GUIDE TO CONNECTING YOUR EXISTING SINGLE SIGN-ON TO DOCUMOTO

Summary

This document serves as a comprehensive guide to connect your existing Single Sign-On (SSO) implementation to Documoto for user authentication. It outlines the requirements, communication flow, configuration steps, and the information required for the setup.

Documoto SSO Requirements

- Documoto exclusively supports SP-initiated SSO and SAML 2.0.
- Your metadata file should be publicly accessible via a URL.
- SHA-256 encryption is recommended.
- Documoto does not support SSO logout functionality.
- SSO implementation must use SAML Assertion signing.
- SSO can be combined with URL parameters for various purposes, such as auto-navigation within the application and configuration settings customization.
- SSO is not supported if Documoto is iframed.

How Documoto Supports SSO

Documoto supports SSO access to Documoto accounts via Secure Assertion Markup Language (SAML). SAML is an XML-based standard data format for exchanging authentication and authorization data between web-based applications.

SAML is comprised of the following main components:

- **Principal**: the user trying to authenticate into a web-based application.
- **Identity Provider (IdP)**: your server or authorization authority the user initially authenticates with.
    - *When connecting your existing SSO implementation to Documoto, the Identity Provider (IdP) is your server.*
- **Service Provider (SP)**: the web-based application that the user tries to access.
    - *When connecting your existing SSO to Documoto, the Service Provider (SP) is Documoto.*

Documoto SSO Communication Flow

1. Your Identity Provider maintains a public and private key.
2. Provide a metadata endpoint URL that advertises your public key.
3. Your Identity Provider makes an authentication/authorization decision and either:
    a. Redirects the user to Documoto with a signed SAML response.
    b. Informs the user they do not have an active session.
4. Documoto uses your IdP's public key to verify the signature. If the signature is valid, Documoto authenticates the user using the organization/user group(s)/email address provided by the SAML response.
5. SSO is initiated by forwarding a user to Documoto sign-on URL:
    - **Integration (Test) environment**: https://**[tenantkey]**.integration.documoto.com/ui/login?sso=true
    - **Production environment**: https://**[tenantkey]**.app.documoto.com/ui/login?sso=true
6. Upon receiving the sign-on URL, Documoto knows that the user wants to login via SSO.
7. If the Identity Provider passes valid attributes to Documoto, the user is authenticated, and redirects with an Authnrequest.

How to Configure SSO

To setup SSO with Documoto, follow these steps:

Identity Provider Setup

1. Import the relevant Documoto metadata URL to populate all necessary fields in your Identity Provider.

Documoto Environment	Metadata URL
Documoto Integration ("Test")	https://integration.digabit.com/saml/metadata
Documoto Production	https://documoto.digabit.com/saml/metadata

2. If metadata import is not feasible, manually configure the following settings:

Documoto Environment	Identifier or Entity ID	Reply URL (Assertion Consumer Service)
Documoto Integration ("Test")	com:documoto:int:sp	https://integration.digabit.com/saml/SSO
Documoto Production	com:documoto:prod:sp	https://documoto.digabit.com/saml/SSO

Documoto Setup

The following information must be provided to Documoto for configuration:

1. The URL to your Identity Provider's metadata file
2. IdP max session timeout
3. Define the following field names, as specified by your Identity Provider:
    - IdP attribute used to send Documoto Organization
    - IdP attribute used to send Documoto User Group
    - IdP attribute used to send Documoto Email Address

> ***NOTE: because Documoto maps the IdP email address field to the Documoto username field, Documoto cannot support usernames that are not an email address.***

Documoto will map these IdP field names to the corresponding Documoto fields and set the IdP max session timeout accordingly.

Validate SSO Setup

After configuring the Identity Provider and Documoto, initiate an SSO session by directing a user to the relevant sign-on URL using a web browser:

Documoto Environment	Sign-On URL
Documoto Integration ("Test")	https://**[tenantkey]**.integration.documoto.com/ui/login?sso=true
Documoto Production	https://**[tenantkey]**.app.documoto.com/ui/login?sso=true

SSO Support

If you have any questions or require assistance with Single Sign-On configuration, please contact your Documoto Customer Success Manager or Documoto Support at support@documoto.com.

Appendix A: Documoto URL Support for SSO & Integration Parameter Cross Reference

URL Type	Supports Direct URL Parameters?	Supports Single Sign-On?	Supports Integration URL Params?	Supports URL Parameter Refresh?
Base URL for Authentication documoto.com/ui/login	• **Open to Content**: Yes • **Execute a Search**: Yes	Yes	Yes	Yes
Base URL to Target & Open Media documoto.com/ui/mediaidentifierredirect	• **Open to Media**: Only opens Media • **Execute a Search**: Only executes a search within Media	Yes	Yes	Yes
Base URL to Execute a Search documoto.com/ui/search	• **Open to Media**: No • **Execute a Search**: Yes	Yes	Yes	Yes
Base URL to Execute a Search & Refresh User's Cookie documoto.com/api/redirect	• **Open to Media**: Yes • **Execute a Search**: Yes	No	Only the following parameters are supported: • rqid • cno	Yes
Documoto-Generated URL documoto.com/ui/	• **Open to Media**: Yes • **Execute a Search**: Yes	Yes	Yes	Yes