***Scenario:***  
You are an IT administrator for a financial company that is implementing strict security measures to protect sensitive data and comply with industry regulations. As part of these efforts, you are required to configure Azure Conditional Access Policies to manage how users access corporate resources.  
  
The organization has the following security requirements:  
1.    MFA Requirement:  
Employees accessing the company’s Office 365 apps from any location must go through Multi-Factor Authentication (MFA) to ensure secure access, especially since these apps contain critical financial information.  
2.    Trusted Network Access:   
Employees accessing resources from within the corporate network (trusted IP addresses) should not be required to use MFA. They should have seamless access to Office 365 applications.  
3.    Block Access from Specific Countries:   
Due to increasing concerns about data theft, your organization wants to block access to Azure resources from high-risk countries like Russia and China. Users trying to access from these countries should receive an immediate access block.  
4.    Device Compliance Requirement:  
Employees must access Azure resources using company-managed and compliant devices (devices that meet specific security standards). Any attempt to access the resources from a non-compliant device must be blocked, regardless of location.  
5.    Exceptions:  
The CEO of the company frequently travels to various countries and uses multiple devices. As such, the CEO should be excluded from the MFA requirement and country-based access restrictions. The CEO should always be able to access resources without facing these restrictions.  
  
Task:  
  
As an Azure administrator, configure the appropriate Conditional Access policies in Azure Active Directory to meet the above requirements.  
  
Steps to Solve:  
1.    Multi-Factor Authentication (MFA) Policy:  
•    Create a Conditional Access policy that enforces MFA for all users accessing Office 365 apps from any location.  
•    Exclude the trusted network (corporate IP addresses) from this policy so that users inside the corporate network can access resources without MFA.  
2.    Trusted Network Access:  
•    Define the corporate network IP range under Named Locations and mark it as a trusted location.  
•    Ensure this trusted location is excluded from the MFA requirement in the policy configuration.  
3.    Blocking Access from Specific Countries:  
•    Create a Conditional Access policy to block access from Russia and China.  
•    Use Named Locations to specify these countries in the policy, and apply the blocking action for all users trying to access from these locations.  
4.    Device Compliance Policy:  
•    Create a Conditional Access policy that requires users to access resources only from compliant devices.  
•    Ensure that only devices meeting the organization’s security standards (such as mobile device management, up-to-date antivirus, etc.) are considered compliant.  
5.    Exception for the CEO:  
•    Add an exception for the CEO, allowing access to all resources without requiring MFA or blocking access based on location. This ensures that the CEO is excluded from the restrictions that apply to other users.

***Creating user:-***

**Preview Features:**

Access to new or experimental Azure AD features before they are generally available.

**Diagnose and Solve Problems:**

Tools and recommendations to help troubleshoot issues within your Azure AD environment.

**Manage:**

This section is key to managing different aspects of your directory, including users, roles, and security settings.

**Users:** Manage all users in your directory. This includes adding new users, modifying user details, or disabling accounts.

**Groups:** Create and manage security or distribution groups that you can use to organize users and control access to resources.

**External Identities:** Manage how external users (guests) access your applications and resources.

**Roles and Administrators:** Assign administrative roles, such as Global Admin or User Admin, to users who manage Azure AD.

***Security:-***

***Protect:***

The Protect section focuses on safeguarding user identities and controlling access.

**Conditional Access:**

Define policies that allow or deny access to applications based on conditions like user location, device state, or risk.

For example, you can require multi-factor authentication (MFA) for users logging in from outside your organization's network.

**Identity Protection:**

Detect and respond to identity risks such as compromised accounts, risky sign-ins, and suspicious activity.

Automate mitigation actions like enforcing MFA or blocking access for risky users.

**Security Centre:**

A centralized dashboard providing insights and recommendations for improving the overall security of your Azure AD environment.

You can monitor alerts, security trends, and compliance suggestions here.

**Verified ID:**

Manage decentralized identities and issue verifiable credentials that users can present to access resources or verify their identity.

***Manage:***

The Manage section provides tools to actively manage security measures and authentication policies.

**Identity Secure Score:**

A metric that measures the security of your Azure AD tenant based on implemented recommendations.

It provides insights into security weaknesses and gives actionable steps to improve your security posture.

**Named Locations:**

Define trusted or risky geographical locations for Conditional Access policies.

You can use this to allow or block access from specific regions or IP ranges.

**Authentication Methods:**

Configure and manage the various authentication methods allowed in your organization, such as password-based, FIDO2 keys, and biometric options.

Customize settings for security questions, tokens, or authenticator apps.

**Multifactor Authentication (MFA):**

Enforce MFA to add an additional layer of security for users signing in to your organization’s applications.

You can configure settings for MFA enforcement, exceptions, and notification methods.

**Certificate Authorities:**

Manage trusted certificate authorities for certificate-based authentication.

This is useful for organizations using digital certificates for secure logins.

***Steps:-***

1. Create user
2. Assign role - Add security administrator ,global administrator

***Scenario Recap:***

Your financial company requires the following security policies:

1. Enforce Multi-Factor Authentication (MFA) for all employees accessing Office 365 from any location.

2. Employees within the trusted corporate network (specific IP range) should not need to use MFA.

3. Block access from high-risk countries like Russia and China.

4. Ensure that only compliant devices (managed and meeting security standards) can access Azure resources.

5. Exclude the CEO from all these policies so they can access resources without restrictions.

**Pre-requisites:**

You must be an Azure Global Administrator to configure these policies.

Ensure that Azure Active Directory Premium P1 or P2 is enabled in your Azure subscription to use Conditional Access.

**Step 1:** Enforce MFA for Office 365 Apps

We will first create a policy that requires MFA for users accessing Office 365, with exceptions for the corporate network and the CEO.

**Steps:**

Sign in to the Azure Portal at https://portal.azure.com.

Navigate to Azure Active Directory > Security > Conditional Access.

Click + New Policy to create a new policy.

Name the policy: e.g., “MFA for Office 365 Apps.”

Configure Policy:

**Users:**

Select All users to apply the policy universally.

Click Exclude and add the CEO user account (e.g., ceo@company.com) to ensure they don’t face MFA restrictions.

**Cloud Apps or Actions:**

Under Cloud apps, select Office 365 (or Microsoft 365 apps).

**Conditions:**

Go to Locations > Include: Select All Locations.

Exclude: In this section, we will exclude the corporate network (set up in the next step).

**Grant Access Control:**

Under Grant, select require multi-factor authentication.

**Enable Policy:** Toggle the policy to on and click Create.

**Create conditional access:**

**Assignments:**

**Users:** Defines which users or groups the policy will apply to.

**Target Resources:** Defines the resources (apps or services) the policy applies to, such as Microsoft 365, Azure management, or specific applications.

**Conditions:**

Conditions allow you to define when the policy should be applied. These conditions could include:

Sign-in risk (based on suspicious activities)

Device compliance (whether the device meets security standards)

Locations (where the sign-in attempt is coming from)

Client apps (which application is being accessed)

**Step 2:** Exclude MFA for Trusted Network (Corporate IP Range)

To exempt the trusted corporate network from MFA requirements, you need to define the trusted network and exclude it from the MFA policy.

**Steps:**

In Azure Active Directory, navigate to Security > Conditional Access > Named Locations.

Click + New location.

Name the location (e.g., “Corporate Network”).

Under IP Range, input the IP range of your corporate network (e.g., 192.168.1.0/24).

Mark this location as a trusted location.

Go back to the policy you created in Step 1:

Under Conditions > Locations, click Exclude.

Select the Corporate Network you just defined.

Save the changes to the policy.

**Step 3:** Block Access from High-Risk Countries

Now, we will create a policy that blocks access from high-risk countries like Russia and China.

**Steps:**

Go to Azure Active Directory > Security > Conditional Access > Policies.

Click + New Policy and name it “Block Access from High-Risk Countries.”

Configure Policy:

**Users:**

Select all users, excluding the CEO (add them under Exclusions).

**Cloud Apps:**

Apply this to All cloud apps (you can select specific apps if necessary).

**Conditions:**

Go to Locations > Include: Select Countries/Regions.

Click + New Location and define Russia and China as Named Locations.

Select Block access from these countries.

**Grant:**

Under Access controls, select Block Access.

Enable Policy: Toggle the policy to on and click Create.

**Step 4**: Enforce Device Compliance Requirement

In this step, you’ll ensure that only compliant, company-managed devices can access Azure resources.

**Steps:**

Go to Azure Active Directory > Security > Conditional Access > Policies.

Click + New Policy and name it “Require Compliant Devices.”

Configure Policy:

**Users:**

Select all users, excluding the CEO under Exclusions.

**Cloud Apps**:

Apply this to all cloud apps (or select the specific apps).

**Conditions:**

Go to Device platforms: Select the relevant device types (e.g., Windows, iOS, Android).

**Grant Access Control:**

Under Grant, select require device to be marked as compliant.

Enable Policy: Toggle the policy to on and click Create.

***Verification:-***

To verify that your Azure Conditional Access policies are working as expected, follow these steps to test each part of the scenario. This will ensure that MFA, trusted network access, country blocks, device compliance, and CEO exclusions are functioning correctly.

**1. Verify MFA Enforcement for Office 365 (External Location)**

- **\*\*Goal\*\*:** Ensure that employees accessing Office 365 from outside the corporate network are prompted for MFA. Which is 182.70.94.188/32 is corporate network

**Steps:**

**1. \*\*Simulate an external login\*\*:**

- Use a device that is \*\*not\*\* connected to the corporate network.

- Sign in to an Office 365 application (e.g., Outlook or One Drive) using an employee account (not the CEO).

**2. \*\*Expected Outcome\*\*:**

- The user should be prompted to complete MFA (e.g., via an authenticator app or SMS).

- If MFA works, this part of the policy is verified.

**2. Verify Seamless Access from the Corporate Network (Trusted IP Range)**

- **\*\*Goal\*\*:** Ensure employees accessing Office 365 from within the corporate network are not required to use MFA.

Steps:

**1. \*\*Simulate an internal login\*\*:**

- Connect a device to the corporate network (within the trusted IP range you specified in Azure).

- Sign in to Office 365 using an employee account (not the CEO).

**2. \*\*Expected Outcome\*\*:**

- The user should \*\*not\*\* be prompted for MFA.

- Access should be seamless if the trusted network policy is correctly applied.

**3. Verify Blocking Access from High-Risk Countries (e.g., Russia/China)**

- **\*\*Goal\*\*:** Ensure access is blocked for users attempting to connect from Russia and China.

**Steps:**

**1. \*\*Simulate access from a high-risk country\*\*:**

- Use a VPN service to simulate accessing Azure from an IP address in Russia or China.

- Attempt to sign in to any Azure resource or Office 365 application using a regular employee account.

**2. \*\*Expected Outcome\*\*:**

- The user should receive an \*\*access denied\*\* message due to the location-based restriction.

- If the user is blocked, this part of the policy is working.

**4. Verify Device Compliance Requirement\*\***

**- \*\*Goal\*\*:** Ensure only compliant, company-managed devices can access Azure resources.

**Steps:**

**1. \*\*Simulate login from a non-compliant device\*\*:**

- Use a device that is \*\*not\*\* managed or marked as compliant in your organization.

- Attempt to sign in to any Azure resource (such as the Azure portal) using an employee account (not the CEO).

**2. \*\*Expected Outcome\*\*:**

- The user should be \*\*denied access\*\* because the device is non-compliant.

- If access is blocked, this confirms that the device compliance policy is functioning.

**\*\*5. Verify CEO Exclusions\*\***

**- \*\*Goal\*\*:** Ensure that the CEO is not subjected to any MFA, country block, or device compliance restrictions.

**Steps:**

**1. \*\*Sign in as the CEO\*\*:**

- Using the CEO’s account (e.g., ceo@company.com), try logging into an Office 365 app or an Azure resource.

- Perform this test from various locations, including high-risk countries (using a VPN) and from a non-compliant device.

**2. \*\*Expected Outcome\*\*:**

- The CEO should be able to access resources \*\*without being prompted for MFA\*\*, facing location restrictions, or device compliance checks.

- If the CEO is unrestricted, the exception policy is confirmed.

---

### \*\*Final Testing Checklist\*\*:

- **\*\*MFA\*\*:** Employees accessing from an external network must complete MFA.

**- \*\*Trusted Network\*\*:** Employees on the corporate network should access resources without MFA.

**- \*\*Country Blocks\*\*:** Employees from Russia and China should be blocked.

**- \*\*Device Compliance\*\*:** Non-compliant devices should be denied access.

**- \*\*CEO Exception\*\*:** The CEO should bypass MFA, location-based blocking, and device compliance checks.