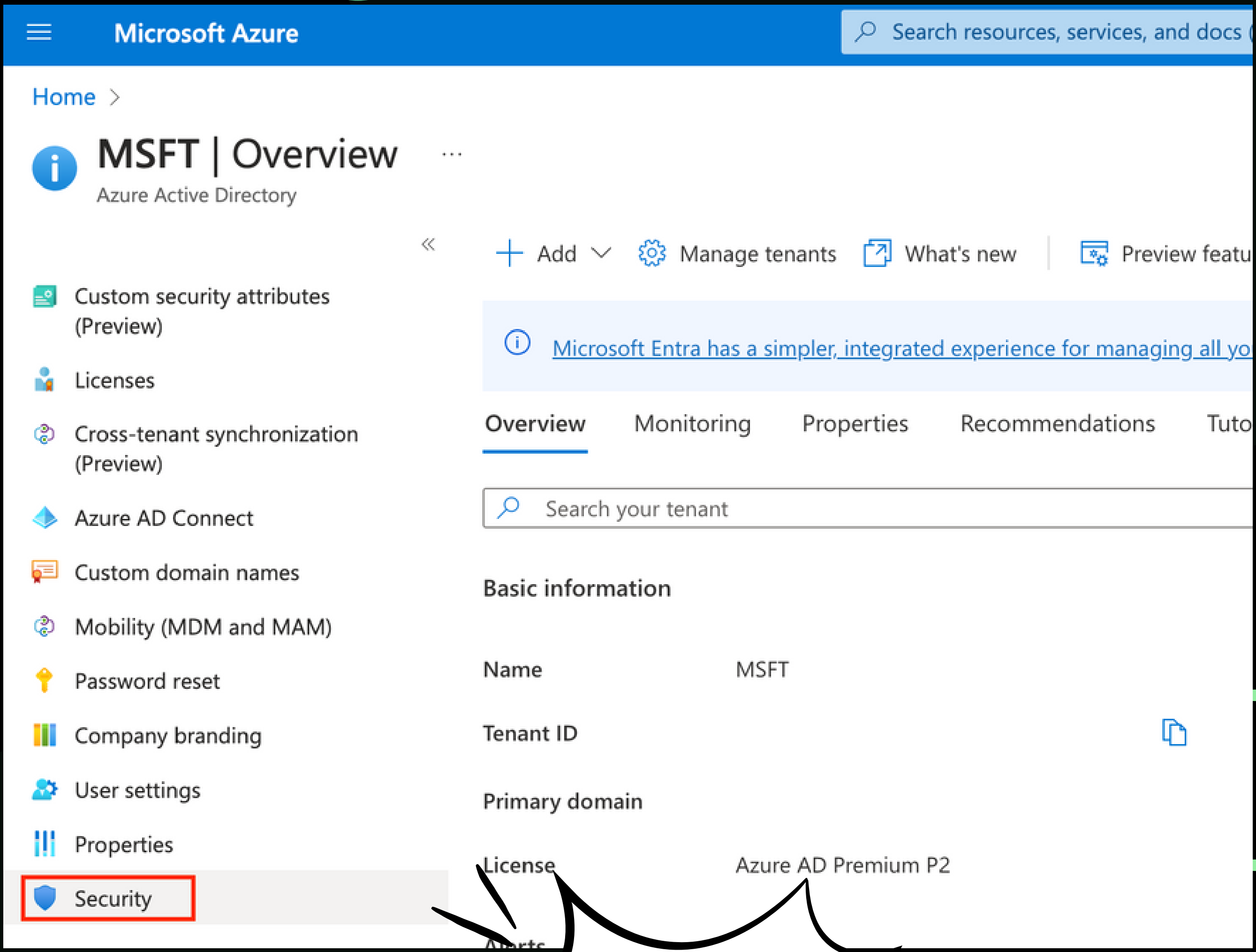
JIADONG CHEN

USERS' BEHAVIOR IS TYPICALLY TRACKABLE, AND IF IT DEVIATES FROM THE NORM, IT MAY BE RISKY TO GRANT THEM ACCESS WITHOUT ADDITIONAL SECURITY MEASURES, SUCH AS BLOCKING OR REQUIRING MULTIFACTOR AUTHENTICATION.

STEP BY STEP

ENABLE SIGN-IN RISK-BASED MULTIFACTOR AUTHENTICATION WITH CONDITIONAL ACCESS POLICY

JIADONG CHEN



Microsoft Azure

Search resources, services, and docs

Home >

MSFT | Overview

Azure Active Directory

- Custom security attributes (Preview)
- Licenses
- Cross-tenant synchronization (Preview)
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security

+ Add | Manage tenants | What's new | Preview featu

Microsoft Entra has a simpler, integrated experience for managing all yo

Overview | Monitoring | Properties | Recommendations | Tuto

Search your tenant

Basic information

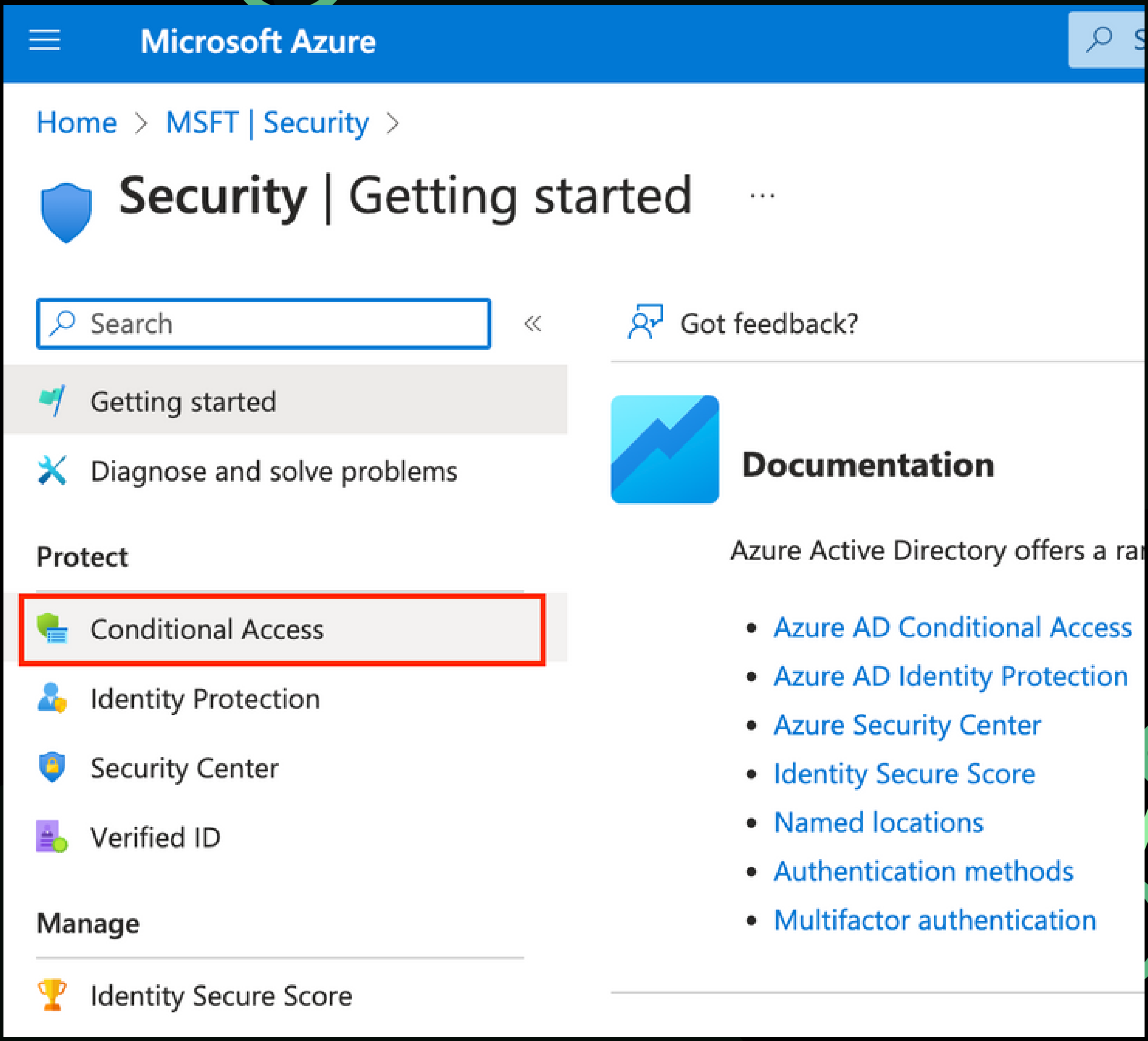
Name	MSFT
Tenant ID	
Primary domain	
License	Azure AD Premium P2

Alerts

Azure AD Premium P2 licenses are needed to create Conditional Access policies incorporating Azure AD Identity Protection sign-in risk detections.

BROWSE TO AZURE ACTIVE DIRECTORY > SECURITY > CONDITIONAL ACCESS.

JIADONG CHEN



Security | Getting started ···

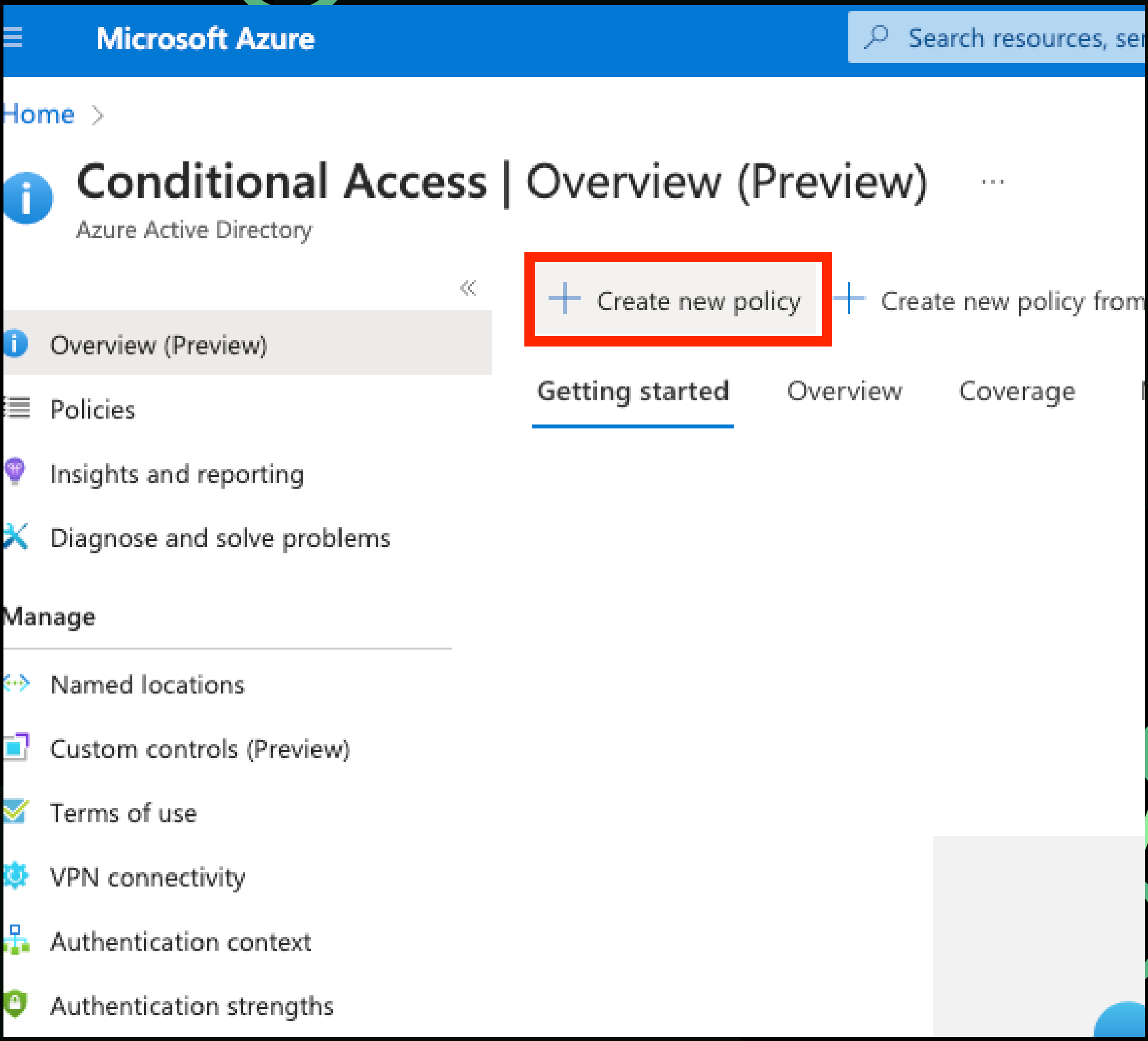
Documentation

Azure Active Directory offers a ra

- Azure AD Conditional Access
- Azure AD Identity Protection
- Azure Security Center
- Identity Secure Score
- Named locations
- Authentication methods
- Multifactor authentication

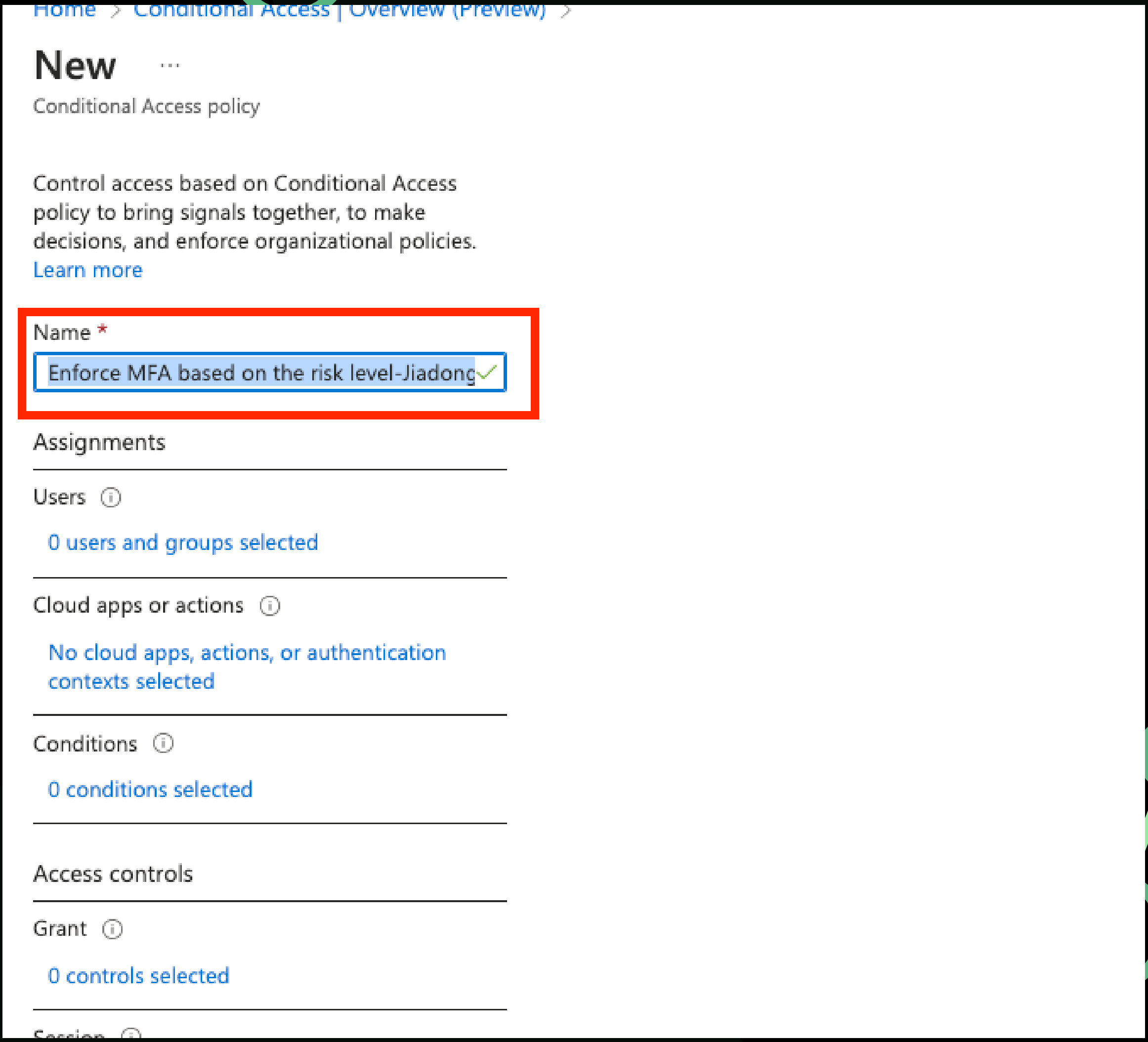
BROWSE TO AZURE ACTIVE DIRECTORY > SECURITY > CONDITIONAL ACCESS.

JIADONG CHEN



CLICK CREATE NEW POLICY.

JIADONG CHEN



Home > Conditional Access | Overview (Preview) >

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 *

Enforce MFA based on the risk level-Jiadong ✓

Assignments

Users ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

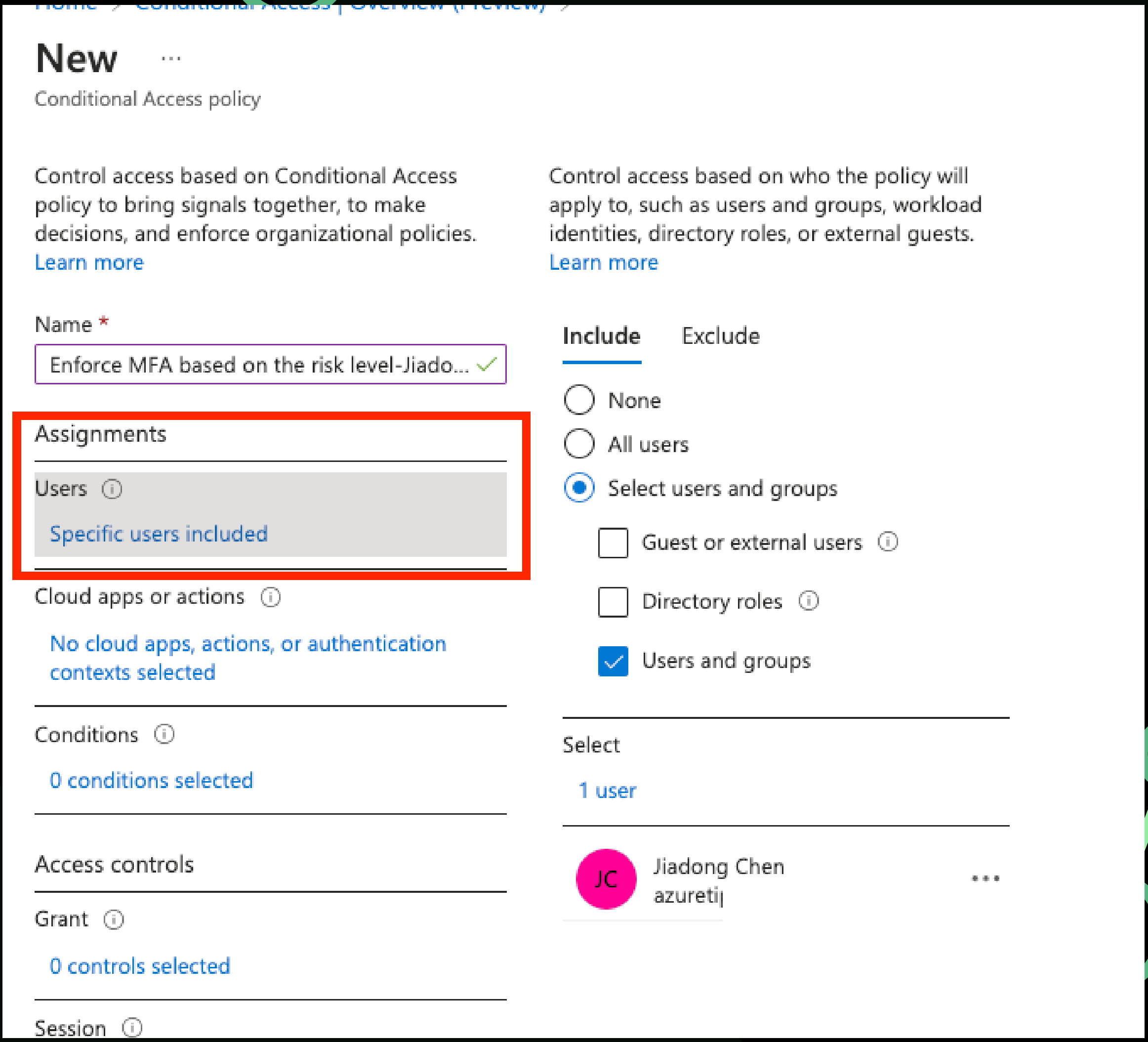
Grant ⓘ

0 controls selected

Session ⓘ

GIVE YOUR POLICY A NAME.

JIADONG CHEN



Home > Conditional Access | Overview (Preview) >

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 *

Enforce MFA based on the risk level-Jiado... ✓

Assignments

Users ⓘ

Specific users included

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

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

Include   Exclude

○ None

○ All users

● Select users and groups

□ Guest or external users ⓘ

□ Directory roles ⓘ

☑ Users and groups

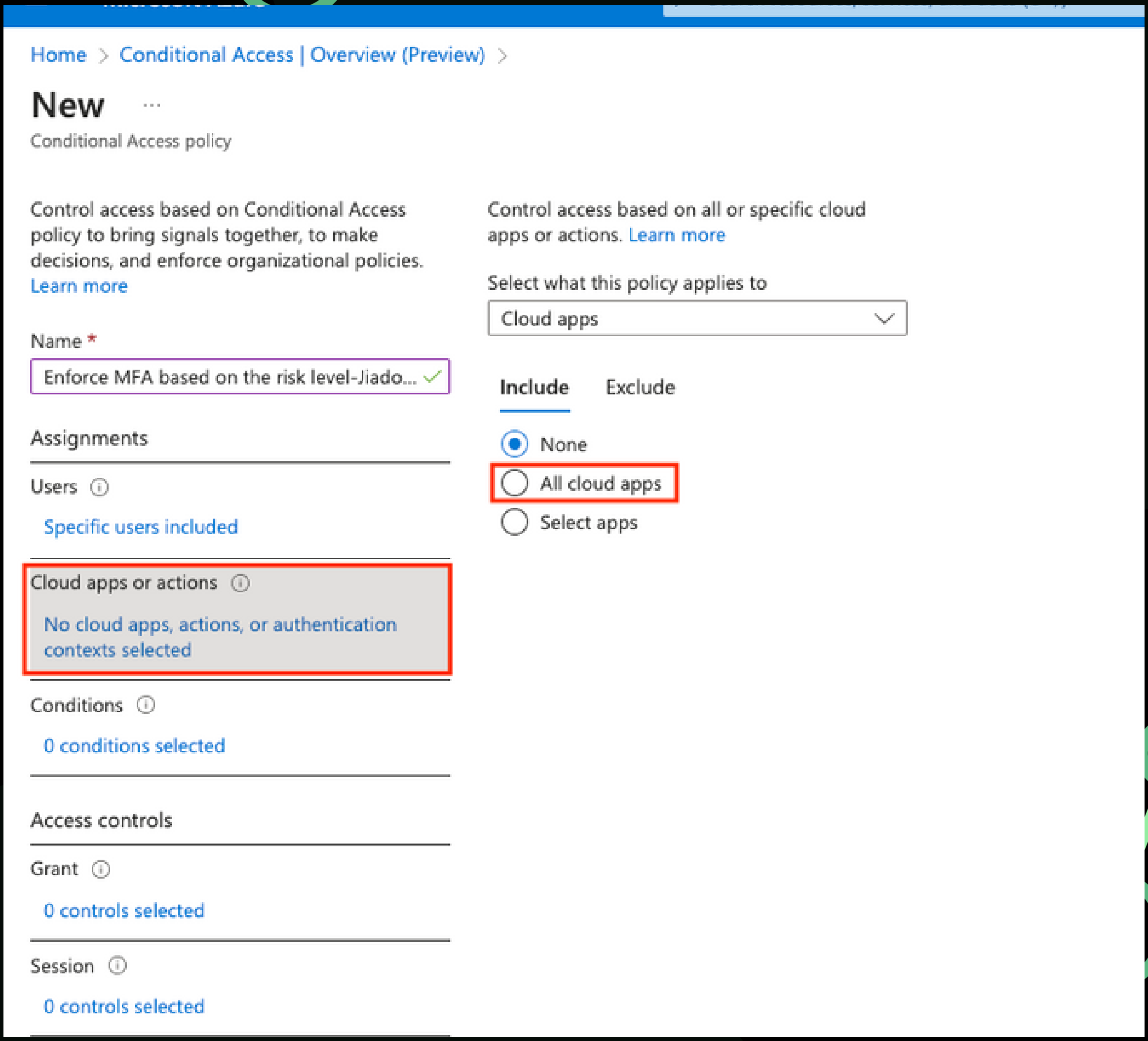
Select

1 user

JC Jiadong Chen
azuretij ···

UNDER ASSIGNMENTS, SELECT USERS, THEN SELECT THE USERS OR GROUPS YOU WANT TO INCLUDE OR EXCLUDE

JIADONG CHEN



Home > Conditional Access | Overview (Preview) >

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 *

Enforce MFA based on the risk level-Jiado... ✓

Assignments

Users ⓘ

Specific users included

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

Control access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to

Cloud apps

Include Exclude

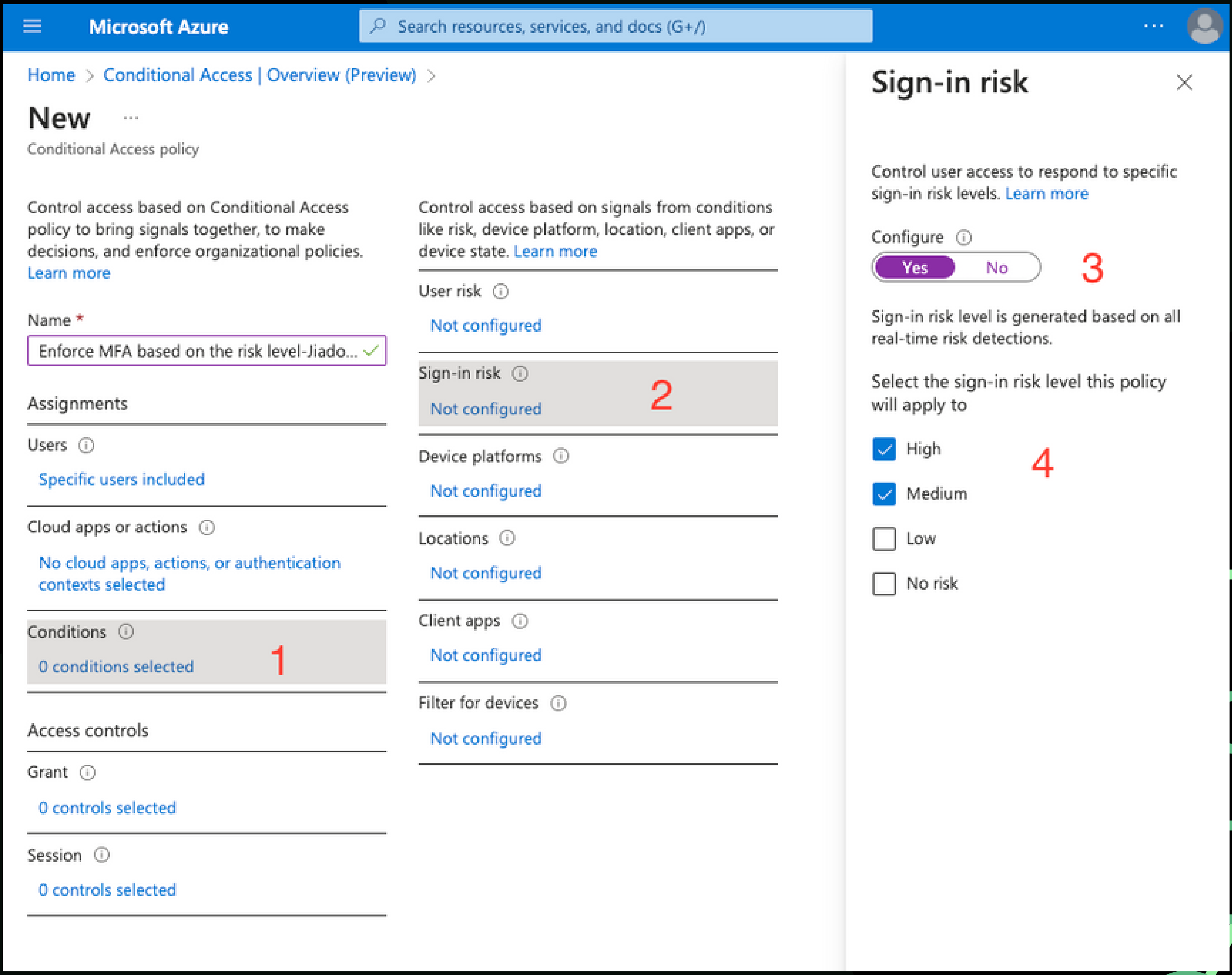
● None

○ All cloud apps

○ Select apps

UNDER CLOUD APPS OR ACTIONS > INCLUDE, SELECT ALL CLOUD APPS.

JIADONG CHEN



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Conditional Access | Overview (Preview) >

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 *

Enforce MFA based on the risk level-Jiado... ✓

Assignments

Users ⓘ

Specific users included

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected 1

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

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

User risk ⓘ

Not configured

Sign-in risk ⓘ

Not configured 2

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Filter for devices ⓘ

Not configured

Sign-in risk ×

Control user access to respond to specific sign-in risk levels. Learn more

Configure ⓘ

[✓ Yes] No 3

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 4

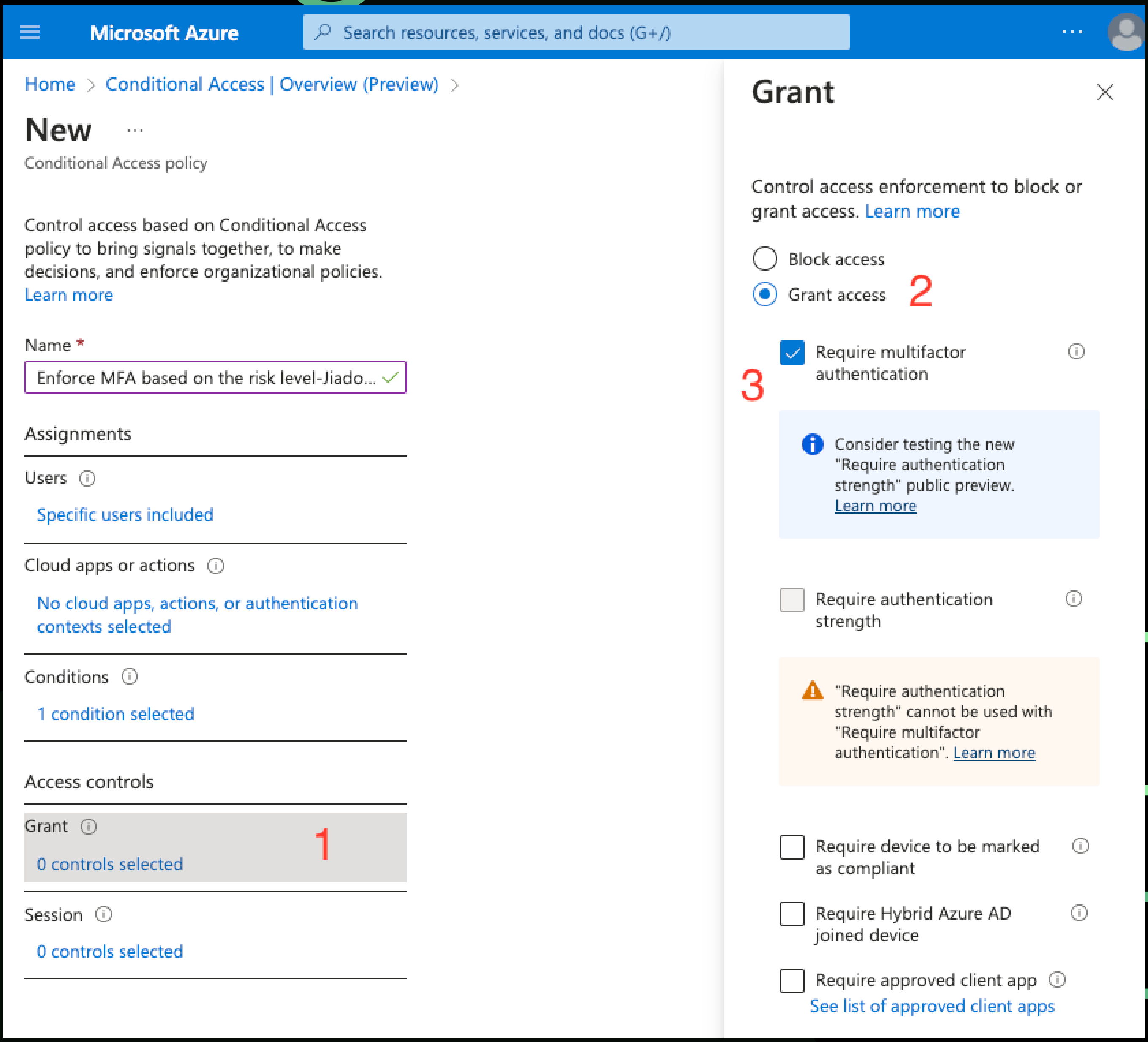
☑ Medium

□ Low

□ No risk

UNDER CONDITIONS > SIGN-IN RISK, SET CONFIGURE TO YES.
UNDER "SELECT THE SIGN-IN RISK LEVEL THIS POLICY WILL APPLY TO"
SELECT THE LEVELS.

JIADONG CHEN



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Conditional Access | Overview (Preview) >

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 *

Enforce MFA based on the risk level-Jiado... ✓

Assignments

Users ⓘ

Specific users included

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ 1

0 controls selected

Session ⓘ

0 controls selected

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access 2

3 ☑ Require multifactor authentication ⓘ

Consider testing the new "Require authentication strength" public preview. Learn more

□ Require authentication strength ⓘ

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

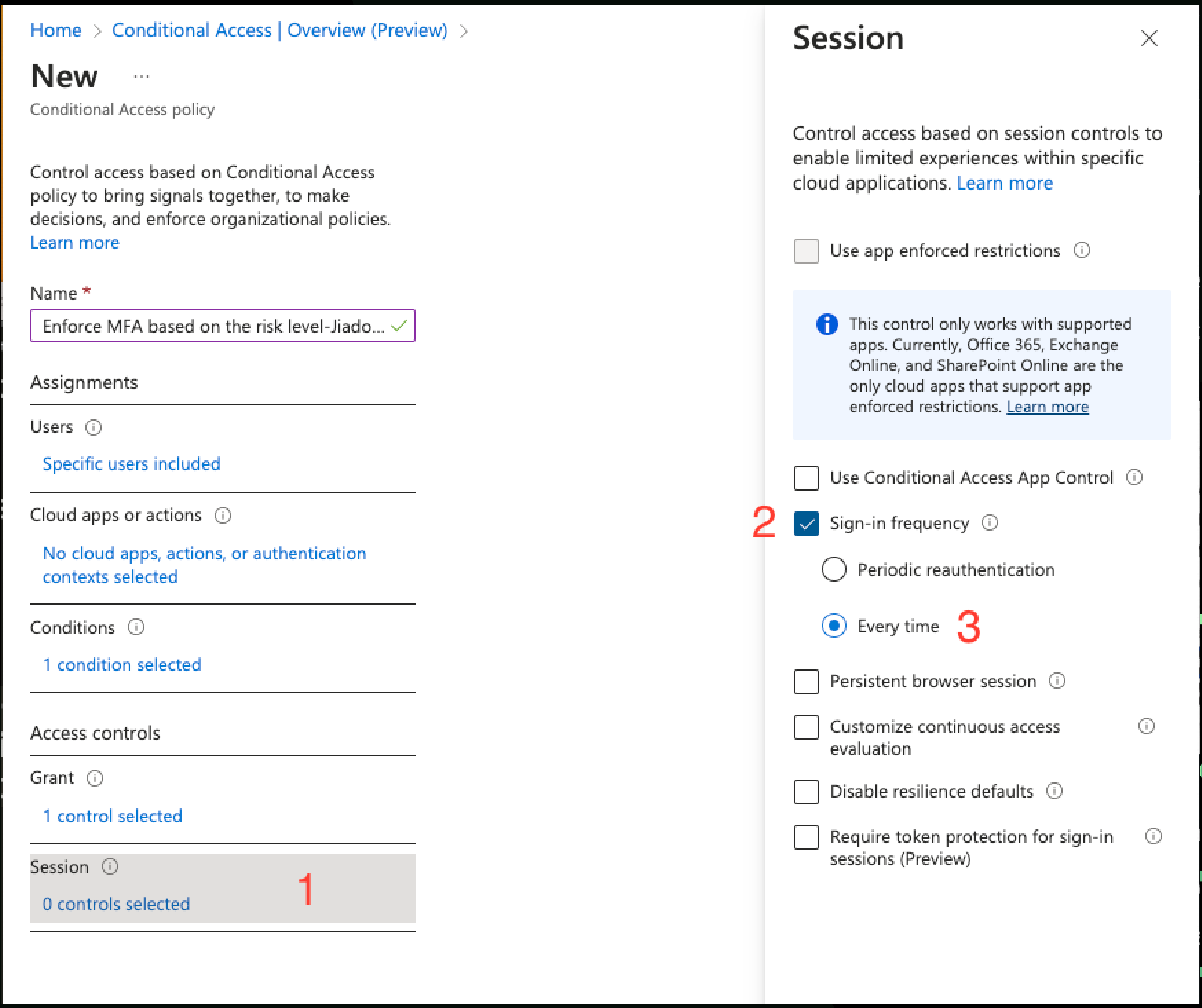
□ Require device to be marked as compliant ⓘ

□ Require Hybrid Azure AD joined device ⓘ

□ Require approved client app ⓘ
See list of approved client apps

UNDER ACCESS CONTROLS > GRANT
SELECT GRANT ACCESS,
REQUIRE MULTIFACTOR AUTHENTICATION.

JIADONG CHEN



Home > Conditional Access | Overview (Preview) >

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 *

Enforce MFA based on the risk level-Jiado... ✓

Assignments

Users ⓘ

Specific users included

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected 1

Session ✕

Control access based on session controls to enable limited experiences within specific cloud applications. Learn more

☐ Use app enforced restrictions ⓘ

ⓘ 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. Learn more

☐ Use Conditional Access App Control ⓘ

2 ☑ Sign-in frequency ⓘ

○ Periodic reauthentication

● Every time 3

☐ Persistent browser session ⓘ

☐ Customize continuous access evaluation ⓘ

☐ Disable resilience defaults ⓘ

☐ Require token protection for sign-in sessions (Preview) ⓘ

UNDER SESSION
SELECT SIGN-IN FREQUENCY
ENSURE EVERY TIME IS SELECTED.

JIADONG CHEN

READ MORE:

- CONDITIONAL ACCESS COMMON POLICIES
- WHAT IS IDENTITY PROTECTION?