Conditional Access Policy Documentation

1. Purpose

This document outlines the Conditional Access (CA) policies configured in Microsoft Entra ID (formerly Azure Active Directory). These policies are designed to enforce secure access, protect privileged roles, and block insecure legacy protocols. Each policy follows the principles of Zero Trust and least privilege access.

2. Policy: Require MFA for All Users

Description: This policy ensures that all users must complete multi-factor authentication to access cloud apps.

Targets: All Users (excluding break-glass accounts)

Conditions: All cloud apps; Sign-in risk: High (optional)

Access Controls: Grant access -> Require multi-factor authentication

Status: Enabled

Screenshot: Require multi-factor authentication

3. Policy: Block Legacy Authentication

Description: Blocks access from legacy clients using basic authentication (POP, IMAP, SMTP, etc.).

Targets: All Users

Conditions: Client apps: Legacy authentication clients

Access Controls: Grant access -> Block

Status: Enabled

Screenshot: Legacy authentication clients

4. Policy: Require MFA for Admin Roles

Description: Adds mandatory MFA for all privileged directory roles to prevent account compromise.

Targets: Global Admin, Security Admin, Privileged Role Admin

Conditions: All cloud apps

Access Controls: Grant access -> Require MFA

Status: Enabled

Screenshot: Require MFA