



PrestaWard Authenticator | 0.0.13 | ES

PrestaWard Authenticator - Guía de usuario

0.0.13 | ES | GO ON Agency

PrestaWard Authenticator protege el acceso de los empleados al Back Office con autenticación TOTP, códigos de recuperación de un solo uso, dispositivos de confianza y controles de intentos repetidos. El QR se genera localmente. Prepare una aplicación de autenticación y un lugar seguro para los códigos de recuperación.

Antes de comenzar

La compatibilidad declarada comprende PrestaShop 1.7-9. Utilice una versión de PHP admitida por su versión de PrestaShop. Instale primero en una copia de prueba y conserve una copia de seguridad actual de la base de datos y los archivos. Necesita permisos de instalación y configuración de módulos. En multitienda, seleccione la tienda correspondiente antes de cambiar sus ajustes.

Instalar y comenzar de forma segura

- 1 Suba el ZIP adquirido en Módulos > Gestor de módulos, instálelo y abra PrestaWard Authenticator.
- 2 Mantenga el modo Desactivado durante la configuración. Utilice Solo auditoría antes de imponer una política.
- 3 Defina políticas por perfil y tienda. Abra Mi autenticación para cada empleado afectado.
- 4 Confirme la contraseña actual, escanee el QR local y valide el código de la aplicación.
- 5 Guarde los códigos de recuperación sin conexión. Compruebe otro inicio de sesión antes de activar el modo obligatorio y conserve una vía de recuperación autorizada.

Configurar la protección

Elija Desactivado, Solo auditoría u Obligatorio de forma deliberada. Las políticas por perfil y tienda pueden exigir, permitir o desactivar MFA; prevalece el requisito más estricto. Revise los límites de intentos de contraseña y MFA, bloqueo, duración de confianza e invalidación tras cambiar la contraseña. Configure proxies de confianza y cabeceras de IP solo si conoce la red: un ajuste incorrecto puede identificar mal al cliente.

Uso diario

Cada empleado gestiona sus factores y dispositivos desde Mi autenticación. Utilice filtros y exportación firmada de registros para investigar. Revise los fallos antes de cambiar límites. Pruebe el correo con la acción del módulo: activarlo no demuestra su entrega. No envíe contraseñas, secretos TOTP, imágenes QR ni códigos de recuperación al soporte.

Recuperación y resolución de problemas

Si pierde el autenticador, utilice un código de recuperación no usado mediante el flujo disponible. Sustituya el factor desde Mi autenticación con la contraseña actual y el factor requerido. La recuperación de emergencia es un procedimiento administrativo: configure y proteja su clave antes de un incidente. No modifique tablas ni debilite políticas para evitar un fallo de acceso.

Preguntas frecuentes

¿Puedo acceder si pierdo la aplicación? Use un código de recuperación sin utilizar y siga el procedimiento de recuperación autorizado.

Privacidad y soporte

Descargue el diagnóstico desde Logs y soporte de GO ON seleccionando una tienda asociada a su empleado. Se requieren permiso de edición, token válido y POST. El JSON manual está limitado a 256 KiB y excluye registros en bruto, datos personales y secretos. El informe se descarga a petición y no se envía automáticamente a soporte. Adjunte el JSON y los pasos de reproducción al canal de soporte de la plataforma de compra.

La conectividad Integrity es independiente de la protección local. Compruebe red y entrega de correo en su entorno; ningún servicio sustituye la copia de seguridad o recuperación. Mantenga PrestaShop, PHP y el módulo actualizados. Esta guía describe la versión indicada, no campos futuros del SDK ni integraciones sin verificar.