SOP: MFA & Single Sign-On (SSO) Configuration

Owner: IFC-IT Team
Version: 1.0
Date Created: 2025-06-15

1. Purpose

To provide a precise and current workflow for implementing and managing Multi-Factor Authentication (MFA) and Single Sign-On (SSO) through Microsoft Entra (Azure AD) and Microsoft 365. This ensures strong identity protection, secure application access, and seamless user authentication aligned with the latest UI and platform updates.

2. Scope

This SOP applies to IT and security administrators responsible for:

- Enrolling user authentication using MFA
- Configuring Conditional Access policies to enforce MFA
- Setting up SSO with SaaS and internal applications via SAML or OIDC
- Testing, rolling out, and maintaining MFA and SSO configurations

3. Prerequisites

- Admin role: **Global Administrator**, **Security Administrator**, or **Conditional Access Administrator**
- Active Microsoft 365 license: **E3/E5 or Azure AD Premium P1/P2**
- Defined user groups (e.g., Admins, Staff, Contractors)
- Selected SaaS apps for SSO integration
- Access to application SSO metadata or SAML/OIDC configuration details

4. Procedures

4.1 Enabling MFA

4.1.1 Deploying MFA via Conditional Access

1. In Entra Admin Center, go to **Security** → **Conditional Access** → **Policies**
2. Click **+ New policy**, name as CA_EnableMFA_[TargetGroup]_[Date]
3. Under **Assignments** → **Users or workloads**:
    - Include appropriate groups (e.g., All users, or specific roles)
4. Under **Cloud apps or actions**:
    - Select **All cloud apps** or targeted apps only
5. Under **Conditions** (optional):
    - Exclude trusted network ranges or compliant devices
6. Under **Access controls** → **Grant** → select **Require multi-factor authentication**
7. Set policy mode to **Report-Only** (testing)
8. Save and record policy ID, scope, and mode in the policy register

4.1.2 Enforcing and Monitoring

1. Review **Sign-in logs** for MFA challenges and failures after certain days.
2. Move policy from **Report-Only** to **On** once verified.
3. Notify users of impending MFA enforcement.

4.2 Configuring Single Sign-On (SSO)

4.2.1 Registering an Enterprise Application

1. In Entra Admin Center → **Identity** → **Application** → **Enterprise Applications** → **+ New application**
2. Choose from gallery or select **Create your own application**
3. Name the app, e.g., AppName_SSO, and click **Add**

4.2.2 Configuring SAML-based SSO

1. Open the application → go to **Single sign-on** → select **SAML**
2. Input **Basic SAML Configuration**:
    - Identifier (Entity ID): from vendor
    - Reply URL (ACS): from vendor
    - Sign-on URL (optional)
3. Under **User Attributes & Claims**, configure:
    - NameID → user.userprincipalname (default)
    - Additional claims (e.g., email, givenname, surname)
4. Upload **Certificate (Base64)** from Microsoft for vendor configuration
5. Download **Federation Metadata XML** or manually collect parameters
6. In vendor's SSO dashboard, upload metadata or configure manually
7. Save configuration and set **SAML Signing Certificate** to **Active**

4.2.3 Configuring OpenID Connect (OIDC-based SSO)

1. In app → **Single sign-on** → select **OpenID Connect**
2. Enter:
    - Redirect URI
    - Logout URL (if applicable)
    - Client ID and Secret issued by Microsoft
3. Save configuration

4.2.4 Assigning Users to the Application

1. In Entra Admin Center → app → **Users and Groups**
2. Click **+ Add user/group**, select approved users
3. Assign role (if applicable)
4. Save assignment and log details

4.3 Testing MFA and SSO Implementation

4.3.1 MFA Testing

1. Log in as a test user within the targeted group
2. Confirm MFA challenge appears (Authenticator app, SMS, FIDO, etc.)
3. Validate fallback methods (e.g., phone call)
4. If fails, review Conditional Access policy and MFA settings

4.3.2 SSO Testing

1. Access the app via Microsoft 365 **My Apps portal** or direct link
2. SAML: Ensure SAML response includes correct claims
3. OIDC: Verify token is issued, and user is logged in
4. Check **Sign-in logs** in Entra Admin Center under **Monitoring**
5. Troubleshoot:
    - NameID mismatch
    - Incorrect certificate
    - Misconfigured reply URLs

5. Conclusion

This SOP ensures a robust, repeatable process for deploying MFA and SSO across Microsoft 365 and enterprise applications. By following standardized policies, phased rollout, and ongoing reviews, the organization achieves secure authentication, compliance readiness, and a streamlined user experience.