

A graphic element on the left side of the slide features a stylized map of Thailand. The map is composed of several overlapping triangles in shades of red, blue, and grey, creating a layered effect. The word "THAILAND" is overlaid on this graphic in large, white, sans-serif capital letters.

THAILAND

Cyber
Security



 Microsoft Security

Cloud SECURITY Intensive





Identity

Entra 
Intune 



SC-900

SECURITY
COMPLIANCE
IDENTITY

Azure AD Licenses

Free/O365/P1/P2

Different feature sets

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Default Directory | Overview

Azure Active Directory

Overview

Preview features

Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy

Add Manage tenants What's new

Microsoft Entra has a simpler, integrated experience for managing users and groups. [Microsoft Entra admin center \(Preview\)](#)

Overview Monitoring Properties Tutorials

Search your tenant

Basic information

Name	Default Directory
Tenant ID	31dd4bda-8730-47a3-8d1c-5af9179cf52
Primary domain	nol121hotmail.onmicrosoft.com
License	Azure AD Free

Alerts

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory > Licenses

Licenses | Licensed features

Default Directory - Azure Active Directory

Overview

Diagnose and solve problems

Manage

- Licensed features
- All products
- Self-service sign up products

Activity

Audit logs

Troubleshooting + Support

New support request

The current license plan for this Azure AD organization is Azure AD Free. For how to purchase/upgrade an Azure Active Directory paid license, or if you just want to know the features included in each edition, see [Azure Active Directory pricing page](#).

Search features Filter by category All features

Features	Description	Feature available
Directory objects	Object limit of 500,000 with Azure AD Free license; no limit for other licenses	Yes
Single Sign-On (SSO)	Support for unlimited apps with Azure AD Free	Yes
User provisioning	Learn more	Yes
Federated Authentication (ADFS or 3rd party IDP)	Learn more	Yes
User management (add/update/delete)	Learn more	Yes
Group management (add/update/delete)	Learn more	Yes
Device registration	Learn more	Yes
Cloud Authentication (Pass-Through Auth, Password Hash sync, Seamless SSO)	Learn more	Yes
Azure AD Connect sync (extend on-premises directories to Azure AD)	Learn more	Yes
Self-Service Password Change for cloud users	Learn more	Yes
Azure AD Join: desktop SSO and administrator bitlocker	Learn more	Yes



Azure AD Join: desktop SSO and administrator self-service password reset	Learn more	Yes
Password Protection (global banned password)	Learn more	Yes
Multifactor authentication for administrator roles	Learn more	Yes
Advanced security and usage reports	Learn more	Yes
Azure AD features for guest users	Learn more	Yes
Company branding (customization of logon and 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
Multifactor 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
Group access management	Learn more	Try Azure AD Premium Available in Azure AD for Office 365 / Azure AD Premium P1 / Azure AD Premium P2
Service Level Agreement (SLA)	Learn more	Try Azure AD Premium Available in Azure AD for Office 365 / Azure AD Premium P1 / Azure AD Premium P2
Service write-back (device objects two-way synchronization between on-premises directories 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



Azure AD Licenses

Free/O365/P1/P2

Different feature sets

		AD Premium P2
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

SC-900

SECURITY
COMPLIANCE
IDENTITY



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

Microsoft 365 admin center

Search results: 17 products

Search: 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

No need for any
M365 service to
sync Hybrid Identity

On-Premises + Cloud

= AD DS + AAD

use Azure AD Connect sync



SC-900

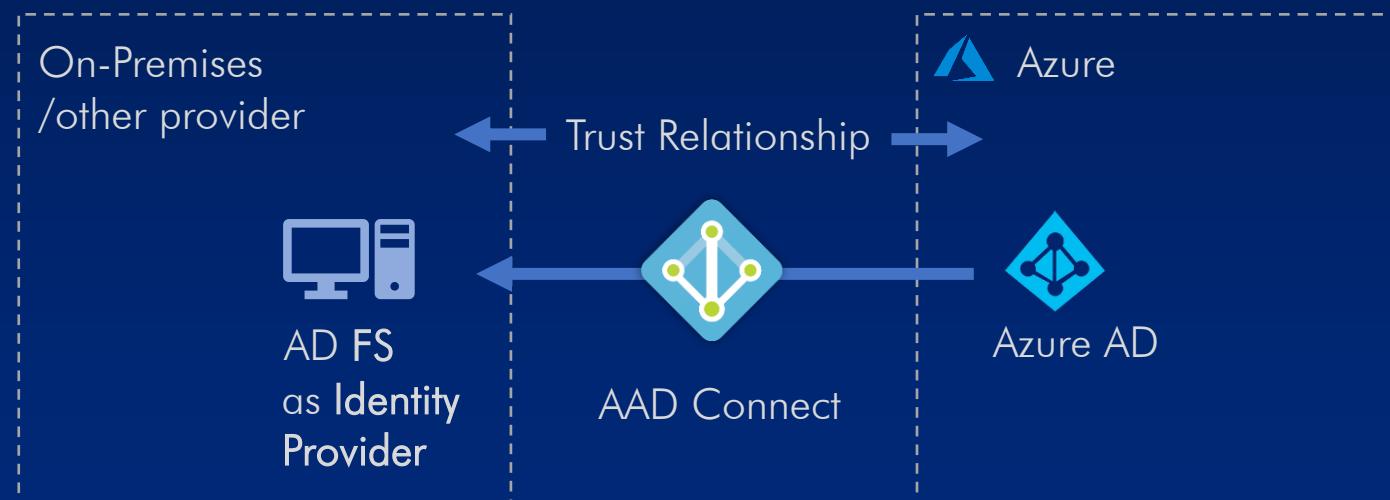
SECURITY
COMPLIANCE
IDENTITY



Federation

Trust Relationship

AD FS etc. as Identity Provider



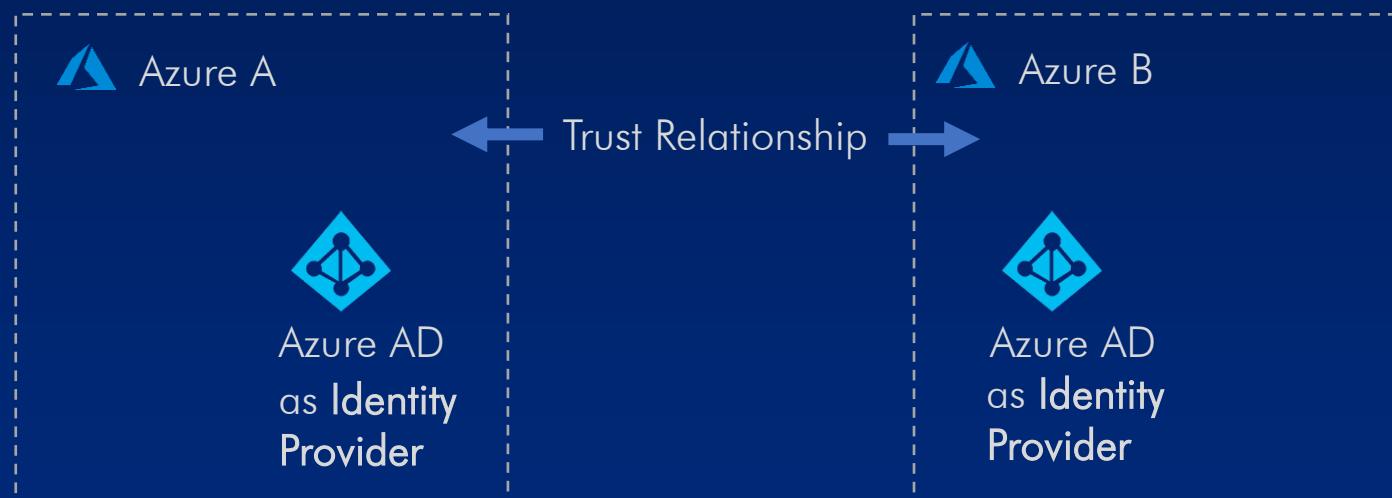
SC-900

SECURITY
COMPLIANCE
IDENTITY



B2B
(Business-to
-Business)

with Business Partner Azure
as External Users



SC-900

SECURITY
COMPLIANCE
IDENTITY



PIM (Privilege Identity Management)

no PIM (AAD P2 License)

The screenshot shows the Microsoft Azure portal interface under the 'Application administrator' section. A modal window displays a green checkmark and the message 'Successfully added assignments'. Below it, another message states 'Successfully added 2 assignments'. A tooltip at the bottom of the screen reads 'PIM: A privileged directory role was assigned outside of PIM'. The main pane shows a table of users assigned to roles, with two entries: 'DebraB' and 'Alex Wilber'. The table includes columns for Name, UserName, and Assignment details.

Limit time window privilege to complete tasks

Just In Time (JIT) access

with PIM (AAD P2 License)

The screenshot shows the Microsoft Azure portal interface under the 'Add assignments' section. It highlights the 'Setting' tab. Under 'Assignment type', the 'Active' radio button is selected. The 'Maximum allowed assignment duration' is set to 'permanent'. The 'Permanently assigned' checkbox is checked. The 'Assignment starts' date is '07/21/2022' and the 'Assignment ends' date is '01/17/2023'. A red box highlights the 'Assignment ends' field. At the bottom, there is a text input field for 'Enter justification' with the placeholder text 'ถ้าการไม่สำเร็จแล้วให้รีบแจ้ง ^_^'.

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 * Select Teams + groups

Group * SarahTest

Scope * All users

*Review type *Reviews Settings *Review + Create

Determine review stages, reviewers, and timeline below.

Multi-stage review *

Specify reviewers

Select reviewers *

Users or Groups *

Specify recurrence of review

Duration (in days) *

Review recurrence *

Start date *

End Never

End on specific date

End after number of occurrences

Home > Sarah AHA co.,ltd. > Roles and administrators >
New access review ...

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

Configure additional settings, including decision helpers and upon completion settings.

Upon completion settings

Auto apply results to resource

If reviewers don't respond

At end of review, send notification to

No sign-in within 30 days

Enable reviewer decision helpers

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



SC-900

SECURITY
COMPLIANCE
IDENTITY



AAD Role

Microsoft Azure

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

New custom role

All roles

Got feedback?

Basics Permissions Review + create

Roles created here will be available for assignment on other resources as well. [Learn more](#)

Name * ThaiCySec Test Custom Role

Description อะไรดีน้า

Baseline permissions Start from scratch Clone from a custom role

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

Global Admin, etc.

One User, can be many roles

Can create custom roles

Basics Permissions Review + create

Add permissions for this custom role. Currently, permissions for Application registrations and Enterprise applications are supported in custom roles. [Learn more](#)

Search by permission name or description

Permission	Description
<input checked="" type="checkbox"/> microsoft.directory/application... Read all properties (including privil...	
<input type="checkbox"/> microsoft.directory/application... Update all properties (including pri...	
<input type="checkbox"/> microsoft.directory/application... Update standard properties of applic...	
<input checked="" type="checkbox"/> microsoft.directory/application... Create application policies.	
<input type="checkbox"/> microsoft.directory/application... Create application policies, and cre...	
<input checked="" type="checkbox"/> microsoft.directory/application... Delete application policies.	



SC-900

SECURITY
COMPLIANCE
IDENTITY



MFA (Multi Factor Authentication)

The screenshot shows the "multi-factor authentication" settings page in the Azure portal. It includes sections for "users" and "service settings", "app passwords", "trusted ips", and "verification options". The "trusted ips" section contains the IP address "192.168.1.0/24". The "verification options" section lists four methods: "Call to phone" (unchecked), "Text message to phone" (checked), "Notification through mobile app" (checked), and "Verification code from mobile app or hardware token" (checked).

Additional verification

3 methods

SMS
Authenticator App
Phone Call



SC-900

SECURITY
COMPLIANCE
IDENTITY

AAD Identity Protection

User/Sign-in/Workload Risk Detection + export to 3rd party

The screenshot displays the Microsoft Azure Identity Protection interface across three browser tabs:

- Top Tab:** Shows the "User risk" configuration page for a "User risk remediation policy". It includes sections for "Policy Name" (User risk remediation policy), "Assignments" (Users, All users, User risk: Low and above), and "Controls" (Access, Block access).
- Middle Tab:** Shows the "Conditional Access > User risk level" configuration page. It includes sections for "Name" (ThaiSec User-Risk), "User risk level" (Not configured), "Sign-in risk level" (Not configured), and "Device platforms" (Not configured).
- Bottom Tab:** Shows the "Risky User Details - Microsoft Azure" page for user "Nol 121". It displays basic info (User: Nol 121, Roles: Limited admin, Username: nol121@nol121.onmicrosoft.com, User ID: 9853ec9e-d7c2-4700-9097-f017982564a8, Risk state: At risk, Risk level: Low), recent risky sign-ins, and actions (Reset password, Confirm user compromised, Dismiss user risk, Block user, Investigate with Azure Defender).

On the right side of the slide, there is a summary of the user's investigation priority score (0) and a chart showing alerts and activities contributing to the score over the last 7 days.

AAD Identity Protection

Home > Sarah AHA co.,ltd. > Security > Conditional Access >

New ...

Conditional Access policy

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

Name * ✓

Assignments

Users or workload identities [\(1\)](#)
0 users or workload identities selected

Cloud apps or actions [\(1\)](#)
No cloud apps, actions, or authentication contexts selected

Conditions [\(1\)](#)
2 conditions selected

Access controls

Grant [\(1\)](#)

Enable policy [Report-only](#)

[Create](#)

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

User risk level [\(1\)](#)
2 included

Sign-in risk level [\(1\)](#)
2 included

Device platforms [\(1\)](#)
Not configured

Locations [\(1\)](#)
High
Medium
Low

Client apps [\(1\)](#)
Not configured

Filter for devices [\(1\)](#)
Not configured

User risk level

Configure [\(1\)](#)

Sign-in risk level

Control user access to respond to specific sign-in risk levels. [Learn more](#)

Configure [\(1\)](#)

Sign-in risk level is generated based on all real-time risk detections.

Select the sign-in risk level this policy will apply to

High

Medium

Low

No risk

Grant

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

Block access

Grant access

Require multifactor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app

[See list of approved client apps](#)

Require app protection policy

[See list of policy protected client apps](#)

Require password change



Detect if password leak to public

Invoke MFA based on risk level (via Cond.Access)

SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED

Grant

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

Block access

Grant access

Require multifactor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app See list of approved client apps

Require app protection policy See list of policy protected client apps

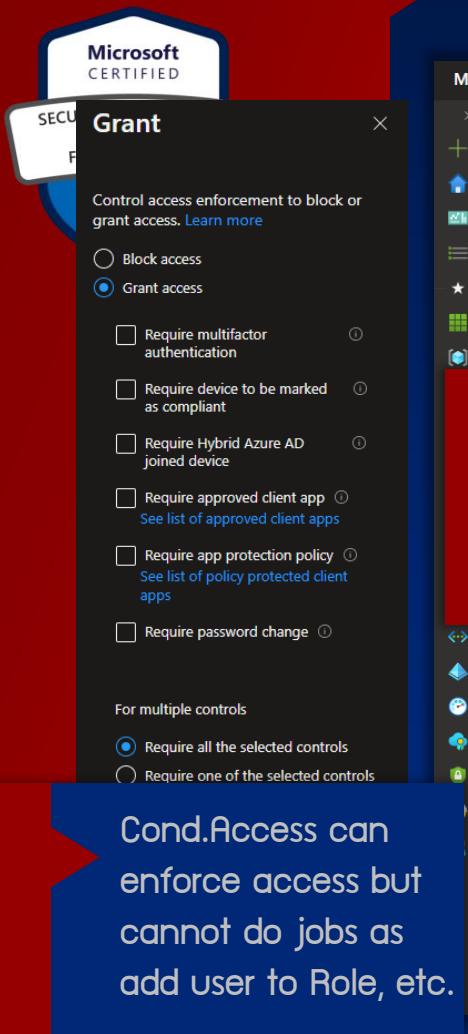
Require password change

For multiple controls

Require all the selected controls

Require one of the selected controls

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



Conditional Access

Microsoft Azure Search resources, services, and docs (G+)

Home > Conditional Access > New ... Conditional Access policy

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

Name *

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

2 conditions selected

Access controls

Grant 0 controls selected

Session 0 controls selected

For multiple controls

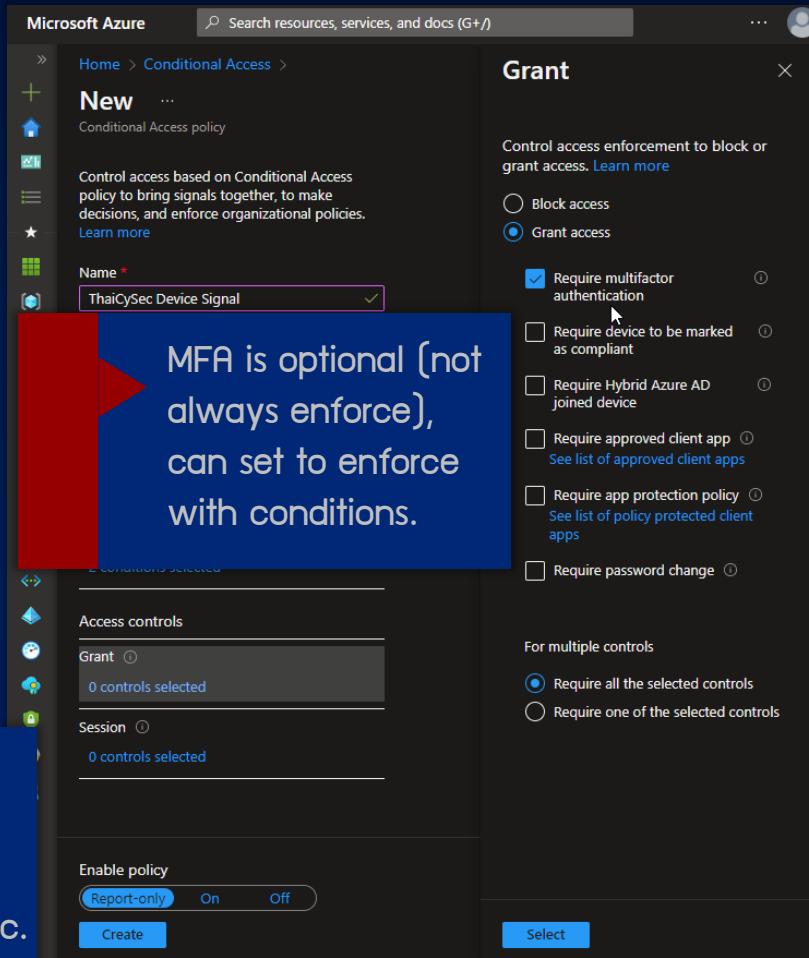
Require all the selected controls

Require one of the selected controls

Enable policy

Report-only On Off

Create **Select**



Authorization after 1st factor Authentication

Get Signals:

Users – even Global Admin
Device State Platform

Filter for devices

Configure a filter to apply policy to specific devices.

Configure Yes No

Devices matching the rule:

Include filtered devices in policy

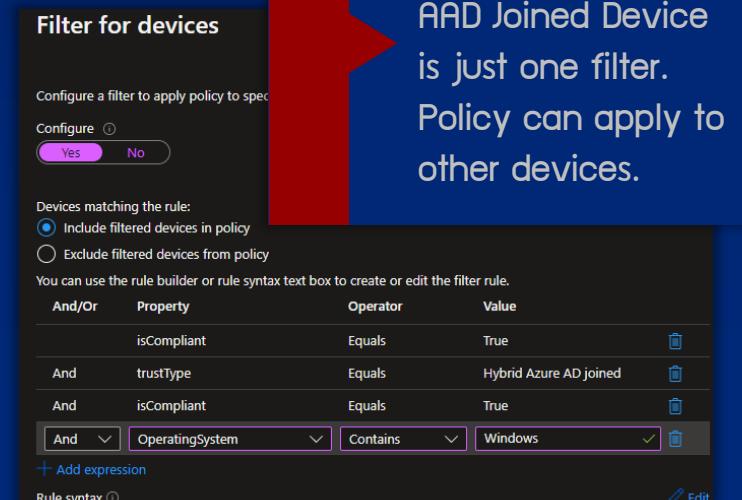
Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
And	isCompliant	Equals	True
And	trustType	Equals	Hybrid Azure AD joined
And	isCompliant	Equals	True
And	OperatingSystem	Contains	Windows

+ Add expression

Rule syntax Edit



Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure Yes No

Include Exclude

Any device

Select device platforms

Android

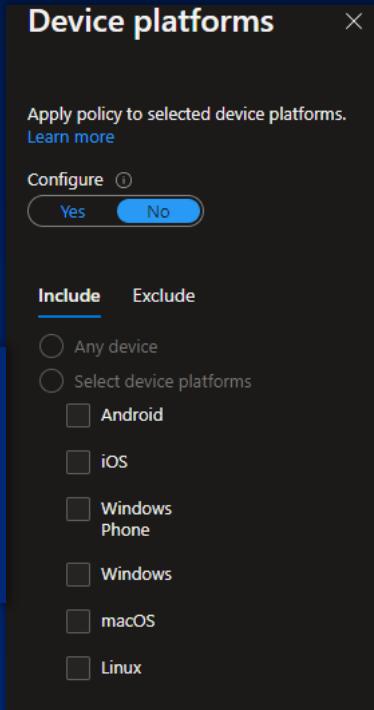
iOS

Windows Phone

Windows

macOS

Linux



SC-900

SECURITY
COMPLIANCE
IDENTITY



Conditional Access

New location (Countries)

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

Name *

Determine location by IP address (IPv4 only)

Determine location by IP address (IPv4 only)

Determine location by GPS coordinates

Search countries

Name

Afghanistan

Åland Islands

Albania

Algeria

American Samoa

Andorra

Angola

More Signal Named/Trust Location

Microsoft Azure Search resources, services, and docs (G+)

Home > Conditional Access

Conditional Access | Named locations

Named locations are used by Azure A Conditional Access policies. Learn more

Location type : All types

Name * My office

Mark as trusted location

Update location (IP ranges)

Upload Download Delete

Configure named location IPv4 and IPv6 ranges. Learn more

Location type : All types Trusted type : All types

Name Multifactor authentication trusted IPs IP ranges Yes

My office IP ranges Yes

THCS

A large red arrow points from the "My office" entry in the "Update location (IP ranges)" section down to the "Selected locations" dropdown in the "Conditional Access policy" section, indicating the connection between the two.

SC-900

SECURITY
COMPLIANCE
IDENTITY

App Regis

Become Service Principal

Sarah AHA co.,ltd. | App registrations

New registration Endpoints Troubleshooting Refresh Download

All applications Owned applications Deleted applications

Start typing a display name or application (client) ID to filter these results

1 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
AK akeakecheckstock	6268ee4e-da6c-4bab-bdb1-9fa91d9b2b93	12/20/2021	-

Overview Preview features Diagnose and solve problems Manage Users Groups External identities Roles and administrators Administrative units Enterprise applications Devices App registrations

Microsoft Azure Search resources, services, and docs (G+)

Home > Sarah AHA co.,ltd. > Security > Conditional Access > New

Conditional Access policy

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

Name * Example: 'Device compliance app policy'

Assignments

Users or workload identities 0 users or workload identities selected

Cloud apps or actions No cloud apps, actions, or authentication contexts selected

Select apps "Select apps" must be configured

Conditions

Select what this policy applies to

Cloud apps

Include Exclude

None

All cloud apps

Select apps

Select

None

Select at least one a

Selected items

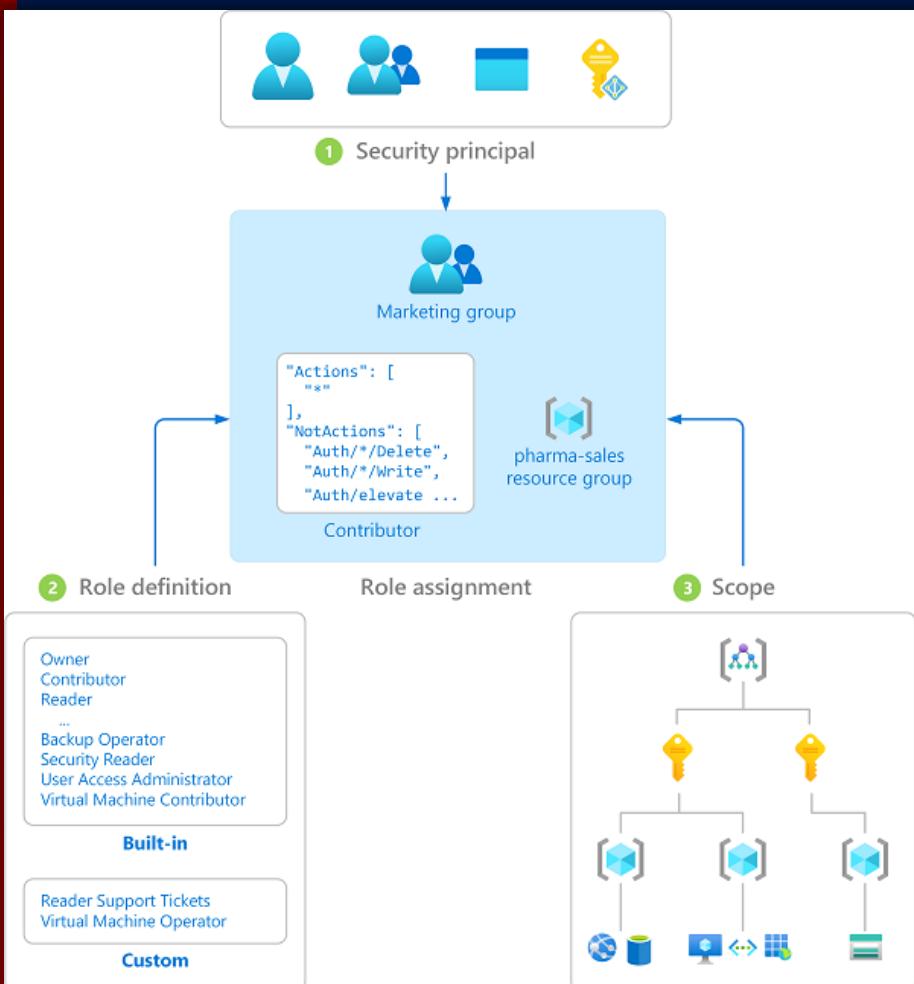
AK akeakecheckstock 6268ee4e-da6c-4bab-bdb1-9fa91d9b2b93	Remove
--	--------





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

=
Managed Identity Enterprise Application

The Managed Identity is an Enterprise Application within Azure AD, which can be used by an Azure Resource to authenticate to any service that supports Azure AD authentication, without having credentials in your code



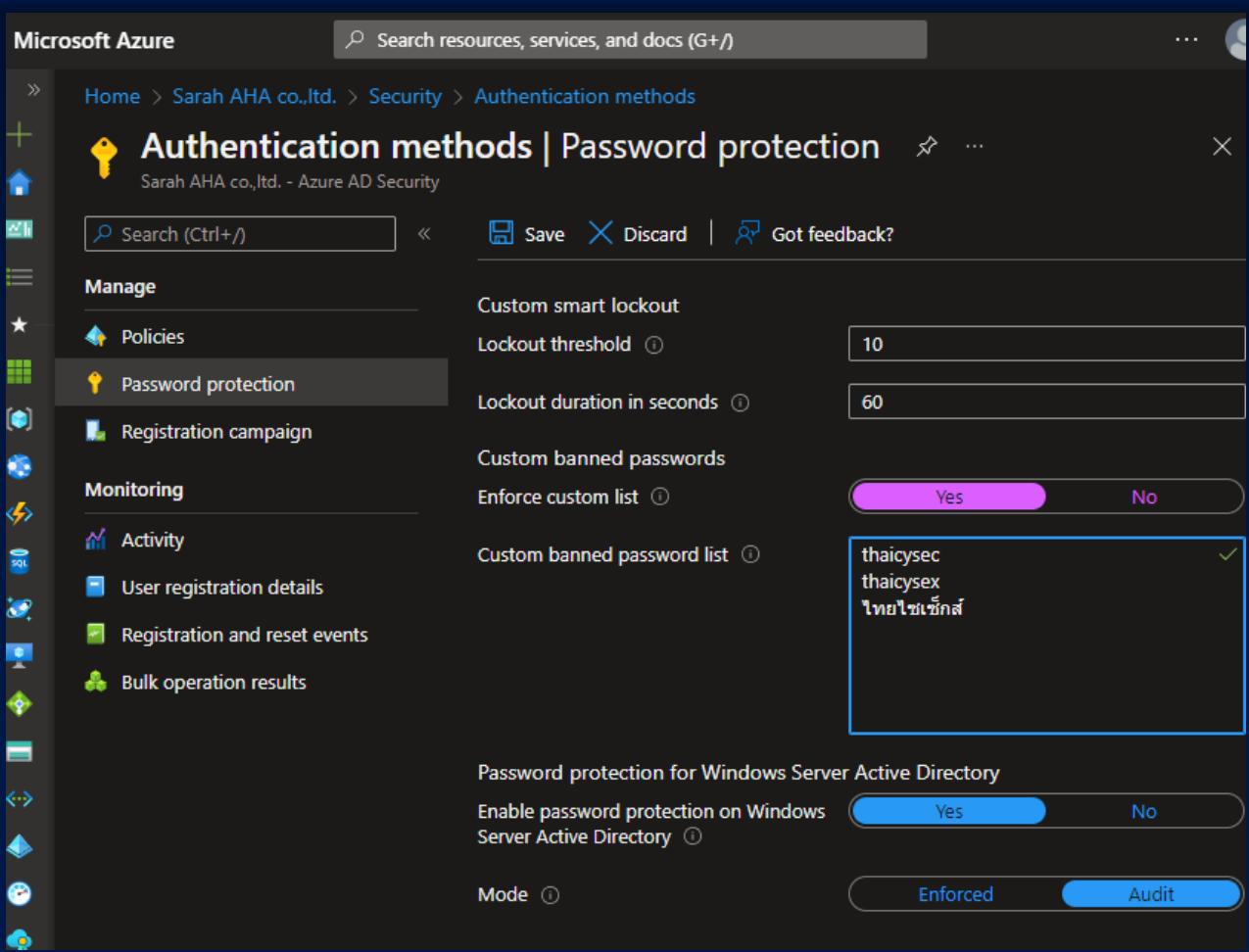
SC-900

SECURITY
COMPLIANCE
IDENTITY



Password Protection

Prevent using specific words



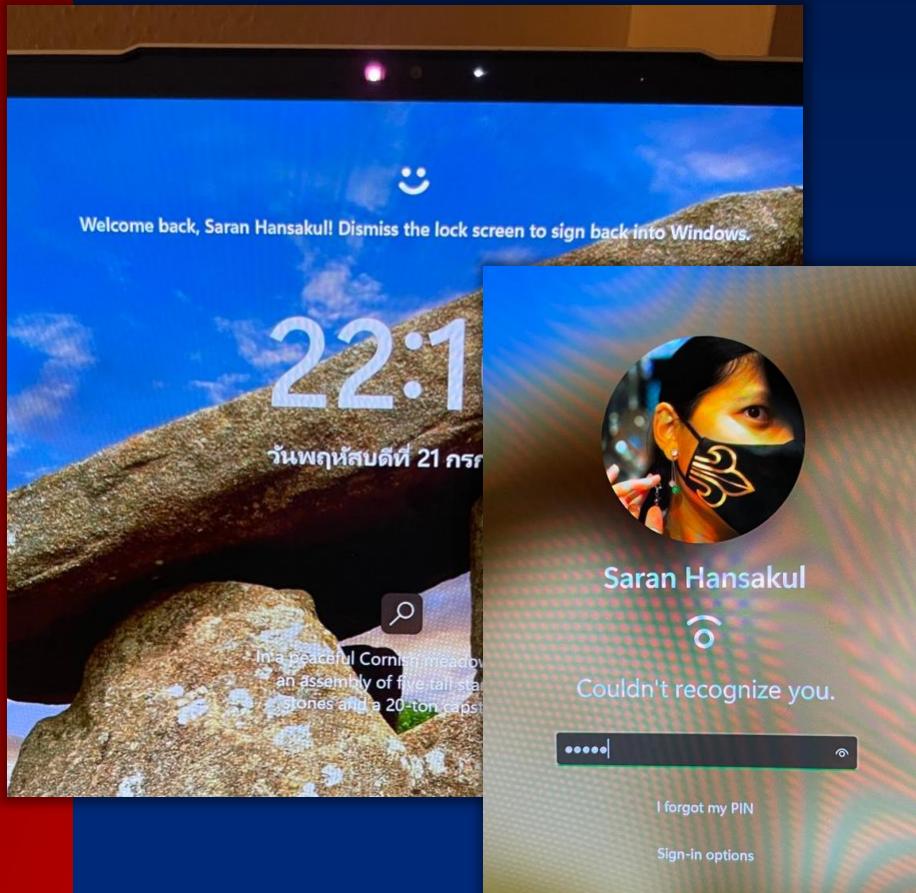
The screenshot shows the "Authentication methods | Password protection" page in the Microsoft Azure portal. The left sidebar lists "Manage" sections: Policies, Password protection (which is selected), Registration campaign, and "Monitoring", "Activity", "User registration details", "Registration and reset events", and "Bulk operation results". The main content area has a "Custom smart lockout" section with "Lockout threshold" set to 10 and "Lockout duration in seconds" set to 60. It also includes a "Custom banned passwords" section where the "Enforce custom list" switch is turned "Yes". A list of banned passwords is shown, with three entries highlighted: "thaicysec", "thaicysex", and "ไทยไซเบอร์". Below this is a "Password protection for Windows Server Active Directory" section with "Enable password protection on Windows Server Active Directory" set to "Yes" and "Mode" set to "Enforced".

SC-900

SECURITY
COMPLIANCE
IDENTITY



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)



SC-900

SECURITY
COMPLIANCE
IDENTITY

Security Default

Microsoft

Home > Default Directory

Default Directory | Properties

Azure Active Directory

Security Governance

Application proxy

Custom security attributes (Preview)

Licenses

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

User settings

Properties

Security

Monitoring

Sign-in logs

Audit logs

Provisioning logs

Log Analytics

Diagnostic settings

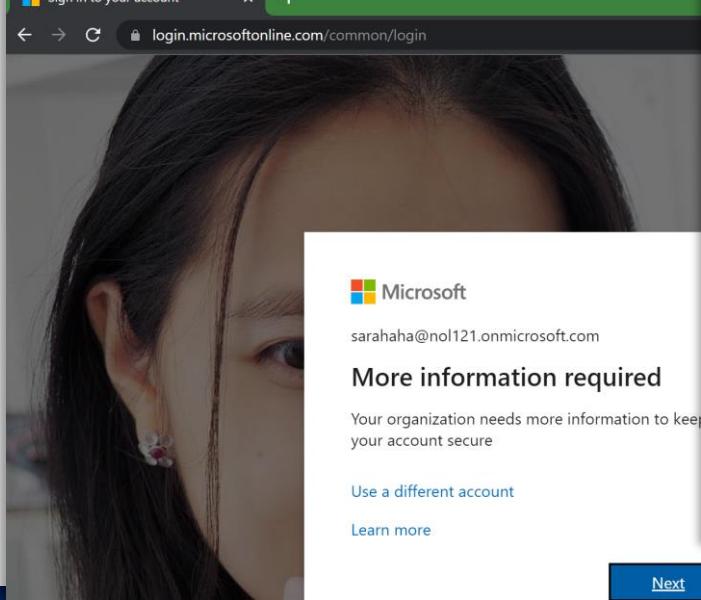
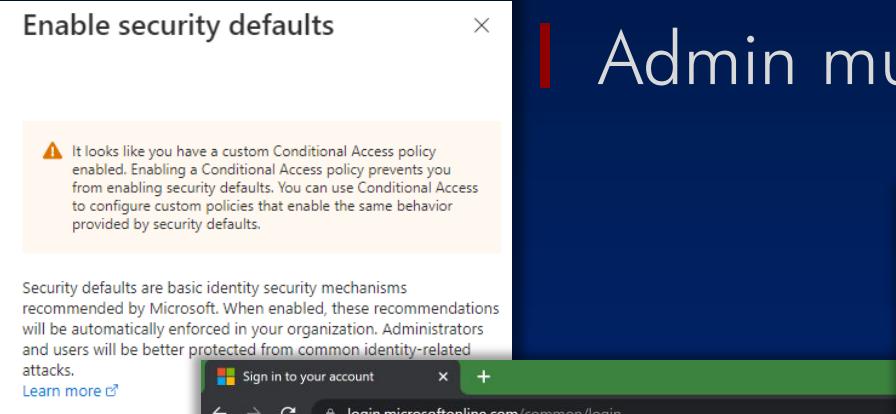
Workbooks

Usage & insights

Bulk operation results (Preview)

Troubleshooting + Support

Manage security defaults



Enable MFA (force everyone to regis MFA within 14 days)

Admin must use MFA

My Sign-Ins | Register | Microsoft

mysignins.microsoft.com

Incognito

Sarah AHA co.,ltd.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

You can prove who you are by texting a code to your phone.

What phone number would you like to use?

United States (+1) Enter phone number

Text me a code

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next



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

The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left, a sidebar menu includes "Endpoint security" (which is highlighted with a red box), "Conditional access" (also highlighted with a red box), and other options like "Reports", "Users", "Groups", "Tenant administration", and "Troubleshooting + support". The main content area is titled "Conditional Access | Policies" under "Azure Active Directory". It features a "Policies" section with a "+ New policy" button, and sections for "What is Conditional Access?", "Conditions", and "Controls". A table shows examples: "When any user is outside the company network" leads to "They're required to sign in with multi-factor authentication"; "When users in the 'Managers' group sign-in" leads to "They are required be on an Intune compliant or domain-joined device". There are also sections for "Get started" and "Interested in common scenarios?".



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

The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left, there's a navigation sidebar with options like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled 'Users | Sign-in logs'. It includes a search bar, download and export buttons, and a troubleshooting link. Below these are sections for 'Date' (Last 7 days), 'Show dates as: Local', and 'Add filters'. There are two tabs: 'User sign-ins (interactive)' and 'User sign-ins (non-interactive)'. The main table lists sign-in logs with columns for Date, Request ID, User, Application, Status, IP address, Location, Conditional Acc..., and Authentication r... . Each row contains a timestamp, a unique Request ID, the user's name (e.g., Nol 121), the application used (e.g., Azure Portal), the status (e.g., Success or Interrupted), the IP address, the location (e.g., Bangkok, Krung The...), the conditional access status (e.g., Not Applied), and the authentication method (e.g., Single-factor auth). The table has several rows of data.

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar includes links for Home, Conditional Access, Overview, Policies, Insights and reporting (which is highlighted in grey), Diagnose and solve problems, Manage, Monitoring, Sign-in logs, Audit logs, and Troubleshooting + Support. The main content area is titled 'Conditional Access | Insights and reporting' under 'Azure Active Directory'. It features a 'Sign-in events - Total' section with a search bar and a table of sign-in events. The table has columns for TimeGenerated, UserPrincipalName, AppDisplayName, and ConditionalAccessStatus. The data shows multiple entries from November 22, 2022, at various times, all associated with the user 'nol121@nol121.onmicrosoft.com' and the application 'Azure Portal', with the status 'notApplied'. The entire table is highlighted with a blue box.



Intune

Compliance Policy
Grace Period

Grace Period = Days after “noncompliance”

Start when “enrolled” or “not compliant”

Default is 0day = Immediately

https://endpoint.microsoft.com/#view/Microsoft_Intune_DeviceCompliance

Microsoft Endpoint Manager admin center

Home > Devices | Compliance policies > Compliance policies | Policies >

Windows 10/11 compliance policy

Windows 10 and later

Basics Compliance settings Actions for noncompliance Assistant

Specify the sequence of actions on noncompliant devices

Action	Schedule (days after noncompliance) ⓘ	Message template
Mark device noncompliant	10 days	
Send email to end user	1 days	Selected
Add device to retire list	Immediately	



Intune

Devices

Joined vs Registered

<input type="checkbox"/> Name	Enabled	OS	Version	Join Type
<input type="checkbox"/> SARAHAMA-LENOVO	Yes	Windows	10.0.22623.891	Azure AD registered
<input type="checkbox"/> iPad	Yes	iPad	15.0.2	Azure AD registered
<input type="checkbox"/> 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

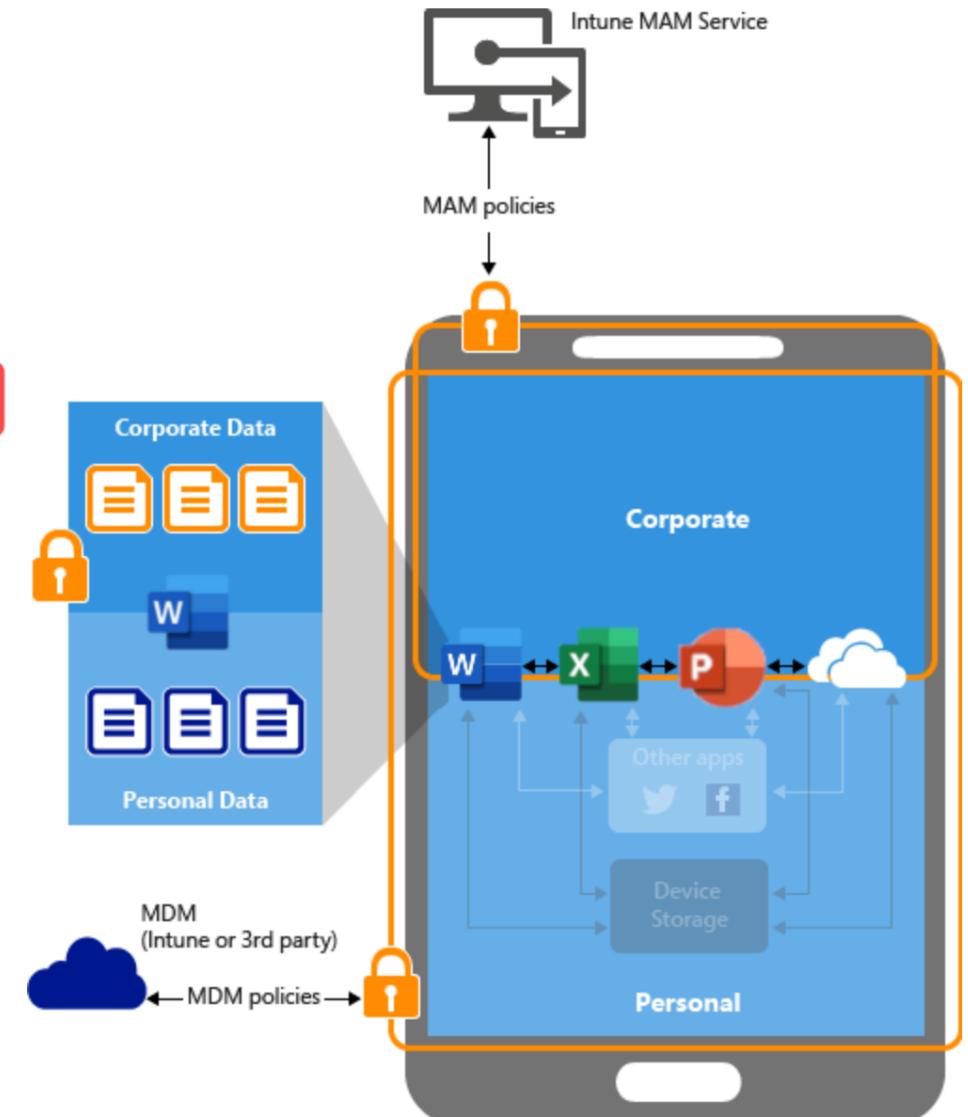
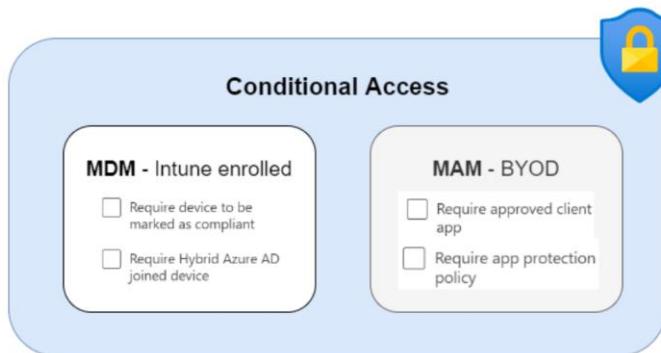
Remote Wipe for all Data (even personal)



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

Microsoft Endpoint Manager admin center

Home > Apps | App protection policies > Create policy

Action Not Allowed

Your organization only allows you to transfer its data to other managed apps.

OK

App Access Blocked

To access your data associated with account kenny@emskings.com, your organization requires this app to run on an iOS model allowed by your IT admin. You can remove this account from the app, or go back.

Remove Account

Go Back

Basics Apps Data protection Access requirement

This group includes the Data Loss Prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps.

Data Transfer

Backup org data to iTunes and iCloud backups

Send org data to other apps

Allow Block

None

Basics Apps Data protection Access requirements

Keyboard restrictions will apply to all areas of an app. Personal accounts for apps that support multiple identities will be affected by this restriction. [Learn more](#).

Encryption

Encrypt org data

Require Not required

Functionality

Sync policy managed app data with native apps or add-ins

Allow Block

Printing org data

Allow Block

Restrict web content transfer with other apps

Microsoft Edge

Jailbroken/rooted devices

Min OS version

Max OS version

Device model(s)

Max allowed device threat level

Primary MTD service

Value Action

Require

Numeric

Allow

4

Allow

Simple PIN

Select minimum PIN length

Touch ID instead of PIN for access (iOS 8+/iPadOS)

mvp skill change the world by contributions

M>

THCS

Spark Tech Thailand



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 😞)

Group type *

Security groups are used to give group members access to applications, resources and assign licenses. Group members can be users, devices, service principals, and other groups.

Microsoft 365 groups are used for collaboration, giving members access to a shared mailbox, calendar, files, SharePoint site, and so on. Group members can only be users.

Microsoft Endpoint Manager admin center

Home > Apps | App protection policies > Intune App Protection | Properties >

Edit policy

TestAssignGroup

① Assignments ② Review + save

Included groups

Add groups

Groups

SarahAkeakeDeviceTest

Total count of Azure AD security group members including direct and nested members. User count includes both licensed and unlicensed user objects and device count includes both managed and unmanaged devices. A membership count is not displayed for "All users" and "All devices" as they are Intune virtual groups.

Group Members ⓘ

1 devices, 0 users Remove

learn.microsoft.com/en-us/mem/intune/a...

⚠ Note

App protection policies can only be applied to groups that contains users, not groups that contain devices.

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

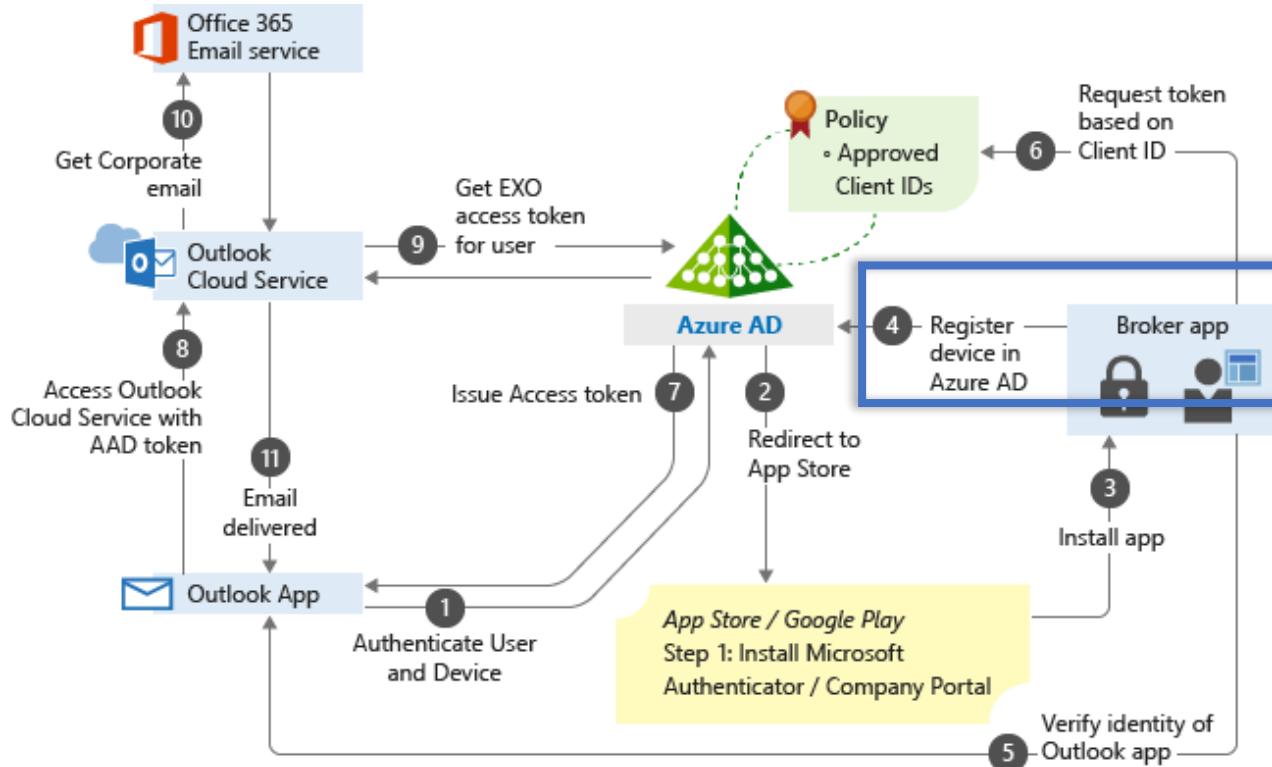


Intune

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



Microsoft Endpoint Manager admin center

All services > Endpoint security | Conditional access

New ...

Conditional Access policy

Learn more

Name * Device compliance App Policy ✓

Assignments

Users or workload identities ⓘ 0 users or workload identities selected

Cloud apps or actions ⓘ No cloud apps, actions, or authentication contexts selected

Conditions ⓘ 0 conditions selected

Access controls

Grant ⓘ 0 controls 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 (Preview) ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client ⓘ

Device must use policy protected apps. [Learn more](#)

Require app protection policy

See list of policy protected client apps

Require password change ⓘ



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

Azure Active Directory admin center

Dashboard > Conditional Access | Policies >

New Conditional Access policy

Select what this policy applies to: Cloud apps

Include Exclude

None

All cloud apps

Select apps

Edit filter (Preview)
None

Select
Office 365 SharePoint Online and 2 more

Office 365 ...
Office 365 Exchange Onli...
Office 365 SharePoint Onl...

⚠️ Selecting SharePoint Online will also affect apps such as Microsoft Teams, Planner, Delve, MyAnalytics, and Newsfeed.

⚠️ Selecting Office 365 Exchange Online will also affect apps such as OneDrive and Teams.

New Conditional Access policy

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

Name * Example: 'Device compliance app policy'

Assignments

Users or workload identities 0 users or workload identities selected

Cloud apps or actions 1 app included

Conditions 0 conditions selected

Access controls

Grant 0 controls selected

Session 0 controls selected

Session

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

Use app enforced restrictions ⓘ

Use Conditional Access App Control ⓘ

Sign-in frequency ⓘ

Persistent browser session ⓘ

Access Denied

Due to organizational policies, you can't access this resource from this untrusted device

Here are a few ideas:
 Please contact your organization.

If this problem persists, contact your support team and include these technical details:
Correlation ID: 300fae9a-50a0-7000-2280-2a523ab5ba8f
Date and Time: [redacted]
Issue Type: U

Unmanaged devices

ⓘ We will automatically change the "Apps that don't use modern authentication" setting to block access (because these apps can't enforce this device-based restriction).

The setting you select here will apply to all users in your organization. [Learn more](#). To customize conditional access policies, save your selection and go to the Azure AD admin center.

Allow full access from desktop apps, mobile apps, and the web

Allow limited, web-only access

Block access

If you don't want to limit or block access organization-wide, you can do so for specific sites. [Learn how](#)

Save Cancel



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

Name *
App control test

Assignments

Users or workload identities ①
0 users or workload identities selected

Cloud apps or actions ①
No cloud apps, actions, or authentication contexts selected

Conditions ①
0 conditions selected

Access controls

Grant ①
0 controls selected

Session ①
0 controls selected

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

Use Conditional Access App Control
Monitor only (Preview)
Monitor only (Preview)
Block downloads (Preview)
Use custom policy...
scenarios.

Microsoft 365 Defender

Policies > Create access policy

Create access policy

Access policies provide you with real-time monitoring and control over user logins to your cloud apps.

Policy name *

Policy severity * Category * Access control

Description

You don't have any apps deployed with Conditional Access App Control. Go to the Conditional Access App Control page to deploy an app.



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.

The screenshot shows the Microsoft 365 Defender Threat Explorer interface. On the left, there's a navigation bar with 'Assets', 'Identities', 'Email & collaboration', 'Investigations', and 'Explorer' (which is selected and highlighted with a blue border). In the center, there's a main area titled 'Explorer' with tabs for 'All email', 'Malware', 'Phish', 'Campaigns', and 'Content Malware'. At the top right of this area, there's a 'MDE Settings' button. Below the main area, there's a 'Microsoft Defender Security Center' section with a 'Settings' menu. Under 'General', there's a toggle switch labeled 'Off' for 'Microsoft Defender for Identity integration'. Under 'Advanced features', there's a toggle switch labeled 'On' for 'Office 365 Threat Intelligence connection'. A red arrow points to the 'Advanced features' section, and a red box highlights the 'On' status of the 'Office 365 Threat Intelligence connection' toggle.

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.

Select Technique

Select the social engineering technique you want to use with this simulation. We've curated these from the MITRE Attack framework. Depending on your selection, you will be able to use certain types of payloads.

- **Credential Harvest**
In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a web site, the website often...
[View details of Credential harvest](#)
 - **Malware Attachment**
In this type of technique, a malicious actor creates a message, with an attachment added to the message. When the target opens the attachment, typically some arbitrary code such as a macro...
[View details of Malware attachment](#)
 - **Link in Attachment**
In this type of technique, which is a hybrid of a Credential Harvest and Malware Attachment, a malicious actor creates a message, with a URL in an attachment, and then inserts the attachment into the message. When the target opens the attachment, they are represented with a URL in the actual attachment...
[View details of Link in attachment](#)
 - **Link to Malware**
In this type of technique, a malicious actor creates a message, with an attachment added to the message. However instead of directly



3 Attack

⚠ You must enable multi-factor authentication (MFA) to schedule or terminate attacks. [Learn more about enabling MFA.](#)

Next

Save and close

Cance



Exam Example in SC-900



Identity

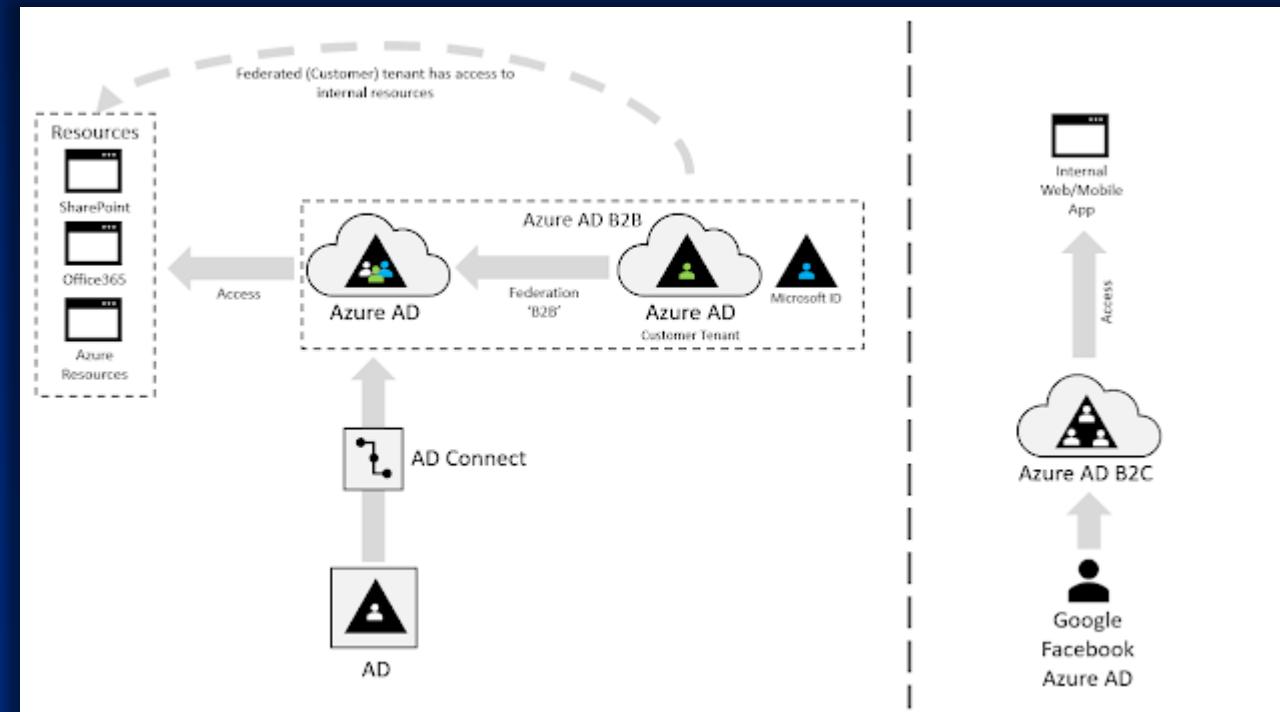
- A. AAD B2C
- B. AAD B2B**
- C. AD DS
- D. AD Conditional Access
- E. Guest Inviting

Answer: Azure Active Directory (AAD)

Business-to-Business (B2B)

Hint: B2B is sharing access to company resources / between organization, authenticated within directory/AAD.

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





About Hybrid Identity:

1. Use Azure AD Connect to establish
2. Must require 2 tenants, Azure or M365, or both
3. Sync between AD DS and AAD

Yes/No

Yes/No

Yes/No

Answer: Y/N/Y

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



About Conditional Access policies:

1. Use Users as signals
2. Use Device states as signals
3. Apply policies even before 1st factor Authen
4. Can trigger MFA when access specific apps/meet specific conditions
5. Can trigger SSPS when access specific apps/meet specific conditions

Yes/No
Yes/No
Yes/No
Yes/No
Yes/No
Yes/No

Answer: Y/Y/N/Y/Y

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



About Conditional Access:

1. Always enable MFA in every case
2. Only affect users and devices joined in AAD
3. Can check location as signal

Yes/No
Yes/No
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.



About Conditional Access:

1. Even Global Admin can still be applied under policies
2. Policies would be applied even before users are authenticated
3. Can check device platforms such as iOS/android as signal
4. Can set to automatically assign roles to users
5. Can force to use MFA when accessing specific app

Yes/No
 Yes/No
 Yes/No
 Yes/No
 Yes/No

Answer: Y/N/Y

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

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



About Azure AD Role:

1. Can be assigned only one role per user
2. Global Admin, Billing Admin, Security Reader are Azure AD Roles
3. Can create your own custom roles with specific privileges

Yes/No
Yes/No
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
2. is the service deployed on On-Premises
3. is Identity Provider/Access Management service
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-Prem**, Azure AD can provide both Identity and Access services, has O365 license that has much more feature than typical free license.



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.



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!



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!**



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



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 to 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 screenshot shows the Azure Active Directory admin center with the URL https://aad.portal.azure.com/. The page is titled "Conditional Access | Policies". A new policy is being created, named "New Conditional Access policy". The "Session" tab is selected. The "Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies." section is visible. Under "Assignments", there are sections for "Users or workload identities" (0 users or workload identities selected) and "Cloud apps or actions" (1 app included). Under "Conditions", 0 conditions are selected. Under "Access controls", "Grant" is set to 0 controls selected. Under "Session", 0 controls are selected. On the right, a sidebar provides information about session controls and links to learn more.



The Compliance policy settings are configured as shown:

Mark devices with no compliance policy assigned as

Not compliant

(i)

Enhanced jailbreak detection

Disabled

Compliance status validity period (days)

30

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.	<input type="radio"/>	<input type="radio"/>
On March 6, 2020, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On March 12, 2020, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer: Y/Y/N

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