Community Deployment Guide

Configuring SAML Authentication

For Community Software Version 4.3+

Revision 1.0

July 20, 2021

CommunityWFM

phone 877-668-6870
web CommunityWFM.com

3400 Waterview Parkway, Suite 101
Richardson, Texas 75080

Table of Contents

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

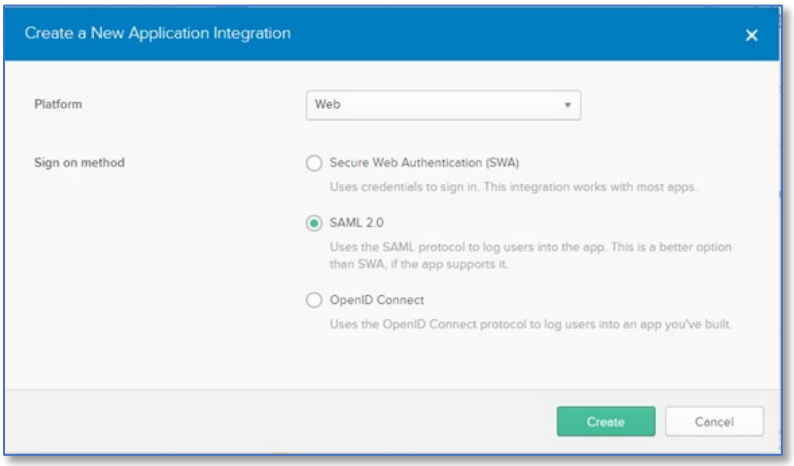
These values are generated or created when an administrator initially defines Community as a Service Provider application within the IdP system. These values must be known prior to performing Community's first-time setup as they are required to define SAML as the authentication method.

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

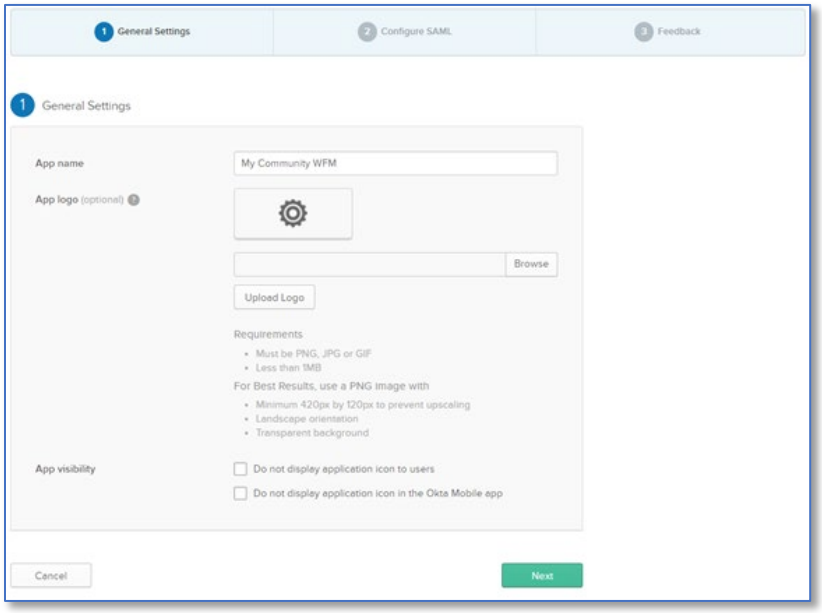
Okta and Community Configuration to Use SAML

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**:

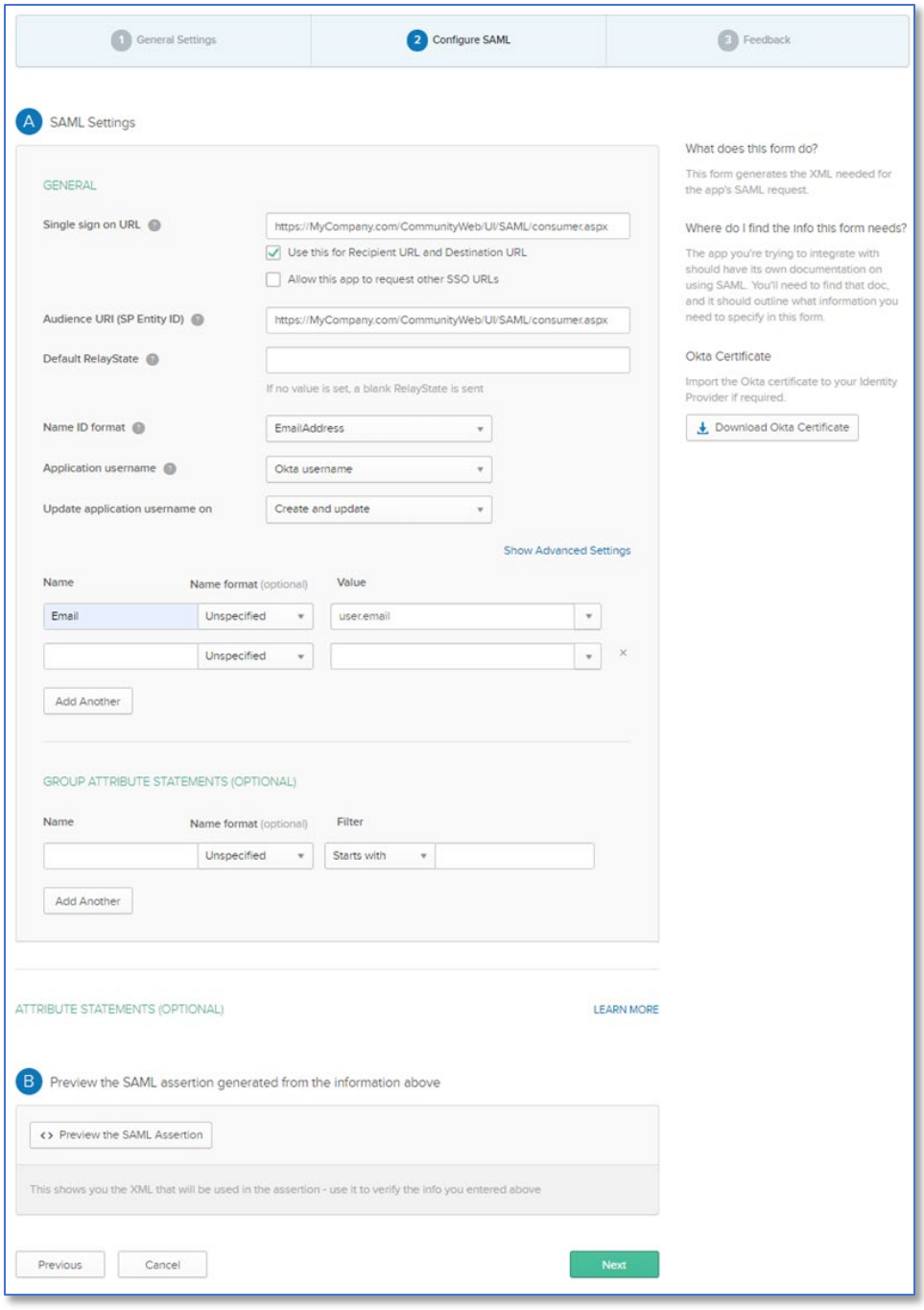


7. SAML Settings:
    a. For both **Single sign on URL** and **Audience URI (SP Entity ID)** use:

    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



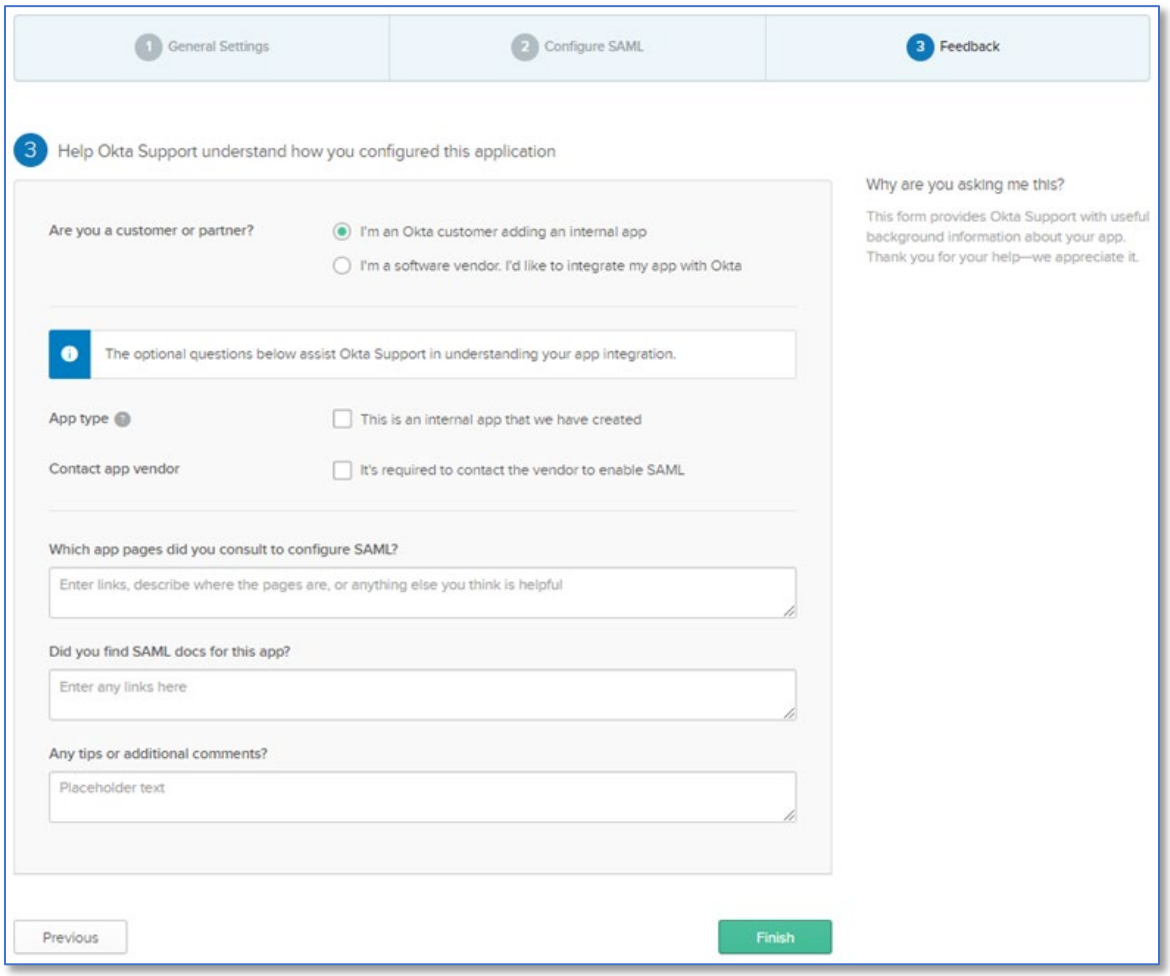
c. Select **Okta username** for Application username

d. Add Another using **Email** for the Name, **Unspecified** for the Name format, and **user.email** for Value and select **Add Another**

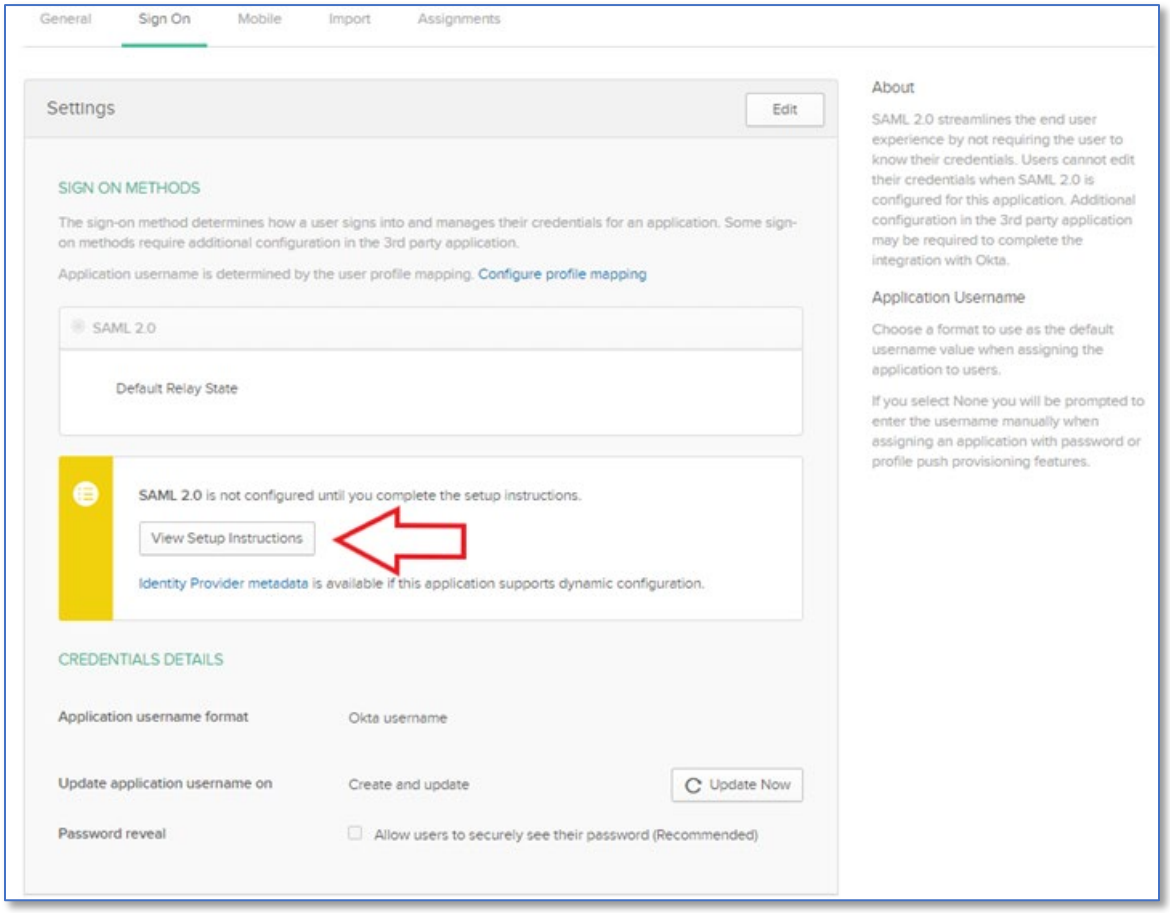
e. Click **Next**

8. Feedback

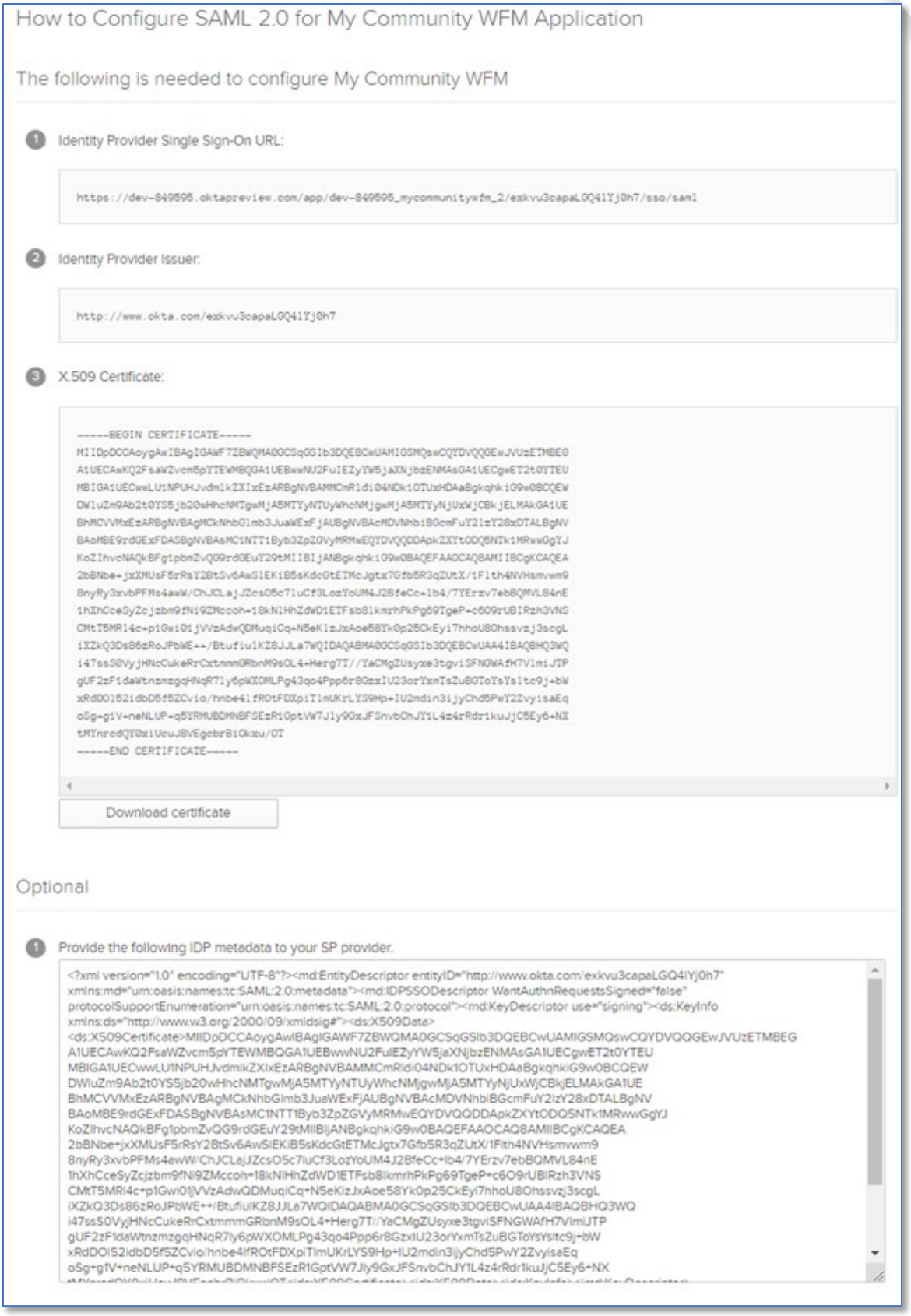
a. Select the options that apply to your company then click on **Finish**



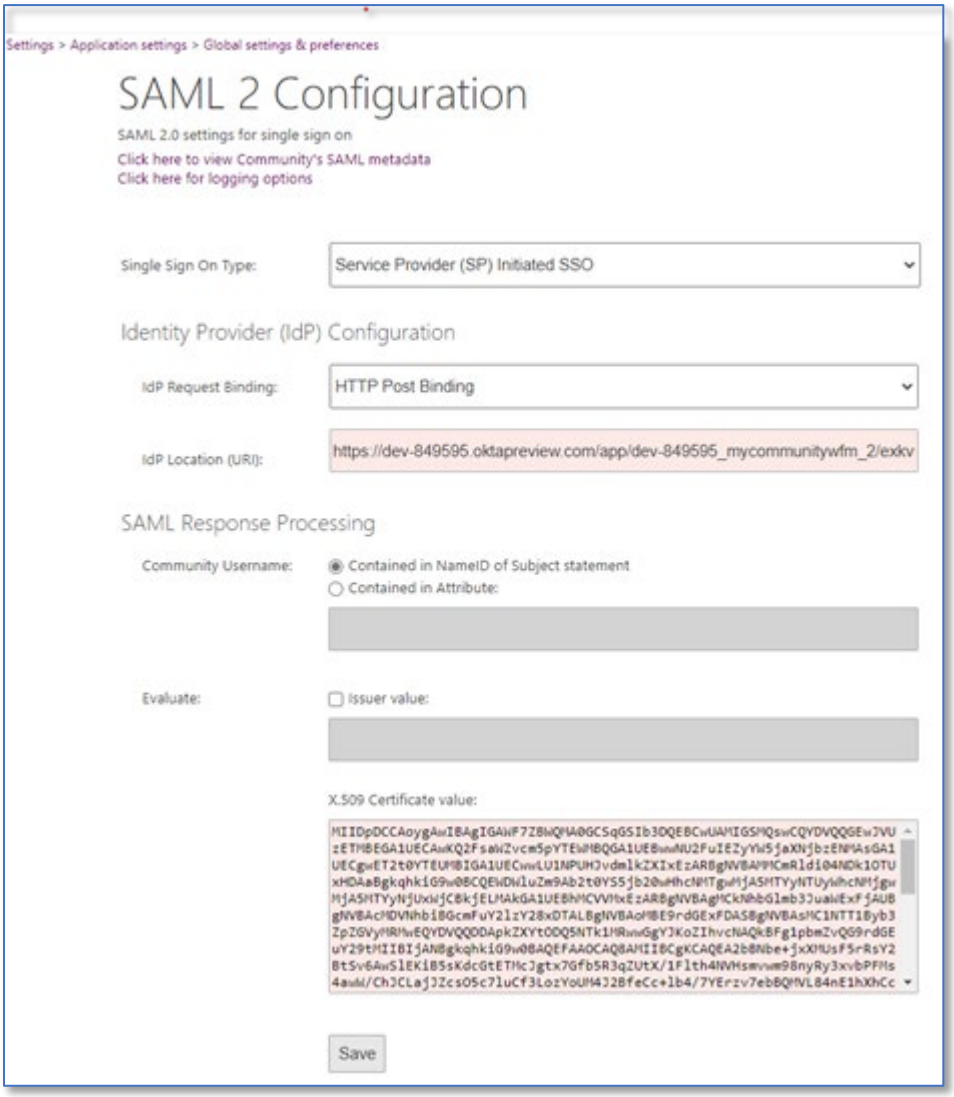
9. Sign On configuration:
    a. Click on **View Setup Instructions**:



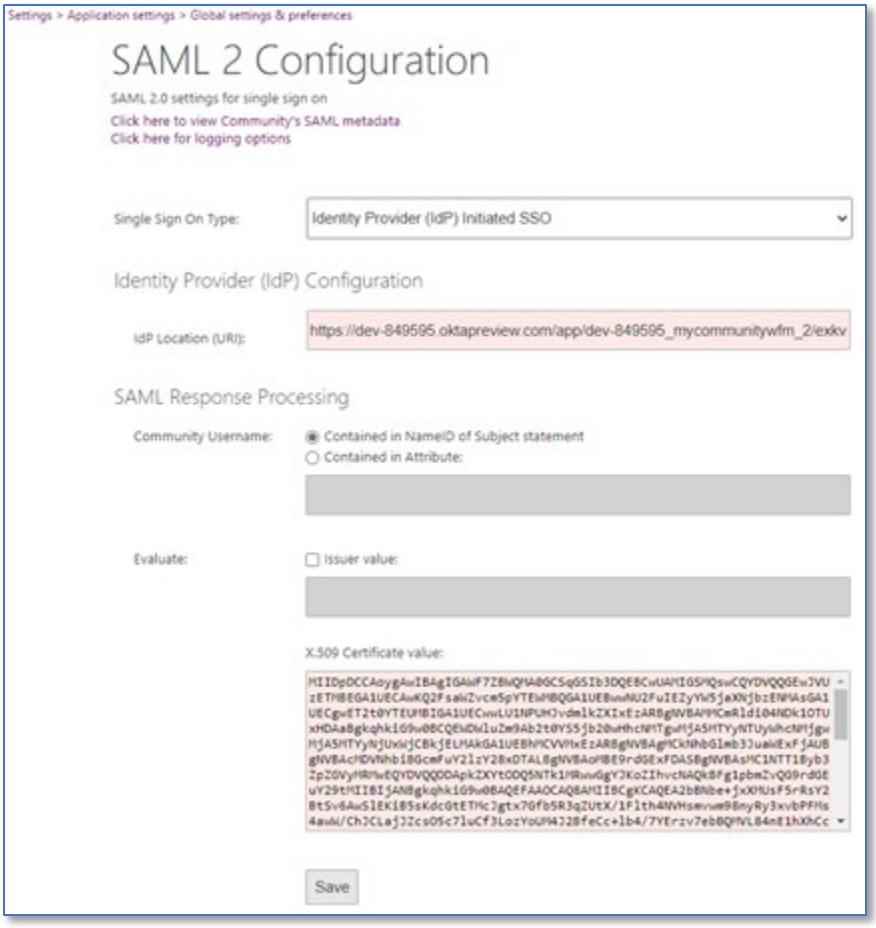
    b. Copy and paste the fields into a text document and provide to CommunityWFM project manager. Following is an example of View Setup Instructions.


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/exkvu3capaLGQ4lYj0h7/sso/saml
2 Identity Provider Issuer:
http://www.okta.com/exkvu3capaLGQ4lYj0h7
3 X.509 Certificate:
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAWF7ZBWQMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCmRldi04NDk1OTUxHDAaBgkqhkiG9w0BCQEW
DWluZm9Ab2t0YS5jb20wHhcNMTgwMjA5MTYyNTUyWhcNMjgwMjA5MTYyNjUxWjCBkjELMAkGA1UE
BhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALBgNV
BAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXYtODQ5NTk1MRwwGgYJ
KoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
2bBNbe+jxXMUsF5rRsY2BtSv6AwSlEKiB5sKdcGtETMcJgtx7Gfb5R3qZUtX/1Flth4NVHsmvwm9
8nyRy3xvbPFMs4aWW/ChJCLajJZcsO5c7luCf3LozYoUM4J2BfeCc+lb4/7YErzv7ebBQMVL84nE
1hXhCceSyZcjzbm9fNi9ZMccoh+18kNlHhZdWD1ETFsb8lkmrhPkPg69TgeP+c6O9rUBIRzh3VNS
CMtT5MRl4c+p1Gwi01jVVzAdwQDMuqiCq+N5eKlzJxAoe58Yk0p25CkEyi7hhoU8Ohssvzj3scgL
iXZkQ3Ds86zRoJPbWE++/BtufiulKZ8JJLa7WQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBHQ3WQ
i47ssS0VyjHNcCukeRrCxtmmmGRbnM9sOL4+Herg7T//YaCMgZUsyxe3tgviSFNGWAfH7VlmiJTP
gUF2zF1daWtnzmzgqHNqR7ly6pWXOMLPg43qo4Ppp6r8GzxIU23orYxmTsZuBGToYsYs1tc9j+bW
xRdDOl52idbD5f5ZCvio/hnbe4lfROtFDXpiTlmUKrLYS9Hp+IU2mdin3ijyChd5PwY2ZvyisaEq
oSg+g1V+neNLUP+q5YRMUBDMNBFSEzR1GptVW7Jly9GxJFSnvbChJY1L4z4rRdr1kuJjC5Ey6+NX
tMYnrdQY0xiUcuJ8VEgcbrBiOkxu/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/exkvu3capaLGQ4lYj0h7"
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>MIIDpDCCAoygAwIBAgIGAWF7ZBWQMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCmRldi04NDk1OTUxHDAaBgkqhkiG9w0BCQEW
DWluZm9Ab2t0YS5jb20wHhcNMTgwMjA5MTYyNTUyWhcNMjgwMjA5MTYyNjUxWjCBkjELMAkGA1UE
BhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALBgNV
BAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXYtODQ5NTk1MRwwGgYJ
KoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
2bBNbe+jxXMUsF5rRsY2BtSv6AwSlEKiB5sKdcGtETMcJgtx7Gfb5R3qZUtX/1Flth4NVHsmvwm9
8nyRy3xvbPFMs4aWW/ChJCLajJZcsO5c7luCf3LozYoUM4J2BfeCc+lb4/7YErzv7ebBQMVL84nE
1hXhCceSyZcjzbm9fNi9ZMccoh+18kNlHhZdWD1ETFsb8lkmrhPkPg69TgeP+c6O9rUBIRzh3VNS
CMtT5MRl4c+p1Gwi01jVVzAdwQDMuqiCq+N5eKlzJxAoe58Yk0p25CkEyi7hhoU8Ohssvzj3scgL
iXZkQ3Ds86zRoJPbWE++/BtufiulKZ8JJLa7WQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBHQ3WQ
i47ssS0VyjHNcCukeRrCxtmmmGRbnM9sOL4+Herg7T//YaCMgZUsyxe3tgviSFNGWAfH7VlmiJTP
gUF2zF1daWtnzmzgqHNqR7ly6pWXOMLPg43qo4Ppp6r8GzxIU23orYxmTsZuBGToYsYs1tc9j+bW
xRdDOl52idbD5f5ZCvio/hnbe4lfROtFDXpiTlmUKrLYS9Hp+IU2mdin3ijyChd5PwY2ZvyisaEq
oSg+g1V+neNLUP+q5YRMUBDMNBFSEzR1GptVW7Jly9GxJFSnvbChJY1L4z4rRdr1kuJjC5Ey6+NX

10. CommunityWFM Server Configuration
    a. Community professional services engineer will paste the configurations provided under **Configure SAML Authentication** page under Settings > Application settings > Global settings & preferences
    b. There are two SSO types available under Single Sign On Type:
        i. Service Provider (SP) Initiated SSO:

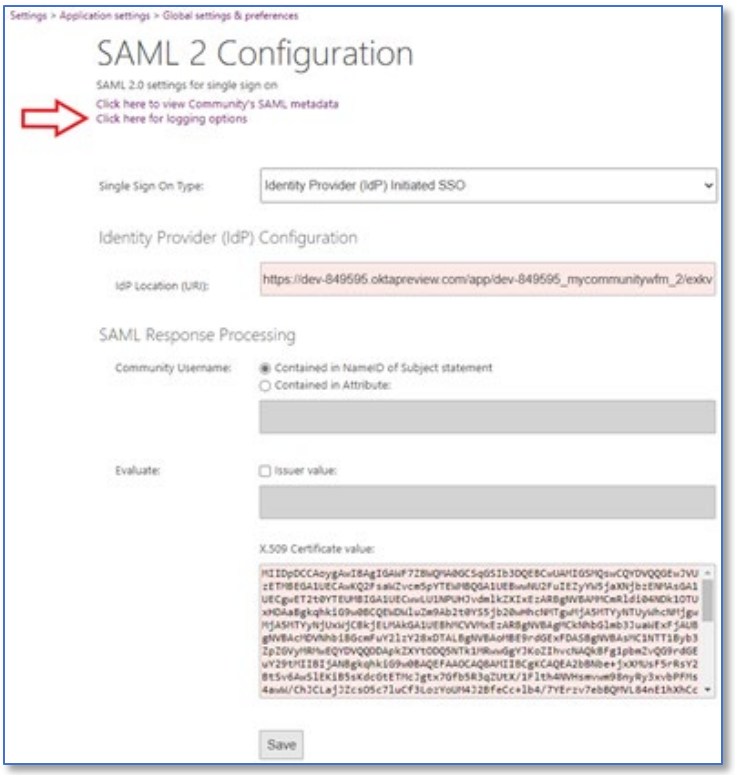


ii. Identity Provider (IdP) Initiated SSO:

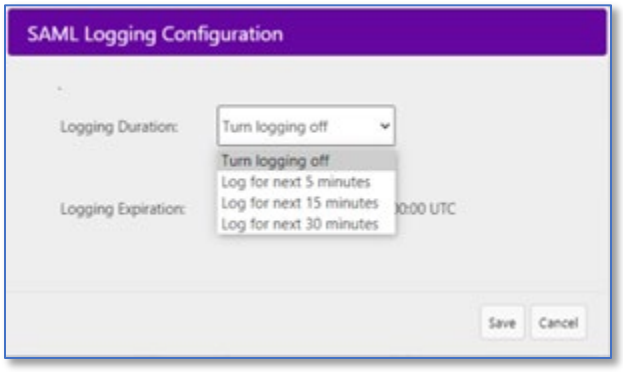


Community's SAML Logging Configuration

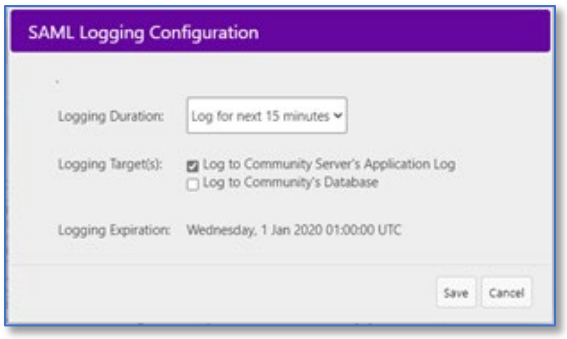
Community Version 4.4 Cumulative Service Release 2 (4.4SP2) provides users the ability to enabled enhanced logging to troubleshoot SAML failures under the **Click here for logging options** link under the **Configure SAML Authentication** page under Settings > Application settings > Global settings &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



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:



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'

CommunityWFM

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:

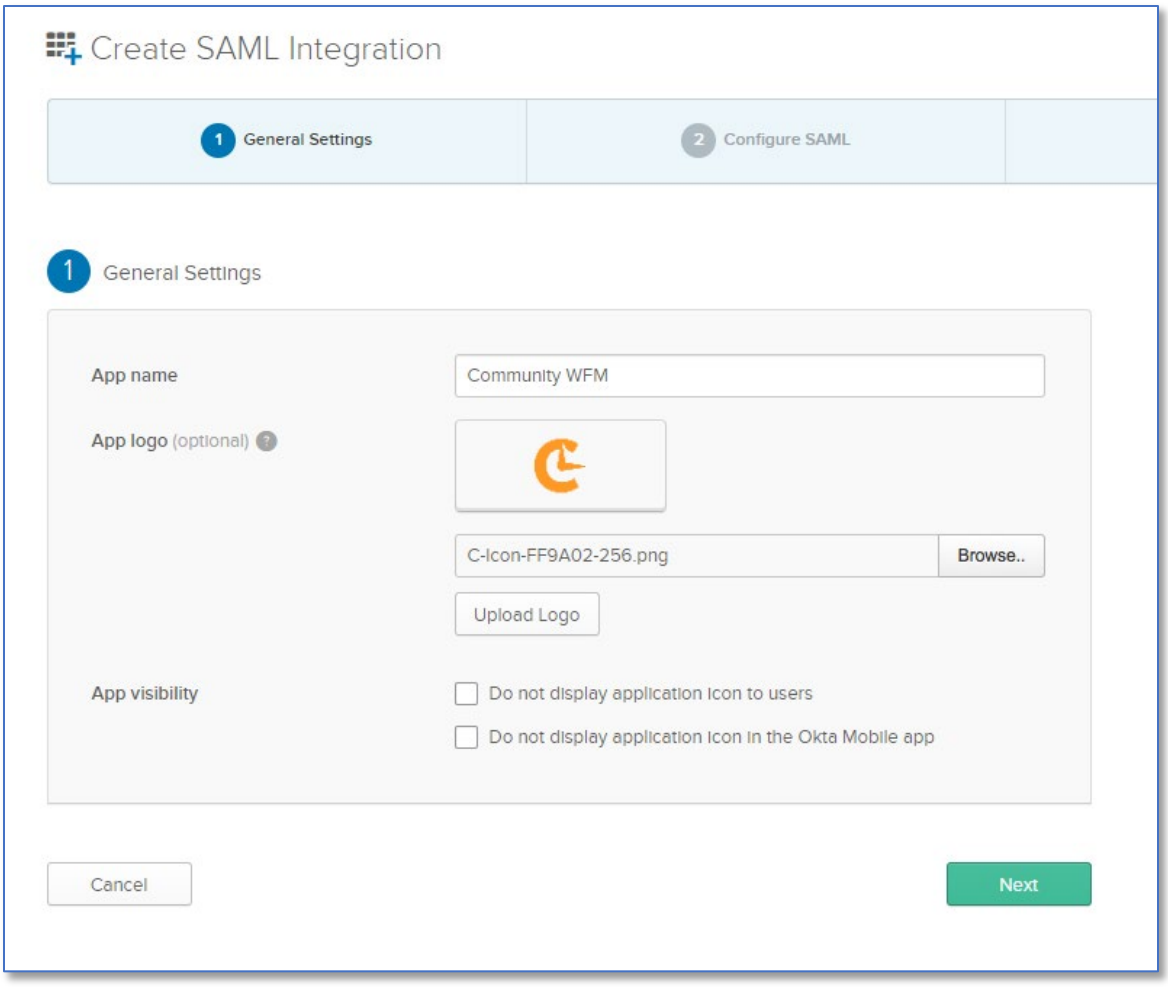
- At the IdP, temporarily change the Community application's consumer endpoint to: https://*companysite*/CommunityWeb/UI/SAML/test.aspx
- Perform a user login
- Community will display a debugging page

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.



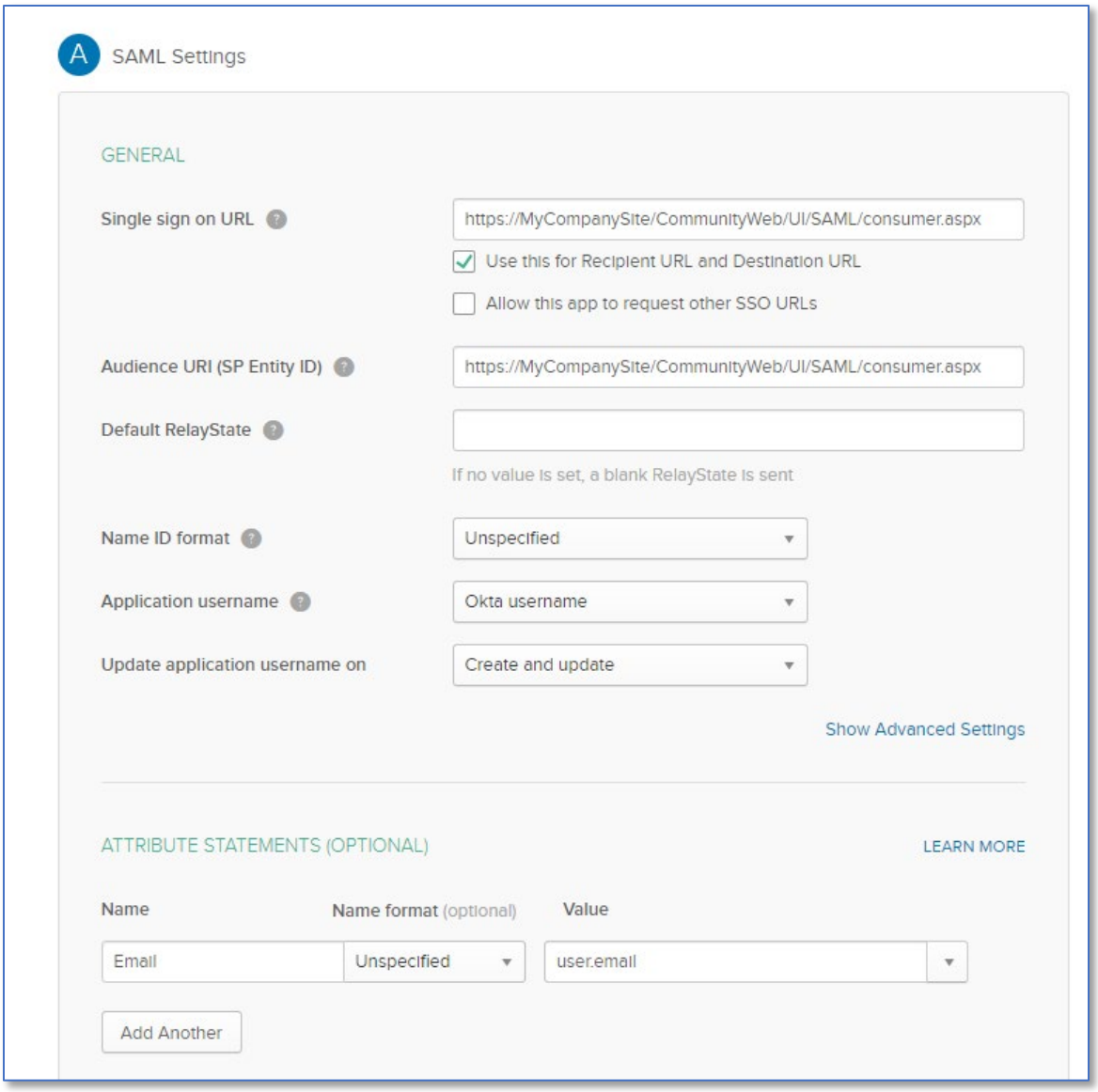
When asked for the Single Sign On URL use:

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.

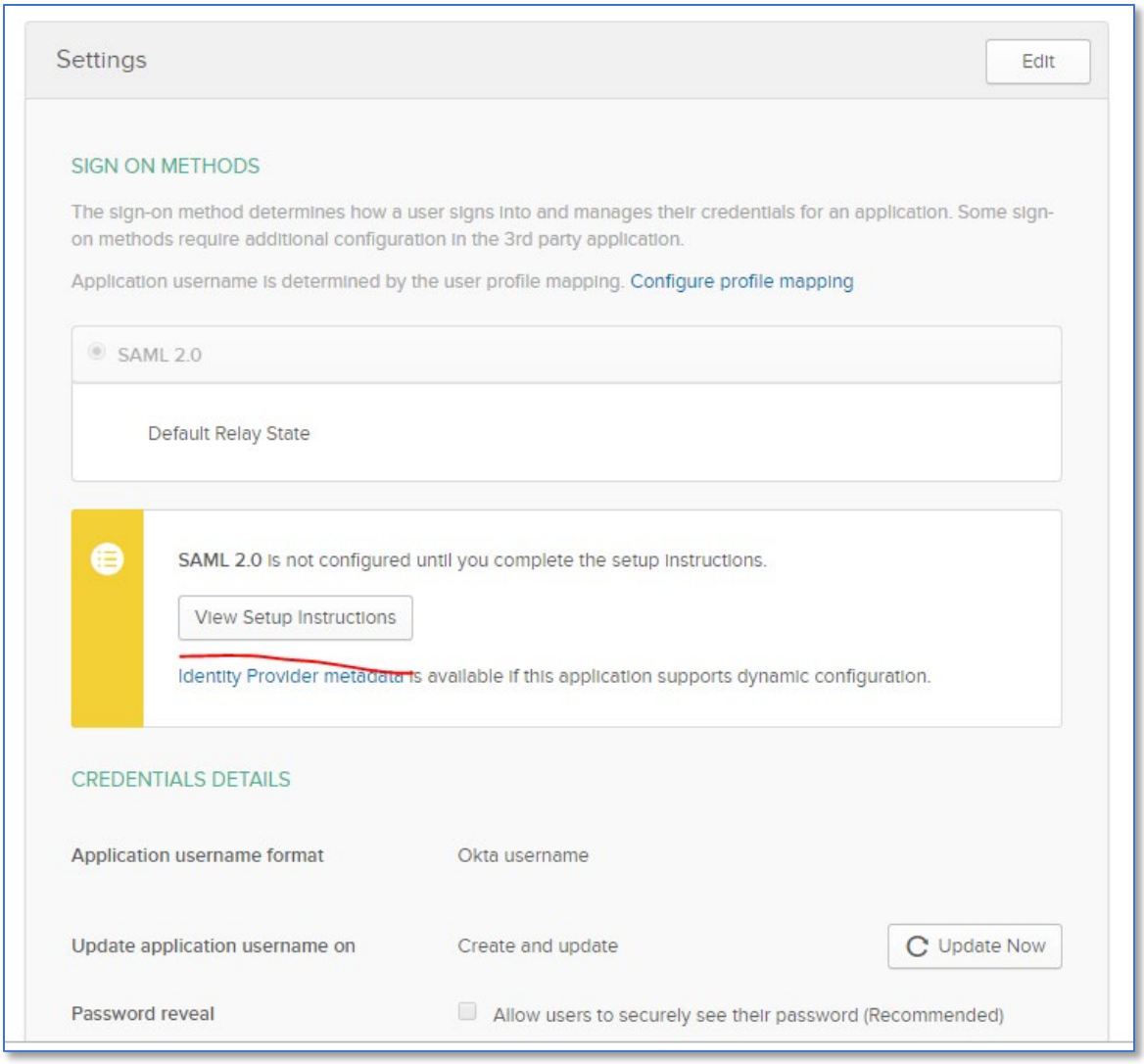
Add an attribute under "Attribute Statements" with name of **Email**, format can remain '**unspecified**" and the value should be **user.email**



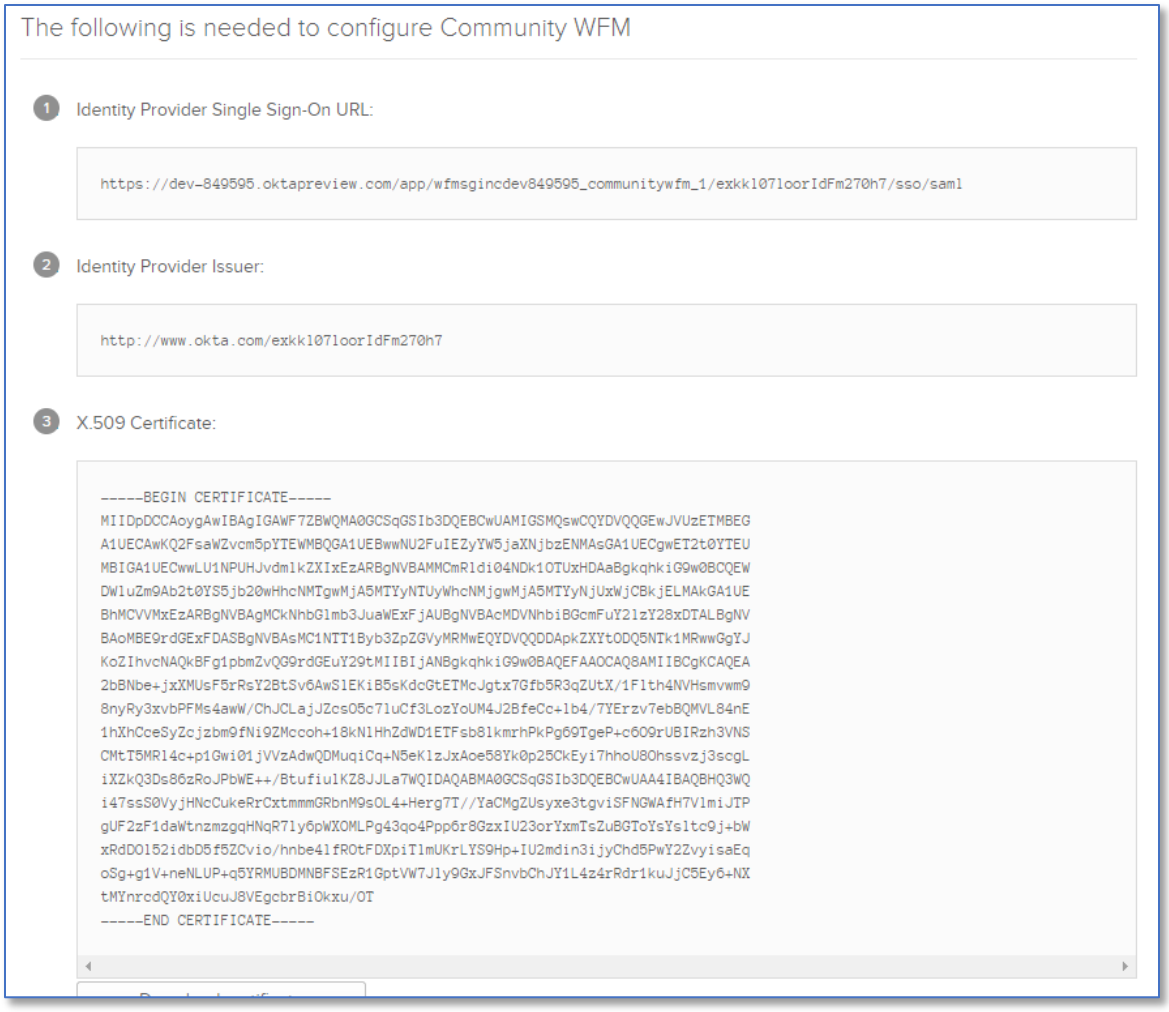
The remainder of the configuration can remain at their defaults.

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

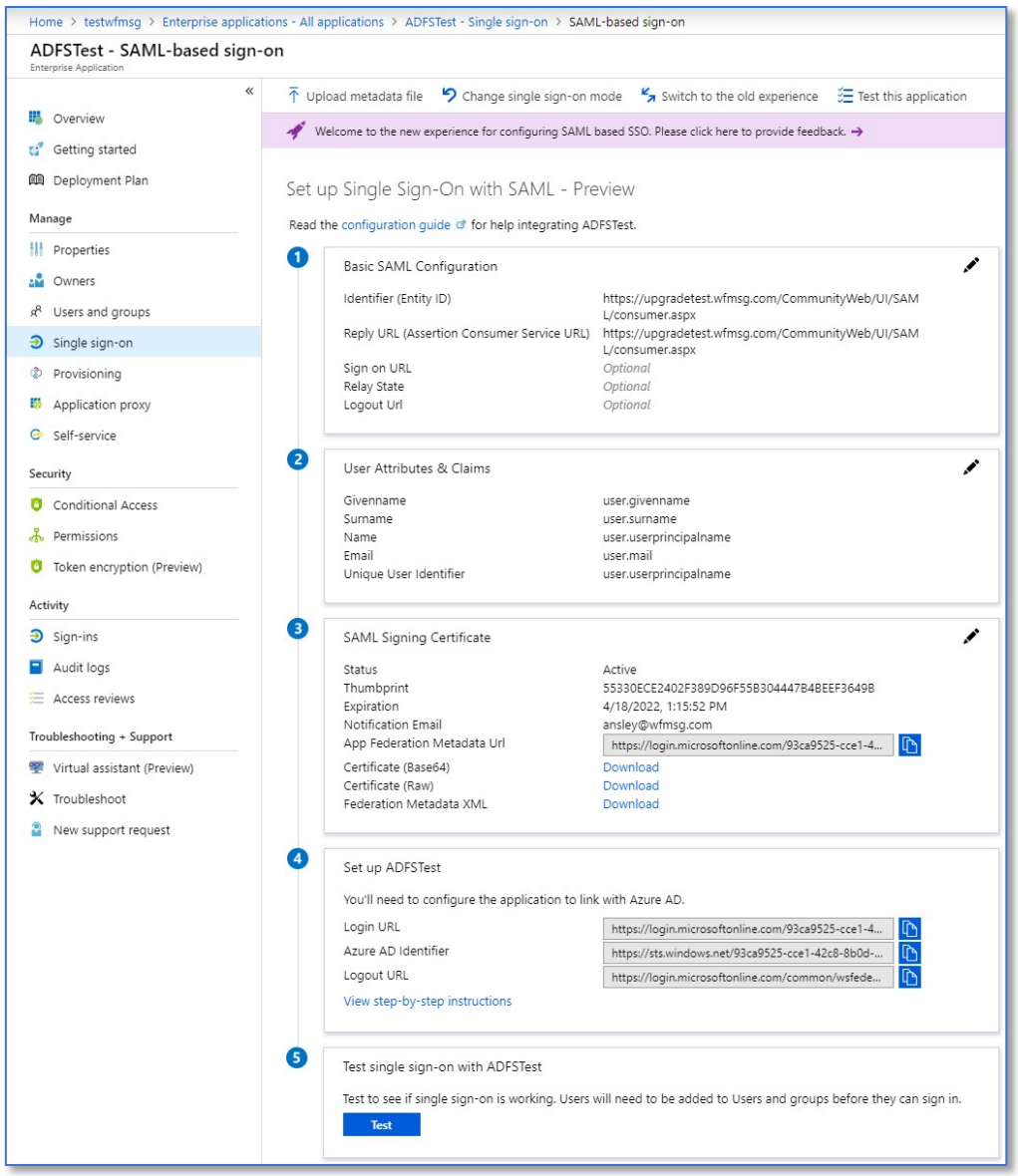


Please copy and paste each of these in their entirety into a text document and provide to WFMSG Project Manager.

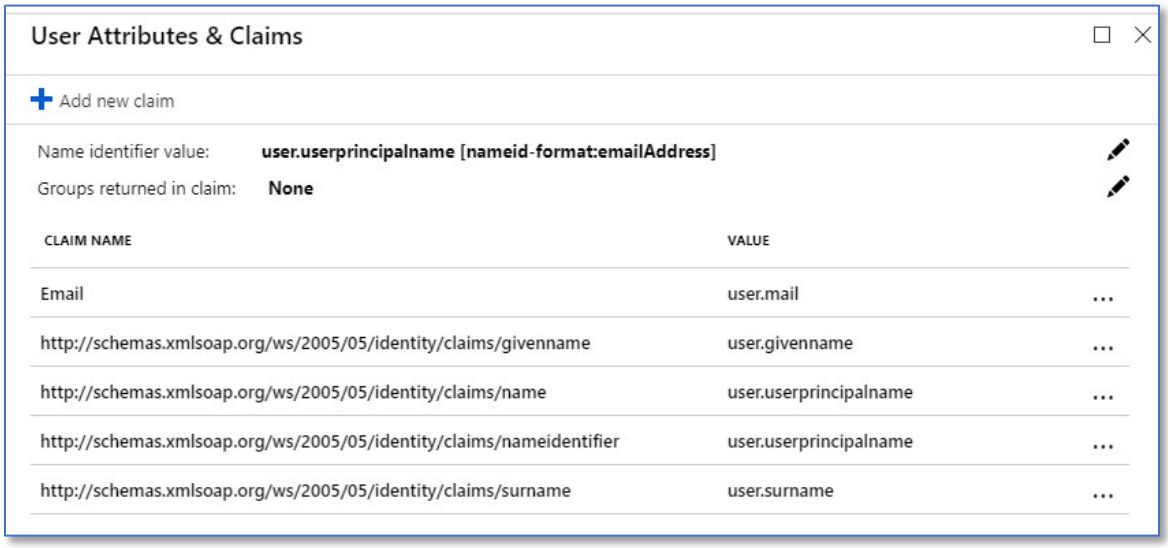
Azure Cloud ADFS

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

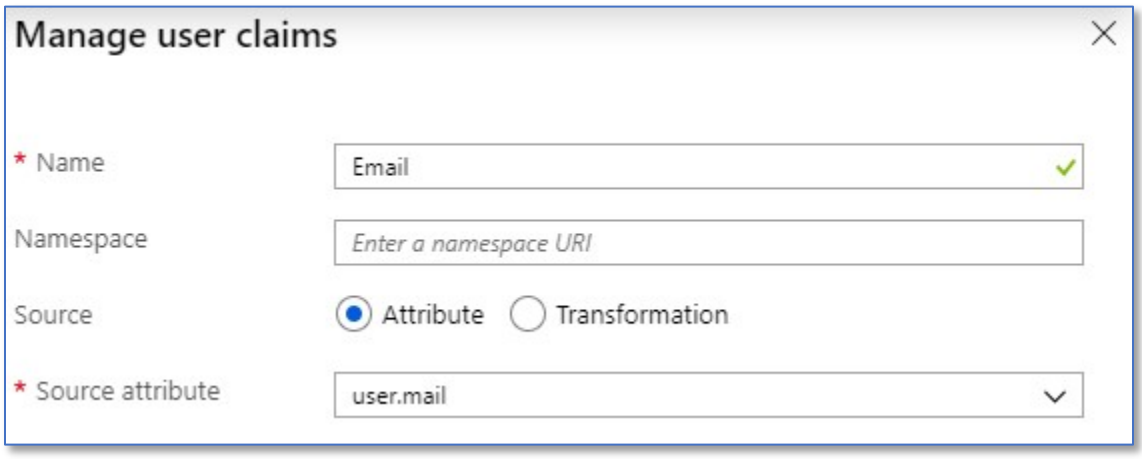
   https://**ReplaceWithYourCompanySite** /CommunityWeb/UI/SAML/test.aspx to test and then replace with the application url once testing is complete
   https://**ReplaceWithYourCompanySite**/CommunityWeb/UI/SAML/consumer.aspx



2. 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".



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



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