Profiles

Profiles

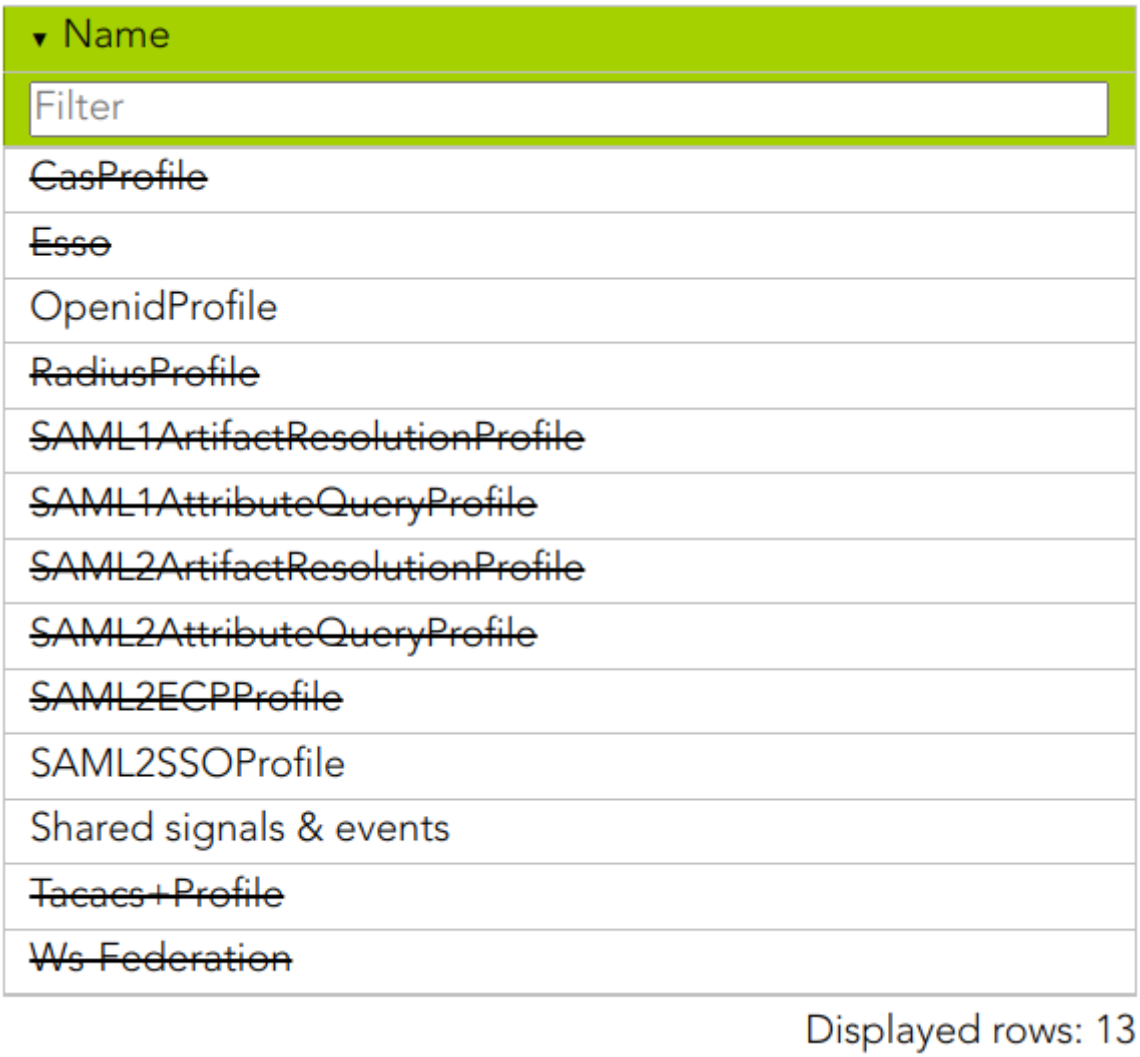
Description

> A profile is a protocol or subset of protocols implemented by the Identity Provider. There are some accepted protocols, those allows a custom config dependent on the selected profile.

The accepted protocols are the following:

1. OpenIDProfile
2. SAML1ArtifactResolutionProfile
3. SAML1AttributeQueryProfile
4. SAML2ArtifactResolutionProfile
5. SAML2AttributeQueryProfile
6. SAML2ECPProfile
7. SAML2SSOProfile
8. CAS
9. Radius
10. Tacacs+
11. Ws-Federation
12. Shared signals & events
13. Esso

Screen overview



When an identity provider is created, by default, all the profiles appear disabled (the profile is displayed strikethrough). It will be necessary to config one by one depending on your company needs. To config a profile you must click on the proper profile, and Soffid will display a new window to config it.

Actions

Open profile	If you click on a row of the profile list, Soffid will display a modal window with the data and configuration of the profile selected.

OpenIDProfile

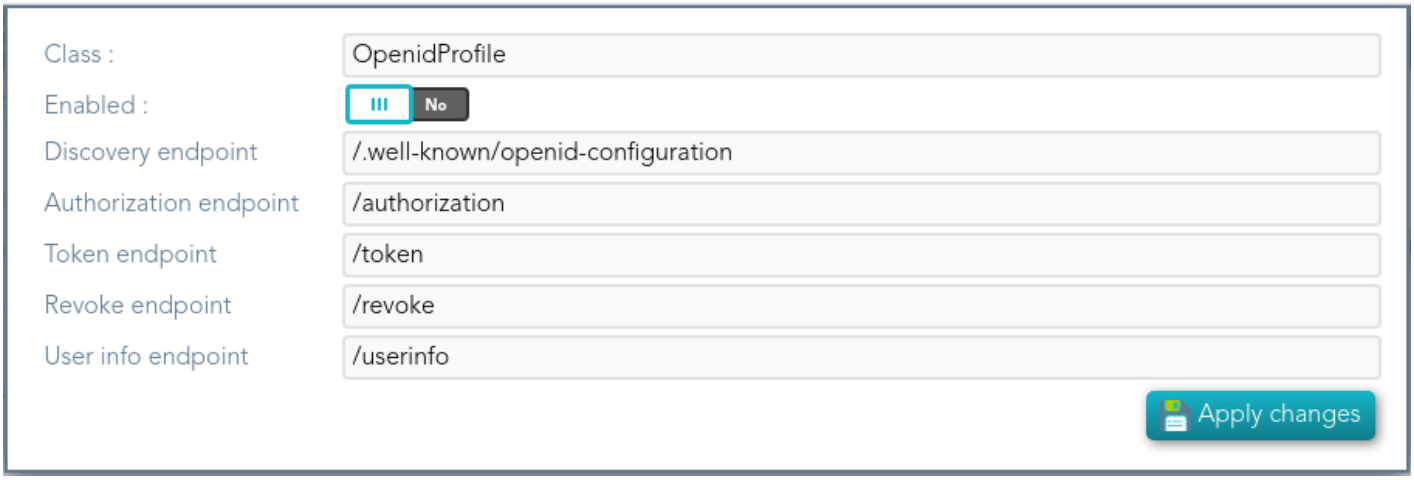
Definition

The Identity Provider will serve the OpenID-Connect protocol. It is possible to accept the default endpoints or modify them.

You can check the server features visiting https://<YOUR-IdP>/.well-known/openid-configuration. That JSON gives you information about the oAuth authentication types allowed, the key URL, the soported authentication methods and the info about the endpoints defined.

> You can download an example openid-configuration.json

Screen overview



Standard attributes

- **Class**: class name (readOnly field).
- **Enabled**: if it is checked (selected option is Yes) that protocol will be enable.
- **Discovery endpoint**: call this endpoint to request the OpenID-Connect provider metadata.
- **Authorization endpoint**: call this endpoint to request or authorization grant.

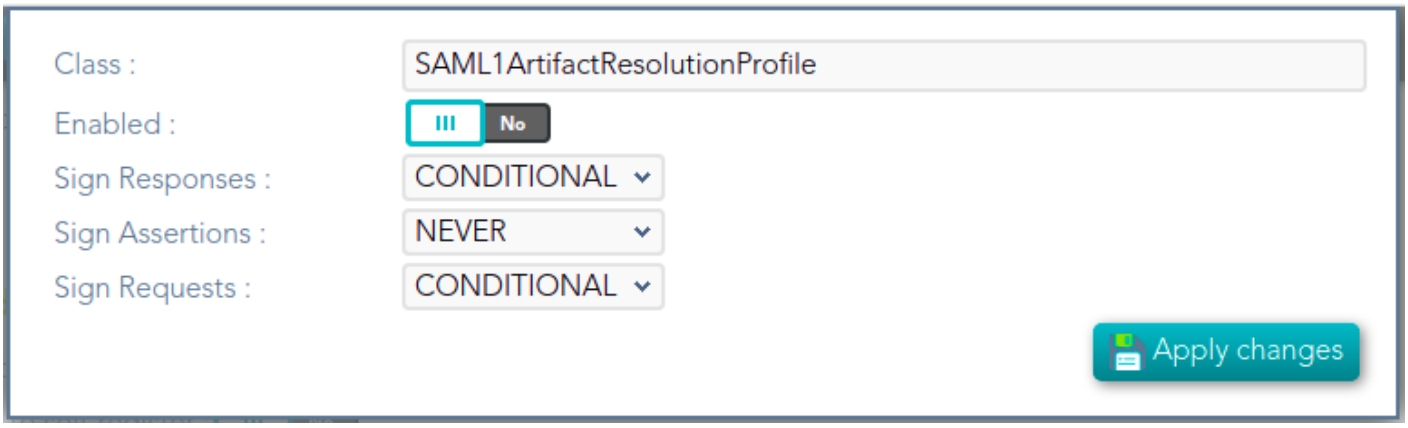
- **Token endpoint**: call this endpoint to get the token or to renew the token.
- **Revoke endpoint:** call this endpoint when you finish and do not need more use the token.
- **User info endpoint**: call this endpoint to request user information.

SAML1ArtifactResolutionProfile

Definition

Based on SAML version 1 standard. This profile is used when the Service Provider wants to resolve or check a received assertion.

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.

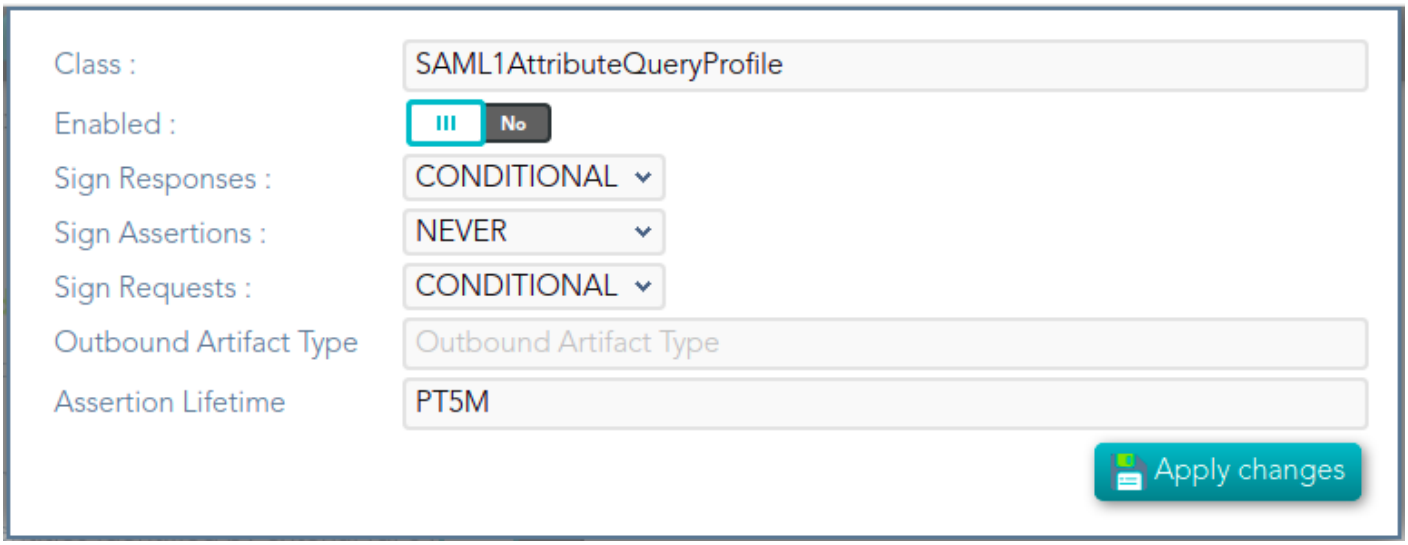
SAML1AttributeQueryProfile

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

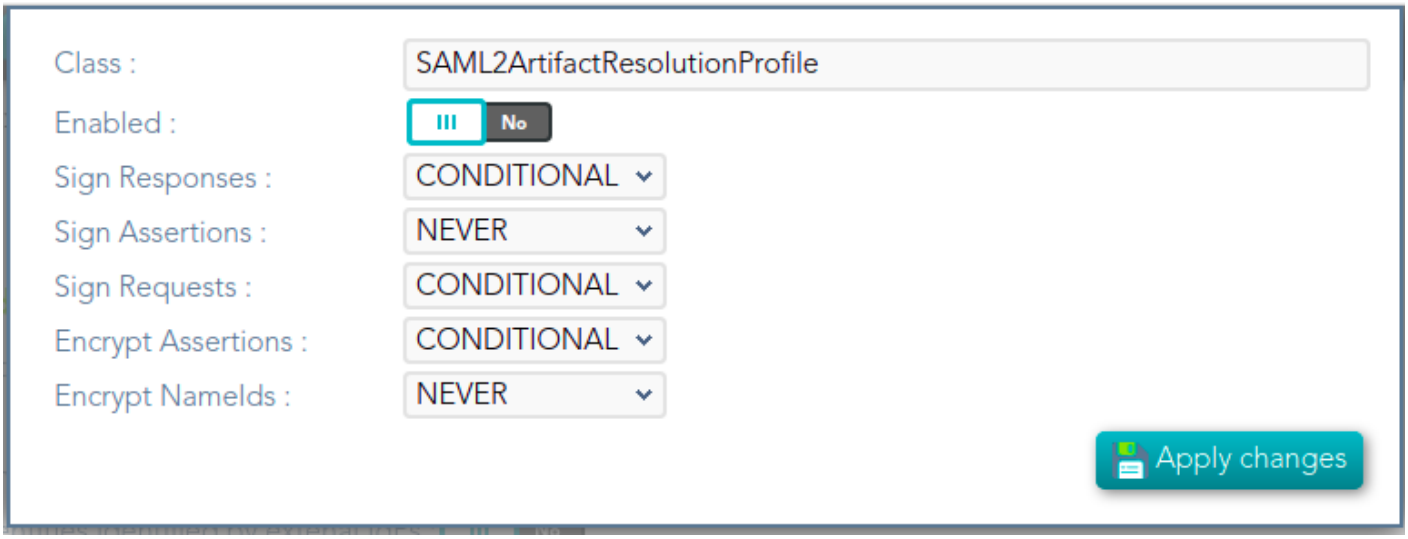
SAML2ArtifactResolutionProfile

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.

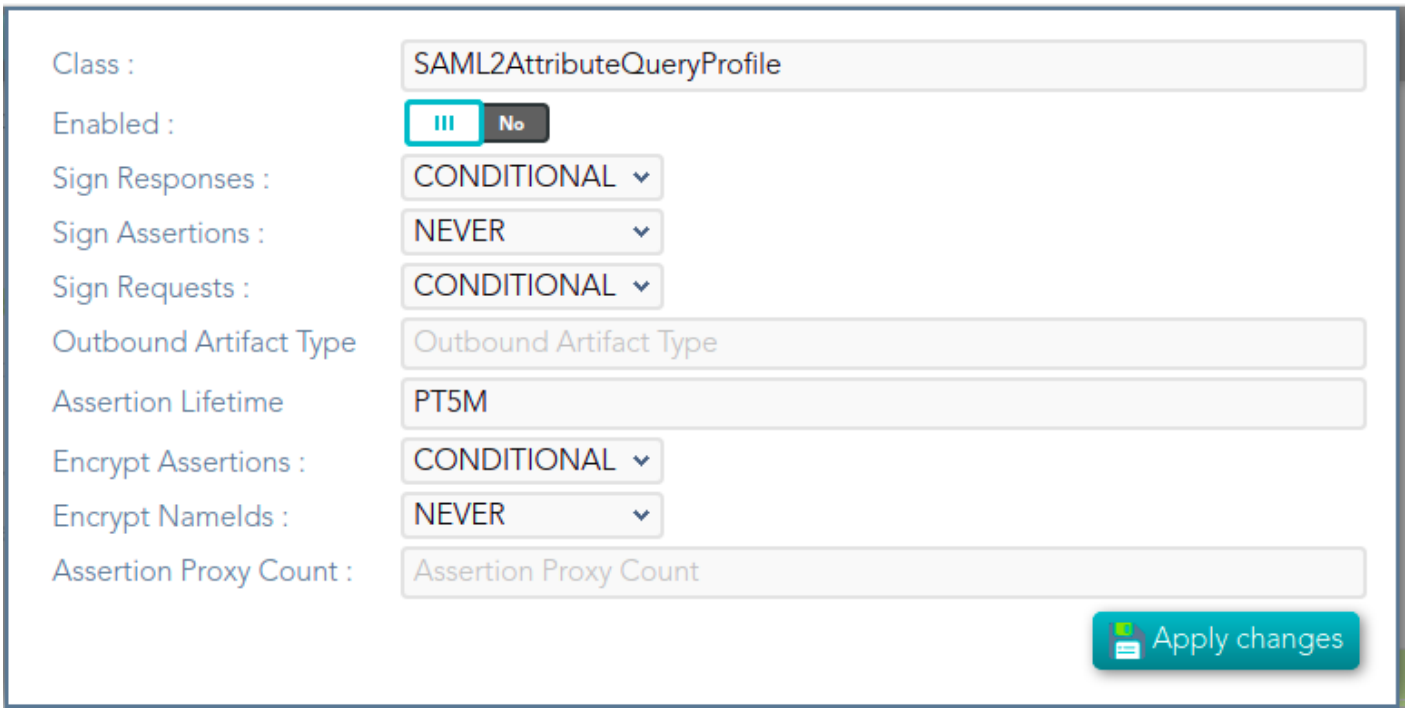
SAML2AttributeQueryProfile

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 is set to conditional or always, so as the service provider can verify the response authenticity.
- **Sign Assertions**: is usually set to never, as long as the response is already signed.

- **Sign Request**: not used, as the service provider will not need to generate requests.
- **Outbound Artifact Type:** usually kept in blank, unless you are using old SAML 1 service.
- **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. This means that PT5M sets a duration of five minutes. For instance, PT1H30M sets a duration of one hour and a half.
- **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.

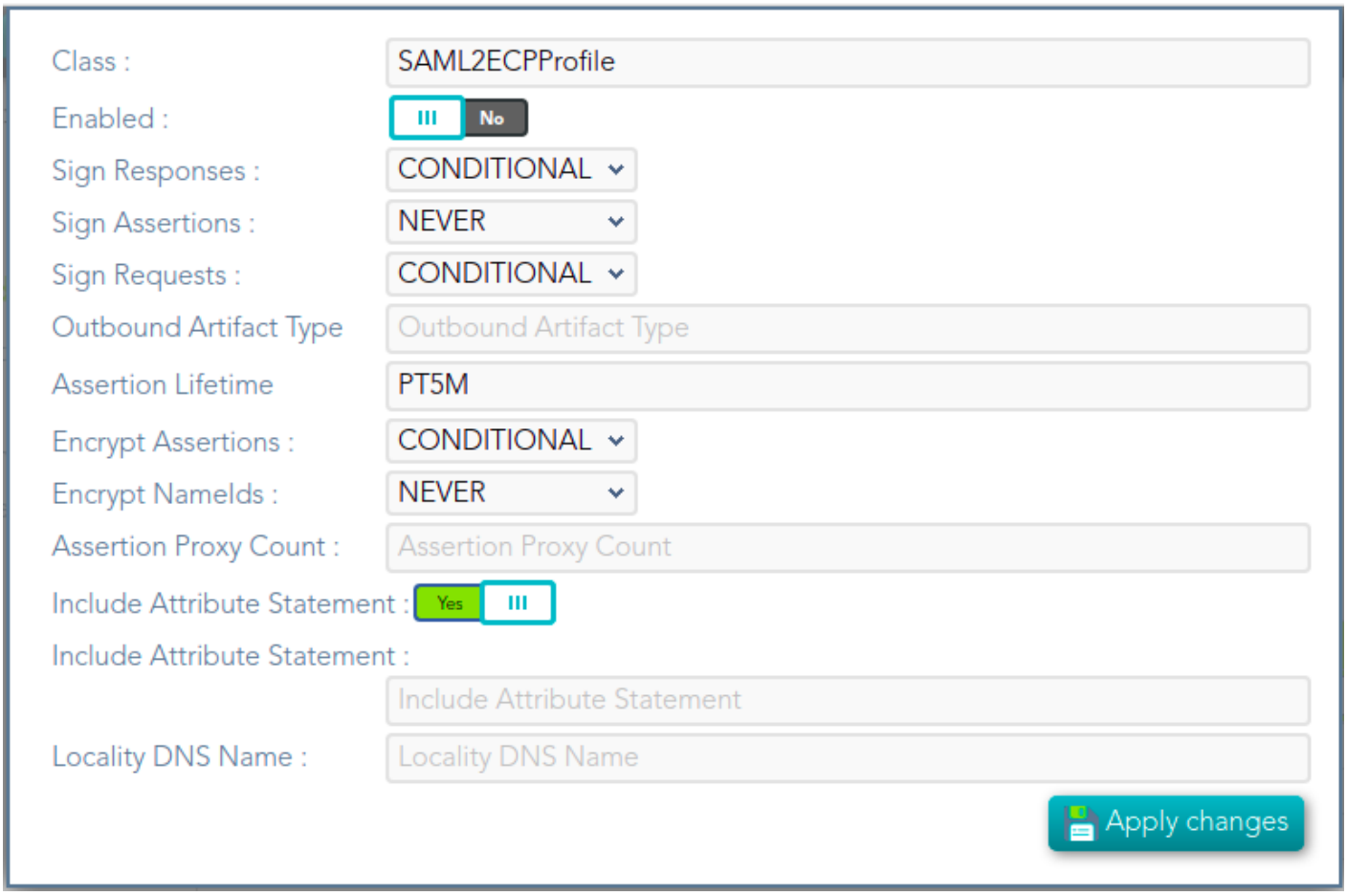
SAML2ECPProfile

Definition

The Enhanced Client Profile is used when the Service Provider is not a web application. Nowadays, it is rarely used, as most mobile applications have shifted to OAuth or OpenIDConnect.

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.
- **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.
- **Locality DNS Name**

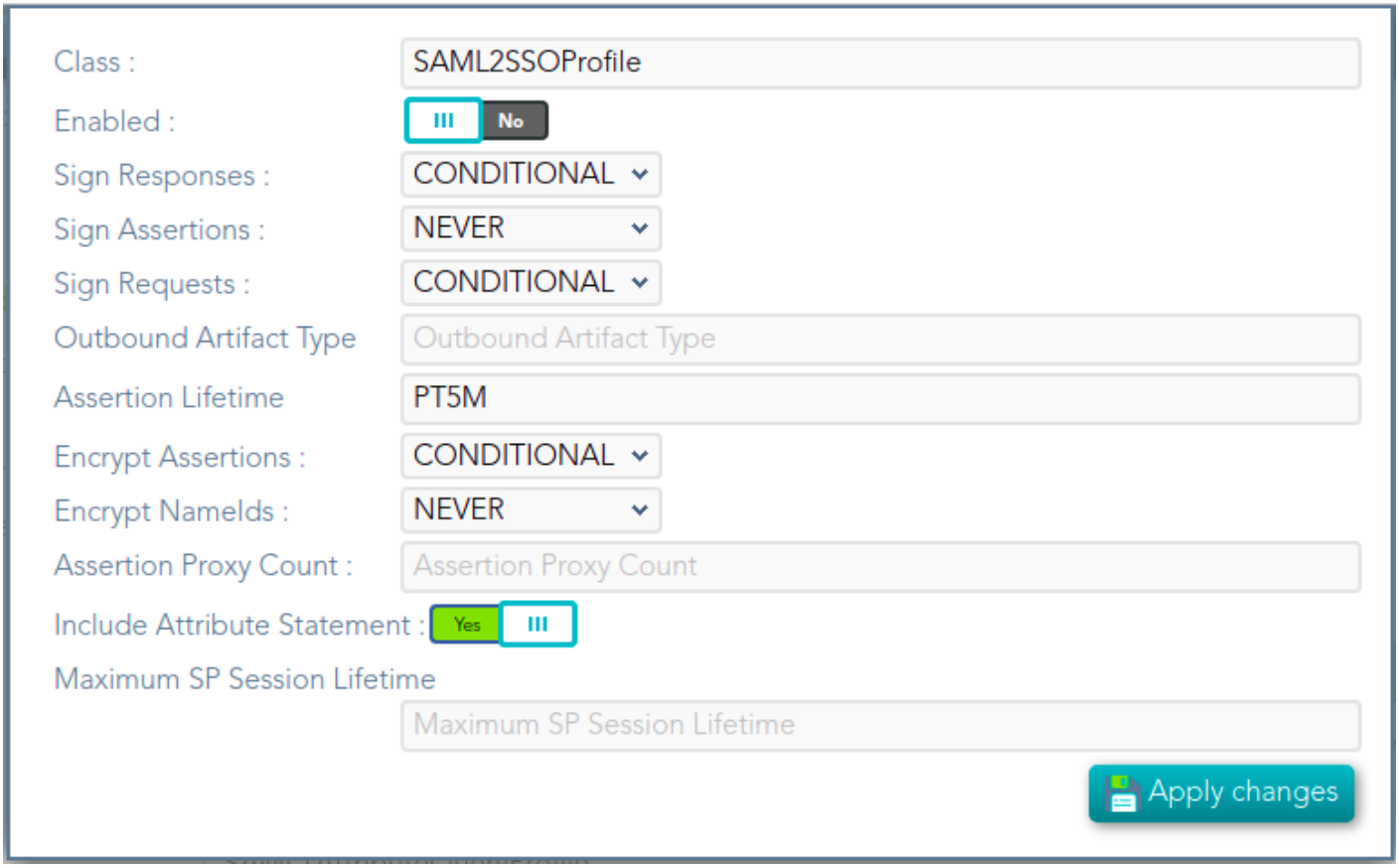
SAML2SSOProfile

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.

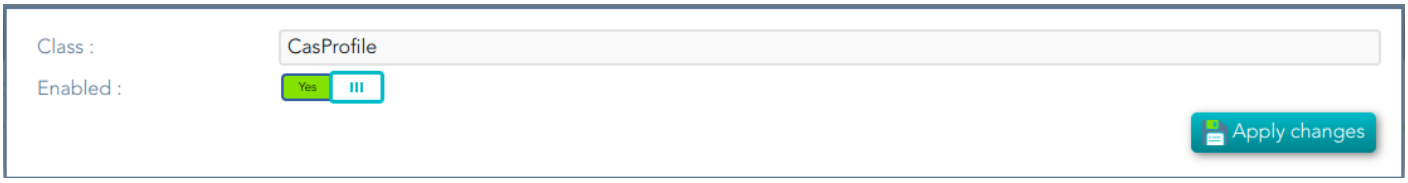
- **Sign Responses**: usually it can be set to never, as long as the assertions are signed. Its preferable to sign assertions rather than responses, because the assertion can be forwarded by the service provider to another service provider, but the response not.
- **Sign Assertions**: it's advisable 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.

CAS

Definition

Cas protocol is rarely used.

Screen overview



Standard attributes

- **Class**: class name (readOnly field).
- **Enabled**: if it is checked (the selected option is Yes) that protocol will be enabled.

Radius

Definition

Networking protocol that authorizes and authenticates users who access a remote network.

Screen overview

Standard attributes

- **Class**: class name (readOnly field).
- **Enabled**: if it is checked (selected option is Yes) that protocol will be enabled.
- **Authentication port**: UDP authentication port. This port is used to log in.
- **Accounting port**: UDP authentication port. This port is used to manage the session, when the session starts and when finishes.
- **Enable PAP (unsecure)**: authentication protocol. The password to send is unencrypted.
- **Enable CHAP**: authentication protocol. The password to send is encrypted.
- **Enable MS CHAP v2**: authentication protocol.

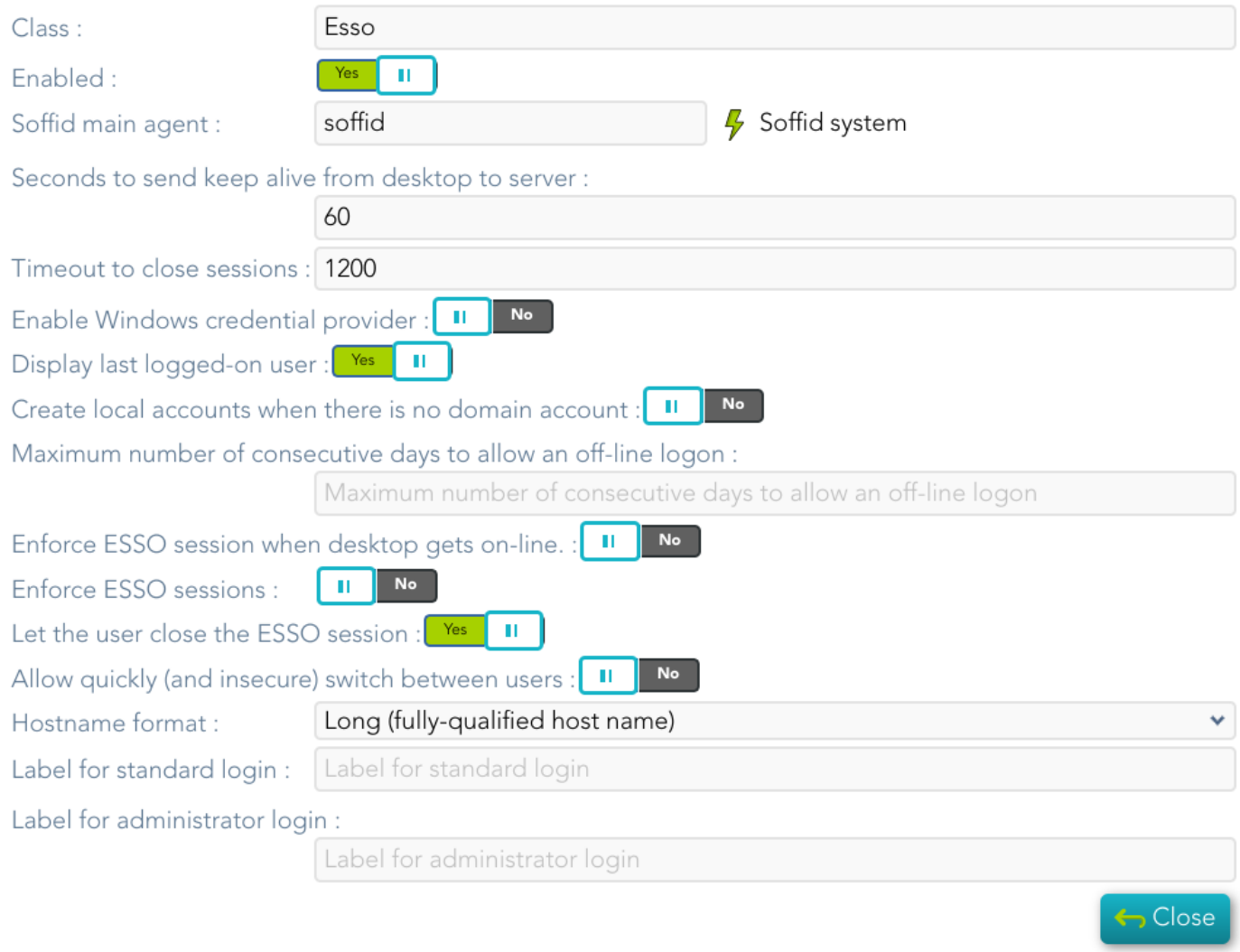
ESSO

Definition

Here is an explanation about how to configure the ESSO profile by using Soffid as Identity Provider.

> Please note that the profile parameters will be automatically updated on the PCs.

Screen overview



Standard attributes

- **Class**: class name (readOnly field).
- **Enabled**: if it is checked (selected option is Yes) that protocol will be enabled.
- **Soffid main agent**: main agent to check the user account.
- **Seconds to send keep alive from desktop to server**:
- **Timeout to close sessions**:
- **Enable Windows credential provider**: if it is checked (selected option is Yes), the soffid logo will be displayed.
- **Display last logged-on user**: if it is checked (selected option is Yes), the last logged-on user will be displayed.
- **Create local accounts when there is no domain account**: if checked (the selected option is Yes) and the account does not exist in the main Soffid agent, the account is created as a local machine user.
- **Let user login as a shared account:** PAM Desktop
- **Maximum number of consecutive days to allow an off-line logon**: the maximum value is 30 days.
- **Enforce ESSO session when desktop gets on-line**: if it is checked (selected option is Yes), the authentication is forced when the connection is retrieved
- **Enforce ESSO sessions**: if it is checked (selected option is Yes), performs authentication against the Windows domain without logging into Soffid.
- **Let the user close the ESSO session**: allow the user to log out from ESSO
- **Allow quickly (and insecure) switch between users**: if it is checked (selected option is Yes),
- **Hostname format**
- **Label for standard login**: label to be displayed for standard user in Windows desktop.
- **Label for administrator login**: label to be displayed for adminsitrator user in Windows desktop.

Configuration

Once you have configured the Esso profile you must add an Adaptive authentication rule.

> For more information, visit the Condition for Adaptive authentication page.

Adaptive authentication

Description : Esso

Condition : isEsso

Always ask for credentials : No

First autl	Passwor	Kerberos	External	OTP	Email	SMS	PIN	Certifica	FIDO	Push
Passworc	☐	☐	☐	☑	☐	☐	☐	☐	☐	☑
Kerberos		☐	☐	☐	☐	☐	☐	☐	☐	☐
External			☐	☐	☐	☐	☐	☐	☐	☐
OTP				☐	☐	☐	☐	☐	☐	☐
Email					☐	☐	☐	☐	☐	☐
SMS						☐	☐	☐	☐	☐
PIN							☐	☐	☐	☐
Certificat								☐	☐	☐
FIDO									☐	☐
Push										☐

Close