

WP API Authentication via Application Passwords

Tags

Engineering Documentation

For authenticating API requests via WordPress Application Passwords, you will need to add the following HTTP Header to your API request: `Authorization: Basic <auth token>`

The `auth token` is a base64 encoding of this string: `<author's username>:<application password>`

It is preferred to create an application password specific for API access rather than using the author's WP password. To create a password, navigate to the WP user page from `http://<site domain>/wp-admin/users.php` and towards the bottom you can enter your desired name in the `New Application Password Name` field, for example `rsoc-post-api` and get the password.

Account Management

New Password

[Set New Password](#)

Application Passwords

Application passwords allow authentication via non-interactive systems, such as XML-RPC or the REST API, without providing your actual password. Application passwords can be easily revoked. They cannot be used for traditional logins to your website.

New Application Password Name

[Add New](#)

Your new password for My New App is: **Cben CvDb ZNQD p2y9 SVPO sClz**



Be sure to save this in a safe location. You will not be able to retrieve it.

Name	Created	Last Used	Last IP	Revoke
My New App	October 21, 2020	—	—	Revoke
Name	Created	Last Used	Last IP	Revoke
Revoke all application passwords				

[Update User](#)

In this example, the auth token string to be encoded will be **<author>:Cben CvDb ZNQD p2y9 SVPO sClz** which then needs to be appended into the Authorization header (post base64 encoding).