Two-Factor Authentication Guida d'uso

Modulo PrestaShop · Compatibile con PrestaShop 1.7, 8 e 9

Proteggi il tuo negozio con un secondo fattore

Two-Factor Authentication aggiunge i codici monouso TOTP (Google Authenticator, Authy, Microsoft Authenticator) al back office e all'account cliente: registrazione via QR, segreti cifrati a riposo, codici di recupero monouso e blocco anti-bruteforce. È completamente autonomo — nessun servizio esterno, nessuna chiamata di rete, nessuna libreria aggiuntiva.

1. Installazione

1. Nel back office vai su **Moduli → Gestione moduli → Carica un modulo** e seleziona lo ZIP del modulo.
2. A installazione completata, clicca **Configura** per aprire la procedura guidata.

> **Gli aggiornamenti sono automatici.** Sono legati al tuo dominio — nessuna chiave di licenza da inserire. I domini di sviluppo (`.local` , `.test` , `localhost`) sono sempre ammessi. Quando esce una nuova versione viene segnalata dentro al modulo.

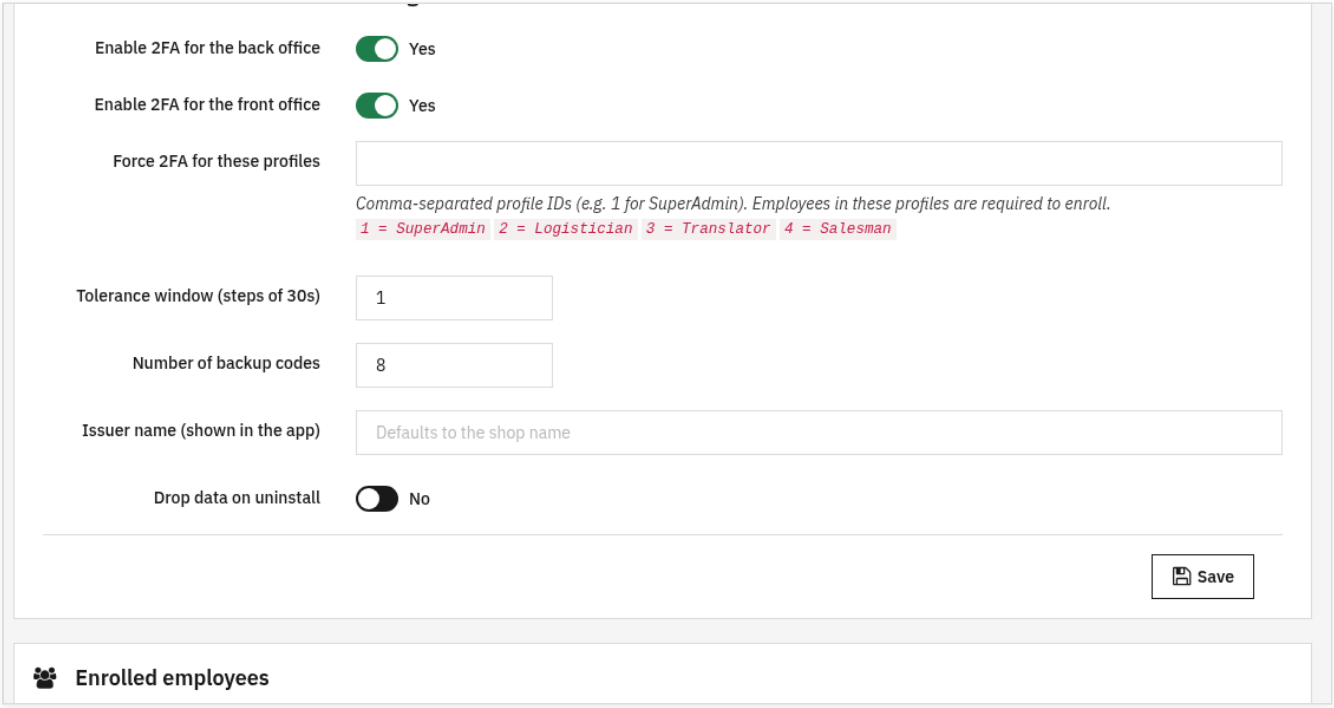
2. Configurazione — passo per passo

La schermata Configura ha un pannello impostazioni seguito da due elenchi di registrazione. Imposta prima la policy, poi usa gli elenchi per vedere chi è protetto e reimpostare chi è bloccato fuori.

Two-Factor Authentication - Settings `interruttore generale`

Questo pannello definisce dove si applica la 2FA e con quale severità. Salva con il pulsante **Salva** in basso.

- **Abilita 2FA per il back office** — attiva il secondo fattore per i dipendenti che accedono all'amministrazione. Da attivo, ogni richiesta del back office è bloccata finché il codice non viene verificato.
- **Abilita 2FA per il front office** — attiva il secondo fattore per i clienti nell'area del loro account.
- **Forza la 2FA per questi profili** — ID profilo separati da virgola (es. `1` per SuperAdmin). I dipendenti di questi profili sono obbligati a registrarsi; il form elenca ID e nome di ciascun profilo come riferimento.
- **Finestra di tolleranza (passi da 30s)** — quanti passi da 30 secondi di scarto dell'orologio accettare (0–5). Valori più alti sono più tolleranti se l'orologio del telefono è leggermente sfasato; più bassi sono più severi.
- **Numero di codici di backup** — quanti codici di recupero monouso vengono generati alla registrazione (4–20, predefinito 8). Ogni codice funziona una sola volta se l'app authenticator non è disponibile.
- **Nome issuer (mostrato nell'app)** — l'etichetta che appare accanto all'account nell'app authenticator. Lascia vuoto per usare il nome del negozio.
- **Cancella i dati alla disinstallazione** — se Sì, tutti i segreti di registrazione e i codici di backup vengono eliminati quando il modulo viene disinstallato.



Two-Factor Authentication — pannello Impostazioni

Enrolled employees

Elenca ogni dipendente del back office che ha configurato la 2FA, con ID, nome, email, stato (*Attivo* o *In attesa*) e data dell'ultimo aggiornamento.

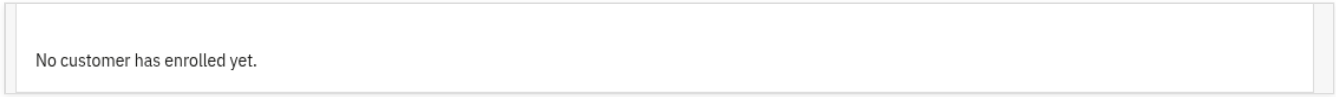
- **Reset 2FA** — rimuove il segreto di quel dipendente e azzera il conteggio dei tentativi falliti, così può registrarsi di nuovo da zero (usalo quando qualcuno perde il telefono o resta bloccato fuori).
- Se nessuno si è ancora registrato, il pannello lo indica.

Dipendenti registrati — vedi lo stato e reimposta l'accesso

Enrolled customers

Lo stesso elenco per i clienti del front office che hanno attivato la 2FA sul proprio account: ID, nome, email, stato e ultimo aggiornamento.

- **Reset 2FA** — cancella la registrazione di un cliente e il conteggio dei fallimenti così può ri-registrarsi, comodo per le richieste di assistenza quando un cliente non riesce più ad accedere.
- Vuoto finché almeno un cliente non si registra.



Clienti registrati — vedi lo stato e reimposta l'accesso

3. Verifica che funzioni

- Abilita la 2FA per il back office, poi esci e rientra: dovresti vedere la richiesta di scansionare un QR code e inserire un codice a 6 cifre prima di arrivare alla dashboard.
- Dopo la registrazione, verifica che il tuo account compaia nell'elenco *Enrolled employees* con stato *Attivo*.
- Esci, rientra e invece del codice dell'app inserisci uno dei tuoi codici di backup — deve farti entrare una sola volta e poi risultare consumato.
- Dal back office, clicca **Reset 2FA** su un account di prova e verifica che sparisca dall'elenco e che al login successivo venga richiesta di nuovo la registrazione.

4. Domande frequenti

Quali app authenticator sono supportate?

Qualsiasi app TOTP standard (RFC 6238) — Google Authenticator, Authy, Microsoft Authenticator e simili funzionano tutte.

Cosa succede se un dipendente perde il telefono?

Può usare un codice di backup, oppure un amministratore può cliccare **Reset 2FA** nell'elenco per fargli registrare un nuovo dispositivo.

Serve una connessione internet o un servizio esterno?

No. I codici vengono generati e verificati localmente; i segreti sono cifrati a riposo. Nessuna chiamata di rete e nessuna dipendenza da terze parti.

È sicuro contro il brute force?

Sì. Codici errati ripetuti attivano un blocco anti-bruteforce e la finestra di tolleranza è configurabile per bilanciare sicurezza e comodità.
