# SSO FAQ

#### Q: Does the application support SAML 2.0, OAuth/OpenID Protocol.

A: We support SAML 2.0, OpenID/OAuth2, Azure AD and native LDAP.

### SAML 2.0

#### Q: What is SAML Consumer URL to post Assertion (Across All Environments)

A: The Incorta URL followed by “!<tenant\_name>“ (Example: [http://<incorta\_base\_url>/incorta/!demo/](http://localhost:8080/incorta/!demo/)).

#### Q: Application URL/Service Provider Start URL (Across All Environments)

A: The Incorta URL followed by “!<tenant\_name>“ (Example: [http://<incorta\_base\_url>/incorta/!demo/](http://localhost:8080/incorta/!demo/)).

#### Q: Provide a list of attributes to be sent as claims in the assertion.

A: Only one attribute  
loginName: Its the value that identifies a user in Incorta (Ex: email or login name).

#### Which SAML flows does the application support (IDP Init, SP Init (Redirect/Post)).

A: Both.

#### Does the application need a cert public key, thumbprint, serial?

A: Cert public key (to be safe we need to download the metadata file downloaded from the SSO provider, this is explained in depth in our documentation).

#### Q: Authentication fallback support?

A: No

### OAuth2.0

* We only support (OAuth2.0 through Auth0).
* Client Redirect URI  
  The Incorta URL followed by “!<tenant\_name>” (Example: [http://<incorta\_base\_url>/incorta/!demo/](http://localhost:8080/incorta/!demo/)callback)
* Scopes: In case of Auth0 (OpenID, profile, email).
* We support logout functionality.