

# OpenID-Connect example

## Identity Provider

### Identification

IdP type :	OpenID Connect
publicID :	OpenIDConnect_ID
Name :	OpenIDConnect_Test
Organization :	Soffid
contact :	pgarcia@soffid.com

### Service configuration

Metadata :	<pre>{   "authorization_endpoint": "https://server/oauth2/auth",   "token_endpoint": "https://server/oauth2/token",   "userinfo_endpoint": "https://server/oauth2/userinfo",   "scopes_supported": [ "openid", "email", "profile" ],   "display": "page" }</pre>
oAuth key :	oAuth key
oAuth secret :	oAuth secret

### Login rules

User regular expression :	Regular expression to detect users of this identity provider
Login hint script :	loginHint
Identity provisioning script :	Script to bind or register a new identity. Return the user name of the owner identity for the authenticated acc

Undo Apply changes

## Service Provider

### Identification

Type :	OpenID Connect
publicID :	openidlab
Name :	OpenID Connect tenant

### Login rules

Allow impersonations :	Target application URL
UID Script :	Script to compute the user name to pass to the target application
Ask for consent :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Roles required to login :	Roles required to login
System where an enabled account is required :	

### OpenID authorization flow

Implicit :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No										
Authorization code :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No										
User's password :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No										
User's password + Client credentials :	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No										
Client id :	tenant										
Client secret :	*****										
Response URL :	https://localhost/return										
Logout response URL :	Logout response URL										
oAuth Session timeout (secs) :	oAuth Session timeout (secs)										
Allowed scopes	<table><thead><tr><th>Scope name</th><th>Required roles</th></tr></thead><tbody><tr><td>Filter</td><td>Filter</td></tr><tr><td>api.person.read</td><td></td></tr><tr><td>api.person.write</td><td></td></tr><tr><td>openid</td><td></td></tr></tbody></table>	Scope name	Required roles	Filter	Filter	api.person.read		api.person.write		openid	
Scope name	Required roles										
Filter	Filter										
api.person.read											
api.person.write											
openid											

Displayed rows: 3

Note that the scope 'openid' will always be accepted.  
A scope with no roles will be granted always.  
A scope with roles will be granted if the identified user has the required role.  
Add the scope \* to allow any scope

Undo Apply changes

Revision #3

Created 25 August 2022 06:18:56 by pgarcia@soffid.com

Updated 25 August 2022 06:24:13 by pgarcia@soffid.com