SIMPLE SSO SETUP

Step by step instructions for setting up “Simple SSO” within Campaign Management.

Step 1

Account manager or Local United Way coordinator and client decide to proceed with SSO setup.
AM or LUW verifies that the client will only be using simple SSO for login and not for adding donors.
AM or LUW contacts FrontStream’s internal IT to begin the process: adminsupport@frontstream.com

Adding donors through SSO is a more complex process and needs to be specified from the beginning

Step 2

FrontStream passes the following information to the client to test decryption. Client decrypts the following string using the encryption parameters and key provided by FrontStream. These parameters have been configured on the CM Administrative site for the campaign.

The information below, which is generated by FrontStream, is provided for example purposes only.
String: wQXsLAa87UcJ/Y1h6/A3X7flC8TJ3SnUBrqp47jlVMaxG4Iel2eQ302BrQXtZRTZi1tQgxeXdUWe1mz6cC/fqw==
Encryption Key: 7DhxUqBky8CPJtkU6vWu1t3YoZJ/B17h Input
Vector: mAcx7gpWY78=
Cipher Mode: CBC Padding
Mode: PKCS7

This will confirm that the key created for the campaign works as expected.
It is at this point that the AM/LUW should setup and configure the campaign with donors to test!

Step 3

Once confirmation that the encryption parameters are working as expected, the company should create a SAML assertion and encrypt it with the encryption parameters in Step 2.

Below is an example of the assertion they need to create.

<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
<saml:AuthenticationStatement AuthenticationMethod="password"
AuthenticationInstant="2009-01-01T10:32:00Z">
<saml:Subject>
<saml:NameIdentifier SecurityDomain="workingforcharity.org" Name="donorID" />
</saml:Subject> </saml:AuthenticationStatement> </saml:Assertion>

In this example the company will put in their own current date/time stamp and the Name should be populated with the "donorID" of the donor they are attempting to log in to our application. Once they have created the SAML assertion and encrypted it with the parameters in Step 2 they should email it back to the account manager and they will confirm with technical support that FrontStream is able to decrypt the data. At this point everything should be ready to test against the Campaign Management application.

Step 4

Client uses the following URL and Query string parameters to test their encrypted SAML assertion.

https://opcssso.unitedeway.org/?campaign=YOURCAMPAIGNCODE&Create=2
or
https://opcssso.frontstream.com/?campaign=YOURCAMPAIGNCODE&Create=2

*Your AM/LUW will provide you with the CAMPAIGNCODE

Client should make sure to generate a new SAML Assertion from the one sent in Step 3 as the date/time stamp cannot be older than 5 minutes.

Step 5

Client tests SSO login and informs AM that SSO is working successfully.