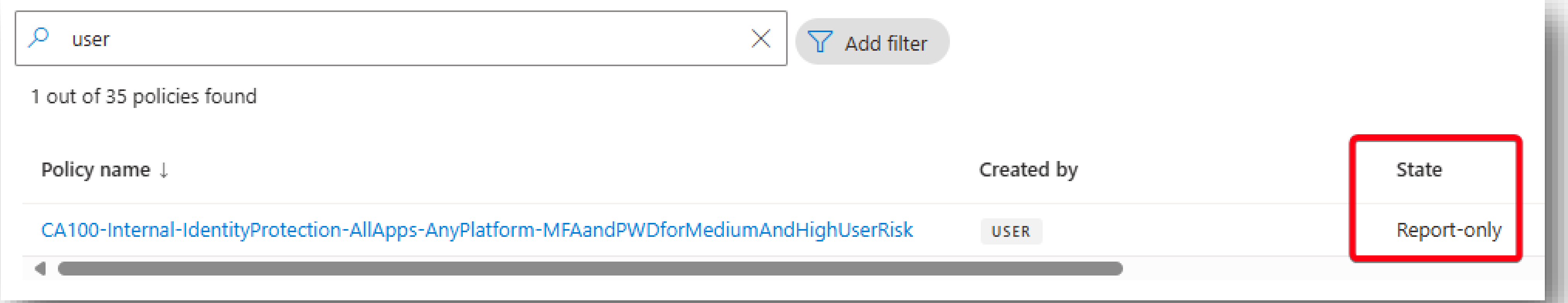
Attention! Attack disruption initiated multiple response actions. For more details, go to the Action center.

Apr 10, 2025 1:25 PM · In progress
Malicious sign in from an IP address associated with recognized AiTM attack infrastructure
[redacted]



Risky User Details

Date	Activity	Actor	Risk sta...	Risk level
25/03/2025, 21:16:49	Unfamiliar sign-in properties, Atypical travel	Microsoft Entra ID	At risk	Medium

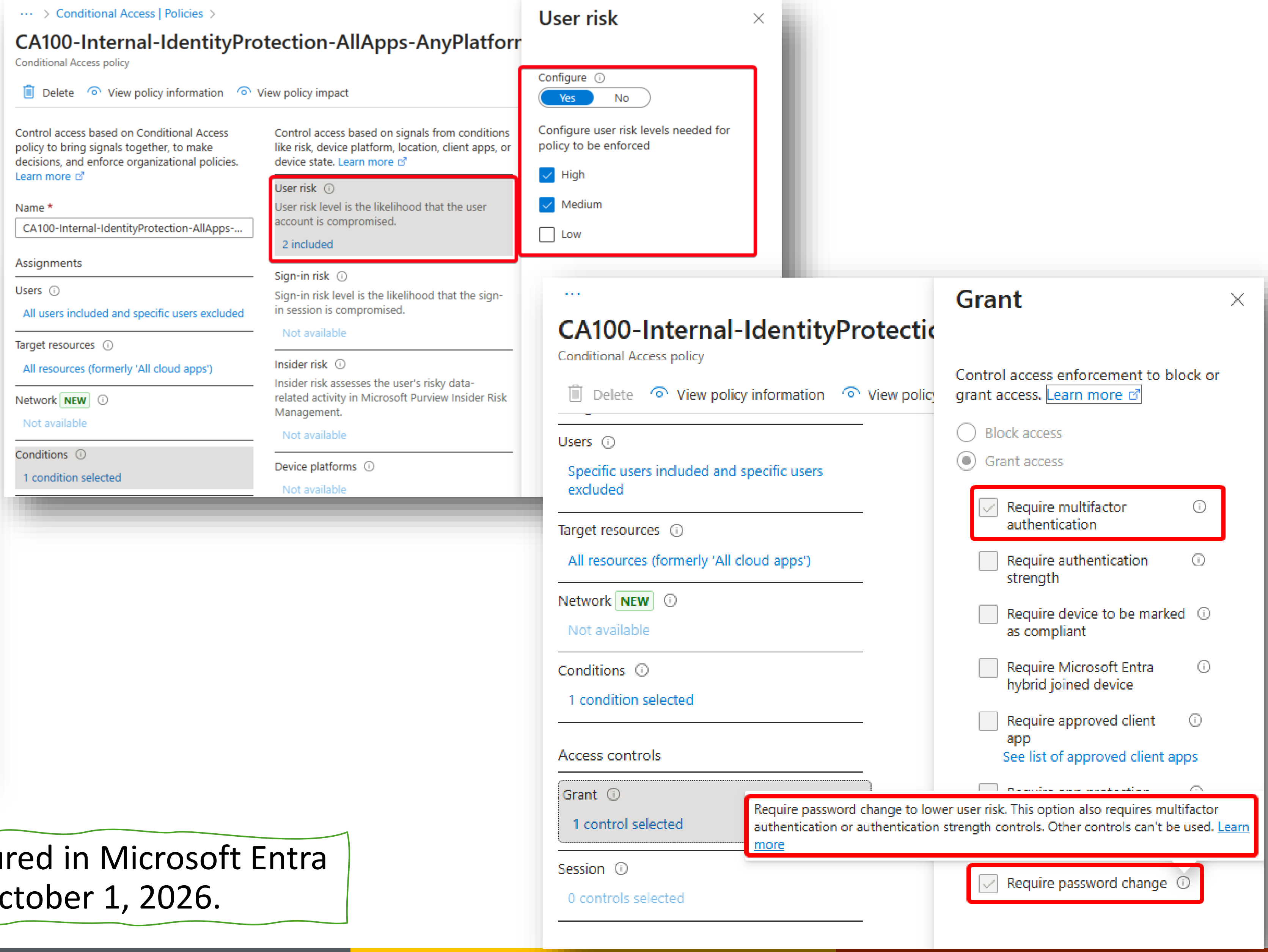


1 out of 35 policies found

Policy name ↓	Created by	State
CA100-Internal-IdentityProtection-AllApps-AnyPlatform-MFAandPWDforMediumAndHighUserRisk	USER	Report-only

Missing Entra ID Protection Policies

www.wpninjas.eu
#WPNinjaS



CA100-Internal-IdentityProtection-AllApps-AnyPlatform
Conditional Access policy

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

Name *
CA100-Internal-IdentityProtection-AllApps-...

Assignments

Users ⓘ
All users included and specific users excluded

Target resources ⓘ
All resources (formerly 'All cloud apps')

Network NEW ⓘ
Not available

Conditions ⓘ
1 condition selected

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

User risk ⓘ
User risk level is the likelihood that the user account is compromised.
2 included

Sign-in risk ⓘ
Sign-in risk level is the likelihood that the sign-in session is compromised.
Not available

Insider risk ⓘ
Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.
Not available

Device platforms ⓘ
Not available

User risk

Configure ⓘ
[✓ Yes] No

Configure user risk levels needed for policy to be enforced

☑ High
☑ Medium
□ Low

CA100-Internal-IdentityProtectio
Conditional Access policy

Users ⓘ
Specific users included and specific users excluded

Target resources ⓘ
All resources (formerly 'All cloud apps')

Network NEW ⓘ
Not available

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

Grant

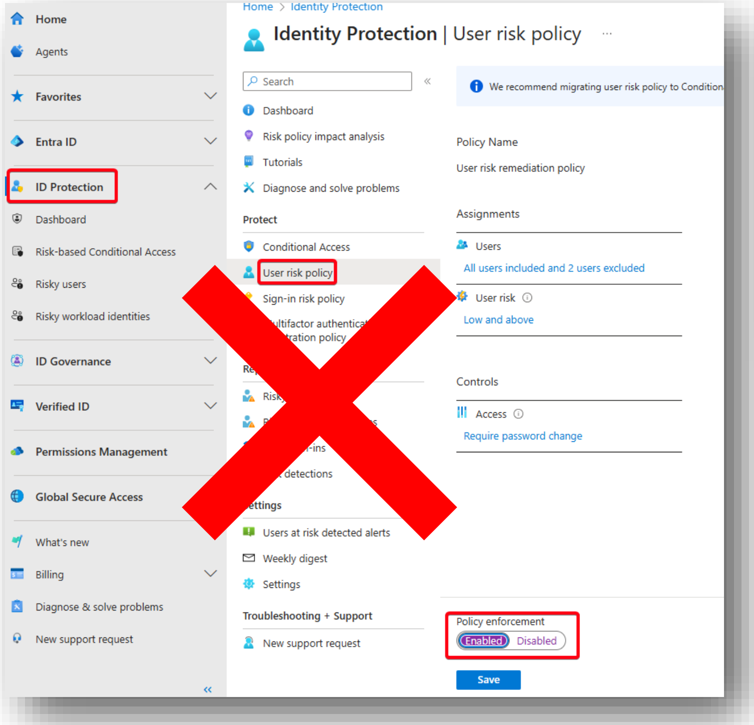
Control access enforcement to block or grant access. Learn more

○ Block access
● Grant access

☑ Require multifactor authentication ⓘ
□ Require authentication strength ⓘ
□ Require device to be marked as compliant ⓘ
□ Require Microsoft Entra hybrid joined device ⓘ
□ Require approved client app ⓘ
See list of approved client apps

Require password change to lower user risk. This option also requires multifactor authentication or authentication strength controls. Other controls can't be used. Learn more

☑ Require password change ⓘ



Identity Protection | User risk policy

We recommend migrating user risk policy to Condition

Policy Name
User risk remediation policy

Assignments

Users
All users included and 2 users excluded

User risk ⓘ
Low and above

Controls

Access ⓘ
Require password change

Policy enforcement
[✓ Enabled] Disabled

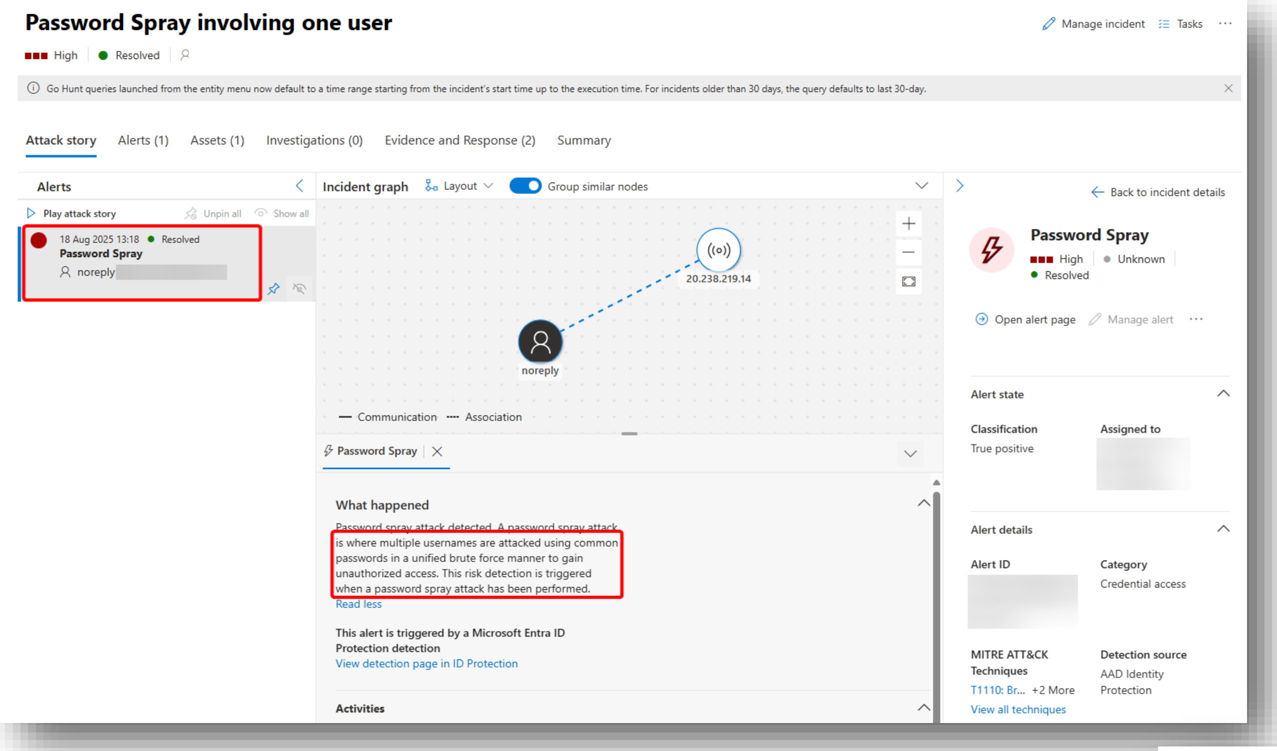
Save

The legacy risk policies configured in Microsoft Entra ID Protection are retiring on October 1, 2026.

Insufficient protection for identities

Misconfiguration	Real-world-environment-distribution
Missing ID Protection Policies	8 out of 10 tenants have either the policies not active or enabled the policy in the legacy blade
Legacy MFA Trusted Location	6 out of 10 tenants have still legacy MFA trusted location active

Legacy MFA Trusted Location



Password Spray involving one user

■■■ High | ● Resolved

ⓘ Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.

18 Aug 2025 13:18 ● Resolved
Password Spray
noreply [redacted]

What happened

Password spray attack detected. A password spray attack is where multiple usernames are attacked using common passwords in a unified brute force manner to gain unauthorized access. This risk detection is triggered when a password spray attack has been performed.
Read less

This alert is triggered by a Microsoft Entra ID Protection detection
View detection page in ID Protection

Activities

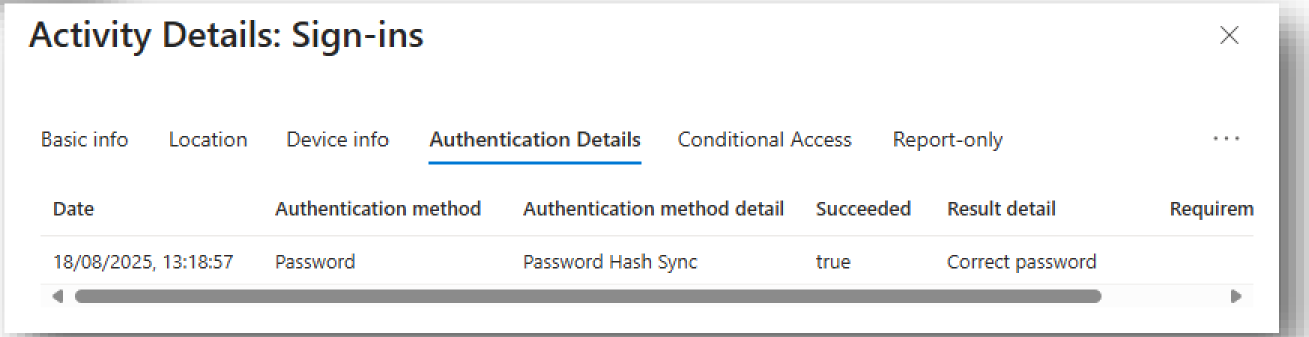
Password Spray
■■■ High | ● Unknown
● Resolved

Alert state

Classification: True positive
Assigned to: [redacted]

Alert details

Alert ID: [redacted]
Category: Credential access
MITRE ATT&CK Techniques: T1110: Br... +2 More
View all techniques
Detection source: AAD Identity Protection

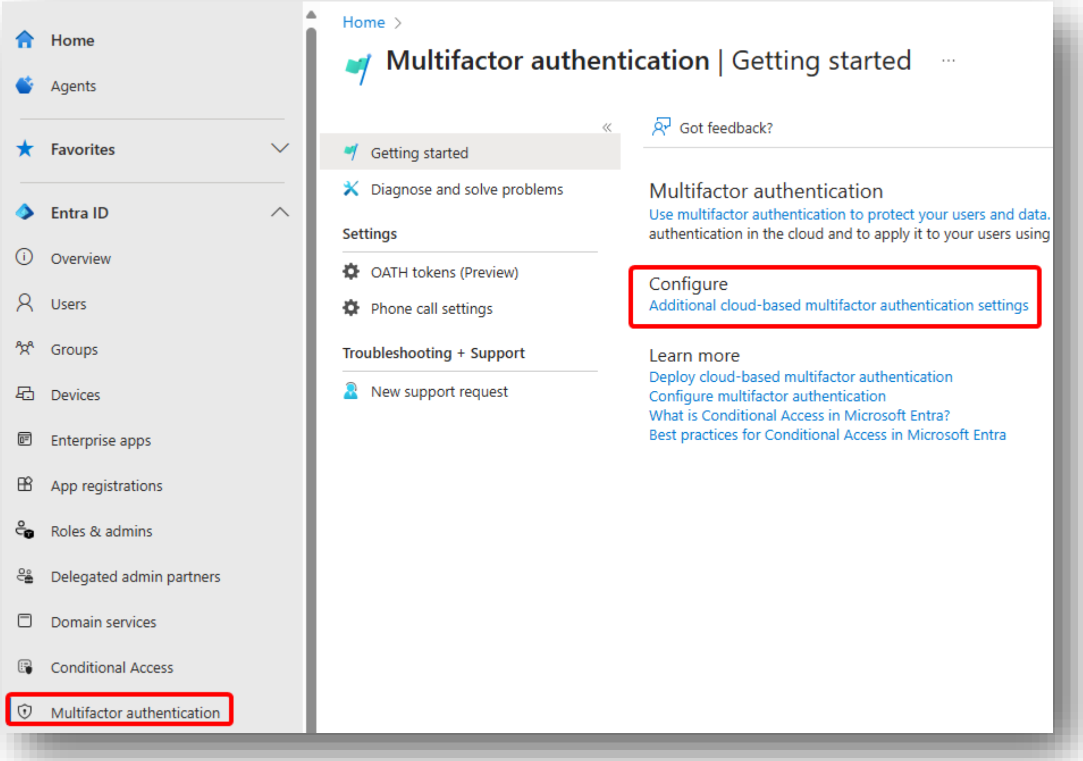


Activity Details: Sign-ins

Date	Authentication method	Authentication method detail	Succeeded	Result detail	Requirem
18/08/2025, 13:18:57	Password	Password Hash Sync	true	Correct password	

Legacy MFA Trusted Location

www.wpninjas.eu
#WPNinjaS



Home >

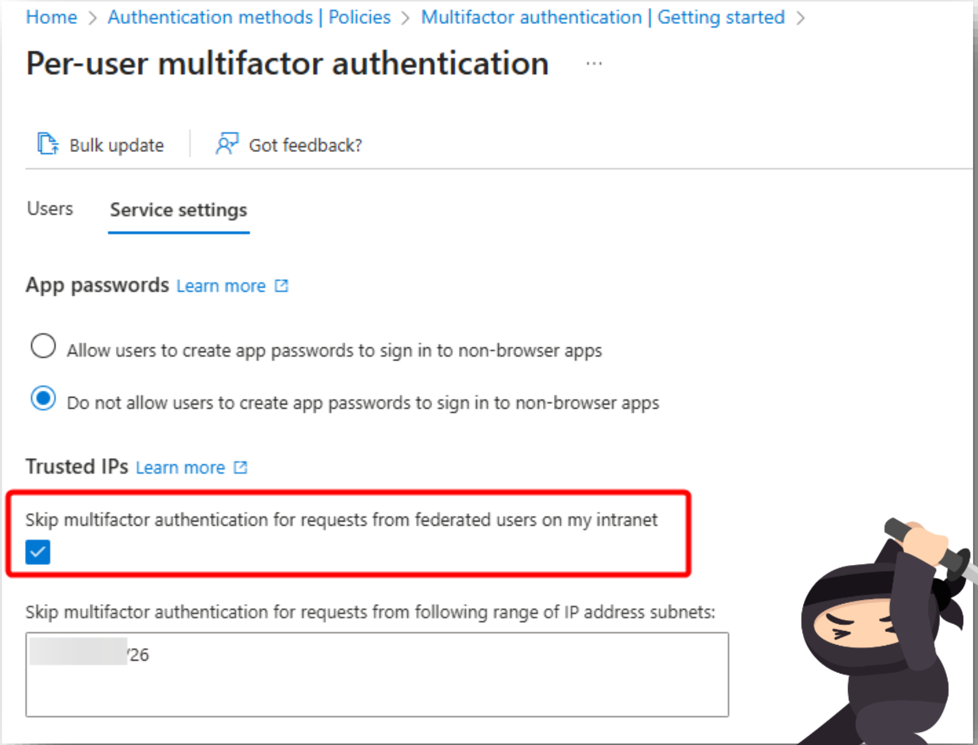
Multifactor authentication | Getting started ...

Multifactor authentication

Use multifactor authentication to protect your users and data.
authentication in the cloud and to apply it to your users using

Configure
Additional cloud-based multifactor authentication settings

Learn more
Deploy cloud-based multifactor authentication
Configure multifactor authentication
What is Conditional Access in Microsoft Entra?
Best practices for Conditional Access in Microsoft Entra



Home > Authentication methods | Policies > Multifactor authentication | Getting started >

Per-user multifactor authentication ...

App passwords Learn more

○ Allow users to create app passwords to sign in to non-browser apps

● Do not allow users to create app passwords to sign in to non-browser apps

Trusted IPs Learn more

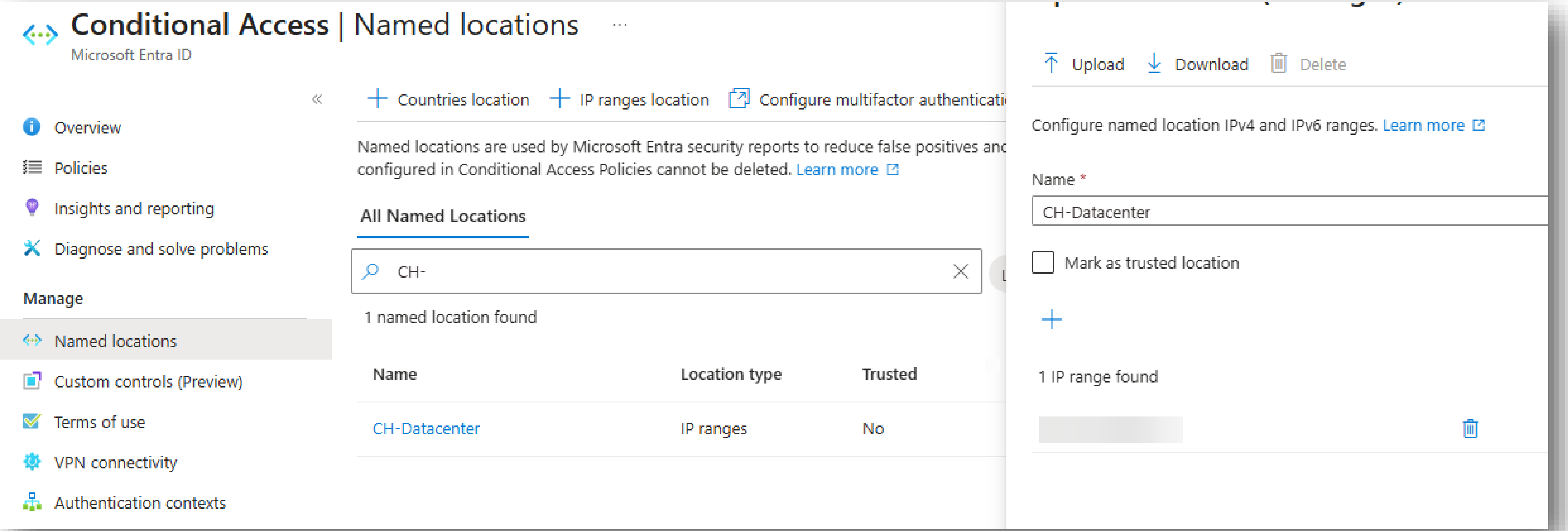
Skip multifactor authentication for requests from federated users on my intranet
☑

Skip multifactor authentication for requests from following range of IP address subnets:

[redacted]/26

With the migration to the new authentication method, the legacy MFA trusted locations will automatically be disabled.
https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-authentication-methods-manage

Legacy MFA Trusted Location



Conditional Access | Named locations ···

Microsoft Entra ID

Named locations are used by Microsoft Entra security reports to reduce false positives and
configured in Conditional Access Policies cannot be deleted. Learn more

CH-

1 named location found

Name	Location type	Trusted
CH-Datacenter	IP ranges	No

Configure named location IPv4 and IPv6 ranges. Learn more

Name *

CH-Datacenter

☐ Mark as trusted location

1 IP range found

Legacy MFA Trusted Location

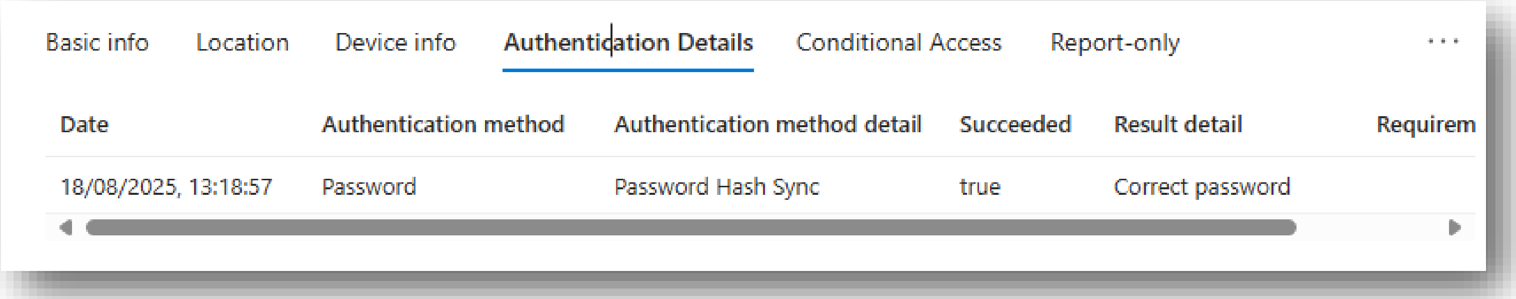
- Create a conditional access policy that excludes service accounts from multi-factor authentication (MFA) with a named location.

Legacy MFA Trusted Location

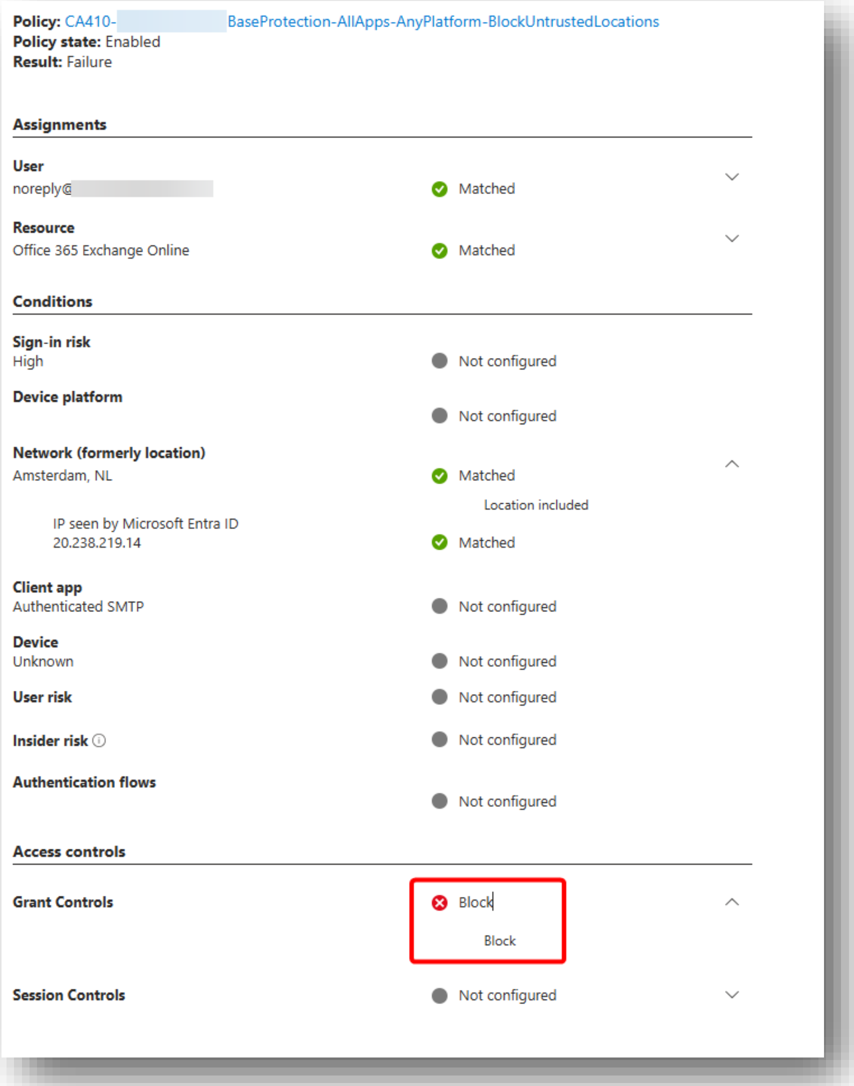
www.wpninjas.eu
#WPNinjaS

Do you remember?

- Username and Password was correct but…



Date	Authentication method	Authentication method detail	Succeeded	Result detail	Requirem
18/08/2025, 13:18:57	Password	Password Hash Sync	true	Correct password	



Policy: CA410-[redacted]BaseProtection-AllApps-AnyPlatform-BlockUntrustedLocations
Policy state: Enabled
Result: Failure

Assignments

User noreply@[redacted]	✓ Matched
Resource Office 365 Exchange Online	✓ Matched

Conditions

Sign-in risk High	● Not configured
Device platform	● Not configured
Network (formerly location) Amsterdam, NL	✓ Matched Location included
IP seen by Microsoft Entra ID 20.238.219.14	✓ Matched
Client app Authenticated SMTP	● Not configured
Device Unknown	● Not configured
User risk	● Not configured
Insider risk ⓘ	● Not configured
Authentication flows	● Not configured

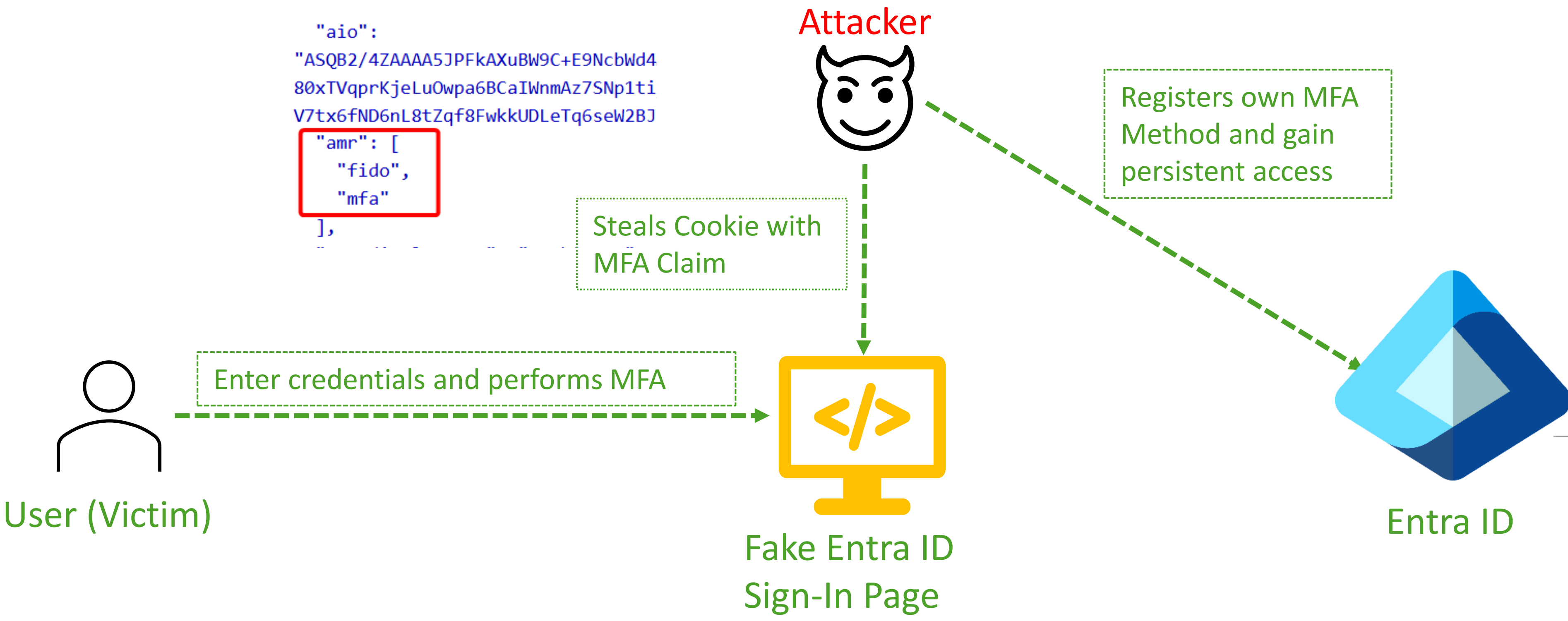
Access controls

Grant Controls	☒ Block Block
Session Controls	● Not configured

Insufficient protection for identities

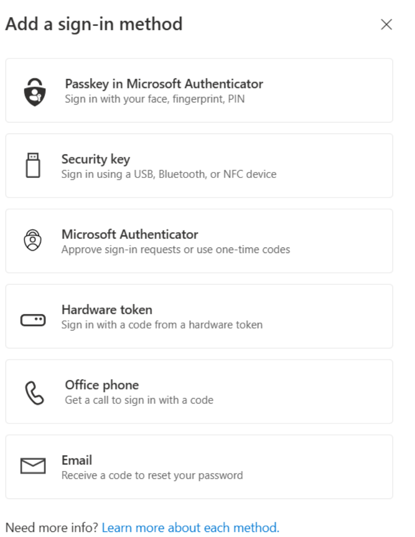
Misconfiguration	Real-world-environment-distribution
Missing ID Protection Policies	8 out of 10 tenants have either the policies not active or enabled the policy in the legacy blade
Legacy MFA Trusted Location	6 out of 10 tenants have still legacy MFA trusted location active
Unsecured MFA Registration	8 out of 10 tenants don’t have secured the MFA registration process

Unsecured MFA Registration



```
  "aio":
"ASQB2/4ZAAAA5JPFkAXuBW9C+E9NcbWd4
80xTVqprKjeLuOwpa6BCaIWnmAz7SNp1ti
V7tx6fND6nL8tZqf8FwkkUDLeTq6seW2BJ
  "amr": [
    "fido",
    "mfa"
  ],
```

Attacker
Steals Cookie with MFA Claim
Registers own MFA Method and gain persistent access
User (Victim)
Enter credentials and performs MFA
Fake Entra ID Sign-In Page
Entra ID



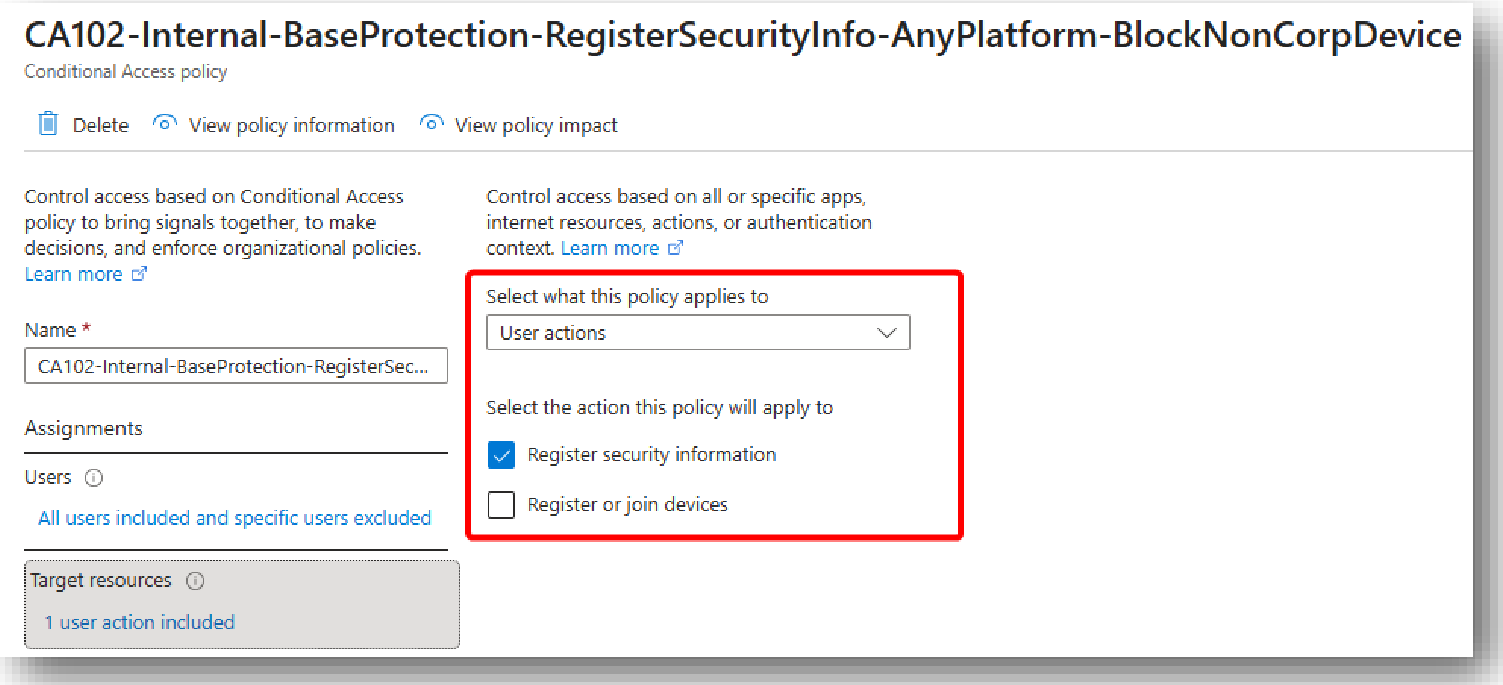
Add a sign-in method ×

- Passkey in Microsoft Authenticator
  Sign in with your face, fingerprint, PIN
- Security key
  Sign in using a USB, Bluetooth, or NFC device
- Microsoft Authenticator
  Approve sign-in requests or use one-time codes
- Hardware token
  Sign in with a code from a hardware token
- Office phone
  Get a call to sign in with a code
- Email
  Receive a code to reset your password

Need more info? Learn more about each method.

Advisory: Persistent MFA Circumvention in an Advanced BEC Campaign on Microsoft 365 Targets

Unsecured MFA Registration



CA102-Internal-BaseProtection-RegisterSecurityInfo-AnyPlatform-BlockNonCorpDevice

Conditional Access policy

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

Name *
CA102-Internal-BaseProtection-RegisterSec...

Assignments

Users
All users included and specific users excluded

Target resources
1 user action included

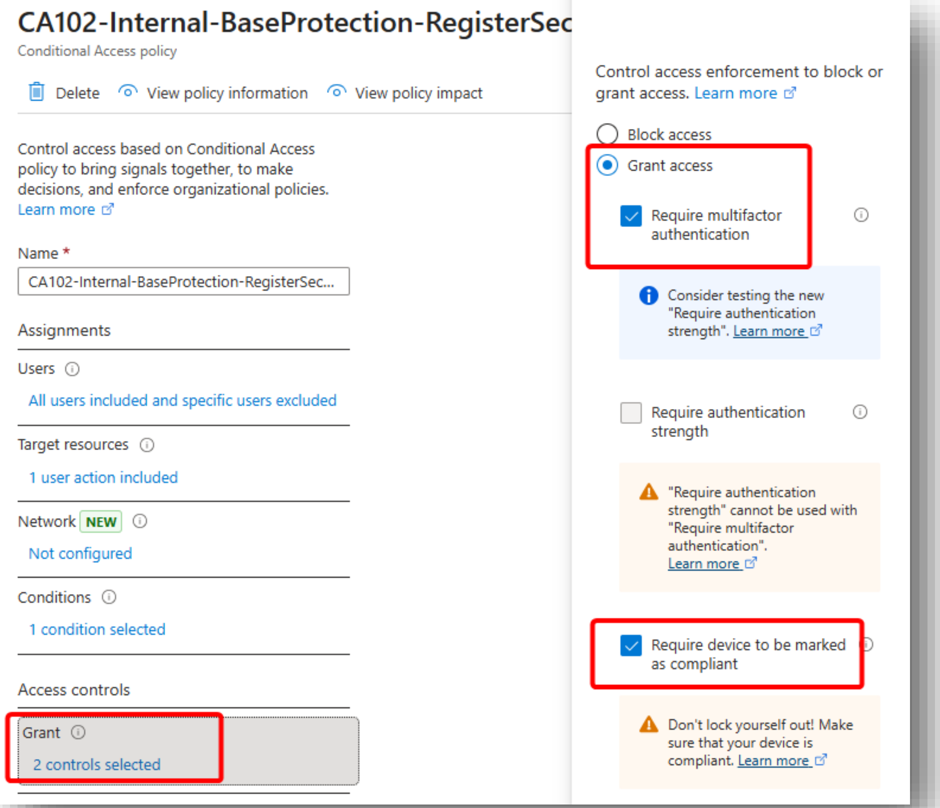
Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more

Select what this policy applies to
User actions

Select the action this policy will apply to

☑ Register security information

□ Register or join devices



CA102-Internal-BaseProtection-RegisterSec

Conditional Access policy

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

Name *
CA102-Internal-BaseProtection-RegisterSec...

Assignments

Users
All users included and specific users excluded

Target resources
1 user action included

Network NEW
Not configured

Conditions
1 condition selected

Access controls

Grant
2 controls selected

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

□ Require authentication strength

"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more

☑ Require device to be marked as compliant

Don't lock yourself out! Make sure that your device is compliant. Learn more

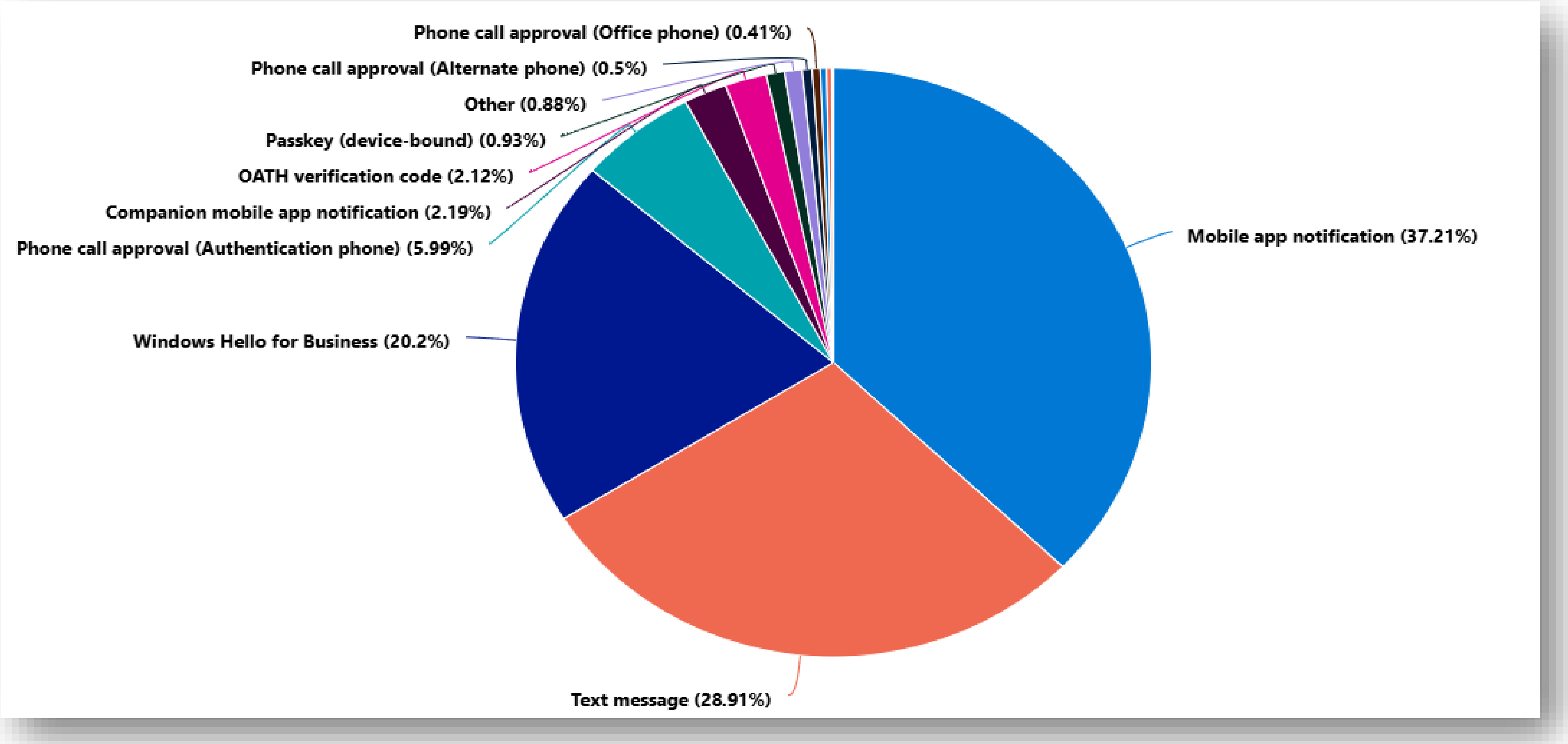
A well-designed MFA registration and sign-in process should be in place that supports all relevant use cases (new hires, external users, corporate users).

Insufficient protection for identities

Misconfiguration	Real-world-environment-distribution
Missing ID Protection Policies	8 out of 10 tenants have either the policies not active or enabled the policy in the legacy blade
Legacy MFA Trusted Location	6 out of 10 tenants have still legacy MFA trusted location active
Unsecured MFA Registration	8 out of 10 tenants don’t have secured the MFA registration process
Weak MFA allowed	7 out of 10 tenants still have weak MFA options.

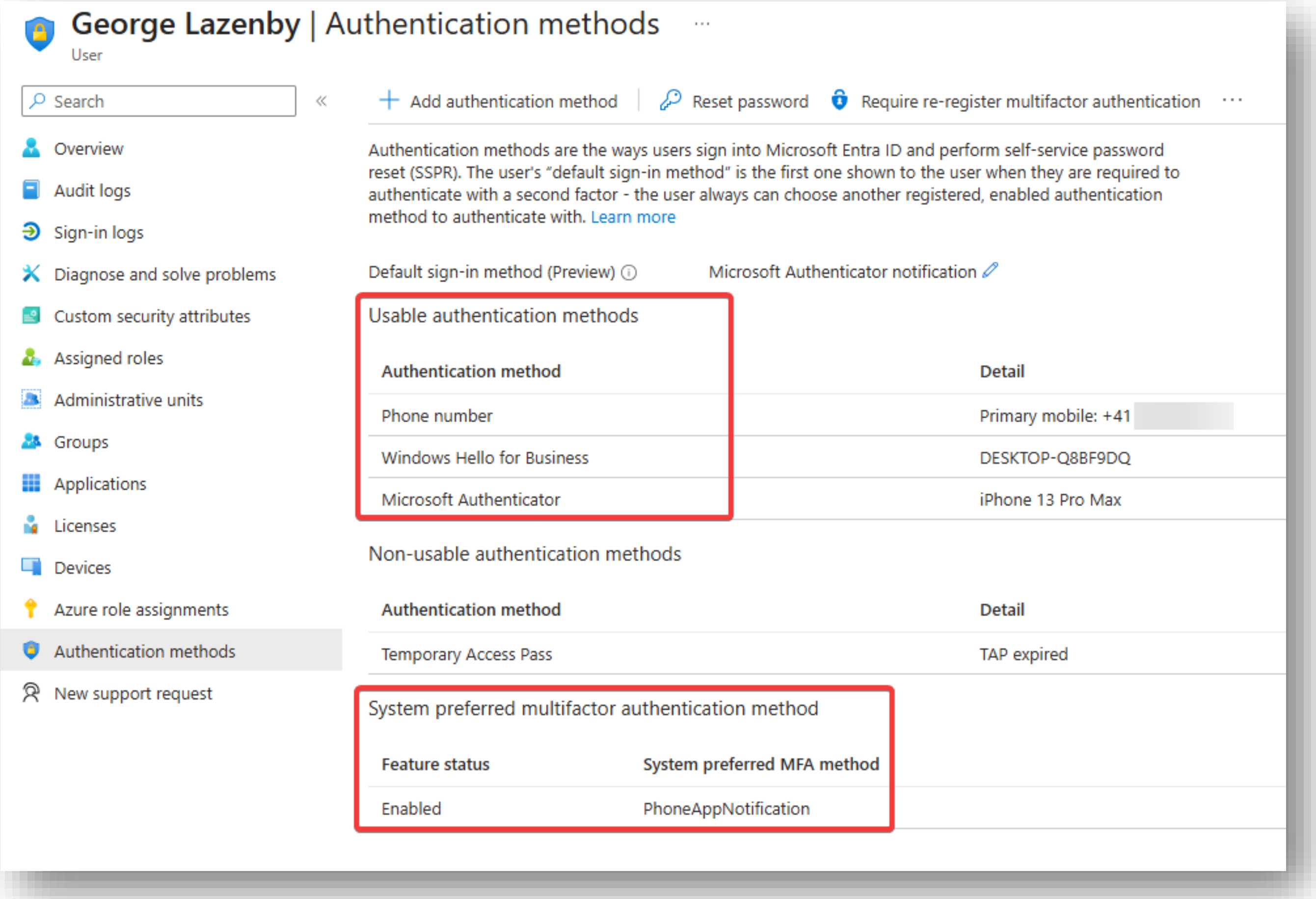
Real-World Example

Used authentication methods within the last 90 days.



Weak MFA allowed

Issue: The user has phone-based MFA enabled based on the authN methods policy.



George Lazenby | Authentication methods

User

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) ⓘ Microsoft Authenticator notification

Usable authentication methods

Authentication method	Detail
Phone number	Primary mobile: +41 [redacted]
Windows Hello for Business	DESKTOP-Q8BF9DQ
Microsoft Authenticator	iPhone 13 Pro Max

Non-usable authentication methods

Authentication method	Detail
Temporary Access Pass	TAP expired

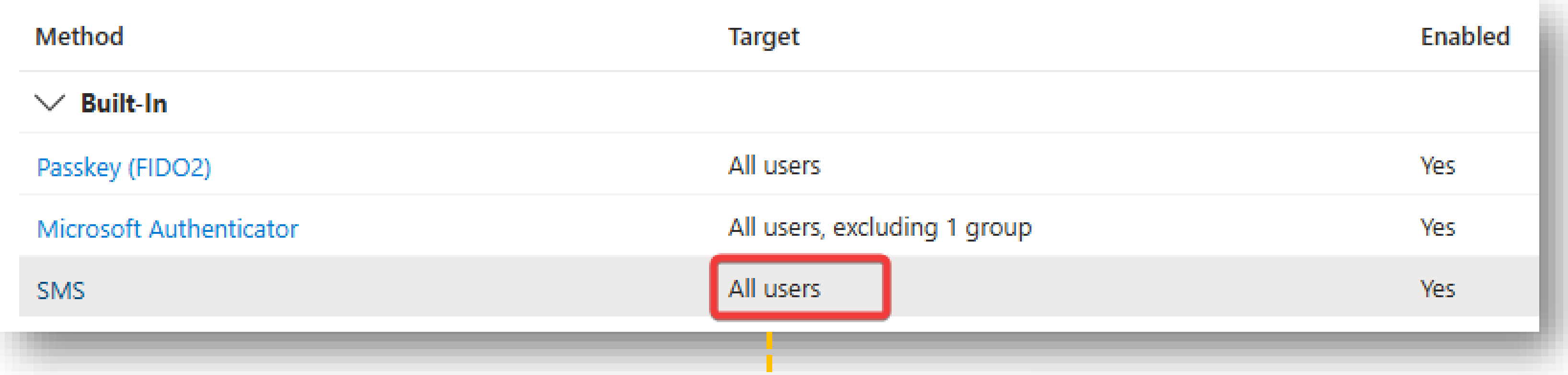
System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	PhoneAppNotification

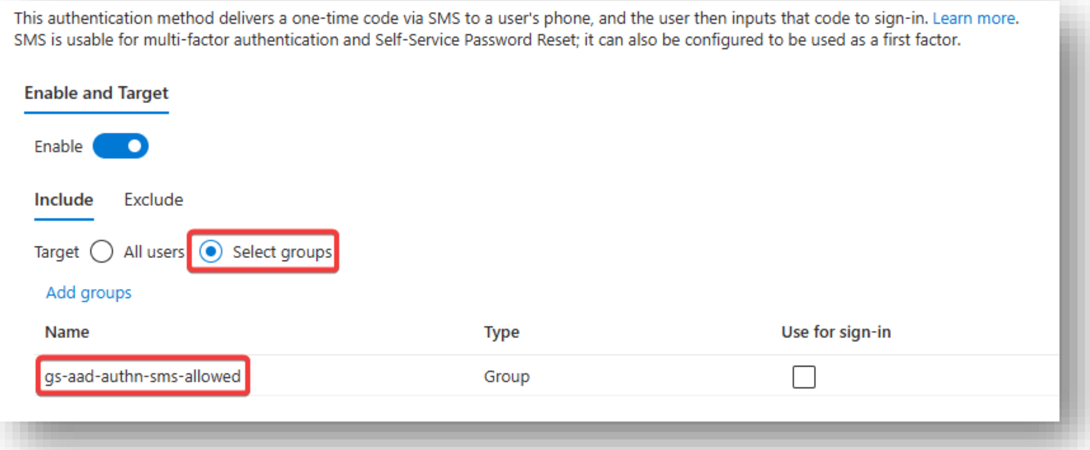
System preferred MFA will nudge the user to select the most secure option, but this is not an enforcement.

Weak MFA allowed

Example of limiting SMS authentication method to a limited group.



Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users, excluding 1 group	Yes
SMS	All users	Yes



This authentication method delivers a one-time code via SMS to a user's phone, and the user then inputs that code to sign-in. Learn more.
SMS is usable for multi-factor authentication and Self-Service Password Reset; it can also be configured to be used as a first factor.

Enable and Target

Enable: On

Include | Exclude

Target ○ All users ● Select groups

Add groups

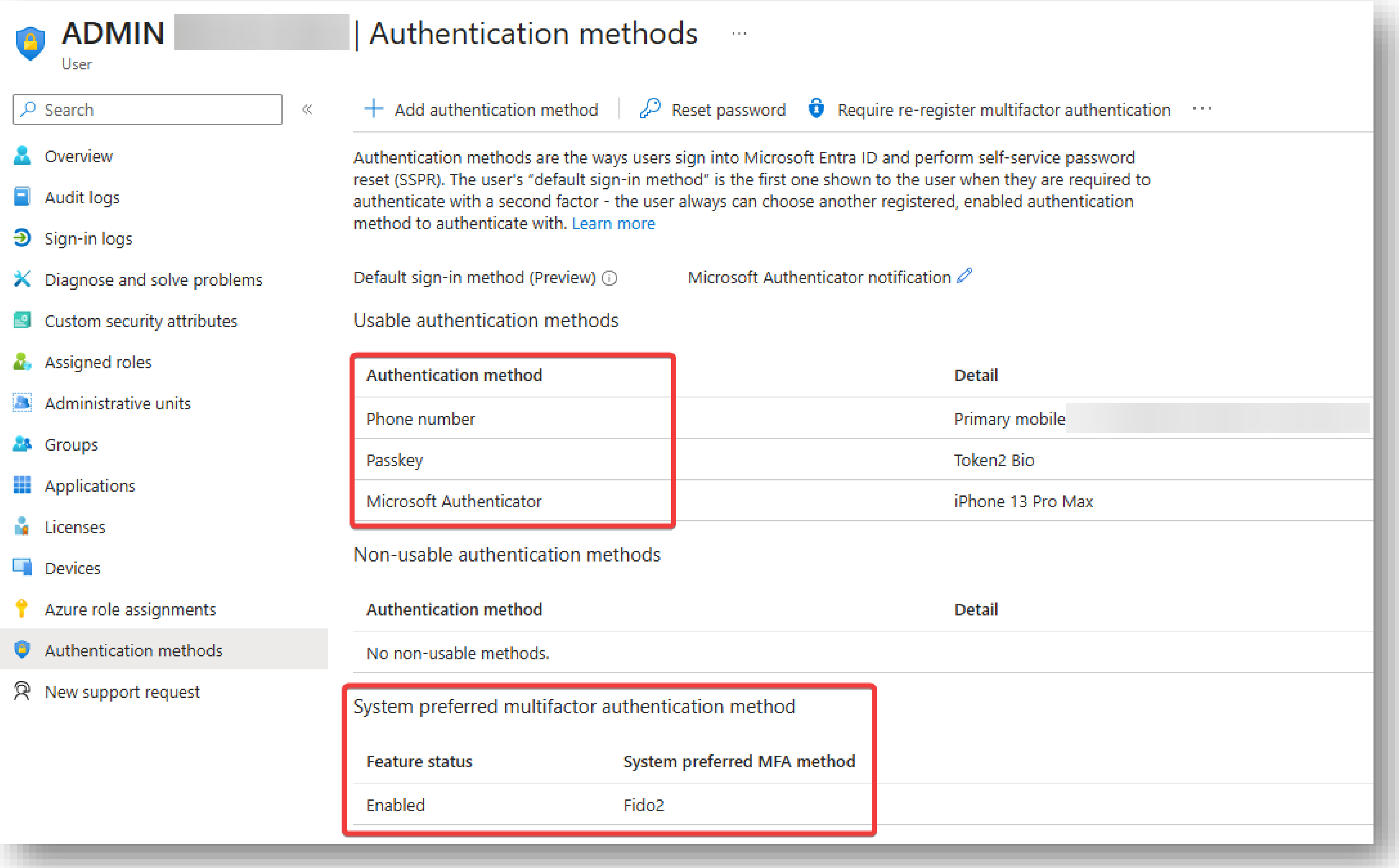
Name	Type	Use for sign-in
gs-aad-authn-sms-allowed	Group	☐

Insufficient protection for identities

Misconfiguration	Real-world-environment-distribution
Missing ID Protection Policies	8 out of 10 tenants have either the policies not active or enabled the policy in the legacy blade
Legacy MFA Trusted Location	6 out of 10 tenants have still legacy MFA trusted location active
Unsecured MFA Registration	8 out of 10 tenants don’t have secured the MFA registration process
Weak MFA allowed	7 out of 10 tenants still have weak MFA options.
Strong MFA not enforced	No figure(s) yet.

Strong MFA not enforced

“This account is secure because it uses FIDO2”



ADMIN [redacted] | Authentication methods ···

User

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) ⓘ Microsoft Authenticator notification

Usable authentication methods

Authentication method	Detail
Phone number	Primary mobile [redacted]
Passkey	Token2 Bio
Microsoft Authenticator	iPhone 13 Pro Max

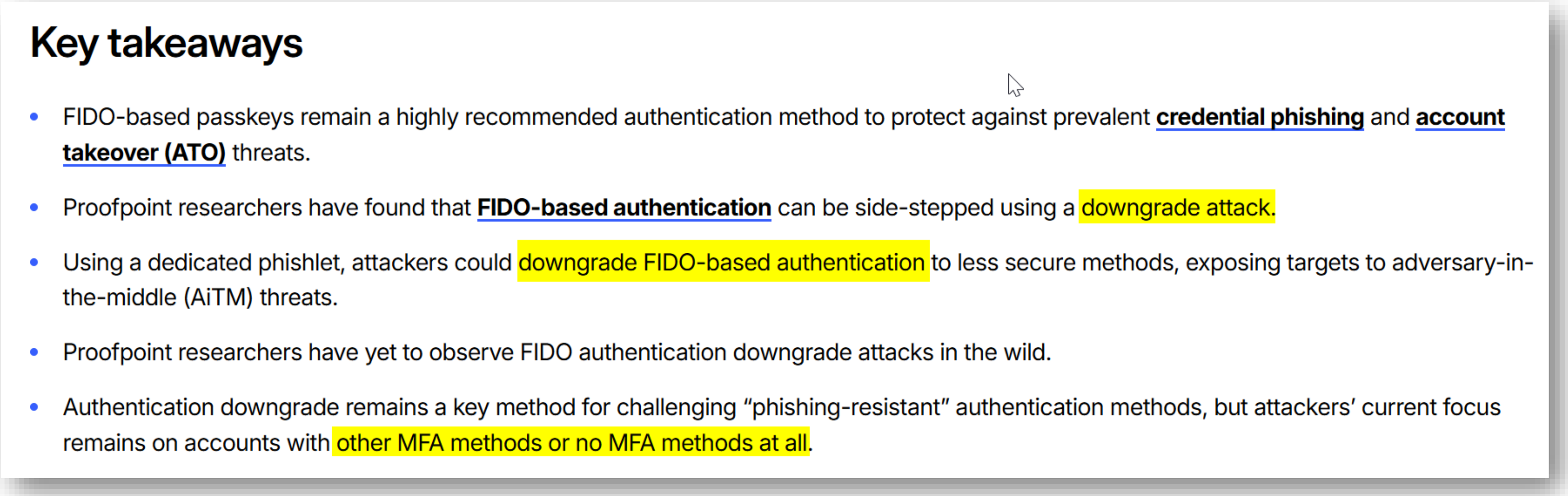
Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	Fido2

Why are insecure MFA methods a risk?



Key takeaways

- FIDO-based passkeys remain a highly recommended authentication method to protect against prevalent **credential phishing** and **account takeover (ATO)** threats.
- Proofpoint researchers have found that **FIDO-based authentication** can be side-stepped using a downgrade attack.
- Using a dedicated phishlet, attackers could downgrade FIDO-based authentication to less secure methods, exposing targets to adversary-in-the-middle (AiTM) threats.
- Proofpoint researchers have yet to observe FIDO authentication downgrade attacks in the wild.
- Authentication downgrade remains a key method for challenging “phishing-resistant” authentication methods, but attackers’ current focus remains on accounts with other MFA methods or no MFA methods at all.

Don’t Phish-let Me Down: FIDO Authentication Downgrade | Proofpoint US

Entra Authentication Methods Refresher

- Entra ID natively supports various Authentication Methods for user accounts.
- But only some meet state of the art capabilities, such as defined by NIST **AAL 3, making them phishing resistant**.

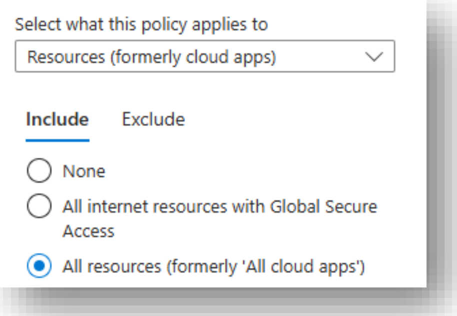
- Microsoft Authenticator & Authenticator Lite
- Windows Hello for Business
- Passkeys (Security Keys & Authenticator)
- QR code
- Certificate-based authentication
- Temporary Access Pass (TAP)
- OATH hardware token
- OATH software token
- SMS
- Voice call

- ~~Microsoft Authenticator & Authenticator Lite~~
- Windows Hello for Business
- Passkeys (Security Keys & Authenticator)
- ~~QR code~~
- Certificate-based authentication
- ~~Temporary Access Pass (TAP)~~
- ~~OATH hardware token~~
- ~~OATH software token~~
- ~~SMS~~
- ~~Voice call~~

Enforcing Strong MFA

www.wpninjas.eu
#WPNinjaS

Enforcing Strong MFA for Sign-In

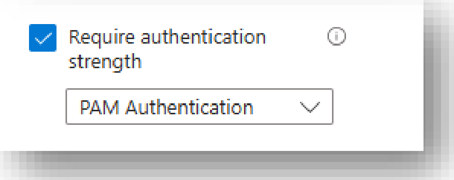


Select what this policy applies to

Resources (formerly cloud apps)

Include | Exclude

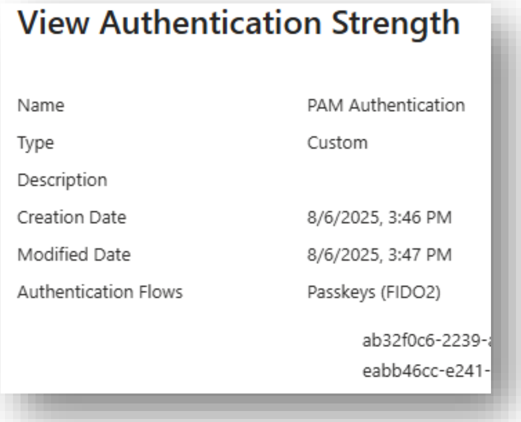
○ None
○ All internet resources with Global Secure Access
● All resources (formerly 'All cloud apps')



☑ Require authentication strength

PAM Authentication

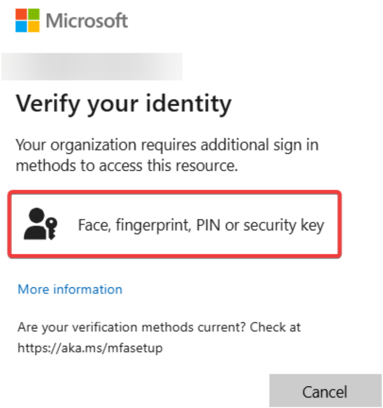
+



View Authentication Strength

Name	PAM Authentication
Type	Custom
Description	
Creation Date	8/6/2025, 3:46 PM
Modified Date	8/6/2025, 3:47 PM
Authentication Flows	Passkeys (FIDO2)
	ab32f0c6-2239- eabb46cc-e241-

=



Microsoft

Verify your identity

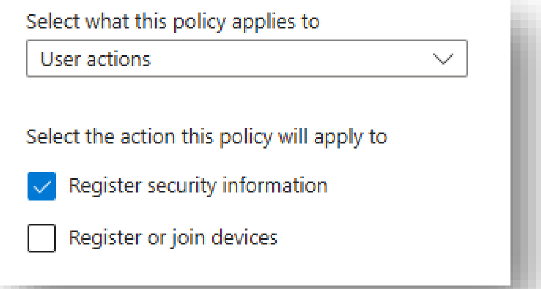
Your organization requires additional sign in methods to access this resource.

Face, fingerprint, PIN or security key

More information

Are your verification methods current? Check at https://aka.ms/mfasetup

Bootstrapping Strong MFA



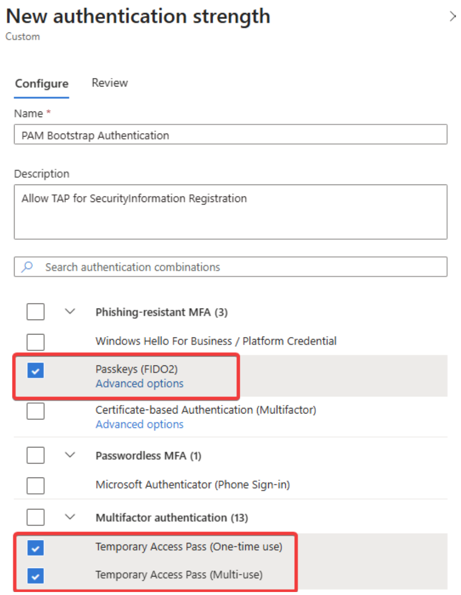
Select what this policy applies to

User actions

Select the action this policy will apply to

☑ Register security information
☐ Register or join devices

+



New authentication strength

Custom

Configure | Review

Name *

PAM Bootstrap Authentication

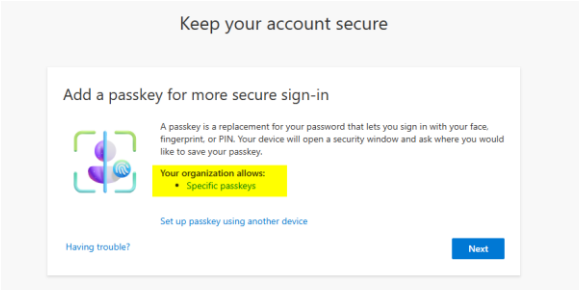
Description

Allow TAP for SecurityInformation Registration

Search authentication combinations

☐ Phishing-resistant MFA (3)
☐ Windows Hello For Business / Platform Credential
☑ Passkeys (FIDO2)
Advanced options
☐ Certificate-based Authentication (Multifactor)
Advanced options
☐ Passwordless MFA (1)
☐ Microsoft Authenticator (Phone Sign-in)
☐ Multifactor authentication (13)
☑ Temporary Access Pass (One-time use)
☑ Temporary Access Pass (Multi-use)

=



Keep your account secure

Add a passkey for more secure sign-in

A passkey is a replacement for your password that lets you sign in with your face, fingerprint, or PIN. Your device will open a security window and ask where you would like to save your passkey.

Your organization allows:
- Specific passkeys

Set up passkey using another device

Having trouble?

Insufficient protection for identities

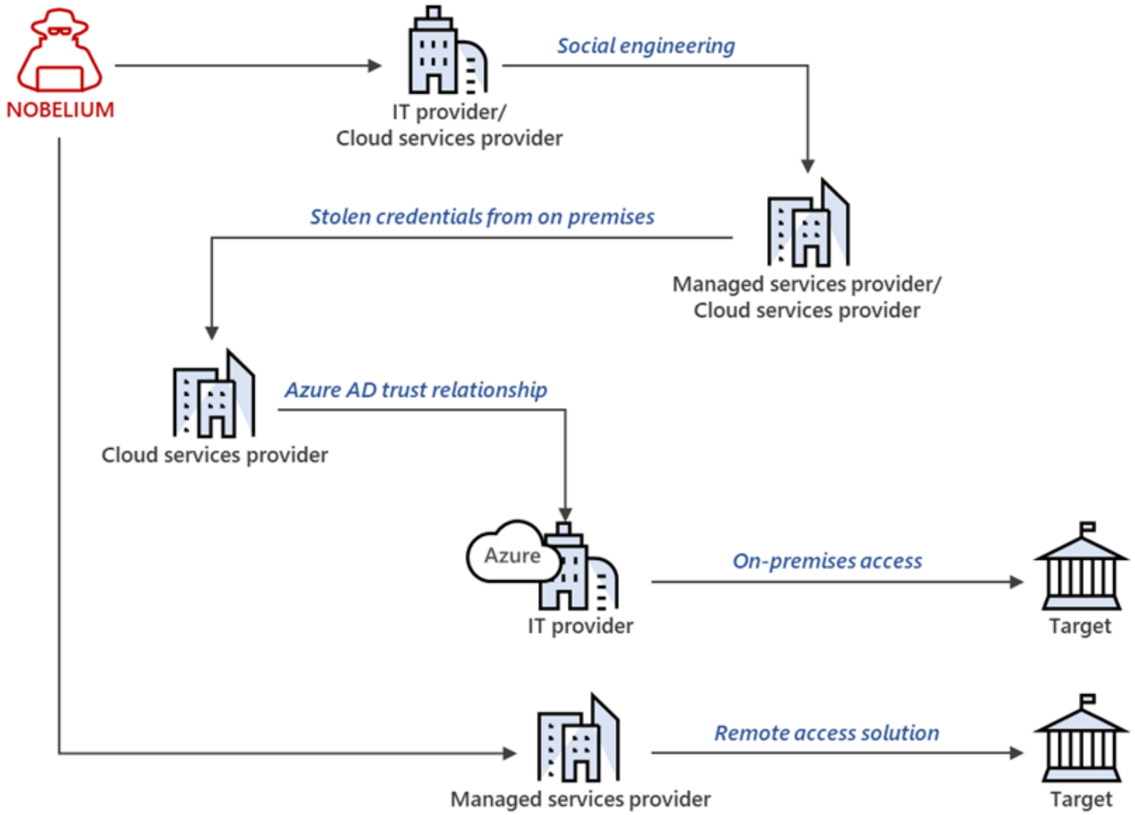
- **Missing ID Protection Policies**
  - Identity protection risk analysis workbook - Microsoft Entra ID | Microsoft Learn
  - Microsoft Entra ID Protection risk-based access policies - Microsoft Entra ID Protection | Microsoft Learn
- **Legacy MFA Trusted Location**
  - How to migrate to the Authentication methods policy - Microsoft Entra ID | Microsoft Learn
  - Configure Microsoft Entra multifactor authentication - Microsoft Entra ID | Microsoft Learn
- **Unsecured MFA Registration**
  - Control security information registration with Conditional Access - Microsoft Entra ID | Microsoft Learn
- **Weak MFA allowed**
  - Manage authentication methods - Microsoft Entra ID | Microsoft Learn
  - How to migrate to the Authentication methods policy - Microsoft Entra ID | Microsoft Learn
  - nathanmcnulty/Entra/operational-groups at main · nathanmcnulty/nathanmcnulty
- **Strong MFA not enforced**
  - Overview of Microsoft Entra authentication strength - Microsoft Entra ID | Microsoft Learn
  - Overview of how Microsoft Entra authentication strength works in a Conditional Access policy - Microsoft Entra ID | Microsoft Learn

Unsecured External User Access

Misconfiguration	Real-world-environment-distribution
Active GDAP / DAP access	5 out of 10 tenants have GDAP or DAP access configured.

Unsecured External User Access

Customers often delegate admin rights to service providers, granting them full control over their tenants just like internal admins, if a service provider is compromised, attackers can pivot into multiple customer tenants that trust the provider.


NOBELIUM
IT provider/ Cloud services provider
Social engineering
Managed services provider/ Cloud services provider
Stolen credentials from on premises
Cloud services provider
Azure AD trust relationship
Azure
IT provider
On-premises access
Target
Managed services provider
Remote access solution
Target

Delegated Admin Privileges (DAP)

- Grants full, persistent Global Admin access to customer tenants
- No scoping or time limits

Granular delegated admin privileges (GDAP)

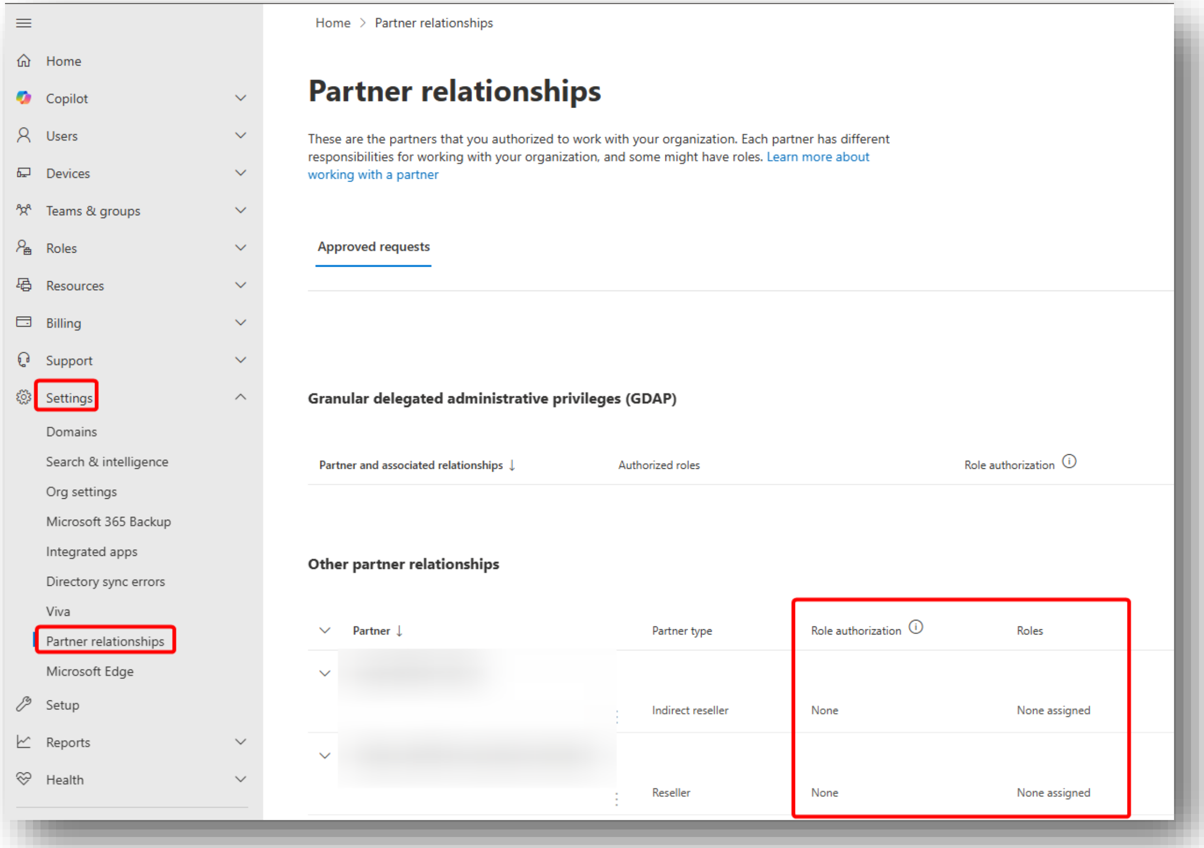
- Enables role-based, time-bound access to specific workloads (e.g., Exchange, Intune).
- Ability to assign roles on a specific scope

NOBELIUM targeting delegated administrative privileges to facilitate broader attacks | Microsoft Security Blog

Unsecured External User Access

www.wpninjas.eu
#WPNinjaS

Verify existing GDAP / DAP configuration and assigned roles via M365 Admin Center or PIM



Home > Partner relationships

Partner relationships

These are the partners that you authorized to work with your organization. Each partner has different responsibilities for working with your organization, and some might have roles. Learn more about working with a partner

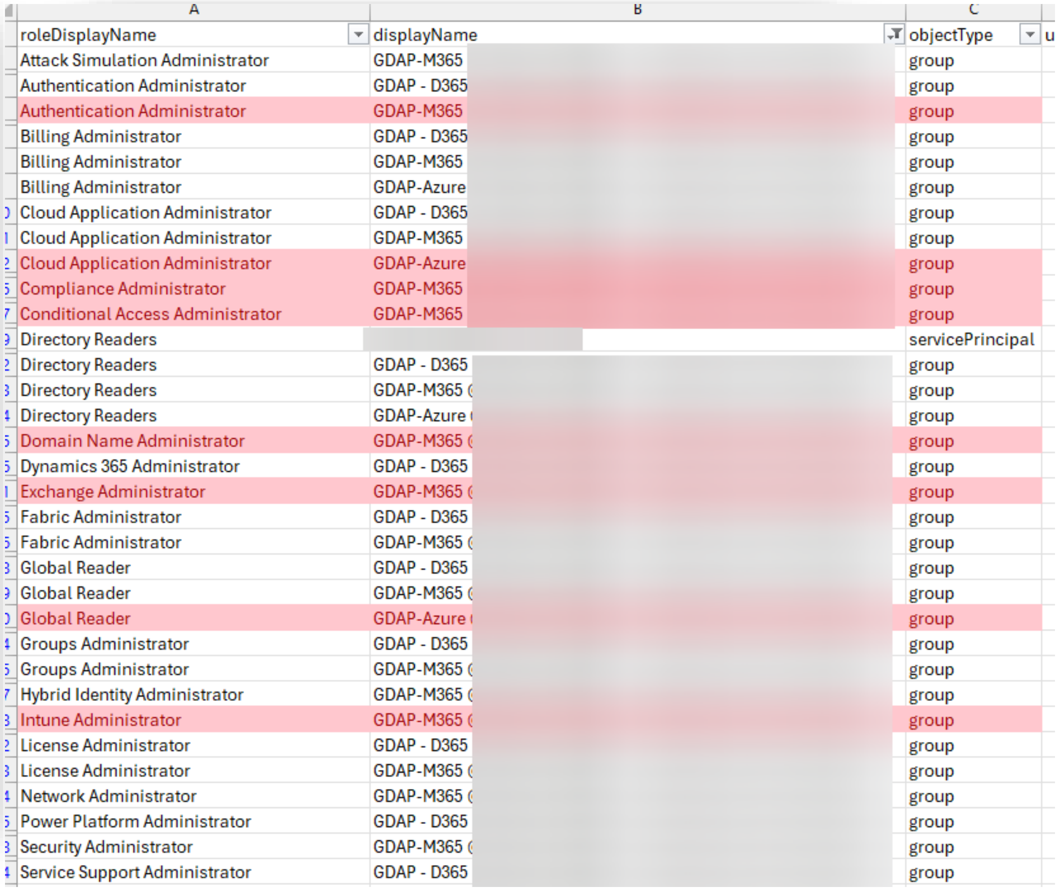
Approved requests

Granular delegated administrative privileges (GDAP)

Partner and associated relationships ↓	Authorized roles	Role authorization

Other partner relationships

Partner ↓	Partner type	Role authorization	Roles
[redacted]	Indirect reseller	None	None assigned
[redacted]	Reseller	None	None assigned



roleDisplayName	displayName	objectType
Attack Simulation Administrator	GDAP-M365 [redacted]	group
Authentication Administrator	GDAP - D365 [redacted]	group
Authentication Administrator	GDAP-M365 [redacted]	group
Billing Administrator	GDAP - D365 [redacted]	group
Billing Administrator	GDAP-M365 [redacted]	group
Billing Administrator	GDAP-Azure [redacted]	group
Cloud Application Administrator	GDAP - D365 [redacted]	group
Cloud Application Administrator	GDAP-M365 [redacted]	group
Cloud Application Administrator	GDAP-Azure [redacted]	group
Compliance Administrator	GDAP-M365 [redacted]	group
Conditional Access Administrator	GDAP-M365 [redacted]	group
Directory Readers	[redacted]	servicePrincipal
Directory Readers	GDAP - D365 [redacted]	group
Directory Readers	GDAP-M365 ([redacted]	group
Directory Readers	GDAP-Azure ([redacted]	group
Domain Name Administrator	GDAP-M365 ([redacted]	group
Dynamics 365 Administrator	GDAP - D365 [redacted]	group
Exchange Administrator	GDAP-M365 ([redacted]	group
Fabric Administrator	GDAP - D365 [redacted]	group
Fabric Administrator	GDAP-M365 ([redacted]	group
Global Reader	GDAP - D365 [redacted]	group
Global Reader	GDAP-M365 ([redacted]	group
Global Reader	GDAP-Azure ([redacted]	group
Groups Administrator	GDAP - D365 [redacted]	group
Groups Administrator	GDAP-M365 ([redacted]	group
Hybrid Identity Administrator	GDAP-M365 ([redacted]	group
Intune Administrator	GDAP-M365 ([redacted]	group
License Administrator	GDAP - D365 [redacted]	group
License Administrator	GDAP-M365 ([redacted]	group
Network Administrator	GDAP-M365 ([redacted]	group
Power Platform Administrator	GDAP - D365 [redacted]	group
Security Administrator	GDAP-M365 ([redacted]	group
Service Support Administrator	GDAP - D365 [redacted]	group

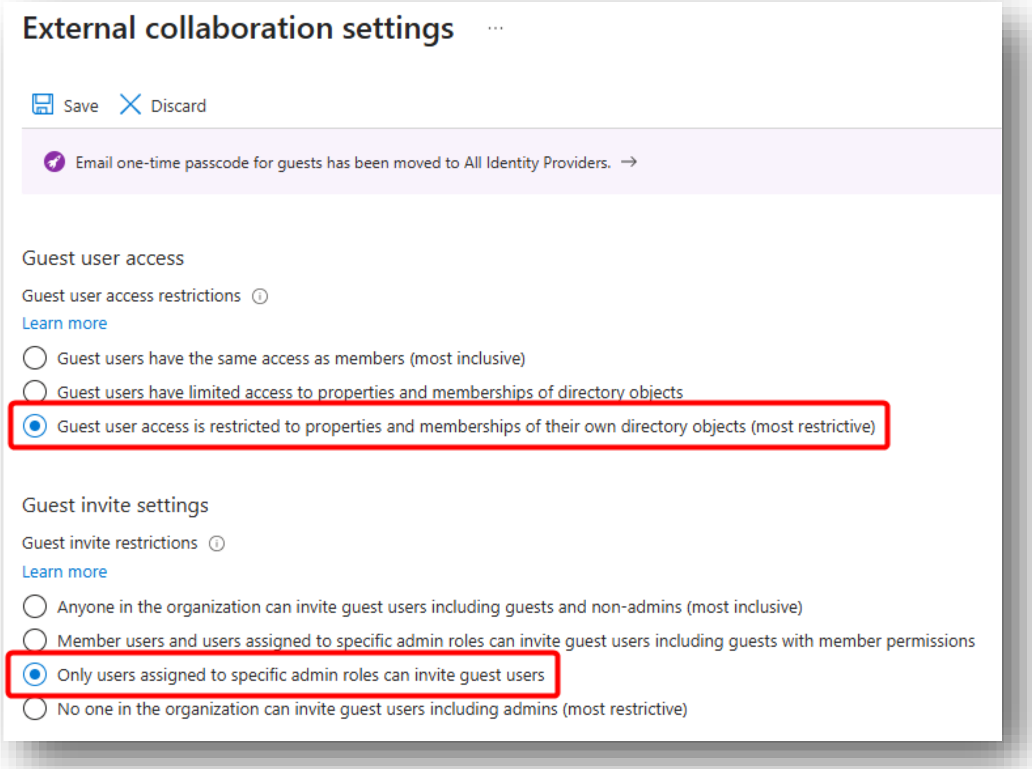
Unsecured External User Access

Misconfiguration	Real-world-environment-distribution
Active GDAP / DAP access	4 out of 10 tenants have GDAP or DAP access configured.
Guest user access not secured	8 out of 10 tenants have not secured their guest account access.

Unsecured External User Access

Protect Guest user access and invitation restrictions

- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive
    - With this setting, guests can access only their own profiles. Guests aren't allowed to see other users' profiles, groups, or group memberships
- Only users assigned to specific admin roles can invite guest users
    - To allow only those users with User Administrator or Guest Inviter roles to invite guests, select this radio button.
- Historical Guest Users and Orgs
    - Only allowlisted orgs
    - Block outbound to new orgs
    - Only allow inbound from selected orgs



External collaboration settings ···

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

Learn more

○ Guest users have the same access as members (most inclusive)

○ Guest users have limited access to properties and memberships of directory objects

● Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

○ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

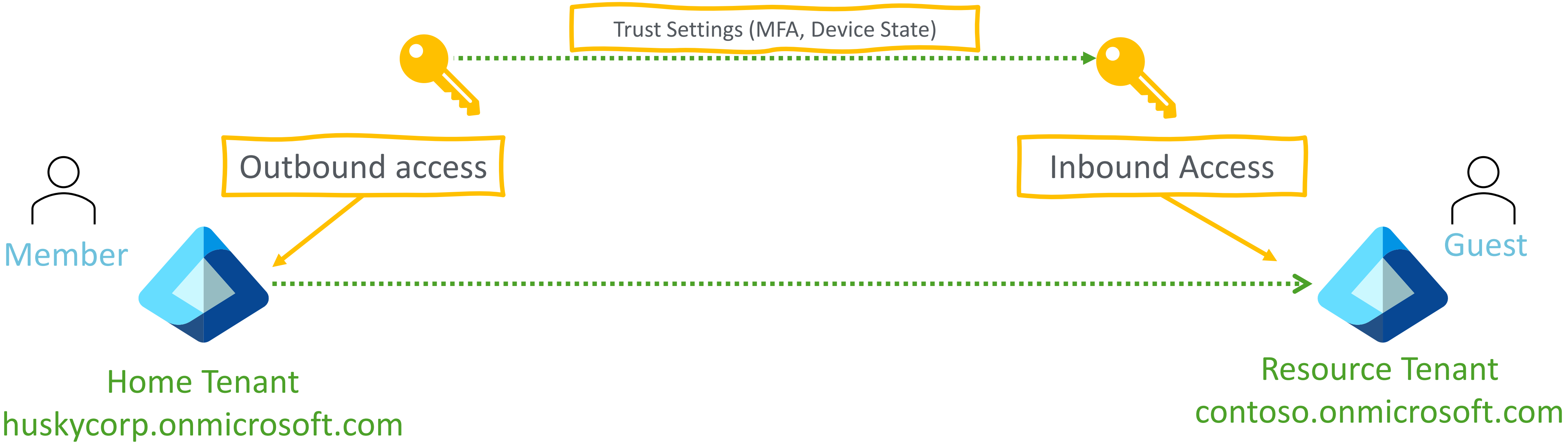
○ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

● Only users assigned to specific admin roles can invite guest users

○ No one in the organization can invite guest users including admins (most restrictive)

Unsecured External User Access

Cross-tenant access settings for guest user



Unsecured External User Access

- Configure Cross-Tenant access settings
- Configure Trust Settings for specific organizations
- Protect Guest Users Sign-Ins via Conditional Access

Unsecured External User Access

- **GDAP / DAP**
  - Microsoft-Led Transition From DAP to GDAP - Partner Center | Microsoft Learn
  - GDAP frequently asked questions - Partner Center | Microsoft Learn
- **Guest user access not secured**
  - Authentication and Conditional Access for B2B users | Azure Docs
  - Require MFA for guest users with Conditional Access - Microsoft Entra ID | Microsoft Learn
  - B2B guest user properties - Microsoft Entra External ID | Microsoft Learn
  - Restrict guest user access permissions - Microsoft Entra ID | Microsoft Learn

Incomplete XDR Deployments

Misconfiguration	Real-world-environment-distribution
Missing Defender for Identity Coverage	9 out of 10 have either not all services onboarded to MDI or have active health issues

Incomplete XDR Deployments

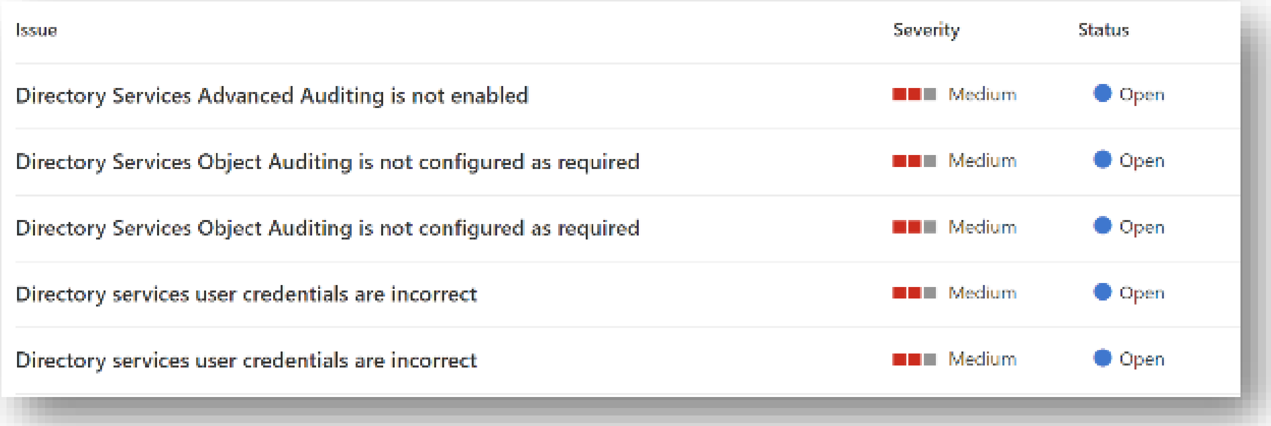
Missing Defender for Identity coverage can be through:

- MDI sensor is not installed on all supported roles
  - Domain Controller, Active Directory Certifies Services, Entra Connect Sync
- Health issues
  - The MDI sensor cannot start the service
  - Not all relevant events are generated and cannot be picked up by the MDI

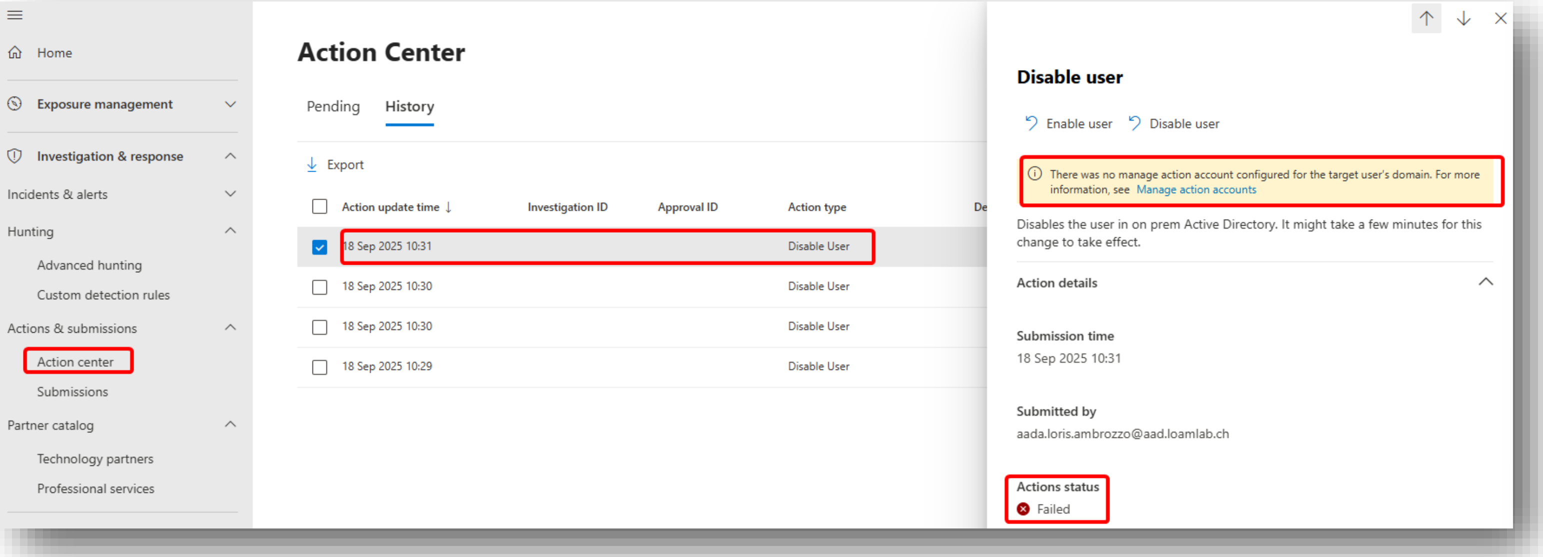
In both cases, it is possible that not all relevant data will be received by MDI and will therefore not be analysed.
This means that:

- Response actions are **unavailable** or only **partially available**.
- Not all MDI alerts can be triggered (based on missing data)

Incomplete XDR Deployments



Issue	Severity	Status
Directory Services Advanced Auditing is not enabled	Medium	● Open
Directory Services Object Auditing is not configured as required	Medium	● Open
Directory Services Object Auditing is not configured as required	Medium	● Open
Directory services user credentials are incorrect	Medium	● Open
Directory services user credentials are incorrect	Medium	● Open



Action Center

Pending History

Export

□	Action update time ↓	Investigation ID	Approval ID	Action type	De
☑	18 Sep 2025 10:31			Disable User	
□	18 Sep 2025 10:30			Disable User	
□	18 Sep 2025 10:30			Disable User	
□	18 Sep 2025 10:29			Disable User	

Disable user

Enable user   Disable user

There was no manage action account configured for the target user's domain. For more information, see Manage action accounts

Disables the user in on prem Active Directory. It might take a few minutes for this change to take effect.

Action details

Submission time
18 Sep 2025 10:31

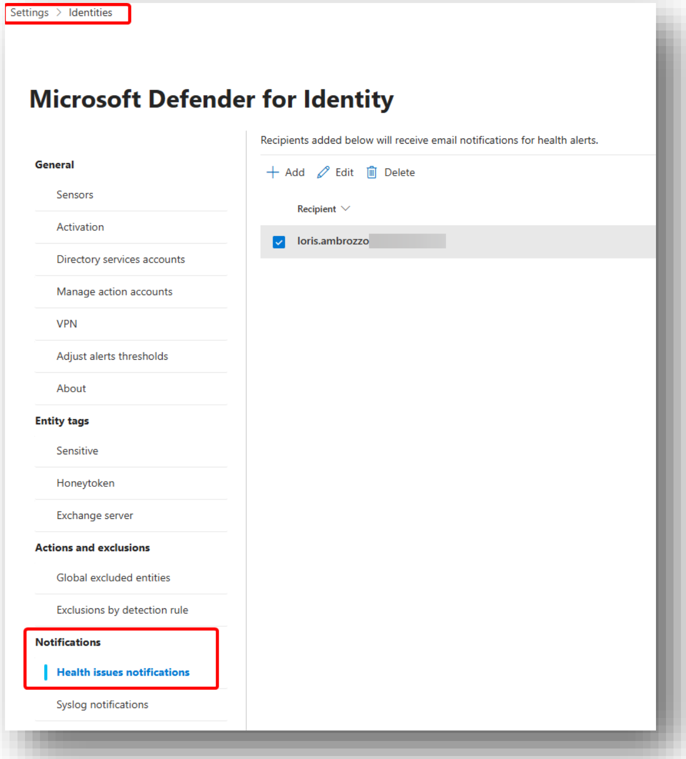
Submitted by
aada.loris.ambrozzo@aad.loamlab.ch

Actions status
☒ Failed

Incomplete XDR Deployments

Health issues via E-Mail

- Set up a health issue notification via E-Mail to be notified as soon as a new health issue appears



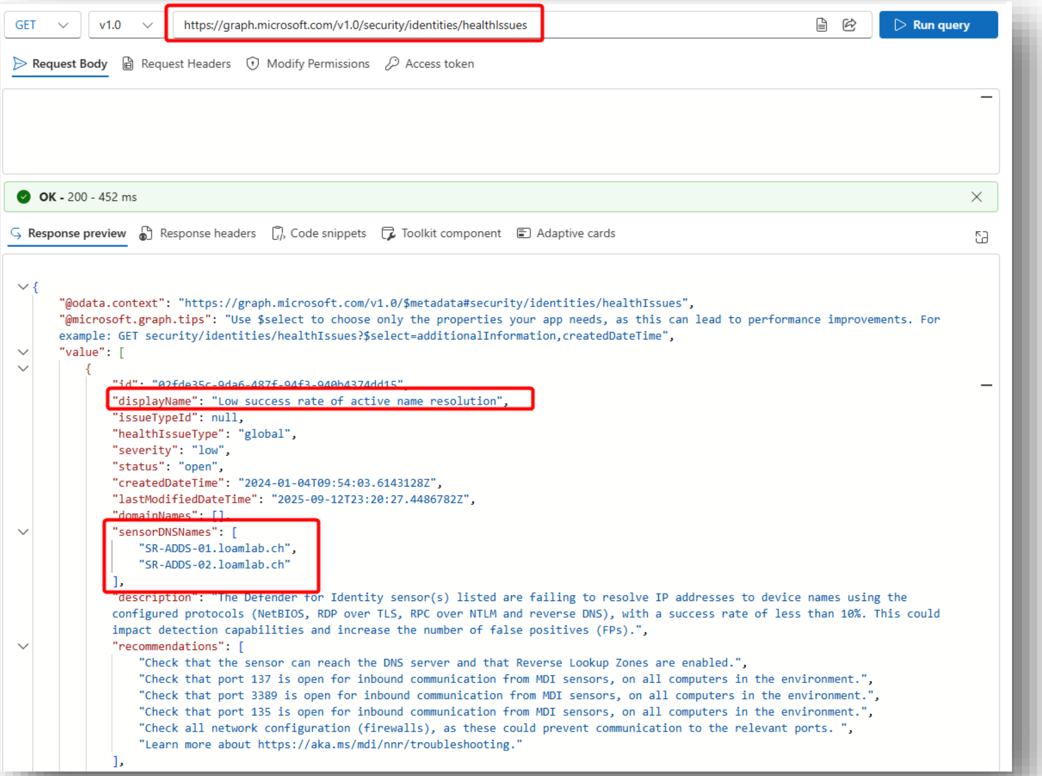
Microsoft Defender for Identity

Recipients added below will receive email notifications for health alerts.

☑ loris.ambrozzo[redacted]

Health issues via API-Call

- Query Graph-API to request Health Issues



https://graph.microsoft.com/v1.0/security/identities/healthIssues

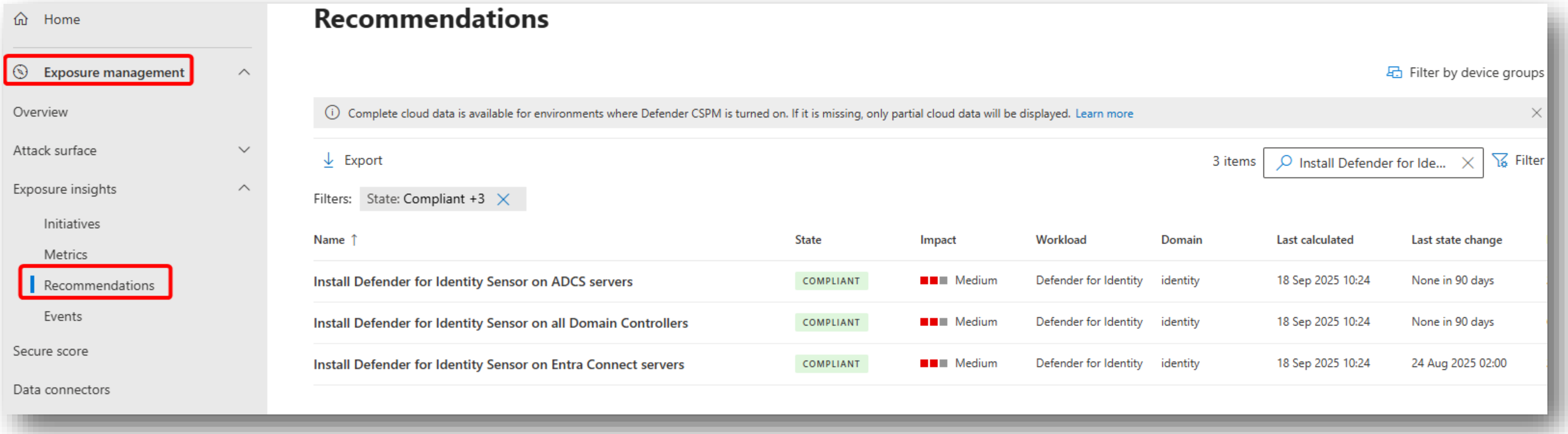
OK - 200 - 452 ms

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#security/identities/healthIssues",
  "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For
  example: GET security/identities/healthIssues?$select=additionalInformation,createdDateTime",
  "value": [
    {
      "id": "02fde35c-9da6-487f-94f3-940b4374dd15",
      "displayName": "Low success rate of active name resolution",
      "issueTypeId": null,
      "healthIssueType": "global",
      "severity": "low",
      "status": "open",
      "createdDateTime": "2024-01-04T09:54:03.6143128Z",
      "lastModifiedDateTime": "2025-09-12T23:20:27.4486782Z",
      "domainNames": [],
      "sensorDNSNames": [
        "SR-ADDS-01.loamlab.ch",
        "SR-ADDS-02.loamlab.ch"
      ],
      "description": "The Defender for Identity sensor(s) listed are failing to resolve IP addresses to device names using the
      configured protocols (NetBIOS, RDP over TLS, RPC over NTLM and reverse DNS), with a success rate of less than 10%. This could
      impact detection capabilities and increase the number of false positives (FPs).",
      "recommendations": [
        "Check that the sensor can reach the DNS server and that Reverse Lookup Zones are enabled.",
        "Check that port 137 is open for inbound communication from MDI sensors, on all computers in the environment.",
        "Check that port 3389 is open for inbound communication from MDI sensors, on all computers in the environment.",
        "Check that port 135 is open for inbound communication from MDI sensors, on all computers in the environment.",
        "Check all network configuration (firewalls), as these could prevent communication to the relevant ports. ",
        "Learn more about https://aka.ms/mdi/nnr/troubleshooting."
      ],
```

Incomplete XDR Deployments

MDI sensor is not installed on servers

- Review Recommendation in Exposure Management
  - *Install Defender for Identity Sensor on all Domain Controllers*
  - *Install Defender for Identity Sensor on ADCS servers*
  - *Install Defender for Identity Sensor on Entra Connect servers*



Recommendations

Complete cloud data is available for environments where Defender CSPM is turned on. If it is missing, only partial cloud data will be displayed. Learn more

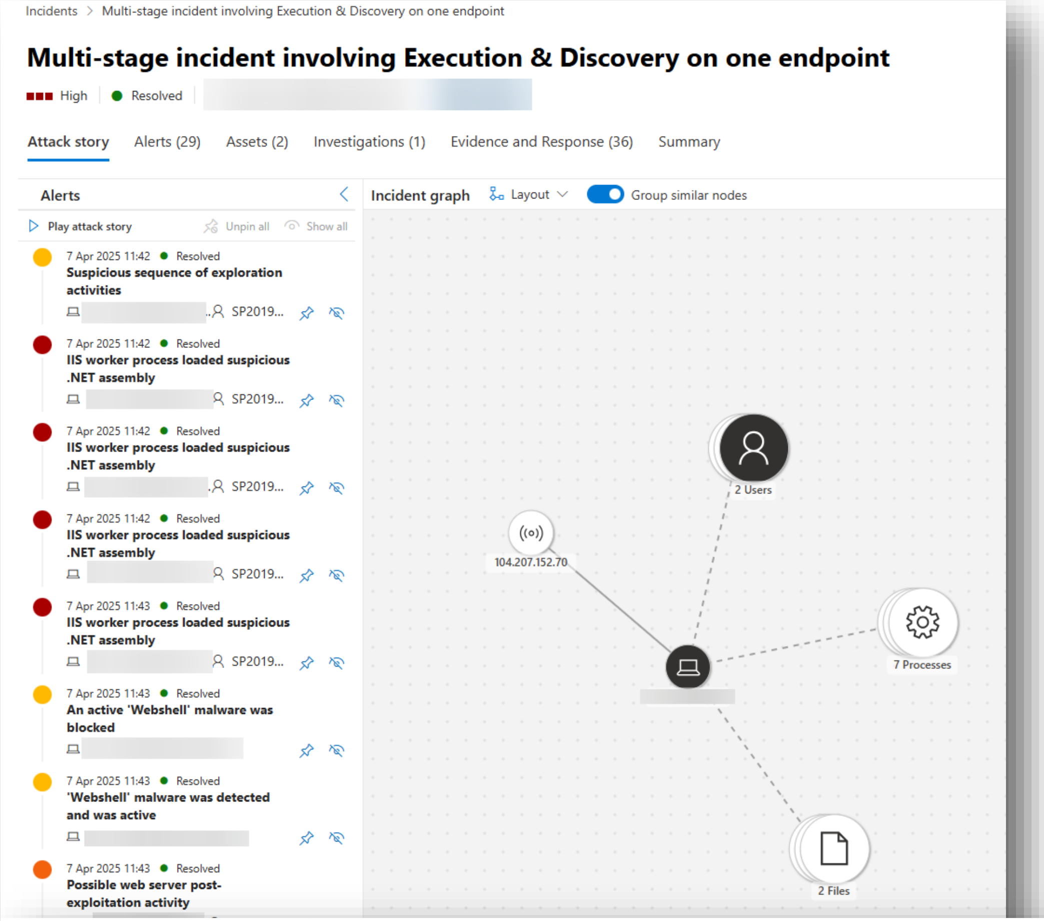
Filters: State: Compliant +3

Name ↑	State	Impact	Workload	Domain	Last calculated	Last state change
Install Defender for Identity Sensor on ADCS servers	COMPLIANT	■■■ Medium	Defender for Identity	identity	18 Sep 2025 10:24	None in 90 days
Install Defender for Identity Sensor on all Domain Controllers	COMPLIANT	■■■ Medium	Defender for Identity	identity	18 Sep 2025 10:24	None in 90 days
Install Defender for Identity Sensor on Entra Connect servers	COMPLIANT	■■■ Medium	Defender for Identity	identity	18 Sep 2025 10:24	24 Aug 2025 02:00

Incomplete XDR Deployments

Misconfiguration	Real-world-environment-distribution
Missing Defender for Identity Coverage	9 out of 10 have either not all services onboarded to MDI or have active health issues
Missing MDE configuration or missing MDE coverage	7 out of 10 have either missing MDE configuration or missing MDE coverage

Incomplete XDR Deployments



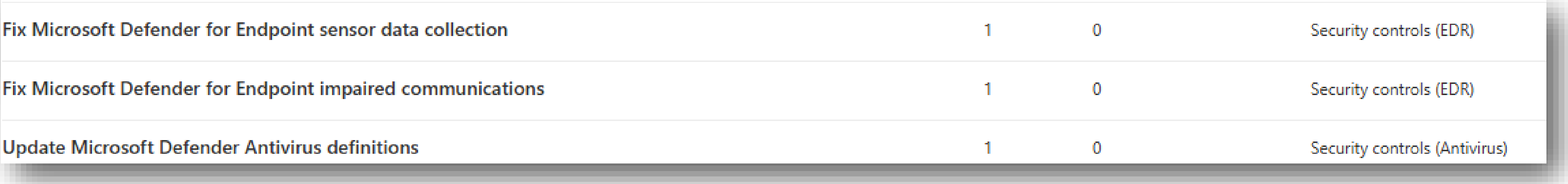
Incidents > Multi-stage incident involving Execution & Discovery on one endpoint

Multi-stage incident involving Execution & Discovery on one endpoint

■■■ High | ● Resolved | [redacted]

- 7 Apr 2025 11:42 ● Resolved
  Suspicious sequence of exploration activities
  [redacted] SP2019...
- 7 Apr 2025 11:42 ● Resolved
  IIS worker process loaded suspicious .NET assembly
  [redacted] SP2019...
- 7 Apr 2025 11:42 ● Resolved
  IIS worker process loaded suspicious .NET assembly
  [redacted] SP2019...
- 7 Apr 2025 11:42 ● Resolved
  IIS worker process loaded suspicious .NET assembly
  [redacted] SP2019...
- 7 Apr 2025 11:43 ● Resolved
  IIS worker process loaded suspicious .NET assembly
  [redacted] SP2019...
- 7 Apr 2025 11:43 ● Resolved
  An active 'Webshell' malware was blocked
  [redacted]
- 7 Apr 2025 11:43 ● Resolved
  'Webshell' malware was detected and was active
  [redacted]
- 7 Apr 2025 11:43 ● Resolved
  Possible web server post-exploitation activity

[redacted]



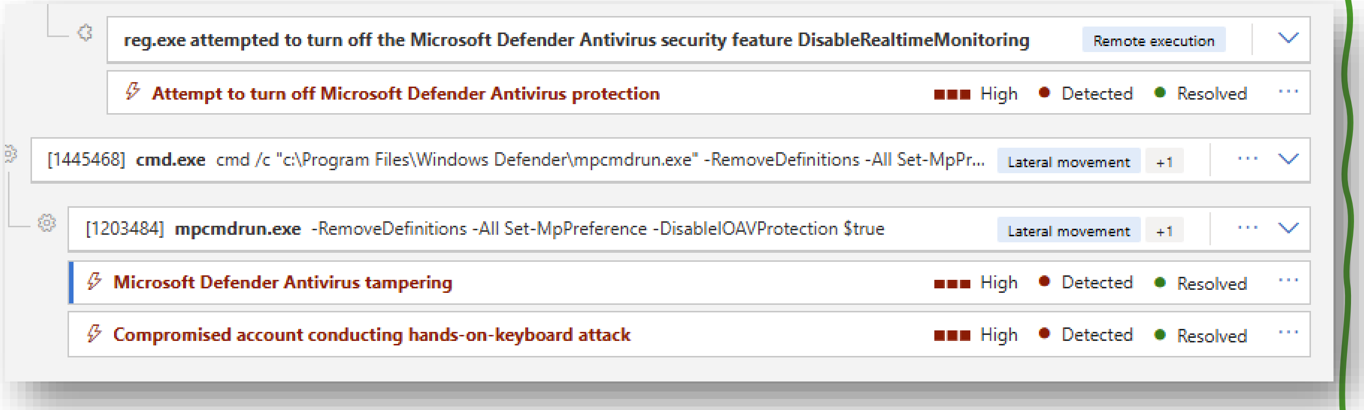
Fix Microsoft Defender for Endpoint sensor data collection	1	0	Security controls (EDR)
Fix Microsoft Defender for Endpoint impaired communications	1	0	Security controls (EDR)
Update Microsoft Defender Antivirus definitions	1	0	Security controls (Antivirus)

Incomplete XDR Deployments

What means incomplete in the area of MDE?

- Each incomplete configuration means that the Defender for Endpoint cannot protect the endpoints.
- These misconfigurations are exactly what an attacker will exploit.

MDE – Tamper Protection



reg.exe attempted to turn off the Microsoft Defender Antivirus security feature DisableRealtimeMonitoring — Remote execution

Attempt to turn off Microsoft Defender Antivirus protection — High · Detected · Resolved

[1445468] **cmd.exe** cmd /c "c:\Program Files\Windows Defender\mpcmdrun.exe" -RemoveDefinitions -All Set-MpPr... — Lateral movement +1

[1203484] **mpcmdrun.exe** -RemoveDefinitions -All Set-MpPreference -DisableIOAVProtection $true — Lateral movement +1

Microsoft Defender Antivirus tampering — High · Detected · Resolved

Compromised account conducting hands-on-keyboard attack — High · Detected · Resolved

Outdated Sense Binaries

MDE Coverage (Platforms)

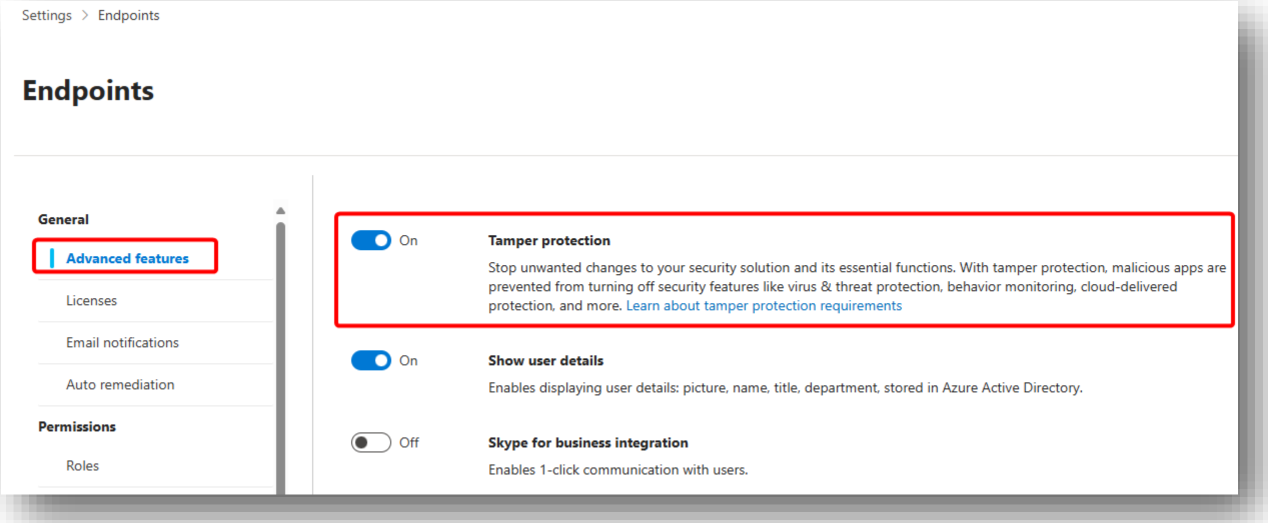
MDE communication blocked

MDE features not enabled

Incomplete XDR Deployments

www.wpninjas.eu
#WPNinjaS

Check that Tamper Protection is tenant wide enabled



Settings > Endpoints

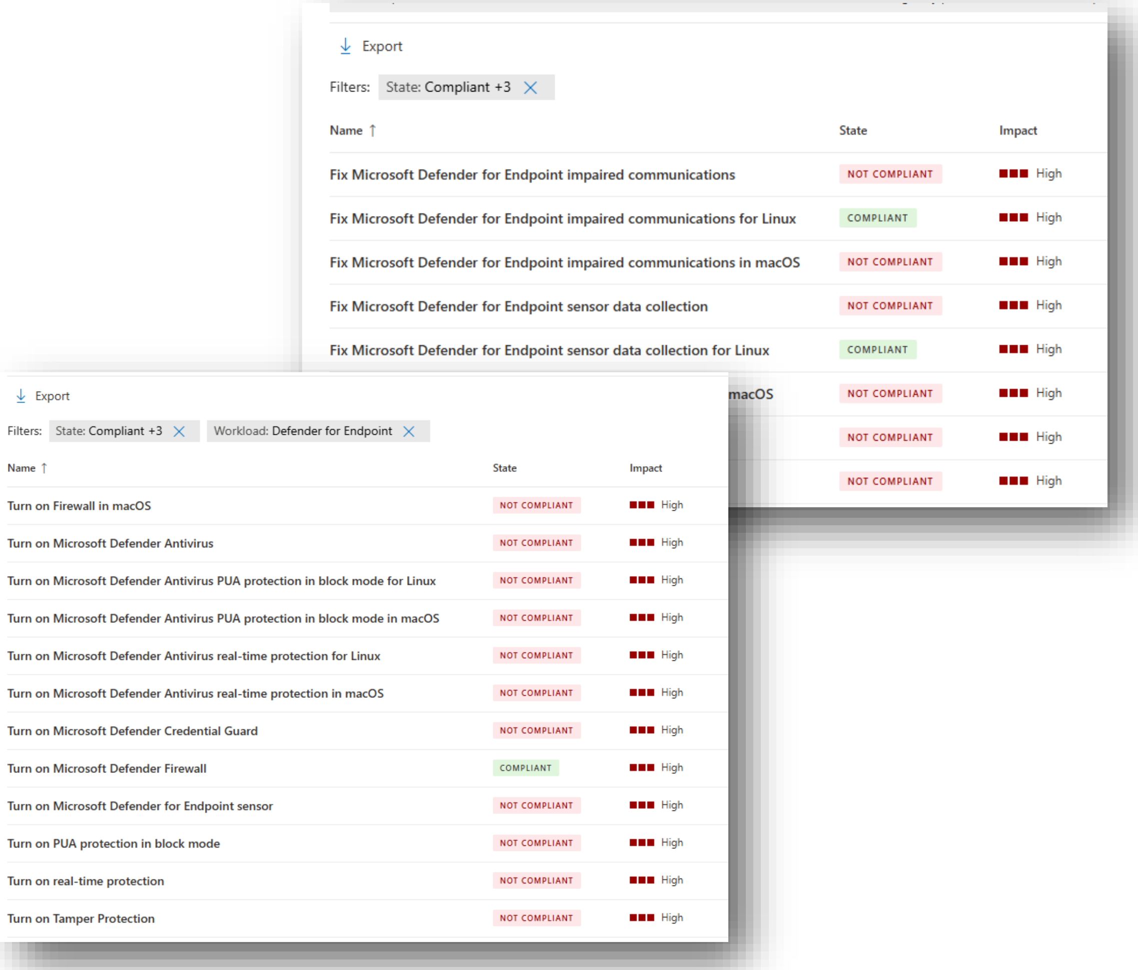
Endpoints

On — **Tamper protection**
Stop unwanted changes to your security solution and its essential functions. With tamper protection, malicious apps are prevented from turning off security features like virus & threat protection, behavior monitoring, cloud-delivered protection, and more. Learn about tamper protection requirements

On — **Show user details**
Enables displaying user details: picture, name, title, department, stored in Azure Active Directory.

Off — **Skype for business integration**
Enables 1-click communication with users.

Check MDE Coverage



Filters: State: Compliant +3

Name ↑	State	Impact
Fix Microsoft Defender for Endpoint impaired communications	NOT COMPLIANT	■■■ High
Fix Microsoft Defender for Endpoint impaired communications for Linux	COMPLIANT	■■■ High
Fix Microsoft Defender for Endpoint impaired communications in macOS	NOT COMPLIANT	■■■ High
Fix Microsoft Defender for Endpoint sensor data collection	NOT COMPLIANT	■■■ High
Fix Microsoft Defender for Endpoint sensor data collection for Linux	COMPLIANT	■■■ High
macOS	NOT COMPLIANT	■■■ High
	NOT COMPLIANT	■■■ High
	NOT COMPLIANT	■■■ High

Filters: State: Compliant +3 Workload: Defender for Endpoint

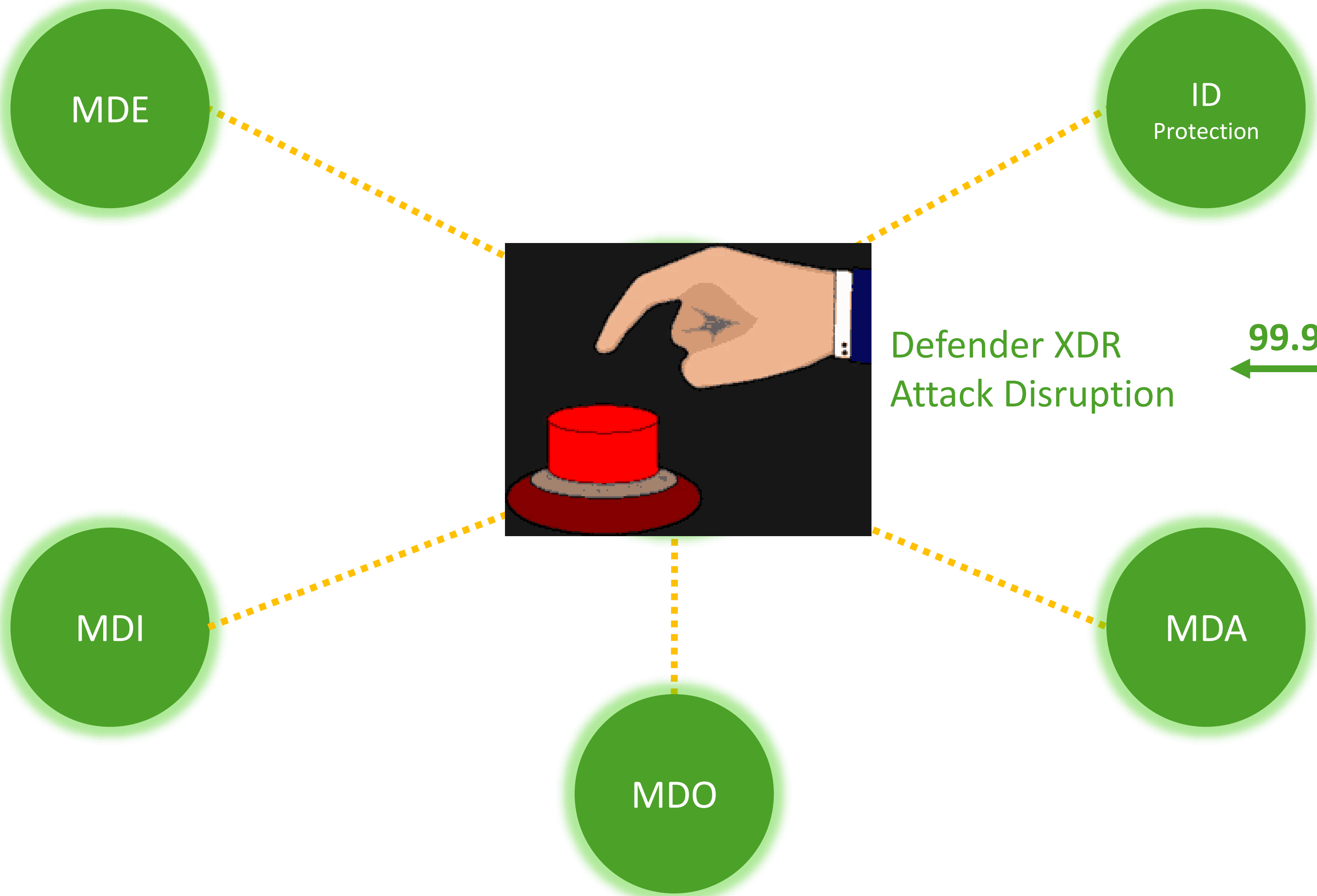
Name ↑	State	Impact
Turn on Firewall in macOS	NOT COMPLIANT	■■■ High
Turn on Microsoft Defender Antivirus	NOT COMPLIANT	■■■ High
Turn on Microsoft Defender Antivirus PUA protection in block mode for Linux	NOT COMPLIANT	■■■ High
Turn on Microsoft Defender Antivirus PUA protection in block mode in macOS	NOT COMPLIANT	■■■ High
Turn on Microsoft Defender Antivirus real-time protection for Linux	NOT COMPLIANT	■■■ High
Turn on Microsoft Defender Antivirus real-time protection in macOS	NOT COMPLIANT	■■■ High
Turn on Microsoft Defender Credential Guard	NOT COMPLIANT	■■■ High
Turn on Microsoft Defender Firewall	COMPLIANT	■■■ High
Turn on Microsoft Defender for Endpoint sensor	NOT COMPLIANT	■■■ High
Turn on PUA protection in block mode	NOT COMPLIANT	■■■ High
Turn on real-time protection	NOT COMPLIANT	■■■ High
Turn on Tamper Protection	NOT COMPLIANT	■■■ High

Incomplete XDR Deployments

Misconfiguration	Real-world-environment-distribution
Missing Defender for Identity Coverage	8 out of 10 tenants have either not all services onboarded to MDI or have active health issues
Missing MDE configuration	5 out of 10 tenants have either missing MDE configuration
Attack Disruption prerequisites not in place	8 out 10 tenants have not all Attack disruption prerequisites not in place

How does a complete XDR deployment help us?

Defender XDR Automatic Attack Disruption

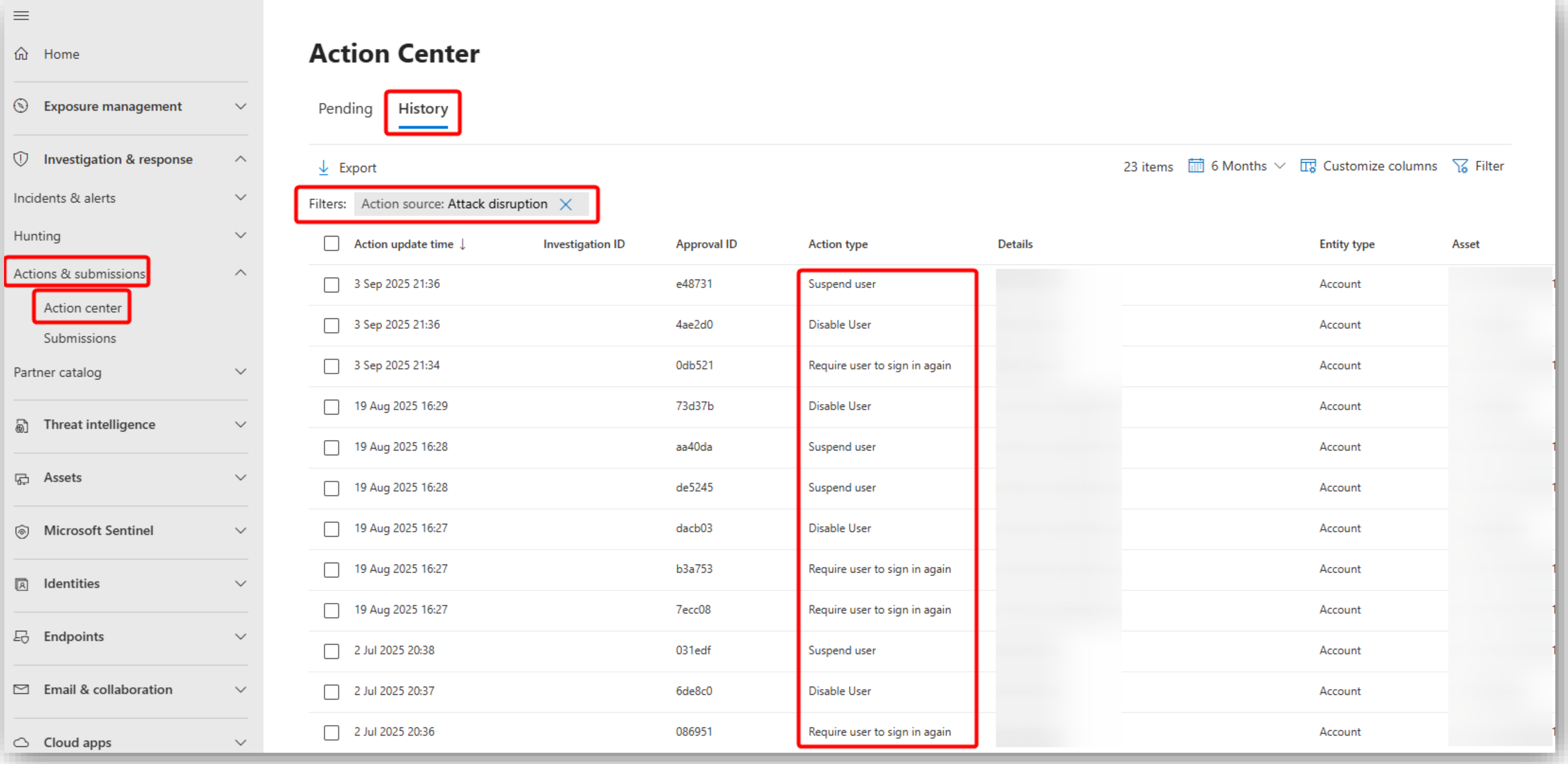


Defender XDR
Attack Disruption

99.9% Confidence

Incomplete XDR Deployments

www.wpninjas.eu
#WPNinjaS



Action Center

Pending | **History**

Export

23 items | 6 Months | Customize columns | Filter

Filters: Action source: Attack disruption

☐	Action update time ↓	Investigation ID	Approval ID	Action type	Details	Entity type	Asset
☐	3 Sep 2025 21:36		e48731	Suspend user	[redacted]	Account	[redacted]
☐	3 Sep 2025 21:36		4ae2d0	Disable User	[redacted]	Account	[redacted]
☐	3 Sep 2025 21:34		0db521	Require user to sign in again	[redacted]	Account	[redacted]
☐	19 Aug 2025 16:29		73d37b	Disable User	[redacted]	Account	[redacted]
☐	19 Aug 2025 16:28		aa40da	Suspend user	[redacted]	Account	[redacted]
☐	19 Aug 2025 16:28		de5245	Suspend user	[redacted]	Account	[redacted]
☐	19 Aug 2025 16:27		dacb03	Disable User	[redacted]	Account	[redacted]
☐	19 Aug 2025 16:27		b3a753	Require user to sign in again	[redacted]	Account	[redacted]
☐	19 Aug 2025 16:27		7ecc08	Require user to sign in again	[redacted]	Account	[redacted]
☐	2 Jul 2025 20:38		031edf	Suspend user	[redacted]	Account	[redacted]
☐	2 Jul 2025 20:37		6de8c0	Disable User	[redacted]	Account	[redacted]
☐	2 Jul 2025 20:36		086951	Require user to sign in again	[redacted]	Account	[redacted]

Incomplete XDR Deployments

Attack Disruption Prerequisites

- **Defender for Endpoint**
  - Device discovery settings must be activated to "Standard Discovery" at a minimum
  - The Minimum Sense Agent version required for the Contain User action to work is v10.8470
  - Remediation Level must be set to 'Semi Approval required for non-temporary folders' at a minimum (Full - remediate threats automatically is recommended)
- **Defender for Identity**
  - The Defender for Identity sensor needs to be deployed on the domain controller where the Active Directory account is to be turned off. In case of a dedicated action account, Defender for Identity needs to have the required permissions to disable the user account.
  - If you have automation in place to activate or block a user, check if the automation can interfere with disruption.
- **Microsoft Defender for Cloud Apps**
  - Microsoft Defender for Cloud Apps must be connected to Microsoft Office 365 through the connector.
  - App Governance must be turned on.
- **Microsoft Defender for Office 365**
  - Mailboxes are required to be hosted in Exchange Online.
  - Mailbox audit logging needs to audit at least: MailItemsAccessed, UpdateInboxRules, MoveToDeletedItems, SoftDelete, HardDelete
  - Safelinks policy needs to be present

Demo Incomplete XDR Deployments

- Review Remediation Level
- Review Exclusions Identities and IP’s
- Review Microsoft Defender for Cloud Apps Microsoft Office 365 connector
- Review App Governance enablement

Incomplete XDR Deployments

- **Missing Defender for Identity Coverage**
  - Microsoft Defender for Identity health issues - Microsoft Defender for Identity | Microsoft Learn
  - Introducing the new Defender for Identity Health Alert API | Microsoft Community Hub
- **Missing MDE configuration**
  - Protect security settings with tamper protection - Microsoft Defender for Endpoint | Microsoft Learn
  - Manage tamper protection for your organization using Microsoft Defender XDR - Microsoft Defender for Endpoint | Microsoft Learn
  - Configure your network environment to ensure connectivity with Defender for Endpoint service - Microsoft Defender for Endpoint | Microsoft Learn
- **Attack Disruption prerequisites not in place**
  - Configure automatic attack disruption in Microsoft Defender XDR - Microsoft Defender XDR | Microsoft Learn

Closing

Summary of the findings

Insufficient protection for identities 1/2

Misconfiguration	Exploitation	Mitigation
Missing ID Protection Policies	- Without Identity Protection, sign-ins from risky locations, with anonymous IP addresses or using compromised credentials are not automatically blocked or challenged.	- Deploy Sign-In Risk and User-Risk Policy via Conditional Access to protect users.
Legacy MFA Trusted Location	- All sign-ins from these addresses are excluded from MFA. - Most customers have excluded IP ranges, e.g. /24 ranges because a few users are not able to do MFA - This means that password spray attacks are possible from these IP addresses.	- Use exclusion with caution and only for a limited set of users. - Migrate exclusion to named locations.
Unsecured MFA Registration	- With no additional security for an MFA registration an attacker has an easy way to remove existing MFA method and registers own MFA method. - The attacker has then persistent access, even e.g. if the password is changed (e.g. with SSPR enabled)	- Deploy a CA policy that targets the register security information user action. - Consider a MFA registration and sign-in process that supports this protection for all relevant use cases (new hires, external users, corporate users).

Summary of the findings

Insufficient protection for identities 2/2

Misconfiguration	Exploitation	Mitigation
Weak MFA allowed	Weak MFA options are not phishing resistant and are suptible to multiple attacks such as sim-swapping, spoofing and malware on authenticators.	Fadeout weak authentication methods via authentication methods policy.
Strong MFA not enforced	Adversaries have a simple option to perform MFA downgrade attacks, by overriding or spoofing a user-agent which does not support current webauthn and CTAP protocols, used by passkeys.	Either disable weak authentication methods via policy and/or enforce authentication strengths via Conditional Access.

Summary of the findings

Unsecured External User Access

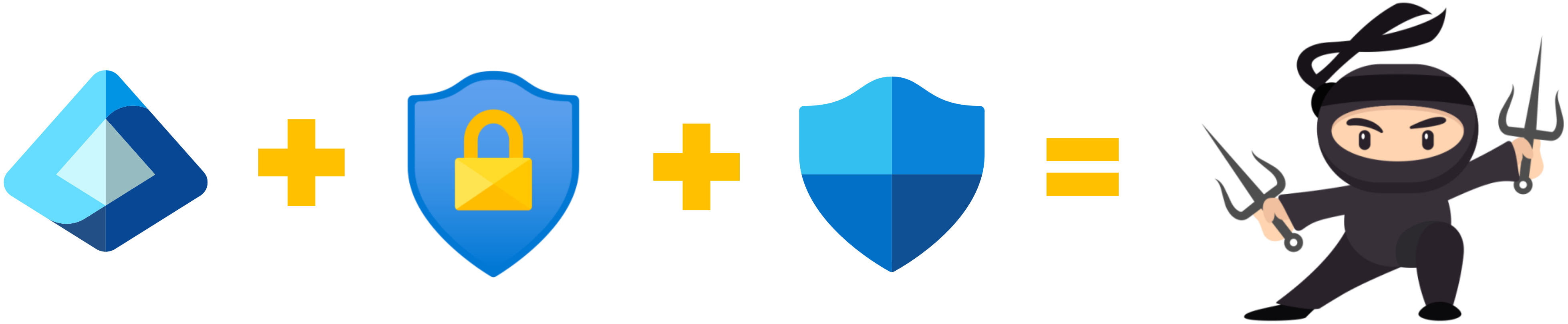
Misconfiguration	Exploitation	Mitigation
Active GDAP / DAP access	• If the CSP tenant is compromised, the attacker will also have direct access to all customer tenants within the CSP who have the appropriate permissions • When a DAP / GDAP relationship is established, the customer tenant sees only the CSP organization as having delegated access. • However, the customer does not see which individual users from the CSP tenant are accessing their environment or when a user was added to access the customer tenant	• Mange external accounts by ourselves • Invite Guest-Accounts (consider Conditional Access and Cross-tenant access settings) • Create dedicated administrative Accounts for the partner. • Assign roles PIM to enforce the principle of Zero-Trust
Guest user access not secured	• If guest user access is not secured, it can lead to either no additional security being enforced, or that to much is trusted for external organizations (e.g. Compliant Device) • Guest users also need protection, not just internal users. We have security measures in place for guest users that are not under our control, such as managed devices.	• Enforce Conditional Access for Guest Users • Review Guest User Restrictions • Review Cross-Tenant Settings and Trust Settings for MFA and Compliant devices

Summary of the findings

Incomplete XDR Deployments

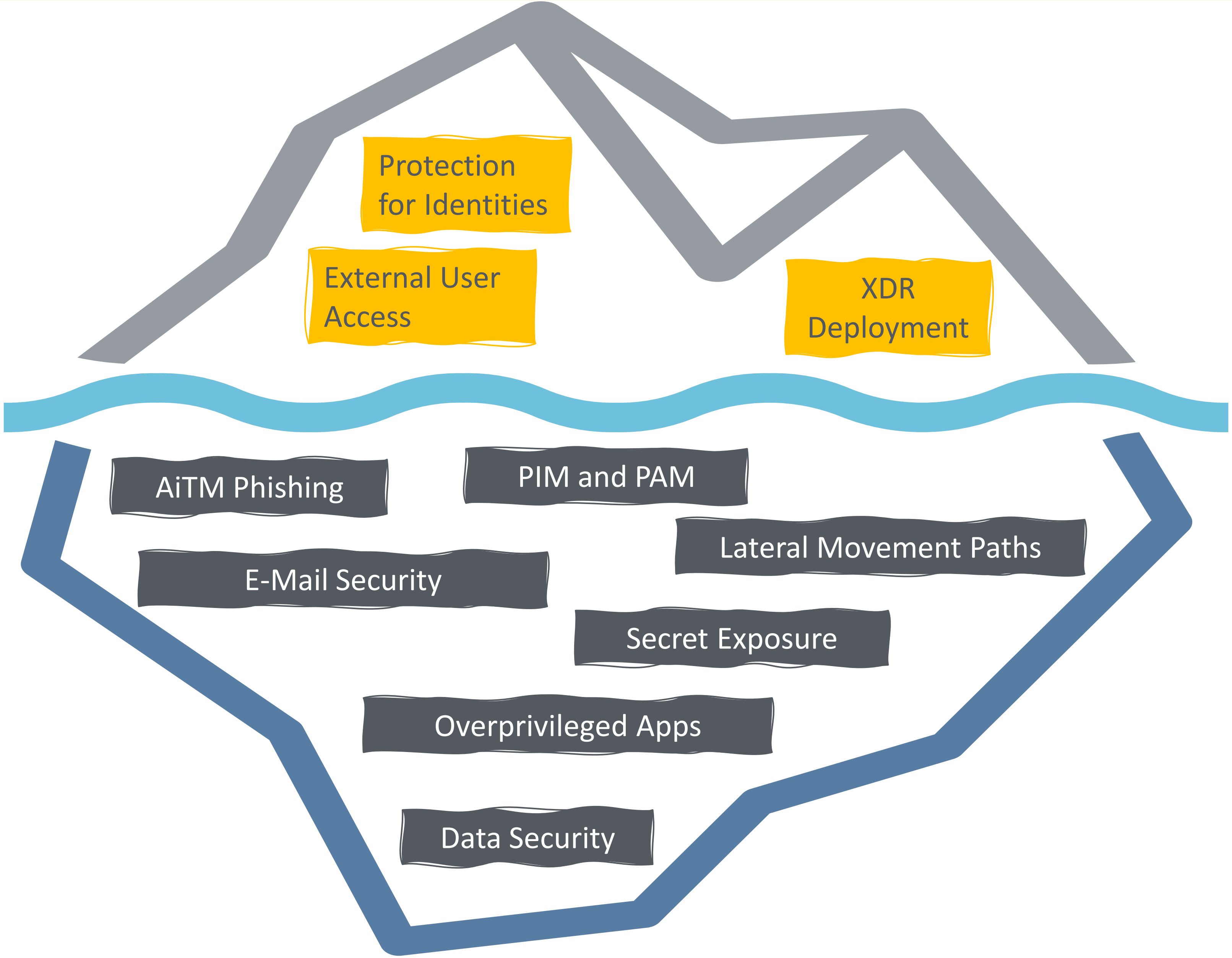
Misconfiguration	Exploitation	Mitigation
Missing Defender for Identity Coverage	• Gaps in coverage or unhealthy XDR workloads can impair the capabilities of defenders in terms of telemetry and response. • Meanwhile, attackers can exploit various tactics and techniques while going undetected or only being partially detected.	• Resolve health issues and review recommendations within exposure management. • Adopt new sensors and capabilities in your environment.
Missing MDE configuration		
Attack Disruption prerequisites not in place	• Microsoft Defender XDR includes powerful, automated attack disruption capabilities to protect your environment from sophisticated, high-impact attacks. • However, if not all prerequisites are in place for each product, automatic attack disruption cannot remediate the attack automatically. • Attackers can exploit this lack of automated remediation.	• Ensure prerequisites for Automatic Attack Disruption are in place

Summary



- Missing ID Protection Policies
- Legacy MFA Trusted Location
- Unsecured MFA Registration
- Weak MFA allowed
- Strong MFA not enforced
- Active GDAP / DAP access
- Guest user access not secured
- Missing Defender for Identity Coverage
- Missing MDE configuration
- Attack Disruption prerequisites not in place

What we didn’t talk about



Protection for Identities

External User Access

XDR Deployment

AiTM Phishing

PIM and PAM

Lateral Movement Paths

E-Mail Security

Secret Exposure

Overprivileged Apps

Data Security

Thank you Sponsors

www.wpninjas.eu
#WPNinjaS

Diamond Sponsor

Microsoft

Platinum Sponsors

2Pint

PATCH MY PC

RECAST SOFTWARE

glueck kanja

Gold Sponsors

nerdio

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

Rimo3

SOFTWARE CENTRAL

eido

EPIC FUSION
BRING IT ALL TOGETHER

Silver Sponsors

APENTO

PROACT

controlup

UMB creating time®

water
IT Security & Defense

We love Feedback

https://wpninjas25.sched.com/

😀 **Great Session!**

😐 **Okay Session!**

🙁 **Not so okay Session!**

Thank You