Microsoft AD FS SAML Single Sign-On Integration to EVERFI Foundry

This documentation reflects Microsoft Active Directory Federation Services (AD FS) as of September 2019. We strive to keep these guidelines up to date and relevant, but be aware that software changes continually and therefore these steps may change over time. If you see a discrepancy, please let us know.

Summary

This document demonstrates how to set up SAML single sign-on for EVERFI as a service provider and your organization's Microsoft AD FS as an identity provider. After you complete this setup successfully, your organization's users will be able to access EVERFI content and have EVERFI securely and seamlessly authenticate their identity through your organization's identity provider.

Microsoft has other identity access management tools which may operate differently. See also separate documentation for more general EVERFI single sign-on instructions; this documentation addresses specific details with AD FS.

There are three main steps you will do:

1. In EVERFI Foundry, get the EVERFI X509 public certificate as well as other SAML properties that will be needed to create a Relying Party Trust for EVERFI in AD FS.

2. In your organization's AD FS, create a Relying Party Trust with Claims for EVERFI.

3. In EVERFI Foundry, add an identity provider configuration by uploading your organization's SAML metadata file, and, if necessary, mapping your claims to corresponding EVERFI attributes (first name, last name, and email address).

Step 1: Gather EVERFI Certificate and Metadata

In this section, you will get a certificate file for the Foundry EVERFI X.509 certificate and get other EVERFI SAML properties. AD FS will need to upload this certificate file to configure a Relying Party Trust for EVERFI.

You also must get three additional SAML properties from Foundry. We recommend you copy and then paste them into a text file (like Notepad) for use later on.

1. Login to Foundry as an admin user, navigate to **Settings** → **Single Sign-On**

2. Click the **View** link next to EVERFI SAML Metadata.

3. From the EVERFI Metadata page, click **Download encryption certificate** to save a certificate file to your local environment.

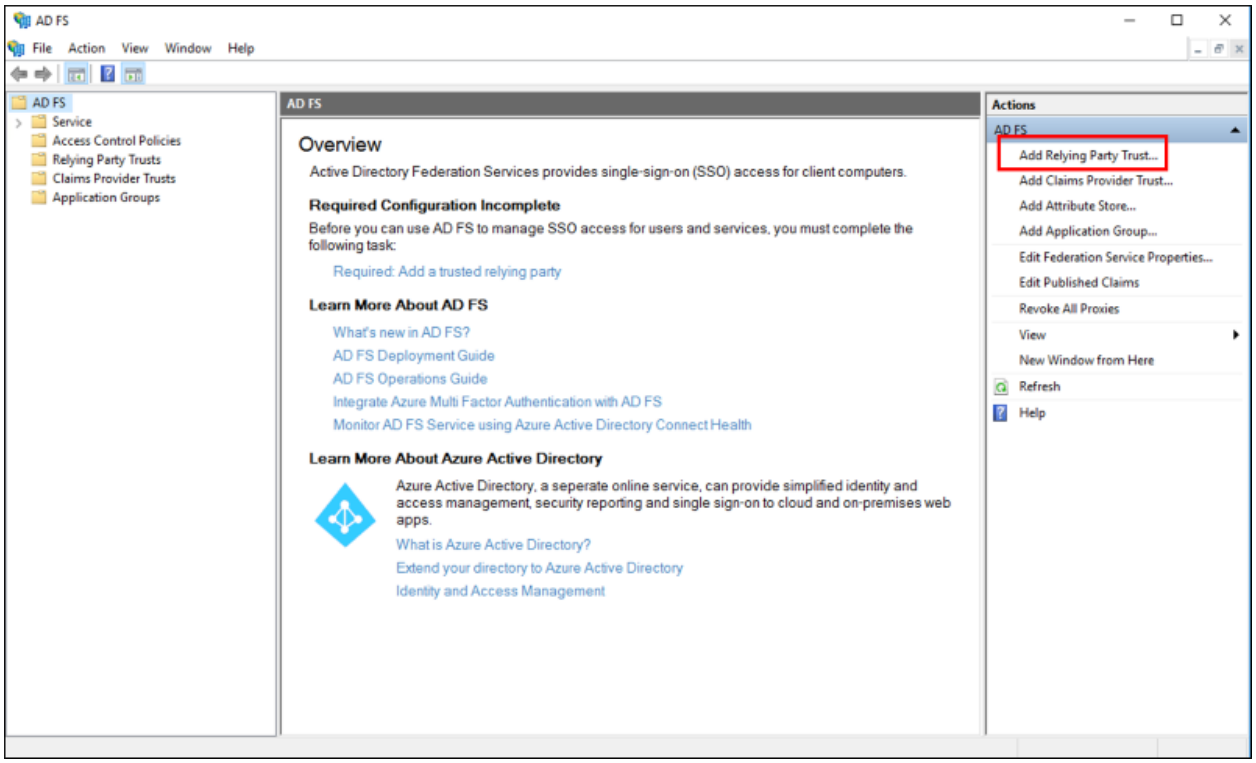
4. Copy then paste into a text file the properties for Entity ID, ACS URL and SLO URL for later use.

Step 2: AD FS - Add Relying Party Trust

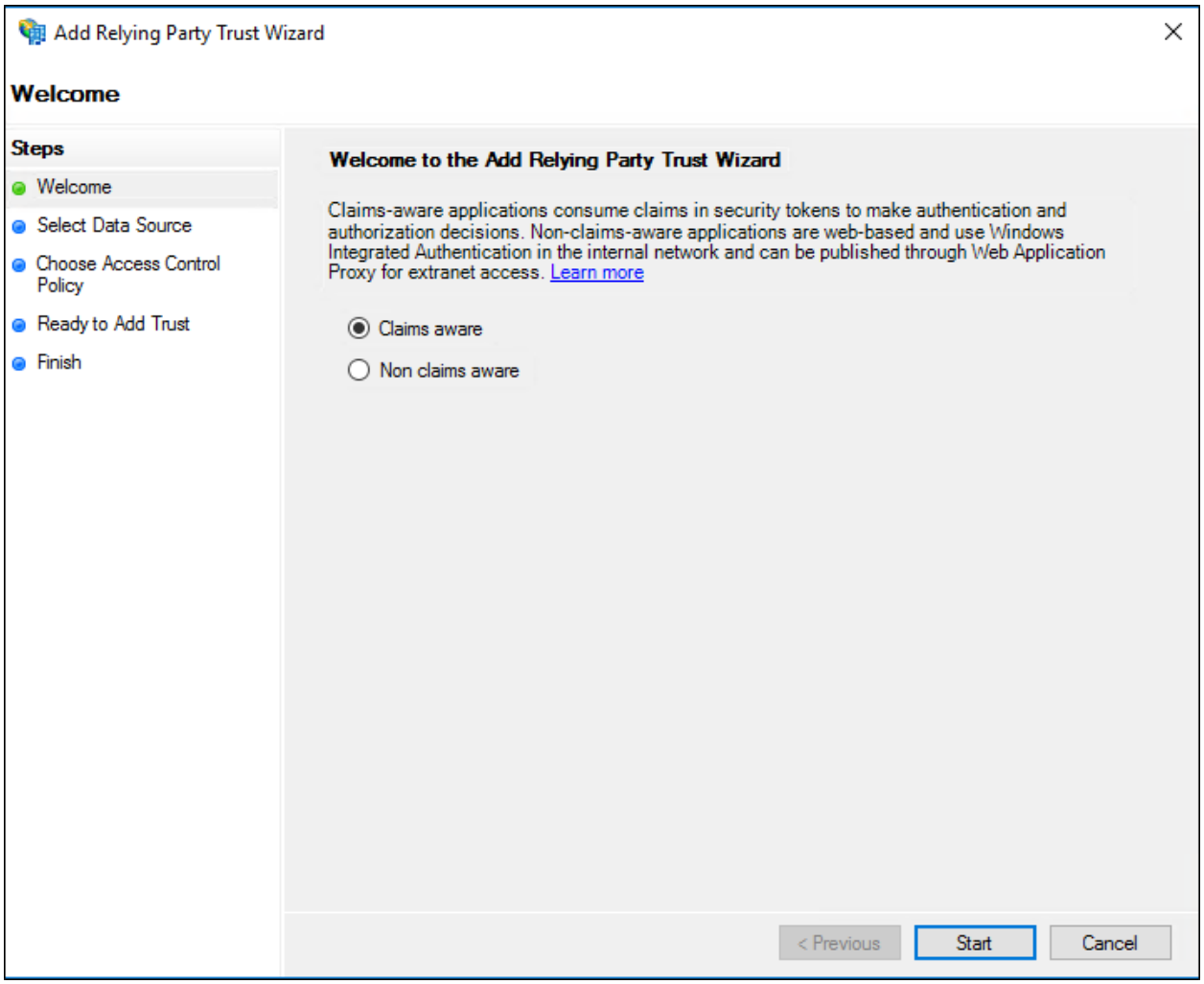
Note: the documentation in this section is adapted from Microsoft's documentation: [Create a Relying Party Trust] for Windows Server 2016. Be aware there may be subtle differences depending on the Windows and AD FS versions you are running.

5. In Server Manager, click **Tools**, and then select **AD FS Management**.

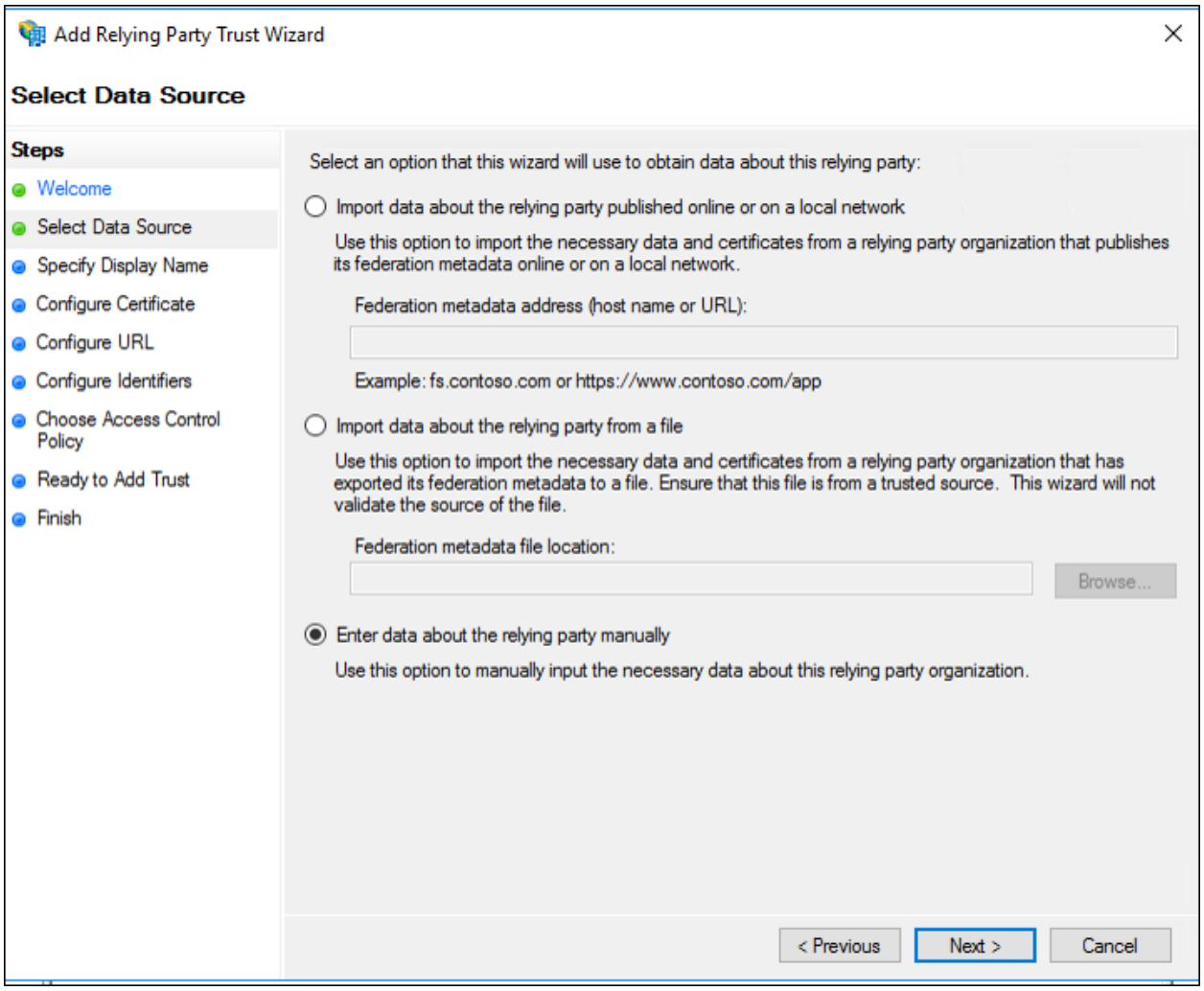
6. Under **Actions**, click **Add Relying Party Trust**.



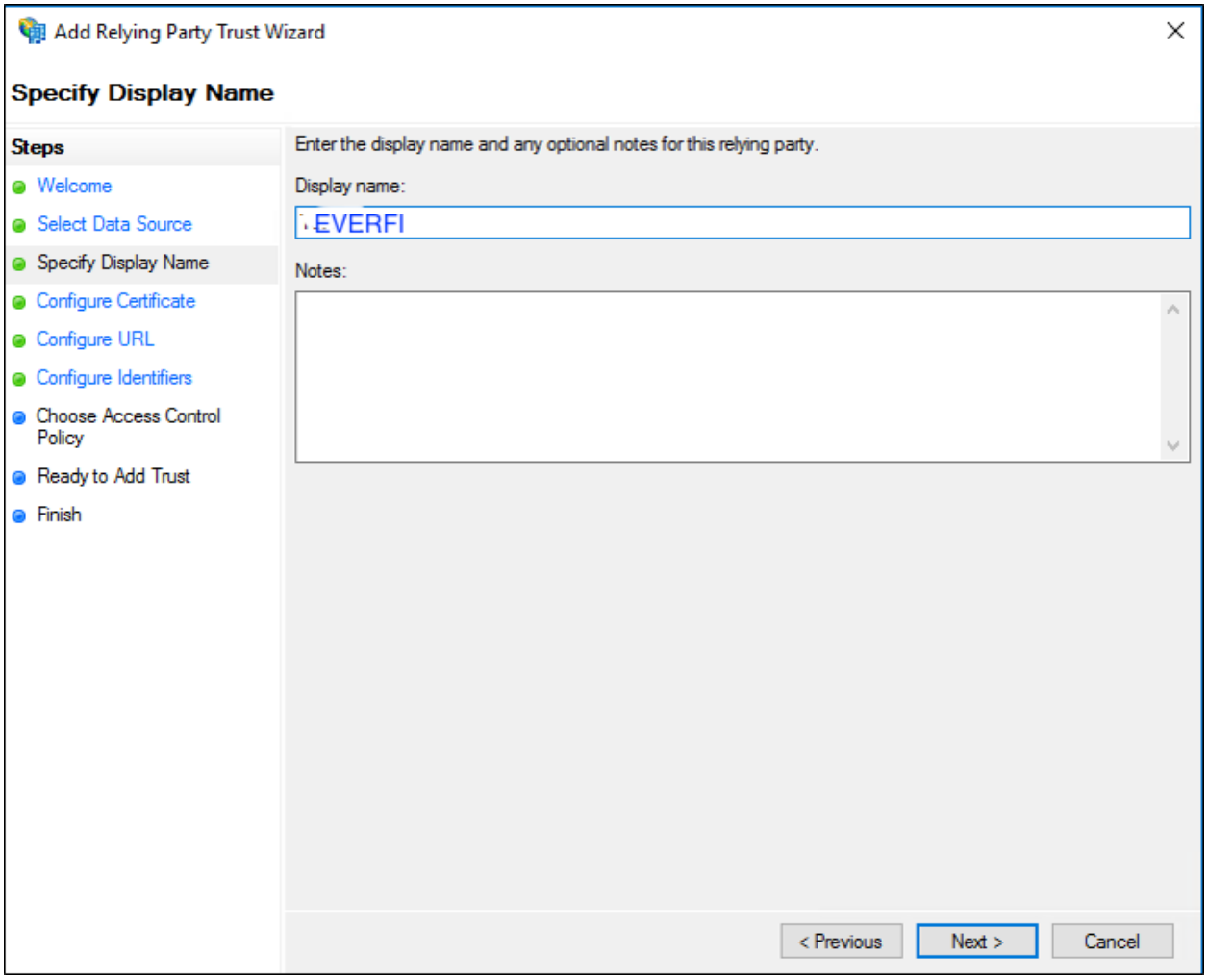
7. On the **Welcome** page, choose **Claims aware** and click **Start**.



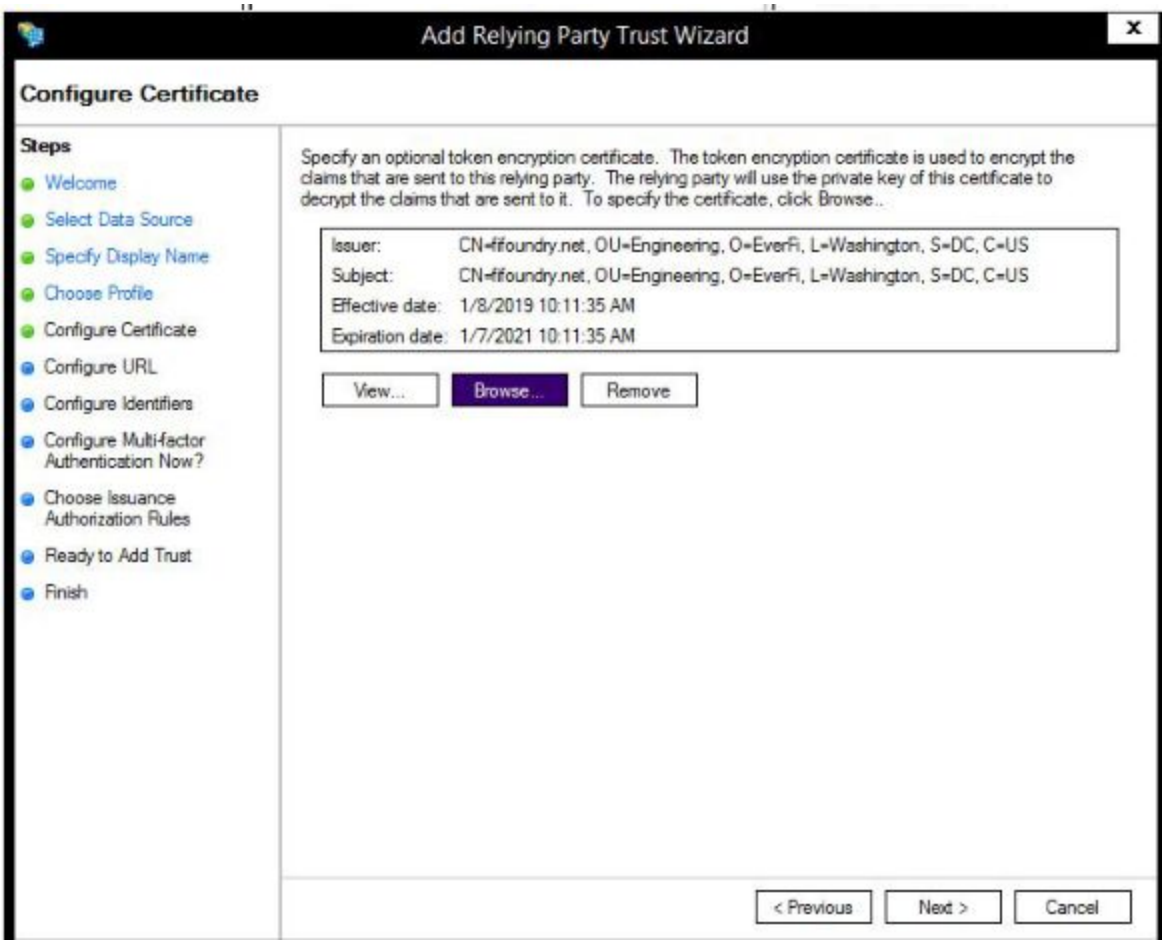
8. On the **Select Data Source** page, click **Enter data about the relying party manually**, and then click **Next**.



9. On the **Specify Display Name** page, type “EVERFI” or a variation in Display name, under Notes type a description, and then click Next. What you enter here is purely descriptive, so there is no “wrong answer.” We recommend you not use spaces or unusual characters.

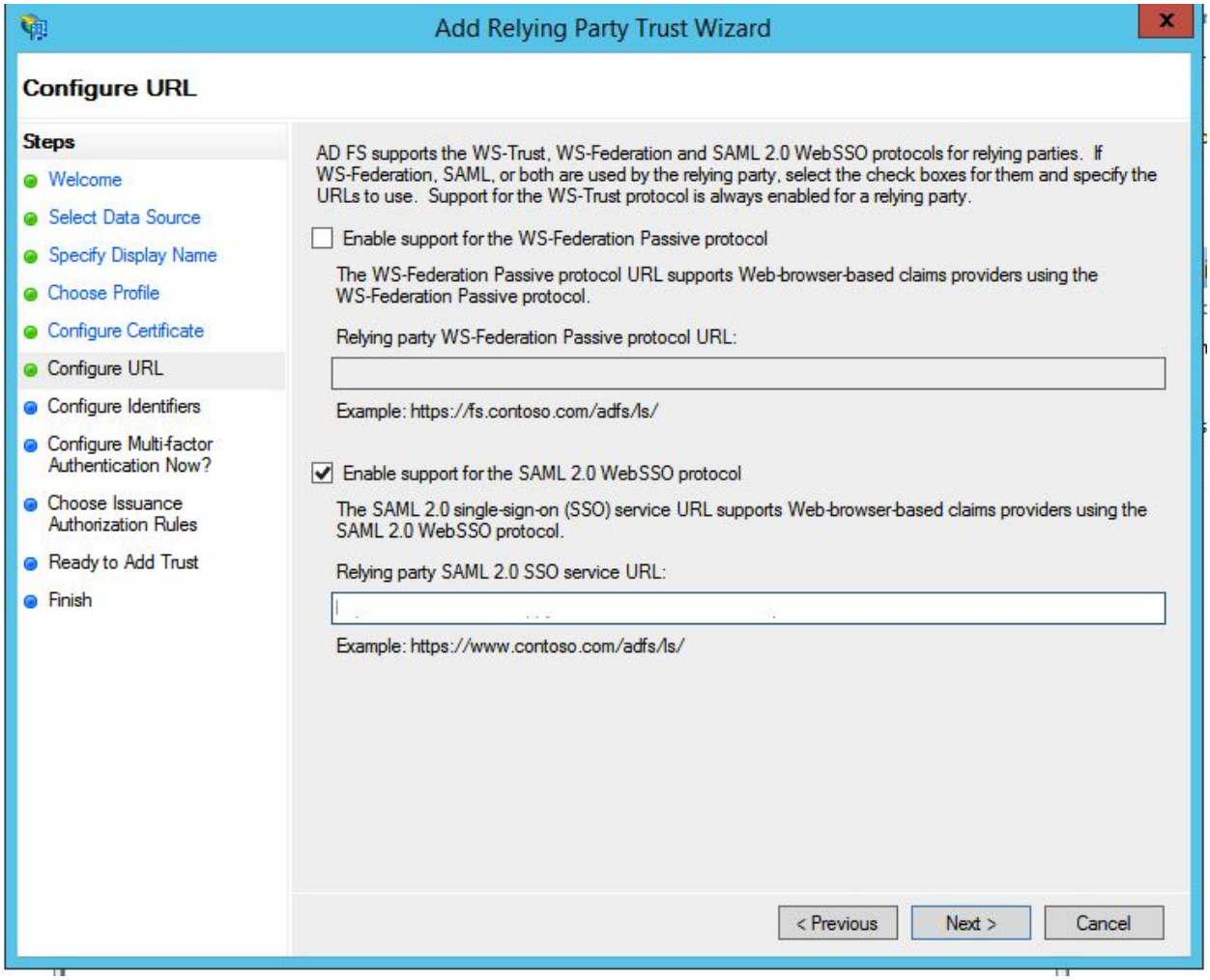


10. On the **Configure Certificate** page, browse for and upload the EVERFI certificate file you downloaded earlier and click **Next.** After uploading the certificate, you should see the Issuer, Subject and dates.



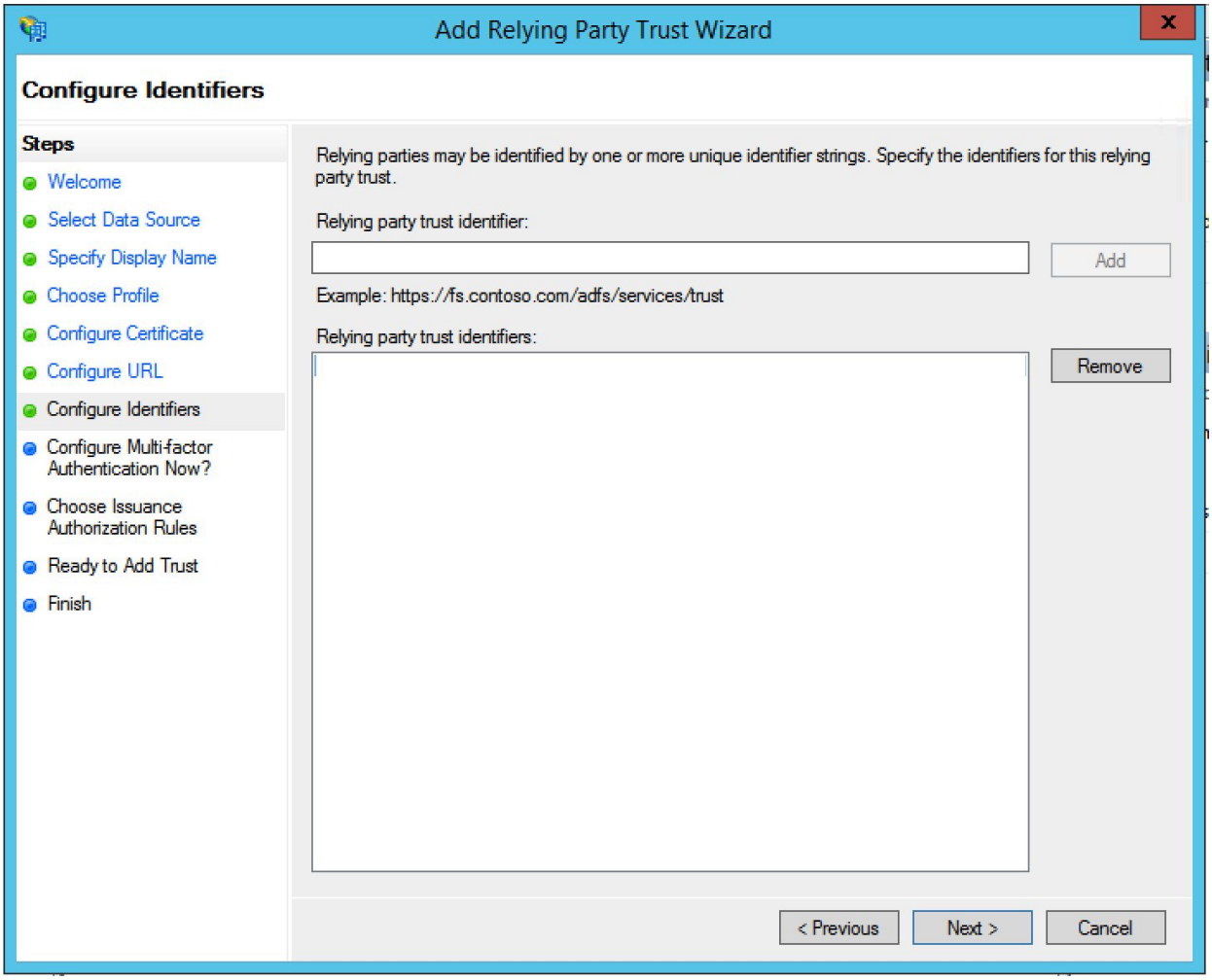
11. On the **Configure URL** page:

- Do not select the Enable support for the WS-Federation Passive protocol check box.
- Select the **Enable support for the SAML 2.0 WebSSO protocol** check box. Under **Relying party SAML 2.0 SSO service URL**, enter the EVERFI ACS URL you got earlier for the Security Assertion Markup Language (SAML) service endpoint URL for this relying party trust, and then click **Next**.



Enter your specific ACS URL into the **Relying party SAML 2.0 SSO service URL** *above*

12. On the **Configure Identifiers** page, enter your EVERFI SAML entityID you got earlier into **Relying party trust identifier** and click **Add**, and then click **Next**.

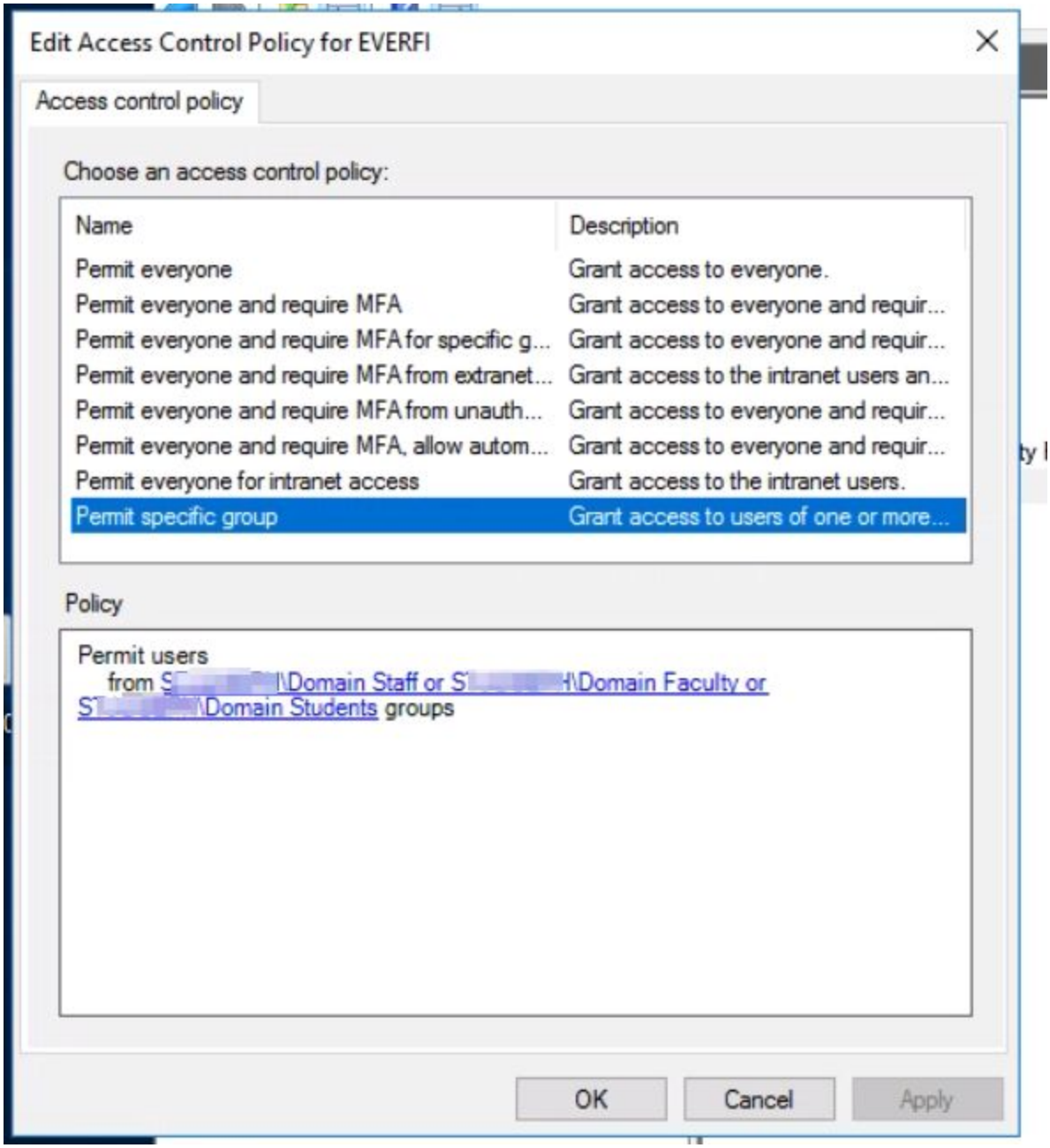


*Enter your organization's specific EVERFI entityID into **Relying party trust identifier** above*

EVERFI

13. Access Control Policy

On this page, choose the security groups who will be able to access Foundry through this relying trust:



If you are not creating new users in Foundry, which means your users will be matched against existing Foundry users, then be aware that even if you “over assign” permissions, a user who is not in Foundry will not be able to log in to Foundy because they won’t match to an existing user.

14. Finish

For the rest of the pages in the wizard, configure according to your own organization's protocols.

When you are completed, then you have added a Relying Party Trust for EVERFI as a service provider.

Step 3: Adding Claims in AD FS

Refer to AD FS documentation on how to add claims to an existing relying party trust. For example, to send LDAP attributes as claims, see: Create a Rule to Send LDAP Attributes as Claims.

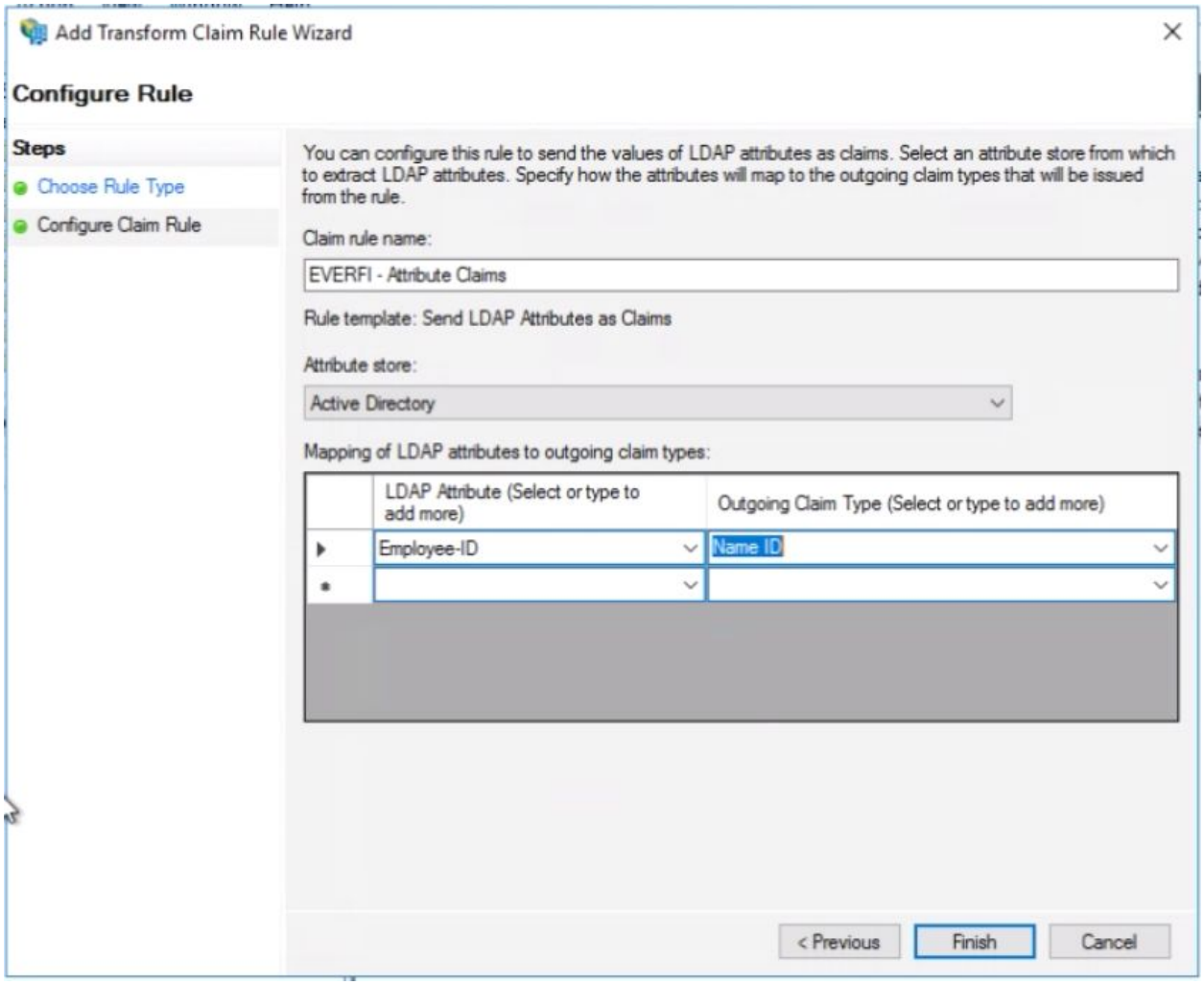
These claims and their values will be included in the SAML assertion your identity provider sends to EVERFI during single sign-on. EVERFI will use this information to identify the authenticated user, and create a new user if applicable.

Name ID Claim

15. Add Name ID Claim

After adding EVERFI as a relying party trust, in AD FS, add **claims** to the EVERFI relying party trust for whichever property in your AD is the unique name; this must match up in Foundry with the value stored in the User SSO ID field. Ensure the **Outgoing Claim Type** is set to **Name ID**.

For example, if Employee-ID is to be used as the unique name, then the mapping would be like this:



Option to Create New Users in EVERFI

If your Foundry users will be added/uploaded separately from SSO, then skip this section. If you wish for new users to get automatically created during SSO, then continue following the instructions in this section. Generally, partners who are in higher education or code and conduct can skip this section because your organization will upload your users into Foundry and not create them during SSO.

If you wish to have SSO create new users in Foundry, then you **must** also provide claims for:

- first name
- last name

- email address. If you already provided email as a Name ID, you will need to add it again as a regular attribute.

If you wish to have SSO create new users in Foundry, then you *may* also provide claims for:

- Location
- User Type
- Role

If you do not provide any of the 3 optional claims listed above, then Foundry will provide defaults instead.

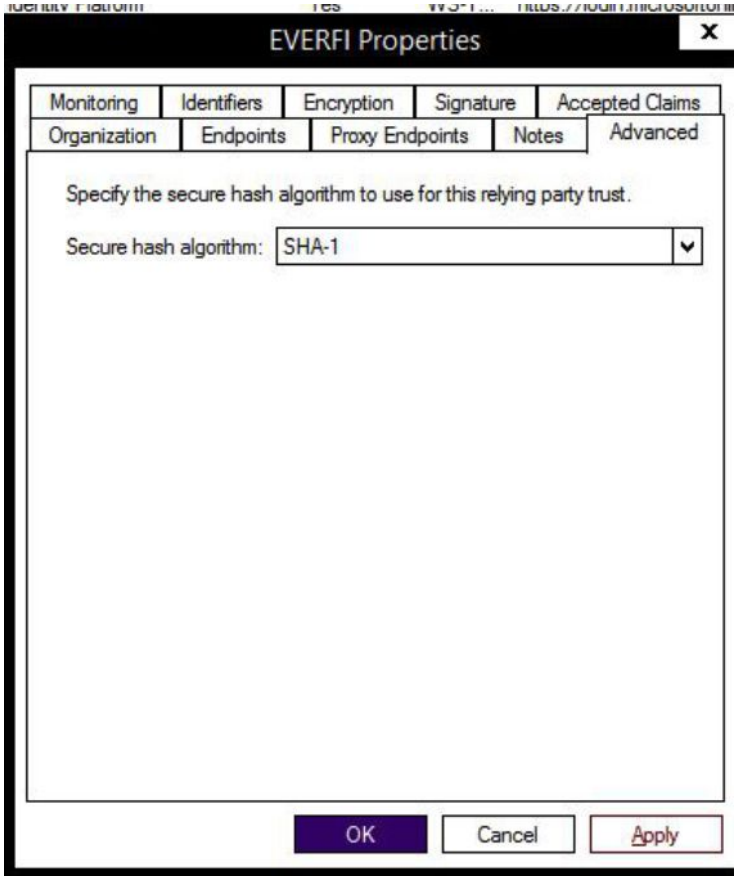
Step 4: Additional Properties

Advanced

16. Algorithm

After saving the relying party trust, edit the EVERFI trust.

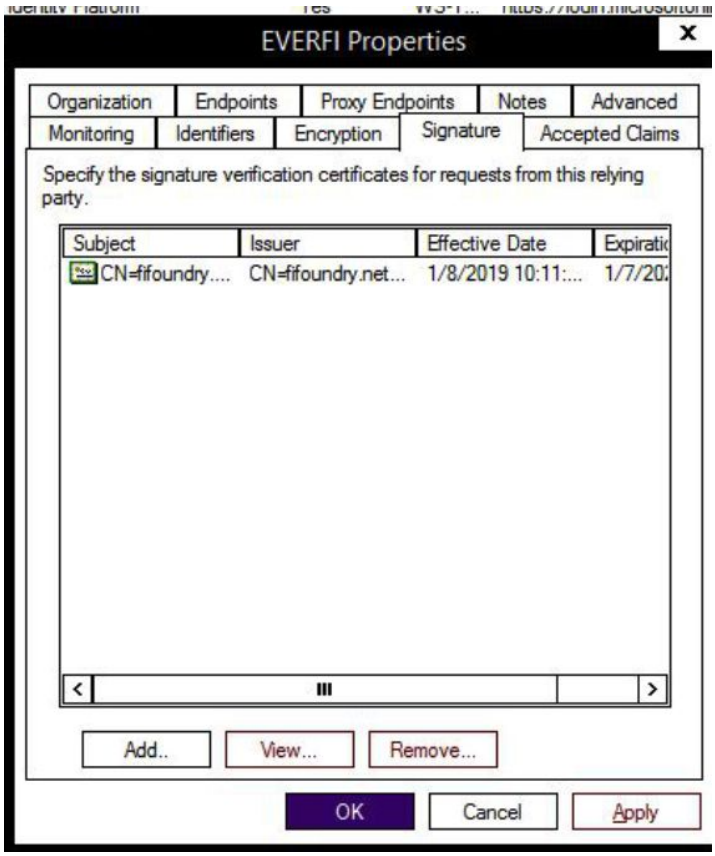
On the Advanced tab, in Secure hash algorithm, choose SHA-1



Signature

17. Upload Certificate to Signature

On the Signature tab, click **Add** to add a signature verification certificate. When prompted to choose a certificate file, select the same EVERFI certificate file used earlier.



Step 5: Foundry Identity Provider Setup

Refer to EVERFI's general SAML documentation for the setup you will need to do in Foundry to configure your identity provider settings. Below are some setup tips specific to most instances of AD FS.

With AD FS. setting up the Identity Provider in Foundry is simple.

In Foundry, you will upload your organization's own SAML Metadata file.

Option to Create Users During SSO

If your Foundry users will be added/uploaded separately from SSO, then skip this section. If you wish for new users to get automatically created during SSO, then continue following the instructions in this section. Generally, partners who are in higher education or code and conduct can skip this section because your organization will upload your users into Foundry and not create them during SSO.

Map attributes from the Microsoft claims to the corresponding EVERFI attributes if you are allowing new user creating via SSO.

By default, the Microsoft claim names map to the corresponding EVERFI attributes as follows:

Microsoft Claim	**EVERFI Attribute**
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	first_name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	last_name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email

Note that your own instance of Active Directory may differ.

Troubleshooting

User Prompted to Enter First and Last Name

If, upon SSO, a user is prompted to enter first name, last name, and email address into a modal window in Foundry, then check the Foundry field mappings in the IdP setup.

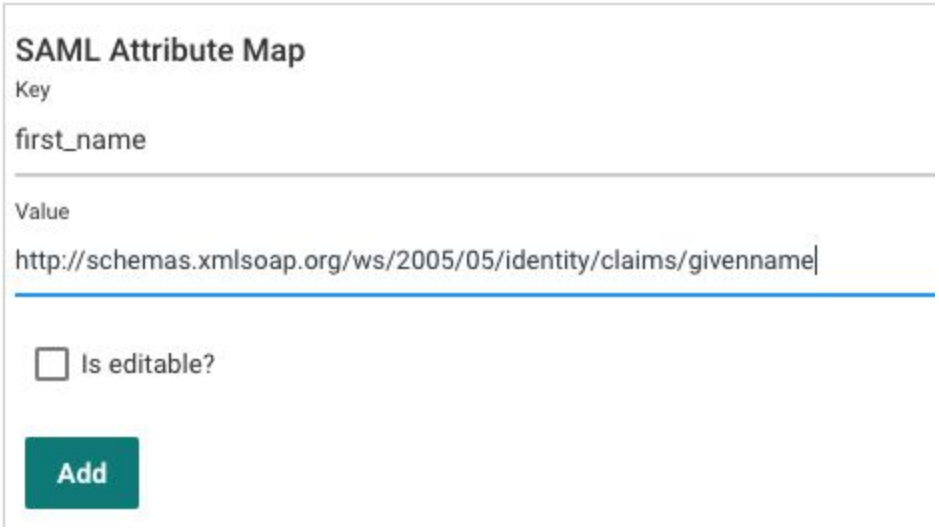
In the Foundry IdP setup, check the attribute maps. Rather than using just Givenname, for example, you might need the full claim name which might include a prepended namespace as shown below.

For example, you may see this AttributeStatement (trimmed for brevity):

```
<AttributeStatement>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
    <AttributeValue>Geoff</AttributeValue>
  </Attribute>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
```

```
    <AttributeValue>Smythe</AttributeValue>
  </Attribute>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
    <AttributeValue>geoff.smythe@somewhere.com</AttributeValue>
  </Attribute>
</AttributeStatement>
```

Note that for Givenname (i.e first name) shown above, the Attribute Name value is "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname", not "Givenname". Microsoft concatenates together the namespace and the claim name into the Attribute Name. Therefore, in Foundry, you will need to provide the full attribute name as shown:



If desired, you might wish to change the claim name that gets written in the SAML Assertion in Active Directory instead. The choice is yours. As long as Foundry can find the "Value" in the SAML assertion, the mapping will succeed.

The status code of the Response was not Success, was Responder

If you get this AD FS error, it usually means that something is amiss with the relying party trust setup. Make sure that you have uploaded the EVERFI certificate to the Signature tab in the EVERFI relying party trust. Also ensure you have set the encryption algorithm on the Advanced tab of the relying trust to SHA-1.

SSO Error: Current time is earlier than NotBefore condition

This error can happen with AD FS identity providers where there is a slight time offset between systems. To remedy this, in your AD FS Windows Server, in a command shell (not a DOS

command line) run this command where “TrustName” is the actual name of the relying party trust for EVERFI, without double quotes; for example, you might have actually named it “EVERFI”:

```
PS C:\> Set-ADFSRelyingPartyTrust -NotBeforeSkew "5" -targetname
TrustName
```

*(**PS C:\>** illustrates the prompt; you should run the command starting from “Set…”)*

See NotBefore causing troubles when server times slightly out of sync for background. The command above is for ADFS2. If running ADFS1 there is a different command.

Documentation Updates

Version	Date	Update
1.0	01/30/2019	First version of document
1.1	03/15/2019	Document additional settings in relying party trust for algorithm, and signature certificate. Document additional details about claims
1.2	03/28/2019	Expand various sections to add more details
1.3	5/9/2019	Reflect variable entityID and ACS and SLO URLs, described more at: https://foundrysupport.everfi.com/knowledgebase/saml-sso-entityid-change/
1.4	6/7/2019	Minor editing
1.5	9/9/2019	Re-write certificate and Foundry metadata section with easier way to get certificate and metadata properties

This table and the document name will be updated whenever significant changes are made to this document. This versioning is for the documentation itself, not for the actual software products.