True View SSO - SAML Implementation

Overview

Implementing Single Sign On to our application via SAML 2.0 enables the capability to automatically authenticating the user.

To connect to the True View application via SAML, we will need to know:

- What identifying attribute will be used for each member? (e.g. email, ssn, etc)
- Do you sign your SAML messages?
- Do you encrypt your SAML messages?
- Do you have a separate environment set up to test SAML connections?

Requirements

- An identifier for each member (e.g. email, ssn, etc.) for member account identification
- A signed SAML assertion. Optum will need to be provided with your public certificate used to validate the signed assertion.

Supported Options

- SAML assertion encryption. Optum provides the public certificate to be used when encrypting their SAML assertion at the metadata path listed at the bottom of this document.
- Plan benefits attributes. Optum supports the ability to pass in plan benefit values in order to see the data reflected on the True View dashboard.
- Non-Production Environment testing. If you have a separate environment within your infrastructure for testing, we can use that space for testing prior to go-live.

Process

1. Client will generate public and private certificates and share the public certificate with Change Healthcare. We will need the certificates shared prior to testing in our Staging and UAT environments so that it can be pre -validated prior to Production.

2. For our transparency application, the user's account credentials (member identifier) should be established in our member database before authentication for the client as a subsequent validation check. This typically arranged as a batch eligibility file import, with updates ongoing as determined through the implementation cycle.

3. The Client's Member must be authenticated into Client's portal through Client's authentication procedures. We recommend that the link to our applications is not made available until after Client portal user authentication, preventing any failure to authenticate notification back to the unauthenticated user.

4. After the user is authenticated in the Client Portal, the Client sends (via an HTTP POST action) a standard SAML Response to Change Healthcare.

5. The SAML assertion is processed, at which time the member account identifier is validated in the member database. The following actions may occur:

a. SAML SSO is successful: Member accesses the True View application

b. SAML SSO fails: Error message describing the failed request is displayed

Required SAML Assertion Details

Information	Description
Name Identifier	Identifies the subject of a SAML assertion, which is typically the user who is being authenticated. It corresponds to the <saml:Subject><saml:NameID> element in the SAML assertion. Should be the unique ID sent to Optum in the client's eligibility file. This will be the way that Optum connects a client member to their appropriate member account during the SAML process.
Issuer	Identifies the Identity Provider making the request. It corresponds to the <saml:Issuer> element in the SAML assertion. Optum uses this to make sure that collisions are avoided when looking up the Name Identifier for user being authenticated.

SAML URLs and Paths

Name	HTTP Base URL	Metadata Path	Assertion Path
UAT	https://*.uat.changehealthcare.com	/saml/metadata	/saml/callback
Prod	https://*.changehealthcare.com	/saml/metadata	/saml/callback

Replace the * above with the subdomain for your access.

E.g. https://acmehealthcare.uat.changehealthcare.com/saml/metadata