Okta Single Sign-On Integration to ComplyEQ Foundry

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 and single logout (optionally) for ComplyEQ as a service provider and your organization's Okta instance as an identity provider. After you complete this setup successfully, your organization's users will be able to access ComplyEQ content and have ComplyEQ securely and seamlessly authenticate their identity through your organization's identity provider.

These are the main steps you will do:

1. In ComplyEQ Foundry, download the ComplyEQ certificate file that will be needed in Okta. Also, gather necessary SAML SP properties for Foundry that you'll need in Okta.

2. In Okta, create an App for Foundry. Get the IDP metadata URL for this App as this will be needed later in Foundry.

3. In Okta, assign Groups to the App.

4. Back In Foundry, add an identity provider configuration by linking to the SAML metadata URL for the COMPLYEQ App in Okta, and configuring a few additional settings. Optionally, map Okta attributes to corresponding COMPLYEQ attributes.

Part 1: Gather ComplyEQ Certificate and Metadata

In this section, you will get a certificate file for the Foundry ComplyEQ X.509 certificate. In Okta, you will need to upload this certificate file if you want to encrypt assertions or set up single logout (SLO). If you don't want to encrypt assertions or set up SLO, then you can skip this step.

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

Sensitivity: Public

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

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

3. From the ComplyEQ 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.

Part 2: Okta - Add App

5. In Okta, log in as an administrative user who has permissions to add Apps.

6. In Okta, click the **Admin** button.

*Note: the next steps are from the Okta **Classic UI** interface option.*

7. From the Admin dashboard, click **Applications** from the nav menu.

8. From the Applications section, click **Add Application.**

9. Click **Create New App**.

10. On the **Create a New Application Integration** popup window, for **Platform** choose **Web** and for **Sign on method** choose **SAML 2.0**, then press **Create**.

11. You are now in the **Create SAML Integration** wizard. Enter an **App name** like “ComplyEQ” and upload the ComplyEQ Logo located at ComplyEQ logo (download the image file from the link, then upload it to Okta), then click **Next**.

12. Now you are on the **SAML Settings** page. In **Single sign on URL**, enter the ACS URL value you got earlier from ComplyEQ.

13. Leave the defaults for **Use this for Recipient URL and Destination URL** (checked) and **Allow this app to request other SSO URLs** (unchecked).

14. In **Audience URI (SP Entity ID)**, enter the EntityID value you got earlier from ComplyEQ.

15. In **Name ID format**, leave the default of **Unspecified**.

Sensitivity: Public

16. In **Application username**, choose the Okta property you want to send to Foundry as the username. The Foundry users must have this value in the **SSO ID** field for SSO to succeed. See SAML NameID and ComplyEQ SSO ID for more details.

17. Click **Show Advanced Settings** to display additional settings

18. In **Response**, choose **Signed** (the default)

19. In **Assertion Signature**, choose **Signed** (the default)

20. In **Signature Algorithm**, leave the default setting unless you wish to change.

21. In **Digest Algorithm**, leave the default setting unless you wish to change.

22. For **Assertion Encryption**, we recommend **Encrypted**. If you run into issues where you need to troubleshoot, you might want to temporarily change it Unencrypted to see the cleartext assertions in diagnostics but remember to switch it back to Encrypted when done.

23. If you chose to Encrypt the assertion, then in the next fields, enter the **encryption algorithm**, **key transport algorithm**, and in **encryption certificate,** upload the ComplyEQ certificate you downloaded earlier.

24. If you wish to **Enable Single Logout**, then check this box. As of this writing, we have observed that Okta supports SP-initiated SLO but not IDP-initiated SLO[1]. Later, be sure to also check the **Also log users out of this provider when logging out of Foundry** checkbox in the Foundry IDP setup described in Part 4.

25. If you chose to Enable Single Logout, then enter the **Single Logout URL** you got earlier from the ComplyEQ SAML metadata.

26. If you chose to Enable Single Logout, then enter the **SP Issuer** from Step 8a.

27. If you chose to Enable Single Logout, then for **Signature Certificate**, browse for the ComplyEQ certificate you downloaded earlier, and click **Upload Certificate**.

28. In **Attribute Statements**, add any SAML attributes you wish to send to Foundry if you desire for new users to get created during SSO.

[1] Is IDP-initiated Single Log-Out supported? | Okta Knowledgebase "Question: Is IDP-initiated Single Log-Out supported? Answer: No. Only SP-initiated SLO is supported." May 13, 2020

Sensitivity: Public

If your Foundry users will be added/uploaded separately from SSO, then skip this step. If you wish for new users to get automatically created for just-in-time user provisioning during SSO, then continue following the instructions in this step. Generally, organizations who are in 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** provide attributes for:

- first name
- last name
- email address. Even if you already provided email as the Okta username, you still must add this again as a regular attribute.

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

- Location - be sure to map to an Okta value that contains the same exact **location name** as it is in Foundry (not ID). Location name is case sensitive.
- User Type (for example `fac_staff_learner` for a faculty/staff learner or `cc_learner` for a code and conduct learner)
- Role - for example, `supervisor` or `non_supervisor`, but exact values may vary depending on the UserType and your line of business

You can name the attributes anything you wish; later on, in Foundry, you'll need to specify those attribute names. If you do not provide any of the 3 optional claims listed above, then Foundry will provide defaults instead based on the settings in the Foundry identity provider configuration.

If you want to specify the user's role, then the assertion **must** also specify the User Type, even if the User Type is the same as the default user type in the IDP configuration. See the table below for the various User Type + Role combinations depending on your organization's line of business:

Line of Business	Group of People / User Type	User Type Attribute Value	Role Attribute Value (choose 1)
Code & Conduct	"Employee Learners"	cc_learner	supervisor non_supervisor
Adult Financial Services	Learner	next_learner	default

Sensitivity: Public

Setting Supervisor or Non-Supervisor Role

> *This section is a case study illustration. Your organization's own unique instance of Okta will be different from this. Refer to your own organization's specific Okta settings when you configure the Foundry app and do not replicate this example letter-for-letter.*

The one Attribute value that can be complex to set is the role. You will need to determine which property or condition in Okta means that a user is or is not a supervisor/manager. Depending on your Okta configuration, this might be a custom user property, or it could be based on belonging to a group, or it could be some other setting.

As an illustration, your Okta instance might have a custom user property called `IsManager` which is "true" or "false"; this value might be set by your separate user system (like LDAP). *This is just an example; your own instance of Okta is sure to be different.*

When you add the role attribute, you cannot simply set this to be the `user.IsManager` property because Foundry requires the Attribute value to be either `supervisor` or `non_supervisor` if the User Type is "Employee Learner" or "Faculty/Staff Learner". Therefore you will need a custom expression like this for the attribute Value:

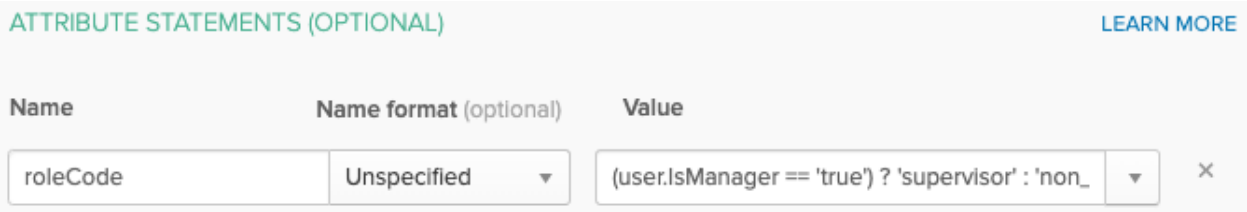
```
(user.IsManager == 'true') ? 'supervisor' : 'non_supervisor'
```

Another possibility is that the user might be in a certain group, for example **HRManagers** (this is just a made-up example):

```
user.isMemberOfGroupName("HRManagers") ? 'supervisor' : 'non_supervisor'
```

When complete, the specific Attribute might look like the following in Okta. Note that the complete Value is clipped by the user interface.

Sensitivity: Public



Remember that if you specify a **role**, then you must also specify the **User Type**.

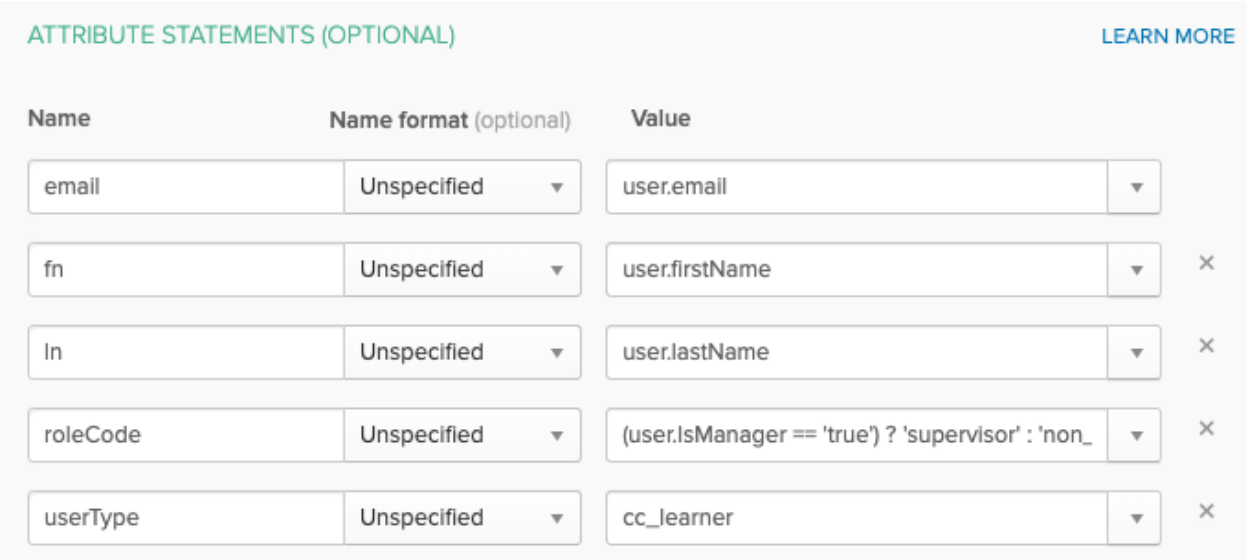
Ultimately, you'll want your Okta assertion XML to look like this, if you have chosen to name the User Type Attribute userType and the role attribute roleCode:

```
<saml2:Attribute Name="userType"
                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified"
                 >
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
                          xsi:type="xs:string"
                          >cc_learner</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="roleCode"
                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified"
                 >
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
                          xsi:type="xs:string"
                          >non_supervisor</saml2:AttributeValue>
</saml2:Attribute>
```

Looking at the Assertion XML above, if the learner is a supervisor, then the AttributeValue will be `supervisor` instead.

The Attributes setup in Okta might look like this when you are done. Notice in this example that the `userType` attribute Value is hard coded to `cc_learner`.

Sensitivity: Public



Given the Okta Attributes above, In Foundry, the Foundry identity provider configuration **Attribute Maps** section will look like the following setup below. Be sure that you name the SAML attributes the exact same as the attribute names you entered in Okta; attribute names are case sensitive. Note that the top-to-bottom sorting of the attribute names in Foundry doesn't matter.

Foundry User Pro...	SAML Attribute	Is editable?	Actions
User Type	userType	No	Remove
Email	email	No	Remove
Last Name	ln	No	Remove
First Name	fn	No	Remove
Role	roleCode	No	Remove

After setting up attributes, click **Next**

33. In **Help Okta Support understand how you configured this application,** fill in the various questions to assist Okta support if necessary.

34. Click **Finish**. You've now added the App for Foundry in Okta.

Sensitivity: Public

Part 3: Okta Assignments

35. In Okta, assign any **Groups** and **People** to the ComplyEQ App you have just created. Remember that the User still must exist in Foundry to SSO, unless you enable the option for Foundry to create new users upon SSO.

Part 4: 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.

With Okta, setting up the Identity Provider in Foundry is simple.

36. In Foundry, you will configure your organization's SSO Metadata with the **Use a URL** option on the Foundry IDP setup page. The URL will be that of **Identity Provider Metadata** link that is on the **Sign On** tab of the App in Okta. You can "copy" this URL and then "paste" it into the Foundry setup page.

Enter the other properties as described in the documentation.

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 code and conduct can skip this section because your organization will upload your users into Foundry and not create them during SSO.

37. In the Foundry IDP setup, check the "Allow automatic registration during SSO" checkbox.

38. Set up default values for new users for **user type**, **role** and **location** (omit location for financial education organizations).

39. In the **SAML Attribute Map** section, add Attribute maps for the Okta Attributes to the corresponding ComplyEQ attributes. Be sure to Save the identity provider after adding or updating the Attributes.

Documentation Updates

Version	Date	Update
1.0	06/04/2019	First version of document

Sensitivity: Public

1.1	9/9/2019	Minor updates
1.3	12/02/2019	Minor updates
1.4	3/5/2020	Correct error relating to certificates. The certificates to upload into the Foundry App are the Foundry certificates.
1.5	4/9/2020	Add more details Provide detailed instructions on User Type and Role attributes
1.6	3/16/26	Minor updates, rebranding

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.

Sensitivity: Public