



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

This documentation reflects Microsoft Active Directory Federation Services (AD FS) version 6.3 as of August 2020. 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.

Make sure you're reading the latest version of this documentation. Go to [Foundry SSO with ADFS](#) to get the latest version. This is version V2.

Summary

This document demonstrates how to set up SAML single sign-on and single logout for EVERFI as a service provider and your organization's Microsoft AD FS as the identity provider. After you complete this setup successfully, your organization's learners will be able to access EVERFI content and have EVERFI securely and seamlessly authenticate their identity through your organization's AD FS 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, download the Foundry SAML metadata file 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, email address, etc.).

Step 1: Download Foundry Metadata File

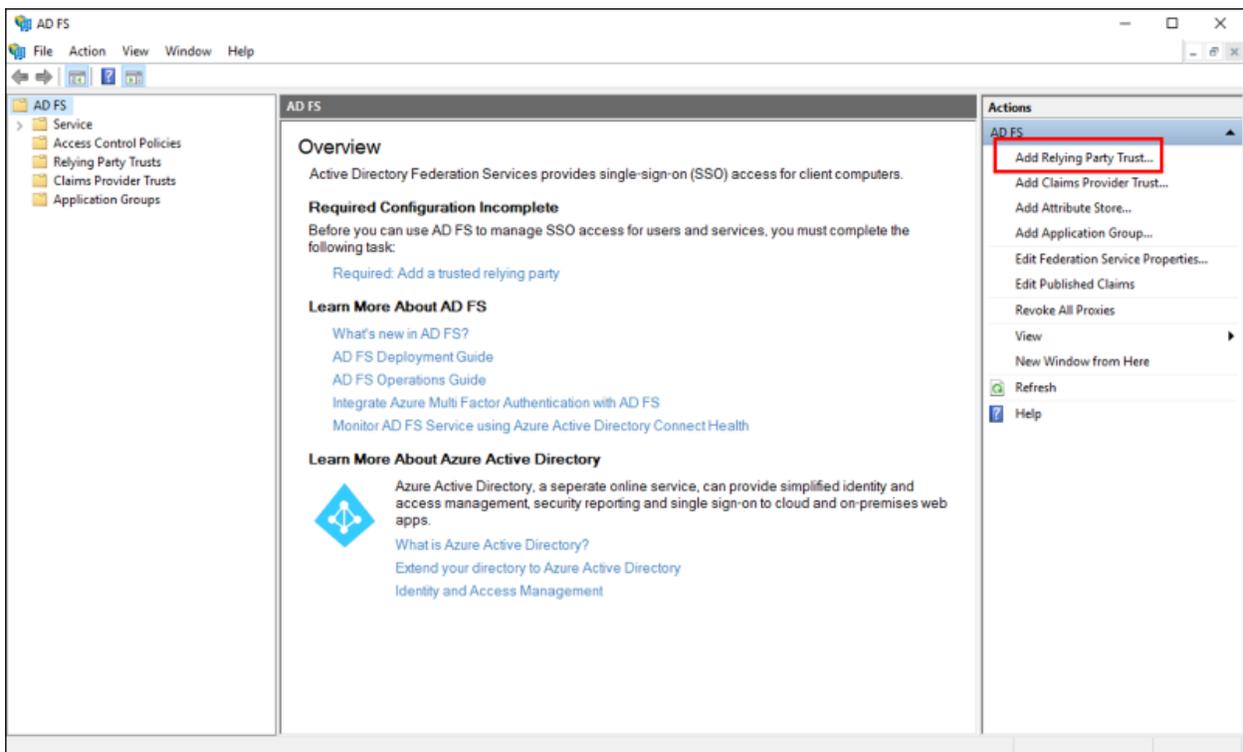
1. Login to Foundry customer admin portal as an admin user and navigate to **Settings** → **Single Sign-On**
2. Click the **View** link next to EVERFI SAML Metadata.

3. From the EVERFI Metadata page, click **Download Full Metadata** to save the file to your local environment. Place that file where it can be accessible to AD FS when you add the Relying Party Trust.

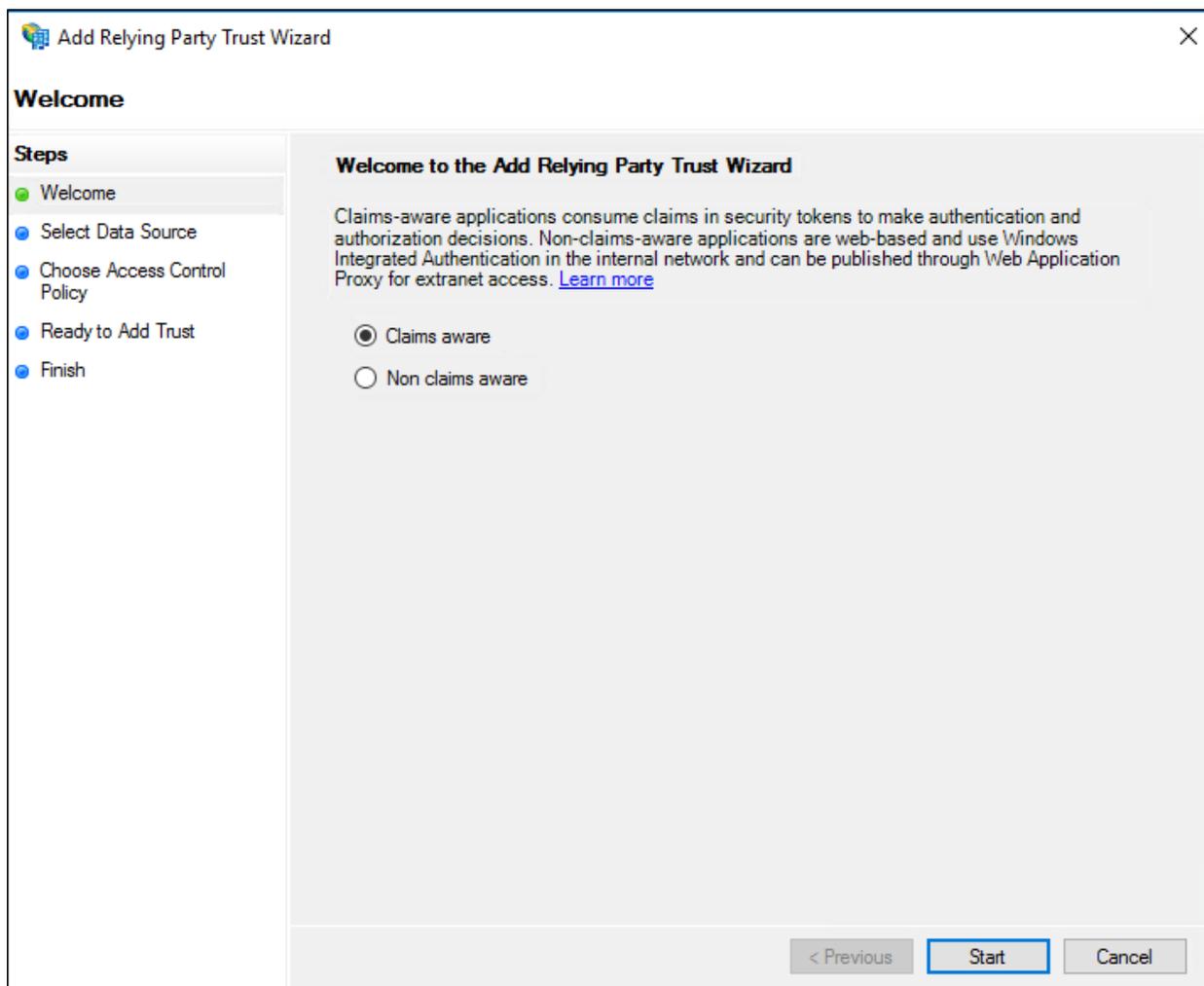
Step 2: AD FS - Add Relying Party Trust

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.

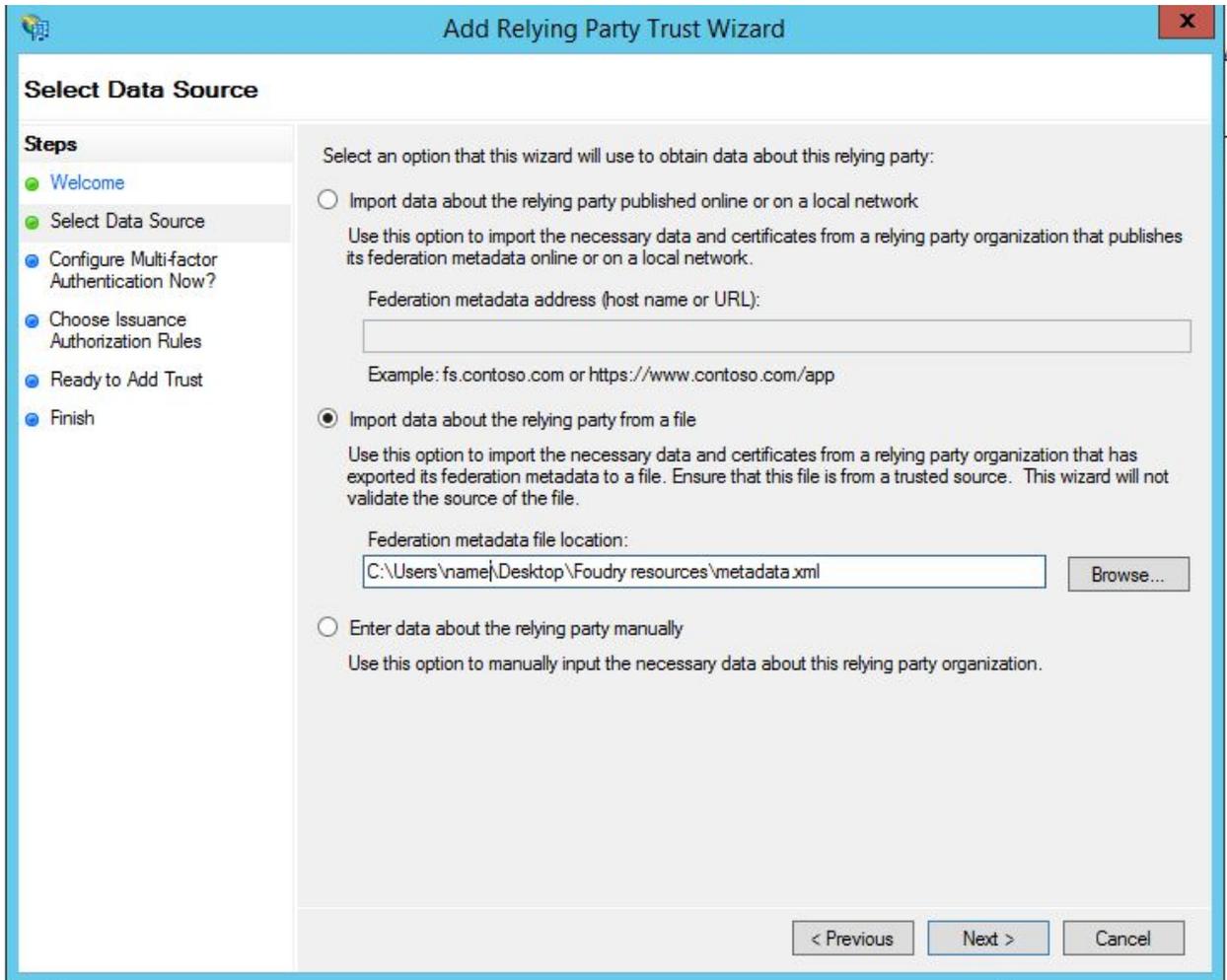
4. In Server Manager, click **Tools**, and then select **AD FS Management** to launch AD FS.
5. Under **Actions**, click **Add Relying Party Trust**.



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



7. On the **Select Data Source** page, click **Import data about the relying party from a file**, then **Browse** to select the Foundry metadata file, and then click **Next**.



8. On the **Specify Display Name** page, enter “EVERFI” or a variation in **Display name**, under **Notes** type an optional description, and then click **Next**. What you enter here is purely descriptive, so there is no “wrong answer.” Learners may see what you enter in **Display name** so make sure it will make sense to them.

Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name:

Notes:

< Previous **Next >** Cancel

Click through the next several steps in the wizard.

9. For **multi-factor authentication**, configure according to your organization’s practices.
10. On **Choose Issuance Authorization Rules**, choose **Permit all users to access this relying party**. Later, you can refine this according to your organization’s practices. Alternately, choose the **Deny** option and then refine later to grant authorization to this relying party as needed. Click **Next**.
11. On the **Finish** step, make sure the **Open the Edit Claims Rules** checkbox is checked, then press **Close**.

12. Add Name ID Claim

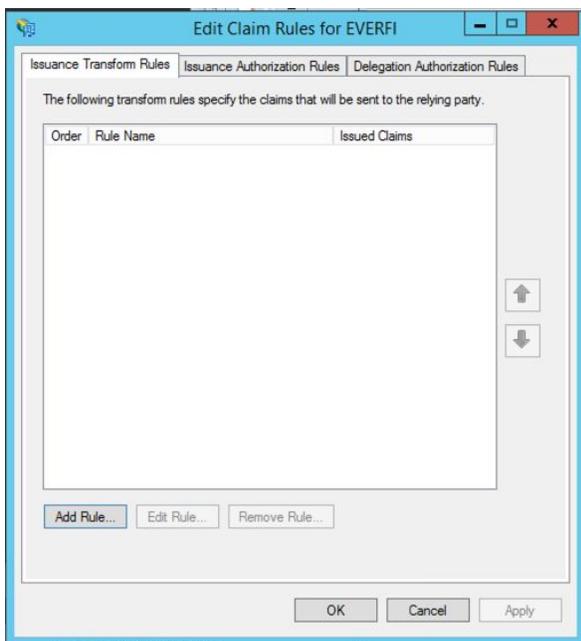
Refer to AD FS documentation on how to add claims to an existing relying party trust. For example, to send LDAP attributes as claims, see: [Create a Rule to Send LDAP Attributes as Claims](#).

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.

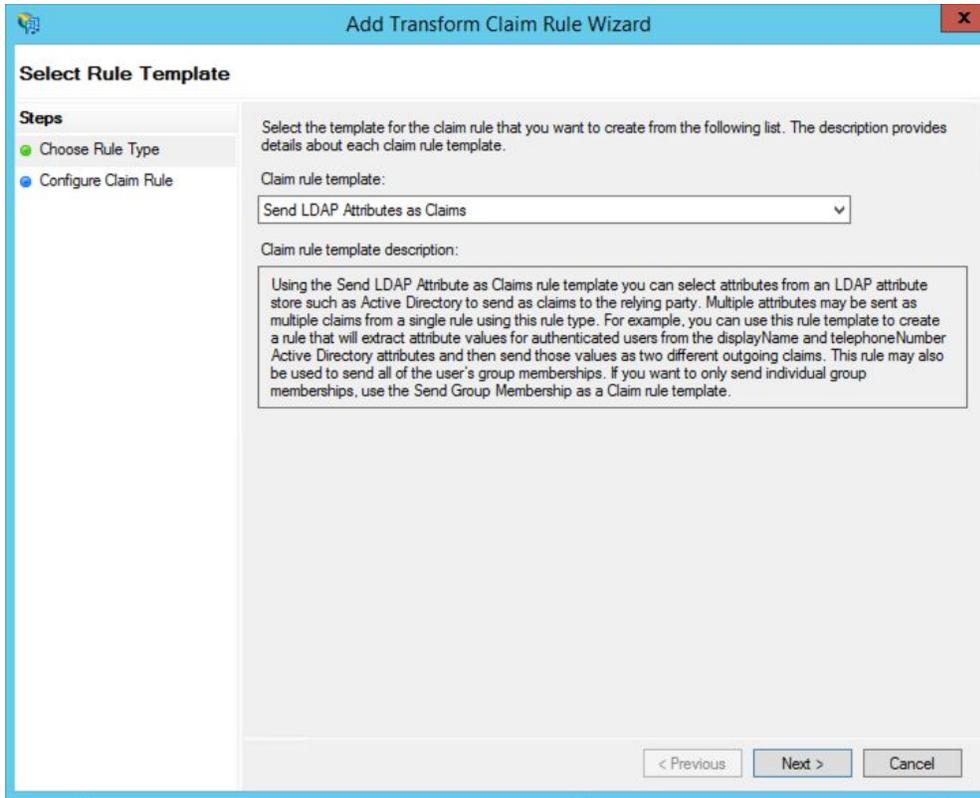
After adding EVERFI as a relying party trust, in AD FS, add a **claim** to the EVERFI relying party trust for whichever property in your system should go in the SAML NameID. This must match up in Foundry with the value stored in the User SSO ID field. Ensure the **Outgoing Claim Type** is set to **Name ID**.

To add a Claim, continue with the wizard or right-click the Relying Party Trust and choose **Edit Claims Rules**.

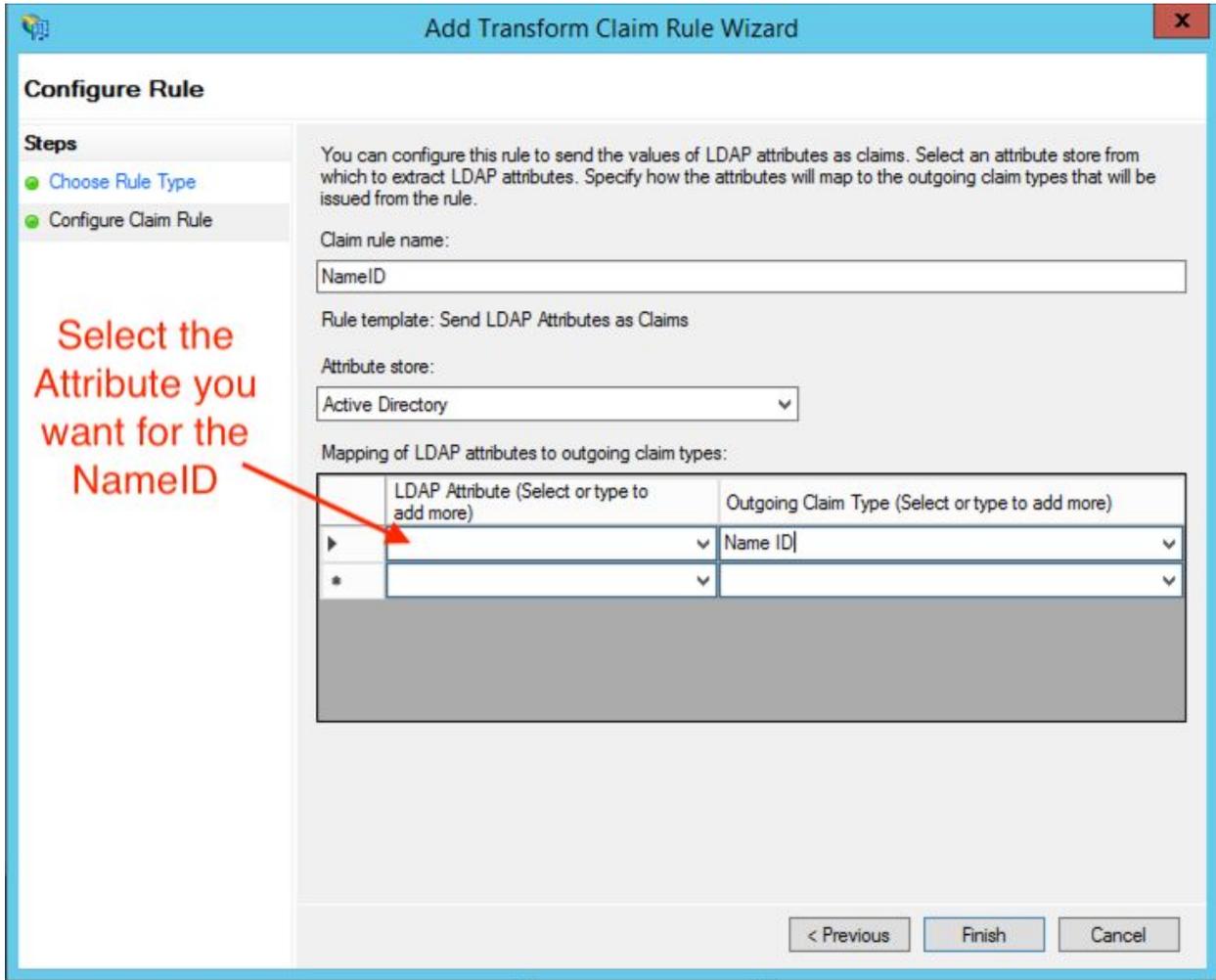
From the **Edit Claims Rules** window, click the **Add Rule** button



In Choose Rule Type, select the **Claim rule template** for your organization and click **Next**.



On the Configure Claim Rule step, enter **NameID** in the **Claim rule name**, choose the **Attribute store** and select the **Attribute** whose value should be passed in the NameID, and set the **Outgoing Claim Type** to be **Name ID**. Click **Finish** to save the Claim Rule.

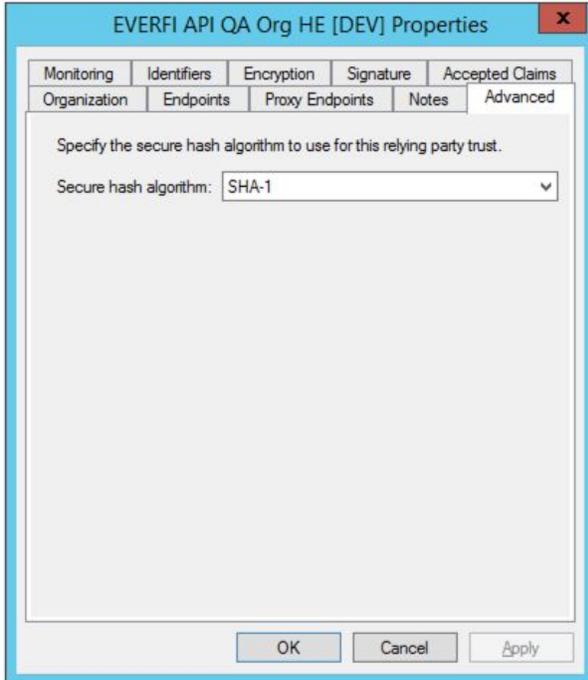


The sample below shows Active Directory as the Attribute store, but your organization may have a different configuration.

13. Algorithm

After saving the relying party trust, edit the EVERFI trust's properties again to adjust some settings.

On the **Advanced** tab, in the **Secure hash algorithm**, choose **SHA-1** and save.



14. Permissions

Verify the permissions by right-click the Relying Party Trust, choose **Edit Claims Rules**, then select the **Issuance Authorization Rules** tab and adjust the rules as needed.

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 Foundry because they won’t match to an existing user.

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. See [SSO User Registration](#) for more.

15. Additional Claims for User Provisioning (Optional)

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 3: Foundry Identity Provider Setup

16. Add your Identity Provider settings in Foundry

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 identity provider 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 creation during 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

How can I see the claims when they are encrypted?

If you are trying to troubleshoot the NameID or claims, you can temporarily disable encryption, then re-enable encryption after you've resolved the issue.

To do this, edit the properties of the relying party trust and on the **Encryption** tab, remove the EVERFI certificate. Remember to go back later to add the EVERFI certificate so that your Assertions are encrypted.

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:

SAML Attribute Map

Key

first_name

Value

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname|

Is editable?

Add

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.

“The signature verification failed” Error when Uploading SAML Metadata

Make sure you have a new version of the metadata file. Older versions of this file generated prior to 8/25/2020 produce this error when you attempt to upload them when adding a relying party trust.

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
1.6	5/12/2020	Single logout section and additional edits
2.0	8/25/2020	Major rewrite after ability to add relying party trust from SAML metadata file is released. No longer necessary to enter properties and certificate manually.

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 software products.