

## Enhancing Secure Access with Azure AD Conditional Access

*Prepared By:*

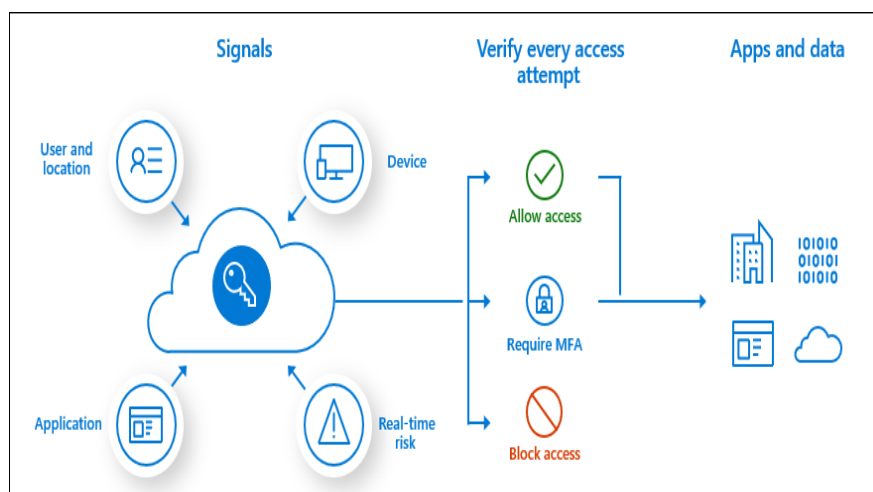
--Vatsal Patel

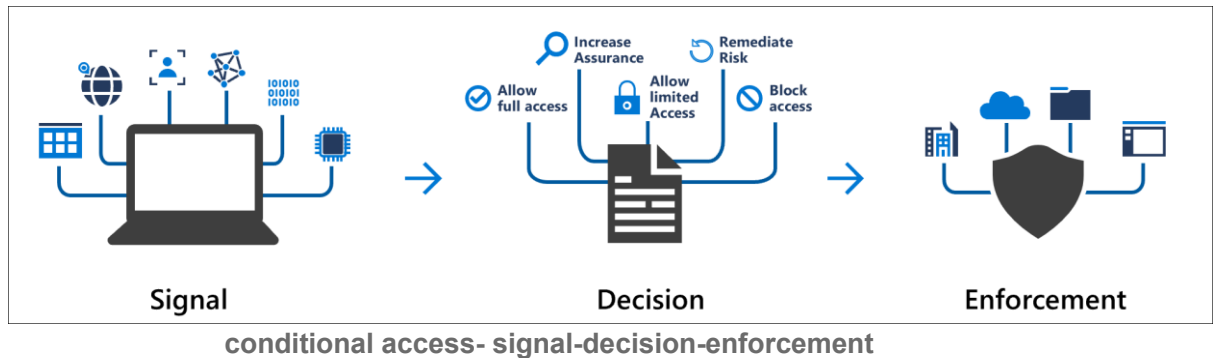
--Yash Shah

*Reviewed By:*

-- Meet Shah

- In this Document, we have explained the basic principles and 4 use cases for Azure AD Conditional Access, explain the fundamental concepts, and illustrate how they may be used to secure access to resources.
- **With the following topics to focus on:**
  - Assignments (Users, Roles).
  - Conditions.
  - Access Controls (Grant and Session).
- **Overcoming Challenges with Azure AD Conditional Access:**
  - In today's digital landscape, enterprises must have secure access to resources. However, they confront difficulties in safeguarding their assets. Cyberattacks are becoming more sophisticated, insider risks are on the rise, and monitoring access from many endpoints is becoming increasingly difficult.
  - To overcome these issues, enterprises can use solutions such as Azure AD Conditional Access. This framework allows access controls to be enforced depending on characteristics such as user risk, sign-in risk, device compliance, and client app trustworthiness.
- **Azure AD Conditional Access:**
  - Conditional Access enhances security by enforcing access policies in Azure AD. It helps to protect resources and ensures secure user authentication with features like MFA and device compliance.





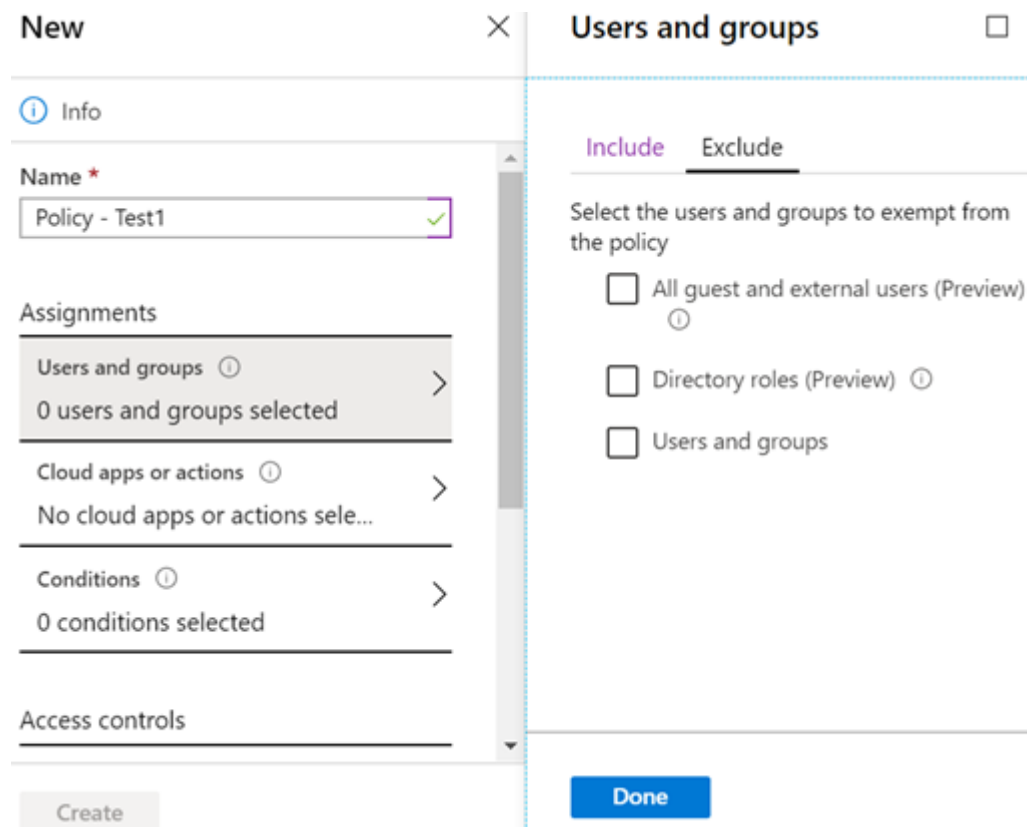
- Conditional Access brings signals together to make decisions and enforce organizational policies in Azure AD. At their most basic, conditional access policies are if-then statements: if a user wants to access a resource, they must first act.
- Azure Active Directory Conditional Access is a feature that allows companies to set access restrictions based on certain criteria and limitations. It improves security by enforcing these regulations and requiring users to fulfil specific criteria before accessing resources.
- Organizations can enforce multi-factor authentication, limit access from certain places or devices, and apply additional security measures to secure their data and applications by considering variables such as user risk, sign-in risk, and device compliance.

#### ➤ Assignments:

- Assignments in Azure AD Conditional Access decide which users or roles are subject to the access policies.

The screenshot shows the 'New' policy configuration page in Azure AD. The 'Name' field is set to 'Policy - Test1'. Under 'Assignments', the 'Users and groups' section is expanded, showing '0 users and groups selected'. The 'Access controls' section is also visible. The 'Users and groups' panel on the right shows the 'Include' tab selected, with options for 'None', 'All users', and 'Select users and groups'. The 'Select users and groups' option is currently selected.

include users & groups



#### exclude users & groups

- It enables enterprises to target individuals or groups, assuring customized access restrictions inside Azure AD based on employment responsibilities, departments, or assigned roles.
- **Users:** With user assignments, organizations can target specific individuals or groups of users to enforce tailored access policies. This can be based on factors such as job roles, departments, or specific user accounts.
- **Roles:** Role assignments, allow organizations to apply access policies to predefined roles within Azure AD. This simplifies the management of access controls by associating policies with roles instead of individual users. Roles can include built-in roles like Global Administrator or custom roles created by the organization.
- **For example,** assigning a Conditional Access policy to a specific role could be to require MFA for all users with the Global Admin role. This ensures that only authorized individuals have access to critical administrative functions.

➤ **Conditions:**

- Azure AD Conditional Access examines risk levels and context elements for access controls.

**Name \***

Example: 'Device compliance app policy'

---

**Assignments**

Users and groups ⓘ >  
0 users and groups selected

---

Cloud apps or actions ⓘ >  
No cloud apps or actions selected

---

Conditions ⓘ >  
0 conditions selected

---

**Access controls**

Grant ⓘ >  
0 controls selected

---

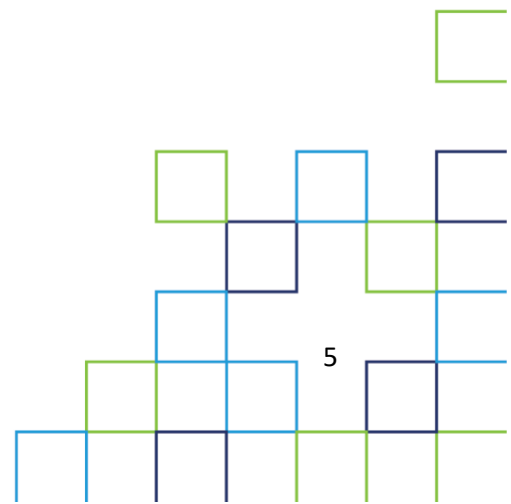
Session ⓘ >  
0 controls selected

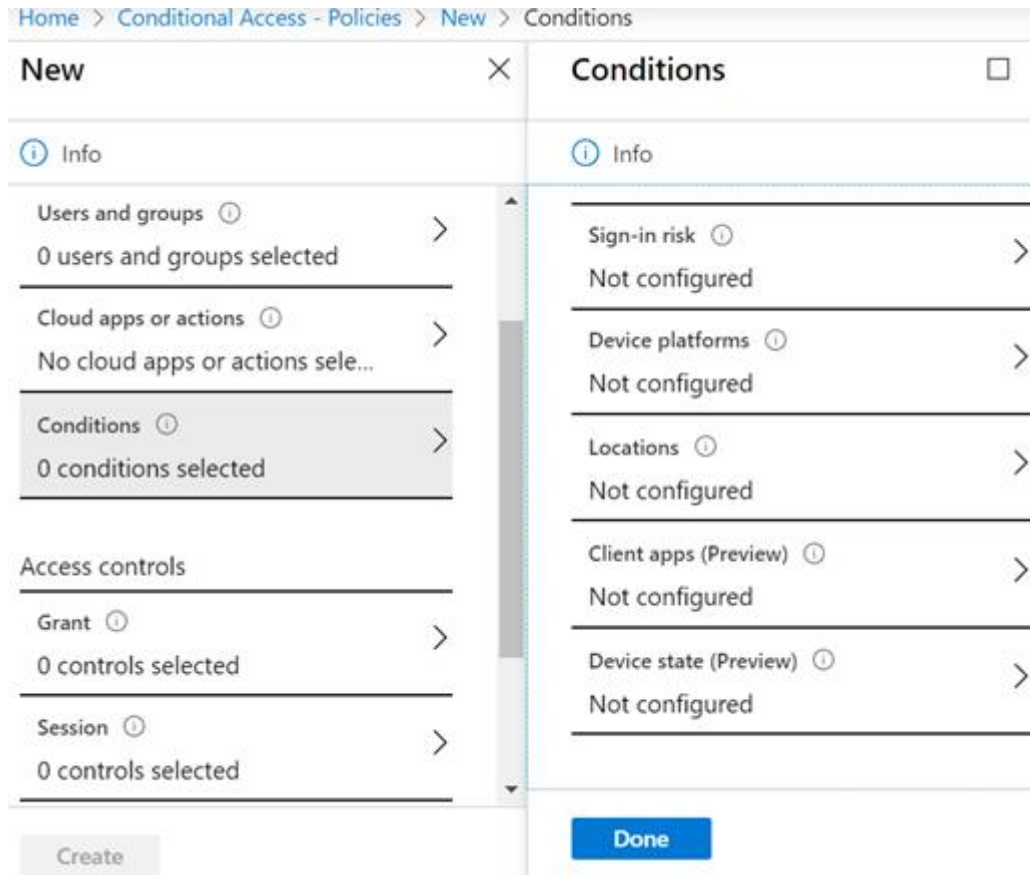
---

**Enable policy**

**Report-only** On Off

Create Conditional Access policy





### Conditional Access conditions

- Conditions in Azure AD Conditional Access are criteria used to define and determine when access controls and policies should be applied, based on various contextual factors.
- By leveraging these conditions effectively, and making intelligent access decisions, it must assess user risk, sign-in risk, device compliance, location, and client app attributes. This dynamic evaluation increases security and protects key resources.
- For example, setting a condition in Azure AD Conditional Access based on a user's sign-in risk allows organizations to require additional security measures when the sign-in risk is deemed high. This ensures that users with suspicious sign-in activities or high-risk behaviours are subjected to an extra layer of verification, enhancing the overall security posture.

## ➤ Access Controls (Grant and Session):

- Grant Controls and Session Controls are the two components of Azure AD Conditional Access.

### Grant □ ×

Select the controls to be enforced.

☐ Block access  
☒ Grant access

☐ Require multi-factor 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 (preview) ⓘ  
[See list of policy protected client apps](#)

For multiple controls

☐ Require all the selected controls  
☒ Require one of the selected controls

### Session □ ×

Session controls enable limited experiences within a cloud app. Select the session usage requirements.  
[Learn more](#)

☐ Use app enforced restrictions ⓘ

☐ Use Conditional Access App Control ⓘ

☐ Sign-in frequency (preview) ⓘ

☐ Persistent browser session (preview) ⓘ

### Grant & Session Controls

## ➤ Grant Controls:

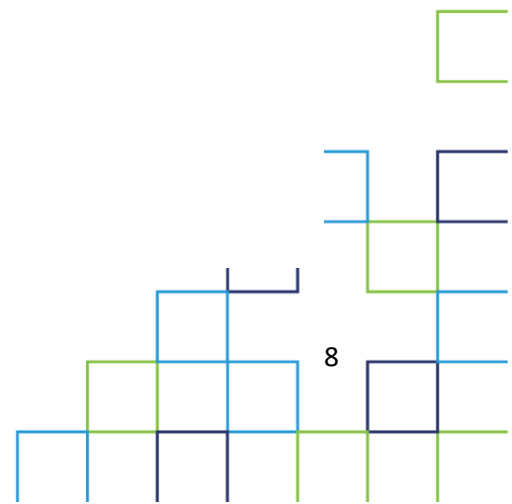
- The level of access granted to users is determined by Grant Controls based on the requirements and risk assessments. They specify which behaviours are permitted or prohibited when a user asks for access to a resource. Grant controls can include things such as demanding MFA or limiting access from specified places or devices.
- For example, requiring multi-factor authentication while accessing sensitive resources. To improve security, users must give an additional layer of authentication.

➤ **Session Controls:**

- Session Controls, on the other hand, governs the behaviour and security of user sessions once they have been allowed access. They concentrate on regulating user behaviours during the session to reduce potential dangers. Session controls can include features like session timeouts, conditional session management, and limiting certain actions within the session.
- For example, Setting a session timeout limit for user sessions. The session will automatically expire after a specific amount of inactivity, lowering the danger of unauthorized access if a user forgets to sign out or leaves their session unattended.

➤ **User risks & Sign-in risk:**

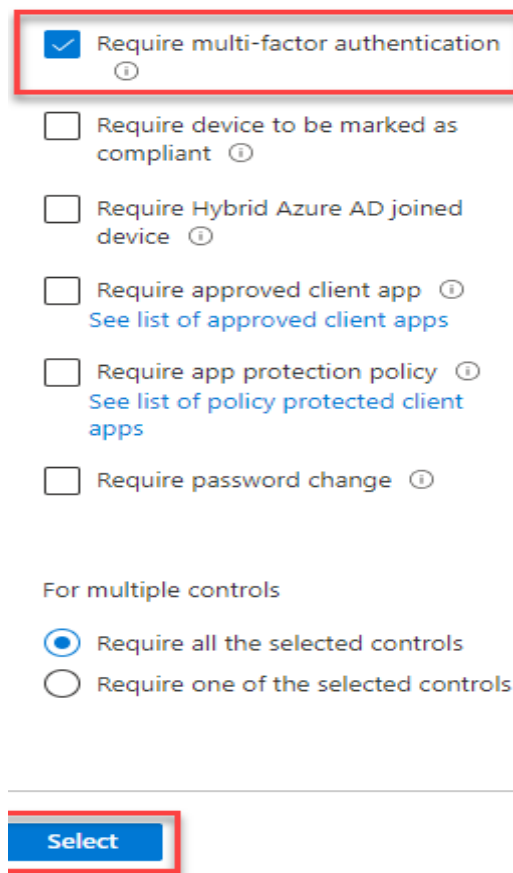
- User risks and sign-in risk are two factors that organizations can consider when implementing Azure AD Conditional Access to enhance security.
- **User risks:** focus on the overall risk level associated with a user account. It takes into consideration various factors such as past behaviour, security incidents, or the user's assigned role. By evaluating user risks, organizations can assess the trustworthiness and potential security threats posed by individual users. This assessment helps in applying appropriate access controls based on the user's risk profile.
- **Sign-in risk :** evaluates the risk level of a specific sign-in attempt. It considers factors like IP location, device trustworthiness, unusual activity patterns, or known malicious entities. Sign-in risk analysis provides real-time risk assessment for each authentication attempt, allowing organizations to dynamically adjust access controls based on the immediate risk factors associated with the sign-in event.
- By considering both user risks and sign-in risk, organizations can implement conditional access policies that adapt to the changing risk landscape.
- For example, when a user with a high-risk profile attempt to sign in from an unrecognized device or suspicious location, additional security measures like MFA can be enforced. This ensures that high-risk sign-in attempts receive heightened security scrutiny while maintaining a seamless experience for users with lower-risk profiles.
- Effectively leveraging user risks and sign-in risks in Azure AD Conditional Access allows organizations to implement a risk-based approach to access controls. It enables them to strike a balance between user convenience and security by applying appropriate security measures based on the risk levels associated with both the user and the sign-in attempt.





➤ **Here are some used cases:**

1. **Client Apps:** The software that the user employs to access the cloud app.
  - Organizations may guarantee that only trustworthy and approved applications have access to critical resources by regulating client apps through conditional access policies. This improves security, prevents illegal access, and safeguards sensitive data from potential dangers.
  - For example, Apps such as browsers, mobile applications, and desktop clients. By default, all newly created Conditional Access rules will apply to all client app types, even if the client app's condition is not specified.
2. **MFA Require:** MFA (Multi-Factor Authentication) is a security mechanism that adds an extra layer of protection to user authentication.



The screenshot shows the 'Require multi-factor authentication' checkbox selected. Below it are five other checkboxes: 'Require device to be marked as compliant', 'Require Hybrid Azure AD joined device', 'Require approved client app' (with a link to 'See list of approved client apps'), 'Require app protection policy' (with a link to 'See list of policy protected client apps'), and 'Require password change'. Under the heading 'For multiple controls', the 'Require all the selected controls' radio button is selected. At the bottom, there is a 'Select' button.

### MFA require

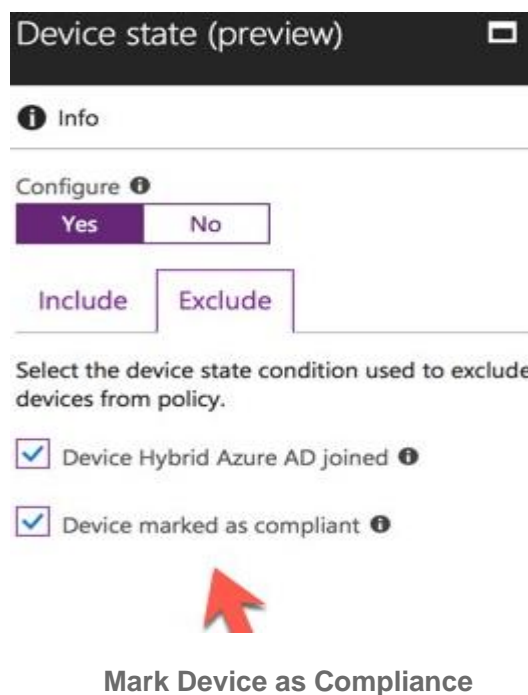
- When MFA is needed, users must give extra verification methods in addition to their standard username and password, such as a unique code from a mobile app, a text message with a verification code, or other authentication such as fingerprint or face recognition.
- Even if a user's credentials are compromised, using MFA in Azure AD Conditional Access helps decrease the danger of unwanted access. It substantially improves security by guaranteeing

that only authorized persons with a trusted device and the appropriate additional verification factor have access to protected resources.

- By implementing MFA, enterprises may effectively safeguard sensitive data, prevent illegal access, and meet regulatory requirements. It is a vital security measure that improves the overall security posture of an organization's identity and access management architecture.

### 3. Require device to mark as compliant:

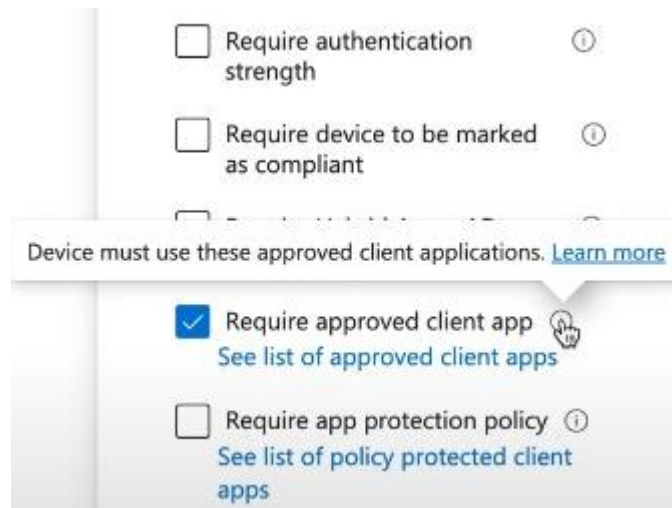
- This is an Azure AD Conditional Access condition that requires users to access resources from devices that have been designated as compliant by the organization's device management system.



- This helps to guarantee that only trustworthy and safe devices are granted access, improving overall security and reducing the chance of illegal access or data breaches.
- Devices that meet the compliance requirements will be granted access, while non-compliant devices may be blocked or required to go through additional security measures, before accessing resources.
- For example, if a user attempts to access sensitive data from a non-compliant device, they may be blocked or prompted to go through additional security measures, such as multi-factor authentication (MFA), before accessing the resources. This helps enhance overall security and reduces the risk of unauthorized access or data breaches from non-compliant devices.

#### 4. Require approved client app:

- This condition in Azure AD Conditional Access allows companies to limit access to approved and trusted client apps.



#### Require Client App

- Enforcing this requirement means that only approved apps may access resources, boosting security and lowering the danger of unauthorized or insecure app usage.
- Enforcing the “Require approved client app” condition, for example, guarantees that users may only access business resources through approved apps such as Microsoft Outlook or the official company mobile app, lowering the risk of data exposure through untrusted or unauthorized programs.
- For example, an organization may enforce this condition to ensure that users can only access business resources through approved apps. By doing so, the organization reduces the risk of data exposure through untrusted or unauthorized applications, enhancing security and maintaining control over the apps used to access sensitive resources.