Simple OTP Login — User guide

News · https://kyzoe.be/en/docs/simple-otp-login-user-guide/

Version 2.1.0 Questions or need help? Feel free to get in touch via hallo@kyzoe.be or visit kyzoe.be.

1. What is Simple OTP Login?

Simple OTP Login replaces the classic WordPress password system with a **one-time login code** that is sent automatically by email. OTP stands for *One-Time Password* — a code that is valid only once and expires automatically after use or once its validity period has passed.

Why is this better than a password?

A password is something you remember — and it can be forgotten, guessed, stolen or leaked. A one-time code is created at the moment you log in and sent to an email address that only the rightful owner can access. No password also means no password that can be stolen.

In summary:

- Users no longer need a password
- Logging in works via email — fast and familiar
- Expired codes are automatically unusable
- Brute-force attacks are actively blocked
- Fully configurable to suit the needs of your website

2. How does logging in work?

The login process always takes place in two steps.

Step 1 — Request a code

The visitor goes to the login page and enters their **email address or username**. After clicking *Send login code*, the plugin automatically sends an email with a login code to the associated address.

Step 2 — Enter the code

The visitor enters the code they received on the login page. If the code is correct and still valid, the user is logged in and redirected to the dashboard or the configured redirect page.

```
Login page
    |
    ▼
[Enter email address or username]
    |
    ▼
Email sent with login code
    |
    ▼
[Enter code on the login page]
    |
    ▼
Logged in ✓
```

> **Please note:** When the *Require OTP login* setting is enabled (the default setting), logging in with a password is completely disabled for all users — including the administrator.

3. Installation

Via the WordPress dashboard (recommended)

1. Go to **Plugins → Add New Plugin**
2. Click **Upload Plugin**
3. Select the file `simple-otp-login.zip`
4. Click **Install Now**, then **Activate**

The plugin is active immediately after activation. Password login is disabled straight away.

Manually via FTP

1. Unzip the zip file on your computer
2. Upload the `simple-otp-login` folder to `/wp-content/plugins/` on your server
3. In the WordPress dashboard, go to **Plugins** and activate *Simple OTP Login*

> ⚠ **Important before activation**
>
> Make sure WordPress can send emails before you activate the plugin. If it can't, you will no longer be able to log in after activation because the login code will never arrive.
>
> Not sure? First install an SMTP plugin such as *WP Mail SMTP* or *FluentSMTP* and test whether emails arrive. You can then safely activate Simple OTP Login.

4. Settings — overview

You can find all settings in the WordPress dashboard under **Settings → Simple OTP Login**.

The settings page is divided into four tabs:

Tab	What you set here
General	Code length, validity period, OTP required or optional
Email Settings	Subject and content of the email containing the login code
IP Blocks	Overview of blocked IP addresses, unblocking
Login Log	View, filter and manage all login attempts

5. Tab: General

Settings → Simple OTP Login → General

This tab determines the behaviour of the login code itself.

Code length

Choose how many digits the login code contains: **4**, **6** or **8** digits.

Option	Example	Use
4 digits	`4829`	Lowest threshold — easy to type
6 digits	`482971`	Default — good balance
8 digits	`48297134`	Highest security — a little more typing

The login page automatically adjusts the input fields based on the chosen length.

Validity period:

How long is a code that has been sent valid?

Option	Explanation
5 minutes	Stricter — the user has to be quick
10 minutes	Default — ample but not too long
15 minutes	More lenient — more time for slow email delivery

Once the period has expired, the code can no longer be used. The user can easily request a new code via the back button on the login page.

Recommendation: Use 10 minutes as the default setting. Consider 15 minutes if your users regularly complain that codes have expired — this may indicate slow email delivery.

OTP required (toggle)

This switch determines whether logging in with a password is still possible.

Enabled (default — recommended)

The standard WordPress login form is completely hidden. Logging in with a password is blocked for all users. The only way to log in is with the one-time code.

Disabled

The OTP form is shown above the standard WordPress form. Users can choose: log in with the code or with their password. The login page shows a clear dividing line between the two options.

> ⚠ **Warning:** When the toggle is disabled, password login remains active. A yellow warning banner appears in the admin area as a reminder. We recommend leaving the toggle enabled for maximum security.

6. Tab: Email settings

Settings → Simple OTP Login → Email Settings

Here you can customise the email that users receive when they request a login code.

Subject and message text

You can freely customise both the subject and the full message text. The text supports **variables** (also called *placeholders*) that are automatically replaced with the correct values at the moment of sending.

Available variables

Variable	Is replaced by
`{otp}`	The login code itself (e.g. `482971`)
`{name}`	The user's display name
`{site}`	The name of your website
`{expires}`	The number of minutes the code is valid

Required: The `{otp}` variable must always be present in the message text. Without this variable, the user will not receive a code and will not be able to log in.

Live preview

While you edit the subject or message text, the panel on the right (or below) shows a **live preview** of what the email will look like for the recipient. The variables are already filled in with sample values.

Restoring the default text

Using the **Restore defaults** button, you reset the subject and message text to the original texts supplied with the plugin. A confirmation dialogue appears before the change is applied.

Example of a default email

```
Subject: [My Website] Your login code

Hello Jan de Vries,

Your one-time login code is:

  482971

This code is valid for 10 minutes.
```

```
If you did not attempt to log in, you can safely ignore this email.

— My Website
```

> **Tip:** Would you like the email entirely in Dutch? Replace the message text with your own Dutch text and use the same variables. The *Save settings* button saves your changes.

7. Tab: IP blocks

Settings → Simple OTP Login → IP Blocks

When someone repeatedly enters an incorrect code, the plugin automatically blocks that visitor's IP address. This tab gives you a complete overview and lets you lift blocks manually.

Statistics

At the top of the tab you will see three counters:

- **Currently blocked** — number of IP addresses that are actively blocked at the moment
- **Failed attempts** — IP addresses with failed attempts that have not yet been blocked
- **Total in log** — total number of recorded IP addresses

Actively blocked IP addresses

In the *Currently blocked IP addresses* table you will see for each IP address:

Column	Explanation
IP address	The blocked IP address
Attempts	Number of failed attempts
Blocked until	Time at which the block expires automatically
Time remaining	Countdown timer that updates live in the browser
Last attempt	Time of the last attempt
Action	Button to lift the block immediately

Using the **Unblock** button, you lift the block on one specific IP address. Using **Unblock all** (at the top right of the table), you lift all active blocks at once — a confirmation dialogue appears.

IP addresses with failed attempts (not blocked)

Below you will find IP addresses that have recorded failed attempts but have not yet reached the threshold of 5 attempts. Using the **Remove from log** button, you remove such an address from the overview.

How does automatic blocking work?

After **5 consecutive failed login attempts** — whether through incorrect codes or by requesting a code for a non-existent account — the plugin automatically blocks the IP address for **15 minutes**.

Once the block time has elapsed, the address is automatically unblocked. You don’t need to do anything for this.

8. Tab: Login log

Settings → Simple OTP Login → Login Log

The login log records every login attempt made via the plugin — successful or failed. This gives you complete insight into who is logging in to your website and whether there is any suspicious activity.

Statistics

At the top of the tab there are four counters:

Counter	Meaning
Total attempts	All login attempts in the log
Successful	Successful login attempts
Failed	Failed attempts (incorrect code, expired code)
Blocked	Blocked attempts (IP or account was already blocked)

Viewing log entries

For each login attempt, the table shows the following information:

Column	Explanation
Time	Date and time of the attempt
User	Username that was entered
IP address	The visitor’s IP address
Status	Successful / Failed / Blocked (colour-coded)
Reason	Description of the error for a failed attempt

Rows are visually distinguished by a coloured stripe on the left:

- **Green** — Logged in successfully
- **Orange** — Failed attempt
- **Red** — Blocked attempt

Filtering by status

Using the filter buttons above the table, you can limit the view to one specific status:

- **All** — all attempts
- **Successful** — successful logins only
- **Failed** — failed attempts only
- **Blocked** — blocked attempts only

Pagination

When there are many log entries, the results are split into pages of 50 per page. At the bottom of the table you will find navigation buttons to browse through the pages.

Setting the retention period

By default, log entries are kept for **30 days**. After that, they are cleaned up automatically. You can change the retention period to a value between **1 and 365 days**.

Change the value in the *Keep log entries for* field and click **Save**.

Clearing the log

Using the **Clear login log** button, you delete all log entries in one go. A confirmation dialogue appears. Please note: this action is **irreversible**.

9. Login form on your own page

By default, Simple OTP Login shows the login form on the standard WordPress login page (`/wp-login.php`). If you want to show the form on a page of your own — for example a page in your own house style — you can use the following shortcode:

```
[simple_otp_login_form]
```

Paste this shortcode into the content of any WordPress page. The form will automatically appear in that location. If the user is already logged in, the shortcode shows a message saying they are already signed in.

Usage:

1. Create a new page (e.g. *Log in*)
2. Add the shortcode `[simple_otp_login_form]` in the editor
3. Publish the page

> **Tip:** You can also use the shortcode in widget areas or in page builders such as Elementor or Divi.

10. Security — how does the protection work?

Simple OTP Login contains several layers of protection against abuse.

One-time codes

Each code works only once. After it has been entered successfully, the code is invalidated immediately. Someone who intercepts the same code can do nothing with it.

Automatic expiry

Each code has a limited validity period (configurable: 5, 10 or 15 minutes). Expired codes are rejected — there is no way to reuse an expired code.

Account lockout after failed attempts

After **5 consecutive incorrect codes**, the user account is automatically locked for **15 minutes**. During the lockout, no new codes can be requested or entered for that account.

IP block

In addition to the account lockout, the visitor’s IP address is also blocked after 5 failed attempts. This prevents someone from trying again with a new account.

Privacy for unknown accounts

When someone requests a code for an email address or username that does not exist, the plugin always shows the same neutral message: "*If this account exists, you will receive an email.*" This prevents attackers from finding out which accounts do exist on your website.

Timing-safe comparison

When checking the code entered, the plugin uses a special method (`hash_equals`) that always takes the same amount of time, regardless of whether the code is right or wrong. This protects against *timing attacks* — attacks in which someone tries to guess whether a code is correct based on the response time.

CSRF protection

All forms are protected with a WordPress *nonce* — a one-time security token that prevents malicious websites from submitting forms on behalf of your visitors.

11. Frequently asked questions

Can users still log in with their password?
No, not when the *Require OTP login* setting is enabled (the default). Password login is then completely blocked. You can change this behaviour in the *General* tab.

What if I accidentally get logged out myself and don’t receive an email?
First check your spam or junk mail folder. If emails consistently fail to arrive, ask your web host or Kyzoe to temporarily deactivate the plugin via FTP or the hosting environment, so that you can log in with your password and solve the email problem.

What if a user no longer has access to their email address?

As an administrator, you can change a user's email address via **Users → All Users** in the WordPress dashboard. The user can then log in with the new address.

Does this also work with WooCommerce or other login forms?The plugin works on the standard WordPress login page. For login forms from WooCommerce or other plugins, we recommend using the shortcode `[simple_otp_login_form]` on a separate page.

Can several users have the same IP address?

Yes, this is possible in office environments or on shared networks. If one user causes an account block, the IP address may be temporarily blocked for all users on that network. You can unblock the IP address manually via the *IP Blocks* tab.

How long are login attempts kept?

30 days by default. You can change this in the *Login Log* tab (configurable from 1 to 365 days).

Is the plugin available in Dutch?

The admin interface is written in English for publication in the WordPress.org directory. You can fully customise the email that users receive in Dutch via the *Email Settings* tab.

Does the plugin work on any WordPress hosting?

Yes, as long as WordPress version 5.8 or higher is running and PHP version 7.4 or higher is available. The plugin does not use any external services — everything runs on your own server.

What happens when the plugin is deleted?

When it is deleted via the WordPress dashboard, all plugin settings, the login log and the database table are cleaned up automatically. Nothing is left behind in your database.

Simple OTP Login is developed and maintained by Kyzoe.