SAML Authentication Setup

Download the PDF of this article.

In this Article

Related Articles

Overview

SAML (Security Assertion Markup Language) can be used to secure access to your FormAssembly account.

Requirements

- SAML Metadata from your IdP
- Your FormAssembly username must match your SAML username

Single Sign-On (SSO) Setup

1. Navigate to the Admin Dashboard.
2. Click **Security** from the left side menu.
3. Scroll to the SAML section.
4. Click **Configure**.
    - If you're not logged in, you'll receive a notification saying, "You're not currently authenticated with your SAML Server." Click **OK** on the notification and log into your SAML Domain.
5. Under **Update Method**, choose your metadata option.
    - **Metadata URL Endpoint**
        - This is provided by the Identity Provider.
        - Enter your URL Endpoint.
        - Select **Update Domain**.
    - **Metadata File**
        - This is provided by the Identity Provider.
        - Upload your Metadata File.
        - Select **Update Domain**.
    - **Manual (Advanced)**

        - Add SAML data manually.
        - After entering your data, click **Apply**.
        - Select **Update Domain**.
6. After changes have been saved, your domain is set up and more options are shown for updating.
7. Click **Retrieve Attributes**.
    - If you're not logged in, you'll receive a notification saying, "You're not currently authenticated with your SAML Server." Click **OK** on the notification and log into your SAML Domain.
8. Your IdP attributes will be shown in the User Authentication table.
9. These attributes will be disabled by default so you can enable the attributes that you'd like to use.
10. Enable a **Unique SAML Attribute** from the table.
    - If you do not select a unique SAML attribute, you'll receive a red error indicating your changes were not saved.
    - Your unique SAML attribute must be **enabled** for SAML to be used.
11. Enter an **Authentication Formula**, if needed.
12. Click **Apply** to save your changes.

SAML Login Enforcement

Administrators can enforce a standardized login method for all users of the FormAssembly Instance or allow logins to be managed by user-level login preferences.

Login by Instance

1. Locate the **Instance Login Method** section, on the Security page in the Admin Dashboard.
2. Select **SAML** from the dropdown.
3. Select whether to allow administrators to override the SAML login method.
    - Allowing an administrator to override the login method would enable an admin to quickly recover the instance in the case of the SAML provider outage.
4. Click **Save** at the top of the page to save your settings.

Login by User

1. Access your All Users list.
2. Locate and edit the User(s) that need to use SAML
    - Select **SAML**, under the **User Login Method** of the Account section.
    - Click **Save User** at the top of the page to save the change.

Advanced Configuration of Metadata Fields

The following metadata fields may require additional consideration or special formatting:

NameIdFormat

The default value for this field is *urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*. If this field is left blank, the default value will be used.

The following formats are supported:

- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
- urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
- urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
- urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
- urn:oasis:names:tc:SAML:2.0:nameid-format:entity
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient
- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted

RequestedAuthNContext

The default value for this field is *urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport*. If this field is left blank, the default value will be used.

The following formats are supported (*Multiple values may be entered separated by a comma ","*):

- urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
- urn:oasis:names:tc:SAML:2.0:ac:classes:Password
- urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
- urn:oasis:names:tc:SAML:2.0:ac:classes:X509
- urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
- urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
- urn:federation:authentication:windows
- urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient

Updating Your SAML SSL Certificate

If you need to update your SAML SSL certificate you will use the self-serve configuration steps above to do so.

- If you already have a SAML configuration set up in your FormAssembly account you would update that configuration with your new metadata file with the new certificate, which you will import as part of the configuration.
- If you do not have a SAML configuration set up in your FormAssembly account, and your SAML configuration was originally set up by FormAssembly you will need to follow the process in this document to set up a SAML configuration in your FormAssembly account to update your SAML SSL certificate.