THAILAND Cyber Security

Microsoft Security

Cloud

SECURITY

Intensive

4 Identity

Entra

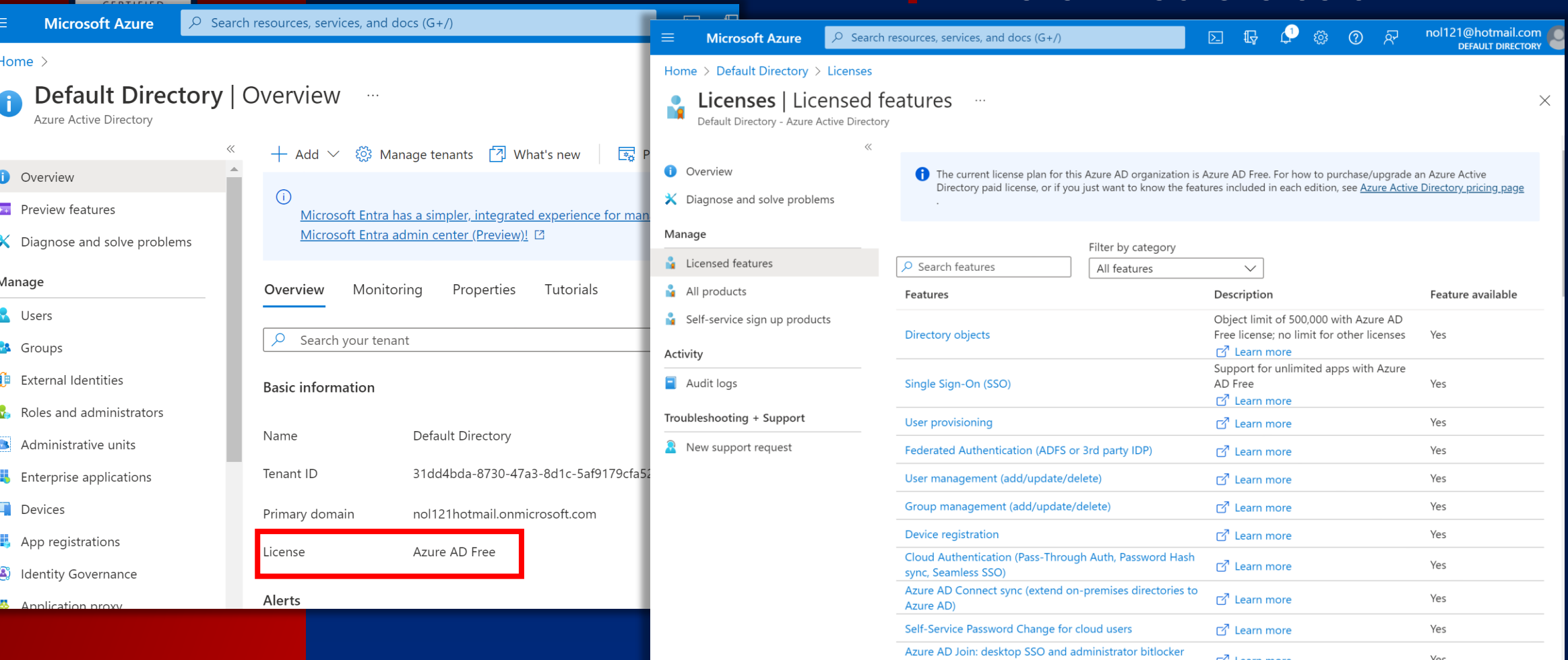
Intune

SC-900

SECURITY
COMPLIANCE
IDENTITY

Azure AD Licenses

- Free/O365/P1/P2
- Different feature sets



ure AD Join: desktop SSO and administrator ocker recovery	Learn more	Yes
ssword Protection (global banned password)	Learn more	Yes
ltifactor authentication for administrator es	Learn more	Yes
sic security and usage reports	Learn more	Yes
ure AD features for guest users	Learn more	Yes
mpany branding (customization of logon d logout pages, access panel)	Learn more	Try Azure AD Premium Available in Azure AD for Office 365 / Azure AD Premium P1 / Azure AD Premium P2
ltifactor authentication (phone and sms)	Learn more	Try Azure AD Premium Available in Azure AD for Office 365 / Azure AD Premium P1 / Azure AD Premium P2
oup access management	Learn more	Try Azure AD Premium Available in Azure AD for Office 365 / Azure AD Premium P1 / Azure AD Premium P2
rvice Level Agreement (SLA)	Learn more	Try Azure AD Premium Available in Azure AD for Office 365 / Azure AD Premium P1 / Azure AD Premium P2
vice write-back (device objects two-way chronization between on-premises ectories and Azure)	Learn more	Try Azure AD Premium Available in Azure AD for Office 365 / Azure AD Premium P1 / Azure AD Premium P2
Password Protection (custom banned password)	Learn more	Available in Azure AD Premium P1 / Azure AD Premium P2
Password Protection for Windows Server Active Directory (global and custom banned password)	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2
Self-service password reset, change, unlock with on-premises write-back	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2
Azure AD Join: MDM auto enrollment and local admin policy customization	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2
Azure AD Join: self-service bitlocker recovery, enterprise state roaming	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2
Advanced security and usage reports	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2
Application Proxy	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2
Connect Health	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2

SC-900

SECURITY
COMPLIANCE
IDENTITY

Azure AD Licenses

- Free/O365/P1/P2
- Different feature sets

Advanced Group Access Management (dynamic groups, group creation permission delegation, group naming policy, group expiration, usage guidelines, default classification)	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2
Conditional Access	Learn more	Try Azure AD Premium Available in Azure AD Premium P1 / Azure AD Premium P2
Identity Protection	Learn more	Try Azure AD Premium Available in Azure AD Premium P2
Privileged Identity Management (PIM)	Learn more	Try Azure AD Premium Available in Azure AD Premium P2
Access Reviews	Learn more	Try Azure AD Premium Available in Azure AD Premium P2
Entitlement management	Learn more	Try Azure AD Premium Available in Azure AD Premium P2

THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

https://admin.microsoft.com/#/catalog

Microsoft 365 admin center

Search

Home
Users
Billing
Purchase services
Your products
Licenses
Bills & payments
Billing accounts
Payment methods
Billing notifications
Setup
Show all

Search results: 17 products

azure ad

Some Azure security and identity products are available in Purchase services. Additional Azure services are available through the Azure website or your Microsoft partner. Learn more about flexible purchasing options for Azure

Security and identity

Security comes standard in all Microsoft products and technologies. No matter the size of your organization, use these practical resources to get secure today and protect against threats in the future.

Azure Active Directory Premium P2 Managed Trial

Azure Active Directory Premium P2: A comprehensive cloud Identity and access management solution with advanced identity protection for all your users and administrators

Trial

Details Compare

Azure Active Directory Premium P1

A robust set of capabilities to empower organizations with more demanding needs on identity and access management.

From $6.00 licenses/month

Details Compare

Azure Information Protection Premium P1

Helps classify, label and protect confidential documents and emails persistently. Access to information can also be controlled by specifying permissions on shared data. It's simple to use an...

From $2.00 licenses/month

Details Compare

Azure Active Directory Premium P2

Azure Active Directory Premium P2: A comprehensive cloud Identity and access management solution with advanced identity protection for all your users and administrators

From $9.00 licenses/month

Details Compare

THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

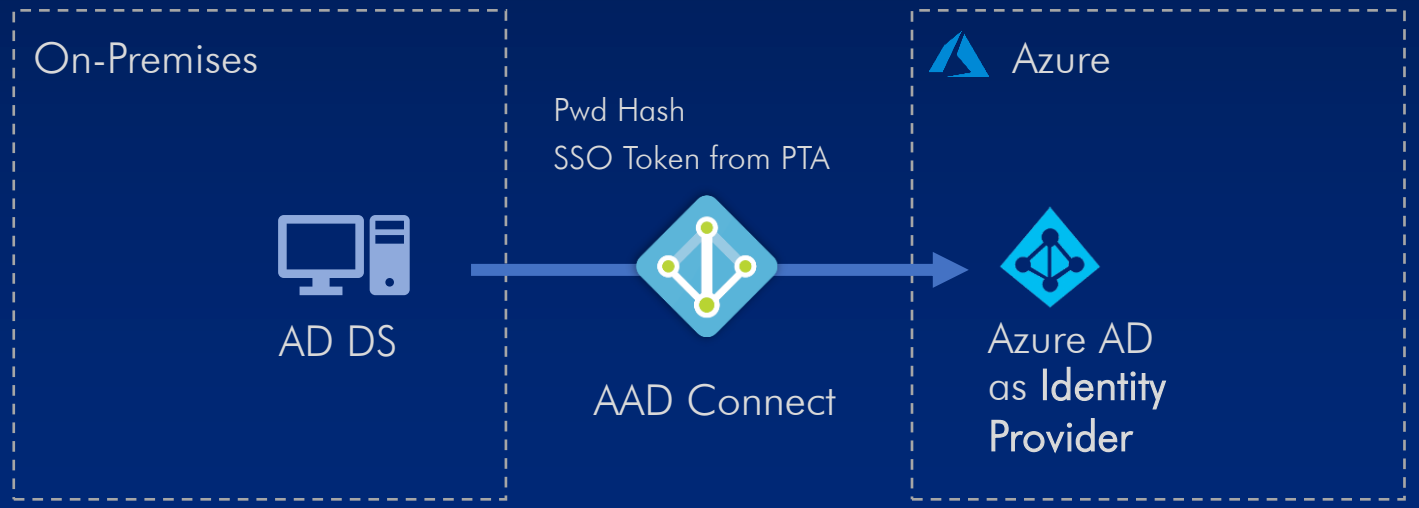
Hybrid

On-Premises + Cloud

= AD DS + AAD

use Azure AD Connect sync

No need for any M365 service to sync Hybrid Identity



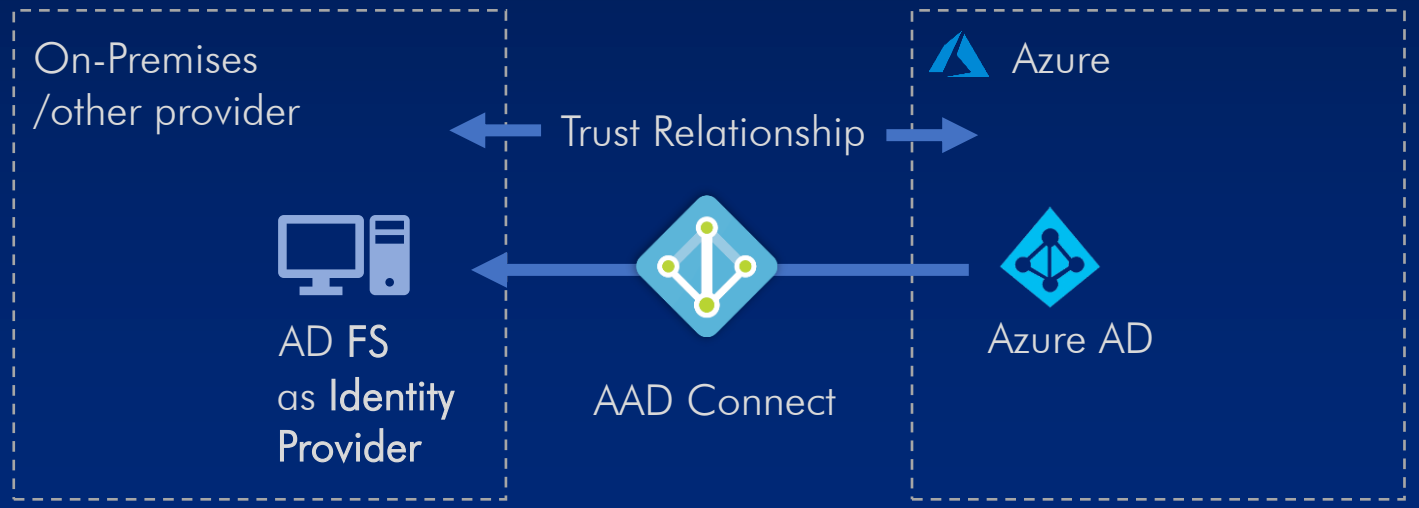
THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

Federation

- Trust Relationship
- AD FS etc. as Identity Provider



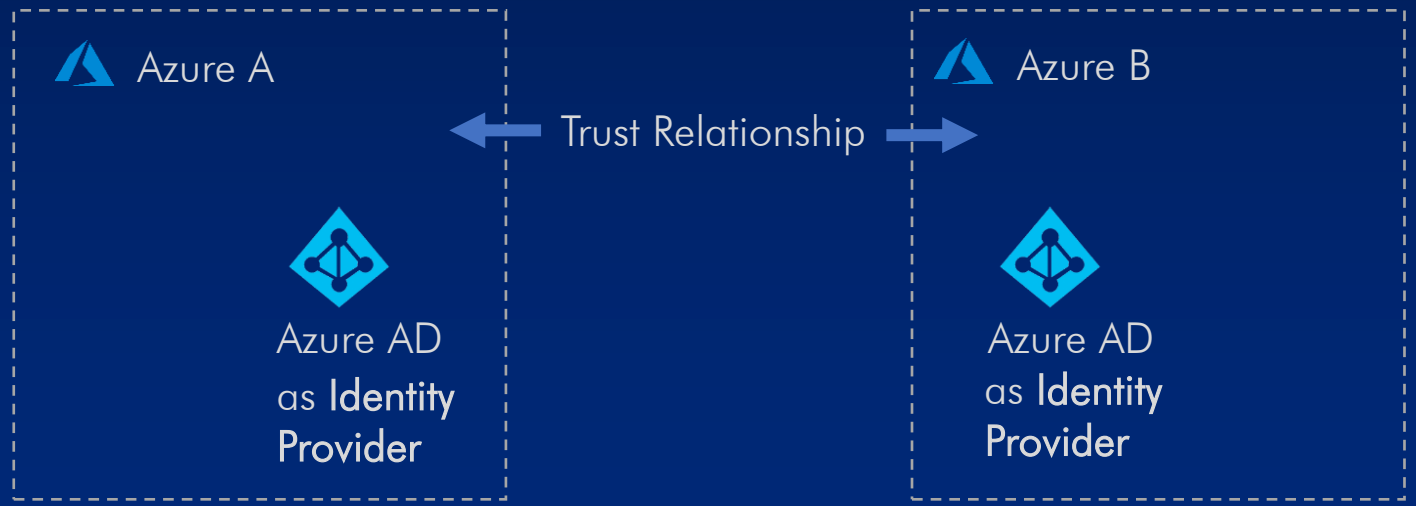
SC-900

SECURITY
COMPLIANCE
IDENTITY

B2B (Business-to-Business)

with Business Partnet Azure

as **External Users**



SC-900

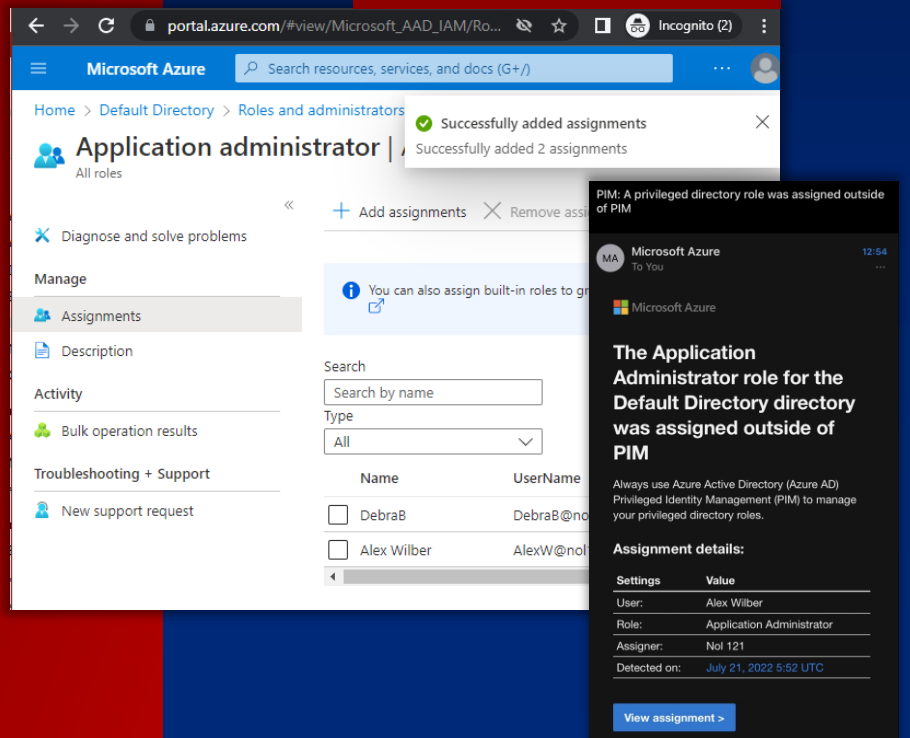
SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

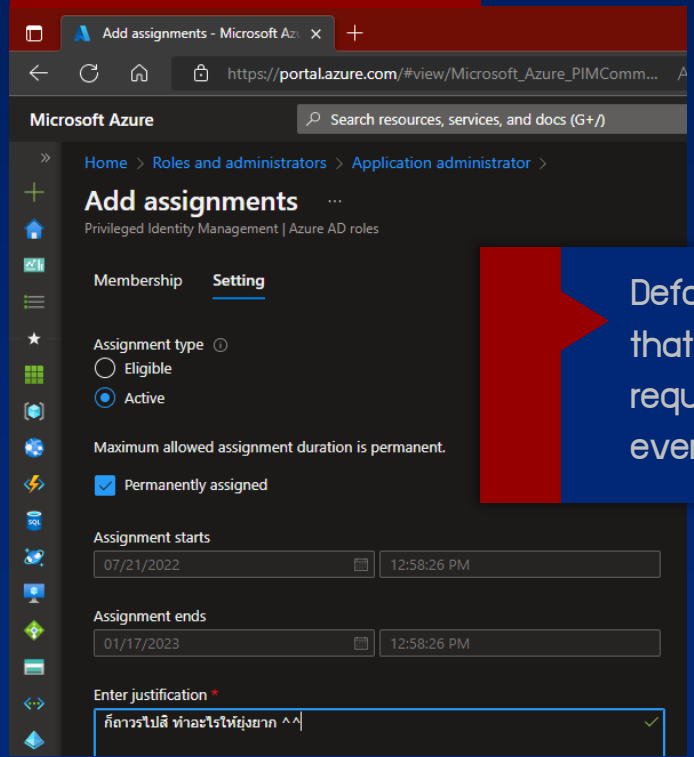
PIM
(Privilege Identity Management)

- Limit time window privilege to complete tasks
- Just In Time (JIT) access

no PIM (AAD P2 License)



with PIM (AAD P2 License)



Default is “eligible” that need to request to access every time

SC-900

SECURITY
COMPLIANCE
IDENTITY

Access Review — Let user evaluate group membership/app/role

Home > Sarah AHA co.,ltd. > Roles and administrators >

New access review

*Review type | *Reviews | Settings | *Review + Create

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles.
Learn more

Select what to review: Teams + Groups

Review scope *: All Microsoft 365 groups with guest / Select Teams + groups

Group *: SarahTest

Scope *: Guest users only / All users

*Review type | *Reviews | Settings | *Review + Create

Determine review stages, reviewers, and timeline below.

Multi-stage review *

Specify reviewers

Select reviewers *: Selected user(s) or group(s)

Users or Groups *: Nol 121

Specify recurrence of review

Duration (in days) *: 6

Review recurrence *: Weekly

Start date *: 07/21/2022

End: Never / End on specific date / End after number of occurrences

https://portal.azure.com/#vi

Microsoft Azure | Search resources, services, and

Home > Sarah AHA co.,ltd. > Roles and admini

New access review

*Review type | *Reviews | Settings | *Review

Configure additional settings, including decision he

Upon completion settings

Auto apply results to resource

If reviewers don't respond: No change

At end of review, send notification to

Enable reviewer decision helpers

No sign-in within 30 days

No change
Remove access
Approve access
Take recommendations

Reviews

Reviewers
1 selected user(s) or group(s)

Frequency
Weekly

End
No end

Settings

Auto-apply results to resource
Enabled

If reviewers don't respond
Remove access

Action to apply on denied guest users
Remove membership

At end of review, send notification to
0 selected user(s) or group(s)

Decision helpers
Enabled, 30 days with no sign-in activity

Justification required
Enabled

Email notifications
Enabled

Reminders
Enabled

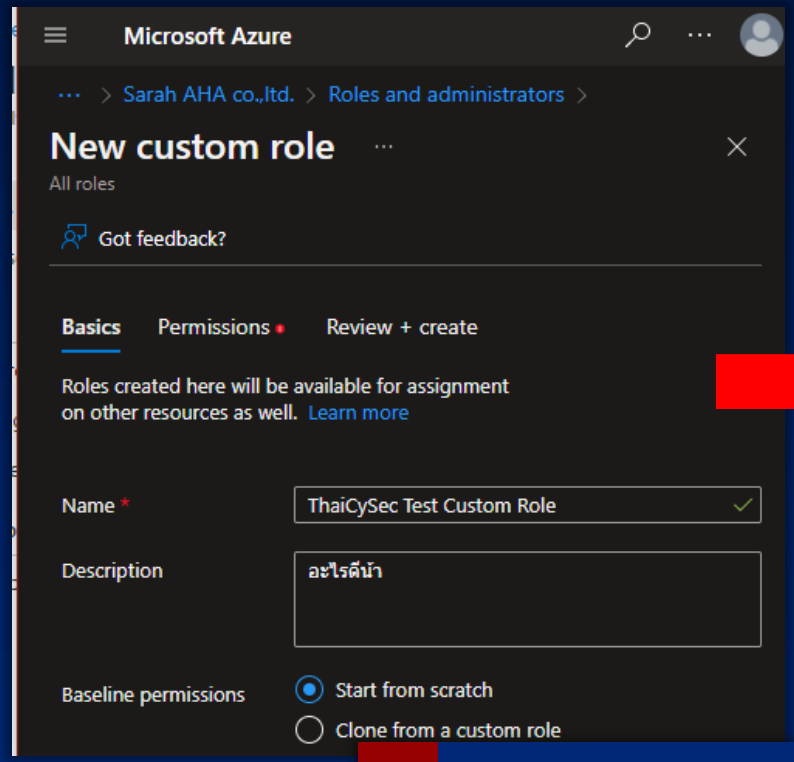
THCS

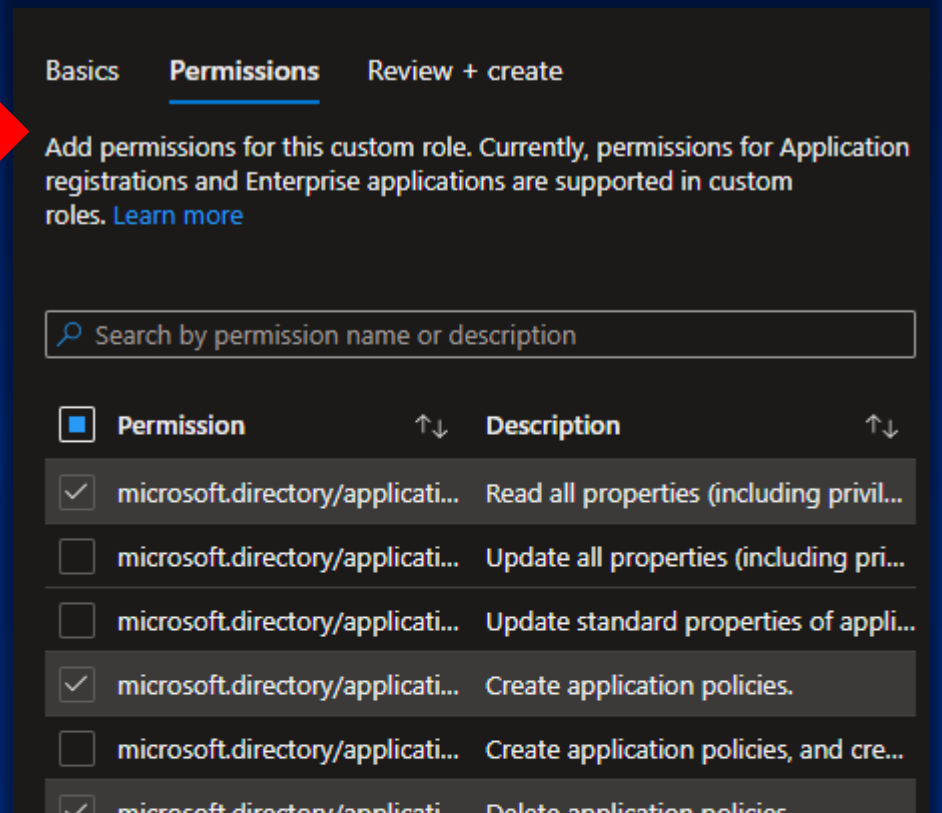
SC-900

SECURITY
COMPLIANCE
IDENTITY

AAD Role

- Global Admin, etc.
- One User, can be many roles
- Can create custom roles





Role (definitions) = collection of **permissions** (so can be built-in or new custom roles)

THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

MFA
(Multi Factor Authentication)

Additional verification

3 methods

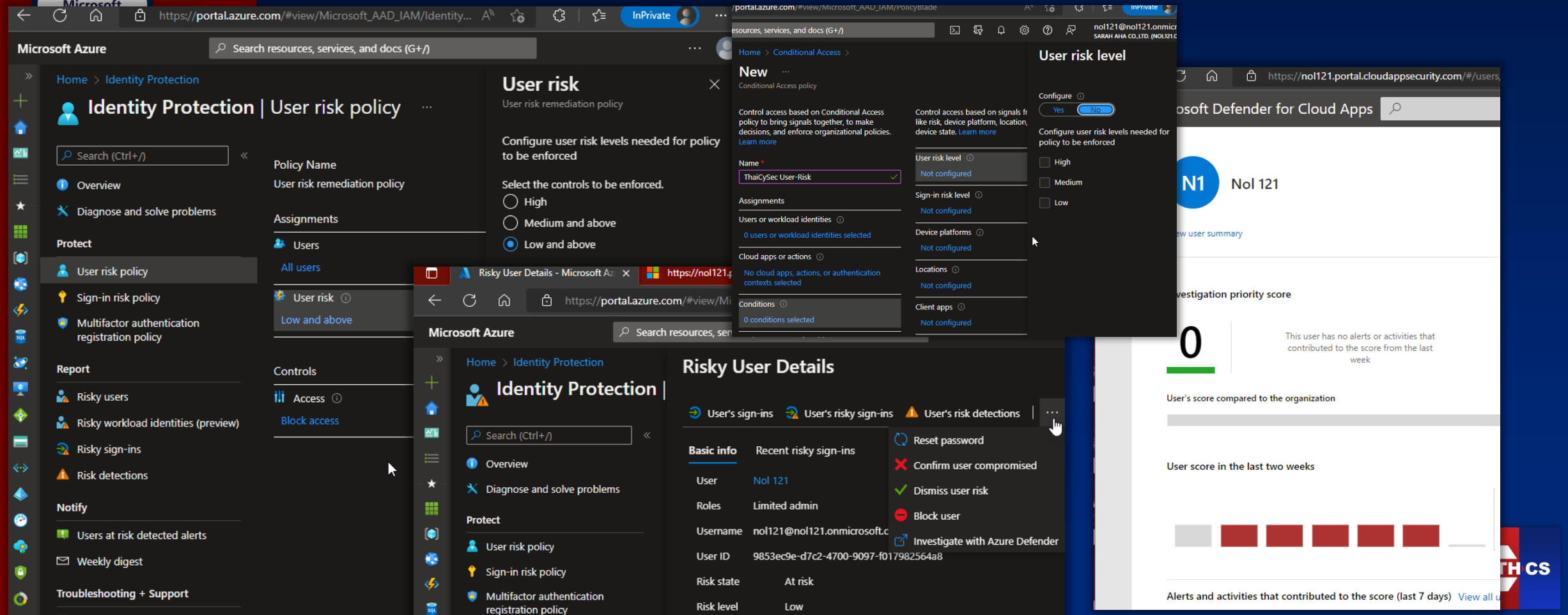
SMS
Authenticator App
Phone Call

THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

AAD Identity Protection — User/Sign-in/Workload Risk Detection + export to 3rd party

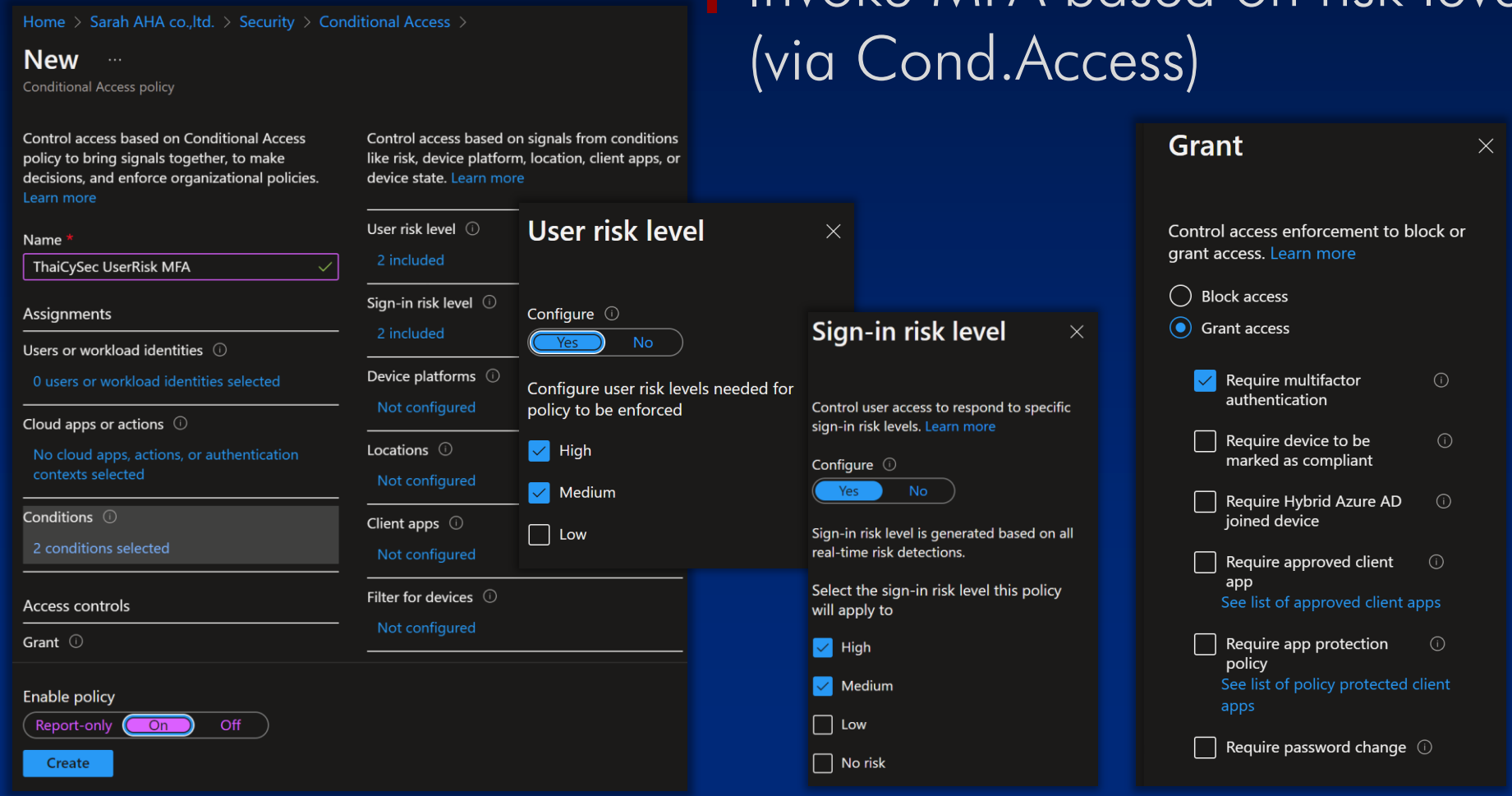


SC-900

SECURITY
COMPLIANCE
IDENTITY

AAD Identity Protection

- Detect if password leak to public
- Invoke MFA based on risk level (via Cond.Access)



SC-900

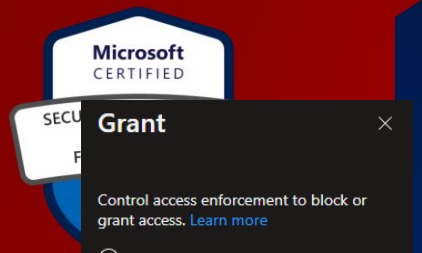
SECURITY
COMPLIANCE
IDENTITY

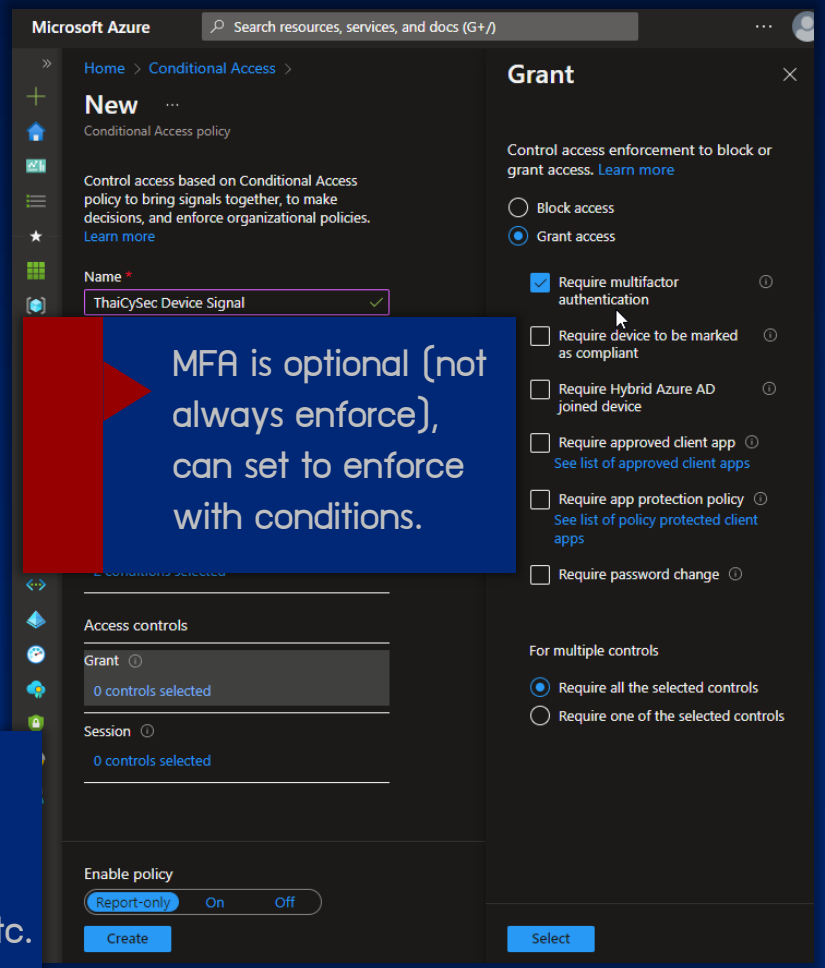
Conditional Access

Authorization after 1st factor Authentication

Get Signals:

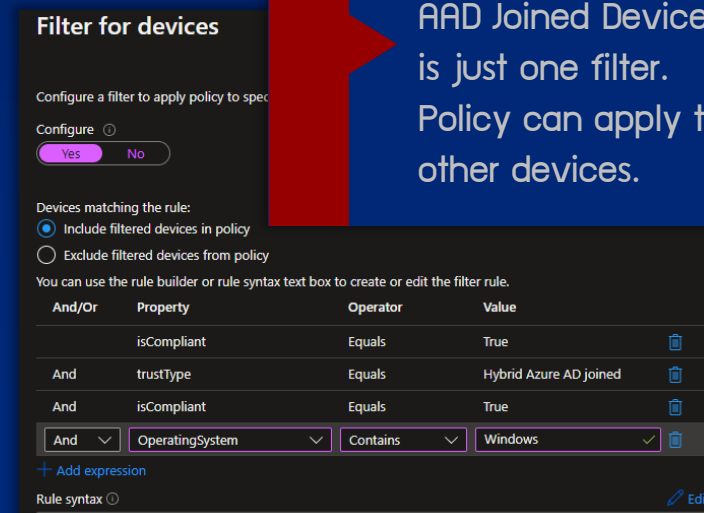
- Users – even Global Admin
- Device
  - State
  - Platform



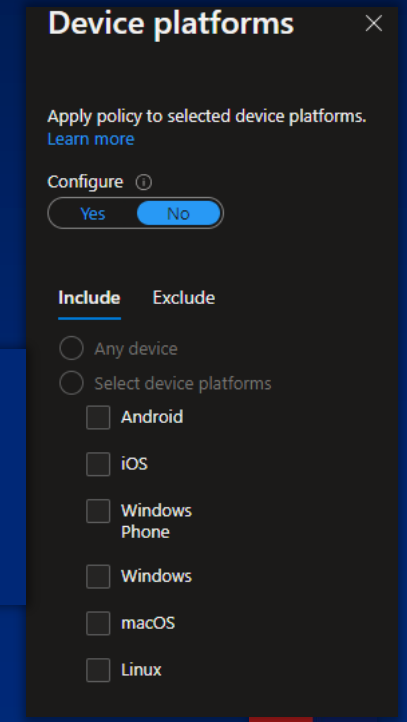


MFA is optional (not always enforce), can set to enforce with conditions.

Cond.Access can enforce access but cannot do jobs as add user to Role, etc.



AAD Joined Device is just one filter. Policy can apply to other devices.



THCS

SC-900

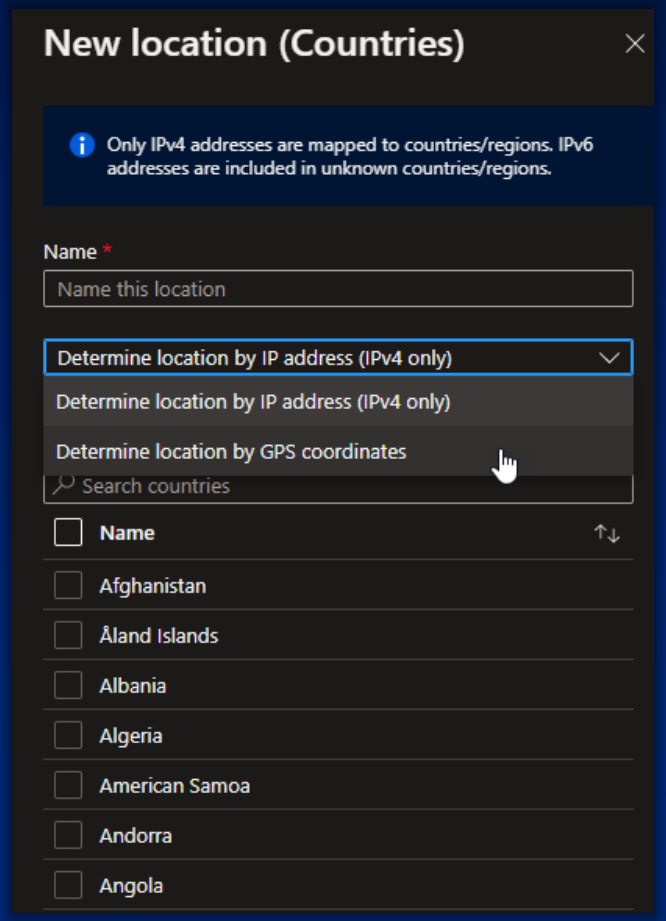
SECURITY
COMPLIANCE
IDENTITY

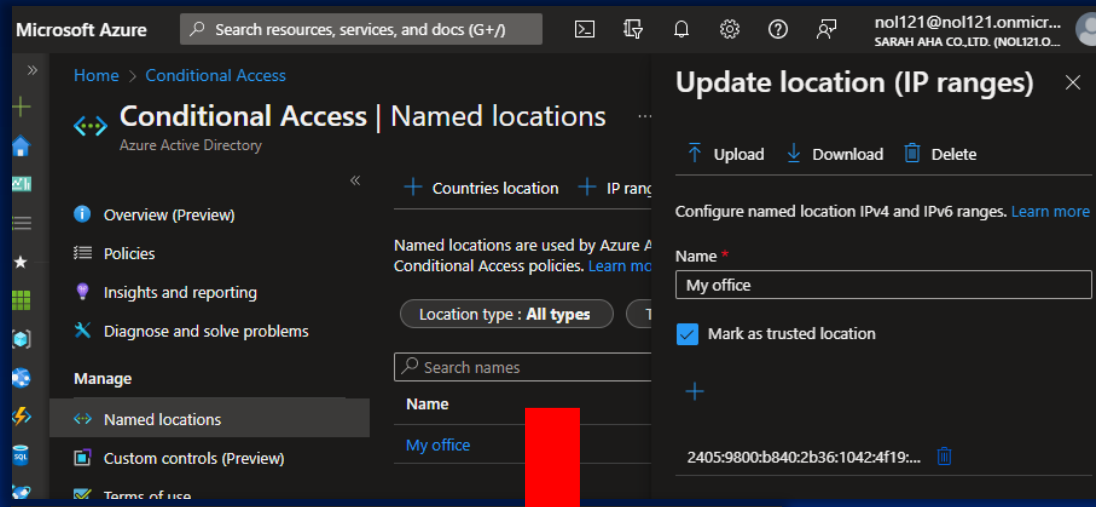
Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

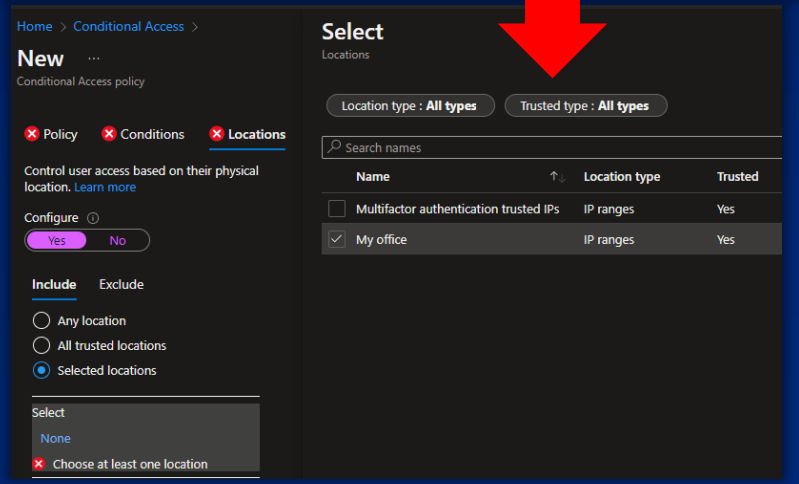
Conditional Access

More Signal

Named/Trust Location





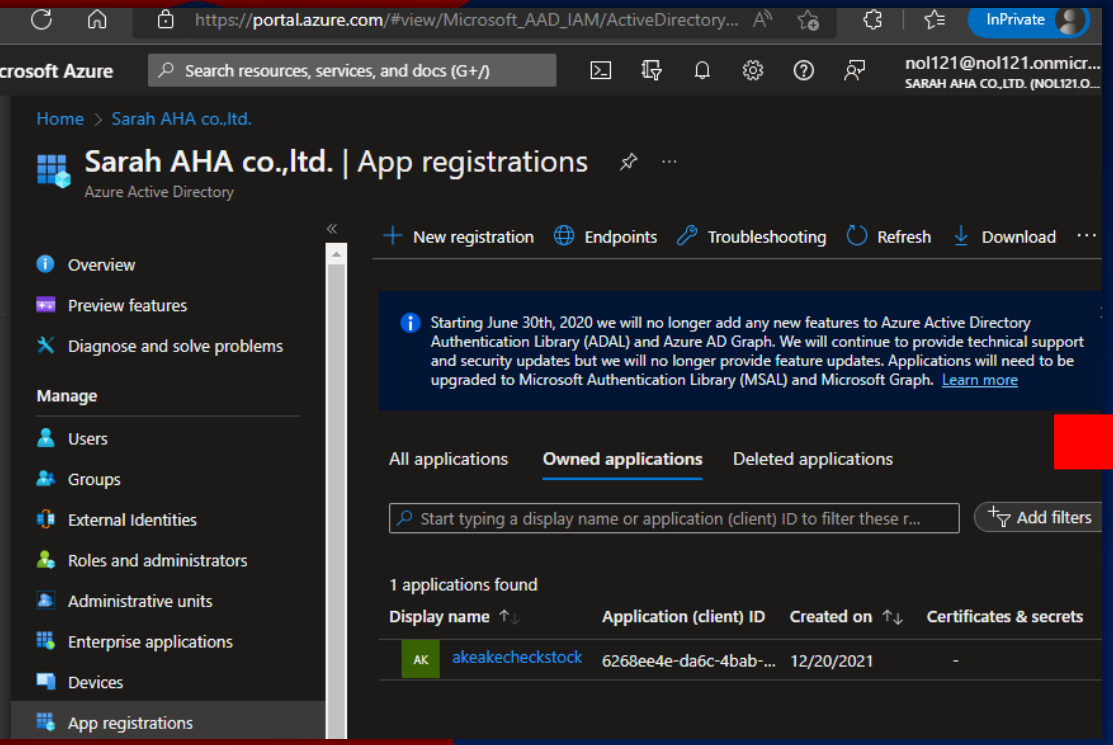


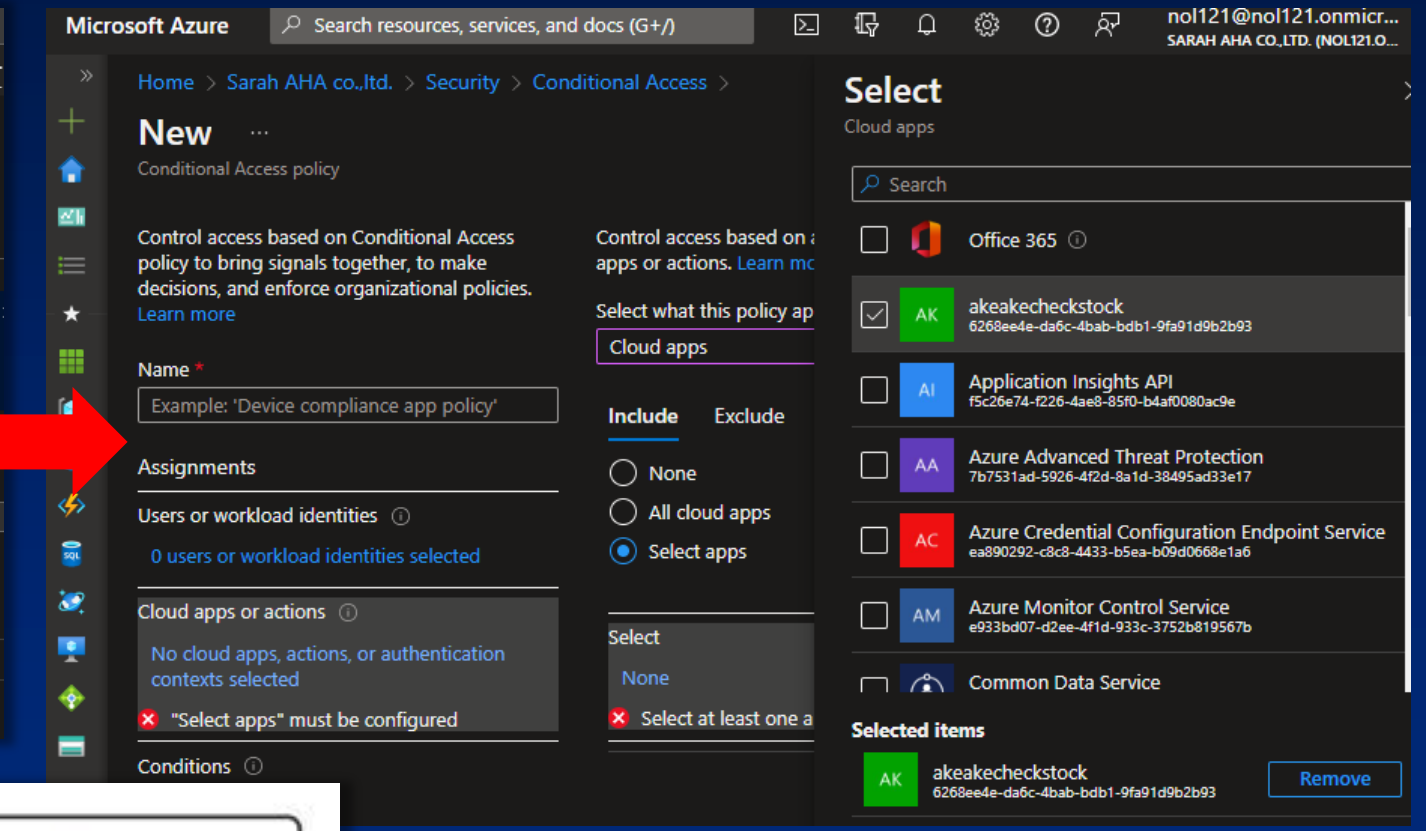
THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

App Regis ⟷ Become Service Principal



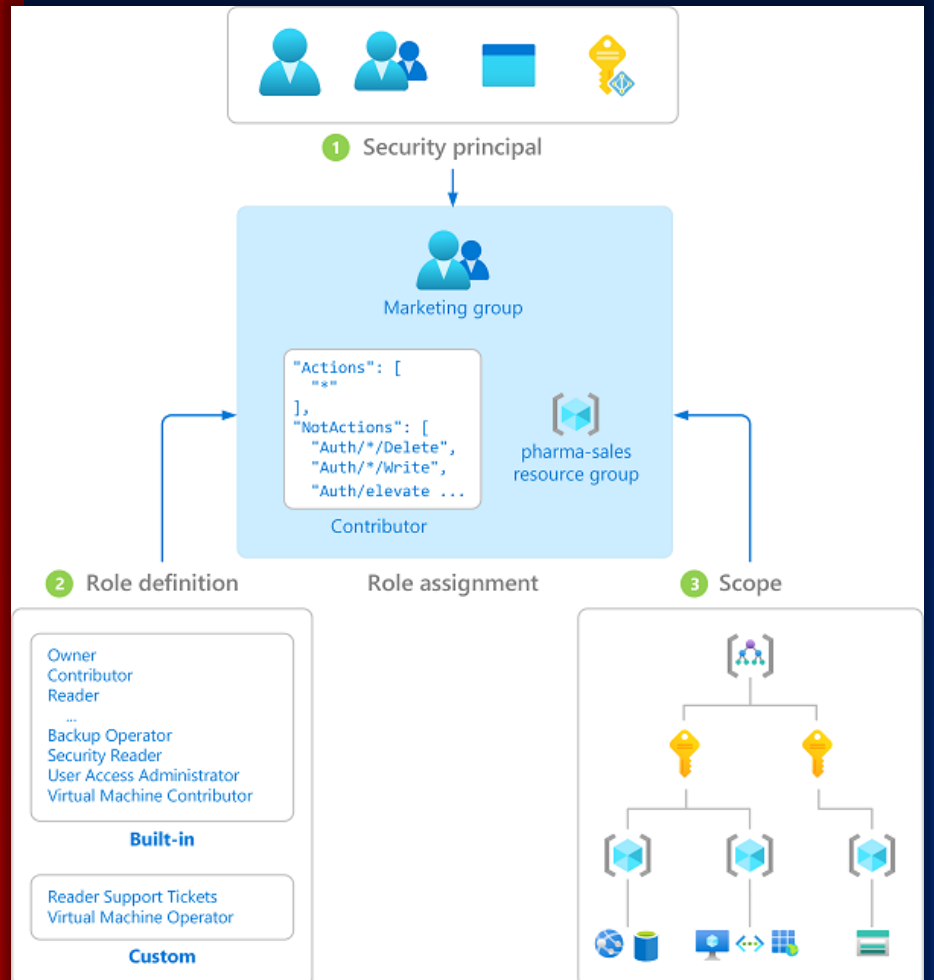


SC-900

SECURITY
COMPLIANCE
IDENTITY

Security Principal (SP)

Identity "regis to AAD" to get permission to AAD resources



User

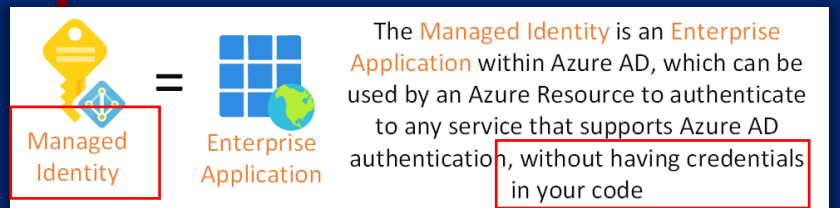
has user profiles in Azure AD

Group

M365/Sec groups that can be assigned to roles

Service Principal

Apps/services or automated tools



THCS

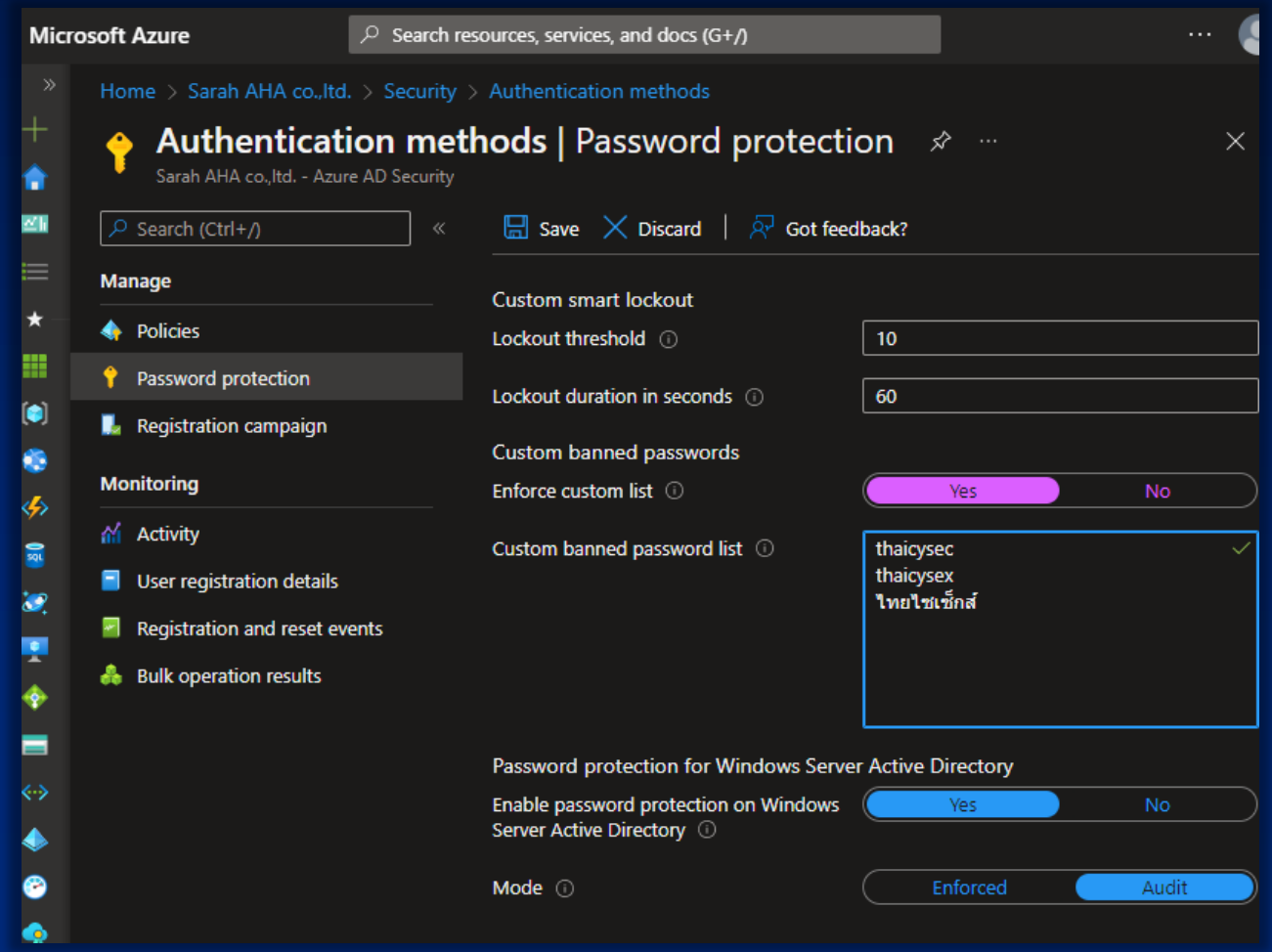
SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Password Protection

Prevent using specific words



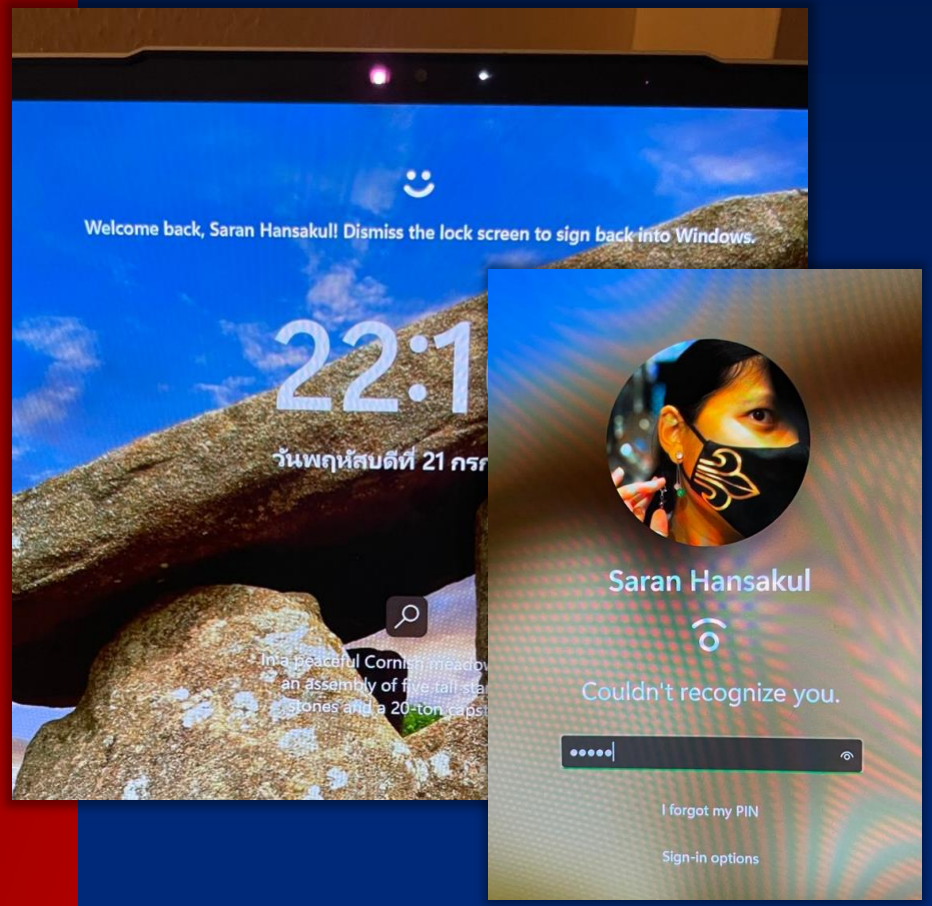
THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Windows Hello



- Store Biometric/PIN on local
- 3 methods – store/specific to one device
  - PIN
  - Fingerprint
  - Facial
- Hello for Business
  - Configured by GPO/MDM
  - **Always** use Key/Cert-based for request authentication with server
  - (Biometric Data still be stored on local devices)

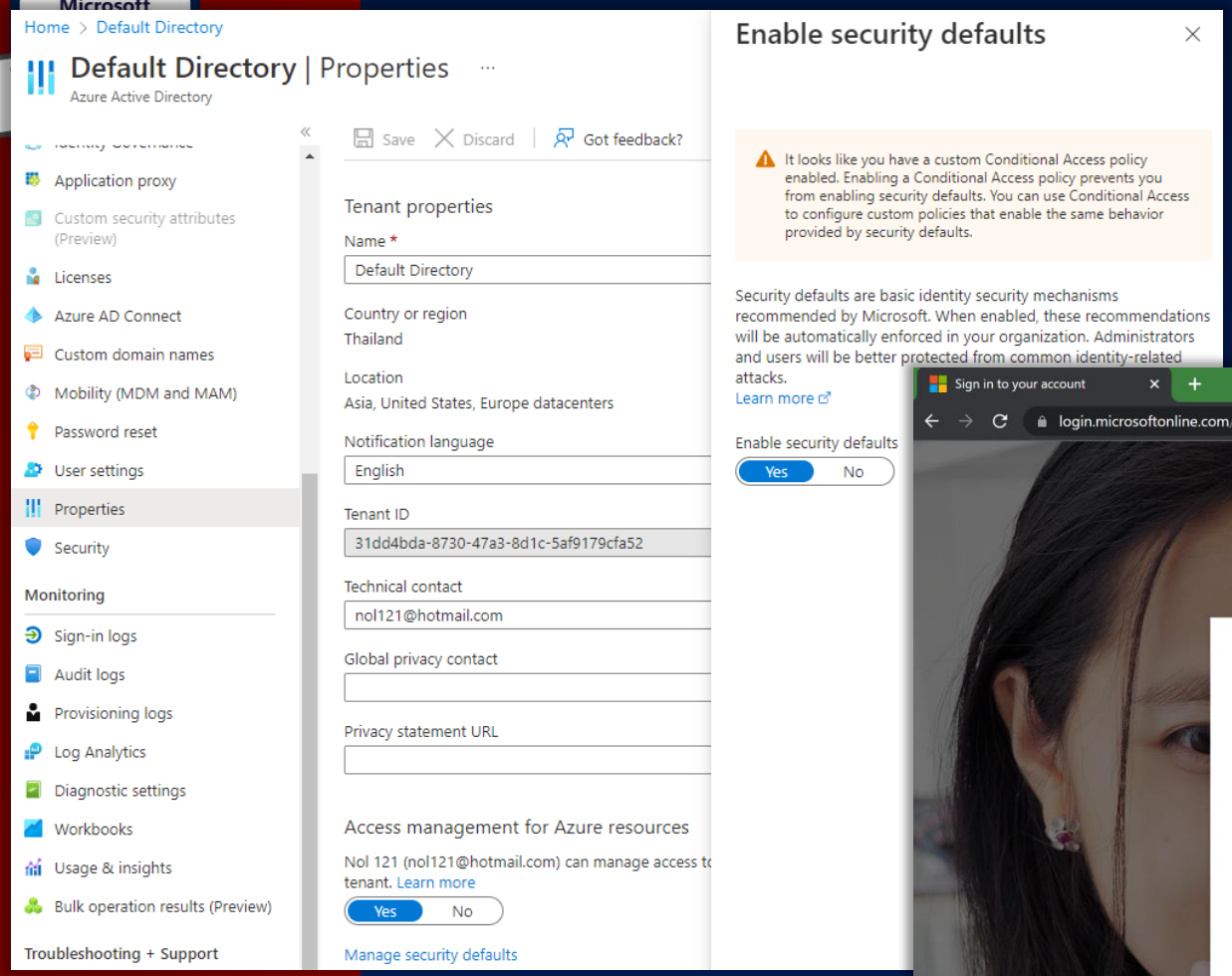
THCS

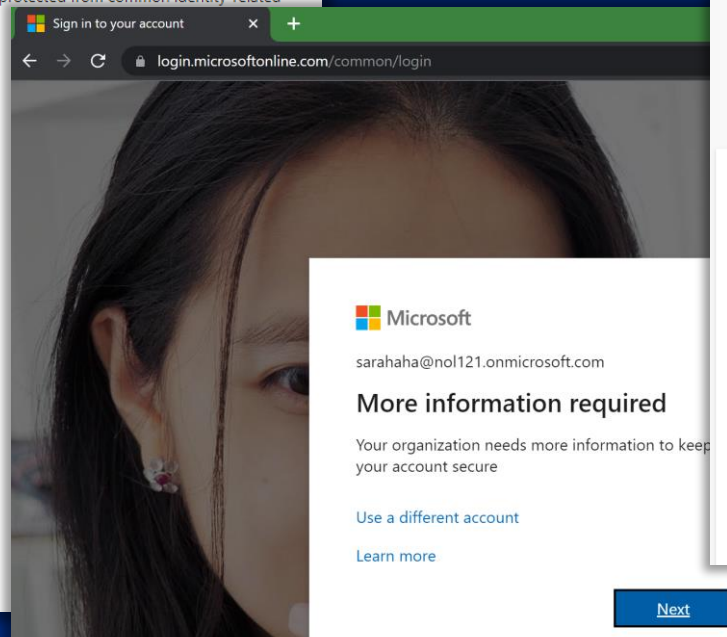
SC-900

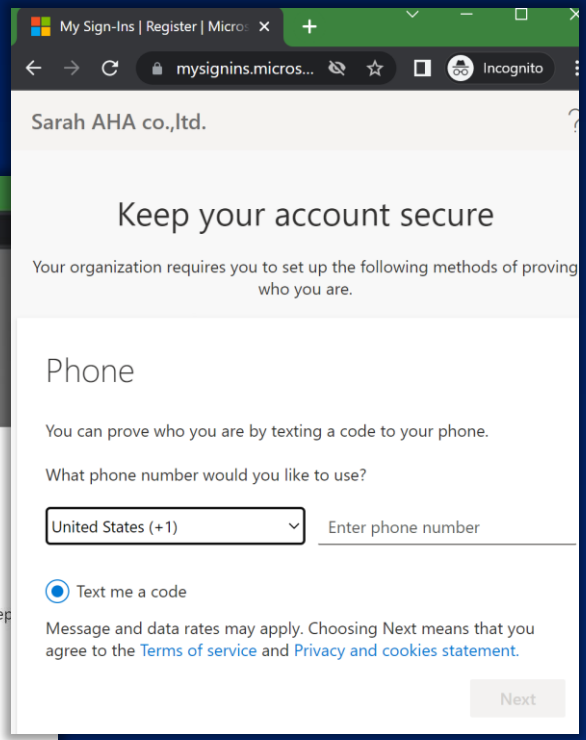
SECURITY
COMPLIANCE
IDENTITY

Security Default

- Enable MFA (force everyone to regis MFA within 14 days)
- Admin must use MFA







SC-900

SECURITY
COMPLIANCE
IDENTITY

Managed both Org-owned (AD Joined) and personal (AD Regis) devices

Cannot provision resource such as AD Subscription

Intune

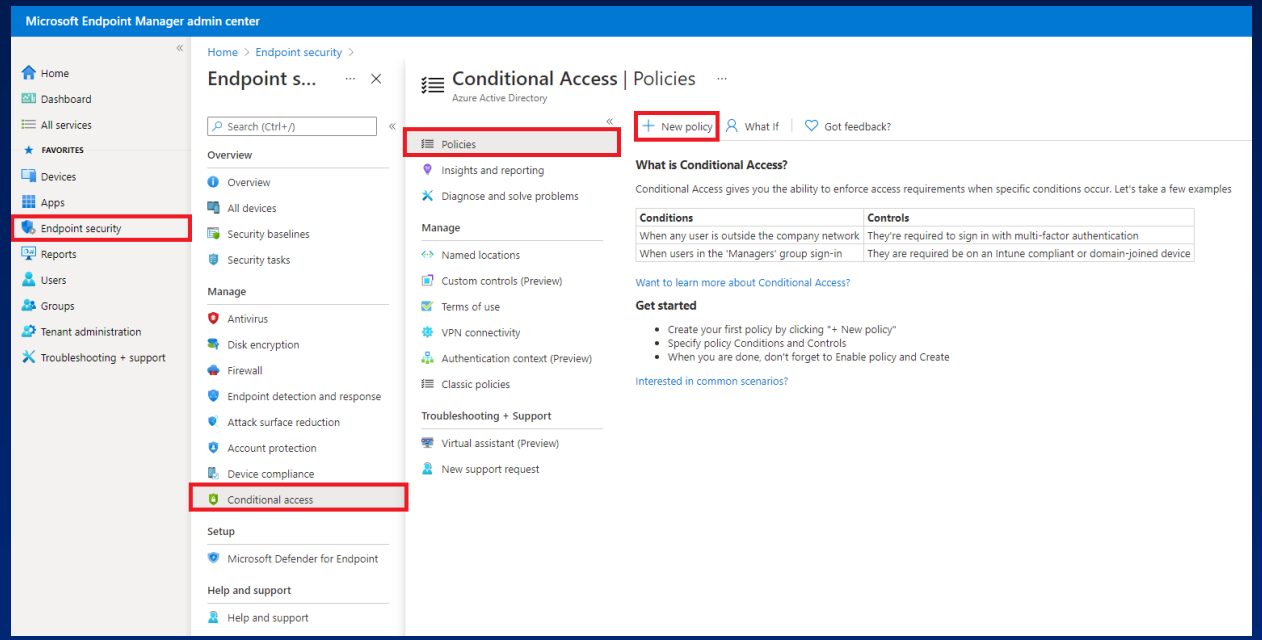
Portal: **Endpoint Manager** admin center

- devicemanagement.portal.azure.com

endpoint.microsoft.com

Manage Win/iOS/**Android Org/Personal** Devices

Device-based **Conditional Access**



THCS

Intune

Conditional Access
Sign-in/Access Activity/logs

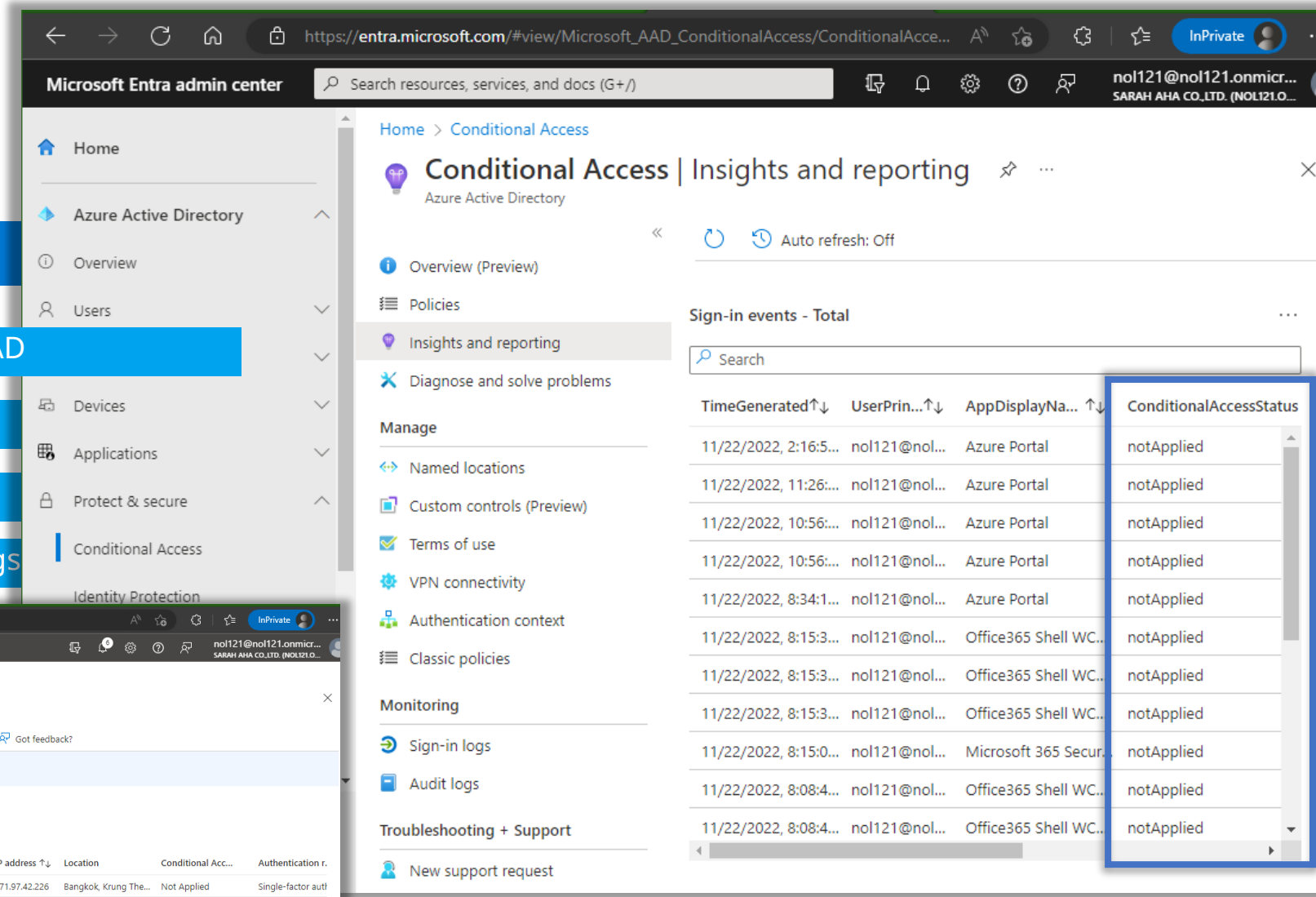
Cond.Acc is in Entra > AAD

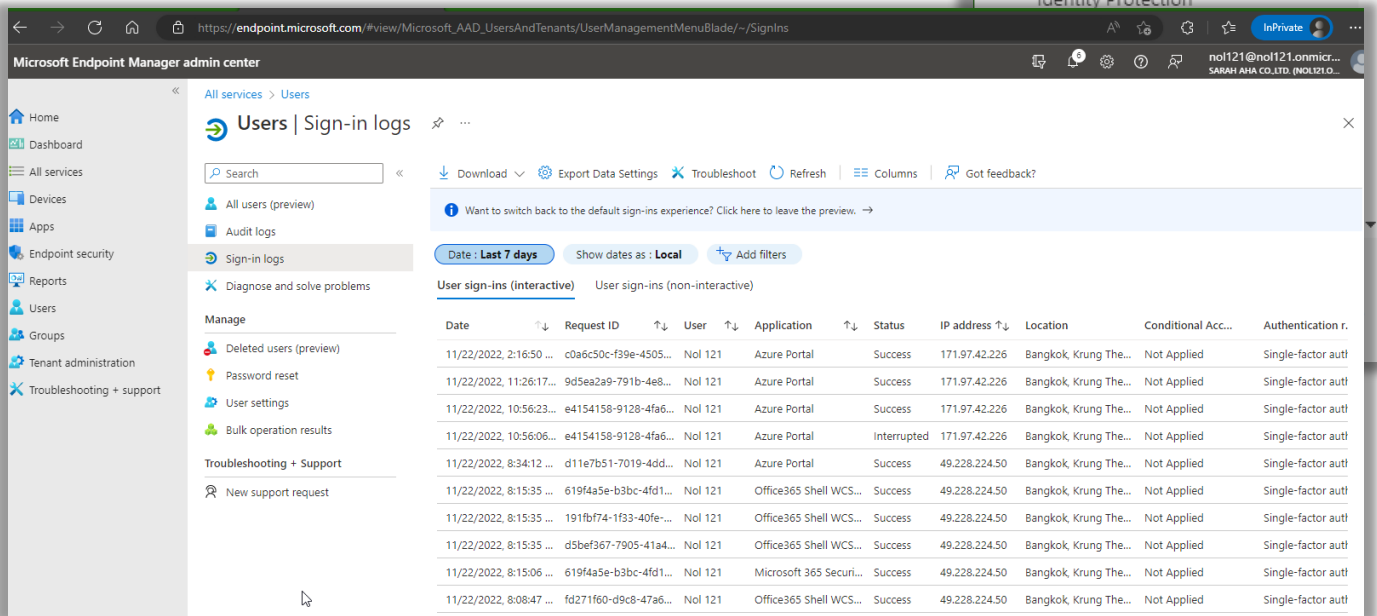
So should be in “Sign-in logs” in AAD

Or “Insights and Reporting”

No access log in MEM admin page

Except in MEM > Users > Sign-in logs



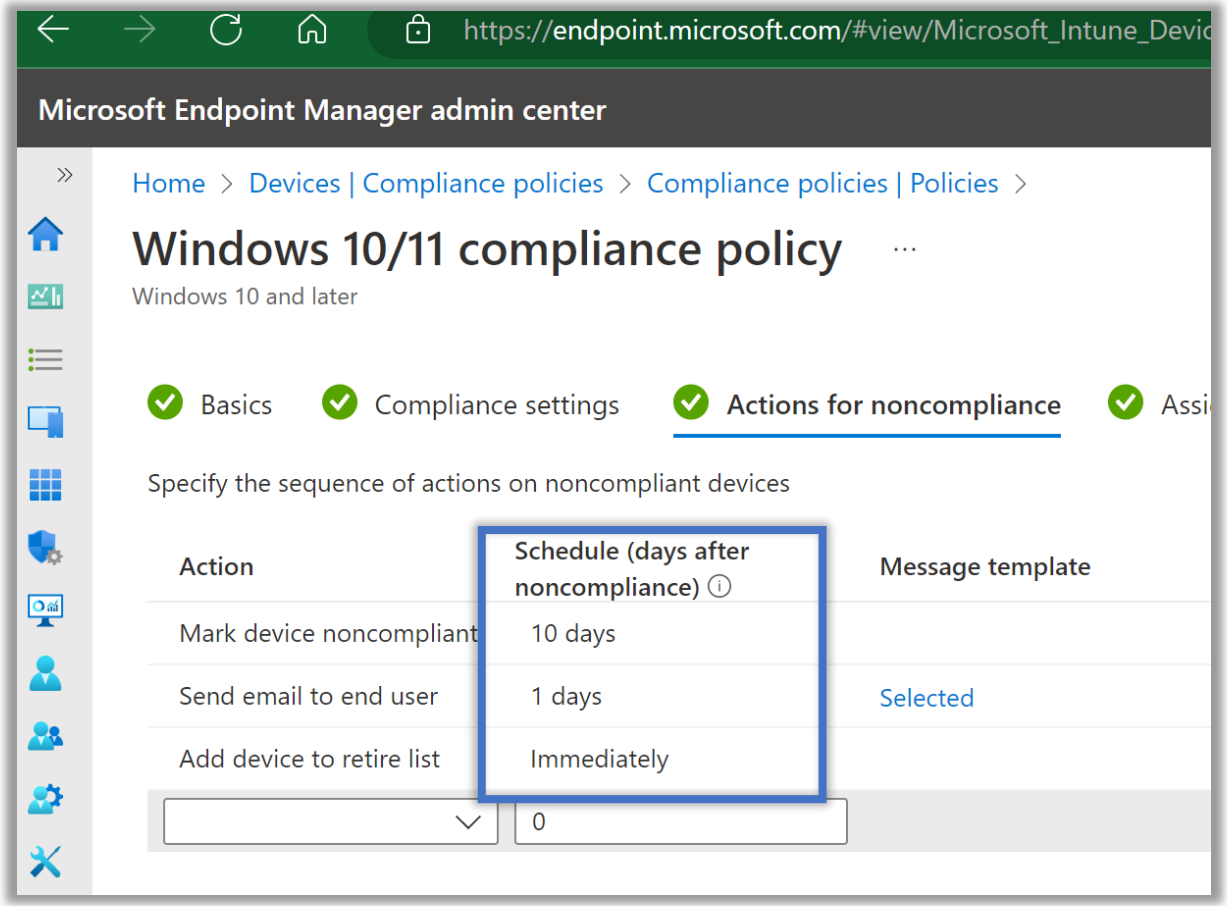


Intune
Compliance Policy Grace Period

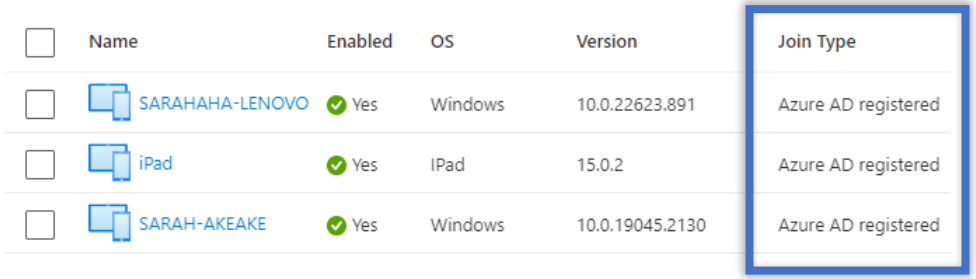
Grace Period = Days after “noncompliance”

Start when “enrolled” or “not compliant”

Default is 0day = Immediately



Intune
Devices
Joined vs Registered

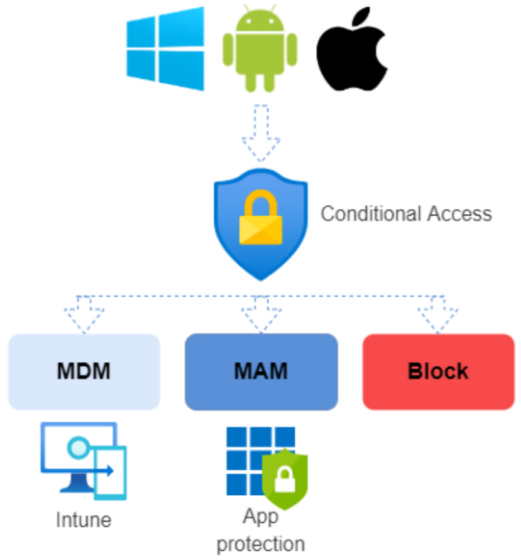


Name	Enabled	OS	Version	Join Type
SARAHAHA-LENOVO	Yes	Windows	10.0.22623.891	Azure AD registered
iPad	Yes	IPad	15.0.2	Azure AD registered
SARAH-AKEAKE	Yes	Windows	10.0.19045.2130	Azure AD registered

	Domain "Joined"	Hybrid AD "Joined"	Azure AD "Joined"	Azure AD "Registered"
Domain Controller	On-prem AD	Hybrid AD+AAD	Azure AD (AAD)	Azure AD (AAD)
Device Login ID	User ID in AD	User ID in AD+AAD	User ID in AAD	Their own/Personal ID
Corp.Resource Login ID	User ID in AD	User ID in AD+AAD	User ID in AAD	User ID in AAD
Managed by	GPO	GPO or +MDM ex. Intune (ConfigMgr)	MDM ex. Intune	MDM ex. Intune (or not enforced)
Ideal for	Corp.owned/in-office/on-site PC etc.	Corp.owned PC, laptops	Corp.owned laptops, mobiles in cloud only	Personally owned devices
Apps can be accessed	Local corp.apps via Kerberos/NTLM/LDAP	Local corp.apps via Kerberos/NTLM/LDAP and Cloud apps via Oauth, SAML	Cloud apps only	Cloud apps and locally installed apps on devices

✨ Azure AD joined devices can log into on-prem apps with SSO (w/ on-prem AD DS.)

Intune
MDM vs MAM

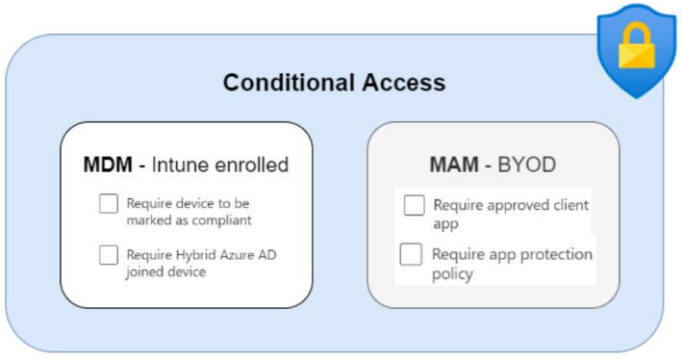


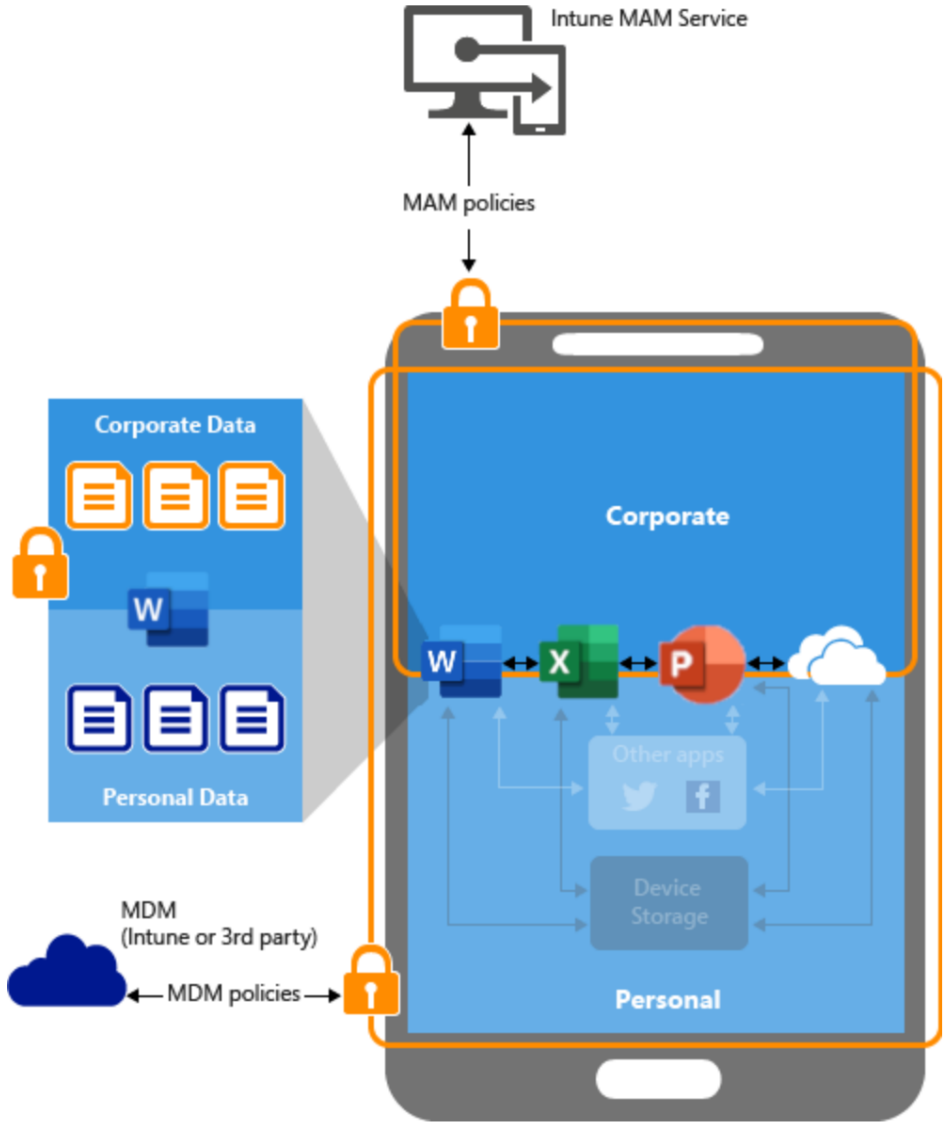
MDM: manage “Device”

- Enrolled
- App Install/Uninstall
- Remote Wipe for all Data (even personal)

MAM: manage “Data” on certain apps

- Independent from MDM
- = App Protection Policy



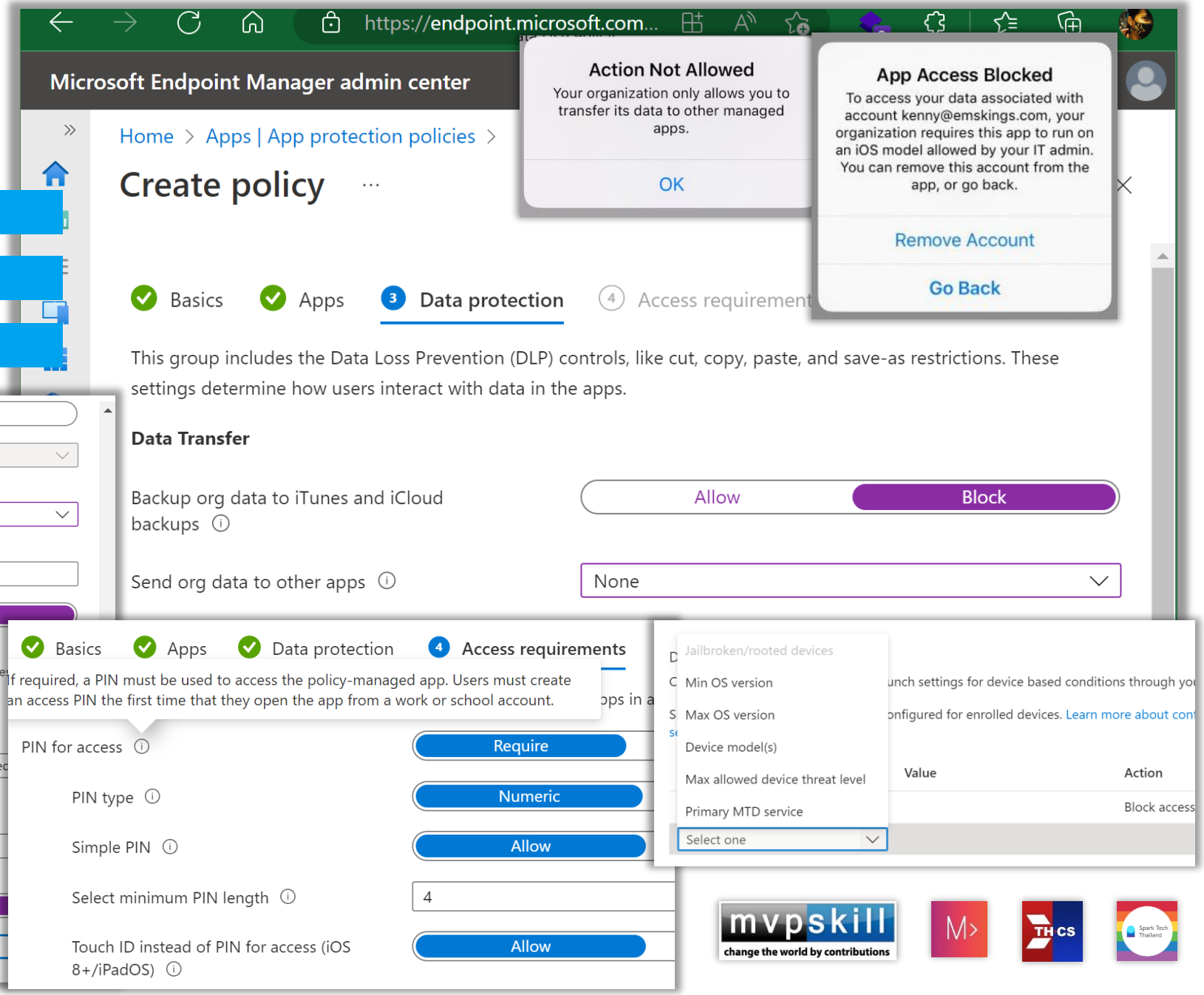


Intune
App Protection (MAM)

Prevent Data moving outside “mobile” apps

Independent with MDM, or even “not enrolled”

Suitable for “Personal” (BYOD) devices

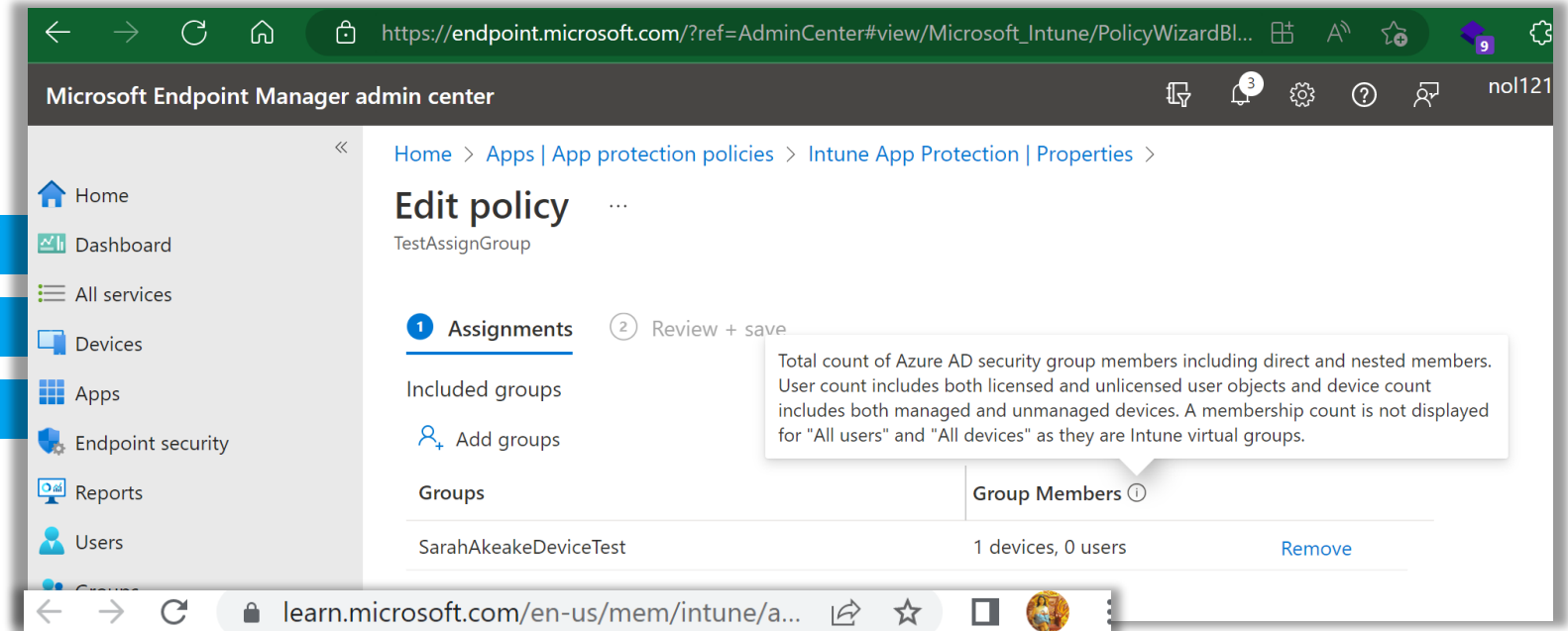


Intune
App Protection (MAM)

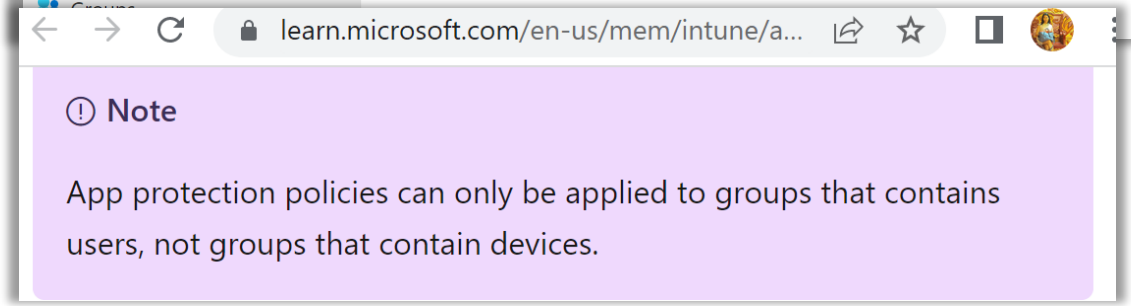
Can only be applied to groups that contain “users”

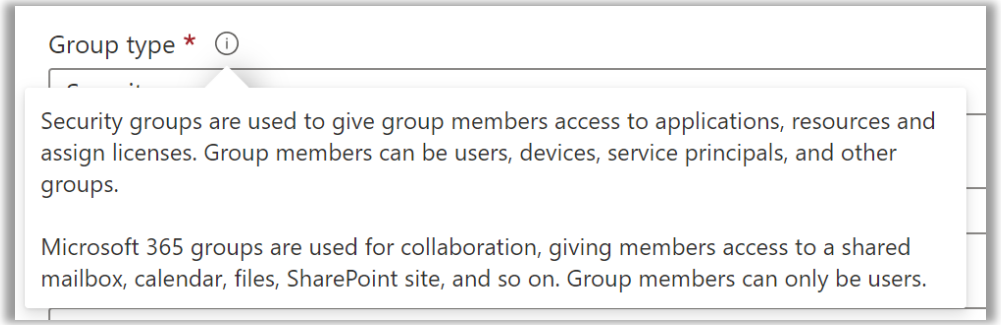
Not assign to groups with only devices

So… consider from “users” first!



✨ Note1! MEM portal may accept the device-only security group assignment, but practically cannot be applicable. (according to MS docs 😒)





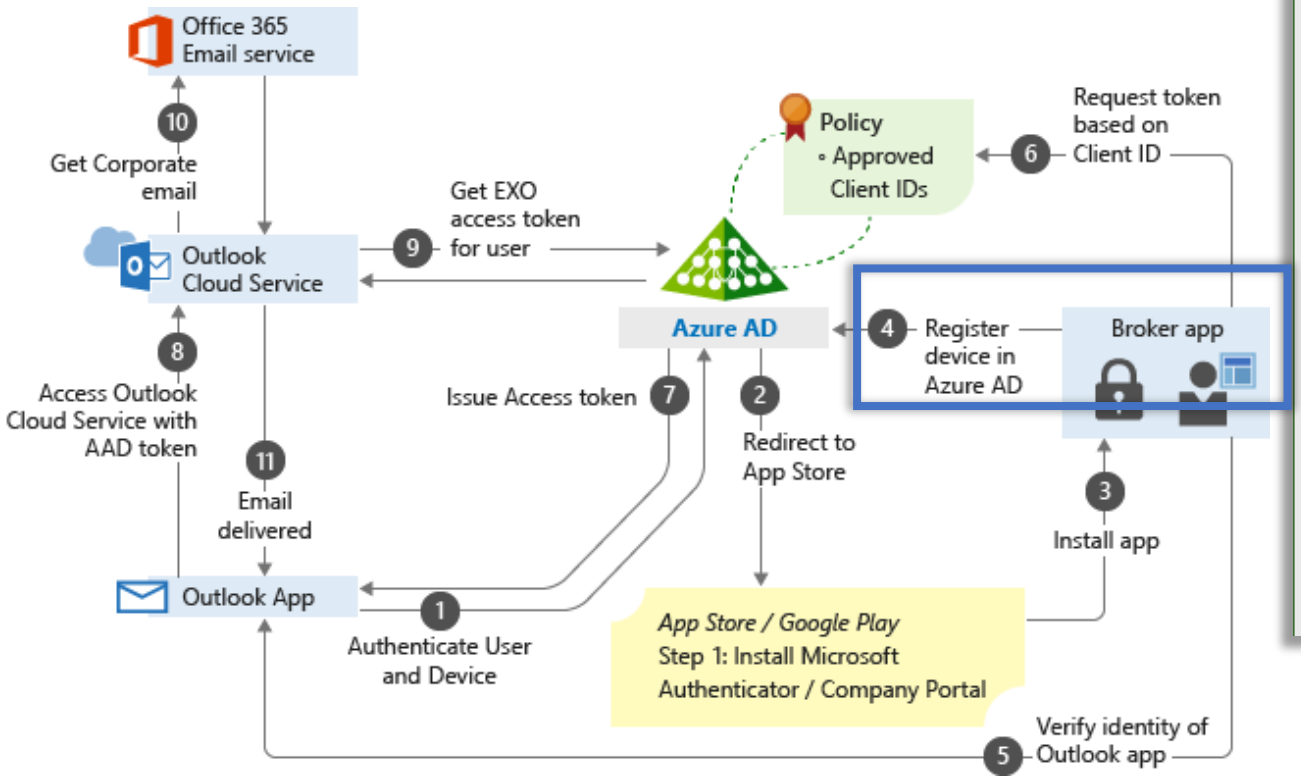
✨ Note2! “Security” Group can contain vary SP (user/device/SP/groups) but “M365” Group can have only “users”.

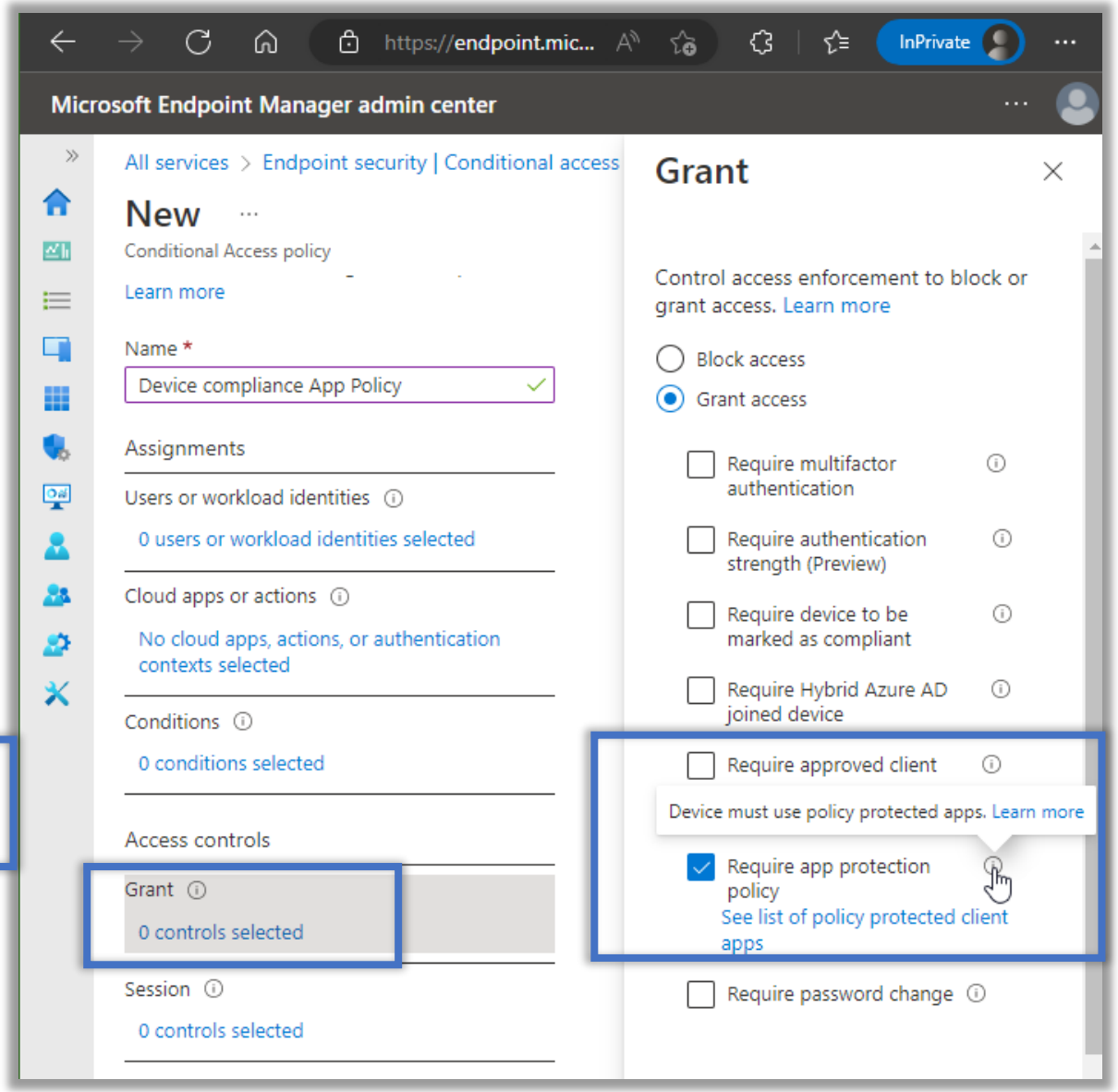
Intune

App Protection (MAM) w/ Cond.Acc. Grant Control

Others than assign to users/group directly in policies

Use “Grant” access in Cond.Acc. for both MDM/MAM





Intune

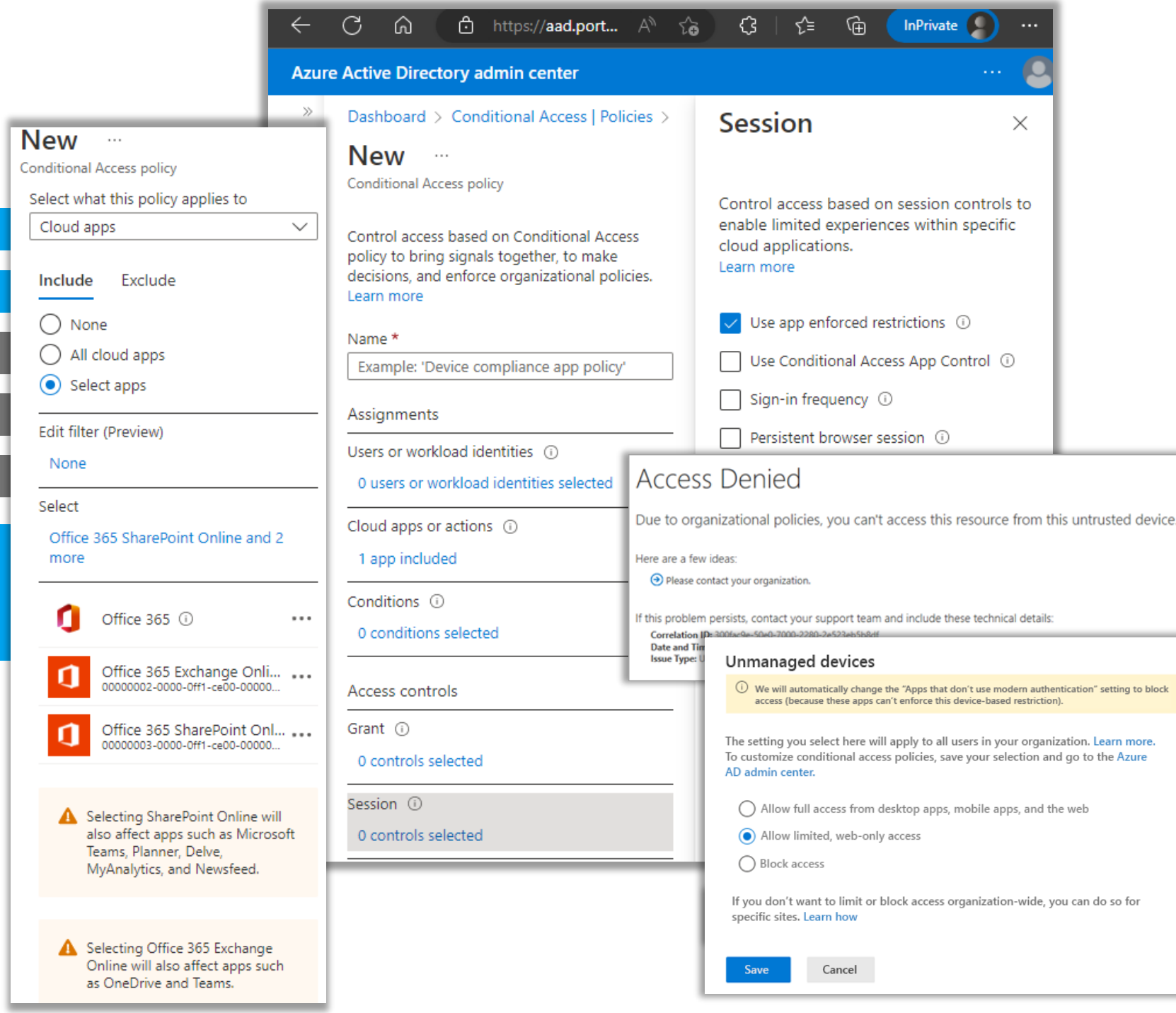
w/ Cond.Acc. Session Control App Enforce Restriction

Use “Sessions” control in Conditional Access

Pass “Device state” to specific apps:

- Office 365
- Sharepoint Online
- Exchange Online

Let these apps limit experiences on fully-managed (Hybrid AD joined = MDM enrolled/company own) and compliant vs others

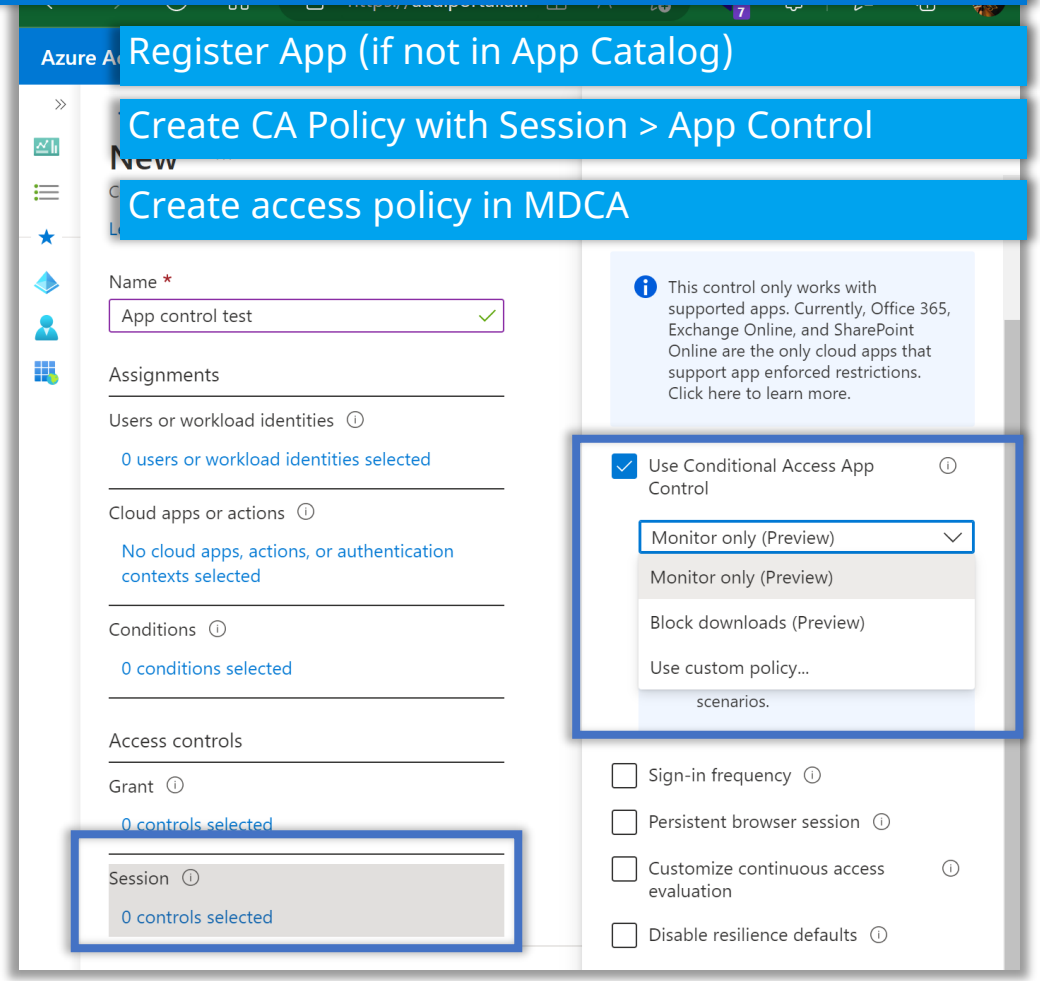


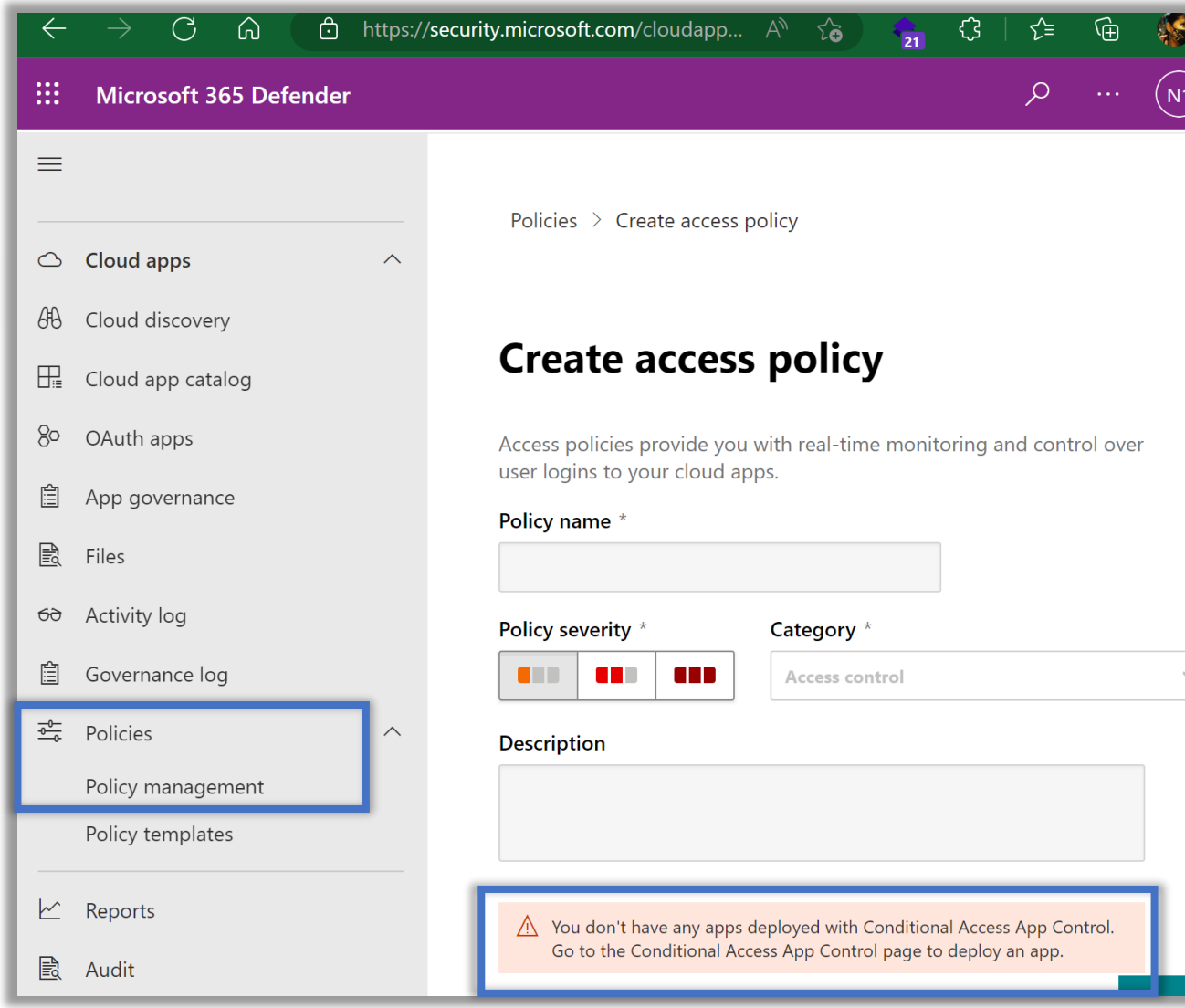
Defender for Cloud Apps

Access Policy

Instruction to review sessions in real-time:

- Register App (if not in App Catalog)
- Create CA Policy with Session > App Control
- Create access policy in MDCA





Defender for Office 365

Connect to MDE

Integrate with MDE

To share info, esp. about endpoints

Turn on Connect to MDE, in MDE Settings on Explorer page

Then turn on “Office 365 Threat Intelligence connection” in Settings > Endpoints > Adv Feat.

Microsoft Defender for Endpoint connection

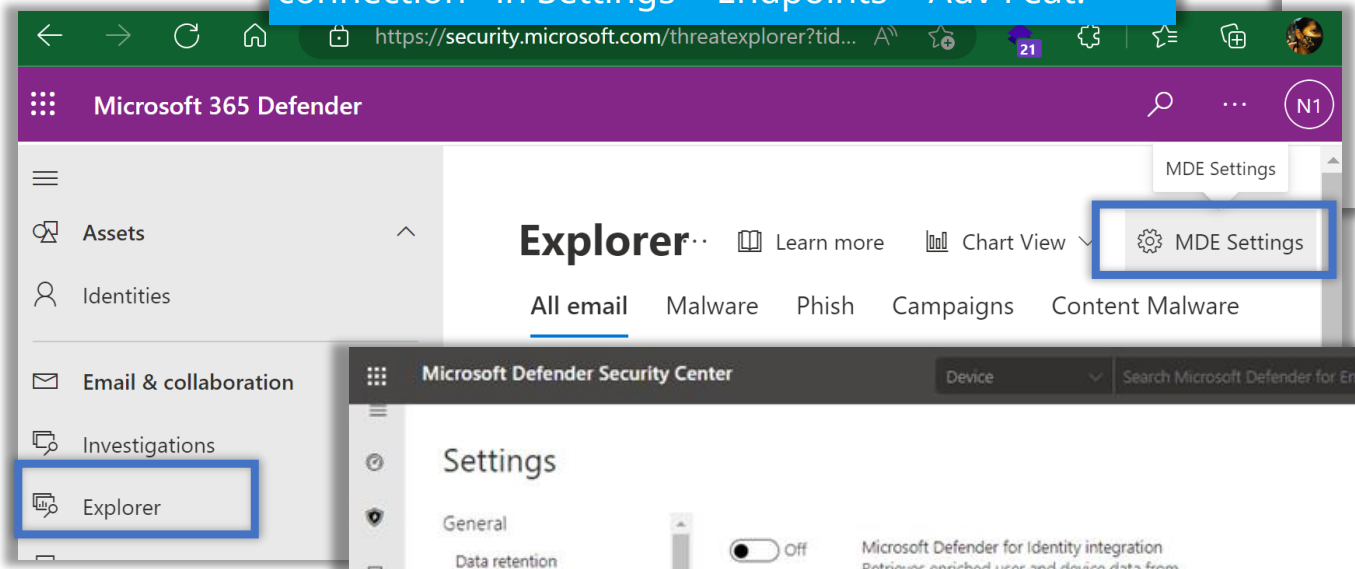
Connect to Defender for Endpoint — On

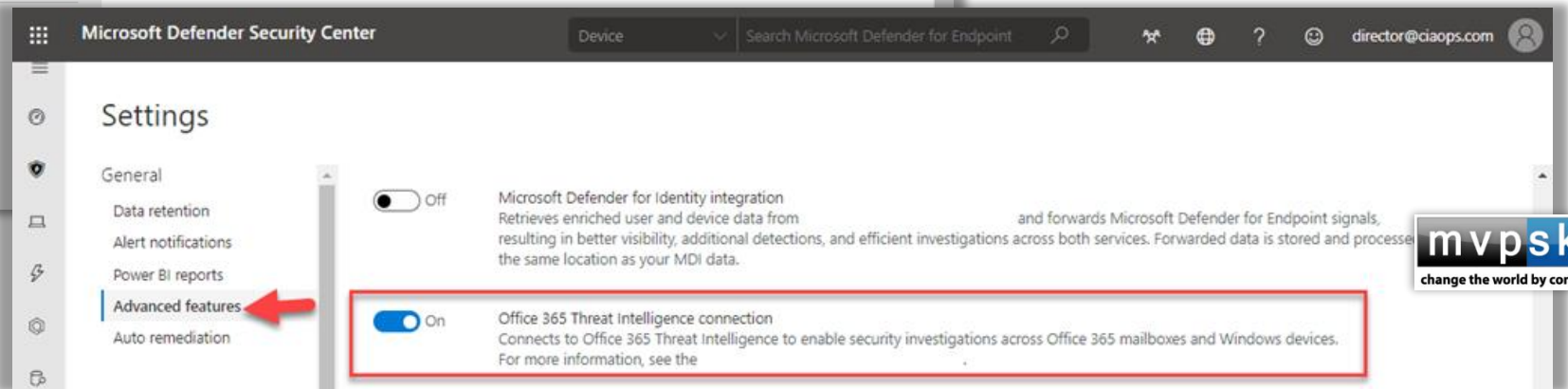
Use this feature to investigate threats between Office 365 and windows devices. When you turn this on:

- You will be able to view device details and Microsoft Defender for Endpoint alerts from the Threat Explorer.
- Microsoft Defender for Endpoint will be able to query Office 365 for email data in your organization and show links back to filtered views in the Threat Explorer.

Note: To turn on this connection, your organization must have a Microsoft Defender for Endpoint subscription and security analysts must have access to Defender for Office 365 P2 and Microsoft Defender for Endpoint.
Learn more about Microsoft Defender for Endpoint

ⓘ After enabling this feature in Office 365, enable the connection from the Windows Security Center.



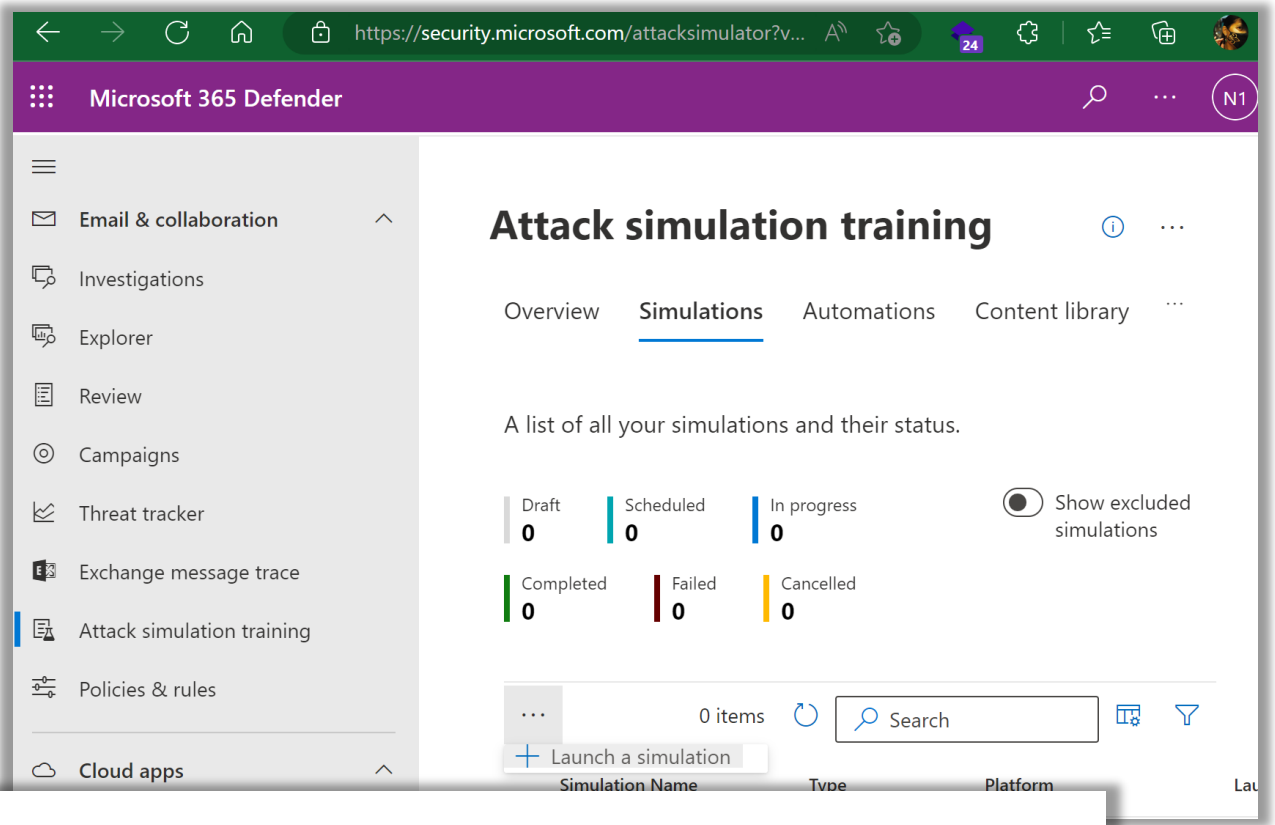


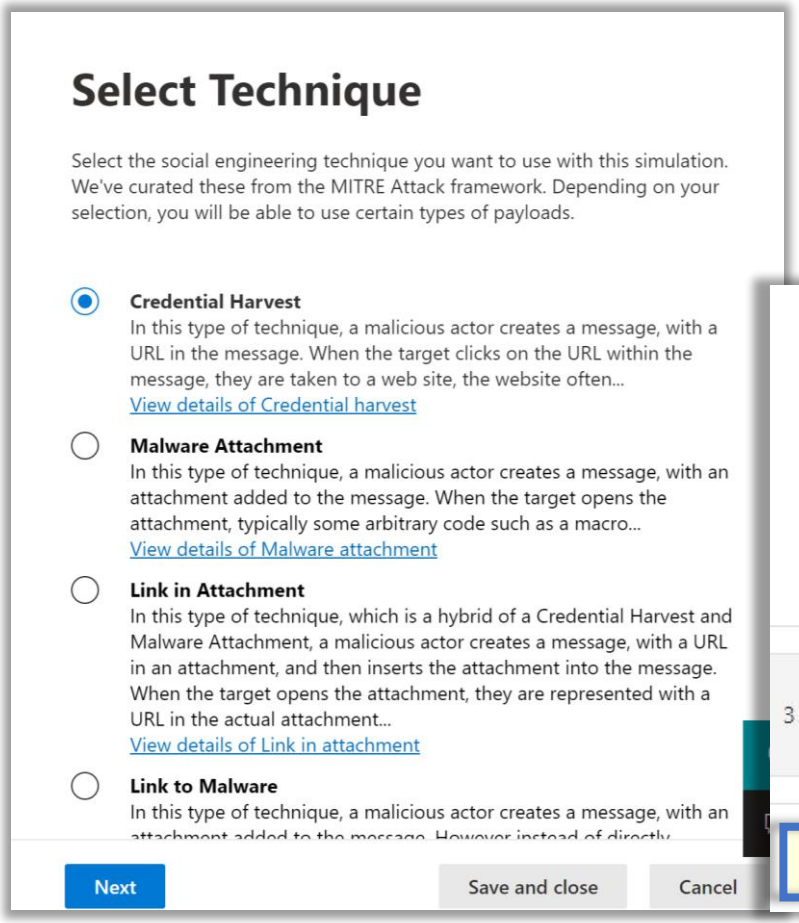
Defender for Office 365

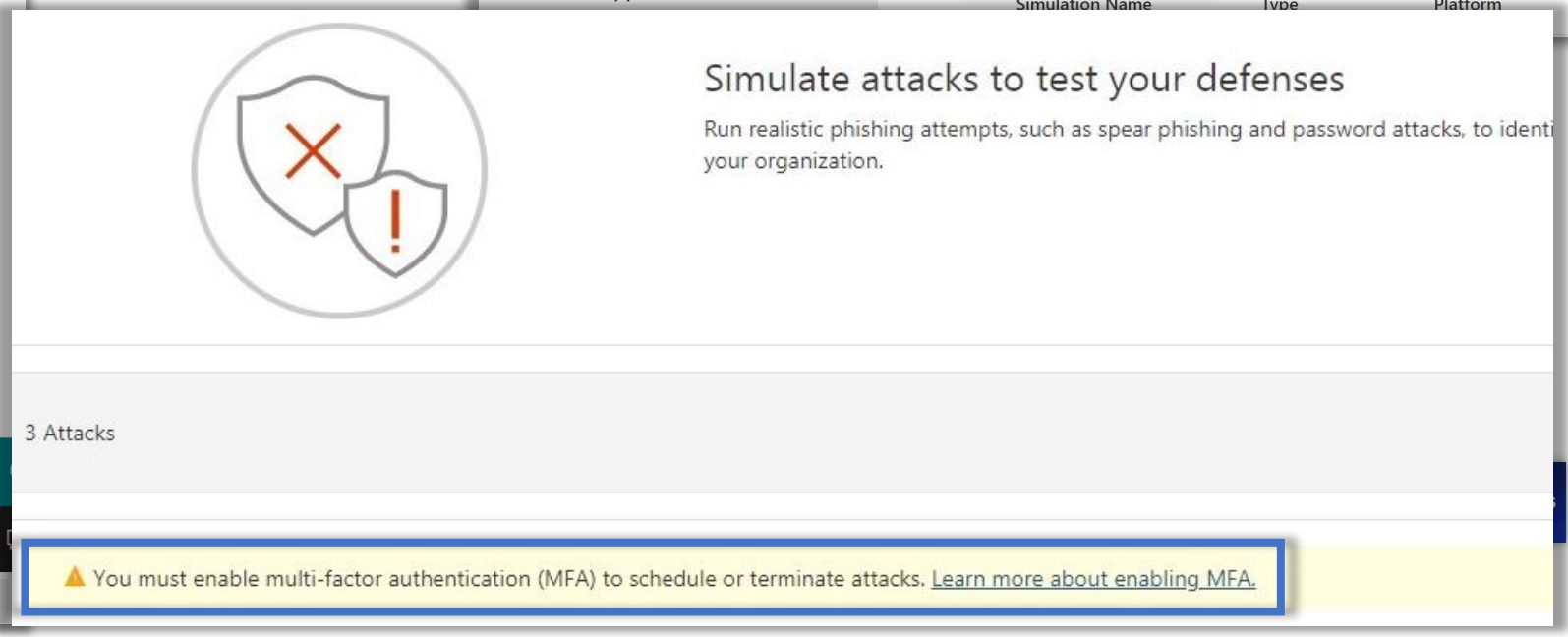
Attack Simulation

Target mailbox must be on-cloud: Exchange Online

Org.Mgmt/Sec Admin/Attack Admin “who launch” the attack have to enable MFA for security.







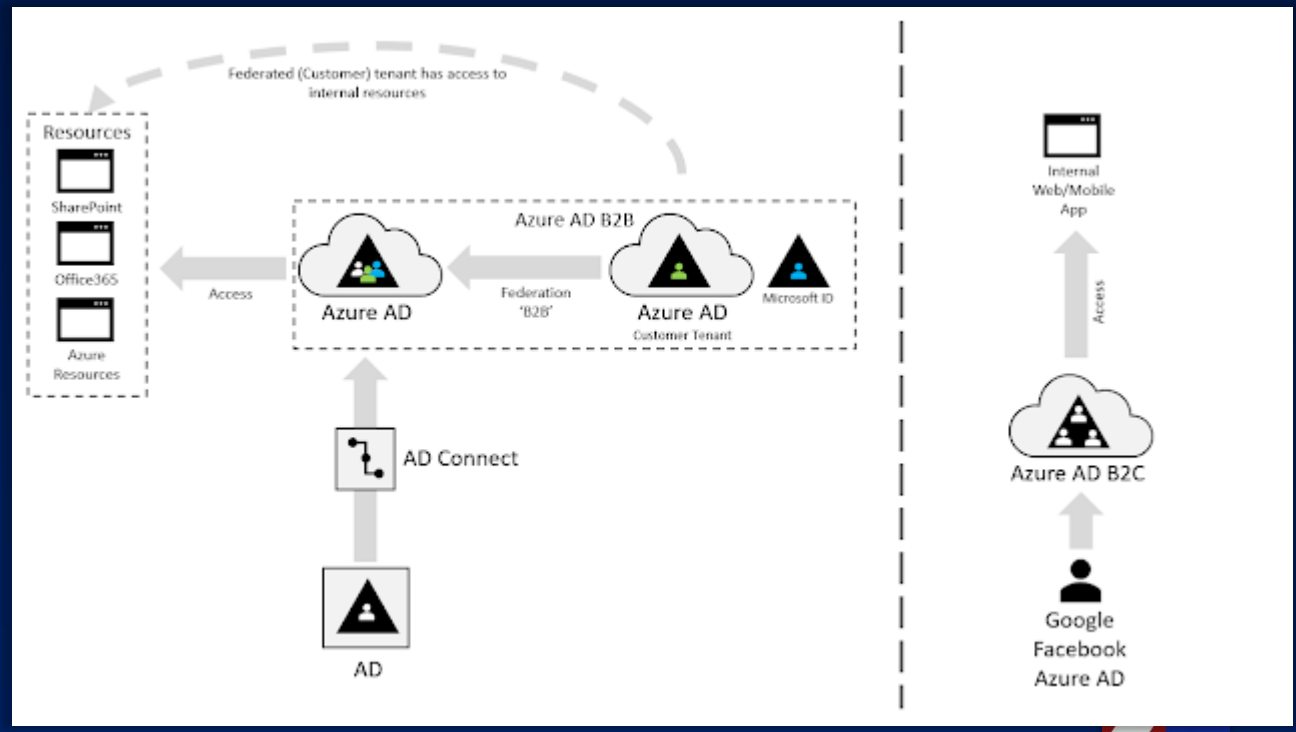
Exam Example in SC-900

Identity

[ ] is collaboration feature for communicating with external organizations, that let them appeared as guest/external users in our AAD.

A. AAD B2C
B. AAD B2B
C. AD DS
D. AD Conditional Access
E. Guest Inviting

Answer: **Azure Active Directory (AAD) Business-to-Business (B2B)**
Hint: **B2B** is sharing access to **company resources /** between organization, authenticated within **directory**/AAD.



Exam Example in SC-900

Identity

About Hybrid Identity:

1. Use Azure AD Connect to establish — Yes/No
2. Must require 2 tenants, Azure or M365, or both — Yes/No
3. Sync between AD DS and AAD — Yes/No

Answer: **Y/N/Y**

Hint: **Hybrid** means On-Prim (AD DS) syncing with Cloud (Azure AD), that use AAD Connect to sync from On-Prim to only one Cloud tenant.

Exam Example in SC-900

Identity

About Conditional Access policies:

1. Use Users as signals Yes/No
2. Use Device states as signals Yes/No
3. Apply policies even before 1st factor Authen Yes/No
4. Can trigger MFA when access specific apps/meet specific conditions Yes/No
5. Can trigger SSPS when access specific apps/meet specific conditions Yes/No

Answer: **Y/Y/N/Y/Y**

Hint: Cond.Access is access management = Authorization after 1st factor login/Authen

Exam Example in SC-900

Identity

About Conditional Access:

1. Always enable MFA in every case — Yes/No
2. Only affect users and devices joined in AAD — Yes/No
3. Can check location as signal — Yes/No

Answer: **N/N/Y**
Hint: MFA is optional (such as no need for AAD joined (company's) devices.
Affect all AD registered (BYOD) and joined (company own) devices, regardless of enrolled/onboard or not.
Can check location via IP and GPS.

Exam Example in SC-900

Identity

About Conditional Access:

1. Even Global Admin can still be applied under policies Yes/No
2. Policies would be applied even before users are authenticated Yes/No
3. Can check device platforms such as iOS/android as signal Yes/No
4. Can set to automatically assign roles to users Yes/No
5. Can force to use MFA when accessing specific app Yes/No

Answer: **Y/N/Y**

Hint: Cond.Access can control Global Admin, so beware!

Cond.Access is access management, **not privilege/role management**

Exam Example in SC-900

Identity

About Azure AD Role:

1. Can be assigned only one role per user Yes/No
2. Global Admin, Billing Admin, Security Reader are Azure AD Roles Yes/No
3. Can create your own custom roles with specific privileges Yes/No

Answer: **N/Y/Y**

Hint: **Azure AD Roles** are for access AD resources (user/group/app/SP) vs Azure Role (RBAC that specific to one resource such as Owner/Contributor), could be both built-in and custom roles, one user can be assigned many roles.

Exam Example in SC-900

Identity

About Azure AD:

1.	is the service on Azure Cloud	Yes/No
2.	is the service deployed on On-Premises	Yes/No
3.	is Identity Provider/Access Management service	Yes/No
4.	is also provided as a part of M365 subscription	Yes/No

Answer: **Y/N/Y/Y**

Hint: **Azure AD = On Cloud, AD DS = On-Prim,** Azure AD can provide both Identity and Access services, has O365 license that has much more feature than typical free license.

Exam Example in SC-900

Identity

Which agent you would use to sync user data, etc., from On-Premises AD DS up to Azure AD?

A. Azure Password Protection agent
B. Azure Information Protection agent
C. AD Pass-through Authentication server/agent
D. Azure AD Connect
E. AD Federation server

Answer: **Azure AD Connect**
Hint: AD **Connect**

Exam Example in SC-900

Identity

When register App in AAD, What the App would automatically be?

A. Users
B. Devices
C. Service Principal
D. Managed Identity
E. Security Principal

Answer: **Service Principal**
Hint: Service = **App**

Exam Example in SC-900

Identity

Which feature of Azure AD you can use to limit time window for user to get specific administrative privilege such as three-hours as security admin?

A. Conditional Access
B. Multi-factor Authentication
C. Enterprise Application
D. Privilege Identity Management
E. Identity Protection
F. Entitlement

Answer: **Privilege Identity Management**
Hint: PIM use to assign “limit time window” role as Just-In-Time (JIT) access.

Exam Example in SC-900

Identity

Windows Hello stores user's biometric data in …

A. Local Device
B. Azure AD
C. Windows Hello Server
D. AD DS
E. Azure KeyVault

Answer: **Local Device**
Hint: it is not sent outside device, so it is safe from data breach!

Exam Example in SC-900

Identity

Which feature would be enabled to all users when Security Default is turned on?

A. MFA
B. Password Protection
C. Identity Protection
D. Conditional Access
E. Privilege Identity Management

Answer: **MFA**

Hint: enable = **can** use (in this case, just force to regis MFA), but **not force to use!**

Exam Example in SC-900

Identity

Which two situations would be when Security Default is still turned on?

A. Every users must register MFA (within 14 days)
B. Every users must use MFA when signing in
C. Admins must use MFA when signing in
D. Every users must use Windows Hello for Business
E. Admins must use Windows Hello for Business

Answer: **A,C**
Hint: Security Default = force to **register**, and force **admin** to use

Exam Example in SC-900

Identity

Azure MFA use 3 authentication methods:

A. Email
B. SMS
C. Phone Call
D. Authenticator App
E. SAML
F. Security Question

Answer: **SMS/Phone/App**
Hint: Email/Question is for SSPR (Password Reset) only

Your company has a Microsoft 365 subscription.
The company does not permit users to enroll personal devices in mobile device management (MDM).

Users in the sales department have personal iOS devices.
You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.

The users must be prevented from backing up the app's data to iCloud.
What should you create?

A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
B. an app protection policy in Microsoft Endpoint Manager
C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
D. a device compliance policy in Microsoft Endpoint Manager

Answer: B, use App Protection in Intune

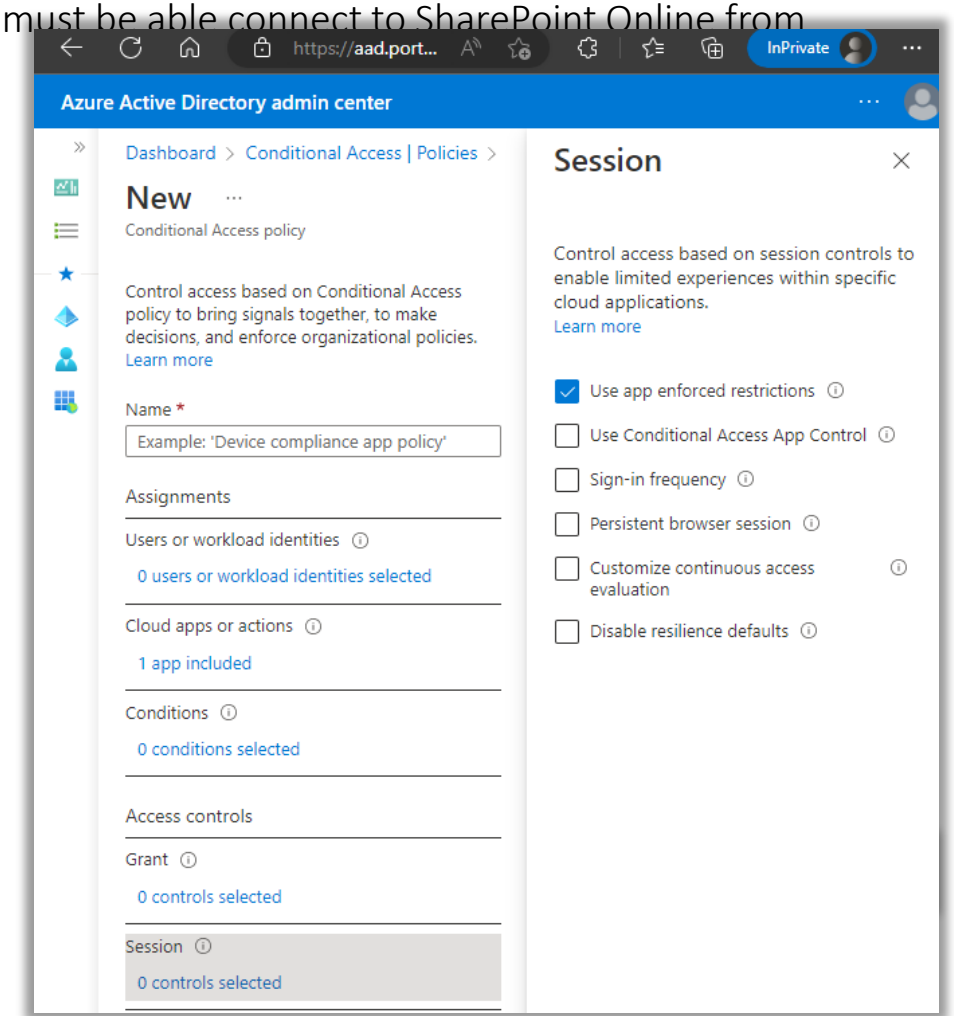
You can use Intune app protection policies independent, or even “not enrolled” of any mobile-device management (MDM) solution.

You have a Microsoft 365 tenant.
You need to implement a policy to enforce the following requirements:
☞ If a user uses a Windows 10 device that is NOT hybrid Azure Active Directory (Azure AD) joined, the user must be allowed to connect to Microsoft SharePoint
Online only from a web browser. The user must be prevented from downloading files or syncing files from SharePoint Online.
☞ If a user uses a Windows 10 device that is hybrid Azure AD joined, the user must be able connect to SharePoint Online from any client application, download files, and sync files.
What should you create?

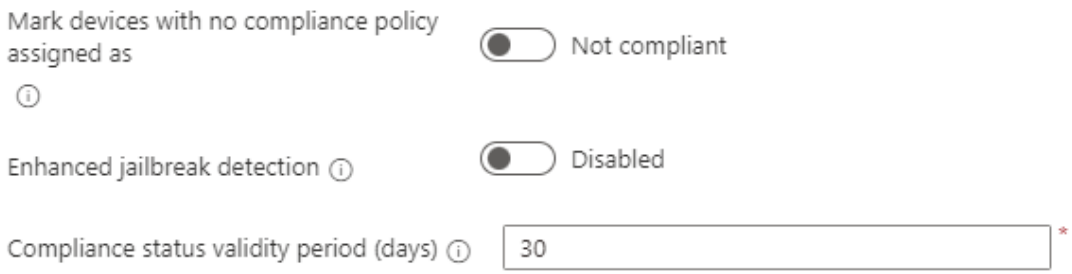
A. a conditional access policy in Azure AD that has Client apps conditions configured
B. a conditional access policy in Azure AD that has Session controls configured
C. a compliance policy in Microsoft Endpoint Manager that has the Device Properties settings configured
D. a compliance policy in Microsoft Endpoint Manager that has the Device Health settings configured

Answer: B "Session" controls in Cond.Acc

Use App Enforce Restriction for Office 365, Sharepoint, Exchange Online



The Compliance policy settings are configured as shown:



On February 25, 2020, you create the device compliance policies:

Name	Require BitLocker Drive Encryption (BitLocker)	Require Secure Boot	Mark device as not compliant	Assigned to
Policy1	Yes	No	5 days after noncompliance	Group1
Policy2	No	Yes	10 days after noncompliance	Group1, Group2

On March 1. 2020, users enroll Windows 10 devices as:

Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Answer: Y/Y/N

Grace period start when “enrolled” or “not compliant”