



Community Deployment Guide

Configuring SAML Authentication

For Community Software Version 4.3+

Revision 1.0

July 20, 2021



phone 877-668-6870

web CommunityWFM.com

3400 Waterview Parkway, Suite 101

Richardson, Texas 75080

Table of Contents

Introduction.....	3
SAML 2.0 as a Mechanism for SSO Implementation	3
SAML 2.0 Terms:.....	3
Community’s Implementation of SSO via SAML 2.0.....	3
The Authentication Process:.....	4
SAML 2.0 Configuration Requirements	5
Identity Provider Requirements	5
Community Requirements	5
Okta and Community Configuration to Use SAML.....	6
Community’s SAML Logging Configuration.....	13
Troubleshooting SAML Authentication in Community.....	15
The Windows Server Application Log.....	15
Community’s SAML Debugging Endpoint	15
Setup notes utilizing various SAML IdPs.....	16
Okta	16
Azure Cloud ADFS.....	20



Introduction

As organizations implement multiple software systems, each with their own access control mechanisms, maintaining user identity and authentication information becomes a burdensome administrative task. The users of these systems are also burdened as they must remember multiple usernames and passwords and authenticate separately in each application.

To solve these issues, the concept of Single Sign On (SSO) was conceived.

SSO attempts to singly define the access control of multiple related software systems. With SSO, a user signs in with a single username and password and gains access to multiple systems without having to provide separate authentication to each system.

SAML 2.0 as a Mechanism for SSO Implementation

Security Assertion Markup Language (SAML) is a standard created for exchanging authentication data between applications or security domains. The SAML 2.0 protocol allows user information to be shared between a SAML 2.0 compliant authority and SAML 2.0 compliant applications. SAML 2.0 is an XML based protocol and all data exchanges are passed as standard XML documents. The SAML standard is maintained by The Organization for the Advancement of Structured Information Standards (OASIS).

Useful tutorial: <https://www.okta.com/integrate/documentation/saml/>

SAML 2.0 Terms:

Identity Provider (IdP) – A system that manages user information and provides authentication services for relying applications. An identity provider can be established using the services of vendors such as OneLogin, Okta and others. Organizations may alternatively choose to implement their own private IdP system. One popular example is the Gluu Server project.

Service Provider (SP) – Any software system used by an organization that relies on an IdP for access control. The WFMSG Community product is an example of a SP application.

Community's Implementation of SSO via SAML 2.0

The SAML 2.0 specification is vast and supports many possible methods of authenticating users. Community implements a redirection model of authentication. When Community senses that a



user needs to be authenticated, it redirects the user's browser to the configured IdP's site where authentication occurs.

The Authentication Process:

1. A user attempts to access a Community resource
2. Community senses the need to authenticate the user
3. Community redirects the user to the configured IdP endpoint
4. If the IdP has not previously authenticated the user, it prompts for username and password
5. If login is successful, the IdP generates a SAML 2.0 compliant XML authentication document
6. The IdP POSTs the XML document to Community's SAML 2.0 consumer at <https://companysite/CommunityWeb/UI/SAML/consumer.aspx>
7. Community verifies the authenticity of the XML document and reads the username
8. Community verifies the username internally, sets up the user's session, and presents the Community Today (home) page



SAML 2.0 Configuration Requirements

Identity Provider Requirements

When the Community application is set up with the identity provider, the SAML consumer endpoint within Community must be provided as part of the setup. The endpoint is:

<https://companysite/CommunityWeb/UI/SAML/consumer.aspx>

All firewall and security implementations must be configured to allow connectivity between the IdP and this endpoint.

Community Requirements

The following SAML parameters are required by Community:

- IdP endpoint URL
- IdP Issuer URL
- Community user ID XML tag name
- X.509 security certificate

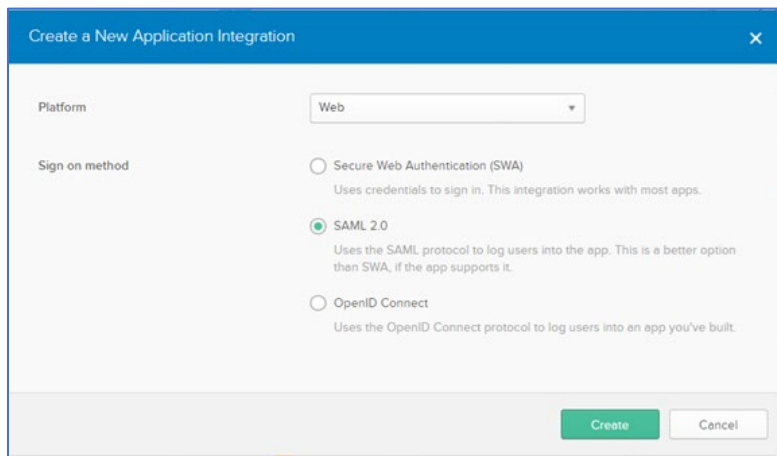
These values are generated or created when an administrator initially defines Community as a Service Provider application within the IdP system. These values must be known prior to performing Community's first-time setup as they are required to define SAML as the authentication method.

WFMSG requires an SSO user account be created for WFMSG support with access to the Community application.

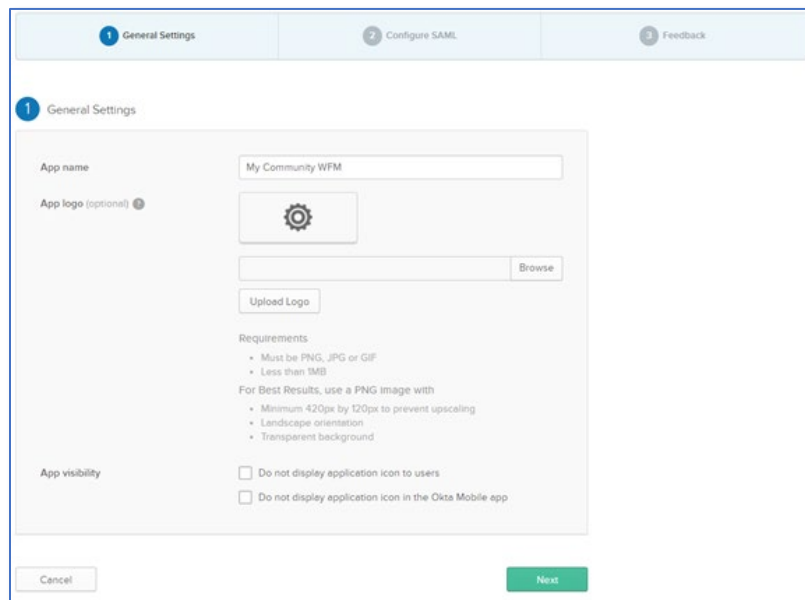
Okta and Community Configuration to Use SAML

From the Okta **Applications** menu page (using **Classic UI**):

1. Select **Add Application**
2. Select **Create New App**
3. Select **Web** for Platform
4. Select **SAML 2.0** for Sign on method
5. Click on **Create**:



6. General Settings:
 - a. Type in the App name and click **Next**:





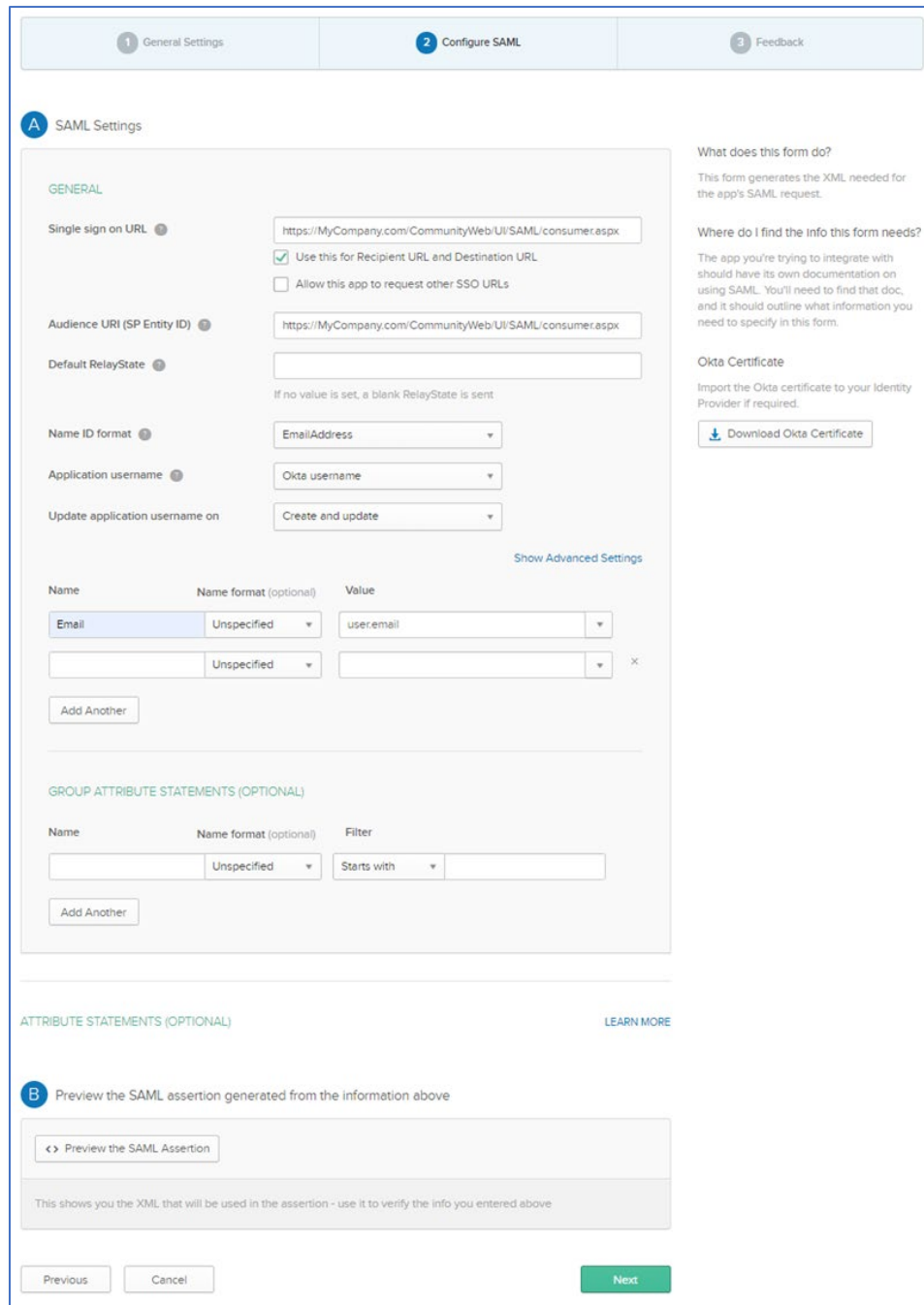
7. SAML Settings:

- a. For both **Single sign on URL** and **Audience URI (SP Entity ID)** use:

<https://MyCompany.com/CommunityWeb/UI/SAML/consumer.aspx>

Note: replace MyCompany.com with your Community server name/URL

- b. Select **EmailAddress** for Name ID format



1 General Settings 2 Configure SAML 3 Feedback

A SAML Settings

GENERAL

Single sign on URL

Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

Name	Name format (optional)	Value
Email	Unspecified	user.email
<input type="text"/>	Unspecified	<input type="text"/>

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
<input type="text"/>	Unspecified	Starts with <input type="text"/>

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

B Preview the SAML assertion generated from the information above

This shows you the XML that will be used in the assertion - use it to verify the info you entered above



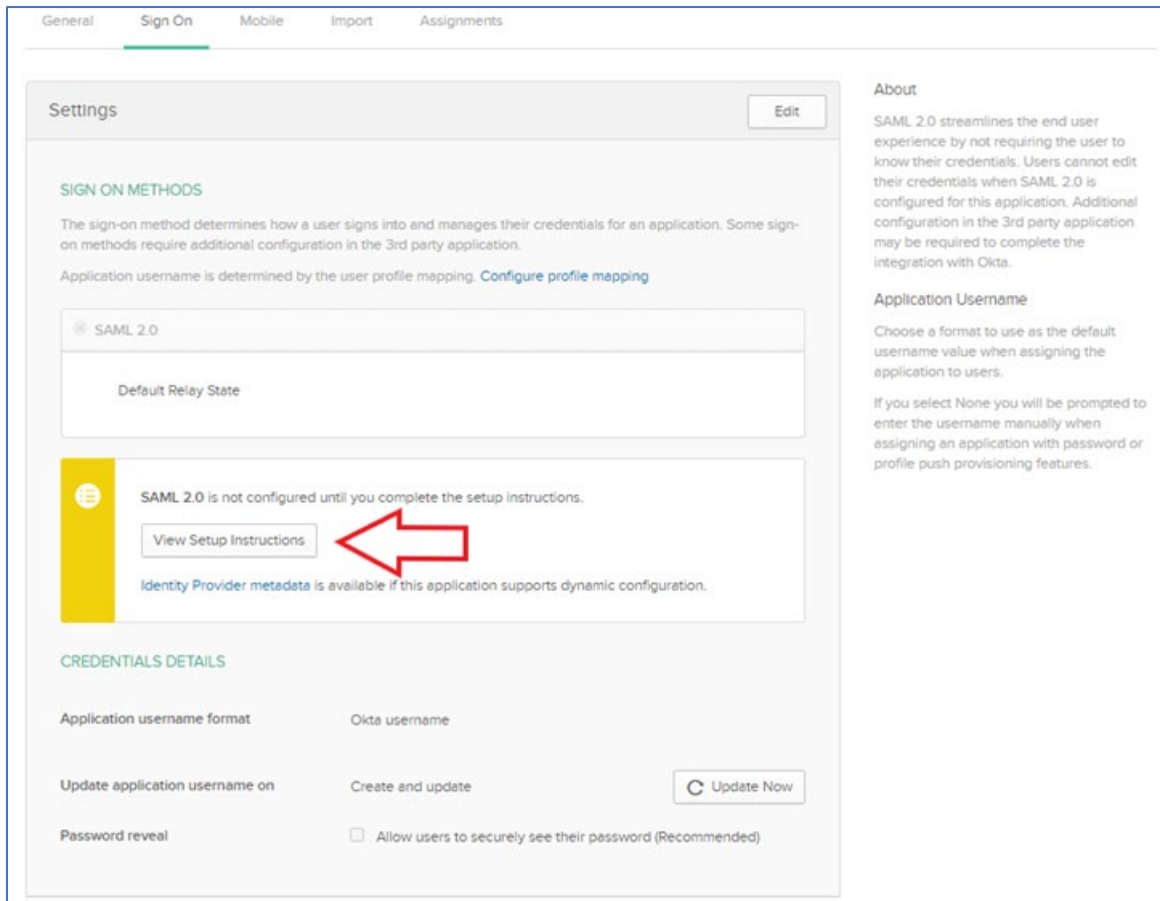
- c. Select **Okta username** for Application username
- d. Add Another using **Email** for the Name, **Unspecified** for the Name format, and **user.email** for Value and select **Add Another**
- e. Click **Next**

8. Feedback

- a. Select the options that apply to your company then click on **Finish**



9. Sign On configuration:
 - a. Click on **View Setup Instructions**:



- b. Copy and paste the fields into a text document and provide to CommunityWFM project manager. Following is an example of View Setup Instructions.



How to Configure SAML 2.0 for My Community WFM Application

The following is needed to configure My Community WFM

1 Identity Provider Single Sign-On URL:

```
https://dev-849595.oktapreview.com/app/dev-849595_mycommunitywfm_2/exkvv3capaLQ41Yj0h7/ssp/saml
```

2 Identity Provider Issuer:

```
http://www.okta.com/exkvv3capaLQ41Yj0h7
```

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDpDCCAOygAwIBAgIQAUF7ZBwQMA0GCsQGS1b3DQEBcUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNNUJ2FueiZyYW5jaXNjbzENMAsGA1UECgwET20YTEU
MBIGA1UECwWU1NPUHJvdmlkZXIxEzARBgNVBAMMcmR1di04NDk1OTUxHDAaBgkqhkiG9w0BCEQEW
DWluZm9Ab2t0YS5jb20wHhcNMjgwMjA5MjYyNTUyWncNMjgwMjA5MjYyNTUyWncjCBkzJELMAkGA1UE
BhMCMVVMxZzARBgNVBAGMCKNhbG1mb3JuaWExZjAUBG9NVBACMDVNBhBjBGMFuY2l2Y28xDTALBgNV
BAQMBE9rdGEzFDASBgNVBAsMCINT1B5b3ZpZGVyMRMwEQYDVQDDApkZXIYtODQ5NTk1MRwwGgYJ
KoZlHvcNAQkBFg1pbmZvQ9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
2b8Nbe+jXUMUsF5rRsY2BtSv6AwSIEK1B5SkdcGtETMcJgtx7Gfb5R3qZUtx/1F1th4NVHsmvwm9
8nyRy3xvbPFM4awW/ChJCLaJZcs05c71uCF3LozYoUM4J2BfcC-1b4/7YErzv7ebBQMVL84nE
1hXhCceSyZcjbzm9fN19ZMccoh+18kNIHhZdWD1ETfSb81kmrPkg69TgeP+c609rUBIRzh3VNS
CMtSMR14c+piGwi01jVvzAdwQDMuqCq+N5eKizJxAoe58Yk0p25CkEyi7hhoUBHssvzj3scgk
IXZkQ3Ds86RojPbWEE+/BtufiulKZ8JLa7WQIDAQABMA0GCsQGS1b3DQEBcUAA4IBAQBHQ3WQ
i47ss0VYjHnCukeRrCxtmmGRbnM9sOL4+Herg7T//YeCMgZUusyxe3tgv1SFNGWAfH7V1miJTP
gUF2zF1dWtzmzqgHnR7ly6pWXOMLPg43qo4Ppp6r8GzxIU23orYxmTsZuBGToYsYs1tc9j+bW
xRdDO1521dbD5f5ZCvio/hnbe41fR0tFDXpiTImUKrLYS9Hp+IU2mdin3jyChd5PwY2ZvyisaEq
o5g+gIV+neNLUP+q5YRMUBDMNBFSEzR1GptVW7Jly9GxJF5nvcChJYL4z4rRdr1kuJc5EY6+NX
tMTrcdQTOx1UcuJBVEgobrB1Okxu/OT
-----END CERTIFICATE-----
```

Download certificate

Optional

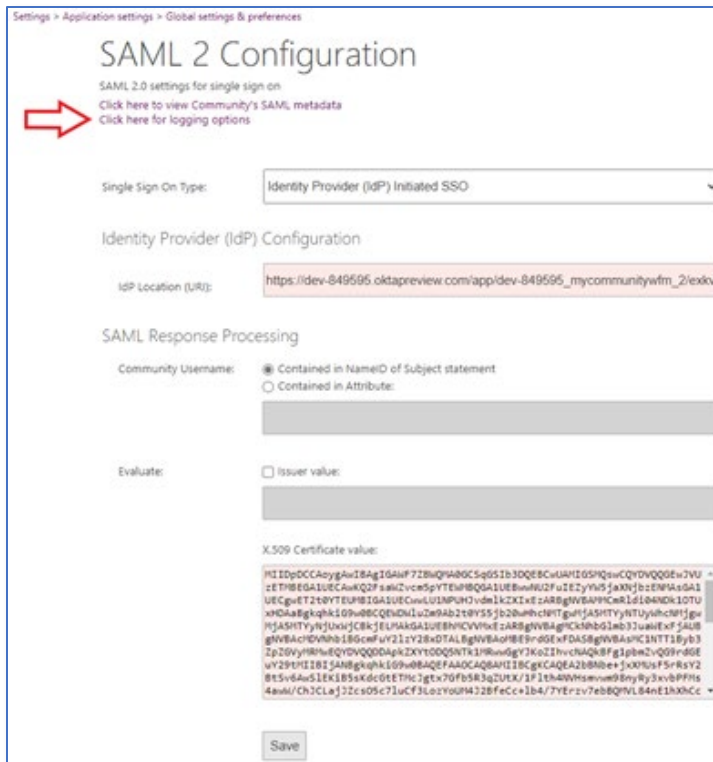
1 Provide the following IDP metadata to your SP provider.

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor entityID="http://www.okta.com/exkvv3capaLQ41Yj0h7"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"><md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data>
<ds:X509Certificate>MIIDpDCCAOygAwIBAgIQAUF7ZBwQMA0GCsQGS1b3DQEBcUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNNUJ2FueiZyYW5jaXNjbzENMAsGA1UECgwET20YTEU
MBIGA1UECwWU1NPUHJvdmlkZXIxEzARBgNVBAMMcmR1di04NDk1OTUxHDAaBgkqhkiG9w0BCEQEW
DWluZm9Ab2t0YS5jb20wHhcNMjgwMjA5MjYyNTUyWncNMjgwMjA5MjYyNTUyWncjCBkzJELMAkGA1UE
BhMCMVVMxZzARBgNVBAGMCKNhbG1mb3JuaWExZjAUBG9NVBACMDVNBhBjBGMFuY2l2Y28xDTALBgNV
BAQMBE9rdGEzFDASBgNVBAsMCINT1B5b3ZpZGVyMRMwEQYDVQDDApkZXIYtODQ5NTk1MRwwGgYJ
KoZlHvcNAQkBFg1pbmZvQ9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
2b8Nbe+jXUMUsF5rRsY2BtSv6AwSIEK1B5SkdcGtETMcJgtx7Gfb5R3qZUtx/1F1th4NVHsmvwm9
8nyRy3xvbPFM4awW/ChJCLaJZcs05c71uCF3LozYoUM4J2BfcC-1b4/7YErzv7ebBQMVL84nE
1hXhCceSyZcjbzm9fN19ZMccoh+18kNIHhZdWD1ETfSb81kmrPkg69TgeP+c609rUBIRzh3VNS
CMtSMR14c+piGwi01jVvzAdwQDMuqCq+N5eKizJxAoe58Yk0p25CkEyi7hhoUBHssvzj3scgk
IXZkQ3Ds86RojPbWEE+/BtufiulKZ8JLa7WQIDAQABMA0GCsQGS1b3DQEBcUAA4IBAQBHQ3WQ
i47ss0VYjHnCukeRrCxtmmGRbnM9sOL4+Herg7T//YeCMgZUusyxe3tgv1SFNGWAfH7V1miJTP
gUF2zF1dWtzmzqgHnR7ly6pWXOMLPg43qo4Ppp6r8GzxIU23orYxmTsZuBGToYsYs1tc9j+bW
xRdDO1521dbD5f5ZCvio/hnbe41fR0tFDXpiTImUKrLYS9Hp+IU2mdin3jyChd5PwY2ZvyisaEq
o5g+gIV+neNLUP+q5YRMUBDMNBFSEzR1GptVW7Jly9GxJF5nvcChJYL4z4rRdr1kuJc5EY6+NX
-----END CERTIFICATE-----
</ds:X509Certificate></md:KeyDescriptor></md:IDPSSODescriptor></md:EntityDescriptor>
```



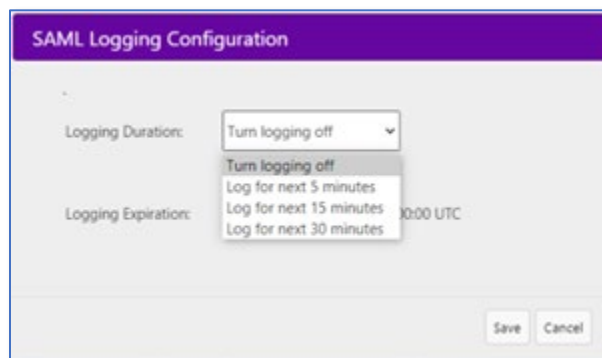

Community's SAML Logging Configuration

Community Version 4.4 Cumulative Service Release 2 (4.4SP2) provides users the ability to enable enhanced logging to troubleshoot SAML failures under the **Click here for logging options** link under the **Configure SAML Authentication** page under Settings > Application settings > Global settings & preferences:



The screenshot shows the 'SAML 2 Configuration' page. At the top, there are two links: 'Click here to view Community's SAML metadata' and 'Click here for logging options'. A red arrow points to the 'Click here for logging options' link. Below the links, the 'Single Sign On Type' is set to 'Identity Provider (IdP) Initiated SSO'. The 'Identity Provider (IdP) Configuration' section shows the 'IdP Location (URL)' as 'https://dev-849595.oktapreview.com/app/dev-849595_mycommunitywfm_2/enxv'. The 'SAML Response Processing' section has 'Community Username' set to 'Contained in NameID of Subject statement'. The 'Evaluate' section has 'Issuer value' checked. The 'X.509 Certificate value' section contains a long alphanumeric string. A 'Save' button is at the bottom.

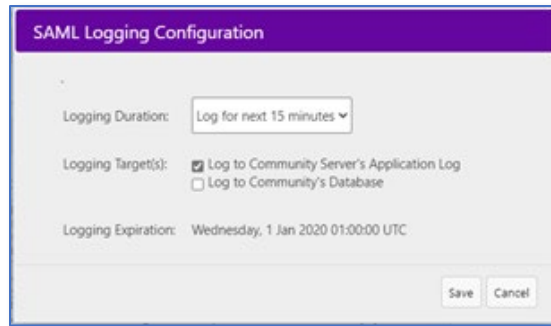
Users have the option to enable enhanced logging duration for the next 5 minutes, 15 minutes, or 30 minutes. The logging will automatically stop after reaching the specified duration:



The screenshot shows the 'SAML Logging Configuration' dialog box. It has a purple header. The 'Logging Duration' dropdown is set to 'Turn logging off'. The 'Logging Expiration' dropdown is set to 'Log for next 5 minutes'. The 'Logging Expiration' field also shows '10:00 UTC'. There are 'Save' and 'Cancel' buttons at the bottom.



In addition, the user has the option to select the logging target(s): **Log to Community Server's Application Log** and/or **Log to Community's Database**:



Following is an example of the logs reported:

```
[/SAML/consumer.aspx] SAML consumer called at 11/16/2020 2:46:34 PM.
[/SAML/consumer.aspx] Attempting to read Community's SAML configuration...
[/SAML/consumer.aspx] Community's SAML configuration was successfully read.
[/SAML/consumer.aspx] HTTP POST binding detected.
[/SAML/consumer.aspx] POST data successfully read. (Length: 6275)
[/SAML/consumer.aspx] SAMLResponse was successfully read. (Length: 6208)
[/SAML/consumer.aspx] Decode was successful.
[/SAML/consumer.aspx] Creating Response object...
[/SAML/consumer.aspx] Response object created.
[/SAML/consumer.aspx] StatusCode evaluation...<PASS>
[/SAML/consumer.aspx] IssueInstant evaluation...<PASS>
[/SAML/consumer.aspx] Reading Community username from attribute Email...
[/SAML/consumer.aspx] Failed to read from Attribute Email
[/SAML/consumer.aspx] These Attributes were presented...
Key: 'http://schemas.microsoft.com/identity/claims/tenantid' Holds Value: '93ca9525-cce1-42c8-8b0d-8ce24900b910'
Key: 'http://schemas.microsoft.com/identity/claims/objectidentifier' Holds Value: '26254ad1-37b4-43da-9a19-79f032f9b8fc'
Key: 'http://schemas.microsoft.com/identity/claims/identityprovider' Holds Value: 'https://sts.windows.net/36ee4888-e62d-476c-924a-a7dc71ba90fe/'
Key: 'http://schemas.microsoft.com/claims/authnmethodsreferences' Holds Value: 'http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password'
Key: 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name' Holds Value: 'agentname@wfmsg.com'
Key: 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email' Holds Value: 'agentname@wfmsg.com'
```

Troubleshooting SAML Authentication in Community

The Windows Server Application Log

When the SAML authentication process fails, the user is presented with a generic “SAML authentication failure” page without details of why the failure occurred. Specific details about the failure can be found in the Community server’s application log.

Community’s SAML Debugging Endpoint

Community also provides a debugging endpoint that provides useful details while troubleshoot SAML failures.

To use this resource:

- At the IdP, temporarily change the Community application’s consumer endpoint to:
<https://companysite/CommunityWeb/UI/SAML/test.aspx>
- Perform a user login
- Community will display a debugging page

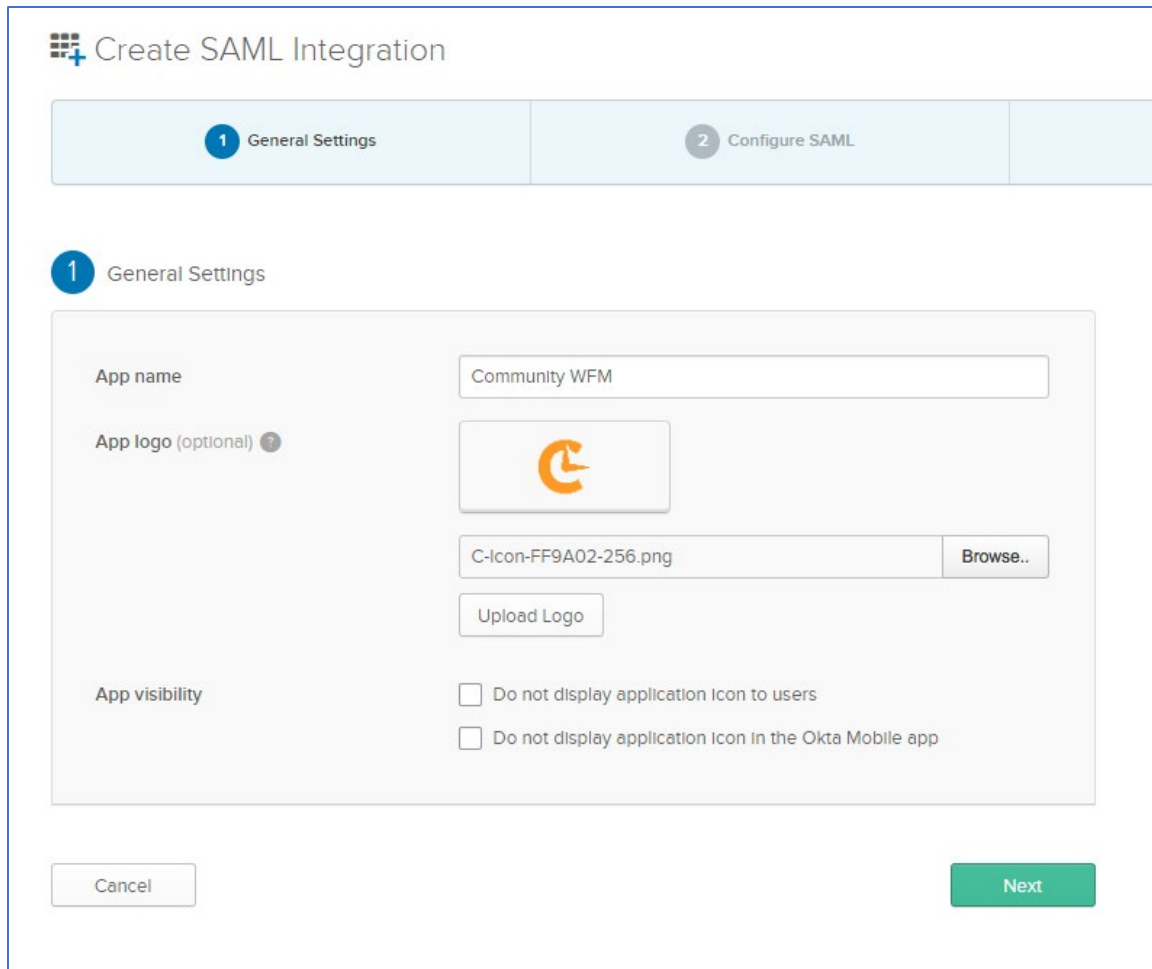
The debugging page displays the exact parameter values that were contained in the XML document received from the IdP. These values can be used to identify and repair any mismatches contained in Community’s SAML configuration.



Setup notes utilizing various SAML IdPs

Okta

From the Okta Applications menu page, select Add Application| Create New App. Create a platform “web”, **SAML 2.0** application.



The screenshot shows the 'Create SAML Integration' wizard in Okta. It has two steps: '1 General Settings' and '2 Configure SAML'. The 'General Settings' step is active and contains the following fields and options:

- App name:** A text input field containing 'Community WFM'.
- App logo (optional):** A section containing a logo preview of the CommunityWFM logo, a file input field with the filename 'C-Icon-FF9A02-256.png', a 'Browse..' button, and an 'Upload Logo' button.
- App visibility:** Two checkboxes:
 - Do not display application Icon to users
 - Do not display application Icon in the Okta Mobile app

At the bottom of the form, there are 'Cancel' and 'Next' buttons.

When asked for the Single Sign On URL use:

<https://ReplaceWithYourCompanySite//CommunityWeb/UI/SAML/test.aspx> to test and then replace with the application url below

<https://ReplaceWithYourCompanySite/CommunityWeb/UI/SAML/consumer.aspx>,

use the same URLs for Audience as used for Single Sign On.



Add an attribute under “Attribute Statements” with name of **Email**, format can remain ‘**unspecified**’ and the value should be **user.email**

A
SAML Settings

GENERAL

Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

Name	Name format (optional)	Value
Email	Unspecified	user.email

The remainder of the configuration can remain at their defaults.

After progressing through the wizard and completing the creation of the app, it should bring you to the “Application Sign On Page”:



Select "View Setup Instructions." This has the parameters necessary to configure the Community side of the connection.

The screenshot shows a 'Settings' window with an 'Edit' button in the top right corner. The main heading is 'SIGN ON METHODS'. Below this, there is explanatory text: 'The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.' and 'Application username is determined by the user profile mapping. [Configure profile mapping](#)'. A radio button labeled 'SAML 2.0' is selected. Below it is a text input field for 'Default Relay State'. A yellow warning banner contains a list icon, the text 'SAML 2.0 is not configured until you complete the setup instructions.', a 'View Setup Instructions' button, and the text 'Identity Provider metadata is available if this application supports dynamic configuration.' Below the warning is the 'CREDENTIALS DETAILS' section, which includes: 'Application username format' set to 'Okta username'; 'Update application username on' set to 'Create and update' with an 'Update Now' button; and 'Password reveal' with an unchecked checkbox and the text 'Allow users to securely see their password (Recommended)'.



The following is an example of what is displayed after selecting "View Setup Instructions."

The following is needed to configure Community WFM

- 1 Identity Provider Single Sign-On URL:

https://dev-849595.oktapreview.com/app/wfmsgincdev849595_communitywfm_1/exkk1071oorIdFm270h7/sso/saml

- 2 Identity Provider Issuer:

http://www.okta.com/exkk1071oorIdFm270h7

- 3 X.509 Certificate:


```

-----BEGIN CERTIFICATE-----
MIIDpDCCAOyGAWF7ZBwQMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FueIEZyYW5jaXNjbzENMAAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBGNVBAAMCmR1di04NDk1OTUxHDAaBqkqhkiG9w0BCQEW
DW1uZm9Ab2t0YS5jb20wHhcNMjAwMjA5MjYyNTUyWhcNMjAwMjA5MjYyNTUyWhcNMjAwMjA5MjYy
BhMCMVVMxEzARBGNVBAAMCmR1di04NDk1OTUxHDAaBqkqhkiG9w0BAQEEFAAOCAQ8AMIIBoCkCAQEA
2b8Nbe+jxXMUsF5rRsY2BtSv6AwS1EKiB5sKdcGtETMcJgtz7Gfb5R3qZUtX/1F1th4NVHsmvwm9
8nyRy3xvbPFMs4awW/ChJCLaJZcs05c71uCF3LozYoUM4J2BfeCc+1b4/7YErzv7ebBQMVL84nE
1hXhCoeSyZcjbzm9fNi9ZMccoh+18kN1HhZdWD1ETfSb81kmrhPkPg69TgeP+c609rUBIRzh3VNS
CMTt5MR14c+p1Gwi01jVvzAdwQDMuqiCq+N5eK1zJxAoe58Yk0p25CkEyi7hhoU80hssvzj3scgL
iXZkQ3Ds86zRoJPbWE++/Btufiu1KZ8JLa7WQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBHQ3WQ
i47ssS0VYjHnCukeRrCxtmm9RbnM9sOL4+Herg7T//YaCMgZUsyxse3tgv1SfNGWAfh7V1miJTP
gUF2zF1daWtnzmqgHNqR71y6pWxOMLPg43qo4Ppp6r8GzxIU23orYxmTsZuBGToYsYs1tc9j+bW
xRdD0152i dbD5 f52Cv io/hnbe41 fR0tFDXpiT1mUKrLYS9Hp+IU2mdin3ijyChd5PwY2Zvy1saEq
oSg+g1V+neNLUP+q5YRMUBDMNBFSEzR1GptVW7J1y9GxJFSnVbChJY1L4z4rRdr1kuJc5EY6+NX
tMYnrCdQY0xiUcuJ8VEgcbR10kxu/OT
-----END CERTIFICATE-----
                
```

Please copy and paste each of these in their entirety into a text document and provide to WFMMSG Project Manager.

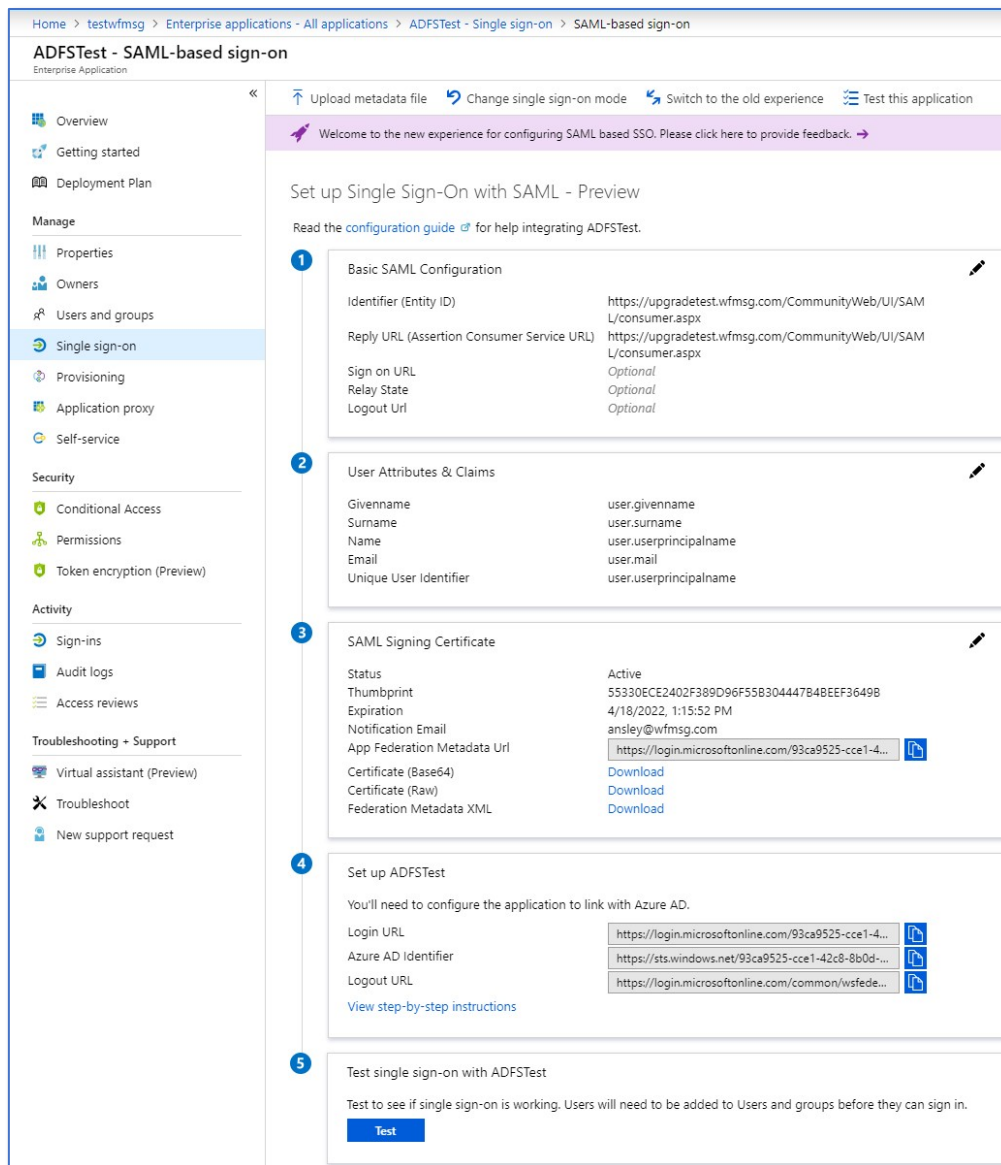


Azure Cloud ADFS

1. In the Basic SAML Configuration section, two values that need to be set on the ADFS side are the "Identifier (Entity ID)" and the "Reply URL (Assertion Customer Service URL)". Those need to be set to

<https://ReplaceWithYourCompanySite/CommunityWeb/UI/SAML/test.aspx> to test and then replace with the application url once testing is complete

<https://ReplaceWithYourCompanySite/CommunityWeb/UI/SAML/consumer.aspx>



The screenshot shows the Azure AD portal interface for configuring SAML-based sign-on for an application named "ADFTTest". The left-hand navigation pane includes sections for Overview, Getting started, Deployment Plan, Manage (Properties, Owners, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service), Security (Conditional Access, Permissions, Token encryption), Activity (Sign-ins, Audit logs, Access reviews), and Troubleshooting + Support (Virtual assistant, Troubleshoot, New support request).

The main content area is titled "ADFTTest - SAML-based sign-on" and includes a navigation breadcrumb: Home > testwfmsg > Enterprise applications - All applications > ADFTTest - Single sign-on > SAML-based sign-on. Below the breadcrumb are links for "Upload metadata file", "Change single sign-on mode", "Switch to the old experience", and "Test this application". A welcome message states: "Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback." Below this is a "Set up Single Sign-On with SAML - Preview" section with a link to the "configuration guide".

The configuration is divided into five numbered steps:

- Basic SAML Configuration:**
 - Identifier (Entity ID): `https://upgradetest.wfmsg.com/CommunityWeb/UI/SAML/consumer.aspx`
 - Reply URL (Assertion Consumer Service URL): `https://upgradetest.wfmsg.com/CommunityWeb/UI/SAML/consumer.aspx`
 - Sign on URL: *Optional*
 - Relay State: *Optional*
 - Logout Url: *Optional*
- User Attributes & Claims:**
 - Givenname: `user.givenname`
 - Surname: `user.surname`
 - Name: `user.userprincipalname`
 - Email: `user.mail`
 - Unique User Identifier: `user.userprincipalname`
- SAML Signing Certificate:**
 - Status: Active
 - Thumbprint: `55330ECE2402F389D96F558304447B48EEF36498`
 - Expiration: 4/18/2022, 1:15:52 PM
 - Notification Email: `ansley@wfmsg.com`
 - App Federation Metadata Url: `https://login.microsoftonline.com/93ca9525-cce1-4...`
 - Certificate (Base64): [Download](#)
 - Certificate (Raw): [Download](#)
 - Federation Metadata XML: [Download](#)
- Set up ADFSTest:**
 - You'll need to configure the application to link with Azure AD.
 - Login URL: `https://login.microsoftonline.com/93ca9525-cce1-4...`
 - Azure AD Identifier: `https://sts.windows.net/93ca9525-cce1-42c8-8b0d-...`
 - Logout URL: `https://login.microsoftonline.com/common/wsfede...`
 - [View step-by-step instructions](#)
- Test single sign-on with ADFSTest:**
 - Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.
 - [Test](#)



- In the User Attributes & Claims section, select edit (pencil icon) and then edit the individual "claim" for the email address. Different from the image below the Claim Name will contain the entire "Namespace".

User Attributes & Claims □ ×

+ Add new claim

Name identifier value: **user.userprincipalname [nameid-format:emailAddress]** ✎

Groups returned in claim: **None** ✎

CLAIM NAME	VALUE	...
Email	user.mail	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname	...

- The "Namespace" needs to be removed and the "Name" should be set to the shorter text of "Email".

Manage user claims ×

* Name ✓

Namespace

Source Attribute Transformation

* Source attribute ▼



4. Please copy and paste each of these in their entirety into a text document and provide to WFMSG Project Manager.
 - a. The ADFS "Login URL" = "SAML IdP Endpoint"
 - b. The ADFS "Azure AD Identifier" = "SAML Issuer"
 - c. The ADFS User Attribute name of "Email" = "SAML XML User Attribute"
 - d. The ADFS Certificate (Base64) = "Security Cert"