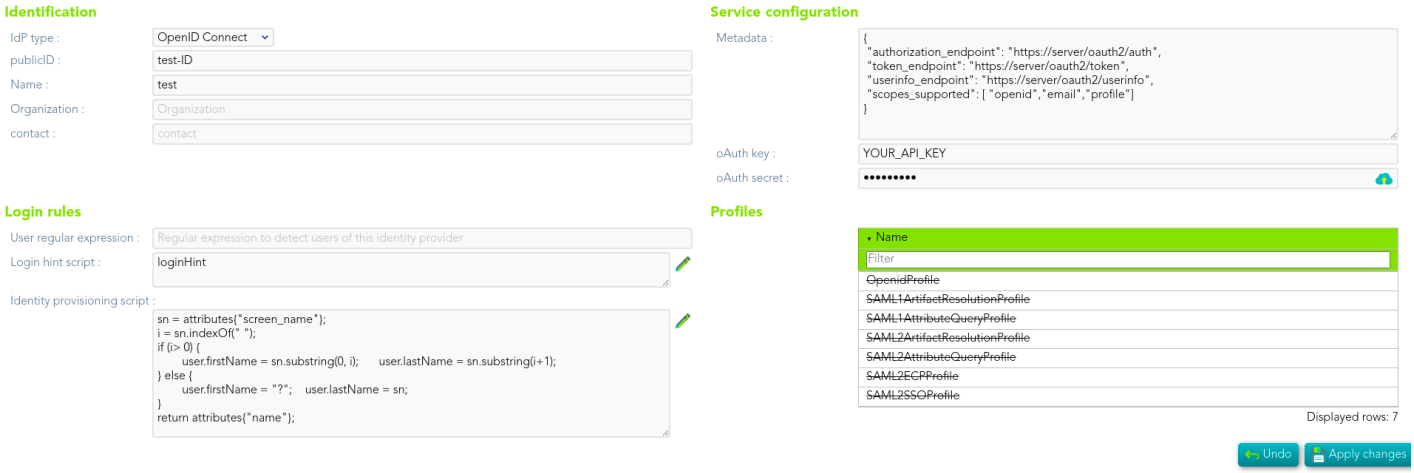
External oAuth / OpenID Identity Providers

Introduction

Soffid federation can be composed by a mix of SAML and oAuth / OpenID-connect servers. In such a scenario, Soffid IdP is able to let users be identified by oAuth servers like Linked-in, Google or Facebook, perform all the provision tasks required and send back a SAML assertion to the service provider requiring user authentication.



To create an external oAuth identity provider, you can choose the Idp type from a list of popular sites, like Google or Facebook, or write you own descriptor.

The descriptor should follow the OpenID connect discovery JSON document. Most parameters are optional, but these are required:

- **authorization_endpoint**: contains the oAuth endpoint to forward the user to get the authorization token.
- **token_endpoint**: contains the oAuth endpoint to get the access token, based on the authorization token got at previous step.
- **userinfo_endpoint**: if remote IdP is OpenID-connect compliant, the token endpoint should have sent an access token along a JWT OpenID token containing user claims. If this is not the case, Soffid will use this user_info endpoint to fetch user claims. This

mechanism is needed for oAuth2 servers.
- **scopes_sopported**: The list of scopes specified here will be used at first step, when redirecting the user to the authorization endpoint.

Next, you must register Soffid IdP with your oAuth server. After registering, you will get a oAuthKey (some kind of username) and an oAuthSecret (some kind of password). To register Soffid IdP, your oAuth server will require you to specify the redirection endpoint. This redirection endpoint refers to your Soffid IdP and will receive the authorization token generated by the oAuth server.

If your Soffid IdP is listening to https://idp.yourdomain.com:2443/, your redirection endpoint will be https://idp.yourdomain.com:2443/**oauthResponse**

As an example, here you have some links to get your oAuth keys and secrets for Google, Facebook and Linkedin.

Revision #4
Created 9 November 2021 08:04:06
Updated 21 June 2022 14:54:40