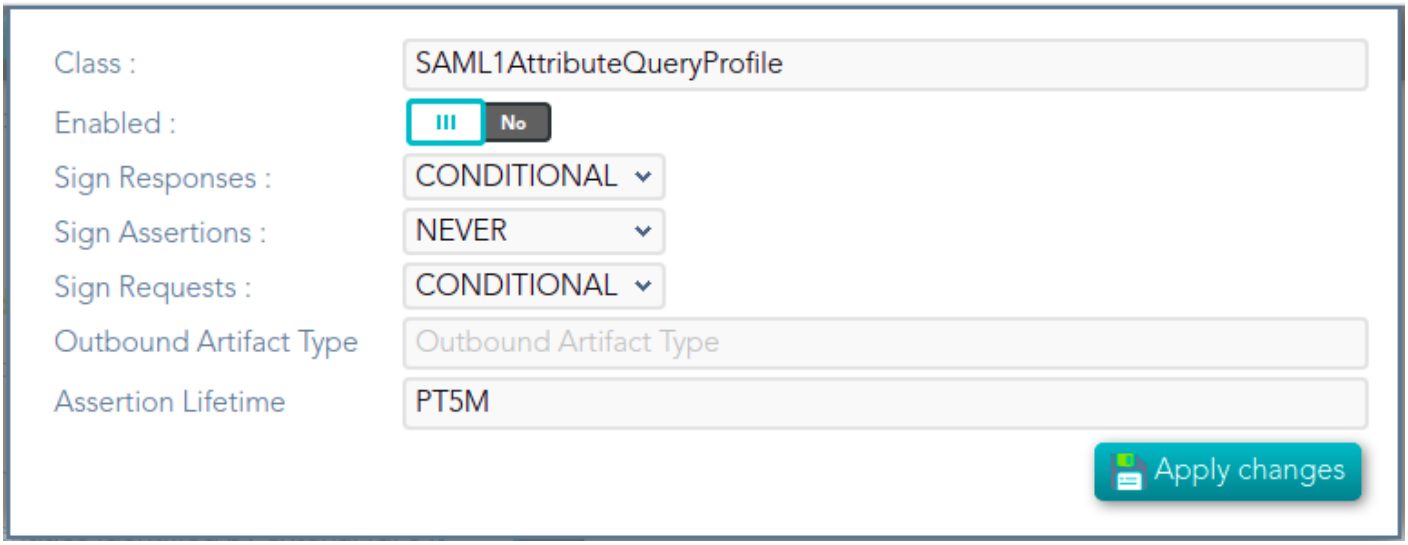
SAML1AttributeQueryProfile

Definition

Based on SAML version 1 standard. This profile is used when the SSOProfile does not include attributes statements in the assertion. This profile allows to the applications request user data.

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.
- **Outbound Artifact Type**: defaults to 4. Any other value is not supported. For more information, see SAML specification.
- **Assertion Lifetime**: specifies the validity period for the generated assertions . The time period is specified using the ISO 8601 notation. The standard format follows the pattern: PnYnMnDTnHnMnS.

Assertion Lifetime examples:

- PT5M sets a duration of five minutes.
- PT1H30M sets a duration of one hour and a half.
- P3Y6M4DT12H30M5S" sets a duration of three years, six months, four days, twelve hours, thirty minutes, and five seconds.

---

https://en.wikipedia.org/wiki/ISO_8601

http://saml.xml.org/saml-specifications

Revision #12
Created 14 September 2021 11:10:56
Updated 15 July 2022 08:43:07