PrestaWard Authenticator - Benutzerhandbuch

0.0.13 | DE | GO ON Agency

PrestaWard Authenticator schützt Mitarbeiterzugänge zum Back Office mit TOTP, einmaligen Wiederherstellungscodes, vertrauenswürdigen Geräten und Begrenzung wiederholter Anmeldeversuche. QR-Codes werden lokal erzeugt. Halten Sie eine Authenticator-App und einen sicheren Speicherort für Wiederherstellungscodes bereit.

Vorbereitung

Der erklärte Kompatibilitätsbereich ist PrestaShop 1.7-9. Verwenden Sie eine von Ihrer PrestaShop-Version unterstützte PHP-Version. Installieren Sie zuerst auf einer Testkopie und sichern Sie Datenbank und Dateien. Sie benötigen Rechte für Modulinstallation und Konfiguration. Wählen Sie bei mehreren Shops den richtigen Shop vor Änderungen.

Sicher installieren und starten

1. Installieren Sie das gekaufte ZIP über Module > Modulmanager und öffnen Sie PrestaWard Authenticator.
2. Lassen Sie das Modul bei der Einrichtung deaktiviert. Nutzen Sie zunächst den Audit-Modus.
3. Legen Sie Profil- und Shop-Richtlinien fest. Öffnen Sie die persönliche Authentifizierungsseite jedes betroffenen Mitarbeiters.
4. Bestätigen Sie das aktuelle Passwort, scannen Sie den lokalen QR-Code und bestätigen Sie einen App-Code.
5. Speichern Sie Wiederherstellungscodes offline. Prüfen Sie eine weitere Anmeldung vor der Durchsetzung und behalten Sie einen autorisierten Wiederherstellungsweg.

Schutz konfigurieren

Wählen Sie deaktiviert, Audit oder Durchsetzung bewusst. MFA kann nach Profil und Shop erforderlich, optional oder deaktiviert sein; die strengste passende Anforderung gilt. Prüfen Sie Passwort-/MFA-Limits, Sperrdauer, Gerätevertrauen und dessen Widerruf bei Passwortänderung. Vertrauenswürdige Proxys und IP-Header nur bei bekannter Netzwerktopologie konfigurieren.

Tägliche Nutzung

Mitarbeiter verwalten Faktoren und Geräte auf ihrer Authentifizierungsseite. Nutzen Sie Protokollfilter und signierten Export. Prüfen Sie Fehler vor einer Limitänderung. Testen Sie E-Mail über die Modulaktion; Aktivierung beweist keine Zustellung. Keine Passwörter, TOTP-Geheimnisse, QR-Bilder oder Wiederherstellungscodes an Support senden.

Wiederherstellung und Fehlerbehebung

Bei Verlust der App nutzen Sie einen unbenutzten Wiederherstellungscode. Faktorwechsel benötigen das aktuelle Passwort und den geforderten Faktor. Notfallwiederherstellung ist ein administratives Verfahren; richten Sie den Schlüssel vorher ein und schützen Sie ihn. Keine Sicherheitstabellen ändern oder Richtlinien umgehen.

Häufige Fragen

Kann ich mich nach Verlust der App anmelden? Verwenden Sie einen unbenutzten Wiederherstellungscode und das autorisierte Wiederherstellungsverfahren.

Datenschutz und Support

Laden Sie die Supportdiagnose im GO ON-Supportbereich für einen Ihrem Mitarbeiter zugeordneten Shop herunter. Bearbeitungsrecht, gültiger Token und POST sind erforderlich. Das manuelle JSON ist auf 256 KiB begrenzt und enthält keine Rohprotokolle, persönlichen Daten oder Geheimnisse. Der Bericht wird auf Anfrage heruntergeladen und nicht automatisch an den Support gesendet. Übermitteln Sie JSON und Reproduktionsschritte über den Supportkanal Ihrer Kaufplattform.

Integrity ist von lokalem Schutz getrennt. Prüfen Sie Netzwerk und E-Mail-Zustellung in Ihrer Umgebung. Kein Dienst ersetzt Backups oder Wiederherstellung. Halten Sie PrestaShop, PHP und Modul aktuell. Diese Anleitung beschreibt die genannte Version, keine künftigen SDK-Felder oder ungeprüften Integrationen.