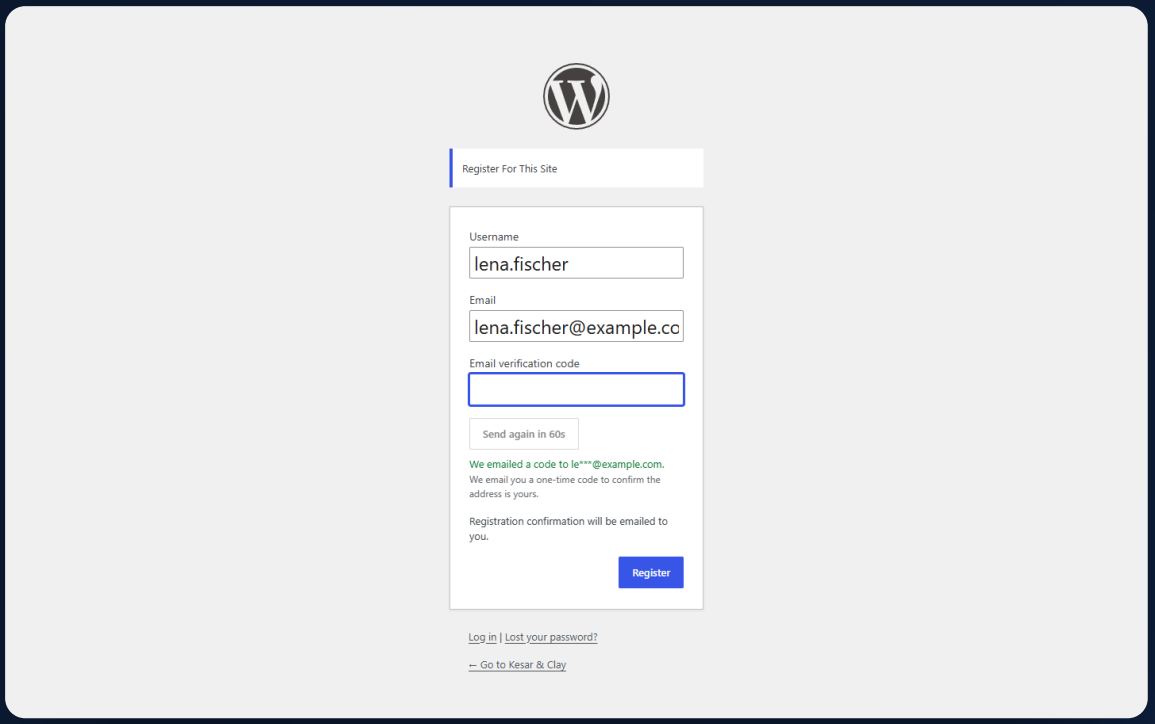
CODE CRAFT
Build. Launch. Grow.

WORDPRESS PLUGIN · USER GUIDE

Codelatch — WordPress OTP Verification & Passwordless Login

Version 1.0.0 · Installation, licence activation, every setting explained, FAQ and troubleshooting.



coodecraft.com/market/product/wp-otp-verification · support: coodecraft.com/contact

Codelatch — OTP Verification & Passwordless Login: user guide

Codelatch adds WordPress OTP verification: one-time codes on registration, login and (Pro) Cash on Delivery checkout. The Free plugin sends codes by email. Pro adds SMS and WhatsApp codes through your own provider account, a COD phone check at checkout, a country code picker with number validation, phone verification and phone login on My Account, a brute-force lockout and a verification log.

---

1. Install

1. In WordPress go to **Plugins** → **Add New** → **Upload Plugin**, choose the Codelatch .zip, click **Install Now**, then **Activate**.
2. Open **Codelatch** → **Settings**.
3. Pro: open **Codelatch** → **Licence**, paste the key from your purchase email and click **Activate licence**. Each licence is for one site.

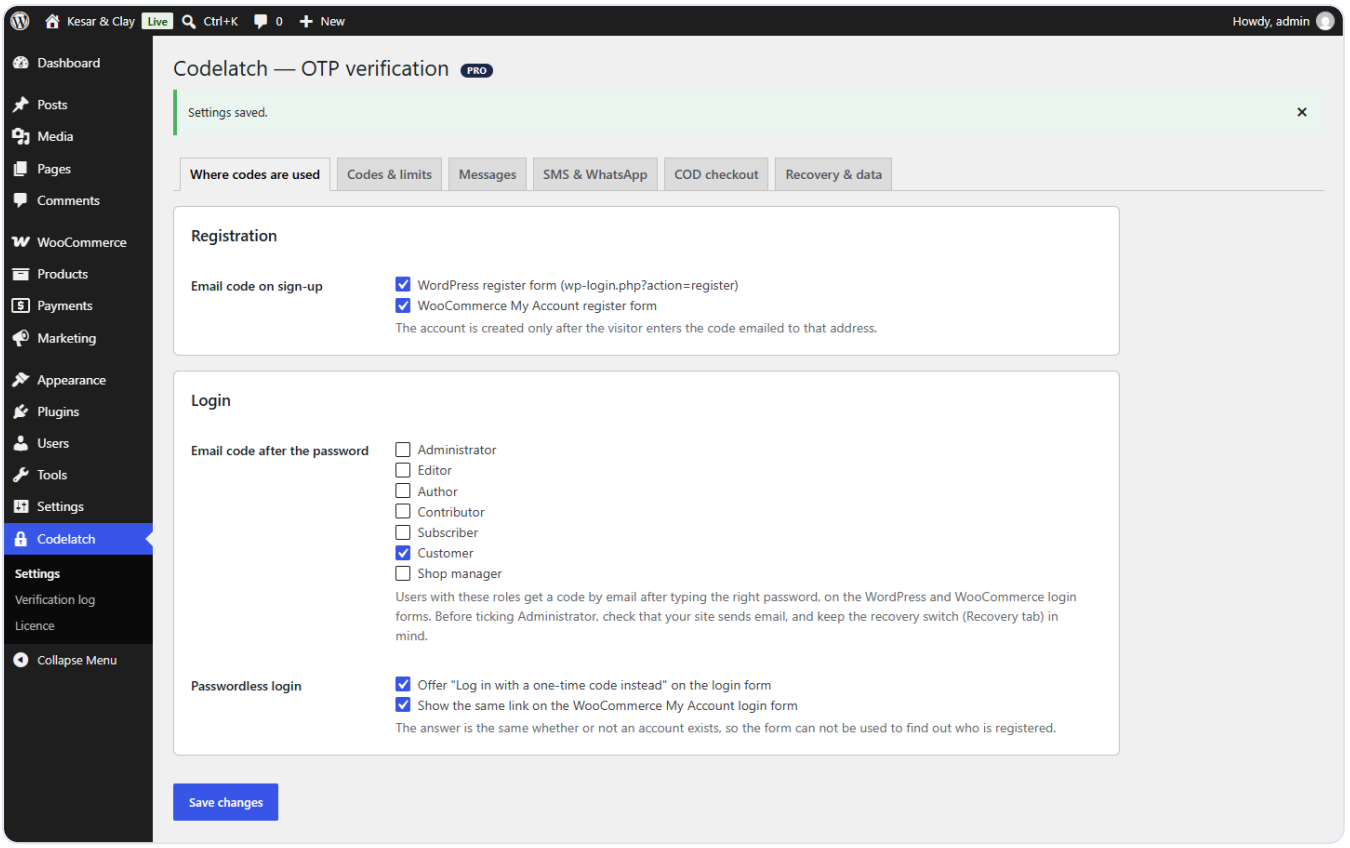
Requirements: WordPress 6.4+, PHP 7.4+. WooCommerce 8.0+ for the WooCommerce forms and the COD check. Tested on WordPress 7.1, PHP 8.3, WooCommerce 10.x/11.x, with a block theme (Twenty Twenty-Five) and a classic theme (Twenty Twenty-One).

Your site must be able to send email for email codes. If you are not sure, install an SMTP plugin and send a test email first.

---

2. Where codes are used (Settings → Where codes are used)

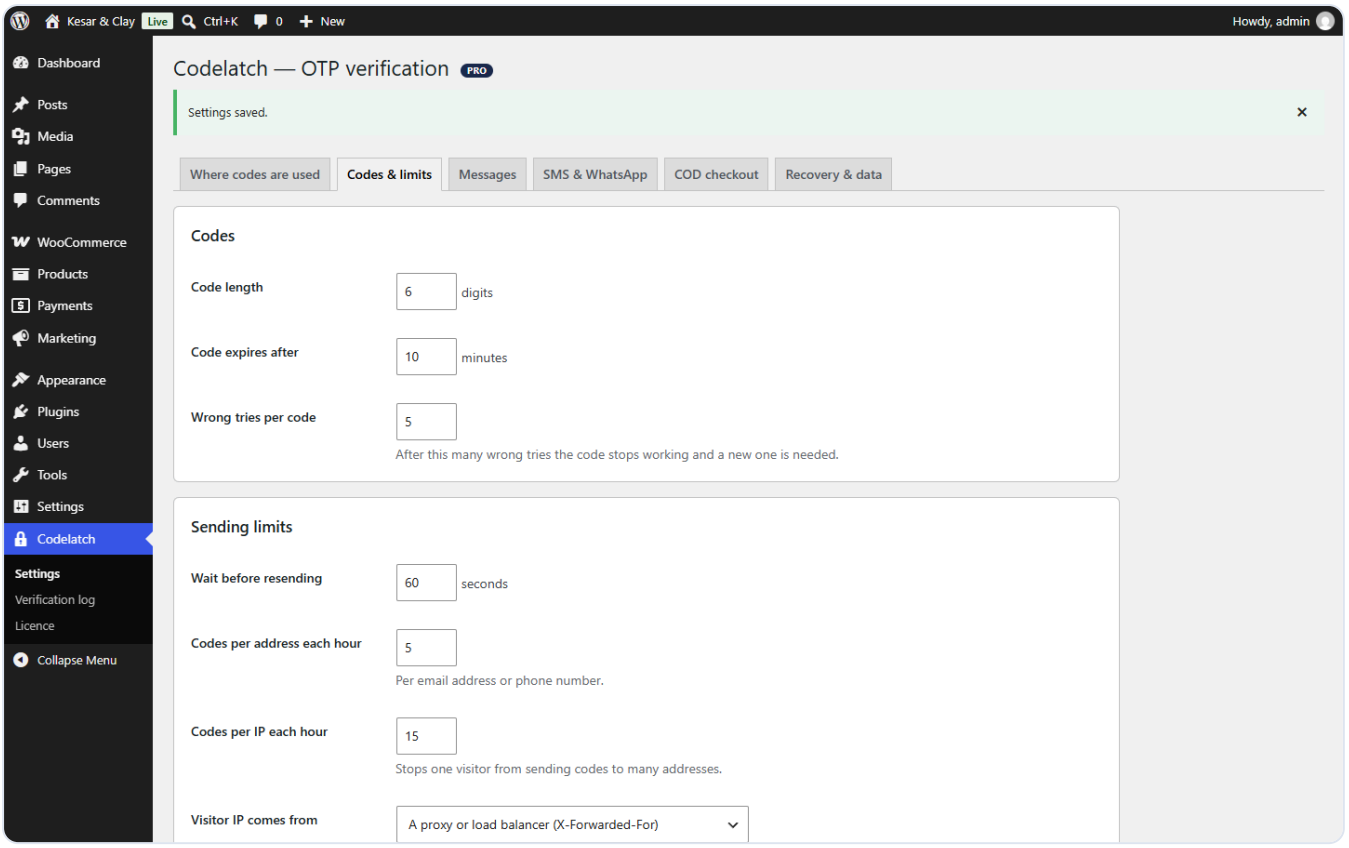
Screenshot:



- **Email code on sign-up** — tick the WordPress register form and/or the WooCommerce My Account register form. The account is created only after the visitor types the code emailed to that address. Codelatch does not send or use up a code until the rest of the form (username, email not yet registered) is fine.
- **Email code after the password** — tick the roles that must enter an emailed code after typing the right password. This works on the WordPress login form and the WooCommerce My Account login form. No login cookie is set until the code is right. Password logins over XML-RPC are refused for these roles; application passwords (REST API) are not affected. Tick Administrator only after you have checked that email arrives, and read section 8.
- **Passwordless login** — adds "Log in with a one-time code instead" under the login form (and, if ticked, under the WooCommerce login form). The visitor types an email address or username and gets a code. The page looks exactly the same whether or not the account exists, and nothing is sent for unknown accounts, so the form can not be used to find out who is registered.

3. Codes & limits

Screenshot:



Setting	Default	What it does
Code length	6 digits	4 to 8 digits
Code expires after	10 minutes	Older codes are refused ("That code has expired")
Wrong tries per code	5	After this many wrong tries the code stops working
Wait before resending	60 seconds	"Please wait N seconds" until then
Codes per address each hour	5	Per email address or phone number
Codes per IP each hour	15	Stops one visitor sending codes to many addresses
Visitor IP comes from	REMOTE_ADDR	Pick Cloudflare or a proxy header only if your site really sits behind it

A newer code replaces the older one, and a used code can never be used again.

How codes are stored: never in plain text. Each code is stored as an HMAC-SHA256 hash with a random salt and checked with a constant-time comparison (hash_equals). Email addresses and phone numbers in the codes table are stored as keyed hashes; the log keeps only masked copies (for example `pr***@example.com`). Code rows are deleted after two days.

Pro: brute-force lockout. After 8 wrong codes within 15 minutes (counted across codes, so asking for a new code does not reset it) the address and the IP are locked for 30 minutes. While locked, no codes are sent to them and none are accepted. All three numbers can be changed.

4. Messages

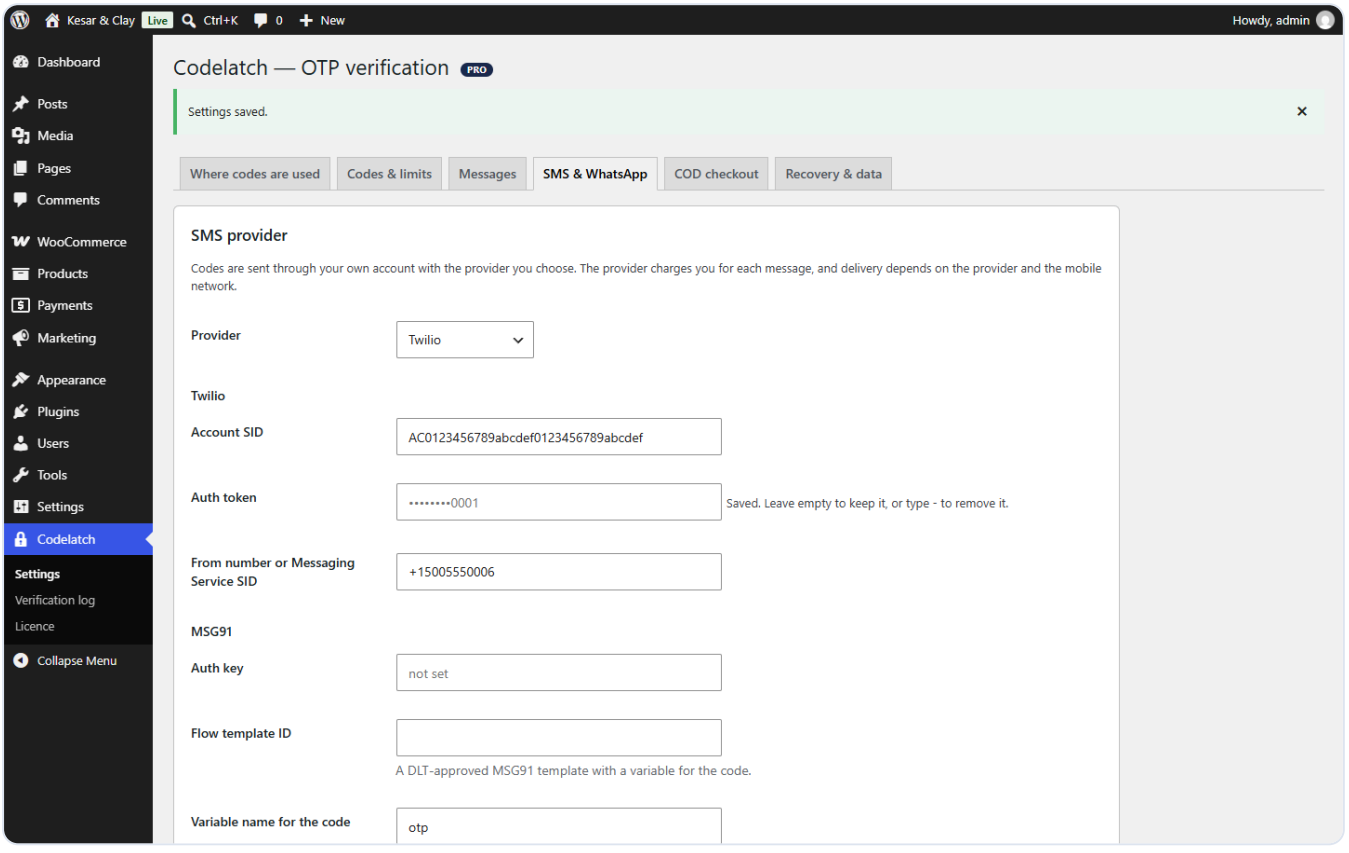
On the **Messages** tab you can write your own email subject and message. Leave them empty to use the built-in text, which is translated into your site language. Placeholders: `{code}`, `{minutes}`, `{site}`. Pro: the SMS text (used by Twilio, Vonage and Plivo). Every message in Codelatch is translatable; the plugin ships a .pot file.

5. What visitors see

- **Registration** (`pro-09-register-code-sent.png`): the visitor fills in the form and clicks **Email me a code** (or just presses Register — without JavaScript the code is sent then). They type the code and press Register again.
- **Login** (`pro-10-login-code-step.png`): after the right password, a code step asks for the emailed code. "Send a new code" sends another one (after the wait).
- **Passwordless** (`pro-11-passwordless-code.png`): "Log in with a one-time code instead" → email or username → code.
- **WooCommerce register form** (`pro-12-woo-register-code.png`): the same code field and button.

6. Pro: SMS & WhatsApp

Screenshot:



Codes are sent through **your own account** with the provider. The provider charges you for each message, and delivery depends on the provider and the mobile network. Keys are stored in a separate option that is not autoloaded and are never shown again in full (only the last 4 characters). Leave a key field empty to keep the saved key; type `-` to remove it.

- **Twilio** — Account SID, Auth token, and a From number or a Messaging Service SID (starting with MG).
- **MSG91** — Auth key, Flow template ID (a DLT-approved template) and the variable name your template uses for the code (default `otp`).
- **Vonage** — API key, API secret, sender ID or number.
- **Plivo** — Auth ID, Auth token, sender number.
- **WhatsApp Cloud API** — phone number ID, a permanent access token, and the name and language of an **approved authentication template**. Tick "copy-code button" if the template has one (authentication templates do). Meta charges per conversation.
- **Default country** — pre-selected in the country picker.
- **Send phone codes by** — SMS or WhatsApp, for My Account phone verification and mobile-number login.

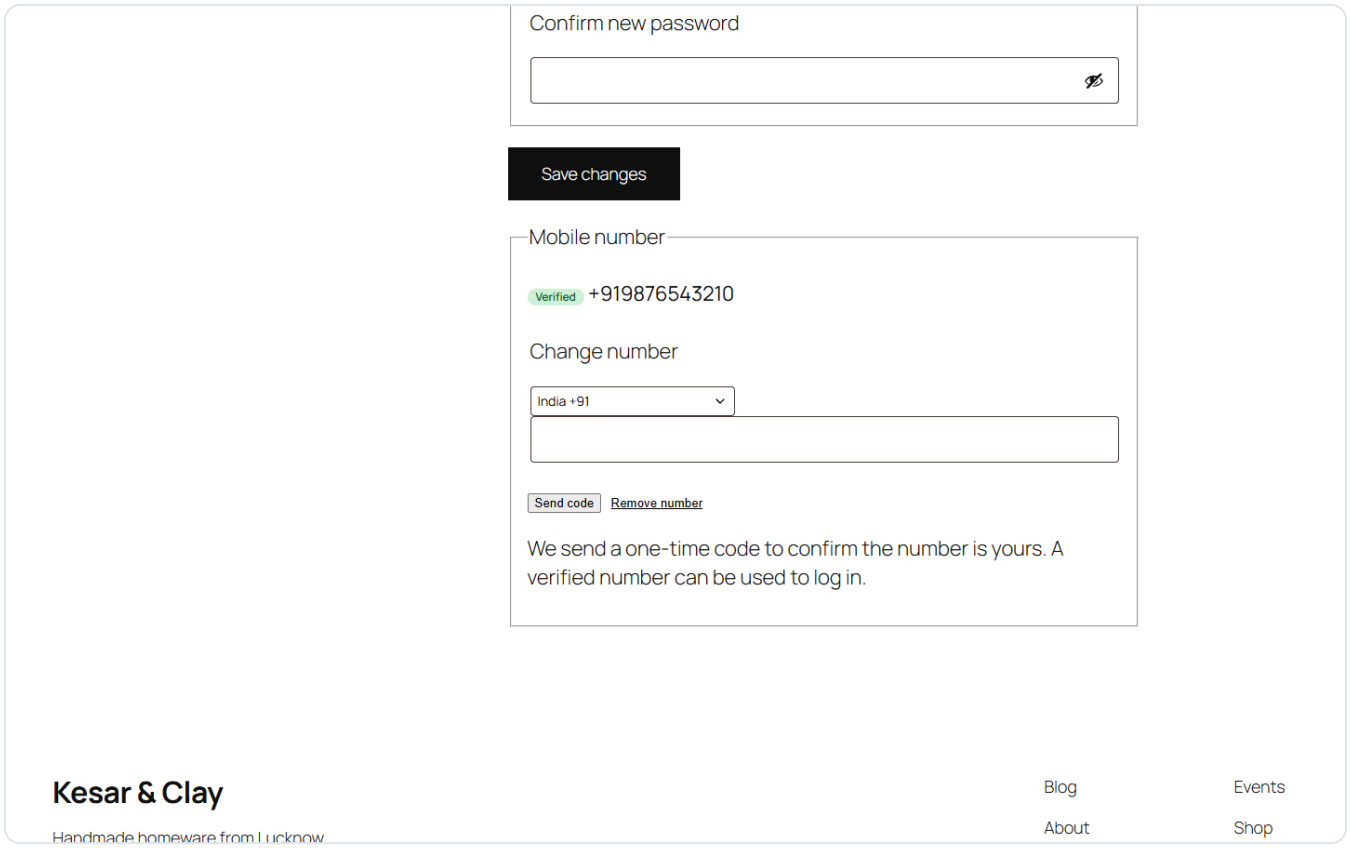
If a provider refuses a message, the visitor sees "We could not send the code right now" and the provider's reply is written to the verification log for you.

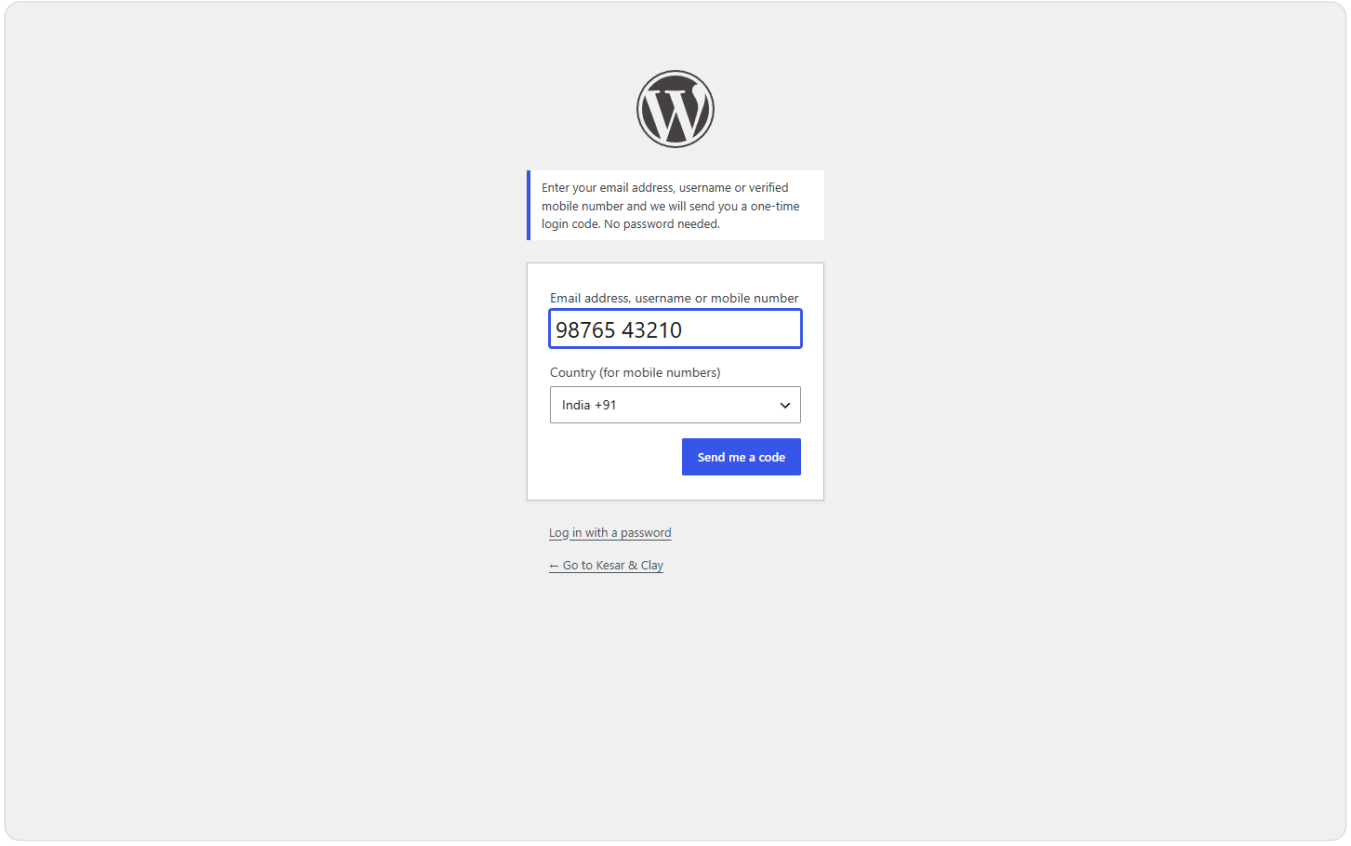
---

7. Pro: phone numbers, My Account and COD checkout

Country picker and validation. Numbers are checked against the country's dialling code and number length and stored in international E.164 format (for example `+919876543210`). A leading 0 (trunk prefix) is removed; numbers typed with `+` or `00` and a country code are accepted whatever country is picked.

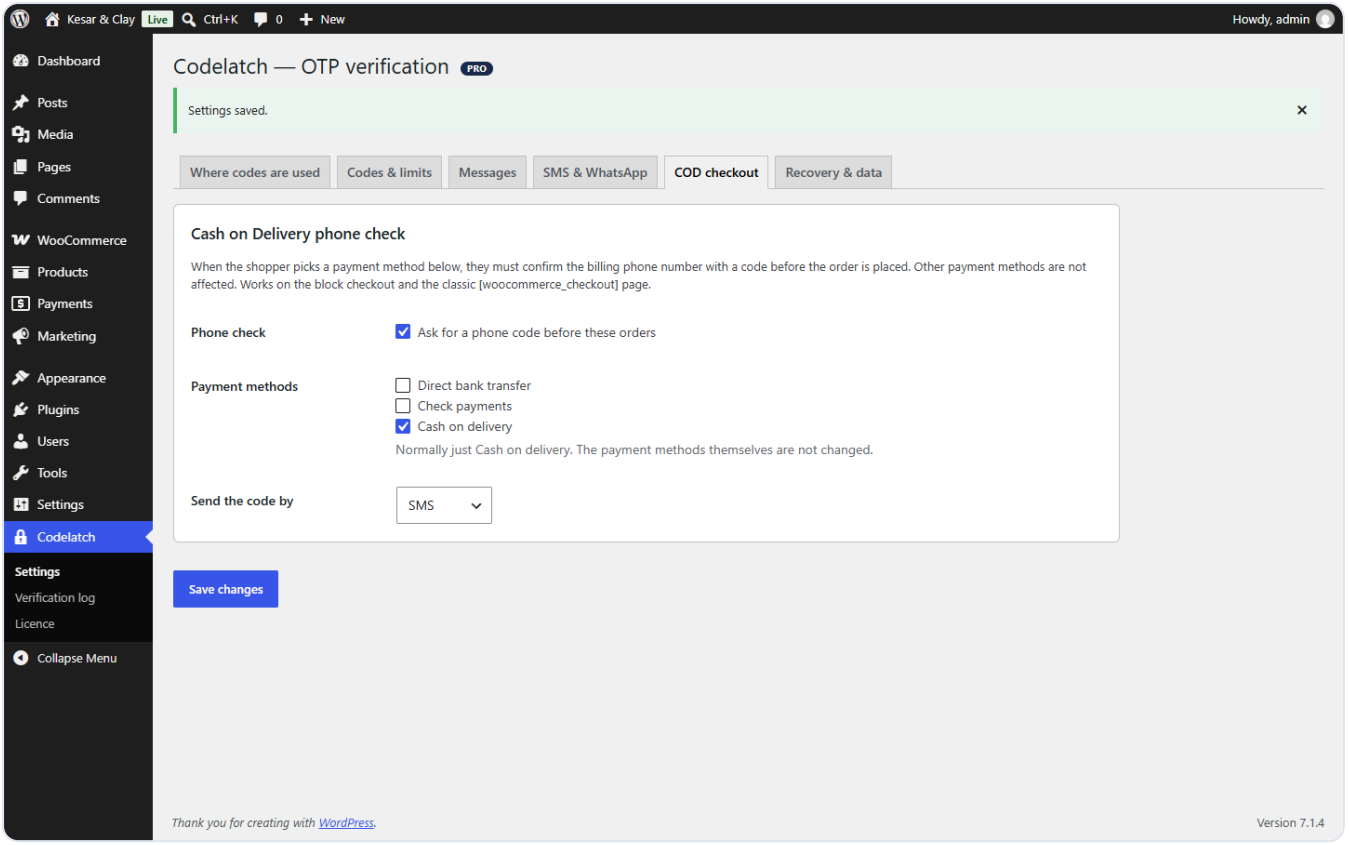
My Account phone ( ): under My Account → Account details, customers pick their country, type their mobile number, click **Send code**, then type the code and click **Verify number**. A number can be verified on one account only. **Mobile-number login** ( ): on the passwordless form customers with a verified number can type it (with the country picker) and get the code by SMS or WhatsApp.

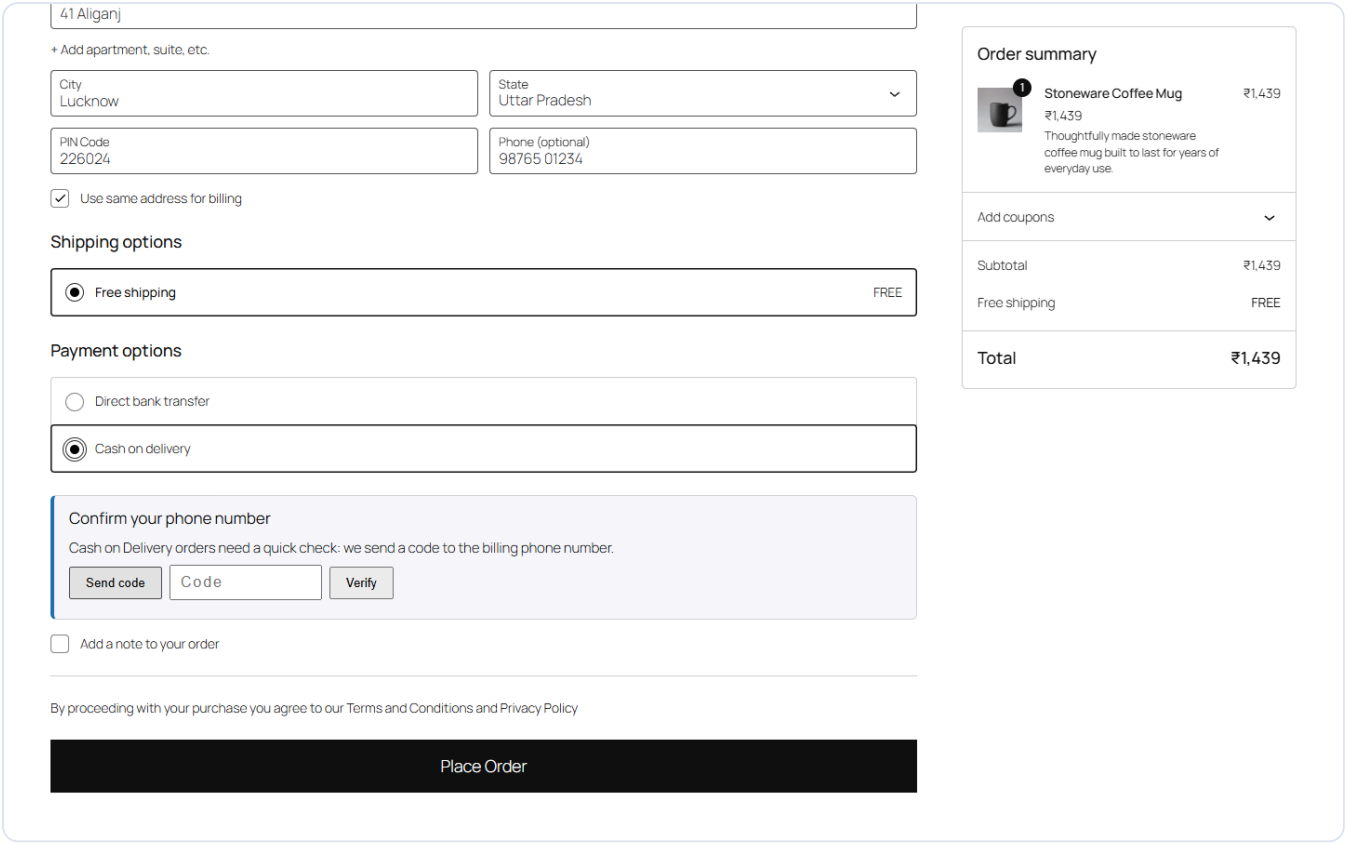


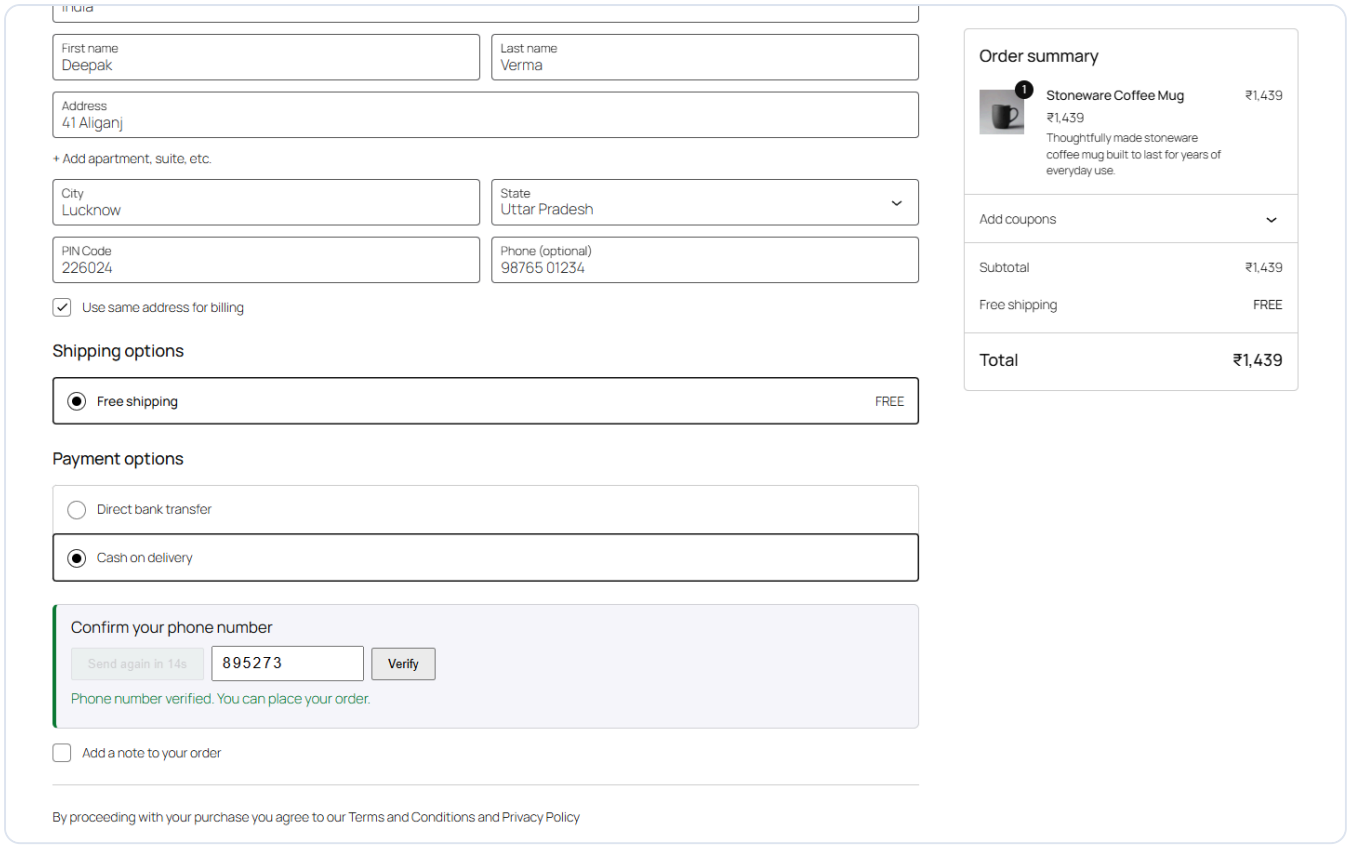


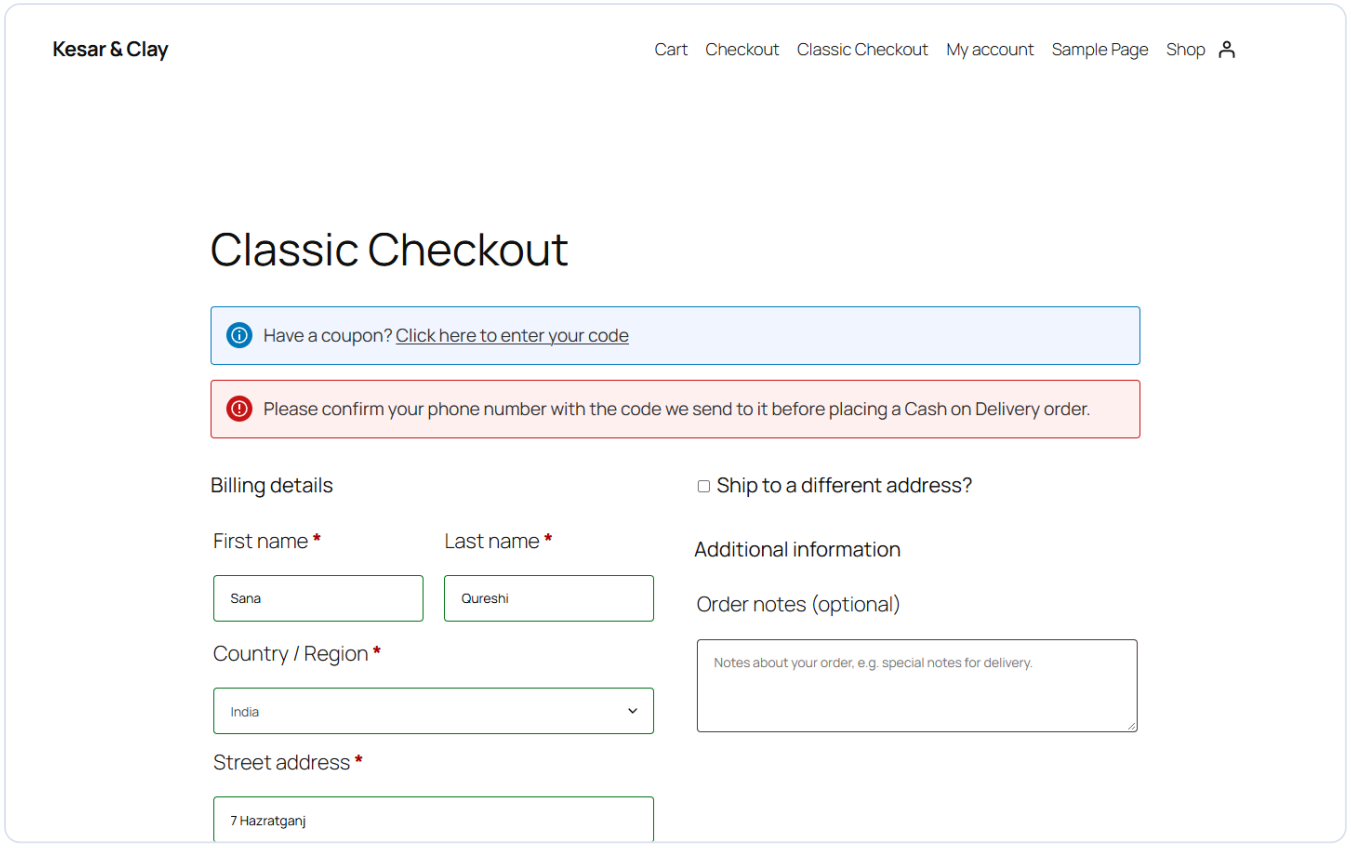
COD checkout (, , ,): on **COD checkout**, tick "Ask for a phone code before these orders", pick the payment methods (normally only Cash on delivery) and the channel. When a shopper picks Cash on delivery, a panel asks them to confirm the billing phone with a code. Until they do, the order is refused with "Please confirm your phone number...". On the classic checkout they can also type the code into the panel and press Place order. Other payment methods (bank transfer, cards...) are not affected and

no payment method's own settings are changed. The order gets a private note and the masked verified number.









8. If you are locked out (recovery)

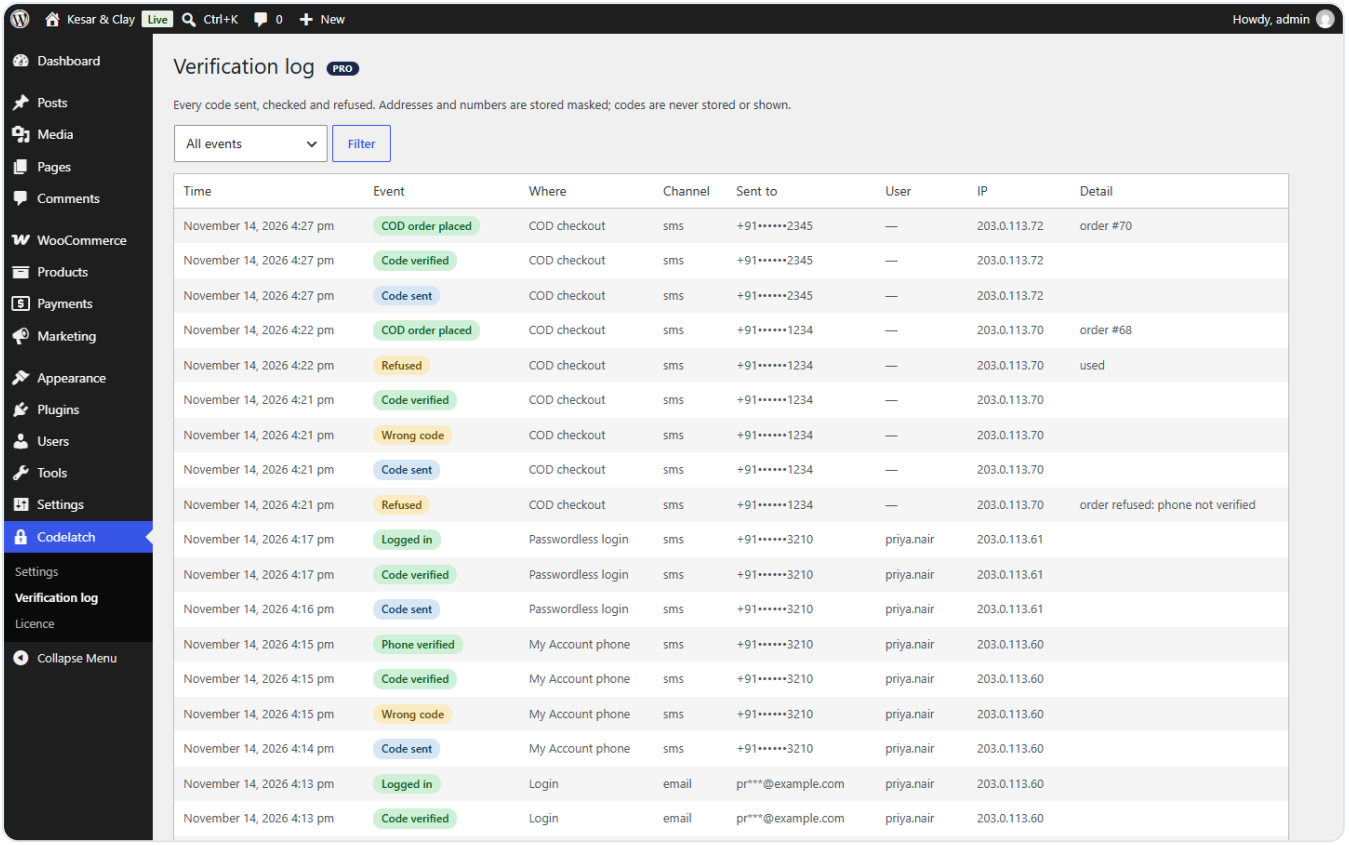
If codes stop arriving and you can not log in, add this line to **wp-config.php** above "That's all, stop editing!":

```
define( 'OGOV_DISABLE', true );
```

While it is there, Codelatch asks for no codes anywhere: you log in with your password, and registration and checkout work as without the plugin. A notice in wp-admin reminds you it is paused. Fix the email or SMS settings, then remove the line.

9. Pro: verification log

Screenshot:



Codelatch → Verification log lists every code sent, verified and refused, wrong codes, rate limits, lockouts, failed sends (with the provider's reply), logins, new accounts, verified phones and COD orders, with masked address, user and IP. Filter by event. Codes are never logged. Entries are kept for 60 days (change on Codes & limits).

10. Licence

Pro unlocks once coodecraft.com confirms your key on **Codelatch → Licence**. Monthly and yearly licences warn you three days before they end. When a licence ends, the Pro features switch off — SMS/WhatsApp sending, the COD check, phone login, lockout and log — while email codes on registration and login, passwordless login and the limits keep working and all settings stay saved. Renew and click **I have paid — check again**.

11. Uninstall

Deleting the plugin removes its data only if you ticked **Delete all plugin data** on the **Recovery & data** tab. Then settings, provider keys, codes, the log and saved phone numbers are removed. Leave it unticked when you swap the Free plugin for Pro.

12. FAQ and troubleshooting

- **No code email arrives.** Check spam, then check that your site sends email at all (an SMTP plugin with a test email helps). Use the recovery line if you are locked out.
- **"Please wait N seconds".** The resend wait is on; wait, or lower it on Codes & limits.
- **"Too many codes were requested".** The hourly limit per address or IP was reached.
- **Caching.** Exclude login, My Account and checkout pages from full-page caching; the forms use WordPress nonces.
- **Not yet supported:** the "create an account" box on the WooCommerce checkout, multisite (not tested), SMS providers other than the four listed.