SOP Single Sign-On (SSO) Implementation through Microsoft Entra ID

Purpose

To define a standardized procedure for ensuring Single Sign-On (SSO) is enforced across all users via Microsoft Entra ID, and to provide a step-by-step process for integrating additional third-party applications into the organization’s SSO environment. Applies to all employees, interns, contractors, and approved partners using Microsoft 365 and any integrated third-party applications. IT personnel are responsible for setup, validation, and support of SSO configurations.

1. About Single Sign-On (SSO)
2. SSO is an authentication process that allows users to access multiple applications or services with a single set of login credentials (usually their organization email and password). Instead of logging in separately to Outlook, SharePoint, InvGate, and other tools, users authenticate once, and that session is trusted across connected applications.
3. Purposes:

* Simplify user access to multiple tools and platforms
* Enhance security by centralizing authentication and enforcing strong policies
* Reduce password fatigue and minimize risky user behavior
* Improve IT efficiency by consolidating identity management and reducing password-related support tickets

1. Benefits:

* Users sign in once and gain access to all connected services
* Centralized MFA enforcement, reduced password reuse, and better control over user access
* Fewer login prompts = increased productivity
* Users don’t forget multiple passwords, reducing helpdesk ticket volume
* Entra ID integrated with thousands of SaaS apps
* IT can deactivate users is one place and revoke access across all apps instantly
* Sign-in logs and alerts are centralized for easier tracking and reporting

1. Challenges:

* If Microsoft Entra ID is compromised or goes down, all connected services may be inaccessible
* Some applications require technical configuration
* If you only use Microsoft for authentication, a service disruption could impact operations
* SSO without MFA increases risk (i.e. if one password is stolen, many systems are exposed)
* Some third-party apps require premium licenses or advanced configuration for SSO integration

1. Enforcing SSO Org-Wide Using Microsoft Entra ID
2. Navigate to [https://entra.microsoft.com](https://entra.microsoft.com/) and verify that Microsoft Entra ID is in use and that all organizational users exist under **Users > All Users**.
3. Confirm that the default sign-in method is set to Microsoft Entra ID-based login for Microsoft 365 Suite, admin portals, and Endpoint Management tools.
4. Go to **Microsoft Entra Admin Center > Protection > Multifactor Authentication** and ensure all user accounts are enforced or enabled.
   1. Verify that Microsoft Authenticator is registered and set as the default second factor.
5. Navigate to **Protection > Conditional Access** and create or review existing policy “Require MFA and SSO for all users”:
   1. Target: **All Users**
   2. Cloud apps: **All Cloud Apps**
   3. Grant Controls: **Require MFA** and **Require device to be marked as compliant** (optional)
   4. Set policy to **Report-Only**, then enable
6. Under **Security > Conditional Access > Policies**, create or review existing policy “Block legacy authentication”:
   1. Assign to **All Users**
   2. Target: **Client apps > Other clients**
   3. Grant: **Block Access**
   4. Enable policy
7. Have a user sign into [https://myapps.microsoft.com](https://myapps.microsoft.com/) and confirm MFA prompt and seamless access to Microsoft 365 services.
   1. Confirm sign-in activity under **Microsoft Entra > Monitoring > Sign-in Logs**.
8. At this point, SSO is enforced across all users within the organization.
9. Integrating a New Application into Microsoft SSO
10. Go to **Microsoft Entra admin center > Identity > Applications > Enterprise Application > + New Application** and select the app from the app gallery OR create a non-gallery application if custom SAML is required.
11. Navigate to the app > Single Sign-On/SSO tab:
    1. Choose SAML (recommended)
    2. Manually configure Entity ID, Reply URL, and Sign-on URL between Microsoft Entra and the app OR
    3. Download Microsoft Federation Metadata XML and provide to the app administrator or upload on the app’s configuration screen.
12. In the app, navigate to the users tab, assign to all users or a specific test group for a phased rollout.
13. Use test account and navigate to [https://myapps.microsoft.com](https://myapps.microsoft.com/).
    1. Select the newly-integrated app and confirm SSO authentication and app access.
    2. Check **Sign-in logs** in Entra for success/failure.
14. Apps Available in the Entra App Gallery with Pre-Built SSO Integration

* Zoom
* Box
* DocuSign
* Notion
* GitHub
* Okta
* LinkedIn Learning
* Workday