



Guía de usuario — PrestaWard Authenticator

Instalación, configuración y despliegue seguro de la versión 0.0.8 en equipos con varios empleados.

PDF público:

<https://go-onagency.es/prestaward-authenticator/prestaward-authenticator-user-guide.pdf>

Soporte:

hola@go-onagency.es

Página del producto:

<https://go-onagency.es/modulos/prestaward-authenticator/>

Actualizado:

31/07/2026

Qué protege

PrestaWard Authenticator añade un segundo factor TOTP al Back Office de PrestaShop. Incluye códigos personales de recuperación, recuperación de emergencia por consola, respaldo opcional por email, límites independientes para contraseña y MFA, políticas por perfil y tienda, dispositivos de confianza revocables y registros encadenados.

Responsabilidades separadas: el administrador controla la política global, el despliegue, las alertas y los registros. Cada empleado configura y mantiene únicamente su propia autenticación desde «Mi autenticación».

Compatibilidad verificada

PrestaShop	PHP	Validación
1.7.8.11	7.4	Instalación, actualización, TOTP, multitienda, recuperación, correo real, registros y permisos.
8.2.7	8.1	Instalación, actualización, TOTP, multitienda, recuperación, correo real, registros y permisos.
9.1.4	8.5	Instalación, actualización, TOTP, multitienda, recuperación, correo real, registros y permisos.

Flujo de implantación recomendado

1. Realiza una copia de seguridad de la tienda y de la base de datos.

2. Instala el ZIP desde el Gestor de módulos y mantén el modo **Desactivado**.
3. Configura la política predeterminada y las reglas por perfil y tienda.
4. Genera la clave de emergencia y guárdala fuera de PrestaShop.
5. Cada empleado configura TOTP en su propia cuenta y guarda los códigos de recuperación.
6. El administrador revisa el estado del equipo desde el panel administrativo.
7. Activa **Solo auditoría** y comprueba los accesos y las alertas.
8. Activa **Forzar** cuando la recuperación y el acceso de todo el equipo estén comprobados.

No actives el modo forzado de forma inmediata. Primero comprueba un inicio de sesión real y conserva al menos un método de recuperación fuera de la tienda.

Capturas verificadas en PrestaShop 1.7, 8 y 9

PrestaShop

203.0.113

Acceso rápido

Buscar

Modo depuración

Ver mi tienda

Inicio

VENDER

Pedidos

Catalogo

Cientes

Servicio al Cliente

Estadísticas

PERSONALIZAR

Modulos

Diseño

Transporte

Pago

Internacional

Marketing

CONFIGURAR

Parametros de la tienda

Parametros Avanzados

PRESTAWARD SNAPSHOT

Dashboard

PRESTAWARD AUTHENTICATOR

Mi autentificación

¡Lanza tu tienda!

0%

RESUMEN

Detener módulo Primeros pasos

PRESTAWARD AUTHENTICATOR / Administracion MFA

Ayuda

SEGURIDAD DEL BACK OFFICE DE PRESTASHOP

PrestaWard Authenticator

Base MFA para Back Office con TOTP, códigos de recuperación, dispositivos de confianza, logs y alertas por email.

Protege el acceso de los empleados manteniendo el despliegue y la recuperacion bajo control administrativo.

Ver página del producto

Guía de usuario PDF

GO ON AGENCY

Diseño de producto, ingeniería PrestaShop y operaciones ecommerce.

go-onagency.es

hola@go-onagency.es

MODO MFA

Desactivado

Valor seguro por defecto

EMPLEADOS CONFIGURADOS

0

Empleados con TOTP confirmado

EMPLEADOS CON TOTP CONFIRMADO

0

Passkey/WebAuthn queda en el roadmap.

ACTIVAR ALERTAS POR EMAIL

Sí

-

Valor seguro por defecto.

En modo forzado, los empleados sin TOTP son redirigidos a Mi autentificación hasta completar la configuración.

Actualizaciones del módulo

Todavía no se ha realizado ninguna comprobación de actualizaciones.

Versión instalada: 0.0.8

COMPROBAR ACTUALIZACIONES

Ver página del producto

Guía de usuario PDF

La comprobación descarga unicamente el manifiesto publico. No se envia telemetria ni informacion de la tienda.

Panel administrativo real en PrestaShop 1.7.

La comprobación descarga únicamente el manifiesto público. No se envía telemetría ni información de la tienda.

ESTASHOP

9.1.4

Acceso rápido

Buscar

Modo depuración

Ver mi tienda

BIENVENIDO

Inicio

Care Center

VENDER

Pedidos

Catálogo

Cientes

Servicio al Cliente

Estadísticas

PERSONALIZAR

Módulos

Diseño

Transporte

Pago

Internacional

Marketing

CONFIGURAR

Parámetros de la tienda

Parámetros Avanzados

COMUNIDAD

Muro de la fama

Administración MFA

Ayuda



SEGURIDAD DEL BACK OFFICE DE PRESTASHOP

PrestaWard Authenticator

Base MFA para Back Office con TOTP, códigos de recuperación, dispositivos de confianza, logs y alertas por email.

Protege el acceso de los empleados manteniendo el despliegue y la recuperación bajo control administrativo.

Ver página del producto

Guía de usuario PDF



GO ON Agency

Diseño de producto, ingeniería PrestaShop y operaciones ecommerce.

go-onagency.es

hola@go-onagency.es

MODO MFA

Desactivado

Valor seguro por defecto

EMPLEADOS CONFIGURADOS

0

Empleados con TOTP confirmado

EMPLEADOS CON TOTP CONFIRMADO

0

Passkey/WebAuthn queda en el roadmap.

ACTIVAR ALERTAS POR EMAIL

Sí

-

Valor seguro por defecto. En modo forzado, los empleados sin TOTP son redirigidos a Mi autenticación hasta completar la configuración.

Actualizaciones del módulo

Todavía no se ha realizado ninguna comprobación de actualizaciones.

Versión instalada: 0.0.8

200

@admin_legacy_controller_r

n/a ms

20.0 MiB

↓ 3

1197

348 in 9.84 ms

11

lab-ps9@go-onagency.es

52 ms

9 in 47 ms

13 in 8.95 ms

Hooks (5)

Commands / Queries

P 9.1.4

Panel administrativo real en PrestaShop 9.



SEGURIDAD DEL BACK OFFICE DE PRESTASHOP

PrestaWard Authenticator

Base MFA para Back Office con TOTP, códigos de recuperación, dispositivos de confianza, logs y alertas por email.

Protege el acceso de los empleados manteniendo el despliegue y la recuperación bajo control administrativo.

Ver página del producto

Guía de usuario PDF



GO ON Agency

Diseño de producto, ingeniería PrestaShop y operaciones ecommerce.

go-onagency.es

hola@go-onagency.es

Cabecera administrativa con accesos al producto, la guía y el soporte.

MODO MFA

Desactivado

Valor seguro por defecto

EMPLEADOS CONFIGURADOS

0

Empleados con TOTP confirmado

EMPLEADOS CON TOTP CONFIRMADO

0

Passkey/WebAuthn queda en el roadmap.

ACTIVAR ALERTAS POR EMAIL

Sí

-

Resumen del modo MFA, empleados configurados, TOTP y alertas.

Actualizaciones del módulo

 **Todavía no se ha realizado ninguna comprobación de actualizaciones.**
Versión instalada: 0.0.8

 **COMPROBAR ACTUALIZACIONES**

[Ver página del producto](#)

[Guía de usuario PDF](#)

La comprobación descarga únicamente el manifiesto público. No se envía telemetría ni información de la tienda.

Estado del comprobador de versiones y enlaces de publicación.

Política global. Solo los administradores autorizados pueden cambiar esta configuración.

MFA y avisos

Intentos y bloqueos

Red e IP

Modo MFA

Desactivado ▾

Días de dispositivo de confianza

30

Después de cambiar una contraseña

Invalidar tras cualquier cambio de contraseña ▾

La invalidación revoca los dispositivos de confianza, los retos pendientes y las sesiones MFA verificadas del empleado.

Política predeterminada de los perfiles de empleado

Obligatorio ▾

 Políticas de los perfiles de empleado

Un perfil opcional exige MFA desde que el empleado se enrola. En multitienda, una tienda solo puede hacer más estricta la política efectiva.

PERFIL DE EMPLEADO

POLITICA GLOBAL

SuperAdmin Protegido

Obligatorio ▾

Encargado de logística

Heredar ▾

Traductor

Heredar ▾

Vendedor

Heredar ▾

Destinatarios de email

alertas@tutienda.es

Códigos de recuperación por email

Desactivado ▾

El email es un método de respaldo, no sustituye a TOTP. Para activarlo es necesario completar correctamente una prueba del transporte.

Activar alertas por email

☒ SI

Email al acceder correctamente

☐

Email cuando falla el acceso

☒**Transporte de correo de PrestaShop:** SMTP · smtp.office365.com:587

La entrega depende de la configuración de correo de PrestaShop.

 Origen de las actualizaciones

URL del manifiesto de actualizaciones

https://go-onagency.es/prestaward-authenticator/manifest.json

Se utiliza únicamente para consultar el manifiesto público de actualizaciones. No se envían datos de la tienda.

Enviar email de prueba

Guardar configuración

MFA, alertas y estado del transporte de correo.

Política global. Solo los administradores autorizados pueden cambiar esta configuración.

MFA y avisos

Intentos y bloqueos

Red e IP

Protección del acceso

Los límites se aplican a las contraseñas y los códigos MFA del Back Office. No afectan a clientes ni servicios web.

Intentos de contraseña por IP e identificador	5
Intentos de contraseña por IP	10
Ventana de intentos de contraseña (minutos)	15
Duración del bloqueo de contraseña (minutos)	15
Intentos MFA por IP y empleado	5
Ventana de intentos MFA (minutos)	5
Duración del bloqueo MFA (minutos)	15
Conservación de intentos (días)	90
Conservación de registros de acceso (días)	180

Origen de las actualizaciones

URL del manifiesto de actualizaciones	https://go-onagency.es/prestaward-authenticator/manifest.json
---------------------------------------	--

Se utiliza únicamente para consultar el manifiesto público de actualizaciones. No se envían datos de la tienda.

Límites independientes para contraseña y segundo factor.

Política global. Solo los administradores autorizados pueden cambiar esta configuración.

MFA y avisos

Intentos y bloqueos

Red e IP

Política de red y proxy

Solo se confía en una cabecera de IP reenviada cuando el origen directo es un proxy configurado expresamente.

CIDR de proxies de confianza

192.0.2.0/24
2001:db8::/32

Introduce una regla IPv4, IPv6 o CIDR por línea.

Cabecera de IP del cliente

X-Real-IP

Lista permitida para el límite de contraseña

192.0.2.0/24
2001:db8::/32

Introduce una regla IPv4, IPv6 o CIDR por línea.

Lista de IP bloqueadas

192.0.2.0/24
2001:db8::/32

Introduce una regla IPv4, IPv6 o CIDR por línea.

Origen de las actualizaciones

URL del manifiesto de actualizaciones

https://go-onagency.es/prestaward-authenticator/manifest.json

Se utiliza unicamente para consultar el manifiesto publico de actualizaciones. No se envian datos de la tienda.

Enviar email de prueba

Guardar configuración

Proxies de confianza y reglas de red IPv4, IPv6 y CIDR.

Recuperación de emergencia

La clave de recuperacion de un solo uso autoriza un comando de consola que restablece el MFA de un empleado y obliga a realizar un nuevo enrolamiento. No desactiva el modulo.

No hay ninguna clave de recuperación de emergencia activa.

Contraseña actual

Generar clave de emergencia

Recuperación de emergencia con clave de un solo uso y uso exclusivo por consola.

Despliegue por empleados

ID	EMPLEADO	EMAIL	TOTP	CODIGOS DE RECUPERACION	ACTIVO
1	Empleado de prueba	empleado@tutienda.es	No	0	Si

Seguimiento del despliegue MFA por empleado.

Registros de acceso

Exportar registros firmados

✓ Integridad de los registros verificada. 3 registros encadenados comprobados.

Desde	Hasta	Empleado o email	Evento
dd/mm/yyyy	dd/mm/yyyy		Todos
Resultado	IP	Filas por página	
Todos		25	
APLICAR FILTROS Limpiar filtros			

Mostrando del 1 al 3 de 3 registros.

ID	FECHA	EMAIL	EVENTO	RESULTADO	MENSAJE	IP
3	Empleado de prueba	empleado@tutienda.es	Inicio de sesion detectado	Informacion	El inicio de sesion del Back Office llego al control MFA.	203.0.113.24
2	Empleado de prueba	empleado@tutienda.es	Inicio de sesion detectado	Informacion	El inicio de sesion del Back Office llego al control MFA.	203.0.113.24
1	Empleado de prueba	empleado@tutienda.es	upgrade_fixture	Correcto	Upgrade preservation fixture.	203.0.113.24

Registros encadenados, exportación firmada, filtros y paginación.



PRESTAWORD
Authenticator

AUTOSERVICIO DEL EMPLEADO

Mi autenticación

Configura y manten MFA unicamente para tu propia cuenta del Back Office.



GO ON Agency
go-onagency.es
hola@go-onagency.es

Cabecera de «Mi autenticación», el autoservicio del empleado.

PROTECCIÓN DE LA CUENTA

Tu seguridad MFA

- 1 Confirmar contraseña
- 2 Escanear código QR
- 3 Confirmar código de autenticación
- 4 Guardar códigos de recuperación

Protege tu propia cuenta del Back Office antes de activar el modo forzado.

Contraseña actual

Verificaremos tu contraseña antes de mostrar el código QR.

Configuración personal del autenticador.



GO ON AGENCY

ACCESO SEGURO

La contraseña es correcta. Completa el segundo paso para entrar en el Back Office.

Contraseña verificada

2

Código de autenticación

Introduce el código de seis dígitos de tu aplicación de autenticación o un código de recuperación sin usar.

Código de autenticación o recuperación

Código de seis dígitos o código de recuperación



Confiar en este navegador después de verificar MFA

Utiliza esta opción únicamente en un dispositivo privado bajo tu control.

Continuar al Back Office

Puedes utilizar una vez un código de recuperación si no tienes acceso a tu aplicación de autenticación.

Segundo paso de acceso en español, mostrado después de verificar la contraseña en PrestaShop 1.7.



GO ON AGENCY

ACCESO SEGURO

Contraseña verificada

La contraseña es correcta. Completa el segundo paso para entrar en el Back Office.

2

Código de autenticación

Introduce el código de seis dígitos de tu aplicación de autenticación o un código de recuperación sin usar.

Código de autenticación o recuperación

Código de seis dígitos o código de recuperación



Confiar en este navegador después de verificar MFA

Utiliza esta opción únicamente en un dispositivo privado bajo tu control.

Continuar al Back Office

Puedes utilizar una vez un código de recuperación si no tienes acceso a tu aplicación de autenticación.

Segundo paso de acceso en español, mostrado después de verificar la contraseña en PrestaShop 8.



GO ON AGENCY

ACCESO SEGURO

La contraseña es correcta. Completa el segundo paso para entrar en el Back Office.

Contraseña verificada

2

Código de autenticación

Introduce el código de seis dígitos de tu aplicación de autenticación o un código de recuperación sin usar.

Código de autenticación o recuperación

Código de seis dígitos o código de recuperación



Confiar en este navegador después de verificar MFA

Utiliza esta opción únicamente en un dispositivo privado bajo tu control.

Continuar al Back Office

Puedes utilizar una vez un código de recuperación si no tienes acceso a tu aplicación de autenticación.

Segundo paso de acceso en español, mostrado después de verificar la contraseña en PrestaShop 9.

Panel administrativo

Este panel está destinado a superadministradores. Permite definir la política global, configurar reglas por perfil y tienda, preparar la recuperación de emergencia, revisar el despliegue y comprobar la integridad de los registros. No se utiliza para configurar el TOTP personal de otros empleados.

La postura de seguridad se divide en tres pestañas: **MFA y alertas**, **Intentos y bloqueos** y **Red e IP**. La separación reduce errores de configuración sin ocultar ninguna opción.

Modo	Comportamiento
Desactivado	No exige el segundo factor.
Solo auditoría	Registra el despliegue y permite validar el funcionamiento sin bloquear accesos.
Forzar	Exige un factor válido a las cuentas con TOTP confirmado.

Campos de la política global

Campo	Para qué sirve	Recomendación
Modo MFA	Selecciona Desactivado, Solo auditoría o Forzar.	Completa el despliegue del equipo antes de activar Forzar.

Invalidación tras cambio de contraseña	Decide si el cambio incrementa la época de seguridad y revoca sesiones y dispositivos anteriores.	Utiliza «Cualquier cambio» salvo que exista una necesidad operativa documentada.
Política predeterminada por perfil	Define si los perfiles heredan, exigen, permiten o desactivan MFA.	Los superadministradores siempre quedan obligados en modo Forzar.
Matriz por perfil y tienda	Permite endurecer la política para una tienda concreta.	En multitienda siempre se aplica la política más estricta entre las tiendas accesibles.
Destinatarios de email	Direcciones que reciben avisos de acceso y errores.	Usa un buzón supervisado y valida el email de prueba.
Activar alertas	Habilita o detiene los avisos del módulo.	Actívalo después de comprobar el transporte de correo.
Códigos por email	Permite solicitar un código de ocho dígitos durante un reto MFA.	Déjalo desactivado salvo que se necesite como recuperación; exige una prueba de transporte válida.
Días de dispositivo de confianza	Define cuánto dura un navegador recordado.	Utiliza un periodo corto en equipos compartidos.
Email al acceder correctamente	Avisa después de un acceso MFA válido.	Útil durante la fase de auditoría.
Email cuando falla el acceso	Avisa de intentos rechazados.	Mantén esta alerta activa en producción.
Límites de contraseña	Define intentos por IP e IP-identidad, ventana y duración del bloqueo.	Parte de los valores iniciales y amplíalos solo con evidencia.
Límite MFA	Controla intentos del segundo factor por IP-empleado.	No lo desactives; evita valores que bloqueen por errores aislados.
Retención de registros	Conserva los eventos entre 30 y 730 días.	El valor inicial de 180 días equilibra auditoría y crecimiento.
Proxies de confianza	Permite aceptar una cabecera de IP solo desde redes proxy expresamente configuradas.	No añadas redes amplias ni confíes en cabeceras reenviadas desde Internet.
Lista permitida	Omite únicamente el límite de contraseña para redes controladas.	Nunca omite MFA.
Lista de bloqueo	Rechaza contraseña y MFA antes de comprobar credenciales.	Revisa IPv4, IPv6 y CIDR antes de guardar.
URL del manifiesto	Fuente pública utilizada para comprobar versiones.	Debe conservar la dirección HTTPS oficial de GO ON Agency.

Botones administrativos

Acción	Resultado
Guardar configuración	Aplica la política global y los parámetros de alertas.
Comprobar actualizaciones	Consulta la versión publicada y muestra los enlaces disponibles.
Enviar email de prueba	Comprueba destinatarios y transporte de correo sin esperar a un acceso real.
Generar clave de emergencia	Crea una clave de un solo uso tras confirmar la contraseña. Solo se muestra una vez.
Exportar registros firmados	Descarga un JSON con firma HMAC y registra la propia exportación.

Registros de acceso

La cabecera permite filtrar por intervalo de fechas, empleado, evento, resultado e IP. También se puede elegir el número de filas por página. Cada entrada contiene el HMAC de la anterior; el panel verifica la cadena y avisa si detecta una alteración. La purga por retención conserva un anclaje y la exportación genera un documento firmado.

Recuperación de emergencia por consola

1. Genera la clave desde el panel y guárdala en un archivo fuera del directorio de PrestaShop.
2. Accede a la consola del servidor y ejecuta `php modules/prestawardauthenticator/bin/emergency-access.php --employee=<id> --key-file=<ruta>`.
3. La clave se consume una sola vez, se revocan factores y dispositivos y aumenta la época de seguridad.
4. El empleado valida su contraseña y queda limitado a «Mi autenticación» hasta configurar TOTP de nuevo.

No coloques el archivo de clave dentro de PrestaShop ni en un directorio público. El comando rechaza la ejecución web y no crea un bypass permanente.

Mi autenticación

1. Abre «Mi autenticación» desde el menú PrestaWard Authenticator.
2. En el paso 1, confirma la contraseña actual.
3. En el paso 2, escanea el QR local o copia manualmente el secreto.
4. En el paso 3, introduce el código de seis dígitos y confirma.
5. En el paso 4, copia, descarga o imprime los códigos de recuperación.

El resumen personal muestra TOTP, códigos restantes, dispositivos fiables y última modificación. La sustitución del autenticador, la regeneración de códigos, la revocación de dispositivos y la retirada de MFA requieren la contraseña actual, un factor válido y una confirmación explícita.

Dispositivos de confianza

La opción «Confiar en este navegador» solo crea el dispositivo después de validar la contraseña y el segundo factor. La cookie está limitada al Back Office y utiliza Secure, HttpOnly y SameSite=Lax. El empleado puede revocar sus dispositivos desde «Mi autenticación».

Acceso en modo Forzar

La contraseña se valida primero. Después, la sesión queda limitada a una pantalla mínima hasta introducir un TOTP o un código de recuperación válido. El HTML no contiene menú, accesos rápidos, notificaciones ni contenido del Back Office. Las peticiones normales y AJAX permanecen bloqueadas. Si el empleado todavía no ha configurado TOTP, el módulo le dirige a su configuración personal antes de permitir el resto del Back Office.

Protección contra fuerza bruta

Los fallos de contraseña se contabilizan por IP y por combinación IP-identificador. Los fallos MFA utilizan un contador separado por IP-empleado. Los identificadores desconocidos se almacenan mediante HMAC y un acceso correcto no reinicia el contador agregado de la IP.

Configura la IP real únicamente mediante proxies de confianza. Una cabecera enviada por un cliente directo se ignora. Los bloqueos nuevos pueden generar un aviso, pero el módulo limita la frecuencia para que un atacante no provoque una tormenta de correo.

Alertas y diagnóstico del email

Configura los destinatarios, activa las alertas y utiliza «Enviar email de prueba». La confirmación significa que el servidor de correo ha aceptado el mensaje, no que el buzón final haya confirmado la entrega. Si falla, el módulo distingue entre alertas desactivadas, destinatarios no válidos, correo desactivado, configuración SMTP incompleta, rechazo del servidor y fallo general de PrestaShop.

La recuperación por email es opcional y solo aparece durante un reto MFA. El código tiene ocho dígitos, caduca a los cinco minutos, se almacena mediante HMAC y solo puede utilizarse una vez. No sustituye a TOTP ni a los códigos personales.

Comprobación segura de versiones

La acción «Comprobar actualizaciones» consulta exclusivamente el manifiesto HTTPS oficial. No sigue redirecciones, rechaza redes privadas, limita el tamaño de la respuesta y exige que el manifiesto corresponda a PrestaWard Authenticator. La web, la guía y el correo de GO ON Agency se conservan desde la configuración local y no se aceptan desde la respuesta remota.

Solución de problemas

- **Código rechazado:** comprueba la hora del dispositivo y evita reutilizar un TOTP ya aceptado.
- **Demasiados intentos:** espera el tiempo indicado por el bloqueo configurado y revisa los eventos antes de modificar los límites.
- **Email no recibido:** revisa los destinatarios y la configuración de correo de PrestaShop.
- **Dispositivo no reconocido:** los cambios importantes del navegador pueden exigir MFA de nuevo.
- **Empleado sin acceso:** revisa los permisos del perfil para «Mi autenticación».

Soporte

Web: <https://go-onagency.es/modulos/prestaward-authenticator/>

Email: hola@go-onagency.es

PrestaWard Authenticator 0.0.8 · GO ON Agency · Documento generado el 31/07/2026.