Standard Operating Procedure (SOP): Managing Conditional Access in Microsoft Entra Admin

Document Owner: IFC - IT Department
Date: 03/28/2025
Version: 1.0

Table of Contents

Introduction

Conditional Access in Microsoft Entra Admin strengthens security by enforcing adaptive policies based on user identity, location, device, and risk level. This SOP provides a structured approach to configuring, managing, and monitoring Conditional Access policies to ensure secure and compliant access to organizational resources.

Prerequisites

Before configuring Conditional Access, ensure the following:

- You have **Global Administrator**, **Security Administrator**, or **Conditional Access Administrator** privileges.
- **Microsoft Entra ID** is assigned to enforce Conditional Access policies.
- Users and groups are properly structured within Microsoft Entra Admin.
- A clear understanding of security requirements, business needs, and compliance standards.
- An active **Microsoft Entra Admin Center** account.
- Access to **Azure AD Sign-in Logs** and **Audit Logs** for monitoring.

Procedures

1. Access Microsoft Entra Admin Center > Conditional Access

Step 1: Open Microsoft Entra Admin Center

- Open a web browser and go to **https://entra.microsoft.com**.
- Sign in with your administrator's credentials.

Step 2: Navigate to Conditional Access

- In the **left navigation pane**, click on **Protection** > **Conditional Access**.
- The **Conditional Access Policies** page will open, displaying existing policies and options to create new ones.

2. Creating a Conditional Access Policy

2.1 Defining the Policy Name and Description

Step 1: Click **+ New Policy** at the top of the Conditional Access page.

Step 2: Provide a **clear policy name** (e.g., "MFA for All Users").

2.2 Assigning Users and Groups

1. Under **Assignments**, click **Users and Groups**.
2. Choose one of the following options:
    - **All users** – Enforce the policy on all organization members.
    - **Selected users and groups** – Specify individual users, groups, or roles.
    - **Exclude specific users/groups** – Add exclusions for certain users if necessary (e.g., emergency accounts).
3. Under the enable policy, select among the three options: Report-Only, On, or Off.
4. Click on Create button to finish creating the policy.

3. Managing Conditional Access Policies

3.1 Editing an Existing Policy

1. Navigate to **Conditional Access** > **Policies**.
2. Click on the policy you want to edit.
3. Modify conditions, access controls, or assignments.
4. Click **Save**.

3.2 Disabling or Deleting a Policy

1. Select a policy from the **Conditional Access Policies** page.
2. Click **Disable** to turn it off or **Delete** to remove it permanently.

3.3 Duplicating Policies for Testing

1. Open an existing policy.
2. Click **Copy** and make necessary adjustments.

3. Enable **Report-only mode** to test before full deployment.

4. Monitoring and Reporting Conditional Access Policies

4.1 Viewing Policy Usage and Effectiveness

1. Navigate to **Conditional Access** > **Insights & Reporting**.
2. Review policy impact, blocked sign-ins, and compliance rates.

4.2 Reviewing Sign-in Logs and Policy Failures

1. Go to **Microsoft Entra Admin** > **Sign-in Logs**. (On the Monitoring Section in the second navigation panel)
2. Apply filters to check:
   - Successful vs. failed sign-ins.
   - MFA enforcement logs.
   - Blocked access attempts.

4.3 Exporting Conditional Access Reports

1. In the **Sign-in logs** section, click **Download** to export reports for analysis.

5. Named Locations

5.1 Creating and Managing Named Locations

Step 1: Navigate to Named Locations:

- Go to **Microsoft Entra Admin Center** > **Protection** > **Conditional Access** > **Named Locations**. (Under Manage section).

Step 2: Add a New Location:

- Click **+ Countries location** or **+ IP ranges location**.
- Enter a **name** for the location (e.g., "Head Office").
- Select and add the **country** or the **IP range** of your corporate.

Step 3: Mark as Trusted:

- Optionally, select **Mark as trusted location** to avoid additional security checks, such as MFA, from this location.

Step 4: Apply Named Location to Policies:

- Use the newly created location in your Conditional Access policies. Under **Locations**, select the desired named location to include in your policy.

6. Custom Controls (Preview)

6.1 Creating Custom Controls for Conditional Access

1. **Navigate to Custom Controls**:
   - Go to **Microsoft Entra Admin Center** > **Security** > **Conditional Access** > **Custom Controls (Preview)**. (Under **manage** section)
2. **Create a New Custom Control**:
   - Click on **+ New custom control**.
   - Add the customized JSON code. Include the name of the control on the json file itself.
   - Define the **custom action** or **authentication method** required by the control.
3. **Apply Custom Control to Policies**:
   - After creating the custom control, apply it by selecting it under the **Access Controls** section when defining a Conditional Access policy.

7. Terms of Use

7.1 Configuring Terms of Use for Conditional Access

1. **Navigate to Terms of Use**:
   - Go to **Microsoft Entra Admin Center** > **Security** > **Conditional Access** > **Terms of Use**. (Under **Manage** Section)
2. **Create New Terms of Use**:
   - Click **+ New Terms of Use**.
   - Enter the **Name** for the term (e.g., "Company Acceptable Use Policy").

- Upload the **Terms of Use document** (PDF document).
- Select the default language and enter the display name.

3. **Configure Policy for Terms of Use**:
   - Under **Conditions**, select which groups or users the terms will apply to.
   - Optionally, choose whether users must accept the terms each time they sign in or if it's a one-time acceptance.
4. **Publish Terms of Use**:
   - Once configured, click **Publish** to make the Terms of Use active.

8. VPN Connectivity

8.1 Configuring VPN-Based Conditional Access

1. **Navigate to VPN Connectivity**:
   - Go to **Microsoft Entra Admin Center** > **Protection** > **Conditional Access** > **VPN Connectivity**.
2. **Define VPN Settings**:
   - Under **VPN page,** click on **+ New certificate** and select the duration and click on create.
   - Define whether VPN access is required for specific locations, users, or applications.
3. **Test VPN Connectivity**:
   - Test the policy by connecting to the VPN from a user account assigned to the policy and ensure access is granted only when VPN is active.

9. Authentication Contexts

9.1 Creating and Using Authentication Contexts

1. **Navigate to Authentication Contexts**:
   - Go to **Microsoft Entra Admin Center** > **Protection** > **Conditional Access** > **Authentication Contexts**.

2. **Create a New Authentication Context**:
   - Click **+ New Context**.
   - Define the **context name** and **description** (e.g., "High-Risk Authentication").
   - Select the publish to apps option, select the ID and save it.
3. **Apply Authentication Context to Policies**:
   - In your **Conditional Access** policies, choose to require a specific **Authentication Context** under the **Conditions** or **Access Controls**.

10. Authentication Strengths

10.1 Configuring Authentication Strengths for Policies

1. **Navigate to Authentication Strengths**:
   - Go to **Microsoft Entra Admin Center** > **Protection** > **Conditional Access** > **Authentication Strengths**.
2. **Create a New Authentication Strength**:
   - Click **+ New Authentication Strength**.
   - Enter the name and description of the authentication strength.
   - Select the desired **authentication method** (e.g., MFA, passwordless, or FIDO2 security key).
3. **Apply Authentication Strength to Policies**:
   - In your **Conditional Access** policy, choose to enforce the **authentication strength** for users or groups under **Access Controls**.

11. Monitoring Conditional Access Policies in Microsoft Entra

11.1 Viewing Sign-in Logs in Conditional Access

Step 1: Access Sign-in Logs

- Navigate to **Microsoft Entra Admin Center** > **Protection** > **Conditional Access** > **Monitoring** > **Sign-in Logs**.

Step 2: Apply Filters to Analyze Sign-ins

- Use the **Filters** panel to refine sign-in data by Date, Status, User, Application and more.

Step 3: Review Individual Sign-in Details

- Click on a **specific sign-in attempt** to open the **detailed event log**, which includes:
    - **User Details** (Username, IP address, device info).
    - **Authentication Method Used** (Password, MFA, Conditional Access).
    - **Conditional Access Status** (Success, failure, blocked, bypassed).
    - **Failure Reason (if applicable)** – View policy conflicts or authentication failures.

Step 4: Identify Blocked Sign-ins and Troubleshoot Issues

- Identify sign-ins blocked by Conditional Access policies.
- Investigate **error messages** and **failure reasons** to adjust policies accordingly.

Step 5: Export Sign-in Logs (Optional)

- Click **Download** (top-right corner).
- Select the **desired format** (CSV or JSON).
- Use exported logs for **further analysis, compliance audits, or incident response**.

11.2 Reviewing Audit Logs in Conditional Access

Step 1: Access Audit Logs

- Navigate to **Microsoft Entra Admin CenterProtection** > **Conditional Access** > **Monitoring** > **Audit Logs**.

Step 2: Apply Filters to View Specific Audit Events

- Use the **Filters** panel to refine Audit logs data by Date, Status, User Agent. Service, Target, etc.

Step 3: Analyze Conditional Access Policy Changes

- Click on a log entry to see details like:
  - **Policy Created/Modified** – Identify changes to security settings.
  - **Administrator Actions** – See who changed a policy and when.
  - **Impact on Users** – Check whether new restrictions or access permissions were applied.

Step 4: Investigate Unauthorized or Risky Changes

- Monitor for **unexpected policy modifications** that might weaken security.
- Check for **privilege escalations**, such as unauthorized admin role assignments.
- Identify **high-risk authentication events**, such as multiple failed MFA attempts.

Step 5: Export Audit Logs (Optional)

- Click **Download** (top-right corner).
- Select **CSV or JSON** format.
- Export logs for **compliance reporting, forensic analysis, or security reviews**.

Conclusion

Effective Conditional Access management enhances security while maintaining user productivity. Regular policy reviews, monitoring sign-in and audit logs, and applying best practices help mitigate risks and ensure compliance with organizational security standards.