

Single-Sign-On and Multi-Factor Authentication

Document Locator supports single-sign-on (SSO) in Desktop, Web, and Mobile for both on-premise and hosted systems using SAML or OIDC, and also allows for multi-factor authentication (MFA). Users can conveniently log in using their SSO account without the hassles of creating separate credentials, while multi-factor authentication adds an extra layer of security.

How it Works

Document Locator's SSO integration service connects to Microsoft Entra (Azure AD) via WebTools. Users are prompted for their login credentials and authenticated. Optionally, you can also enable multi-factor authentication.



SSO for Convenience and Security

Single-sign-on is an authentication method that allows users to log into multiple software applications using the same username and password. Users avoid the hassles of remembering login credentials for different systems, and IT has centralized control for enabling and disabling accounts.

MFA for Added Protection

You can optionally add an additional layer of security using multi-factor authentication which requires users to provide additional proof to verify their identity to gain access to the system. For example, after logging into Document Locator, a user would then have to confirm their identity and grant approval via an MFA app on their phone. This helps to ensure the authenticity of users and improves overall security.

Benefits

- Security**
 Improve security by reducing the number of passwords people have to remember, and use MFA to verify identity.
- Ease of use**
 Make user login familiar and comfortable for users who sign in, while centralizing accounts for IT.
- Meet regulatory compliance**
 Regulatory compliance requires that security guidelines are met. Using SSO and MFA helps to meet these guidelines.

(800) 298-1172
www.DocumentLocator.com

ColumbiaSoft Corporation
 15495 S.W. Sequoia Parkway
 Suite 190
 Portland, OR 97224