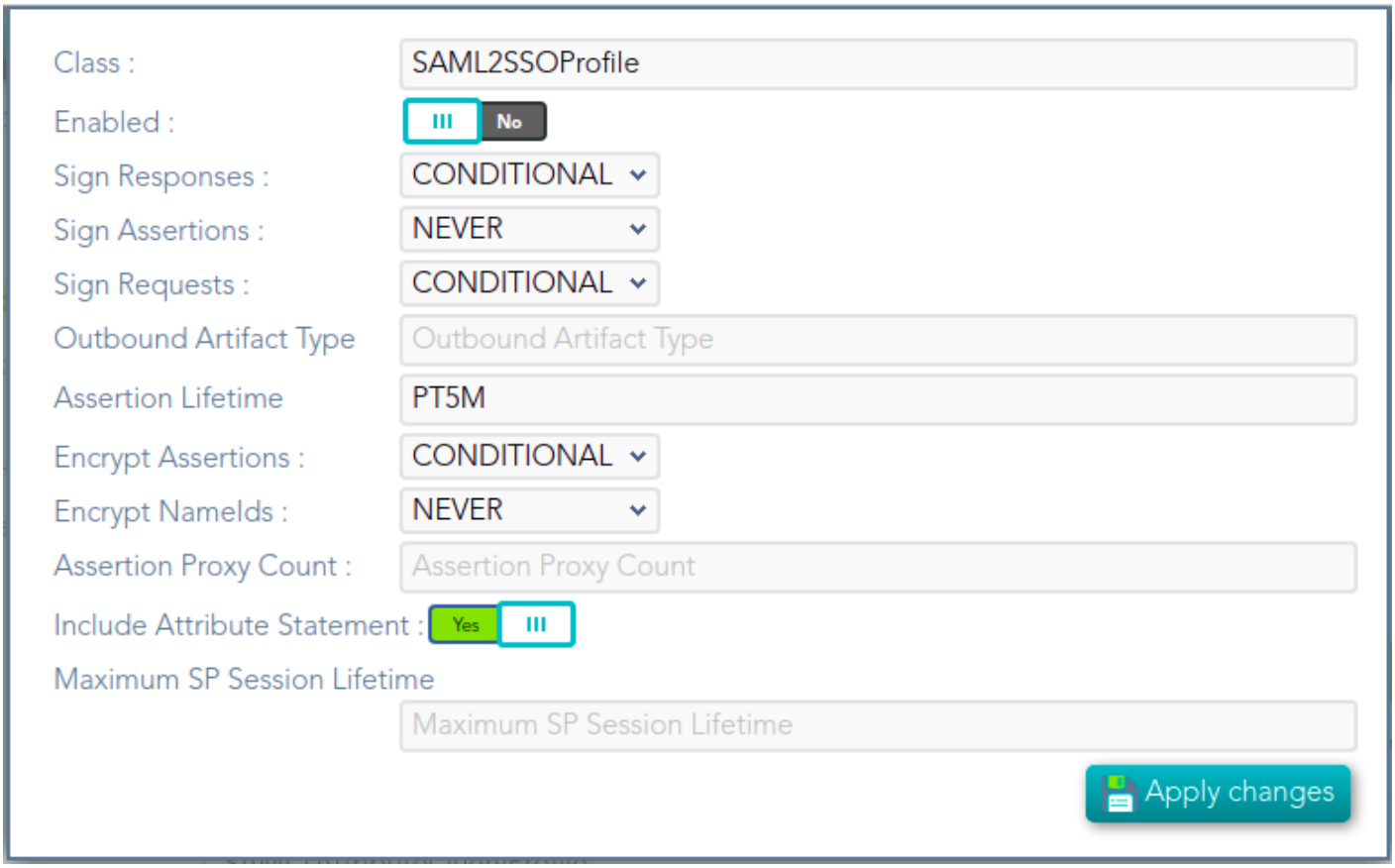
SAML2SSOProfile

Definition

This is the most commonly used SAML profile. It allows the IdP to identify users and to give such information to Service Providers. This profile is used to log in.

When you are configuring the profile, you could define what data will be encrypted and signed.

Screen overview



Standard attributes

- **Class**: class name (readOnly field).
- **Enabled**: if it is checked (selected option is Yes) that protocol will be enabled.
- **Sign Responses**: usually it can be set to never, as long as the assertions are signed. Its preferable to sign assertions rather than responses, because the assertion can be forwarded by the service provider to another service provider, but the response not.
- **Sign Assertions**: it's advisable to sign every assertion, so it avoids assertion spoofing. The assertion can be forwarded by the service provider to another service provider.
- **Sign Request**: the identity provider will issue requests to service providers in order to perform the single logout process. Unless it is needed by any service provider, leave it to conditional.
- **Outbound Artifact Type**: usually kept in blank, unless you are using old SAML 1 service.
- **Encrypt Assertions**: is a desired feature, but some service providers, mainly public cloud service providers do not support it. Thus, the default value is to never encrypt, but you can set it to optional or always as needed.
  - If you set it to optional and the public key of the service provider who is going to receive the assertion is available, it will be used to encrypt it.
  - If you set it to never, it will not ever be encrypted in any case.
  - If you set it to always, but the remote service provider encryption key is unknown, an exception will be raised.
- **Encrypt NameIds**: should be let to never.
- **Assertion Proxy Count**: sets the maximum number of hops that can be accepted for any assertion. A number of 0 does not set any limit
- **Include Attribute Statement**:
  - If the attribute statements are included (selected value is Yes), that is the user attributes are included on the response the performance is increased as this additional step is no longer needed. It is particularly recommended when using public cloud service providers.
  - If attribute statements are not included (selected value is No), the service provider will receive the SAML assertion with the principal name, then the service provider will issue a attribute statement request to the service provider to get them.

Revision #13
Created 14 September 2021 11:11:48
Updated 15 July 2022 08:26:53