OPENID-SAML IDP WEB SERVICE

OpenID-SAML IdP Web Service

Web-Service SSO Federation

OpenID/SAML Identity Provider

The installation of OpenID/SAML IdP is straightforward and only consists in running the self-installer and configure the application in WebADM.

You do not have to modify any files in the OpenID install directory! The web applications configurations are managed and stored in LDAP by WebADM. To configure OpenID/SAML, just enter WebADM as super administrator and got to the 'Applications' menu. Click OpenID/SAML to enter the web-based configuration.

OpenID/SAML application logs are accessible in the Databases menu in WebADM.

Note: To be able to use OpenID/SAML, any LDAP user must be a WebADM account. That means usable LDAP accounts are those containing the webadmAccount LDAP object class. You can enable the WebADM features on any LDAP user/group by extending it with the webadmAccount object class (from object extension list).

Inline WebApps:

You can embed a Web app on your website in an HTML iFrame or Object.

```
#Example
<object data="https://<webadm_addr>/webapps/openid?inline=1" />
```

1. SAML IdP Configuration

SAML IdP requires a certificate and a private key to be set in the configurations. You can generate an X.509 certificate and private key with OpenSSL:

```
openssl genrsa -out server.key 1024
openssl req -new -key server.key -out server.csr
openssl x509 -req -days 3650 -in server.csr -signkey server.key -out server.crt
```

You can copy/paste the server.crt and server.key contents in your configuration.

The SAML clients (Service Providers) need to know about the SAML IdP endpoints. Most clients will accept the auto-configuration with an XML-based metadata URL. The server metadata URL is: `https://yourserver/webappd/openid/metadata/`. If you need to manually enter the IdP service URLs go to the HTML-based metadata URL with your Web browser: `https://yourserver/webapps/openid/metadata/html/`. You will find client configurations like:

- The SAML entityID of the IdP.
- The SAML server certificate.
- The SingleSignOnService URL.
- The SingleLogoutService URL.

⚠ Important

Many SAML Service Providers will require your WebADM to be run with a trusted SSL certificate. You can replace the default WebADM SSL certificate with your own. Just replace the /opt/webadm/pki/httpd.crt and /opt/webadm/pki/httpd.key.

2. OpenID IdP Configuration

Version 1.2x includes the support for OpenID-Connect and OAuth2.

To use your identity provider in OpenID-Connect mode, the client configuration must pass the scope ‘openid’ in the IdP requests. The supported OpenID-Connect scopes are: basic, email, phone and profile.

To use your identity provider in OAuth2 mode, the client must pass the scope ‘profile’ in the IdP requests.