

Manual setup of SSO config

This doc will be useful even if doing an import using a Federation Metadata XML URL, as the field mappings are not yet importable, and they can be gleaned in the same way as in the manual setup.

The first thing we need is the Metadata XML file. If provided the URL, visit that page to find the details

We need the following from the XML contents:

- An Entity ID
- A login URL
- An x509 certificate
- Field mappings (1 unique, preferably 1 each for email, first name, last name)

An example XML file is in the code block below (from 1 of our Azure active directories), and we can find the above by searching:

- ``entityID`` - at the top, it is ``entityID="https://sts.windows.net/667d9a8d-34fd-4ea9-99a5-b740e26edaac/"``. We copy ``https://sts.windows.net/667d9a8d-34fd-4ea9-99a5-b740e26edaac/`` (the final forward-slash is important) over to the SSO config
- ``SignInService`` - at the bottom, it is ``<SingleSignInService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/saml2" />``. We copy over ``https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/saml2``
- ``X509Certificate`` - near the top, in a truncated form, it is ``<ds:X509Certificate>MIIC8DCCAdigAwIBA...</ds:X509Certificate>``. We copy over the `MII...` value
- ``ClaimType`` - we have a number of fields here under `ClaimType`, we want to map 1 that indicates it is unique to ``Unique ID`` our end, and then 1 each for whichever seems like first name, last name and email. Note that if there is no unique ID field, you could probably specify the email field as the unique ID field. In this instance, we do have a unique ID field, so we set up the field mappings:
 - Unique ID - ``http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier``
 - First name - ``http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname``
 - Last name - ``http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname``
 - Email - ``http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress``

```
<?xml version="1.0" encoding="utf-8"?>
<EntityDescriptor ID="_bdf4eff3-677d-403c-a423-f1f87b0d2e0b"
entityID="https://sts.windows.net/667d9a8d-34fd-4ea9-99a5-b740e26edaac/"
```

```
<?xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<Signature
  xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <Reference URI="#_bdf4eff3-677d-403c-a423-f1f87b0d2e0b">
      <<Transforms>
        <<<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <<<<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <<<<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
              <<<<DigestValue>qVgiVoBjIPqfd5mkAsKdIHvBesKcG/jm3AbuvzSmX6M=</DigestValue>
            </Reference>
          </SignedInfo>
          <SignatureValue>o3HzUbjf88RoxzNEV6QNhh5jyw+vWtKRxSkqrsLORCH0w+P/DW9vG7sYnCjj66lVK7duHb07SBrI
+ hAeEXmqEkAW0bSd+dQzXhz3fG8JJ0GUaolxgz7J3K8vDkKFnboKR1XLa60YEPLuCh5ehfg3A8STeE0kp5ky+kVU0BBEkG
ZBKCNEX0cqZh2m6Wembu2C8xS4Ea/M2R64dn03/NKYkcxElvYYjS91HJoYc0MWhl2K6xHY8CCxFgqnHsnXHCNnucKZTp8
N4kiM4AxSWTaJw+Pwlh3vPgZNFuQuFhIvkAsLRW8kZzlan/CAYxZ5n3qoJhzjZM31u9gJgihyqSwyw==</SignatureVal
ue>
        <<<KeyInfo>
          <<<<ds:X509Data
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <<<<ds:X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFEMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMA
YDVQQDEylNaWNYb3NvZnQgXp1cmUgRmVhZG9wIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3
MTYxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRLcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBg
kqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEA7XgcoVwAoh3d4MuFkF61mf58inL9sAyCLEC6RhX+7ZiyT730dK9y+IwvpIU7
c1G0bmfQs51oJ5EdHv+GipDepg4zR8HRLJup9HnS10hMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk60Q0QpNbV0cw6W
0dv7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqwlSqE417aCFnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmwF
dV8/eSJm4PABqbkL0Uih3wMnpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLgtoJh6lFiyrl/Pd6uqLEcBli6vJPC1qo4Q
IDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDnPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSe0hlB3
TTevhAMxxPnlxx/u0i9RE2j6RMMTFS40omhwZ4+0Go02oV6YDPZPkyPvKdwTD6/TywZ0A8ZVThw0Uo04z9085Sub3rJvVQ
42cFR5RlKxRgiNvdZ5GVIZ6lZqQWPuq4Z35Iiq30F131dYWyIglL6aWgh3AjfkqHYFD0ufqK6ZzSZXmd1vthGgzmJGAUv3
B4K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9x0IS/zTscfLW+X/wloaD+PPMNSkpNh0b403</
ds:X509Certificate>
            <<<</ds:X509Data>
          <<<</KeyInfo>
        </Signature>
        <RoleDescriptor xsi:type="fed:SecurityTokenServiceType"
protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
<?xml:namespace prefix="fed" http://docs.oasis-open.org/ws-fed/federation/200706">
  <KeyDescriptor use="signing">
    <KeyInfo
      <?xml:namespace prefix="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFEMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMAYD
          VQQDEylNaWNYb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3MT
          YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRLcmF0ZWQgU1NPIENlcnpZmljYXRlMIIBIjANBgkq
          hkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6RhX+7ZiyT730dK9y+IwvpIU7c1
          G0bmfQs51oJ5EdHv+GipDepg4zR8HRLJup9HnSl0hMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk60Q0QpNbV0cw6W0d
          v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCFnTxuGS6b84YKBmLX7Jkr0a5EkH3JwHqokDMvWmWfDV
          8/eSJm4PABqbkL0Uih3WMNpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGoJh6lFiyrl/Pd6uqLEcBli6vJPC1qo4QID
          AQA0BMA0GCSqGSIb3DQEBwJAA4IBAQDnPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxxv1CtZVXtG/e8uqLAsjSe0h1B3TT
          evhAMxxPn1xx/u0i9RE2j6RMMTF540omhWZ4+0Go02oV6YDPZPkyPvKdwTD6/TywZ0A8ZVThw0Uo04z9085Sub3rJvVQ42
          cFR5RlKxRgiNvdZ5GVIz6lZqQWPuq4Z35Iiq30F131dYWyIglL6aWgh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUv3B4
          K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9x0IS/zTscfLW+X/wloaD+PPMNSkpNh0b403</X5
          09Certificate>
        </X509Data>
      </KeyInfo>
    </KeyDescriptor>
    <fed:ClaimTypesOffered>
      <auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
        <?xml:namespace prefix="http://docs.oasis-open.org/ws-fed/authorization/200706">
          <auth:DisplayName>Name</auth:DisplayName>
          <auth:Description>The mutable display name of the user.</auth:Description>
        </auth:ClaimType>
      <auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"
        <?xml:namespace prefix="http://docs.oasis-open.org/ws-fed/authorization/200706">
          <auth:DisplayName>Subject</auth:DisplayName>
          <auth:Description>An immutable, globally unique, non-reusable identifier of the user that is
          unique to the application for which a token is issued.</auth:Description>
        </auth:ClaimType>
      <auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
        <?xml:namespace prefix="http://docs.oasis-open.org/ws-fed/authorization/200706">
          <auth:DisplayName>Given Name</auth:DisplayName>
          <auth:Description>First name of the user.</auth:Description>
        </auth:ClaimType>
      <auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"
        <?xml:namespace prefix="http://docs.oasis-open.org/ws-fed/authorization/200706">
          <auth:DisplayName>Surname</auth:DisplayName>
          <auth:Description>Last name of the user.</auth:Description>
```

```
</auth: ClaimType>
<auth: ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
  <auth: DisplayName>Email</auth: DisplayName>
  <auth: Description>Email address of the user.</auth: Description>
</auth: ClaimType>
</fed: ClaimTypesOffered>
<fed: SecurityTokenServiceEndpoint>
  <wsa: EndpointReference
    xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsa: Address>https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-
b740e26edaac/wsfed</wsa: Address>
  </wsa: EndpointReference>
</fed: SecurityTokenServiceEndpoint>
<fed: PassiveRequestorEndpoint>
  <wsa: EndpointReference
    xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsa: Address>https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-
b740e26edaac/wsfed</wsa: Address>
  </wsa: EndpointReference>
</fed: PassiveRequestorEndpoint>
</RoleDescriptor>
<RoleDescriptor xsi:type="fed: ApplicationServiceType"
  protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706">
  <KeyDescriptor use="signing">
    <KeyInfo
      xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Data>
        <X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFEMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMAYD
VQQDEylNaWNYb3NvZnQgQXp1cmUgRmVhZG9wIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3MT
YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVYZSBGZWRLcmF0ZWQgU1NPIENlcnpZmljYXRlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6RhX+7ZiyT730dK9y+IwvpIU7c1
G0bmfQs51oJ5EdHv+GipDepg4zR8HRLJup9HnSl0hMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk60Q0QpNbvcw6W0d
v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCfnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmwFdV
8/eSJm4PABqbKLOUih3WMNpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGoJh6lFiyqL/Pd6uqLEcBli6vJPC1qo4QID
AQABMA0GCSqGSIb3DQEBcwJAA4IBAQNPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSe0hLB3TT
evhAMxxPn1xx/u0i9RE2j6RMMTFS40omhwZ4+0Go02oV6YDPZPKyPvKdwTD6/TywZ0A8ZVThwUo04z9085Sub3rJvVQ42
cFR5RlKxRgiNvdZ5GVIZ6LZqQWPuq4Z35Iiq30F131dYWyIglL6aWgh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUv3B4
K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9x0IS/zTscfLW+X/wloaD+PPMNSkpNh0b403</X5
```

```
09Certificate>
<X509Data>
</KeyInfo>
</KeyDescriptor>
<fed: TargetScopes>
<wsa: EndpointReference
  xmlns: wsa="http://www.w3.org/2005/08/addressing">
  <wsa: Address>https://sts.windows.net/667d9a8d-34fd-4ea9-99a5-b740e26edaac/</wsa: Address>
</wsa: EndpointReference>
</fed: TargetScopes>
<fed: ApplicationServiceEndpoint>
  <wsa: EndpointReference
    xmlns: wsa="http://www.w3.org/2005/08/addressing">
    <wsa: Address>https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/wsFed</wsa: Address>
  </wsa: EndpointReference>
</fed: ApplicationServiceEndpoint>
<fed: PassiveRequestorEndpoint>
  <wsa: EndpointReference
    xmlns: wsa="http://www.w3.org/2005/08/addressing">
    <wsa: Address>https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/wsFed</wsa: Address>
  </wsa: EndpointReference>
</fed: PassiveRequestorEndpoint>
</RoleDescriptor>
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <KeyDescriptor use="signing">
    <KeyInfo
      xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Data>
        <X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFEMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMAYD
VQQDEylNaWNYb3NvZnQgXp1cmUgRmVhZG9kIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MjYxMzQ0MjhaFw0yNDA3MT
YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWwlcF0ZWQgU1NPIENlcnpZmljYXRlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6RhX+7ZiyT730dK9y+IwvpIU7c1
G0bmfQs51oJ5EdHv+GipDepg4zR8HRLJup9HnSl0hMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk60Q0QpNbvcw6W0d
v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqW1SqE417aCFnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmwFdV
8/eSJm4PABqbKLOUih3wMnpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLgtoJh6lFiyqL/Pd6uqLEcBli6vJPC1qo4QID
AQABMA0GCSqGSIb3DQEBwJAA4IBAQNPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSe0hLB3TT
evhAMxxPn1xx/u0i9RE2j6RMMTFS40omhwZ4+0Go02oV6YDPZPKyPvKdwTD6/TywZ0A8ZVThw0Uo04z9085Sub3rJvVQ42
cFR5RlKxRgiNvdZ5GVIZ6LZqQWPuq4Z35Iiq30F131dYWyIglL6aWgh3AjfkqHYFD0ufqK6ZzSZXmd1vthGgzmJGAUv3B4
K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9x0IS/zTscfLW+X/wload+PPMNSkpNh0b403</X5
```

```
09Certificate>
<<<</X509Data>
<<<</KeyInfo>
<<<</KeyDescriptor>
<<<<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/saml2" />
<<<<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/saml2" />
<<<<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/saml2" />
<<<</IDPSSODescriptor>
</EntityDescriptor>
```

Revision #1

Created 17 May 2024 07:57:35 by Daniel Jianoran

Updated 12 June 2024 08:12:39 by Daniel Jianoran