Acquiring Access and Refresh Tokens

Access and refresh tokens are strings used to identify a user. The table below indicates the use for each type of token:

Token Type	Description
Access Token	This is required to grant access to the data provided by the API.
Refresh Token	Use this to generate a new access token after the old one expires. This allows access to continue without the need to authenticate again.

An access token and a refresh token are granted after the user has successfully proven their identity through the authentication process. Acquisition of these tokens are done using the endpoints discovered in the previous chapter.

There are three different ways to proceed depending on the type of integration. Use the following table to determine which scenario to use:

Use Case	Description	Authorization Grant
Anonymous Users	Software that only accesses one VideoManager Pro account belonging to the application developer. Users don't need to have a VideoManager Pro account and can use the application anonymously. This use case can be used for both client-side and server-side applications. This should be the appropriate option for most integrations.	Resource Owner Password Credentials
Logged-in Users (client-side)	Software within a user's browser that redirects the user to allow them to login to their VideoManager Pro accounts. Here, a code is given to the browser and traded for an access token.	Authorization Code
Logged-in Users (server-side)	Server-side software that redirects the user to allow them to login to their VideoManager Pro accounts. Here, a code is given to the server and traded for an access token.	Authorization Code

Note the authorization grant; this is the corresponding OAuth authorization grant (or flow) that is used to retrieve the access token.