Microsoft Azure SAML 2.0 Single Sign-On Integration to ComplyEQ Foundry

This documentation reflects Microsoft Azure as of May 2019. We strive to keep these guidelines up to date and relevant but be aware that 3rd party software changes continually and therefore these steps may change over time. If you see a discrepancy, please let us know.

Table of Contents

Summary

This document demonstrates how to set up SAML single sign-on for ComplyEQ Foundry and Microsoft Azure. See also separate documentation for more general ComplyEQ single sign-on instructions at https://help.complyeq.com/technical-documentation#sso.

In general, in Azure, you will add an Enterprise Application for ComplyEQ. An Enterprise Application is the configuration of a SAML 2.0 Service Provider. You will upload the ComplyEQ SAML metadata file to this application, upload your organization's own X.509 certificate to the application, and verify the claims/attributes that will be included in the SAML assertion provided by your identity provider. Then, in Foundry, you will configure some settings to describe your own Identity Provider.

Read on for more detailed steps.

Download the ComplyEQ SAML Metadata File and Certificate

Login to Foundry as an admin user, navigate to **Settings → Single Sign-On**, click **View**, then download the ComplyEQ SAML Metadata File and save it for later use when you will need to upload this file into Azure.

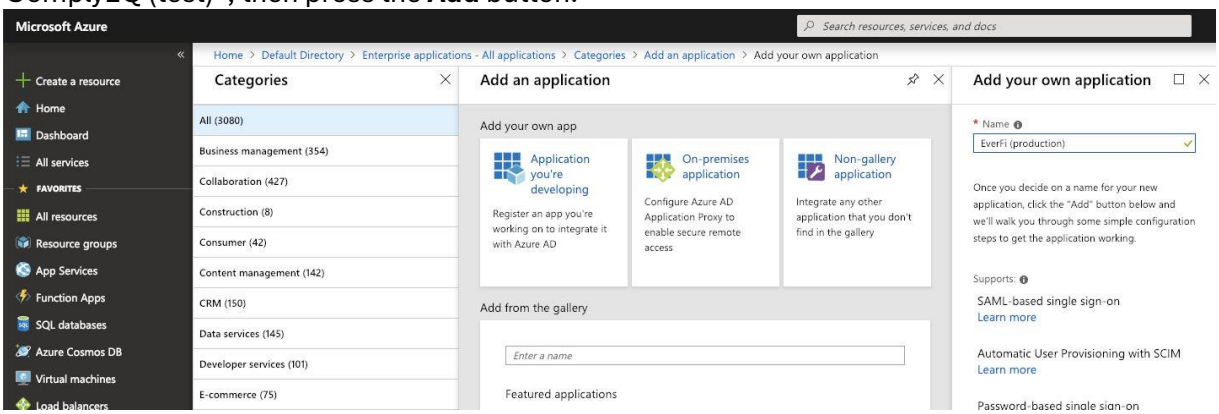
In the same area, download the Foundry certificate for later use.

Azure Application Setup

Add Enterprise Application

Login to Azure. From the Azure dashboard, navigate to **Azure Active Directory**, then Enterprise

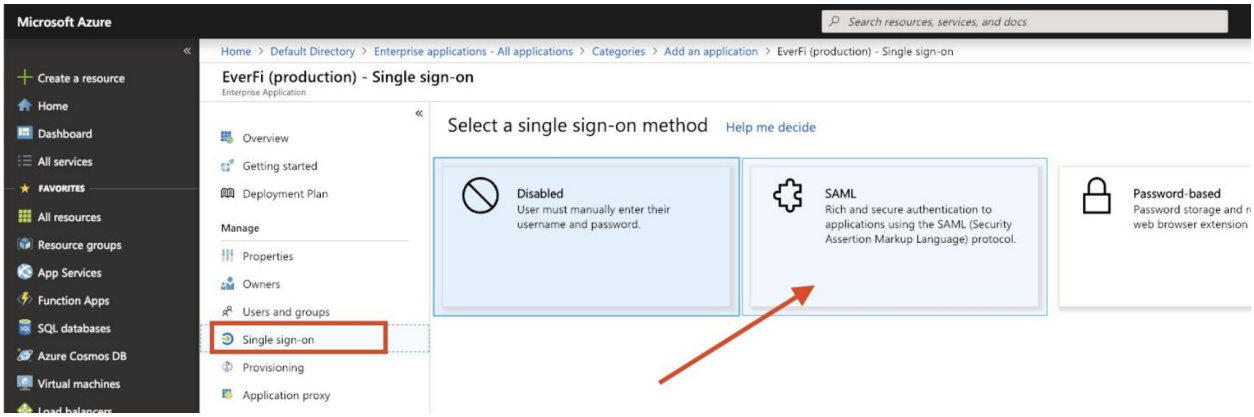
Applications. From Enterprise applications, add a new application, choose Non-gallery application, and enter a Name for the application, for example “ComplyEQ (production)” or “ComplyEQ (test)”, then press the **Add** button.



Upon saving the application, you will land on the application overview page for your newly added application. In Azure an application is the definition of a SAML Service Provider.

Manage Enterprise Application

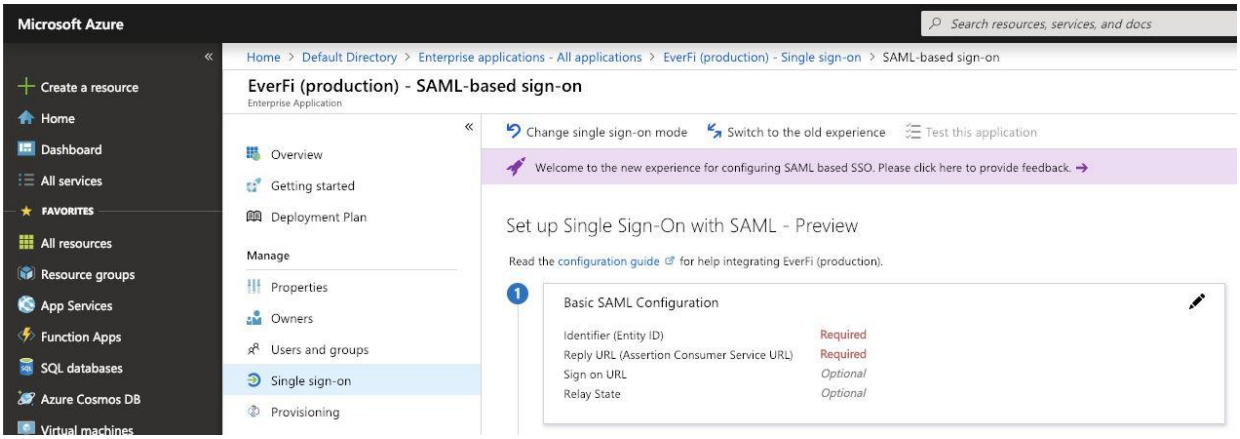
From the menu, choose Manage → Single sign-on, then choose the SAML method:



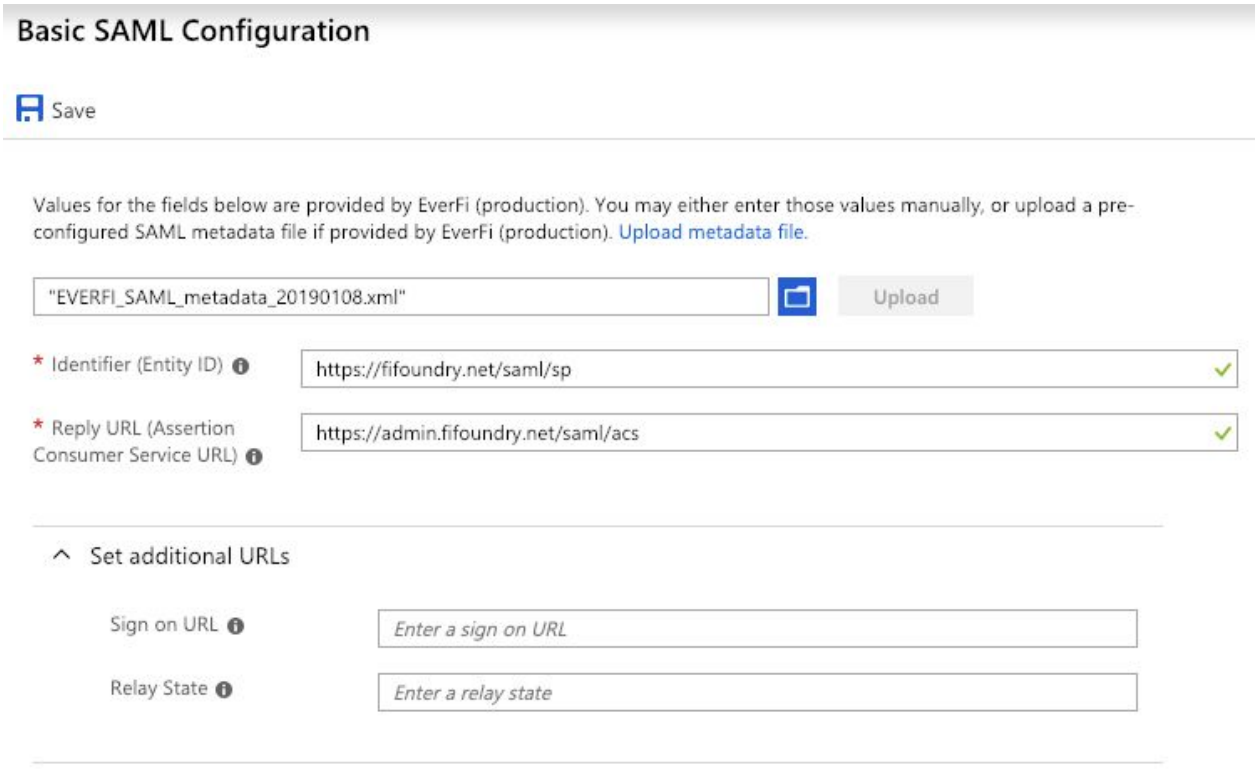
Next you will see the Single Sign-On with SAML setup page which contains several configuration areas.

SAML Configuration

The first section is Basic SAML Configuration.

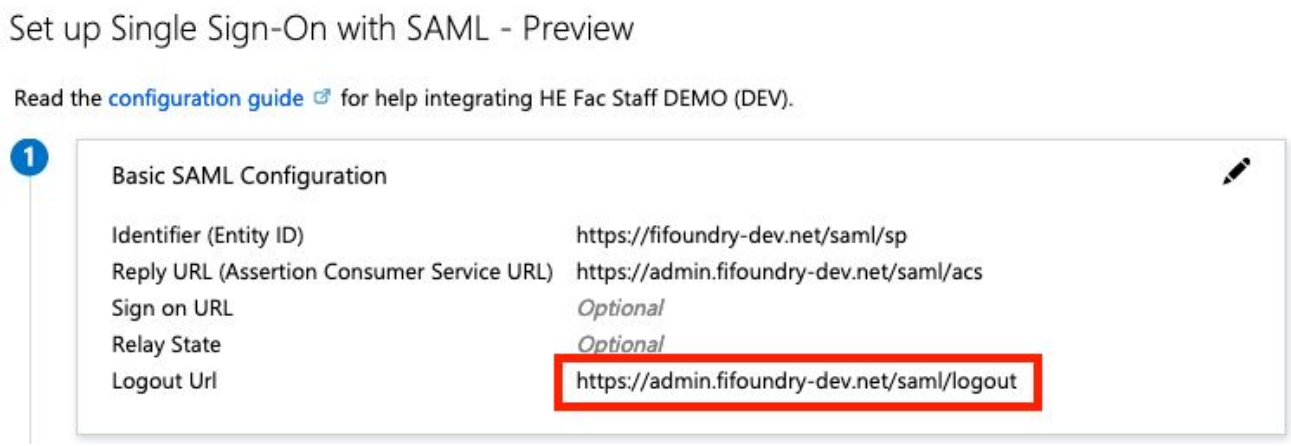


Edit this section and upload the ComplyEQ SAML metadata file that you previously downloaded from Foundry and save it:



Basic SAML Configuration. Note that the metadata file name has been changed from the default name.

If you want to support IDP-initiated single logout (SLO), then ensure that the Foundry SLO URL of **https://admin.fifoundry.net/{org-slug}/saml/logout** is entered in the Logout URL property where **{org-slug}** represents your organization's own unique slug that goes in the URL path.



Attributes & Claims

Next, observe the **User Attributes & Claims** section. If you wish to have new users created in Foundry during SSO, then you will need to refer to these later in Foundry when mapping the Microsoft attributes like first and last name to the corresponding ComplyEQ attributes.

Verify that the **Unique User Identifier** (nameidentifier) claim is correct. Although you can use any property you wish for the Unique User Identifier, ComplyEQ recommends using a unique and persistent value and you must ensure that your Foundry users must have this value in their SSO ID to SSO successfully. See SSO: SAML NameID and ComplyEQ SSO ID for more details.

SAML Certificate

This section is for your organization's SAML X.509 Certificate. You may use the auto generated certificate, create a new certificate or import a different certificate. The choice of your

organization's certificate is an important one, so if you're not sure, check with the people responsible for security at your organization. Also in this section, you can choose whether to sign your assertions, responses or both.

Once you have finalized the settings in Section 3, download the Federation Metadata XML from the hyperlink. This will save a file to your computer. Later you will import this file into the Foundry Identity Provider configuration.

Users and Groups

Consistent with your overall identity management posture, you will need to assign Active Directory Group(s) and/or User(s) to this application so they can access ComplyEQ. Assign Group(s) from the **Manage → Users and groups** menu link. Until you do this, users will not be able to authenticate. Obviously, you'll want to take care to ensure that only the right users have access to the ComplyEQ application. But be aware that even if a user gains Azure access when they should not, the user still must have an account in Foundry in order to SSO.

Token Encryption

We recommend enabling token encryption using ComplyEQ's public SAML X.509 certificate. To do this, you will need to upload into the Azure App the Foundry certificate that you downloaded earlier from the Foundry customer admin portal.

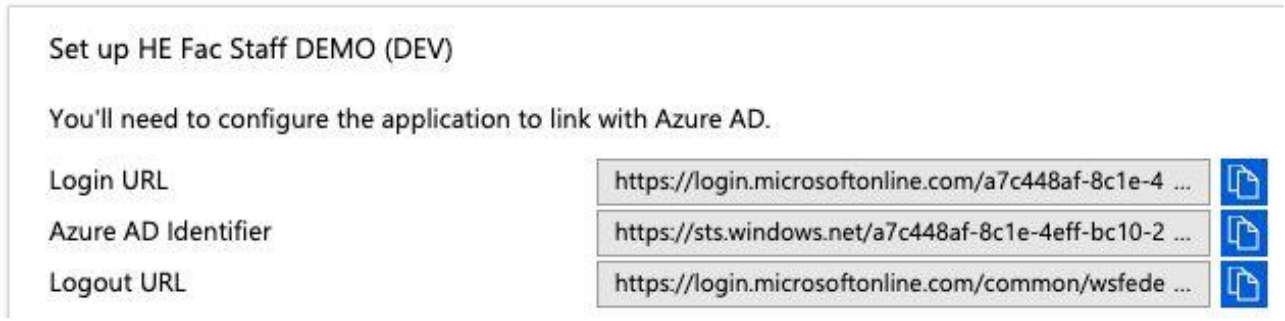
Foundry Identity Provider Setup

Refer to ComplyEQ'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 Azure. With Microsoft Azure, setting up the Identity Provider in Foundry is simple. In Foundry, you will upload your organization's own SAML Metadata file.

Single Logout SLO Setup

Refer to this section only if you want to support Single Logout

In ComplyEQ's experience, sometimes the SingleLogoutService URL property in the Azure IDP SAML metadata file clashes with the **Logout URL** property that is visible in the Azure admin console. If you run into issues with SLO, then you might want to try using the property that is visible in the Azure Admin Console as illustrated:



Try entering the Logout URL value into the corresponding Foundry IDP setup SLO property.

Mapping Claims to ComplyEQ Attributes

If you wish for new users to get created during SSO, then you will need to map attributes from the Microsoft claims to the corresponding ComplyEQ attributes. If you don't wish for new users to get created during SSO, then skip this section.

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

Microsoft Claim	ComplyEQ 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 Azure may differ.

Troubleshooting

User Prompted to Enter First and Last Name

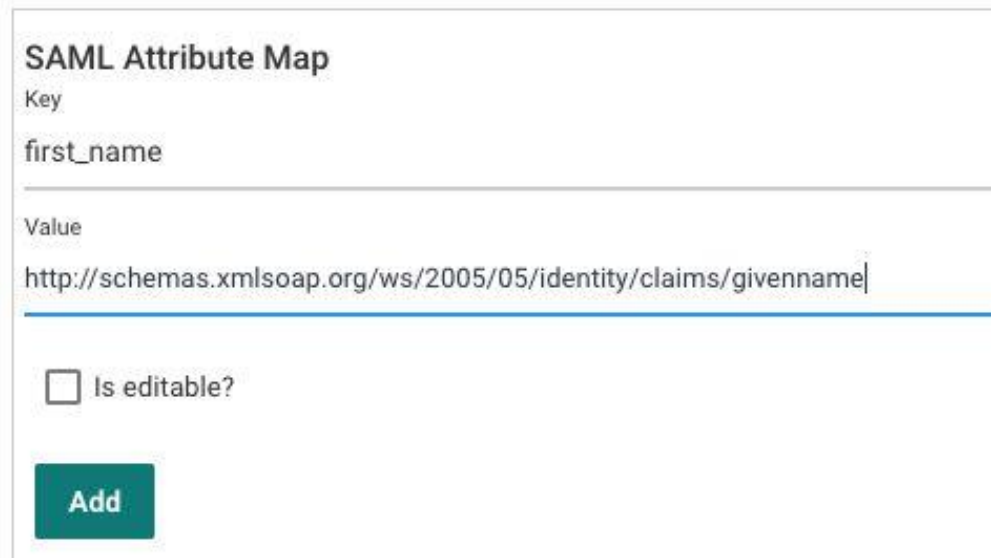
If, upon SSO, a user is prompted to enter first name, last name, and email address into a modal window in Foundry, then check the Foundry field mappings in the IdP setup. In the Foundry IdP setup, check the attribute maps. Rather than using just Givenname, for example, you might need the full claim name which might be prepended with a 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 Azure instead. The choice is yours. As long as Foundry can find the "Value" in the SAML assertion, the mapping will succeed.

FAQ

Rotating the Foundry SAML Certificate

Q: ComplyEQ has released a new certificate in Foundry. How do I rotate the certificate in Azure?

A: In general, SAML identity providers can use a service provider's certificate for token **encryption** and/or **signing** validation.

Encryption: If you have enabled Token Encryption for the Foundry App, then you will need torotate the encryption certificate to the new Foundry certificate. After doing this in Azure, go to your identity provider configuration in Foundry and update the ComplyEQ SAML Certificate to the newest certificate. After doing both steps, you will have fully rotated to the newest certificate.

Signing: Per Microsoft, Azure does not validate signatures in the AuthnRequest sent by service providers like Foundry*. Therefore, there is no update needed for **signing** certificates.

SP-Initiated Single Logout is Inconsistent

Q: When a user logs out of Foundry, sometimes it logs them out of Azure, and sometimes it doesn't. What is going on?

A: In our observations with Azure, we have noticed that if a user starts a Foundry session with SP-initiated SLO, and the user did not have a prior active session with Azure, that SP-initiated SLO does log the user out of Azure as you might expect it to.

If, however, the user already had an active session in Azure prior to launching SP-initiated SLO, then if the user proceeds to log out of Foundry, Foundry does send a SAML logout request to the Azure IDP, but the Azure IDP essentially disregards the logout request from Foundry and keeps the user's prior Azure session active.

Additionally, if the user started SSO from Foundry and without an active Azure session, we have observed the following: if the user is still "background logged-in" to Azure, and opens a new tab or browser window in Azure, if the user then logs out of Foundry, their other Azure session does not get ended, and the other Azure session remains active. We have observed that IDP-initiated SLO with Azure functions as you would expect: the user gets logged out of any Foundry sessions that originated from the Azure IDP-initiated SSO.

*Azure AD does not validate signed authentication requests if a signature is present. Requestor verification is provided for by only responding to registered Assertion Consumer Service URLs." Single Sign-On SAML protocol | Microsoft Azure Product Documentation (5/18/2020)

Documentation Updates

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.

Version	Date	Update
1.0	01/30/2019	First version of document
1.1	03/27/2019	Document single logout setup
1.2	5/2/2019	Misc clarifications and details
1.3	5/9/2019	Reflect the newer SAML URL model described more in: https://foundrysupport.everfi.com/knowledgebase/saml-sso-entityid-change/
1.4	9/25/2019	Correct minor errors (mixing up ADFS and Azure)
1.5	12/02/2020	Add section on Token Encryption Add FAQ section on how to rotate certificate
1.6	3/17/26	Minor updates, rebranding.

NOTE: Azure UI labels and navigation may differ in newer Azure portal experiences. Use this step as conceptual guidance if labels do not match exactly.