PrestaWard Authenticator - User guide

0.0.13 | EN | GO ON Agency

PrestaWard Authenticator protects employee Back Office access with TOTP authentication, one-time recovery codes, trusted devices and controls against repeated password or MFA attempts. Enrollment QR codes are generated locally. Keep an authenticator application and a secure recovery-code storage location ready.

Before you begin

PrestaShop 1.7-9 is the declared compatibility range. Use a PHP version supported by your PrestaShop release. First install on a test copy and keep a current database and file backup. You need Back Office module-installation and configuration permissions. In multistore, select the intended shop before changing shop-specific settings.

Install and start safely

1. Upload the purchased ZIP in Modules > Module Manager and install it. Open PrestaWard Authenticator.
2. Keep the module Disabled while checking configuration. Use Audit only before enforcing a policy.
3. Set profile and shop policies, then open My authentication for each affected employee.
4. Confirm the current password, scan the local QR code and validate the code from the authenticator application.
5. Save the recovery codes securely offline. Check a second login before enabling Enforce. Keep an authorized recovery route available.

Configure your protection

Choose Disabled, Audit only or Enforce deliberately. Policies can require, allow or disable MFA by employee profile and shop; the strictest applicable requirement wins. Review password/MFA attempt limits, lockout duration, trusted-device lifetime and password-change trust invalidation. Configure trusted proxies and client-IP headers only if you know your network topology. Incorrect proxy settings can misidentify clients.

Daily operation

Employees use My authentication to manage factors and trusted devices. Use access-log filters and signed export for investigation. Review repeated failures before changing limits. Test alert configuration through the module action; an enabled setting alone does not establish delivery. Never send a password, TOTP secret, QR enrollment image or recovery code to support.

Recovery and troubleshooting

If an employee loses the authenticator, use an unused recovery code through the supported flow. Replace the factor from My authentication with the required current password and existing factor. Emergency recovery is an administrator-controlled procedure; configure and store its key before an incident. Do not edit security tables or weaken policy to bypass a failed login.

Frequently asked questions

Can I sign in after losing my app? Use an unused recovery code and follow the authorized recovery procedure.

Privacy and support

Download support diagnostic from Logs and GO ON support after selecting one shop associated with your employee profile. Edit permission, a valid Back Office token and POST are required. The manual JSON is limited to 256 KiB; it contains allowed runtime/module information and excludes raw logs, personal data and secrets. The report is downloaded on request and is not automatically sent to support. Attach the JSON and your reproduction steps through the purchase platform support channel.

Integrity connectivity is separate from local protection. Network or mail delivery must be checked in your own environment; no online service replaces your backup or recovery plan. Keep PrestaShop, PHP and the module updated. This guide describes the named version, not future SDK fields or unverified integrations.