Overview of conditional access policies best practice

V1.0

LOCAL DIGITAL Cyber

Overview

Outline guidance and approach of considerations to be given to Conditional Access Policies (CAP's) for all applicable Local Authority Information Systems.

With Conditional Access, you can control the devices and apps that can connect to your email and company resources. Conditional Access policies at their simplest are "if-then" statements, **if** a user wants to access a resource, **then** they must complete an action.
Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

LOCAL DIGITAL Cyber

Overview (cont.)

Conditional Access Policies are mainly used in conjunction with Azure AD (Microsoft 365 / Microsoft Azure) system usage.

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.

LOCAL DIGITAL Cyber

Why are CAPs important?

By their nature, Conditional Access Policies 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).

The benefits of deploying Conditional Access are:

- Increase productivity. Only interrupt users with a sign-in condition like MFA when one or more signals warrants it.
- 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

LOCAL DIGITAL Cyber

Typical policies implemented

- CAP implementation level will vary depending on whether or not you are using Azure AD Premium 2 or not, as some features depend on this licensing model.
- Typical Policies deployed:
  - 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 by Location

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

LOCAL DIGITAL Cyber

Typical policies implemented (cont.)

- Typical Policies deployed (Continued):
  - Blocking Access except 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

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

LOCAL DIGITAL Cyber

Typical policies implemented (cont.)

- Typical Policies deployed (Continued):
  - Requiring multi-factor authentication for Azure management tasks
  - Requiring trusted locations for Azure AD Multi-Factor Authentication registration
  - Blocking risky sign-in behaviors
  - Requiring organization-managed devices for specific applications

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

Conditional access 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

LOCAL DIGITAL Cyber

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

LOCAL DIGITAL Cyber

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

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