SSO Solutions for Windows Devices

**Features and Solutions**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SSO Methods** | | **Single sign-on method** | **Application types** | **When to use** | | --- | --- | --- | | [OpenID Connect and OAuth](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/sso-options#openid-connect-and-oauth) | cloud and on-premises | Use OpenID Connect and OAuth when developing a **new application, best SSO experience**. This protocol simplifies application configuration, has easy-to-use SDKs, and enables your application to use MS Graph. | | [SAML](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/sso-options#saml-sso) | cloud and on-premises | Choose SAML whenever possible for existing applications that do not use OpenID Connect or OAuth. SAML works for **applications that authenticate using one of the SAML protocols**. | | [Password-based](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/sso-options#password-based-sso) | cloud and on-premises | Choose password-based when the application authenticates with username and password. Password-based single sign-on enables secure application password storage and replay using a **web browser extension or mobile app.** This method uses the existing sign-in process provided by the application, but enables an administrator to manage the passwords. | | [Linked](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/sso-options#linked-sign-on) | cloud and on-premises | Choose linked sign-on when the application is configured for single sign-on in another identity provider service. This option doesn't add single sign-on to the application, the **application** **SSO provided by**  **another service such as** **Active Directory Federation Services**. | | [Disabled](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/sso-options#disabled-sso) | cloud and on-premises | Choose **disabled single sign-on** when the app isn't ready to be configured for single sign-on. This mode is the default when you create the app. | | [Integrated Windows Authentication (IWA)](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/sso-options#integrated-windows-authentication-iwa-sso) | on-premises only | Choose IWA single sign-on for applications that use [Integrated Windows Authentication (IWA)](https://docs.microsoft.com/en-us/aspnet/web-api/overview/security/integrated-windows-authentication), or claims-aware applications. For IWA, the Application Proxy connectors use **Kerberos Constrained Delegation (KCD)** to authenticate users to the application. | | [Header-based](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/sso-options#header-based-sso) | on-premises only | Use header-based single sign-on when the **application uses headers for authentication.** Application Proxy uses Azure AD to authenticate the user and then passes traffic through the connector  service. | |
|  | **SSO Planning**  [Plan an Azure Active Directory single sign-on deployment | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-sso-deployment) |
| **SSO for Azure Premium license** | Microsoft recommendation:   * **Enable single sign-on (SSO)** across applications using managed devices or Seamless SSO for non-Windows10 devices. * If reauthentication is required, **use a** [**Conditional Access sign-in frequency policy**](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concepts-azure-multi-factor-authentication-prompts-session-lifetime)**.** * For users that sign in from **non-managed devices** or mobile device scenarios, persistent browser sessions may not be preferable, or you might use Conditional Access to enable persistent browser sessions with sign-in frequency policies. * **Limit the duration** to an appropriate time based on the sign-in risk, where a user with less risk has a longer session duration. |
| **SSO for Microsoft 365 Application with Azure free license** | * **Enable single sign-on (SSO)** across applications using managed devices or Seamless SSO for non-Windows 10 devices. * **Keep the Remain signed-in option enabled** and guide your users to accept it. * For mobile devices scenarios, make sure your users use the **Microsoft Authenticator app**. This app is used as a broker to other Azure AD federated apps, and reduces authentication prompts on the device. |
| **SSO Supported Browsers** | | **OS\Browser** | **Internet Explorer** | **Microsoft Edge\*\*\*\*** | **Google Chrome** | **Mozilla Firefox** | **Safari** | | --- | --- | --- | --- | --- | --- | | Windows 10 | Yes\* | Yes | Yes | Yes\*\*\* | N/A | | Windows 8.1 | Yes\* | Yes\*\*\*\* | Yes | Yes\*\*\* | N/A | | Mac OS | N/A | N/A | Yes | Yes | Yes | |
| SSO for OneDrive | For OneDrive, you will have to activate the [OneDrive silent config](https://docs.microsoft.com/en-us/onedrive/use-silent-account-configuration#enable-silent-configuration) feature for a silent sign-on experience by GPO, or registry key: [HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"SilentAccountConfig"="dword:00000001" |
| Windows 10 Managed Device SSO | * Devices joined to Azure AD using Azure AD Join or Hybrid Azure AD Join receive a [Primary Refresh Tokens (PRT)](https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-primary-refresh-token) to use single sign-on (SSO) across applications. * If a user needs to be asked to sign in more frequently on a joined device for some apps or scenarios, this can be achieved using [Conditional Access Sign-in Frequency](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime). |

**SSO and Conditional Access MFA**

|  |  |
| --- | --- |
| **Conditional Access (CA) Policy - Sign-in Frequency applied to MFA authentication** | Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.  The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.  The sign-in frequency setting **works with apps that have implemented OAUTH2 or OIDC** protocols according to the standards. Most Microsoft native apps for Windows, Mac, and Mobile including the following web applications comply with the setting.   * Word, Excel, PowerPoint Online * OneNote Online * Office.com * Microsoft 365 Admin portal * Exchange Online * SharePoint and OneDrive * Teams web client * Dynamics CRM Online * Azure portal * The sign-in frequency setting **works with SAML applications** as well, as long as they do not drop their own cookies and are redirected back to Azure AD for authentication. * The sign-in frequency setting **works on Azure AD registered Windows devices** **(BYOD)** too. |
| **Configure CA - Sign in Frequency** | * In CA Policy Properties, go to Access controls\Session\Sign-in Frequency:      * Before enabling Sign-in Frequency, make sure other reauthentication settings are disabled in your tenant. If "Remember MFA on trusted devices" is enabled, be sure to disable it before using Sign-in frequency, as using these two settings together may lead to prompting users unexpectedly. |
| **Note on Token lifetime** | Microsoft retired the configurable token lifetime feature for refresh and session token lifetimes on **January 30, 2021** and replaced it with the Conditional Access authentication session management feature. |
| **Multiple CA-Session Lifetime Policies.** | In Azure AD, the most restrictive policy for session lifetime determines when the user needs to reauthenticate. |
| **Microsoft Recommendation** | Enabling Azure AD Multi-Factor Authentication using Conditional Access policies is the [recommended](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates) approach to protect users. |

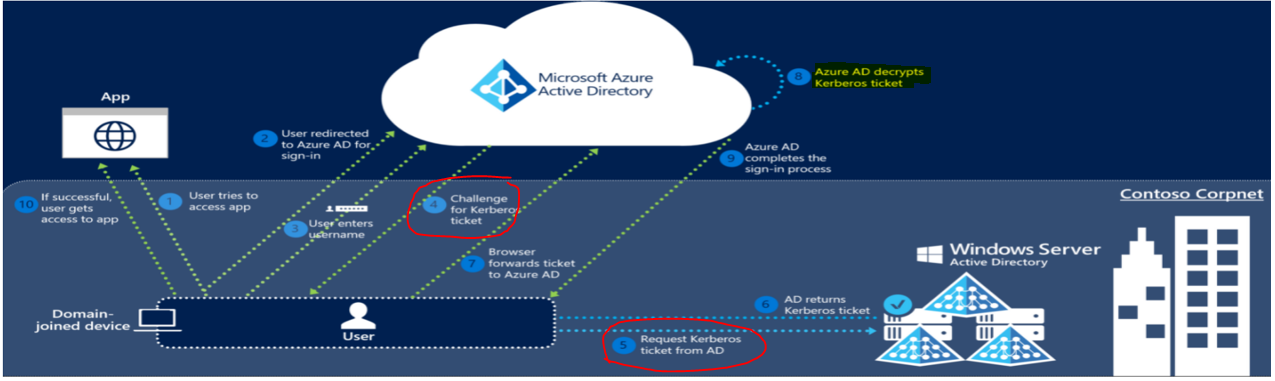
**TROUBLESHOOTING SSO**

|  |  |
| --- | --- |
| **A persistent browser session ( recommended for non Azure AD Premium license only)** | allows users to remain signed in after closing and reopening their browser window.  The Azure AD default for browser session persistence prompt users by showing a “Stay signed in?” dialog box after a successful authentication.  To hide the “Stay signed in”: using the document in [Customize your Azure AD sign-in page](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/customize-branding). (Azure AD\Company Branding\Advanced Settings)    Result on Client Device after User successfully sign in:  **Screenshot of the stay signed in page.**   * Keep me signed in (KMSI) service displays a Stay signed in? prompt after a user successfully signs in. * If a user answers Yes to this prompt, the keep me signed in service gives them a **persistent refresh token**   **MFA prompt:**     * While this setting reduces the number of authentications on web apps, it increases the number of authentications for modern authentication clients, such as Office clients * Setting this value to less than 90 days shortens the default MFA prompts for Office clients, and increases reauthentication frequency. * When used in combined with **Remain signed-in** **or Conditional Access policies, it** **may increase the number of authentication requests.** |
| **Multiple MFA prompts with CA - Sign in Frequency** | Some combinations of CA - Sign in Frequency and “Remember MFA” or CA - Sign in Frequency and Remain signed-in, can result in prompts for your users to authenticate [too often](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concepts-azure-multi-factor-authentication-prompts-session-lifetime#recommended-settings). |
| **SSO connectivity problems** | Use the [Remote Connectivity Analyzer](https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/single-sign-on-issues#how-to-run-remote-connectivity-analyzer-to-test-sso-authentication) tool to identify the problem on Domain Name resolution, port 443, certificates, ADFS metadata, ADFS token service |
| **MFA multiple prompt because of corrupted device account in Azure AD** | A user might see multiple MFA prompts on a device that **doesn't have an identity in Azure AD.** |
| **MFA multiple prompt because of non shared of PRT App** | Each application has its own **OAuth Refresh Token that isn't shared with other client apps**. In this scenario, MFA prompts multiple times as each application requests an OAuth Refresh Token to be validated with MFA. |
| **MFA loop because of conflict between “Keep me signed in” in ADFS and “Remember MFA” in Azure AD MFA** [**Setting**](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#enable-remember-multi-factor-authentication) | If your users select keep me signed in on AD FS and also mark their device as trusted for Multi-Factor Authentication, the user isn't automatically verified after the remember multi-factor authentication number of days expires. Azure AD requests a fresh multi-factor authentication, but AD FS returns a token with the original Multi-Factor Authentication claim and date, rather than performing multi-factor authentication again. This reaction sets off a verification loop between Azure AD and AD FS. |

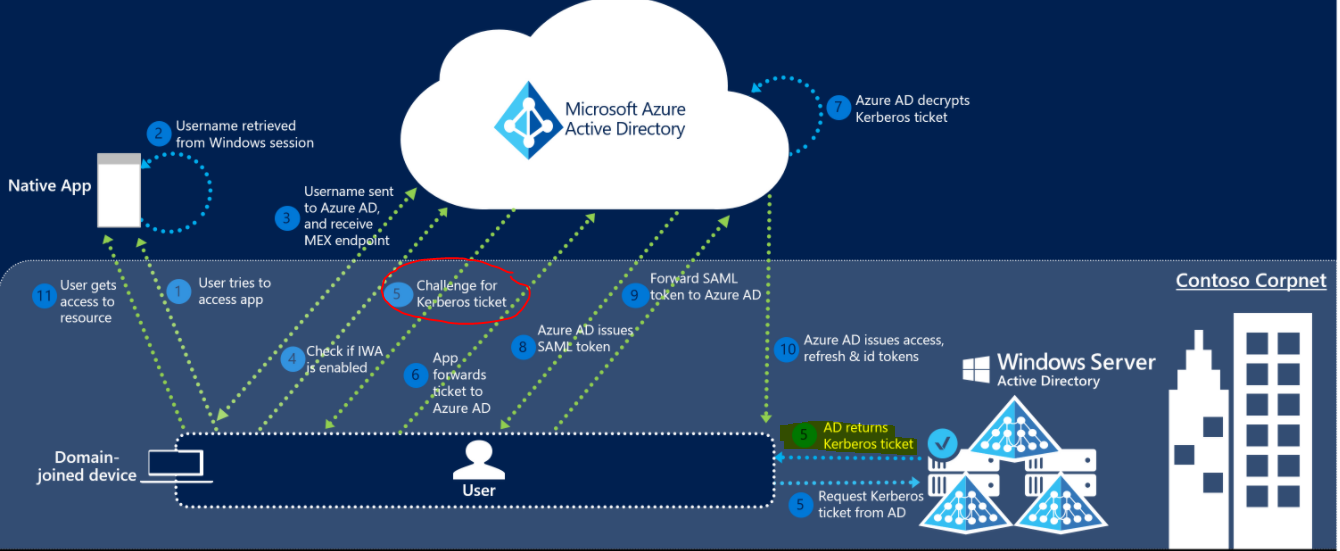
**Seamless SSO for Non-Windows 10**

Applied to Windows 8.1, 7, 2012, 2008R2 who are not joined Azure AD (by workplace join and on-premise Service Connection Point Server) and as a result there is no Device Account in AAD. Instead, Azure AD Connect from On-Premise Server will request AAD to create [AzureADSSOACC](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-how-it-works) for the Non-Windows 10 Devices so AAD could authenticate the Kerberos ticket sent by Non-Windows 10 Device.

**On Browser accessed to Azure Sign-in App:**



**On Native Client App to Azure Sign-in App: (AAD return with refresh token, access token, ID token)**



**Reference:**

* + [Azure AD Multi-Factor Authentication versions and consumption plans | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing)
  + [MFA for Office 365](https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/set-up-multi-factor-authentication)
  + [SSO for Office 365](https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/support-options-of-set-single-sign-on)
  + [Troubleshooting SSO by Remote Connectivity Analyzer](https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/single-sign-on-issues)
  + [Azure Seamless SSO](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-how-it-works)
  + [Customize your Azure AD sign-in page](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/customize-branding).
  + [Plan an Azure Active Directory single sign-on deployment | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-sso-deployment)
  + [SSO Options](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/sso-options)
  + [Azure AD Multi-Factor Authentication prompts and session lifetime | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concepts-azure-multi-factor-authentication-prompts-session-lifetime)
  + [OneDrive Silent Synchronization](https://techcommunity.microsoft.com/t5/microsoft-onedrive-blog/previews-for-silent-sync-account-configuration-and-bandwidth/ba-p/120894)
  + [Previews for Silent Sync Account Configuration and Bandwidth Throttling for OneDrive - Microsoft Tech Community](https://techcommunity.microsoft.com/t5/microsoft-onedrive-blog/previews-for-silent-sync-account-configuration-and-bandwidth/ba-p/120894)
  + [Configure MFA for Users](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userdevicesettings)
  + [MFA for SHA Token device](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#oath-tokens)
  + [Deploying MFA](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted)