Okta Single Sign-On Integration to EVERFI Foundry

This documentation reflects Okta as of January 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.

Summary

This document demonstrates how to set up SAML single sign-on and single logout (optionally) for EVERFI as a service provider and your organization's Otka instance 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.

These are the main steps you will do:

1. In EVERFI Foundry, download the EVERFI certificate file that will be needed in Okta.
2. In Okta, create an App for Foundry.
3. In Otka, assign Groups to the App.
4. Back In Foundry, add an identity provider configuration by linking to the SAML metadata URL for the EVERFI App in Okta, and configuring a few additional settings. Optionally, map Okta attributes to corresponding EVERFI attributes.

Part 1: Gather EVERFI Certificate and Metadata

In this section, you will get a certificate file for the Foundry EVERFI 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.

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.

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**.*

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 “EVERFI” and upload the EVERFI Logo located at EVERFI 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 EVERFI.

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 EVERFI.

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

16. In **Application username**, choose the Otka 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 EVERFI 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 EVERFI 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. Later on, 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 EVERFI 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 EVERFI 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.

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, 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** 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 a Okta value that contains the same **location name** as in Foundry (not ID)
- User Type
- Role - for example, supervisor or non_supervisor, but exact values may vary depending on the UserType and your line of business

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

You can name the attributes anything you wish; later on, in Foundry, you'll need to reference those names.

After setting up any optional 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.

Part 3: Okta Assignments

In Otka, assign any **Groups** and **People** to the EVERFI 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 EVERFI's general SAML documentation for the setup you will need to do in Foundry to configure your identity provider settings.

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

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 Otka. 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 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.

In the Foundry IDP setup, set up default values for user type, role and location, and map attributes from the Okta claims to the corresponding EVERFI attributes if you are allowing new user creating via SSO.

Documentation Updates

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

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.