VERSION V1.01

CoreLogic®

SSO Configuration

OPENID Connect/SAML 2.0

October 2022

Contents

1. SSO Options

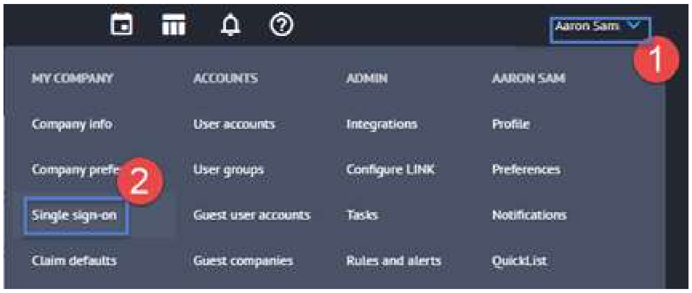
1. Claims Connect offers two ways in which a client can utilise Single Sign-on (SSO).
   - OpenID Connect
   - SAML2.0

2. Companies that wish to use SSO need to contact their Client Success Manager and or Project Manager who can activate the setting for an environment. Activating SSO does not automatically mean the company now uses SSO. It simply allows an Administrator to configure the endpoints and security details that will take the user through the SSO process.

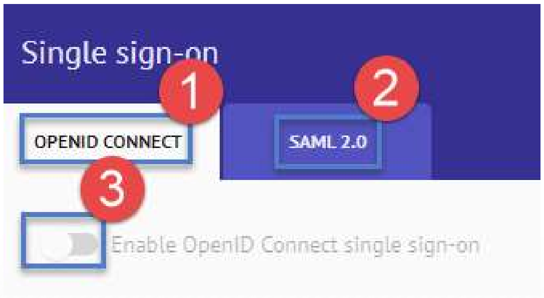
2. Configuring SSO

1. Single sign-on must enabled by Claims Connect support.

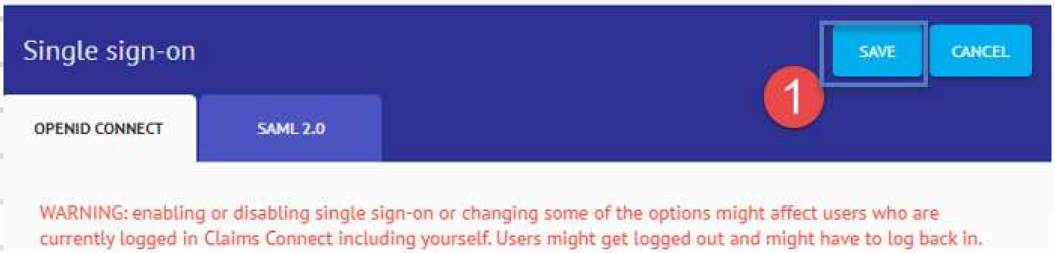
2. Under the main menu a new option will appear for Administrators to access the Single Sign-on blade. Click on the drop down next to your name **(1)**, and click on Single sign-on **(2)**.



3. Here the user will have the option to configure either the settings for OpenID Connect **(1)** or SAML2.0 **(2)**. To allow a user to update the configuration fields move the ‘slider’ to enable SSO **(3)**. For the available options see **Section 4. Appendix.**



4. Once the details have been entered into the data fields click **Save (1)**.



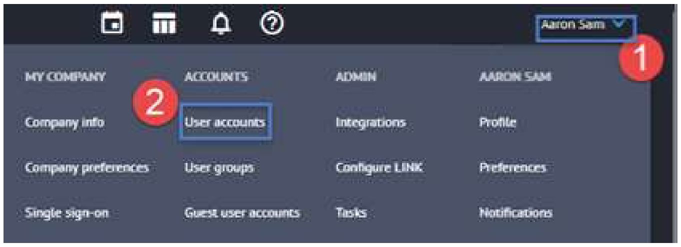
WARNING: enabling or disabling single sign-on or changing some of the options might affect users who are currently logged in Claims Connect including yourself. Users might get logged out and might have to log back in.

5. It is important to note that although the SSO options have been entered and saved, unless a Claims Connect user account is linked to an SSO Identifier then users will still log into Claims Connect using the traditional username/password method.

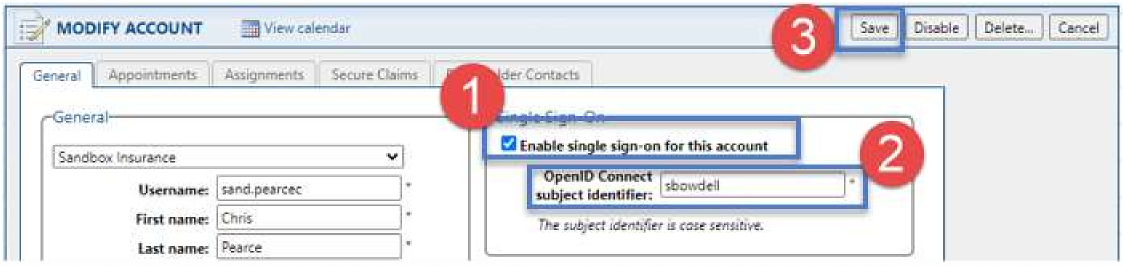
6. Also, where users are already logged into Claims Connect via SSO any changes to this screen may be logged out and have to log back in.

3. User Configuration

1. The final piece of configuration is to link a Claims Connect user account to enable a SSO for a user and enter an SSO Subject Identifier. This can be achieved via the 'User Accounts' option via the main menu. Click on the drop down next to your name (1), then click on User accounts (2).



2. Click on the username from the list provided. A new option will appear when viewing a user's account details. Simply check the box for **Enable single sign-on for this account (1)**, and enter in the **SSO Subject Identifier (2**). Click **Save (3)** and the user will now log into Claims Connect and Mobile Claims via the configured SSO URL Endpoints.



General

Sandbox Insurance

Username: sand.pearcec *

First name: Chris *

Last name: Pearce *

Single Sign-On

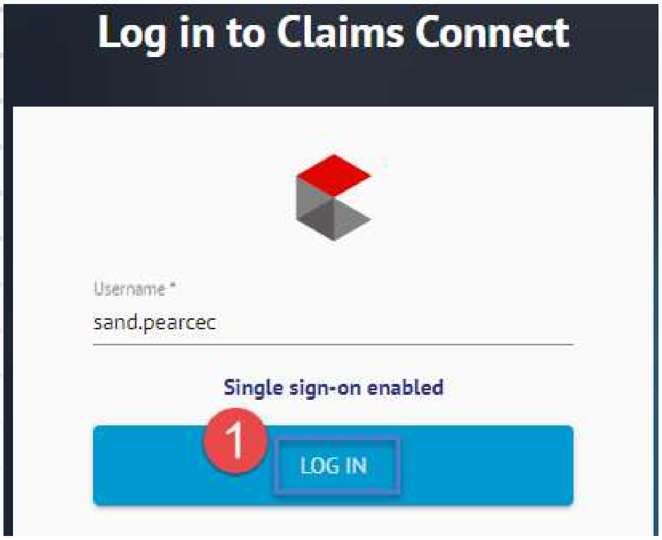
☑ Enable single sign-on for this account

OpenID Connect subject identifier: sbowdell *

The subject identifier is case sensitive.

3. When the user enters their username into Claims Connect or Mobile Claims the password option will disappear.

4. Selecting Log In (1) will take the user to the SSO URL Endpoint where they will enter their username (the one entered in the subject identifier) and the password that corresponds to that account.



Log in to Claims Connect

Username *

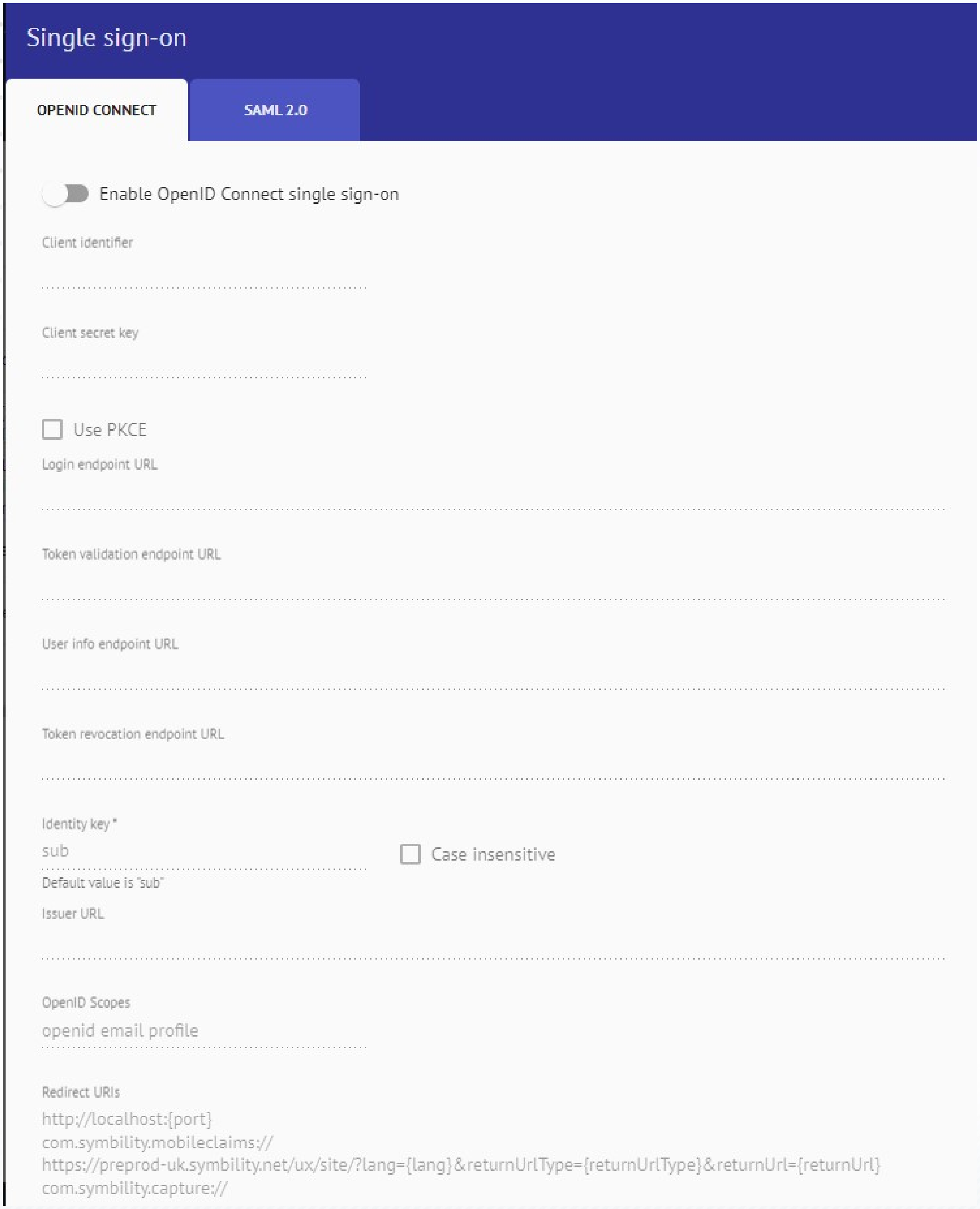
sand.pearcec

Single sign-on enabled

5. Please note that for Mobile Claims, the user must be connected to the internet the first time they attempt to log in with SSO. This is to ensure that the user can authenticate with the clients SSO URL Endpoint. To enable users to continue to use Mobile Claims offline, there is an option to setup an ‘Offline Mode’. Users will be continually reminded of this when they log in and have not set this up. We recommended using a time-based, one-time password (TOTP) such as Google Authenticator.

4. OPENID Connect

OpenID Connect Configuration Options



Single sign-on

OPENID CONNECT

SAML 2.0

Enable OpenID Connect single sign-on

Client identifier

Client secret key

□ Use PKCE

Login endpoint URL

Token validation endpoint URL

User info endpoint URL

Token revocation endpoint URL

Identity key *

sub

□ Case insensitive

Default value is "sub"

Issuer URL

OpenID Scopes

openid email profile

Redirect URIs

http://localhost:{port}
com.symbility.mobileclaims://
https://preprod-uk.symbility.net/ux/site/?lang={lang}&returnUrlType={returnUrlType}&returnUrl={returnUrl}
com.symbility.capture://

4.1.1. [Client Identifier]

- This is a Mandatory field.
- This is a field that will need to be filled by the client. This field is used much like a username. This is how CoreLogic should identify itself with your SSO system.

4.1.2. [Client Secret key]

- This is a Mandatory field.
- This is a field that is coupled with [Client Identifier]. This field is used as a password. This is how CoreLogic should authenticate itself with your SSO system.

4.1.3. [Use PKCE]

- This is an optional additional security feature to the OpenID Connect workflow CoreLogic and your SSO system will use to communicate. The workflow we rely on (Authorization Code exchanged server-side system-to-system) does not benefit much from this option, but some systems require it.

4.1.4. [Login endpoint URL]

- This is a Mandatory field.
- This is the URL that the user will be redirected to confirm his username, when he tries to login into CoreLogic.

4.1.5. [Token validation endpoint URL]

- This is a Mandatory field.
- This is the URL that the CoreLogic servers will contact in order to complete the system-to-system part of the authentication.

4.1.6. [User info endpoint URL]

- This is the URL that CoreLogic servers will contact to fetch additional information to link CoreLogic User attributes to specific attributes to your system. The CoreLogic system can use that information to update its own Users information.

4.1.7. [Token revocation endpoint URL]

- This is the URL that CoreLogic servers will contact in order to let your SSO system know the user has disconnected from CoreLogic.

4.1.8. [identity key]

- This is a Mandatory field.
- This the name of the Attribute sent by your SSO System that will be used to link a User in your SSO system to a CoreLogic User.
- Note that the value matched with this attribute is configurable by for each CoreLogic user independently to match your SSO system. If the value stored in that Attribute should be matched to CoreLogic's systems while ignoring the Case, then the "Case insensitive" checkbox can be used for that.

4.1.9. [Issuer URL]

- This is the name of the SSO system that will be used to identify itself to CoreLogic's system.

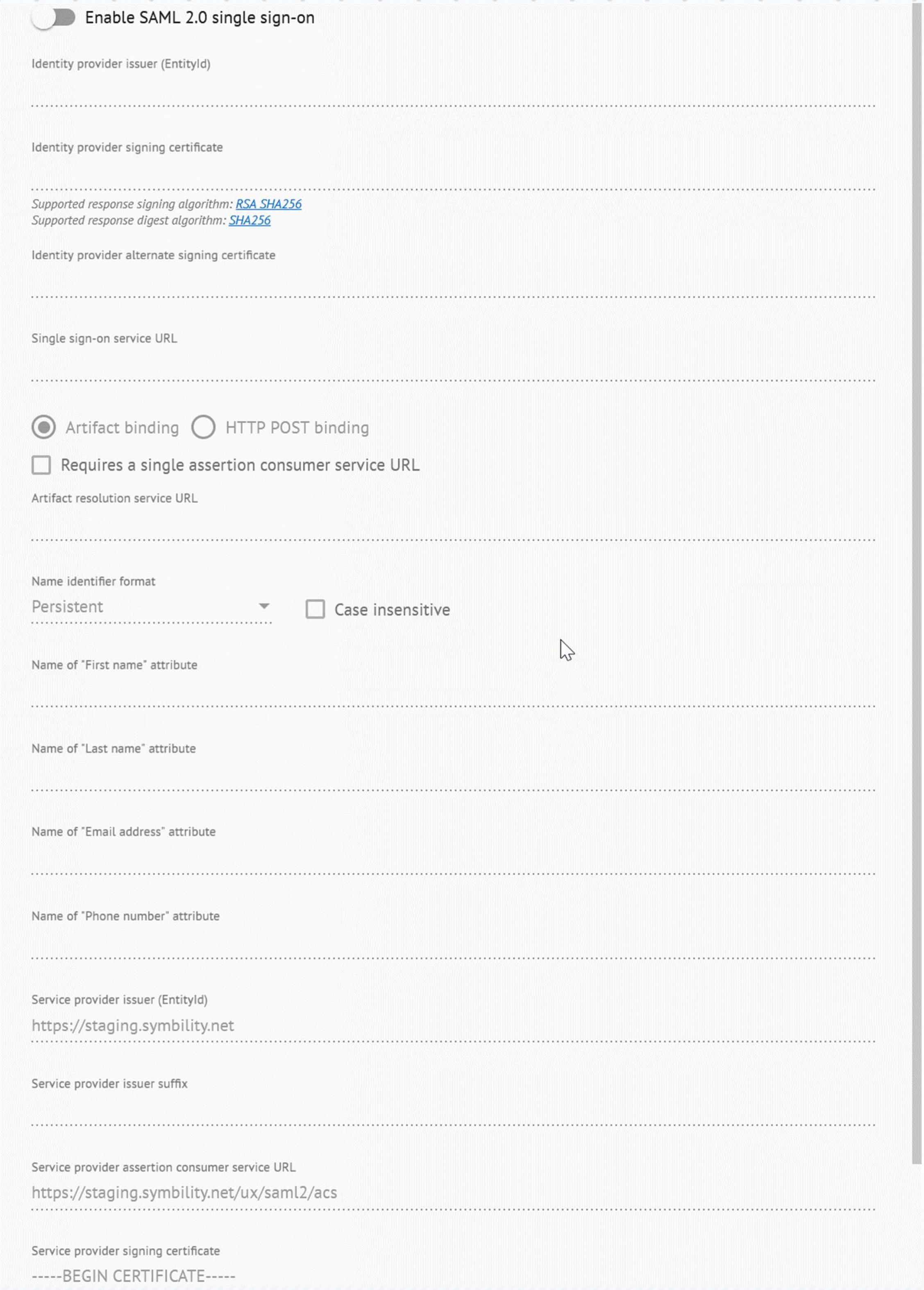
4.1.10. [OpenID Scopes]

- This field cannot be modified by client.
- This is the set of authorizations or information CoreLogic will require when a user tries to login. These only include Login authorization and Profile (User information to update the CoreLogic system).

4.1.11. [Redirect URIs]

- This field cannot be modified by client.
- These fields need to be provided to your IT team.
- These are the URLs your SSO system needs to redirect users to once they have been authenticated. CoreLogic will tell your SSO system which URL it needs the user to be redirected to, but it will always be one of these. Any URL not in this list can be rejected by your SSO system.
- *Note: The parts like {this} in these URLs can be replaced by other strings depending on the exact context and CoreLogic system the user is trying to login to: {port} can be replaced by any numerical value and the others can be replaced by any text not including # or &. Your IT team should take that into consideration during their configuration of your SSO system.*

5. SAML 2.0



Enable SAML 2.0 single sign-on

Identity provider issuer (EntityId)

Identity provider signing certificate

Supported response signing algorithm: RSA SHA256
Supported response digest algorithm: SHA256

Identity provider alternate signing certificate

Single sign-on service URL

● Artifact binding ○ HTTP POST binding

□ Requires a single assertion consumer service URL

Artifact resolution service URL

Name identifier format: Persistent

□ Case insensitive

Name of "First name" attribute

Name of "Last name" attribute

Name of "Email address" attribute

Name of "Phone number" attribute

Service provider issuer (EntityId): https://staging.symbility.net

Service provider issuer suffix

Service provider assertion consumer service URL: https://staging.symbility.net/ux/saml2/acs

Service provider signing certificate: -----BEGIN CERTIFICATE-----

5.1.1. Identity Provider Issuer (EntityId)

- This is a mandatory field.
- This is a field that needs to be supplied by your IT team.
- This is the name of the SSO system that will be used to identify itself to CoreLogic's.

5.1.2. Identity Provider Signing Certificate

- This is a mandatory field.
- This is a field that needs to be supplied by your IT team.
- This is the cryptographic certificate your SSO system uses to confirm its identity to CoreLogic. The text should start with and end with: ----- BEING CERTIFICATE----- // ----- END CERTIFICATE-----

5.1.3. Identity Provider Alternate Signing Certificate

- This field is optional.
- This is a field that needs to be supplied by your IT team.
- This is an alternate cryptographic certificate your SSO system uses to confirm its identity to CoreLogic. This field is useful only when your IT team will be in the process of switching to a new certificate. The text should start with and end with: ----- BEING CERTIFICATE----- // -----END CERTIFICATE-----

5.1.4. Single Sign-on Service URL

- This is a mandatory field.
- This is a field that needs to be supplied by your IT team.
- This is the URL that the user will be redirected to confirm his username, when they try to login into CoreLogic.

5.1.5. Choice of binding (Artifact binding vs HTTP POST binding)

- This is a mandatory field.
- This is a field that needs to be supplied by your IT team.
- This is choosing what internal SAML workflow CoreLogic and your SSO system will use to communicate.

5.1.6. Requires a single assertion consumer service URL

- This is a mandatory field.
- This is a field that needs to be supplied by your IT team.
- This field is only mandatory if Artifact Binding is used.
- This field will be hidden if not needed.
- This is another option regarding the internal SAML workflow between CoreLogic and your SSO system. Not all systems support having multiple/dynamic redirection URLs to send the users to, once they have been authenticated.

5.1.7. Artifact Resolution Service URL

- This is a mandatory field.
- This is a field that needs to be supplied by your IT team.
- This field is only mandatory if Artifact Binding is used.
- This is the URL CoreLogic's server will use to fetch additional login information during the Artifact Binding workflow.

5.1.8. Name of "First name" attribute

- This field is optional.
- This is used to link CoreLogic User attributes to specific attributes to your system.
- The CoreLogic system can use that information to update its own Users information.

5.1.9. Name of "Last Name" Attribute

- This field is optional.
- This is used to link CoreLogic User attributes to specific attributes to your system.
- The CoreLogic system can use that information to update its own Users information.

5.1.10. Name of "Email Address" Attribute

- This field is optional.
- This is used to link CoreLogic User attributes to specific attributes to your systemcorelogic.com.
- The CoreLogic system can use that information to update its own Users information.

5.1.11. Name of "Phone Number" Attribute

- This field is optional.
- This is used to link CoreLogic User attributes to specific attributes to your system.
- The CoreLogic system can use that information to update its own Users information.

5.1.12. Service Provider issuer (EntityId)

- This is a locked field and cannot be modified by client.
- This field needs to be provided to your IT team.
- This is basically the name CoreLogic's system will use to identify itself to your SSO system.

5.1.13. Service Provider issuer suffix

- This field is optional.
- This is a field that needs to be supplied by your IT team.
- If the Service Provider issuer (EntityId) is not precise enough, your SSO system can provide a suffix CoreLogic would add to the name it uses to identify itself to your SSO system. This would be useful if several CoreLogic systems are configured to interact with your SSO system (e.g., a Staging and a Production environment).

5.1.14. Service Provider Assertion Consumer Service URL

- This is a locked field and cannot be modified by client.
- This field needs to be provided to your IT team.
- This is the URL your system needs to redirect users to, once they have been authenticated.

5.1.15. Service Provider signing certificate

- This is a locked field and cannot be modified by client.
- This field needs to be provided to your IT team.
- This is the cryptographic certificate CoreLogic will use to confirm its identity to your system.
- While CoreLogic is in the process of switching its certificate, an alternate certificate will be provided as well (the field doesn't appear if it's not in use). Both should be trusted.
- You don't have to monitor the configuration for the alternate certificate. CoreLogic would reach out via email or some other form of communication when necessary.

CoreLogic Support

Support.claims@corelogic.com or call 1-877-862-8069