OAuth2 Token Revocation

The OAuth Token Revocation functionality is available with WSO2 Identity Server and follows this specification. There are two endpoints exposed as a result of the token revocation feature.

1. REST endpoint at /oauth2/revoke
2. SOAP endpoint at /services/OAuthAdminService with operation revokeAuthzForAppsByResourceOwner

The REST endpoint is for OAuth 2.0 clients who want to revoke any access granted to them by a resource owner. This could be at the discretion of the resource owner or otherwise. In other words, this endpoint is meant for OAuth 2.0 clients only in order to authenticate themselves using client_id and client_secret and revoke the authorization granted to them. They may use the access token or refresh token for this purpose. Regardless of which token the client uses, the result is the same; the client cannot access the user’s resource again until such time the user explicitly provides a grant by authorizing the client at the OAuth 2.0 authorization server.

The following is an example of the request that needs to be sent to the revocation REST endpoint by OAuth 2.0 client to revoke a token:

```
curl -X POST --basic -u "<client id>:<client secret>" -H "Content-Type: application/x-www-form-urlencoded;charset=UTF-8" -k -d "token=<token to revoke>&token_type_hint=access_token" https://localhost:9443/oauth2/revoke
```

The token parameter used here can be an access token or refresh token. The token_type_hint parameter is optional. This parameter can take values of either access_token or refresh_token. The Identity Server uses this parameter to speed up the process of looking up the token by searching first in the set of tokens the client specifies (access_token or refresh_token). If the token is not to be found in the set the client claims it to be in, then the server looks for the token in the other set (refresh_token or access_token).

The SOAP endpoint, on the other hand, is for the resource owners to directly interact with the Authorization server and revoke authorization grants for applications they previously granted access to, without the OAuth 2.0 application/client being an intermediary in the process. The use of this SOAP endpoint is demonstrated by the WSO2 Identity Server’s dashboard under Authorized Apps for resource owners to login and revoke application authorization.

1. Go to the dashboard URL: https://localhost:9443/dashboard/.
2. Click the Login button.
3. Enter your username and password and click the Sign In button. The dashboard appears.
4. Click the View details button to access the components.
5. Once you have logged in, click View details under Authorized Apps. The following page appears, listing out the available apps.

The Authorized Apps page indicates the user has granted authorization to the application 'travelocity created by user ‘admin’.

The token revocation end-point also supports CORS (Cross-Origin Resource Sharing) specification and also JSONP (Remote JSON – JSONP).

CORS is supported through CORS-Filter which can be found here. The CORS Filter is designed to be plugged to a webapp using its deployment descriptor (web.xml). Since the OAuth 2.0 endpoints in WSO2 Identity Server have been written as JAX-RS endpoints, you can add the required CORS configurations to its deployment descriptor.
You can find this webapp at `<WSO2_IS_HOME>/repository/deployment/server/webapps/oauth2.war`. Rather than editing the `web.xml` directly in the deployed directory, it’s easier to copy the `oauth2.war` file into another location, edit the `web.xml` and copy it back into the `webapps` folder and it gets hot deployed.

Example of a JSONP revocation request:

```
curl -X POST --basic -u "<client id>:<client secret>" -H "Content-Type: application/x-www-form-urlencoded; charset=UTF-8" -d "token=<token to revoke>&token_type_hint=access_token&callback=package.myCallback"
https://localhost:9443/oauth2/revoke
```

The `callback` parameter is optional.