SOP: Security Configuration and Monitoring with Conditional Access

Date Created: 06/09/2025
Owner: IT Security Department
Version: 1.0

Table of Contents

1. Purpose

This SOP provides step-by-step procedures to configure and monitor security settings within Microsoft Entra, focusing on Multi-Factor Authentication (MFA) and Conditional Access (CA) policies. The aim is to enhance identity protection, reduce unauthorized access risks, and ensure compliance with internal policies and industry regulations.

2. Scope

This SOP applies to all security and system administrators responsible for managing identity and access protection in Microsoft Entra. It includes:

1. Enabling and enforcing MFA across users and groups.
2. Designing, configuring, testing, and deploying Conditional Access policies.
3. Monitoring sign-in activity, risk-based detections, and access control events.

3. Prerequisites

- Admin account with at least **Security Administrator**, **Conditional Access Administrator**, or **Global Administrator** role.
- MFA must be already configured for admin accounts.
- Access to:
    - Microsoft Entra Admin Center
    - Microsoft 365 Defender (optional for additional monitoring)
- Organizational policies and access control baseline defined.
- Licensing: Microsoft Entra ID P1 for Conditional Access; P2 for Identity Protection.

4. Procedures

4.1 Accessing the Microsoft Entra Admin Center

1. Open a secure browser and navigate to https://entra.microsoft.com.
2. Enter your admin email and password.
3. Complete the MFA prompt.

4. Once logged in, navigate to **"Identity" > "Protection"** > **"Conditional Access"** as needed.

4.2 Configuring Multi-Factor Authentication (MFA)

4.2.1 Modern MFA Enforcement via Conditional Access

1. Navigate to **Protection > Conditional Access > Policies**.
2. Click **+ New policy**.
3. Name the policy (e.g., "Require MFA for All Users").
4. Under **Assignments**:
    - **Users or workload identities:** Select **All Users** or specific security groups.
    - **Cloud apps or actions:** Select **All cloud apps** or Microsoft 365 core services.
5. Under **Conditions**:
    - Configure **Locations** to exclude trusted IP ranges (e.g., office locations).
    - Configure **Device Platforms** (e.g., block legacy authentication clients).
6. Under **Access controls > Grant**:
    - Select **Require multi-factor authentication**.
    - Optionally, check “Require device to be marked as compliant.”
7. Set **Enable policy** to **Report-only** for testing or **On** for enforcement.
8. Click **Create**.
9. Document policy name, scope, and enforcement status in your internal policy registry.

4.2.2 Per-User MFA (Legacy Management)

1. From Microsoft Entra, navigate to **Users > All users**.
2. Click **Multi-Factor Authentication** in the toolbar.
3. On the legacy MFA portal, locate the user(s) to update.
4. Select users > Click **Enable** > Confirm.
5. Notify user(s) that MFA setup will be prompted at next sign-in.

4.3 Creating and Managing Conditional Access (CA) Policies

4.3.1 Design Best Practices

- Use **named security groups** to scope policies instead of individual users.
- Always create a **"Break Glass" Global Admin account** excluded from all CA policies.
- Use **report-only mode** before enabling policies in production.

4.3.2 Create a Basic Conditional Access Policy

1. Go to **Protection > Conditional Access > Policies**.
2. Click **+ New policy** and enter a descriptive name (e.g., “Block Access from Outside US”).
3. Under **Assignments**:
    - **Users**: Select specific departments or roles.
    - **Cloud apps**: Choose one or more apps (e.g., SharePoint, Exchange Online).
    - **Conditions** > **Locations**: Include all locations; exclude named trusted locations.
4. Under **Access controls > Grant**:
    - Choose **Block access**.
5. Set **Enable policy** to **On** or **Report-only**.
6. Click **Create** and record the policy details.

4.3.3 Testing Conditional Access Policies

- Use a non-admin test account in the targeted group.
- Attempt logins from different locations/devices to evaluate enforcement.
- Review sign-in logs (see section 5.4) to confirm the policy triggers.

4.4 Monitoring Security Activity

4.4.1 Viewing Sign-In Logs

1. Under **the Identity** section, click on **show more** option and click on **Monitoring & Health**.
2. Navigate to **Sign-in logs**.
3. Apply filters by:
    - User
    - Application
    - Location
    - Risk Level
4. Review events for:
    - Unusual locations
    - Multiple failed login attempts
    - Sign-ins marked risky
5. Export or archive logs weekly for compliance tracking.

4.4.2 Responding to Identity Risk Detections

1. Go to **Identity**>**Protection > Risky Activities**.
2. Under **Risky Activities**, Navigate to **Report > Risky Users**
3. Identify users flagged for:
    - Atypical travel
    - Anonymous IP usage
    - Malware-linked IP addresses
4. Select a user > Click **Confirm Compromised** or **Dismiss**.
5. Recommended actions:
    - **Reset password**
    - **Force reauthentication**

- **Block sign-in** temporarily

6. Log response and actions taken in internal ticketing system.

4.5 Managing Security Defaults

1. Go to **Identity > Overview** and navigate to **Properties tab**. Scroll down to find Security default heading.
2. Click the "**Manage Security Defaults**" link (this may appear as a clickable sentence or a panel section depending on layout updates from Microsoft).
3. If your organization is not using Conditional Access, **enable Security Defaults** to enforce baseline security.
4. If CA is configured, **disable Security Defaults** to avoid overlap.
5. Save changes and document the setting status.

5. Conclusion

This SOP provides a comprehensive and standardized approach to implementing and maintaining security configurations within Microsoft Entra. By enabling MFA, deploying well-scoped Conditional Access policies, and continuously monitoring identity activity, organizations can protect sensitive data, enforce compliance, and significantly reduce the risk of unauthorized access.