SSO Technical Requirements

Last Modified on 08/09/2023 1:06 pm EDT

Overview

The Single Sign-On (SSO) feature allows users to log in to multiple applications, software, or websites by signing in once using a single sign-on (user id and password).

Related Information/Setup

Please refer to the SSO Frequently Asked Questions article for more information regarding SSO.

- Single Sign-On (SSO) Frequently Asked Questions

SSO Technical Requirements

Before configuring the Resolver SSO feature, the following technical requirements must be met:

- A valid Identity Provider (IdP) must be configured with the SAML 2.0 Web Browser profile using the SAML 2.0 OASIS standard and must provide a valid IdP metadata file containing the following:
  - X509 RSA 2048 bits Public Certificate (RFC 5280) (`<ds:X509Certificate>`)
  - **EntityId** (`<md:EntityDescriptor entityId=" " >`)
  - **SingleSignOnService** URL with HTTP Redirect Binding (`<SingleSignOnService Binding==" " Location==" " >`)
  - **NameIDFormat** in `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`

    IdP must communicate using HTTP over TLS [RFC 2818]
  - A SHA-256 signature in the metadata, response, or assertion

> ***Note:***
> *Resolver does not support SSO redirect/logout URLs in the Metadata file.*

EXAMPLE

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://idp/saml/metadata/622342">
  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIEFzCCAv...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp/trust/saml2/http-redirect/slo/622342"/>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp/trust/saml2/http-redirect/sso/622342"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https:// idp /trust/saml2/http-post/sso/622342"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp/trust/saml2/soap/sso/622342"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```

- Certificates must have at least a three-year expiry and should be valid a minimum of 8 months before expiring.
- The RCS profile requires at least the message or the assertion to be signed.
- The username for the assertion subject statement should be the user's primary email address.

> ***Note:***
> *The username should be identical to the email address used to register the user in Core.*