

WordPress REST API Authentication V3.1.0 WP Plugin Free Download

WordPress REST API Authentication V3.1.0 WP Plugin Free Download.. WordPress REST APIs by default are loose endpoints through which a hacker can control your site remotely... [Download](#)

Rating: Not Rated Yet

Price

[Report Copyright about this product](#)

Description

WordPress REST API Authentication V3.1.0 WP Plugin Free Download

WordPress REST APIs by default are loose endpoints through which a hacker can control your site remotely. You don't want hackers to give access to your WordPress Login and WordPress Register or any other endpoints. With our WordPress REST API Authentication plugin, we promise to have the secure api from unauthorized users and protects WP REST API endpoints from public access using API Key Authentication or JWT Authentication or Basic Authentication or OAuth 2.0 Authentication or third-party OAuth 2.0/OIDC/Firebase provider's token authentication methods. Our plugin is made in a way to make sure that we always have a secure api connection so that data isn't compromised. JWT Authentication is an industry-approved method to secure communication between 2 parties and we also allow you to use that on your wordpress website.

It also allows you to access the WordPress REST APIs using the above-mentioned authentication methods from Android / iOS and desktop applications.

This plugin will make sure that only after the successful authentication, the user is allowed to access your site's resources which adds to our motivation toward secure API. REST API Authentication will make your WordPress login endpoints secure from unauthorized access. You can protect APIs with ease and in a highly secure way using this plugin.

This plugin also provides features for authentication of custom-developed REST endpoints and third-party plugin REST API endpoints like that of Woocommerce, Learndash, Buddypress, Gravity forms, CoCart etc.

You can create the custom routes/REST endpoints in WordPress with another GUI-based plugin Custom API for WordPress.

You will be able to securely log in using the following endpoint:

`https://wp-json/api/v1/token`

USECASES

The WordPress REST API makes CRUD (Create, Read, Update & Delete) operations available from anywhere instead of being limited to just the admin dashboard. It provides a lightweight form of communication between the client and the server making it a great solution for exchanging data.

It can be used to create iOS/Android, etc native apps. We can use any language we want as long as the language can make HTTP requests and interpret JSON such as Node, JS, Express JS, Ruby, Python etc.

WordPress Login and WordPress Registration become secure with REST API Authentication.

Block unauthorized public access to your WordPress and protect API endpoints like /pages, /posts to secure your website from hackers.

**Disable WP REST APIs to prevent data leakage and allow access only to authorized users

Only users authorized using our plugin's authentication methods will be allowed to access the secure API.

Login APIs will be protected from unauthorized access.

Woocommerce, LearnDash, BuddyPress, Gravity forms, CoCart etc. like plugins will be secured with our plugin's authentication methods.

JWT token (JSON Web tokens) from other Identity Providers (OAuth/OIDC providers) Authenticate/Protect/Secure WordPress REST API endpoints with the access token .

Securely Login and register into Mobile or other client applications using REST APIs.

Obtain user-based JWT token to use as an authentication source to login and register on other platforms.

Authenticate Woocommerce REST API endpoints by bypassing WooCommerce consumers' credentials security instead of using their authentication methods to control the data access and thus improving security and removing chances for exposing the WC credentials.

Authenticate/secure WordPress REST APIs access using Firebase JWT token, any external JWT token, any OAuth 2.0/OpenID Connect(OIDC) provider access/id-token like Azure AD, Azure B2C, Okta, Keycloak, ADFS, AWS Cognito etc or that provided by Social login providers like Google, Facebook, Apple.

The plugin provides an interface for applications to interact with your WordPress REST API endpoints by sending and receiving data as JSON (JavaScript Object Notation) objects. Also, It provides a user-friendly user interface of the plugin to configure the methods and implement them very easily. You can easily secure API/protect your WordPress REST API endpoints with ease.

With our plugin, the user credentials are not stored as cookies but with every API call, user credentials or JWT (JSON Web tokens) or API key is passed so that we have secure API transactions.

WORDPRESS REST API AUTHENTICATION METHODS IN OUR WORDPRESS PLUGIN

Basic Authentication: This is a basic authentication method to protect your wordpress endpoints by following methods:

– 1. Username: Password: This method for Basic Authentication authenticates the REST APIs by using username and password in the authorization header in the form of base64 encoded or with highly secure HMAC encryption.

– 2. Client-ID: Client-Secret: This method for Basic Authentication authenticates/protects the REST APIs by using client credentials provided by the plugin in the authorization header in the form of base64 encoded or highly secure HMAC encryption.

API Key Authentication: It allows you to secure wordpress endpoints without exposing user credentials as the plugin generates an API key for accessing any resource which can also be regenerated in the plugin UI.

JWT Authentication: WordPress REST API Authentication itself issues the JWT token and works as an API Authenticator to protect your REST APIs. The plugin itself provides the REST API endpoint through which you can generate the JWT token very easily by passing the valid WordPress user credentials.

OAuth 2.0 Authentication: If you don't have a third-party identity provider, then, in this case, WordPress REST API Authentication works as both OAuth Server(Provider) and API Authenticator to protect your REST APIs. It is the most secure method to authenticate the WordPress REST API endpoints.

– 1. Password Grant: If you want to fetch user-specific content from the database then this method is useful

– 2. Client Credentials Grant: This method uses the OAuth 2.0 protocol with Client Credentials grant to authenticate the WP REST API endpoints to use services that call APIs without users.

Third Party Provider Authentication: if you are already using an external OAuth/OpenID Connect (Identity provider) which provides you with an access token/id token or a JWT token, then that token can be used to authenticate the WordPress REST APIs and the plugin will validate the token directly from these token providers and only on successful validation, API endpoints are allowed to access.

Following are some of the integrations that are possible with REST API Authentication:

WOOCOMMERCE API

WordPress Rest API authentication allows integration of WP Rest API with WooCommerce Rest APIs. You can authenticate the WooCommerce store APIs with your mobile or desktop application & extend the features and functionality of your eCommerce store.

BUDDYPRESS API (BP REST API)

With this plugin you can access BP REST API endpoints and also authenticate those from different Authentication methods like JWT token (JSON Web Token), API Keys etc.

GRAVITY FORM API

This plugin supports interaction with Gravity Forms from an external client application which can be your Android/iOS application. WP REST API Authentication also allows WordPress users to create, read, update and delete forms, entries, and results over HTTP based on their roles.

LEARNDASH API

This plugin allows you to securely access LearnDash user profiles, courses, groups & many more third-party APIs.

CUSTOM BUILT REST API ENDPOINTS

The plugin supports authentication for your own built custom REST API routes/endpoints. You can secure these API endpoints using the plugin's highly secured authentication methods.

EXTERNAL/THIRD-PARTY PLUGIN API ENDPOINTS INTEGRATION IN WORDPRESS

These integrations can be used to fetch/update the data from the third-party side into the WordPress that can be used to display it on the WordPress site as well and this data can be processed further to use with any other plugin or WordPress events.

FEATURES

FREE PLAN

Supports Basic Authentication with username and password along with base64 encoding of the API token to have a secure api.

JWT Token-based Authentication.

Authentication for all the Standard WordPress REST API endpoints like WordPress Login, WordPress Register, etc...

Allow or Deny public access to your WordPress standard REST APIs as per your requirement. Disable REST APIs as needed.

Token endpoint to retrieve user-specific JWT (JSON Web tokens).

Restrict non-logged-in users to access REST API endpoints.

Postman Samples for each Authentication method to test API access with the Postman application

PREMIUM PLANS

Authentication (Protection) for all WordPress REST API endpoints including standard WP REST APIs and custom/third-party plugin REST API endpoints.
Supports Basic Authentication (both WP User credentials and Client credentials), JWT Token Authentication, API Key Authentication, OAuth 2.0 Authentication, and Third-Party OAuth 2.0/OIDC Provider's Token Authentication methods.
HMAC encryption and user-specific Client credentials with Basic authentication.
Token endpoint to retrieve user-specific JWT (JSON Web tokens).
Allow or Deny public access to all the WordPress standard REST APIs as well as custom/third-party plugin REST API endpoints as per requirement.
Universal (Global) API key as well as User-specific API key for authentication.
Supports JWT Authentication with signature validation using highly secured HSA & RSA Signing.
Custom Token Expiry feature for JWT token to further increase security.
Provides the Time-based Access token or JWT token.
WordPress Login using Access token or JWT token.
Authenticate WordPress REST APIs with the token (access token / JWT) provided by your OAuth/OIDC Provider (Third Party Provider) like Azure, AWS Cognito, ADFS, Keycloak, Google, Facebook, ADFS, Firebase or any external JWT (JSON Web tokens) provider etc.
User's WordPress Role and capability-based access to all the WordPress REST API endpoints like posts, pages etc.
Allow or Deny public access to your WordPress REST APIs as per requirement. Disable REST APIs as needed.
Custom Header support rather than just 'Authorization' to increase security.
Create users in WordPress based on third-party provider access tokens (JWT tokens).
Feature to exclude any selected REST API endpoints.
Restrict non-logged-in users to access REST API endpoints.

OUR OTHER POPULAR REST API INTEGRATIONS

Custom API for WP plugin

It allows you to create custom REST API endpoints in WordPress through an easy-to-use GUI without the need to write the code.
It allows you to integrate external APIs in WordPress (Connect to External API in WordPress) such that you can easily connect to any of our external or 3rd-party REST API endpoints in WordPress to display the real-time data or store and use that data for further purposes. Supports all authentication like OAuth 2.0, Basic Auth, JWT, API Key etc.
Sync products to WooCommerce | Import WooCommerce products using API

This plugin allows you to connect to your Supplier, Inventory, ERP, and CRM APIs to sync the products to your WooCommerce store with all the relevant product data automatically.
Sync Custom Posts using External API

This plugin allows you to automatically sync the data to a custom post in WordPress from the external REST API data.
Supports the data sync to custom post fields created using plugins like Advanced Custom Field (ACF)
Supports syncing automatically on a scheduled basis as per the time and Frequency you want.
WordPress JWT Single Sign-On (SSO) Auto login

This plugin helps you sync user sessions or auto-login to WordPress and other connected sites

PRIVACY

This plugin does not store any user data.