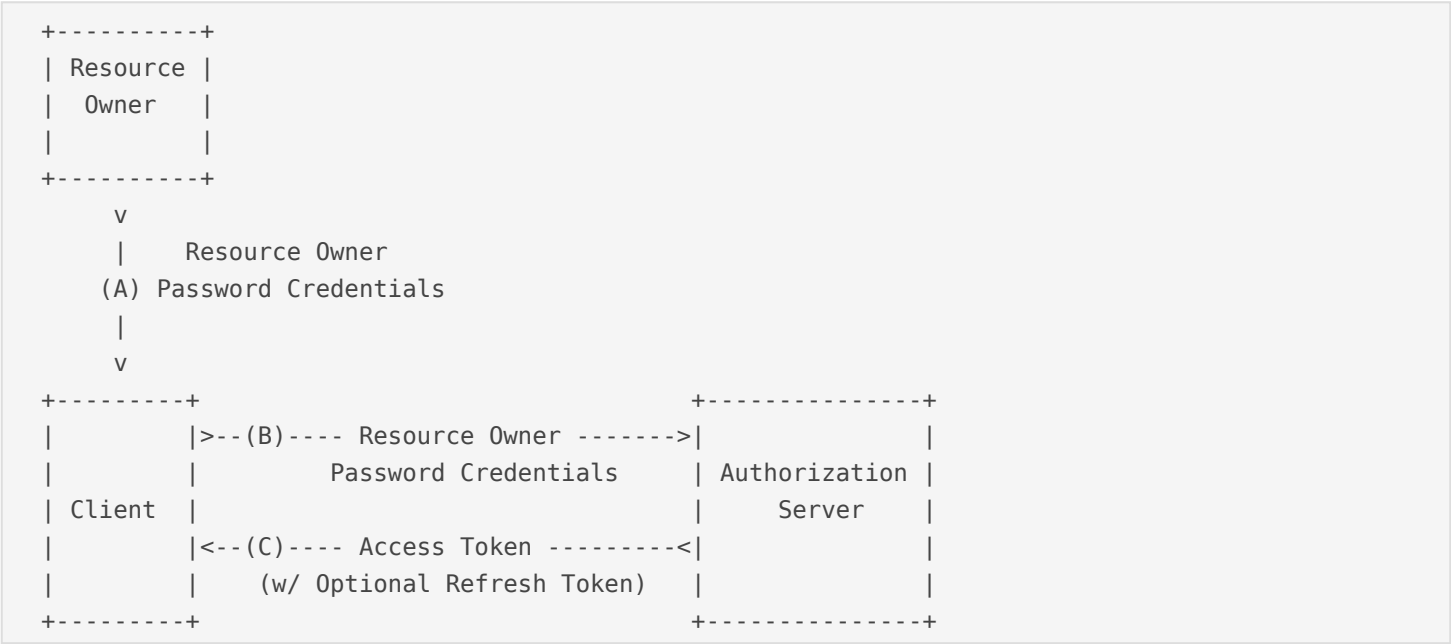


# 4.3. [redacted](4.3. Resource Password Credentials Grant)

## 4.3. [redacted]

[redacted] HTTP [redacted] OAuth



5 [redacted]

5 [redacted]

- A [redacted]
- B [redacted]
- C [redacted]

## 4.3. Resource Owner Password Credentials

# Grant

The resource owner password credentials grant type is suitable in cases where the resource owner has a trust relationship with the client, such as the device operating system or a highly privileged

RFC 6749

OAuth 2.0

October 2012

application. The authorization server should take special care when enabling this grant type and only allow it when other flows are not viable.

This grant type is suitable for clients capable of obtaining the resource owner's credentials (username and password, typically using an interactive form). It is also used to migrate existing clients

using direct authentication schemes such as HTTP Basic or Digest authentication to OAuth by converting the stored credentials to an access token.



### Figure 5: Resource Owner Password Credentials Flow

The flow illustrated in Figure 5 includes the following steps:

- (A) The resource owner provides the client with its username and password.
- (B) The client requests an access token from the authorization server's token endpoint by including the credentials received from the resource owner. When making the request, the client authenticates with the authorization server.
- (C) The authorization server authenticates the client and validates the resource owner credentials, and if valid, issues an access token.

---

Revision #1

Created Wed, Mar 25, 2020 10:55 PM by [ ]

Updated Wed, Mar 25, 2020 10:56 PM by [ ]