Cyber clinic

Conditional Access Policies

9 April 2021

V1.0

LOCAL DIGITAL Cyber

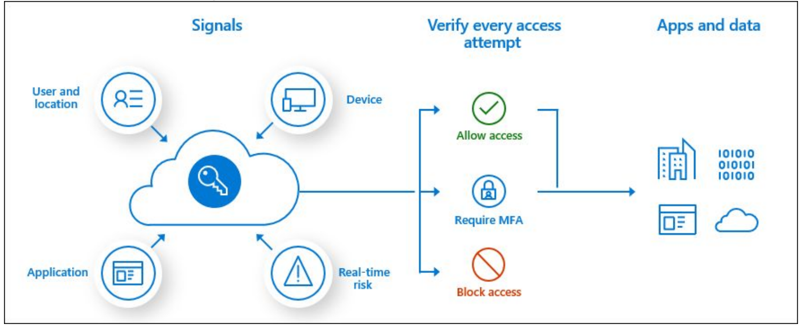
Agenda

Conditional Access Policies

- What are Conditional Access Policies
- Why are Conditional Access Policies important
- Benefits & Considerations
- Typical Policy Implementations
- Subscription Level Information
- Create a CAP
- Interaction Intune
- Further Information

What are Conditional Access Policies ?

Conditional Access policies at their simplest are “if-then” statements, **if** a user wants to access a resource, **then** they must complete an action.



Azure Active Directory (Azure AD) Conditional Access analyses ‘signals’ such as user, device, and location to automate decisions and enforce organizational access policies for resource. You can use Conditional Access policies to apply access controls like Multi-Factor Authentication (MFA). Conditional Access policies allow you to prompt users for MFA when needed for security, and stay out of users’ way when not needed.

LOCAL DIGITAL Cyber

Why are CAPs important?

In essence - with Conditional Access, you can control the devices and apps that can connect to your email and company resources.

By their nature, CAP’s only allow access if certain conditions are met first.

They add an extra layer of security and also can extend out to assist compliance in other areas (such as operating system versions and patching levels).

Conditional Access is an Azure Active Directory capability that is included with an Azure Active Directory Premium license.

Benefits of deploying Conditional Access

- **Increase productivity.** Only interrupt users with a sign-in condition like MFA when one or more signals warrants it. Conditional Access policies allow you to control when users are prompted for MFA, when access is blocked, and when they must use a trusted device.

- **Manage risk.** Automating risk assessment with policy conditions means risky sign-ins are at once identified and remediated or blocked. Coupling Conditional Access with Identity Protection, which detects anomalies and suspicious events, allows you to target when access to resources is blocked or gated.

- **Address compliance and governance.** Conditional Access enables you to audit access to applications, present terms of use for consent, and restrict access based on compliance policies.

Benefits of deploying Conditional Access (cont.)

- **Manage cost.** Moving access policies to Azure AD reduces the reliance on custom or on-premises solutions for Conditional Access, and their infrastructure costs.
- **Control.** Conditional Access policies allow you to control when users are prompted for MFA, when access is blocked, and when they must use a trusted device
- Refer to https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview for more information on CAP

Considerations

Before deploying Conditional Access Policies there are certain things you should consider:

- What you want to achieve.
  - Clearly define what you want to do
  - Define the policies to achieve this
- Licensing implications
  - CAP implementation level will vary depending on what version / combination of Microsoft 365 Services you are running. Some conditional access features are part of Microsoft 365 Business packages, more features run with Azure AD Premium P1. To fully leverage CAP Azure AD Premium P2 is required.

Ref:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common

Typical policies implemented

- Blocking Access by Location
- Blocking risky sign-in behaviors
- Blocking Legacy Authentication
  - Clients that don't use modern authentication (for example, an Office 2010 client).
  - Any client that uses older mail protocols such as IMAP, SMTP, or POP3.
- Requiring MFA
- Requiring a compliant device
- Blocking Access except for Specific Applications
- Requiring organization-managed devices for specific applications
- Sign-in risk-based Conditional Access (Requires Azure AD Premium P2)
- User risk-based Conditional Access (Requires Azure AD Premium P2)
- Requiring trusted location for MFA Registration
- Requiring multi-factor authentication for users with administrative roles

Base CAP Policies

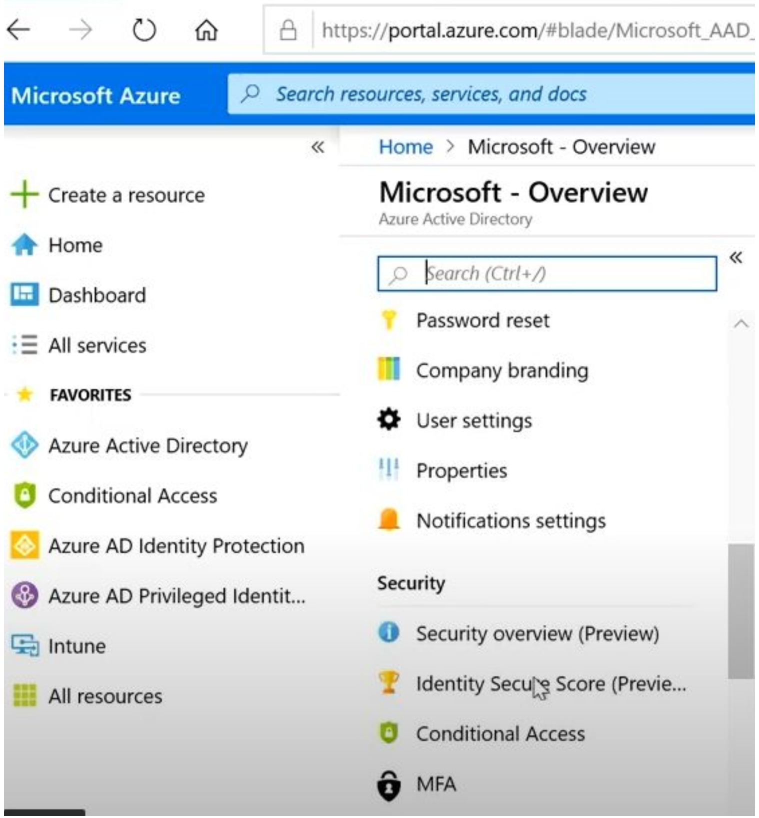
Azure Active Directory (AD) Conditional Access policies are available with Microsoft 365 Business subscriptions. Even with a regular Azure AD, four Conditional Access preview policies are available. With a qualifying Azure subscription, you can create your own Conditional Access Policies (recommended)

- **Blocking Legacy Authentication** - this policy blocks access to: clients that don't use modern authentication (for example, an Office 2010 client), and any client that uses older mail protocols such as IMAP, SMTP, or POP3.
- **Requiring MFA for Admins** - this policy requires the mandatory use of MFA for some administrative roles

Base CAP Policies (cont.)

- **End user protection** - this policy enables the use of MFA for users (the user must complete the MFA registration via the Microsoft Authenticator app within 14 days after the first login)
- **Require MFA for service management** - this policy gives you the MFA requirement for users to sign in to services based on the Azure Resource Manager API (Azure Portal, Azure CLI, PowerShell)

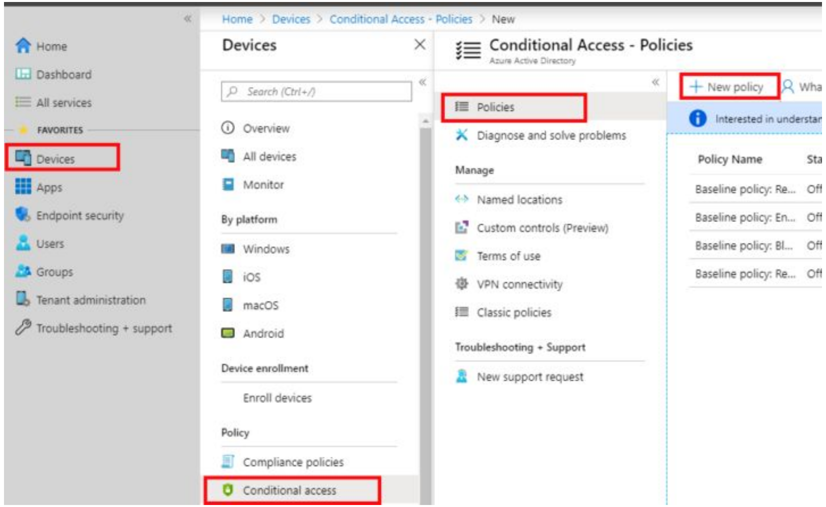
Creating a Conditional Access Policy



This is a very basic guide in taking the first steps to creating a CAP.

Log into your tenant as an administrator and go to the Security > Conditional Access Policies section, then navigate to the Conditional Access 'blade'

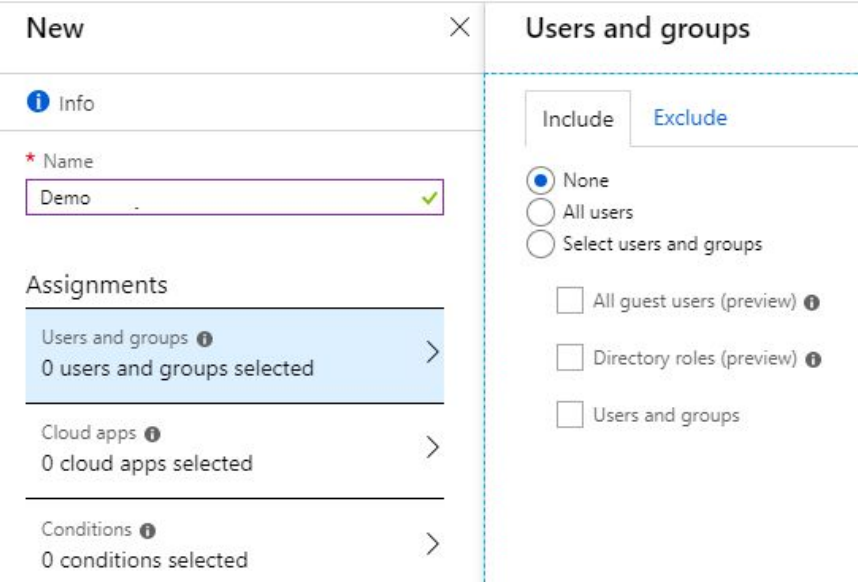
Creating a Conditional Access Policy (cont.)



Policy Name	Sta
Baseline policy: Re...	Off
Baseline policy: En...	Off
Baseline policy: Bl...	Off
Baseline policy: Re...	Off

Then when in the ‘Conditional Access - Policies’ blade click on the ‘+ New policy’

Creating a Conditional Access Policy (cont.)



New ×

Info

* Name

Demo ✓

Assignments

Users and groups
0 users and groups selected

Cloud apps
0 cloud apps selected

Conditions
0 conditions selected

Users and groups

Include | Exclude

● None
○ All users
○ Select users and groups

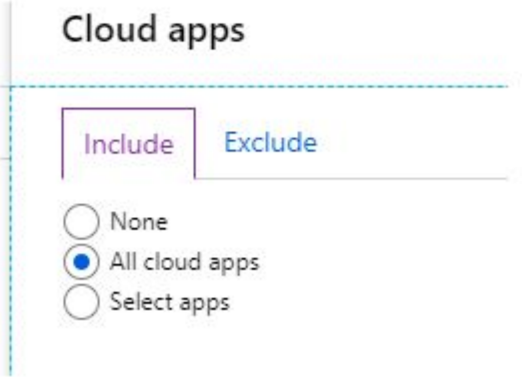
□ All guest users (preview)
□ Directory roles (preview)
□ Users and groups

Name your policy.

Now in the Assignments section of the panes, you now need to specify the conditions for applying the policy.

Proceed to set the scope of the application by selecting users and/or groups. These can be all users in Azure AD or specific groups/users. Exceptions can be specified separately.

Creating a Conditional Access Policy (cont.)

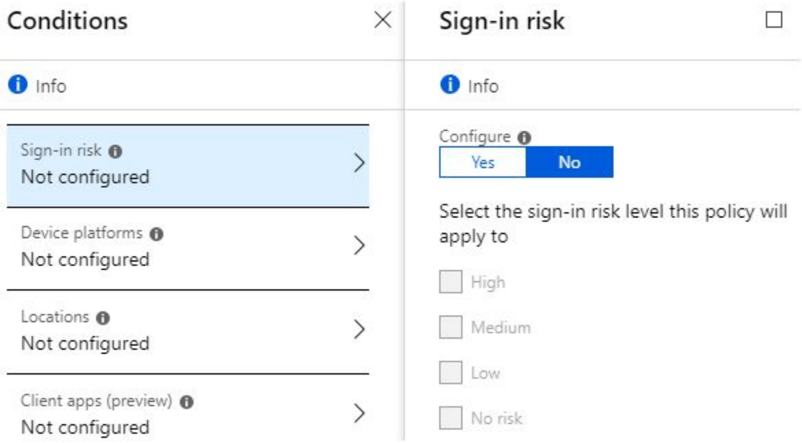


Cloud apps

○ None
● All cloud apps
○ Select apps

In the Cloud Apps Assignment pane, select apps that you have previously registered with Azure AD (none, one or more are acceptable)

Creating a Conditional Access Policy (cont.)



Conditions

ℹ Info

Sign-in risk ℹ
Not configured

Device platforms ℹ
Not configured

Locations ℹ
Not configured

Client apps (preview) ℹ
Not configured

Sign-in risk

ℹ Info

Configure ℹ

Yes [✓ No]

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

☐ High

☐ Medium

☐ Low

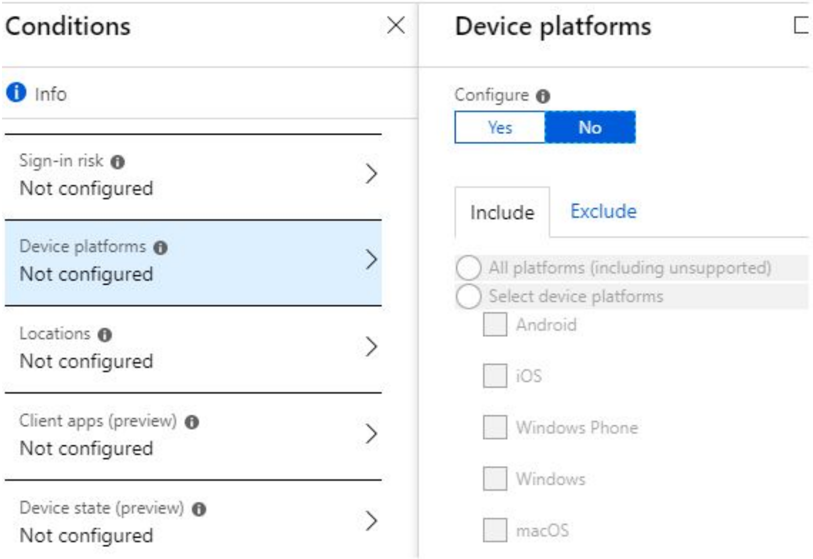
☐ No risk

On the Conditions pane, you can now specify the ‘conditions’ which are needed to be satisfied to grant (or refuse) access.

Note : Sign in risk requires an Azure AD Premium **P2** license.

LOCAL DIGITAL Cyber

Creating a Conditional Access Policy (cont.)



Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (preview)
Not configured

Device state (preview)
Not configured

Device platforms

Configure
Yes [✓ No]

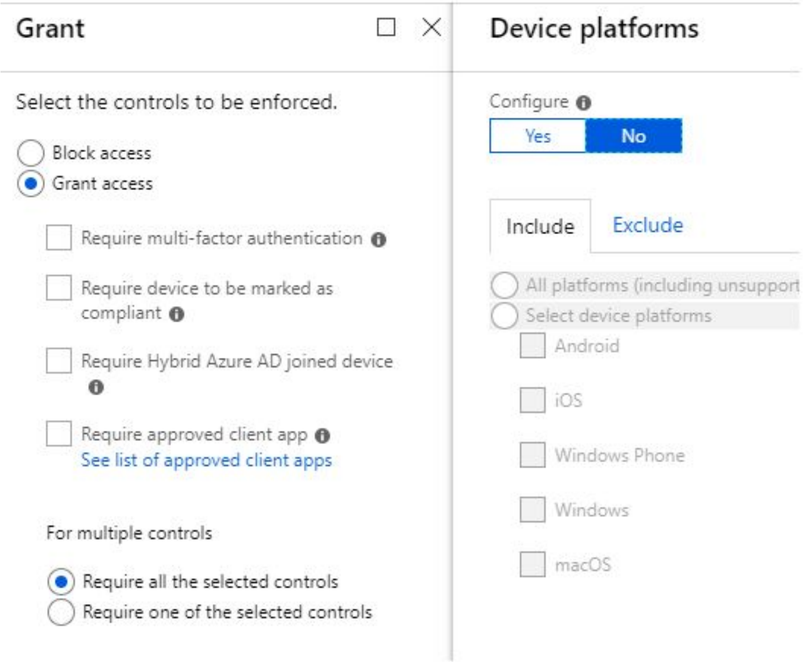
Include | Exclude

○ All platforms (including unsupported)
○ Select device platforms
□ Android
□ iOS
□ Windows Phone
□ Windows
□ macOS

In the Device platforms pane, specify which OS platform the policy is to apply to (or exclude)

The Locations pane allows you to select from the predefined (by yourself) list of trusted IP addresses.

Creating a Conditional Access Policy (cont.)



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

For multiple controls

● Require all the selected controls
○ Require one of the selected controls

Device platforms

Configure

Yes **No**

Include Exclude

○ All platforms (including unsupport
○ Select device platforms

□ Android

□ iOS

□ Windows Phone

□ Windows

□ macOS

In the Grant pane, you can select whether to block or allow (grant) access requests, or require additional security measures.

Conditional access and Intune

- **This section of slides gives a high level overview of the interaction between CAP and Intune.**

- If your organisation uses Intune with your Microsoft 365 configuration, you can leverage the combined features which includes Device Compliance and Mobile Application Management.
- Conditional Access is an Azure Active Directory capability that is included with an Azure Active Directory Premium license.
  Intune enhances this capability by adding mobile device compliance and mobile app management to the solution.

https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access

Conditional access and Intune (cont.)

There are two types of conditional access with Intune:

- Device-based conditional access
- App-based conditional access.

You need to configure the related compliance policies to drive conditional access compliance at your organisation.

Conditional access is commonly used to do things like allow or block access to Exchange, control access to the network, or integrate with a Mobile Threat Defence solution.

https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access

Conditional access and Intune (cont.)

Specific ways to use Conditional Access with Intune:

- Device-based Conditional Access
- Conditional Access for Exchange on-premises
- Conditional Access based on network access control
- Conditional Access based on device risk
- Conditional Access for Windows PCs
  - Corporate-owned
  - Bring your own device (BYOD)
- App-based Conditional Access

https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use

Microsoft Guide Videos

Microsoft have produced a series of video guides on how to work with Conditional Access:

There are several available, but a good starting point would be the following:

What is Conditional Access : https://www.youtube.com/watch?v=ffMAw2IVO7A

How to deploy Conditional Access : https://www.youtube.com/watch?v=c_izIRNJNuk

How to roll out Conditional Access : https://www.youtube.com/watch?v=0_Fze7Zpyvc

Cyber support sessions

Cyber treatment plan & implementation support session available to book here. These are 1:1 sessions between MHCLG cyber team and a council, available for any support, guidance or hands on help for the implementation of your cyber treatment plan.

Cyber clinics are occurring every Friday @10:00-10:30 am where a targeted cyber focus area will be presented, tool sets demonstrated and will be open to questions. Support, guidance and hands-on help is available to assist you in adoption and implementation.

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on Medium
- Follow LDCU on Twitter (@LDgovUK)
- Subscribe to our Cyber newsletter for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the MHCLG Digital blog

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.

LOCAL DIGITAL Cyber

Ministry of Housing,
Communities &
Local Government

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber