



PrestaWard Authenticator | 0.0.13 | FR

PrestaWard Authenticator - Guide utilisateur

0.0.13 | FR | GO ON Agency

PrestaWard Authenticator protège les accès employés au Back Office avec TOTP, codes de récupération à usage unique, appareils de confiance et limitation des tentatives répétées. Les QR sont générés localement. Préparez une application d'authentification et un stockage sécurisé des codes.

Avant de commencer

La compatibilité déclarée couvre PrestaShop 1.7-9. Utilisez une version PHP prise en charge par votre version de PrestaShop. Commencez sur une copie de test et sauvegardez la base de données et les fichiers. Les droits d'installation et de configuration sont nécessaires. En multiboutique, sélectionnez la boutique concernée.

Installer et démarrer en sécurité

- 1 Installez le ZIP acheté dans Modules > Gestionnaire de modules et ouvrez PrestaWard Authenticator.
- 2 Conservez le mode Désactivé pendant la configuration, puis utilisez Audit uniquement.
- 3 Définissez les politiques par profil et boutique. Ouvrez l'authentification personnelle de chaque employé concerné.
- 4 Confirmez le mot de passe actuel, scannez le QR local et validez un code de l'application.
- 5 Conservez les codes de récupération hors ligne. Testez une nouvelle connexion avant d'imposer MFA et gardez une procédure de récupération autorisée.

Configurer la protection

Choisissez Désactivé, Audit uniquement ou Imposer délibérément. MFA peut être requis, facultatif ou désactivé par profil et boutique; l'exigence la plus stricte s'applique. Vérifiez limites de tentatives, verrouillage, confiance des appareils et invalidation après changement de mot de passe. Configurez les proxies et en-têtes IP uniquement avec une connaissance précise du réseau.

Utilisation quotidienne

Les employés gèrent facteurs et appareils dans leur page d'authentification. Utilisez filtres et export signé des journaux. Examinez les échecs avant de modifier les limites. Testez les e-mails par l'action du module; une option active ne prouve pas la livraison. Ne transmettez aucun mot de passe, secret TOTP, QR ou code de récupération.

Récupération et dépannage

En cas de perte de l'application, utilisez un code de récupération inutilisé. Remplacez le facteur avec le mot de passe actuel et le facteur exigé. La récupération d'urgence est administrative; configurez et protégez sa clé avant un incident. Ne modifiez pas les tables de sécurité pour contourner une connexion.

Questions fréquentes

Puis-je me connecter après avoir perdu mon application ? Utilisez un code de récupération inutilisé et la procédure de récupération autorisée.

Confidentialité et assistance

Téléchargez le diagnostic dans le panneau GO ON après sélection d'une boutique associée à votre employé. Droits de modification, token valide et POST sont nécessaires. Le JSON manuel est limité à 256 KiB et exclut journaux bruts, données personnelles et secrets. Le rapport est téléchargé sur demande et n'est pas envoyé automatiquement au support. Joignez JSON et étapes de reproduction au support de la plateforme d'achat.

Integrity est distinct de la protection locale. Vérifiez réseau et livraison des e-mails dans votre environnement; aucun service ne remplace sauvegarde ou récupération. Maintenez PrestaShop, PHP et le module à jour. Ce guide décrit la version indiquée, pas des champs SDK futurs ou intégrations non vérifiées.