Purpose:
To show understanding on how to design and implement Conditional Access (CA) policies for secure access even if the sandbox tenant doesn't allow full creation.

Structure & Content

Title:
Planned Conditional Access Policy, Require MFA for Administrators

Objective:
To enforce multi-factor authentication (MFA) for all administrative accounts in the Microsoft 365 tenant to mitigate the risk of unauthorized access.

Background:
Conditional Access (CA) policies in Microsoft Entra ID (formerly Azure AD) help enforce identity-based controls.
MFA is a critical layer of defense to protect accounts from credential theft and phishing attacks.

Planned Policy Configuration:

Setting	Description
Policy Name	Require MFA for Admin Accounts
Users	All users with admin roles (Global Admin, Security Admin, etc.)
Cloud Apps	All cloud apps
Conditions	None (applies to all locations and devices)
Access Controls	Grant access → Require multi-factor authentication
Session Controls	Not configured
Policy State	Enabled

Expected Behavior:
When an admin user attempts to sign in, they will be prompted to complete MFA verification (via Microsoft Authenticator or SMS) before access is granted.

Screenshot References:

- ca_unavailable.png - showing Conditional Access area in tenant

Outcome:
Although the Developer E5 tenant limits CA policy creation, this document demonstrates understanding of MFA enforcement principles using CA design.