**OAuth**

OAuth is an open standard for delegated authorization. The OAuth authorization infrastructure allows a user to grant a third-party application access to their information stored with another HTTP service without sharing their access permissions or the full scope of their data.

In OAuth, the client, or third-party application, requests access to resources controlled by the resource owner and hosted by the resource server, and is issued a set of credentials distinct from the resource owner's credentials. Instead of using the resource owner's credentials to access protected resources, the client obtains an access token, which is a string indicating a specific scope, duration, and other access attributes. An authorization server issues access tokens to third-party clients with the resource owner's approval. The client uses the access token to access protected resources hosted by the resource server.

OAuth 2.0 is the latest OAuth protocol, and is not compatible with OAuth 1.0. OAuth 2.0 makes it easier for client application developers to use, while providing authorization flows for different types of client applications.

WebSphere® Application Server supports OAuth 2.0 and plays a role as both an OAuth service provider endpoint and an OAuth protected resource application endpoint.

The supported OAuth standard specifications are as follows:

The OAuth 2.0 Authorization Framework

The OAuth 2.0 Authorization Framework: Using Transport Tokens

Summary of Features within WebSphere Application Server OAuth 2.0 Services

Below is a summary of features within WebSphere Application Server OAuth 2.0 Services.

OAuth 2.0 Services

WebSphere Application Server OAuth Services include both the OAuth Authorization Service and the Web Resource Authorization Decision Service.

Invoking the OAuth 2.0 Service

A registered OAuth client can invoke the WebSphere Application Server OAuth Service Authorization endpoint to request an authorization code. A registered OAuth client can also invoke the WebSphere Application Server OAuth Service Token endpoint to request an access token. The client can then use the access token to request protected web resources from WebSphere Application Server.

Customizing an OAuth Provider

The WebSphere Application Server OAuth Service Provider has plug-in points for customization. You can replace the default form login page for user authentication or develop your own user consent form to collect authorization data from the client. WebSphere Application Server OAuth providers also allow custom post-processing for significant events in the issuance of OAuth tokens using mediators.

SQL statements for persistent OAuth service

WebSphere Application Server supports persistent OAuth 2.0 service by persisting OAuth clients and tokens in a database. With persistent OAuth 2.0 services, an authorized client can access the OAuth 2.0 service after the OAuth services are restarted.