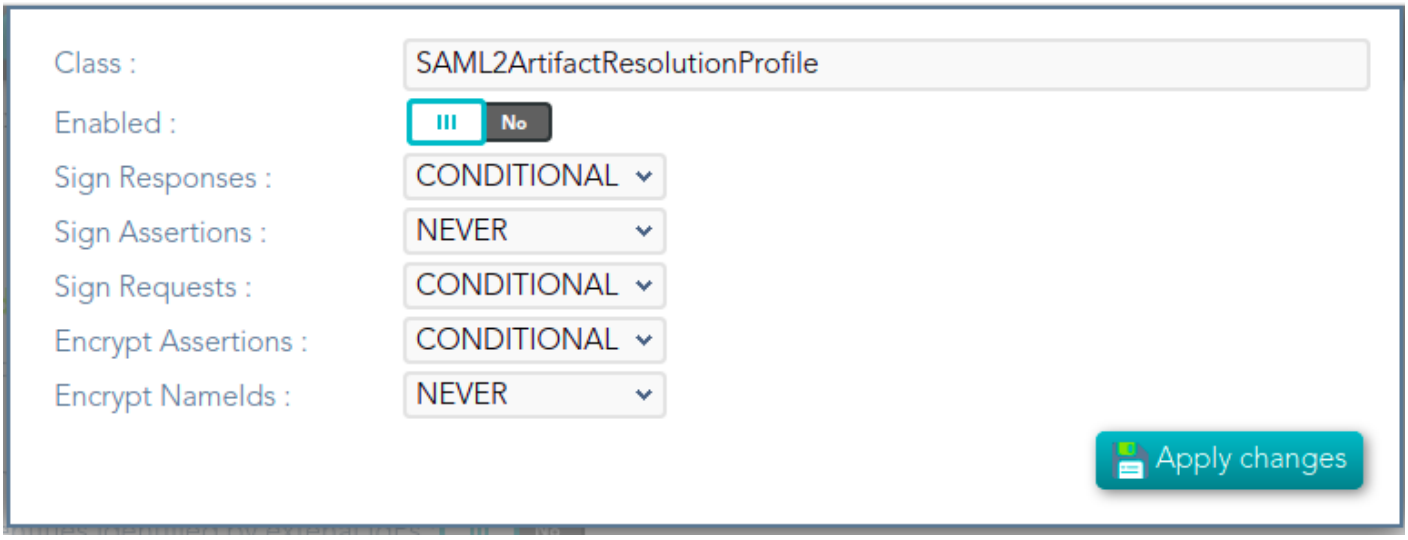
SAML2ArtifactResolutionProfile

Definition

Based on SAML version 1 standard. This profile is used when the Service Provider wants to resolve or check a received assertion. The profile configuration settings are quite similar to those present in SAML2SSOProfile.

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 enable.
- **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.
- **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.

Revision #11
Created 14 September 2021 11:11:10
Updated 15 July 2022 08:42:44