# Difference between Web server OAuth flow, User agent flow OAuth Authentication flow and Username-Password OAuth Authentication flow

### Web server OAuth flow

Typically used for web applications where server-side code needs to interact with Force.com APIs on the user’s behalf, for example DocuSign. Trust that the web server is secure to protect the consumer secret. Client application

1. Client directs user to authorisation end point.
2. User logs in to authorization end point and does not interact with client application at all.
3. Redirect is sent back to users browser appended with authorization code.
4. Client application extracts the access code and sends to authorisation end point.
5. If successful authorisation end point returns access and refresh tokens.
6. Client application uses token to access users data

### User agent flow OAuth Authentication flow

Flow is used for authentication for client applications that reside on users device. Key difference with web server flow is that client cannot keep consumer secret confidential.

1. Client directs user to authorization end point.
2. User logs in to authorisation end point and does not interact with client application at all
3. Redirect is sent back to users browser appended with access token
4. Client application uses access token to access user data

### Username-Password OAuth Authentication flow

This flow can be used where the client application already has the username password of the user. The flow is discouraged due to username and password being used back and forth in requests.

1. Client application requests access code with username/password
2. Authentication end point returns access token if successful
3. Client application uses access token for access