

Mod Auth OpenIDC

Configuration

- Install `mod_auth_openidc` for Apache: https://github.com/zmartzone/mod_auth_openidc/
Use **`apt install libapache2-mod-auth-openidc`** for a Debian system.
- Load the module in Apache via `httpd.conf`:

```
LoadModule auth_openidc_module modules/mod_auth_openidc.so
```

Use **`a2enmod mod_auth_openidc`** and restart Apache for Debian

- Complete Apache's `httpd.conf` file.
The following example requires customization according to your context.

```
<VirtualHost *:443>
    # Server setup
    ServerName myapplication.tld
    # ... your particular directives ...
    # OpenID Connect setup
    OIDCProviderMetadataURL https://mydomain.trustelem.com/app/146XXX/.well-known/openid-
configuration
    OIDCClientID trustelem.oidc.XXXXXXXXXX
    OIDCClientSecret XXXXXXXX
    OIDCRedirectURI https://myapplication.tld/redirect_uri
    OIDCCryptoPassphrase XXXXXXXX
    OIDCScope "openid"
    <Location /sso-login>
        AuthType openid-connect
        Require valid-user
    </Location>
    # Specific session cookie durations (seconds)
    OIDCSessionInactivityTimeout 300
    OIDCSessionMaxDuration 36000
</VirtualHost>
```

The **`OIDCCryptoPassphrase`** parameter is used in particular for encrypting user session cookies.

- For logging out users from inside the application, you have to associate a logout URL to an HTML element like a button or a link. This URL is defined by the `redirect_uri` with a **logout=** parameter and the post-logout URL in a URL-encoded format.

For example, the logout URL could be:

```
https://myapplication.tld/redirect_uri?logout=https%3A%2F%2Fmyapplication.tld
```

- Setup Trustelem with the following parameters:

- **RedirectURI:** this URL is defined in the web server configuration (see `httpd.conf`).

With the previous example, the RedirectURI would be:

```
https://myapplication.tld/redirect_uri
```

- **Login URL:** the application's URL starting the OIDC flow. It is used as a target for the application on the Trustelem user's dashboard.

With the previous example, the URL would be: `https://myapplication.tld/sso-login`

- **PostLogoutRedirectURI:** the URL that indicates where to go after a logout. It is usually defined in the logout HTML element of your application.

With the previous logout example, the PostLogout URL would be:

```
https://myapplication.tld
```

Notes

- The attributes sent by Trustelem are provided to the application under the designation `$_SERVER["OIDC_CLAIM_nom"]`, where the name is defined in the Trustelem-hosted script in the field called **custom claims**.

For example, if you add the following custom claim, you will find the user firstname into the variable `$_SERVER["OIDC_CLAIM_attr1"]`:

```
claims["attr1"] = user.firstname;
```

- If the user authenticated with `mod_auth_openidc` doesn't exist in the application, we recommend to create the user using the attributes sent by Trustelem.
This auto-provisioning system enables the implementation of internal rights management based on attributes sent by Trustelem.
This completes access control policies defined in Trustelem.

Revision #2

Created 1 July 2022 09:01:57 by WALLIX Admin

Updated 9 November 2022 10:25:46 by WALLIX Admin