Scenario

Due to rising security threats, Tailspin Toys requires all remote employees to use Multi-Factor Authentication (MFA) when accessing Azure resources from untrusted locations. Your task is to configure a Conditional Access policy to enforce this.

Objectives

Create a Conditional Access policy requiring MFA for remote access.

Exempt trusted IP ranges (e.g., office networks).

Test the policy with different scenarios.

Instructions

Define Trusted Locations: In Azure AD, navigate to "Conditional Access" and add your office’s public IP range as a trusted location.

Create MFA Policy: Create a new Conditional Access policy targeting "All users" except emergency break-glass accounts. Set the condition to trigger for "Any location" except trusted IPs. Require MFA.

Test the Policy: Attempt to sign in from an untrusted IP (use a VPN if needed). Verify MFA is prompted. Repeat from a trusted IP to confirm exemption.

Refine Policy: Adjust policy settings if false positives/negatives occur (e.g., adding more trusted IPs).

