

SAML Authentication Setup

Download the PDF of this article.

In this Article

[Overview](#)

[Requirements](#)

[Single Sign-On \(SSO\) Setup](#)

[Form by Form Authentication Initial Setup](#)

[Advanced Configuration of Metadata Fields](#)

[SAML Prefill Connector Setup](#)

[Updating Your SAML SSL Certificate](#)

Related Articles

Overview

SAML (Security Assertion Markup Language) can be used to secure access to your FormAssembly account and forms. There are two methods for using SAML with FormAssembly:

Single Sign-On: this will allow users to sign into their FormAssembly account using their SAML credentials.

Form by Form Authentication: by enabling this feature, you will be able to restrict access to your forms by only allowing users who can be authenticated by your SAML server to access a form.

Requirements

- FormAssembly Team plan or above
- SAML Metadata from your IdP
- Your FormAssembly username must match your SAML username

Note: If you are interested in using Salesforce as the identity provider, [you can find more information here](#).

Note: If you are setting up both Single Sign-On and Form by Form Authentication on your FormAssembly instance, you will need two separate Identity Provider (IdP) entries, one for each configuration as noted below.

Single Sign-On (SSO)

(Replace "xxxxx" with your FormAssembly subdomain name)

- Entity ID: <https://xxxxx.tfaforms.net/saml/metadata>
- ACS URL: <https://xxxxx.tfaforms.net/saml/index?acs>

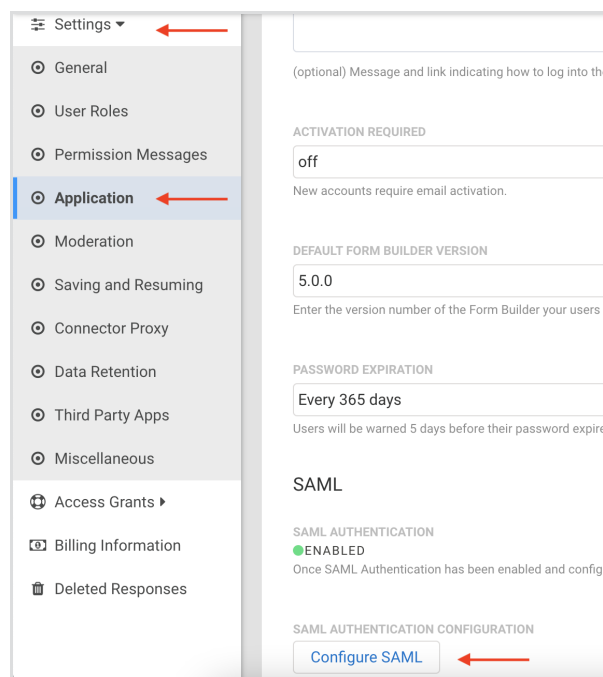
Form by Form Authentication

(Replace "xxxxx" with your FormAssembly subdomain name)

- Entity ID: https://xxxxx.tfaforms.net/authenticator_saml/metadata
- ACS URL: https://xxxxx.tfaforms.net/authenticator_saml/index?acs

Single Sign-On (SSO) Setup

1. Navigate to the Admin Dashboard.
2. Click Settings and then Application from the left side menu.
3. Scroll to the SAML section at the bottom.



4. Click Configure SAML.
 - If you're not currently logged in, you'll receive a popup that says You're not currently authenticated with your SAML Server. Click OK on the popup and log into your SAML Domain.

[Back to Application Settings](#)

Configure SAML for User Login

This feature restricts access to your instance by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

CURRENT DOMAIN

Domain has not been set. Update domain using controls below.

UPDATE METHOD

None (Disables SAML configuration)

[Update Domain](#) [cancel](#)

[Apply](#)

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.

[Back to Application Settings](#)

Configure SAML for User Login

This feature restricts access to your instance by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

UPDATE METHOD

Metadata URL Endpoint

XML METADATA URL PROVIDED BY YOUR IDP *

[Update Domain](#) [cancel](#)

[Apply](#)

- Metadata File
 - This is provided by the Identity Provider.
 - Upload your Metadata File.
 - Select Update Domain.

[Back to Application Settings](#)

Configure SAML for User Login

This feature restricts access to your instance by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

UPDATE METHOD

Metadata File

XML METADATA FILE PROVIDED BY YOUR IDP *

[Choose File](#) No file chosen

[Update Domain](#) [cancel](#)

[Apply](#)

- Manual (Advanced)
 - Add SAML data manually.
 - After entering your data manually, click Apply.
 - Select Update Domain.

[Back to Application Settings](#)

Configure SAML for User Login

This feature restricts access to your instance by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

UPDATE METHOD

Manual (Advanced)

SAML-STRICT

False

SAML-DEBUG

False

SAML-SP

SAML-SP-ENTITYID

<https://uat3.tfaforms.net/saml/metadata>

SAML-SP-ASSERTIONCONSUMERSERVICE

SAML-SP-ASSERTIONCONSUMERSERVICE-URL

<https://uat3.tfaforms.net/saml/index?acs>

SAML-SP-ASSERTIONCONSUMERSERVICE-BINDING

<urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST>

SAML-SP-SINGLELOGOUTSERVICE

6. After changes have been saved, your domain is set up and more options are shown for updating.

IDENTITY PROVIDER (IDP) DOMAIN

CURRENT DOMAIN
https://capriza.github.io/samling/samling.html

[Change Domain](#)

USER AUTHENTICATION

EXPOSE SAML ATTRIBUTES
This list displays the information available about each authenticated user. You may select which pieces of information you want to make available to FormAssembly. Please select at least one attribute.

[Enable All](#) [Retrieve Attributes](#)

ENABLED	ATTRIBUTE	ALIAS NAME
Empty		

UNIQUE SAML ATTRIBUTE *
No SAML attributes enabled

AUTHENTICATION FORMULA
f

(Enter a formula that evaluates to TRUE or FALSE to specify which users can authenticate from your IdP.)

[Apply](#)

7. Click Retrieve Attributes.

- If you're not currently logged in, you'll receive a popup that says You're not currently authenticated with your SAML Server. Click OK on the popup and log into your SAML Domain.

USER AUTHENTICATION

EXPOSE SAML ATTRIBUTES
This list displays the information available about each authenticated user. You may select which pieces of information you want to make available to FormAssembly. Please select at least one attribute.

[Disable All](#) [Retrieve Attributes](#)

ENABLED	ATTRIBUTE	ALIAS NAME
<input checked="" type="checkbox"/>	USERNAME	%%SAML_username%%
<input checked="" type="checkbox"/>	EMAIL	%%SAML_email%%

UNIQUE SAML ATTRIBUTE *
username

AUTHENTICATION FORMULA
f

(Enter a formula that evaluates to TRUE or FALSE to specify which users can authenticate from your IdP.)

[Apply](#)

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. Select Unique SAML attribute in your dropdown.

- If you do not select a unique SAML attribute dropdown, you'll receive a red error that your changes were not saved.
- Your unique SAML attribute must be enabled to be used.

11. Select Authentication formula if needed.

12. Click Apply to save your changes.

User Information

[Deactivate User](#)

EDIT USER

USERNAME
csTest

ROLE
Administrator

PAY-AS-YOU-GO CREDITS
0

AUTHENTICATION TYPE
Single-Sign-On

13. Access your All Users list. Edit Users that need to use SSO and select SSO under the Authentication Type dropdown.
14. Users will use the unique attribute to log in.

Form by Form Authentication Initial Setup

- From the Forms list, hover over Configure and select Processing.
- Choose Allow Responses from SAML Authenticated Users.

Processing Options

Any changes made in the processing section will be reflected everywhere the form is published, including Workflows.

FORM AVAILABILITY:

STATUS:

☒ Active

☐ Archived (no processing)

ALLOW RESPONSES FROM
SAML Authenticated Users

[Configure](#)

- Click **Apply**.

SPAM FILTER OPTIONS:

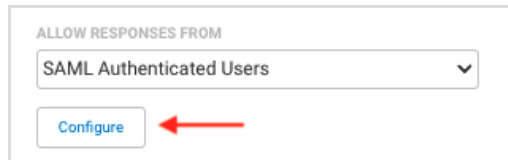
☐ Use Google reCAPTCHA (a challenge that helps prevent spam) ?

E-SIGNATURE:

☐ Enable E-Signature

[Apply](#)

- Click Configure under Allow Responses from SAML Authenticated Users dropdown box.

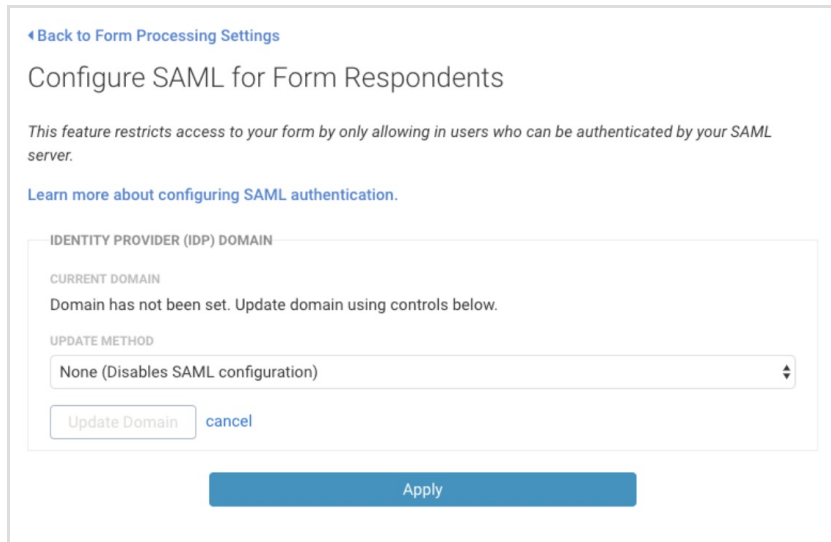


ALLOW RESPONSES FROM

SAML Authenticated Users ▼

Configure

- Under Update Method, choose your metadata option.



[Back to Form Processing Settings](#)

Configure SAML for Form Respondents

This feature restricts access to your form by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

CURRENT DOMAIN

Domain has not been set. Update domain using controls below.

UPDATE METHOD

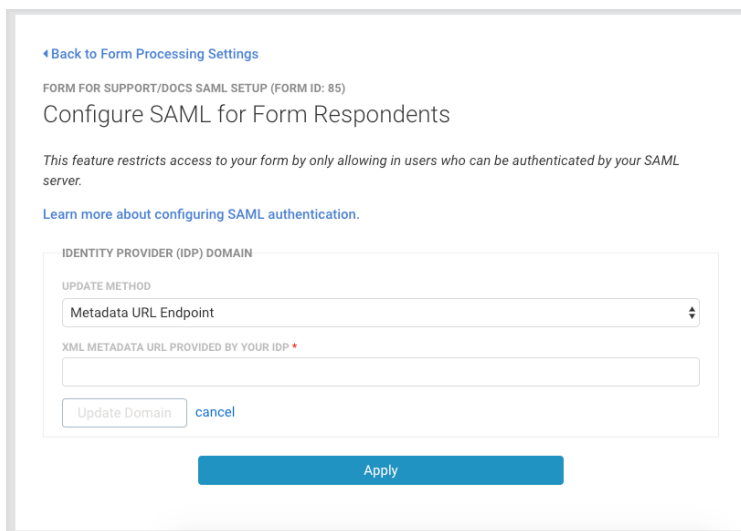
None (Disables SAML configuration) ▼

Update Domain cancel

Apply

- Metadata URL Endpoint.

- This is provided by the Identity Provider.
- Enter your URL Endpoint.
- Select Update Domain.



[Back to Form Processing Settings](#)

FORM FOR SUPPORT/DOCS SAML SETUP (FORM ID: 85)

Configure SAML for Form Respondents

This feature restricts access to your form by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

UPDATE METHOD

Metadata URL Endpoint ▼

XML METADATA URL PROVIDED BY YOUR IDP *

Update Domain cancel

Apply

- Metadata File.

- This is provided by the Identity Provider.
- Upload your Metadata File.
- Select Update Domain.

[Back to Form Processing Settings](#)

FORM FOR SUPPORT/DOCS SAML SETUP (FORM ID: 85)

Configure SAML for Form Respondents

This feature restricts access to your form by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

UPDATE METHOD

Metadata File

XML METADATA FILE PROVIDED BY YOUR IDP *

Choose File No file chosen

Update Domain cancel

Apply

- Copy from Form.

- This is used to copy the SAML settings and setup from another form already using SAML Authentication in your instance.
- Enter the ID of a form that already has SAML Authentication setup.
- Select Update Domain.

[Back to Form Processing Settings](#)

FORM 2 FOR SUPPORT/DOCS SAML SETUP (COPY) (FORM ID: 86)

Configure SAML for Form Respondents

This feature restricts access to your form by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

UPDATE METHOD

Copy From Form

FORM ID TO COPY SAML SETTINGS FROM *

86

Update Domain cancel

Apply

- Manual (Advanced).

- Add SAML data manually.
- After entering your data manually, click Apply.
- Select Update Domain.

[Back to Form Processing Settings](#)

FORM FOR SUPPORT/DOCS SAML SETUP (FORM ID: 85)

Configure SAML for Form Respondents

This feature restricts access to your form by only allowing in users who can be authenticated by your SAML server.

[Learn more about configuring SAML authentication.](#)

IDENTITY PROVIDER (IDP) DOMAIN

UPDATE METHOD

Manual (Advanced)

Update Domain cancel

Apply

- After changes have been saved, your domain is set up and more options are shown for updating.

IDENTITY PROVIDER (IDP) DOMAIN

CURRENT DOMAIN
https://capriza.github.io/samling/samling.html [Change Domain](#)

USER AUTHENTICATION

EXPOSE SAML ATTRIBUTES
This list displays the information available about each authenticated user. You may select which pieces of information you want to make available to FormAssembly. Please select at least one attribute.

[Enable All](#) [Retrieve Attributes](#)

ENABLED	ATTRIBUTE	ALIAS NAME
Empty		

UNIQUE SAML ATTRIBUTE *

Please select ...

AUTHENTICATION FORMULA

(Enter a formula that evaluates to TRUE or FALSE to specify which users can authenticate from your IdP.)

☐ Automatically resume the last saved response once authenticated. (Applies only if Save&Resume is enabled for this form.)

[Apply](#)

- Click Retrieve Attributes.
 - If you're not currently logged in, you'll receive a popup that says You're not currently authenticated with your SAML Server. Click OK on the popup and log into your SAML Domain.
- Choose Attributes

USER AUTHENTICATION

EXPOSE SAML ATTRIBUTES
This list displays the information available about each authenticated user. You may select which pieces of information you want to make available to FormAssembly. Please select at least one attribute.

[Disable All](#) [Retrieve Attributes](#)

ENABLED	ATTRIBUTE	ALIAS NAME
<input checked="" type="checkbox"/>	USERNAME	%%SAML_username%%
<input checked="" type="checkbox"/>	EMAIL	%%SAML_email%%

UNIQUE SAML ATTRIBUTE *

username

AUTHENTICATION FORMULA

(Enter a formula that evaluates to TRUE or FALSE to specify which users can authenticate from your IdP.)

☐ Automatically resume the last saved response once authenticated. (Applies only if Save&Resume is enabled for this form.)

[Apply](#)

- Your IDP attributes will be shown in the User Authentication Table.
- These attributes will be disabled by default so you can enable the attributes that you'd like to use.
- Select Unique SAML attribute in your dropdown.
 - If you do not select a unique SAML attribute dropdown, you'll receive a red error that your changes were not saved.
 - Your unique SAML attribute must be enabled to be used.
- Select Authentication formula if needed.
- Click Apply to save your changes.

- You can test your settings by viewing the form which will now require a login.

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

SAML Prefill Connector Setup

- Ensure SAML Authentication is setup on the Processing page of your form. Follow the steps above to enable.

- To enable the SAML prefill connector, click **Connectors** on the form you'd like to set up
- Next, drag in the **SAML Prefill Connector** into the **view section** of the timeline and click **Configure**.

If Step 1 shows SAML Authentication for Form Respondents is disabled, you'll need to configure your SAML Authentication.

- Then map the fields in your form to the SAML session attributes that you would like to fill those fields.
- When you're finished, click **Apply**

STEP 2 OF 2 - MAPPINGS

FORM FIELD	DATA SOURCE	SOURCE VALUE
<div>Not selected</div>	<div>Formula</div>	<div></div> <div></div>
<div>+ Add a New Field Mapping</div>		

- You're now ready to begin testing your SAML authentication and connector!

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.