

Round-Trip From ColdFusion to Okta using SAML and ColdFusion 2021

Round-Trip From ColdFusion to Okta using SAML and ColdFusion 2021 (<http://ciacfug.org/blog/round-trip-from-coldfusion-to-okta-using-saml-and-coldfusion-2021b>)

Posted by Andy Peterson

14 Dec 2020 07:52 PM

I feel as though when the Adobe ColdFusion 2021 planning committee called their first meeting to order, the number one item on their agenda was how to make a developer's life easier. In addition to the AWS/Azure cloud configuration/integration capabilities I've posted about, I now have Okta integration to play with, via SAML. And with a few lines of code to handle authentication, I now have the ability to leverage SSO, MFA, and much more in my applications.

When working with SAML, there are two settings in the ColdFusion Administrator under the Security tab that need to be addressed: SP (Service Providers) and IDP (Identity Providers). The first I'll cover is the SP Configuration. You own/are the Service Provider, by way of the ColdFusion application you built/host.

SP Configuration

The simplest way to get started is to log into the ColdFusion Administrator, head over to the Security section and click on the SP link. From there, click on the GenerateSP button, and let ColdFusion Administrator do the heavy lifting for you:



Keep all the default settings for your generated SP, except the Identity ID and ACS URL as shown below. Set the ACS to point to a publicly available page on your domain that you will use to "catch" the SAML response.

Edit Service Provider : testSP

Name*

Description

Entity Id* System generated.

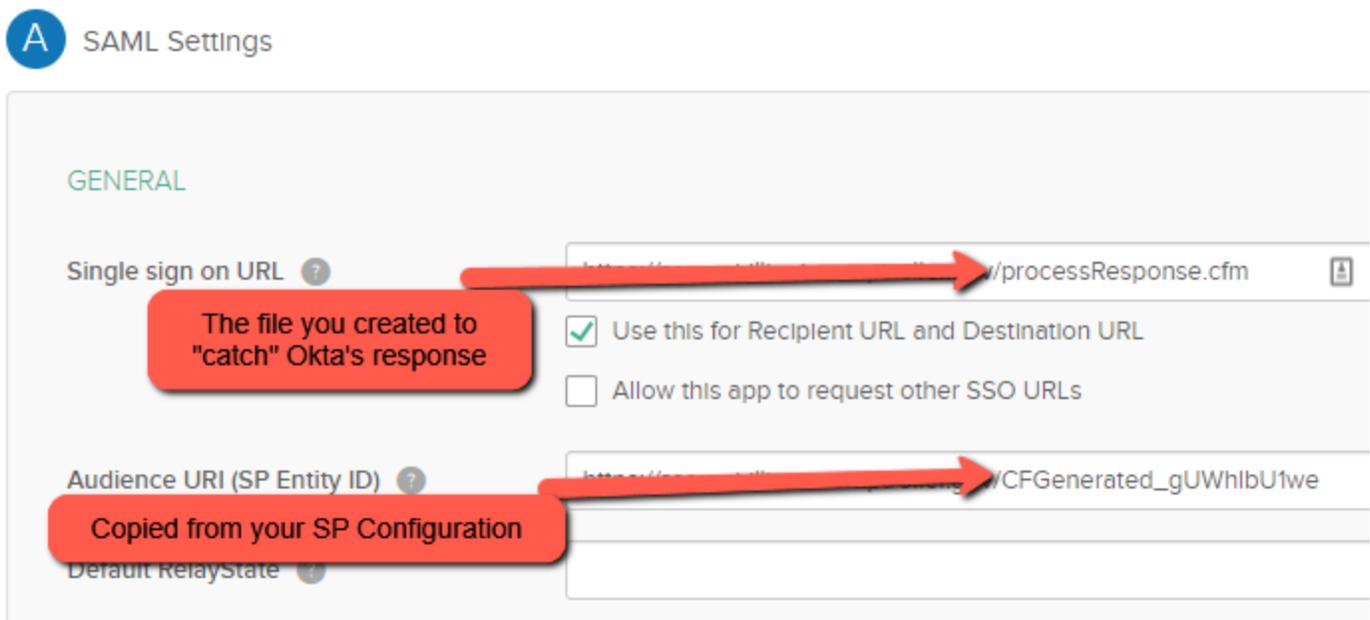
ACS(Assertion Consumer Service) URL* You will create this page.

You will also have to name your SP. I chose testSP."

IDP Configuration

IDP is your identity provider. We are using Okta, and so you will need to log into your Okta account where you can configure your application before configuring the IDP settings in the ColdFusion Administrator. Once you have the application set up in Okta, your application can then leverage Okta. Okta will receive your request to sign in from your IP as defined in ColdFusion, and then return the response after a successful sign-in (ProcessResponse.cfm).

While most of the settings are intuitive, let's take a look at some. In the image below, your Single sign on URL is the same as the ACS (Assertion Consumer Service) URL you configured in the SP Configuration. Also your Audience URI (SP Entity ID) is also picked up from your IP, as shown below.



Now that Okta is set up, you can configure the IDP in the ColdFusion Admin, the Administrator offers a variety of ways, from importing an xml file to manually configuring the settings. For my Okta

configuration, I simply imported the xml file that I exported from Okta that contained the necessary information. Regardless of how you get it, you are going to need the following information, with the defaults for the bindings kept, and the Entity ID and SSO URL the same as above:

Select the type of Identity Provider Configuration:

Import from SAML URL Import from an existing SAML Definition Import from XML file in local

Entity Id*	<input type="text"/>
SSO URL*	<input type="text"/>
SLO URL	<input type="text"/>
Logout Response URL	<input type="text"/>

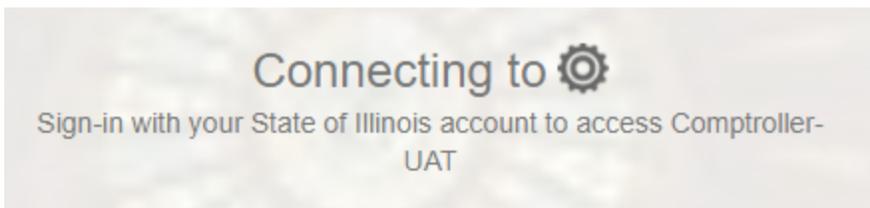
You should have all of this information by now

The Code

You are going to be setting up two pages - the first is your page that sends the request to Okta for the user to log in. The IDP and SP settings you defined are sent on their way to Okta using the built in `InitSAMLAuthRequest()` function:

```
index.cfm
1  <cfset config = {
2
3      idp = {name = "Illinois.gov"},
4
5      sp = {name = "testSP"},
6
7      relayState = "cart"
8
9  }>
10
11 <cfset InitSAMLAuthRequest(config)>
```

Below is a look at the page ColdFusion has sent our user to for authentication.



Sign In

Username

! Please enter a username

Password

Once you enter your username and password, Okta responds by sending you back to the Single sign on URL that you configured, and you should see a response like this:

struct	
ATTRIBUTES	struct [empty]
AUTHENTICATED	YES
NAMEID	andy.peterson@illinoiscomptroller.gov
NAMEIDFORMAT	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
NAMEIDQUALIFIER	undefined
NAMEIDSPQUALIFIER	undefined
RELAYSTATE	cart
SESSIONINDEX	COLDFUSION1f80d75b-5ec4-4300-a08c-39f46bfad3c2

Round trip completed! That is because on that page is this code which includes a call to the ProcessSAMLResponse() function:

```

processResponse.cfm
1  <cfset response = ProcessSAMLResponse("Illinois.gov", "t
2
3  <cfdump var = "#response#">

```

And that's it! So with this code, your users can access their SSO by way of MFA and other security protocols that you no longer have to worry about. Let Okta handle the security/authentication, and you handle your application and authorization!

Tags: CFML (<http://ciacfug.org/blog/category/cfml>), ColdFusion (<http://ciacfug.org/blog/category/coldfusion>), Okta (<http://ciacfug.org/blog/category/okta>), SAML (<http://ciacfug.org/blog/category/saml>)

0 Comments (<http://ciacfug.org/blog/round-trip-from-coldfusion-to-okta-using-saml-and-coldfusion-2021b#comments>)

Copyright © Andy Peterson. All rights reserved.

Powered by ContentBox v4.2.1+737