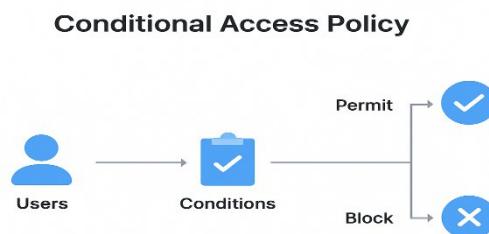


Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada

Conditional Access Policy (Microsoft)

What is Conditional Access Policy: Conditional Access Policy is one of the most powerful tools in Microsoft 365 security. It helps organizations protect against password theft, risky sign-ins, and unauthorized device access by enforcing conditions that must be met before granting access to company resources.



Purpose: As part of Cybersecurity protection/mitigation, conditional access acts as part of an organization's cybersecurity defense strategy. Its primary purpose is to protect and prevent access from:

- Password Theft
- Risky Sign-ins
- Unmanaged Devices

Persona baselines Conditional Access Policies every Company/Business Organization should apply:

What is **Persona baseline**? In Conditional Access policies are a framework that defines minimum access controls for different **user groups, or personas, like internal staff, external vendors, or developers**.

Naming Policy Guidelines: To maintain consistency and clarity, apply a structured naming policy when creating Conditional Access policies.

Example naming structure:

- Who: Target users or groups
- What: Condition or app
- Action: Required control

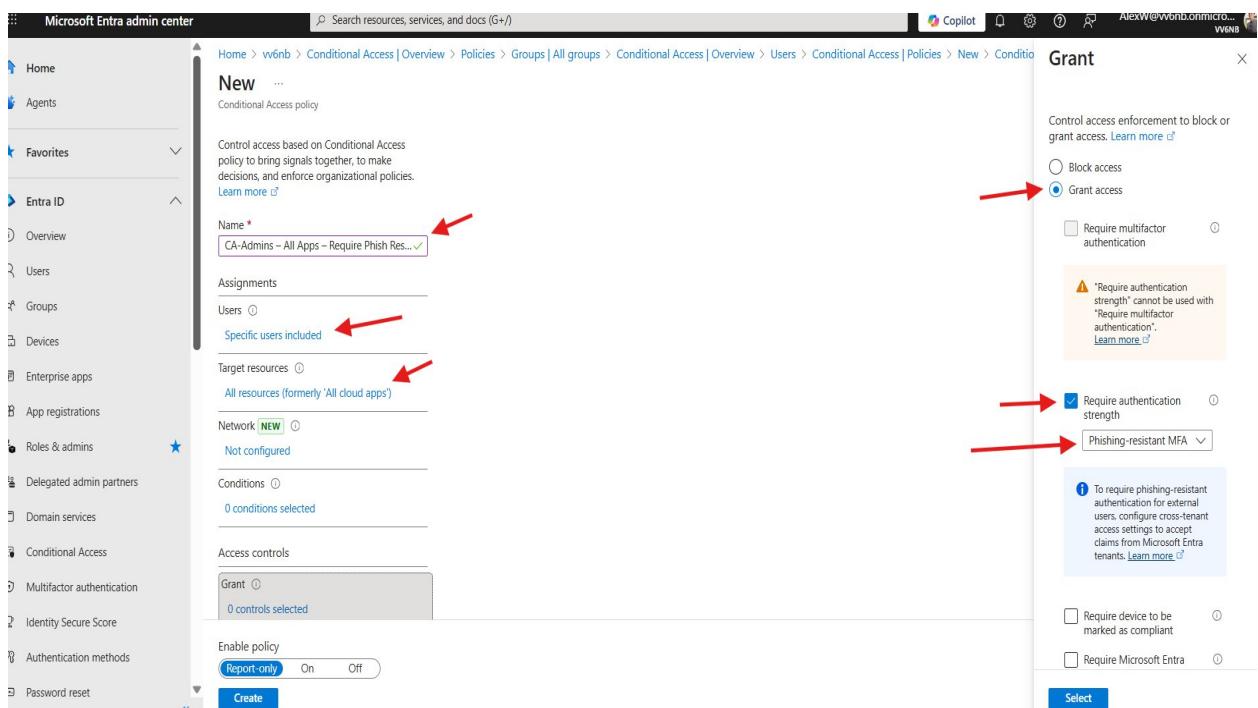
Example: Admins - All Apps - Require MFA

Application/Technical Configuration:

Policy 1: CA-Admins – All Apps – Require Phish Resistant MFA

Create a policy to **CA-Admins – All Apps – Require Phish Resistant MFA**.
Click in Microsoft 365 Admin Center > **Conditional Access** > **Policies** > **New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Admins Group.
- Target Resources > All resources (Formerly “All cloud apps”)
- Grant > Grant Access > Require Authentication Strength > Phishing-resistant MFA > Click Create



- The purpose of this policy is specifically for the **admins**, while regular staff can use the **Required strong MFA**.

Policy 2: CA-Admins – All Apps – Require Company/Compliant Device

Create a policy to **CA-Admins – All Apps – Require Phish Resistant MFA**.
Click in Microsoft 365 Admin Center > **Conditional Access** > **Policies** > **New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Admins Group.
- Target Resources > All resources (Formerly “All cloud apps”)
- Conditions > Filter for Devices > Configure = Yes > Devices matching the rule = Include filtered devices in policy

- Property = DeviceOwnership, Operator = Equal, Value = Company > Click Done

Microsoft Entra admin center

New Conditional Access policy

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

Conditions: 0 conditions selected

Access controls: 0 controls selected

Enable policy: Report-only

Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Confined: Yes

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
	DeviceOwnership	Equals	Company
+ Add expression			

Rule syntax: device.deviceOwnership -eq "Company"

Done

- Grant Control > Grant Access > Require device to be marked as compliant > click Select > click

Microsoft Entra admin center

New Conditional Access policy

Name: CA-Admins – All Apps – Require Company...✓

Assignments: 0 users and groups selected

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

Conditions: 1 condition selected

Access controls: 0 controls selected

Enable policy: Report-only

Grant

Control access enforcement to block or grant access. Learn more

Block access

Grant access

Require multifactor authentication

Require authentication strength

Require device to be marked as compliant

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

Require Microsoft Entra hybrid 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

Select

Policies in Report-only mode requiring compliant devices may prompt users on macOS, iOS, Android, and Linux to select a device certificate. Learn more

Exclude device platforms macOS, iOS, Android, and Linux from this policy.

Proceed with selected configuration. Users on macOS, iOS, Android, and Linux may receive prompts when the device is checked for compliance.

Create

click Create

Policy 3: CA-Staff – All Apps – Require Company/Compliant Device

Create a policy to **CA-Admins – All Apps – Require Phish Resistant MFA**.
Click in Microsoft 365 Admin Center > **Conditional Access > Policies > New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Staff Group.
- Target Resources > All resources (Formerly “All cloud apps”)
- Conditions > Filter for Devices > Configure = Yes > Devices matching the rule = Include filtered devices in policy
- Property = DeviceOwnership, Operator = Equal, Value = Company > Click Done

The screenshot shows the Microsoft Entra admin center interface for creating a new Conditional Access policy. The left sidebar lists various administrative categories like Home, Agents, Favorites, and Global Secure Access. The main pane shows the 'New Conditional Access policy' wizard. In the 'Filter for devices' step, several configuration options are highlighted with red arrows:

- Include filtered devices in policy:** A radio button is selected.
- And/Or:** A dropdown menu is open, with the 'And' option selected.
- Property:** A dropdown menu is open, showing 'DeviceOwnership'.
- Operator:** A dropdown menu is open, showing 'Equal'.
- Value:** A dropdown menu is open, showing 'Company'.
- Rule syntax:** The expression 'device.deviceOwnership -eq "Company"' is displayed in the text area.

- Grant Control > Grant Access > Require device to be marked as compliant > click Select > click

The screenshot continues the process of creating a new Conditional Access policy. The 'Assignments' section is highlighted with red arrows pointing to the 'Users' dropdown and the 'Grant' dropdown. The 'Grant' section is also highlighted with a red arrow. On the right, the 'Grant' configuration pane is open, showing various options:

- Control access enforcement to block or grant access:** 'Grant access' is selected.
- Require device to be marked as compliant:** This checkbox is checked and highlighted with a red arrow.
- Don't lock yourself out! Make sure that your device is compliant.** A note with a warning icon is present.
- Other options:** 'Block access', 'Require multifactor authentication', 'Require authentication strength', 'Require Microsoft Entra hybrid joined device', 'Require approved client app', 'Require app protection policy', and 'Require password change'.



click Create

Policy 3: CA-Guest – All Apps – Block Mobile and Desktop Apps

Create a policy to **CA-Guest – All Apps – Block Mobile and Desktop Apps**. Click in Microsoft 365 Admin Center > **Conditional Access** > **Policies** > **New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Guest Group.
- Target Resources > All resources (Formerly “All cloud apps”)
- Conditions > Client apps > Configure Yes > Uncheck the browser > Click Done

The screenshot shows the 'New Conditional Access policy' page in the Microsoft Entra admin center. On the left, a sidebar lists various Entra ID management sections like Overview, Groups, Devices, etc. The main area has tabs for 'Users', 'Target resources', 'Conditions', 'Access controls', and 'Session'. Under 'Conditions', a red arrow points to the '0 conditions selected' link. Under 'Client apps', a red arrow points to the 'Configure' dropdown set to 'Yes'. Another red arrow points to the 'Browser' checkbox, which is unchecked. The right side of the screen shows a list of client applications: Modern authentication clients (Browser, Mobile apps and desktop clients), Legacy authentication clients (Exchange ActiveSync clients, Other clients), and a note about controlling access to specific client applications not using modern authentication.

- Click Grant > Click Block > Create

Scenario:

In real life, situations may arise such as someone losing their phone, experiencing laptop failure or corruption, or requesting temporary access from a different device. In these cases, we will implement the exclusion command to allow secure, time-bound access while maintaining policy integrity. Also, we will implement the **TAP (Temporary Access Password)**.

To check your Microsoft Entra Admin Authentication Method, this is where we implement the **MFA something you have, something you know and something you are**.

Click > Authentication Methods > Policies

Method	Target	Enabled
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Software OATH tokens	All users	Yes
Voice call		No
Email OTP	All users	Yes
Certificate-based authentication		No
QR code		No

Policy 4: Provide TAP (Temporary Access Password) To the Executive or Administrative Users

- Click Users > All Users > Click the Username > **Click Authentication Method > Add Authentication Method > Choose Method and Choose Temporary Access Pass > Click One-Time use > Click Yes > Click Add**

Authentication method	Detail
Passkey	Charles Yubikey
Windows Hello for Business	HAWTHORNE1
Windows Hello for Business	iPhone 16 Pro
Microsoft Authenticator	
Temporary Access Pass	TAP expired

Policy 5: Another way is the **ID Governance, Access Reviews**.

- Click **ID Governance > Click Access Review > Click New Access Review**

- See below information to review

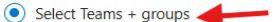
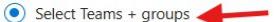
New access review ...

A linked Azure subscription is required to use Entra ID Governance features for guest users. Beginning in November 2025, an Azure subscription must be connected to use Entra ID Governance features.

***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 * 

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

Group * 

Scope * Guest users only 
 All users 

Info In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users only

- Click > Next >

New access review ...

A linked Azure subscription is required to use Entra ID Governance features for guest users. Beginning in November 2025, an Azure subscription must be connected to use Entra ID Governance features.

***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

- Click > Settings >

New access review ...

A linked Azure subscription is required to use Entra ID Governance features for guest users. Beginning in November 2025, an Azure subscription must be connected to use Entra ID Governance features for guests. [Learn more](#)

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

Configure additional settings, including decision helpers and email notifications.

Upon completion settings

Auto apply results to resource

If reviewers don't respond No change Change Remove

At end of review, send notification to + Select User(s) or Group(s)

Enable reviewer decision helpers

No sign-in within 30 days

User-to-Group Affiliation

Advanced settings

Justification required

Email notifications

< Previous **Next: Review + Create**

New access review ...

A linked Azure subscription is required to use Entra ID Governance features for guest users. Beginning in November 2025, an Azure subscription must be connected to use Entra ID Governance features for guests. [Learn more](#)

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

Name new access review

Review name * Leonard Estos 

Description

- **Click > Create**
- Now, verify your creation.

Name	Resource	Status	Warning	Created On
Leonard Estos	Group Leo_WHP_Users	Not started		11/3/2025

Sources:

1. **Advanced Conditional Access for IT Pros | Complete Guide**
<https://www.youtube.com/watch?v=DkCq8wWN9Sc>

2. **How to Set Up Conditional Access in Microsoft 365 (Step-by-Step) By Jonathan Edwards**
<https://www.youtube.com/watch?v=5oMaZink7kc>

” When you train Smarter, you defend Stronger”
Leonard Estos