



# Customer Two-Factor Authentication Documentation

Complete PDF Manual

Guide for Magento administrators, technical project owners, and implementation teams.

LAST UPDATED  
2026-10-13

SOURCE  
[Open complete documentation online](#)

EXTENSION  
[Magento 2 Extension Customer Two-Factor Authentication](#)

# Table of Contents

Customer Two-Factor Authentication Documentation · customer-tfa

## Overview

### Customer Two-Factor Authentication

#### Getting Started

#### Installation

#### Configuration

#### Customer

#### Authenticator Enrollment

#### Login and Recovery Codes

#### Admin

#### Customer TFA Reset

#### Addons

#### Hyvä Compatibility Add-On

#### Reference

#### Configuration Fields

#### Troubleshooting

#### Common Issues

#### FAQ

# Customer Two-Factor Authentication

SoftwareSilo Customer TFA adds authenticator-app verification to Magento storefront customer accounts. After the normal email and password check, an enrolled customer must enter a current six-digit authenticator code or one unused recovery code before Magento creates the signed-in session.

Customers can enroll from My Account when TFA is optional. When it is mandatory, a customer who has not enrolled is redirected to setup from every storefront page — not just account pages; only the TFA setup/verification routes and logout stay reachable until enrollment finishes. An enrolled customer whose verification is pending is likewise held on the verification page.

## Included workflows

- Time-based one-time password (TOTP) enrollment by QR code or manual secret.
- Verification after regular and AJAX customer login.
- Configurable one-time recovery codes.
- Recovery-code regeneration after a current TFA code or customer password check.
- Customer-initiated disablement when TFA is optional.
- Magento Admin status and reset controls with a separate ACL permission.
- An optional bypass for Magento's **Login as Customer** support workflow.

The package protects storefront customer sessions. It does not configure Magento Admin two-factor authentication, send codes by email or SMS, remember trusted devices, or add REST and GraphQL endpoints.

## Start here

- [Install Customer TFA](#)
- [Configure policy and recovery](#)
- [Enroll an authenticator app](#)
- [Sign in and use recovery codes](#)
- [Reset TFA for a customer](#)
- [Use Customer TFA with Hyvä](#)
- [Troubleshoot common issues](#)
- [FAQ](#)

Configuration is under **Stores > Configuration > MageB2B > Customer Two-Factor Authentication**.

# Installation

Install the package from the SoftwareSilo Composer repository. Test enrollment, login and recovery in staging before enabling it for customers.

## Requirements

- Magento 2.4
- PHP 8.1 or newer within the PHP version supported by your Magento release
- the TOTP and QR-code libraries ([spomky-labs/otphp](#), [endroid/qr-code](#)), installed automatically by Composer

Replace [repo.softwaresilo.io](#), [softwaresilo](#), [https://repo.softwaresilo.io/](#) and `<token>` with the repository details shown under **Account > Licenses** in your SoftwareSilo account — see [Installation & Updates](#).

```
composer config bearer.repo.softwaresilo.io <token>
composer config repositories.softwaresilo composer
https://repo.softwaresilo.io/
composer require mageb2b/customer-tfa
php bin/magento module:enable MageB2B_ExtensionManager
MageB2B_CustomerTFA
php bin/magento setup:upgrade
php bin/magento cache:flush
```

Run dependency injection compilation and static-content deployment when your deployment mode requires them.

## Verify the installation

```
php bin/magento module:status MageB2B_CustomerTFA
```

Then confirm:

1. **Stores > Configuration > MageB2B > Customer Two-Factor Authentication** is available.
2. An edited customer has a read-only **Two-Factor Authentication Enabled** status.
3. The customer account dashboard shows the TFA management block after the feature is enabled.

Installation creates hidden, global customer attributes for the enabled state, encrypted authenticator secret and encrypted recovery-code list. Do not expose or edit these attributes through imports or custom forms.

Continue with [Configuration](#).

# Configuration

Open **Stores > Configuration > MageB2B > Customer Two-Factor Authentication > Two-Factor Authentication**. Configure the intended website or store scope before inviting customers to enroll.

Configuration

Scope: Default Config

Save Config

You saved the configuration.

**GENERAL**

**SECURITY**

**CATALOG**

**CUSTOMERS**

**SALES**

**MAGEB2B**

Customer Two-Factor Authentication

**SERVICES**

**ADVANCED**

**Information**

**Two-Factor Authentication**

Enable TFA for Customers (store view) Yes

Enable authenticator-app based two-factor authentication for customer accounts.

Mandatory TFA for Customers (store view) No

If enabled, logged-in customers must set up TFA before using account pages.

Issuer Name (store view) Alpine Industrial Solutions

Name shown in authenticator apps.

Recovery Codes Count (store view) 10

Number of one-time recovery codes generated after setup.

Setup Secret Lifetime (store view) 600

Number of seconds a generated setup QR code remains valid.

Maximum Verification Attempts (store view) 5

Number of invalid login verification attempts before the pending TFA login is cancelled.

Recovery Code Regeneration Authentication (store view) Current TFA Code

Credential customers must provide before regenerating recovery codes.

## Roll out optional TFA first

A cautious rollout starts with:

| Setting                                      | Suggested starting value               |
|----------------------------------------------|----------------------------------------|
| Enable TFA for Customers                     | Yes                                    |
| Mandatory TFA for Customers                  | No                                     |
| Disable TFA During Admin Login as Customer   | Yes, if support uses impersonation     |
| Issuer Name                                  | The recognizable store or company name |
| Recovery Codes Count                         | 10                                     |
| Setup Secret Lifetime                        | 600 seconds                            |
| Maximum Verification Attempts                | 5                                      |
| Allow Customers to Regenerate Recovery Codes | Yes                                    |
| Recovery Code Regeneration Authentication    | Current TFA Code                       |

| Setting                        | Suggested starting value  |
|--------------------------------|---------------------------|
| Allow Customers to Disable TFA | Yes while TFA is optional |

Enroll a staging customer, use a recovery code once, regenerate codes and test an Admin reset. Make TFA mandatory only after customer communication and support recovery are ready.

## Setting reference

### Enable TFA for Customers

Turns the storefront feature on for the current scope. Existing enrolled data remains stored when the feature is switched off, but the login challenge and account controls are inactive.

### Mandatory TFA for Customers

Customers without TFA must complete enrollment after their password is accepted. The enforcement is storefront-wide: a signed-in customer without enrollment is redirected to setup from every frontend page, and an enrolled customer with a pending verification is held on the verification page. Only the TFA setup/verification routes and logout remain reachable until the flow completes. An enrolled customer cannot disable TFA while this setting is active.

### Disable TFA During Admin Login as Customer

When enabled, a session created through Magento's **Login as Customer** workflow bypasses customer TFA. This is convenient for support, but the administrator can then enter the customer's account without the customer's authenticator.

Leave the bypass disabled when impersonated sessions must follow the customer's TFA policy. Test your support workflow either way.

### Issuer Name

This is the name shown in the customer's authenticator app. Installation initially uses the configured store-information name when one is available; otherwise the fallback is **Customer Account**. Use a short name customers recognize.

Changing the issuer changes how newly scanned entries are labelled. It does not rotate secrets already stored for customers.

### Recovery Codes Count

Controls how many ten-character, one-time codes are created during enrollment or regeneration. The default is 10. Generating a new set invalidates the previous set.

## Setup Secret Lifetime

Controls how long the generated setup QR code and secret remain valid, in seconds. The default is 600. After expiry, the customer must reload setup, scan the new QR code and verify again.

## Maximum Verification Attempts

Controls how many invalid codes a pending login can submit. The default is 5. Once the limit is reached, Magento cancels the pending TFA login and sends the customer back to the normal sign-in page.

This is a per-login challenge limit, not a permanent customer-account lock.

## Allow Customers to Regenerate Recovery Codes

When enabled, enrolled customers can replace their recovery-code set from the account dashboard. The module shows only the number of unused codes after enrollment. It never displays the stored codes again. A regenerated set replaces the old set immediately, so codes saved from an earlier set stop working.

Disable this option when recovery-code changes must go through your support team. The regeneration form then disappears from the customer account. Customers can still use an unused recovery code during sign-in.

## Recovery Code Regeneration Authentication

Choose what an already signed-in customer must provide before replacing the recovery-code set:

- **Current TFA Code** verifies the authenticator the account is using.
- **Current Password** verifies the Magento customer password.

This setting appears only while customer regeneration is allowed. Disabling optional TFA always requires the current customer password, regardless of the regeneration setting.

## Allow Customers to Disable TFA

When TFA is optional, this setting controls whether an enrolled customer may remove it without contacting an administrator. The customer must confirm the current account password. A successful removal deletes the authenticator secret and all remaining recovery codes.

The disable form is hidden when this option is off. It is also unavailable while **Mandatory TFA for Customers** is enabled, because a customer could not continue using the account without enrolling again.



DASHBOARD

SALES

CATALOG

CUSTOMERS

MARKETING

CONTENT

REPORTS

STORES

SYSTEM

FIND PARTNERS & EXTENSIONS

STAFF

PRICESYSTEM

SUBLOGIN

PUNCHOUT

B2B QUOTES

Configuration

E-Invoice

One Step Checkout

Dev Bypass Customer Auth

Order Split

Quick Order

B2B Quote

Digital Product Passport

DATEV Export Pro

Universal Commerce Protocol

DevTools

Ordered Products

Punchout

Product fees

Custom Catalog

Customer Documents

Customer ID

Enable authenticator-app based two-factor authentication for customer accounts.

Mandatory TFA for Customers

[store view]

No

Path: customermtfa/general/mandatory

If enabled, logged-in customers must set up TFA before using account pages.

Issuer Name

[store view]

Customer Account

Path: customermtfa/general/issuer\_name

Name shown in authenticator apps.

Recovery Codes Count

[store view]

10

Path: customermtfa/general/recovery\_codes\_count

Number of one-time recovery codes generated after setup.

Setup Secret Lifetime

[store view]

600

Path: customermtfa/general/setup\_secret\_lifetime

Number of seconds a generated setup QR code remains valid.

Maximum Verification Attempts

[store view]

5

Path: customermtfa/general/max\_verification\_attempts

Number of invalid login verification attempts before the pending TFA login is cancelled.

Allow Customers to Regenerate Recovery Codes

[store view]

Yes

Path: customermtfa/general/allow\_recovery\_code\_regeneration

Show recovery-code management in the customer account and allow customers to replace their existing recovery codes.

Recovery Code Regeneration Authentication

[store view]

Current TFA Code

Path: customermtfa/general/recovery\_code\_regeneration\_auth

Credential customers must provide before regenerating recovery codes.

Allow Customers to Disable TFA

[store view]

Yes

Path: customermtfa/general/allow\_customer\_disable

Show the disable action in the customer account and allow customers to remove TFA after confirming their password.

Save Config

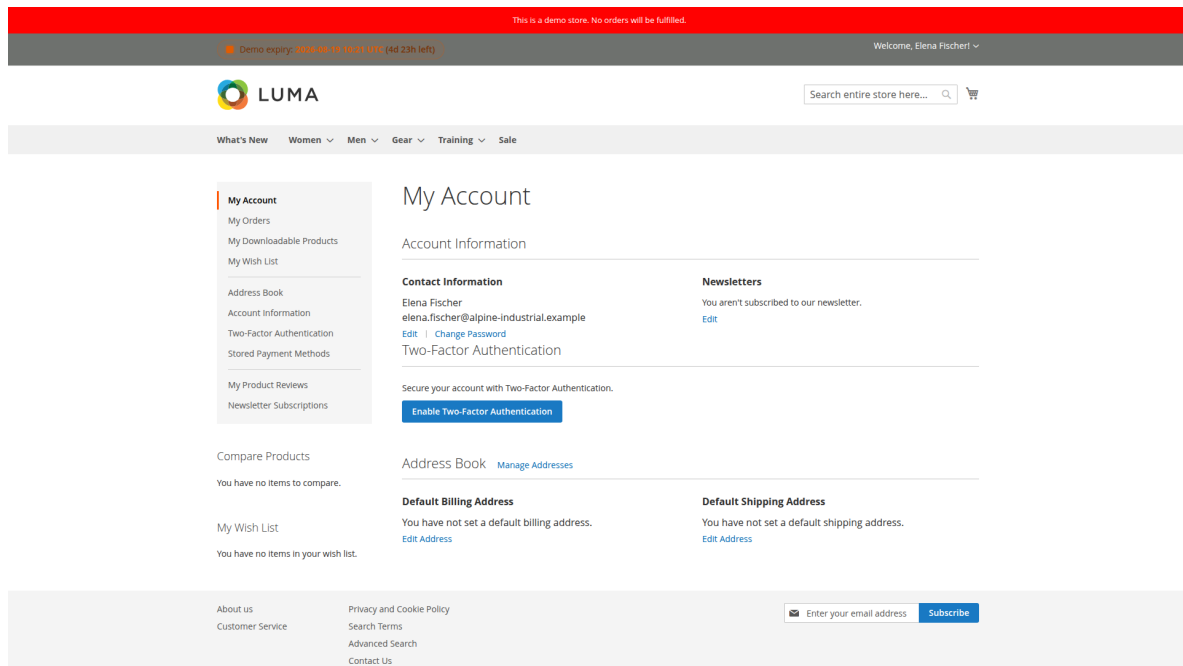
## Admin permissions

Grant **Reset Customer Two-Factor Authentication** only to support roles that handle account recovery. Configuration access uses the separate Customer TFA configuration ACL.

The extension logs enable, disable and Admin reset events with Magento's standard logger. It does not log authenticator secrets or recovery-code values.

# Authenticator Enrollment

When TFA is optional, the customer signs in and opens **My Account > Two-Factor Authentication** or uses the account dashboard action. With mandatory TFA, Magento opens the same setup after the password check and completes the login only after enrollment succeeds.



## Complete setup

1. Open the TFA setup page.
2. Scan the QR code with a TOTP-compatible authenticator app. If scanning is unavailable, enter the displayed secret manually.
3. Enter the current six-digit code from the app.
4. Submit the form before the configured setup-secret lifetime expires.
5. Save the recovery codes shown on the success page.

The issuer comes from configuration and the authenticator entry is labelled with the customer's email address.

## Store the recovery codes

Recovery codes are shown in plain text only immediately after enrollment or regeneration. The customer can print them or download a text file. Returning to the dashboard shows only how many codes remain, not their values.

Each code works once. Store the set in a password manager or another protected location separate from the authenticator device. Do not send recovery codes through an unprotected support ticket.

## If setup expires

---

An expired setup secret is rejected even if the authenticator displays a code for it. Reload setup, scan the newly generated QR code and use the code from the new authenticator entry. Remove the abandoned entry from the app to avoid confusion.

# Login and Recovery Codes

The customer first submits the normal Magento email and password. Magento keeps the customer signed out while it waits for TFA verification. A valid authenticator code completes the session and returns the customer to the original same-store destination when that URL is safe.

The same challenge is used after Magento's regular login form and AJAX login.

The screenshot shows the LUMA Two-Factor Authentication page. At the top, a red banner reads "This is a demo store. No orders will be fulfilled." Below this, a grey bar contains "Demo expiry: 2023" and "Default welcome msg!". The LUMA logo is on the left, and a search bar with "Search entire store here..." is on the right. A navigation bar below the logo lists: What's New, Women, Men, Gear, Training, and Sale. The main heading is "Two-Factor Authentication". Underneath, it says "Enter Verification Code" and "Please enter your two-factor authentication code." There is a text input field for the "Verification Code" and a checkbox labeled "Use recovery code instead". A blue "Verify and Login" button is at the bottom. On the right side, there are links for "Compare Products" (with the message "You have no items to compare."), "My Wish List" (with the message "You have no items in your wish list."), and a "Subscribe" button next to an email input field.

## Use an authenticator code

Enter the current six-digit code from the enrolled authenticator. Codes are time based, so the phone and Magento server need accurate clocks.

After the configured number of invalid attempts, the pending login is cancelled. Start again with email and password.

## Use a recovery code

On the verification page, select **Use recovery code instead** and enter one saved recovery code. The code is removed as soon as it successfully completes a login and cannot be reused.

Magento shows a notice asking the customer to generate a new set. The customer can continue using the remaining codes, but replacing the set is safer when one was needed because the authenticator was lost.

## Regenerate recovery codes

When the store allows customer regeneration, use **Regenerate Recovery Codes** from the customer dashboard and provide the configured credential: either a current authenticator code or the current Magento password.

The screenshot shows the LUMA customer dashboard. At the top, a red banner reads "This is a demo store. No orders will be fulfilled." Below it, a grey bar shows "Demo expiry: 2025-08-18 16:02 (UTC) (48 23h left)" and "Welcome, Elena Fischer!". The main header includes the LUMA logo and a search bar. A navigation bar lists categories: What's New, Women, Men, Gear, Training, and Sale. A green success message states "Successfully logged in." The left sidebar contains links for My Account (My Orders, My Downloadable Products, My Wish List, Address Book, Account Information, Stored Payment Methods, My Product Reviews, Newsletter Subscriptions), Compare Products, and My Wish List. The main content area is titled "My Account" and includes sections for Account Information, Contact Information (Elena Fischer, elena.fischer@alpine-industrial.example, Edit, Change Password, Two-Factor Authentication), Newsletters (You aren't subscribed to our newsletter, Edit), Status (Your account is protected with Two-Factor Authentication), Recovery Codes (10 recovery codes remaining, Current TFA Code, Regenerate Recovery Codes button), Current Password (Disable TFA button), Address Book (Manage Addresses), Default Billing Address (You have not set a default billing address), and Default Shipping Address (You have not set a default shipping address).

The new codes replace every old code. Save them from the one-time success page before leaving it.

If the block is not visible, customer regeneration is disabled for the current store scope. An administrator can still reset TFA from the customer record when the support process calls for a full enrollment reset.

## Disable optional TFA

When TFA is not mandatory, the customer dashboard offers **Disable TFA**. The current Magento customer password is required. Disabling removes the stored authenticator secret and recovery codes.

The block appears only when the store allows customer disablement. When TFA is mandatory, the action is not offered and the service rejects disablement. Magento checks both rules again when the form is submitted.

## Custom login implementations

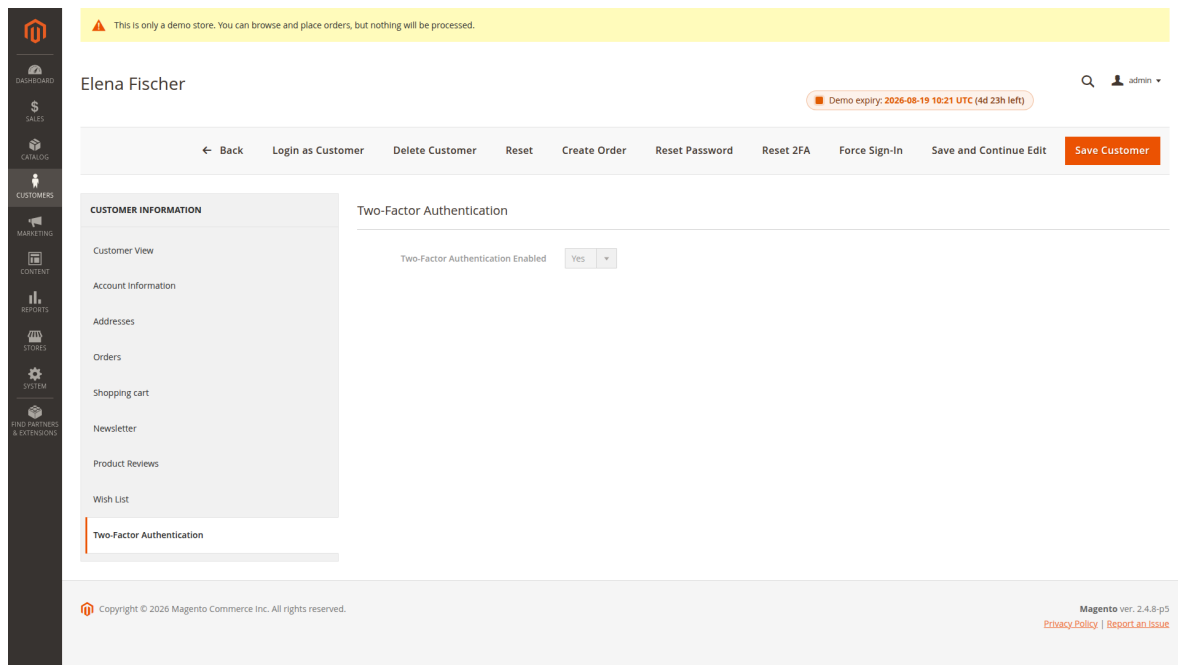
The inline challenge attaches to Magento's `customer_account_loginpost` and `customer_ajax_login` actions. A custom login endpoint of your own does not trigger the challenge inline — the storefront-wide guard redirects the customer to setup or verification on the next page instead.

For a theme or popup that uses the standard `customer_ajax_login` action, the contract is:

- The JSON request body may include `tfa_return_url`, a same-origin destination the customer lands on after verification. Unsafe or off-site values are discarded.
- When a pending challenge exists, the response is `{errors: false, message, redirectUrl}` with `redirectUrl` pointing to `customer_tfa/account/tfaverify` — or `customer_tfa/account/tfasetup` during mandatory enrollment — instead of the normal post-login target.

# Customer TFA Reset

Use an Admin reset when a verified customer has lost both the authenticator and every recovery code. The administrator needs the **Reset Customer Two-Factor Authentication** ACL permission.



## Before resetting

Follow your organization's identity-verification process. A reset removes the second-factor requirement from that account, so an email address or order number alone is not enough evidence of ownership.

## Reset the account

1. Open **Customers > All Customers**.
2. Edit the customer.
3. Check the read-only **Two-Factor Authentication Enabled** status.
4. Choose **Reset Two-Factor Authentication** and confirm the action.
5. Tell the customer to sign in and enroll a new authenticator.

The reset clears the enabled state, encrypted secret and recovery-code set. It does not change the customer's password or terminate unrelated sessions.

If TFA is mandatory, the next normal sign-in sends the customer through setup before completing authentication. If TFA is optional, the customer must enable it again from My Account.

Magento writes an Admin reset event to the standard application log with the internal customer ID, not the secret or recovery codes.

# Hyvä Compatibility Add-On

Customer TFA uses a separate package for storefronts based on Hyvä. The add-on supplies Hyvä and Alpine-compatible templates for enrollment, login verification, recovery codes and account management. The base package still owns the security rules, customer data, routes and Admin configuration.

- Composer package: `mageb2b/customer-tfa-hyva`
- Magento module: `MageB2B_CustomerTFAHyva`
- Required base package: `mageb2b/customer-tfa`
- Required storefront: Hyvä Default Theme

You do not need this package for Luma, Blank or a theme that inherits Magento's standard frontend templates.

## Install the add-on

Install and configure the base package first. Then add the Hyvä bridge:

```
composer config bearer.repo.softwaresilo.io <token>
composer config repositories.softwaresilo composer
https://repo.softwaresilo.io/
composer require mageb2b/customer-tfa-hyva:*

php bin/magento module:enable MageB2B_CustomerTFAHyva
php bin/magento setup:upgrade
php bin/magento setup:di:compile
php bin/magento cache:flush
php bin/magento hyva:config:generate
```

Rebuild the Tailwind CSS for every active Hyvä theme after installation. Use the normal static-content deployment steps required by the Magento mode and storefront locales.

## Storefront coverage

The add-on provides Hyvä templates for the complete customer flow:

| Area                  | What the customer can do                                                            |
|-----------------------|-------------------------------------------------------------------------------------|
| Account dashboard     | See whether TFA is active and start enrollment                                      |
| Enrollment            | Scan the QR code, enter the secret manually and verify the first authenticator code |
| Recovery-code handoff | Save the newly generated one-time codes after enrollment or regeneration            |

| Area               | What the customer can do                                                                  |
|--------------------|-------------------------------------------------------------------------------------------|
| Login verification | Submit an authenticator code or switch to a recovery code                                 |
| Account management | Regenerate recovery codes or disable optional TFA when the store configuration permits it |

The same settings apply to Luma and Hyvä. For example, disabling customer recovery-code regeneration removes that block from the Hyvä account dashboard as well. Mandatory TFA also prevents customer deactivation in both storefronts.

The screenshot displays a customer account dashboard with a sidebar menu on the left and a main content area. The sidebar includes links to Dashboard, My Quotes, Request Quote, Quick Order, Account Information, Address Book, My Orders, My Documents, My Ordered Products, My Downloadable Products, My Wish List, My Designs, Stored Payment Methods, My Sublogin Groups, My Sublogin Roles, My Sublogins Catalog, My Sublogin Budgets, My Product Reviews, Newsletter Subscriptions, My Prices, My Sales Staff, Logout, and Sign Out. The main content area is titled 'Account Information' and contains several sections: 'Contact Information' for Olivia Morgan (tfa.hyva.qa@example.test) with edit and change password links; 'Newsletters' indicating the user is not subscribed with an edit link; 'Two-Factor Authentication' (TFA enabled) with a status indicator, a message that the account is protected, and options to regenerate recovery codes (10 remaining) or disable TFA (requiring a password confirmation); 'Address Book' with a link to manage addresses; 'My Documents' listing Master Service Agreement, Product Catalog 2024, and Safety Data Sheet - Chemical Y; 'Default Billing Address' (not set) and 'Default Shipping Address' (not set) with edit links; and 'Recent Quotes'.

## What remains in the base package

The add-on does not store a second secret or create a separate login session. It replaces storefront presentation only. These functions remain in `MageB2B_CustomerTFA`:

- TOTP secret creation and verification;
- recovery-code generation, hashing and one-time use;
- pending-login and attempt limits;
- website and store-view configuration;
- Login as Customer handling;
- Admin status display and reset action.

Keep both modules enabled. Disabling the base module leaves the Hyvä templates without the services and routes they call.

## Verify the integration

---

Test with a fictional customer on the actual Hyvä store view:

1. enable TFA from the customer account and scan the QR code;
2. save the recovery codes and complete a fresh password login;
3. submit a valid authenticator code, then repeat the login with one recovery code;
4. regenerate recovery codes and confirm that an old code no longer works;
5. disable optional TFA when the action is allowed;
6. enable mandatory TFA and confirm that an unenrolled account is sent to setup;
7. check the same pages at a mobile viewport.

Also test the configured Login as Customer policy. The Hyvä templates do not change whether an impersonated session must complete TFA.

## Troubleshooting

---

### The standard Magento template is still displayed

Confirm that the active store view uses a Hyvä theme and that `MagentoB2B_CustomerTFAHyva` is enabled. Regenerate the Hyvä configuration, rebuild Tailwind CSS and clear Magento caches.

### The page has no styling

Check that the module's `view/frontend/tailwind/module.css` is included in the active theme build. Rebuilding Magento static content alone does not replace the Hyvä Tailwind build.

### An account action is missing

Check the base Customer TFA configuration at the active scope. Recovery-code regeneration and customer deactivation have independent settings. Deactivation is also hidden while TFA is mandatory.

### Verification returns to the login page

Treat this as a base authentication issue rather than a theme setting. Check the pending-login lifetime, verification attempt limit, session and form key, then follow [Common Issues](#).

## Related guides

---

- [Configure Customer TFA](#)
- [Enroll an authenticator app](#)
- [Sign in with Customer TFA](#)
- [Reset TFA for a customer](#)

# Configuration Fields

This reference lists the settings exposed by `mageb2b/customer-tfa` in Magento Admin.

Configuration paths are included for controlled deployments and `config:set`. Use Magento Admin for normal changes so field validation and scope inheritance still apply. The extension status display is not listed because it reports installation state rather than a configurable value.

## Two-Factor Authentication

| Field                                        | Configuration path                                                | Input  | Scope                        |
|----------------------------------------------|-------------------------------------------------------------------|--------|------------------------------|
| Enable TFA for Customers                     | <code>customertfa/general/enabled</code>                          | Select | Default, Website, Store view |
| Mandatory TFA for Customers                  | <code>customertfa/general/mandatory</code>                        | Select | Default, Website, Store view |
| Disable TFA During Admin Login as Customer   | <code>customertfa/general/disable_for_login_as_customer</code>    | Select | Default, Website, Store view |
| Issuer Name                                  | <code>customertfa/general/issuer_name</code>                      | Text   | Default, Website, Store view |
| Recovery Codes Count                         | <code>customertfa/general/recovery_codes_count</code>             | Text   | Default, Website, Store view |
| Setup Secret Lifetime                        | <code>customertfa/general/setup_secret_lifetime</code>            | Text   | Default, Website, Store view |
| Maximum Verification Attempts                | <code>customertfa/general/max_verification_attempts</code>        | Text   | Default, Website, Store view |
| Allow Customers to Regenerate Recovery Codes | <code>customertfa/general/allow_recovery_code_regeneration</code> | Select | Default, Website, Store view |
| Recovery Code Regeneration Authentication    | <code>customertfa/general/recovery_code_regeneration_auth</code>  | Select | Default, Website, Store view |

| Field                          | Configuration path                                      | Input  | Scope                        |
|--------------------------------|---------------------------------------------------------|--------|------------------------------|
| Allow Customers to Disable TFA | <code>customertfa/general/allow_customer_disable</code> | Select | Default, Website, Store view |

Visibility dependencies:

- `customertfa/general/mandatory` is available when `customertfa/general/enabled` is 1.
- `customertfa/general/disable_for_login_as_customer` is available when `customertfa/general/enabled` is 1.
- `customertfa/general/disable_for_login_as_customer` is available when `customertfa/general/mandatory` is 1.
- `customertfa/general/issuer_name` is available when `customertfa/general/enabled` is 1.
- `customertfa/general/recovery_codes_count` is available when `customertfa/general/enabled` is 1.
- `customertfa/general/setup_secret_lifetime` is available when `customertfa/general/enabled` is 1.
- `customertfa/general/max_verification_attempts` is available when `customertfa/general/enabled` is 1.
- `customertfa/general/allow_recovery_code_regeneration` is available when `customertfa/general/enabled` is 1.
- `customertfa/general/recovery_code_regeneration_auth` is available when `customertfa/general/enabled` is 1.
- `customertfa/general/recovery_code_regeneration_auth` is available when `customertfa/general/allow_recovery_code_regeneration` is 1.
- `customertfa/general/allow_customer_disable` is available when `customertfa/general/enabled` is 1 and `customertfa/general/mandatory` is 0.

## Common Issues

### The account dashboard has no TFA controls

Check **Enable TFA for Customers** in the current store scope. The management block and account navigation link are hidden while the feature is disabled.

### The setup code is always rejected

Reload setup and scan the new QR code. The previous secret may have exceeded **Setup Secret Lifetime**. Also confirm that the authenticator device and Magento server use accurate time.

Remove stale duplicate entries from the authenticator app so the customer does not select a code for an expired secret.

### A correct login password does not create a session

This is expected for an enrolled customer. Magento holds authentication in a pending state until the TFA page accepts an authenticator or recovery code.

If the verification page loops, check store scope, session/cookie configuration and whether a custom login implementation bypasses Magento's regular or AJAX customer login actions.

Pending TFA state — the pending login, attempt counter and the one-time recovery-code display — is stored encrypted in the Magento cache backend under a key derived from the customer session, expiring with `web/cookie/cookie_lifetime` (fallback one hour). A `cache:flush` therefore cancels every in-progress login and can drop freshly shown recovery codes. Flush caches between sign-ins, not while a customer is mid-verification.

### Too many invalid attempts

The pending TFA login was cancelled after the configured limit. Return to the customer login page and start again with email and password. The limit does not permanently lock the customer account.

### A recovery code no longer works

Every recovery code is single use. Regenerating codes also invalidates the entire previous set. Try an unused code from the newest set or follow the verified Admin reset process.

### Recovery codes disappeared from the success page

Their plain-text values are read from the session once. They are not shown again on the dashboard. Regenerate the set and save the newly displayed values immediately.

---

## The customer cannot disable TFA

---

Check both settings at the active website or store view. **Allow Customers to Disable TFA** must be enabled and **Mandatory TFA for Customers** must be disabled. The customer also needs the correct current Magento password.

---

## Recovery-code management is missing

---

Confirm that **Allow Customers to Regenerate Recovery Codes** is enabled at the active scope. The form also requires an enrolled customer. Changing **Recovery Code Regeneration Authentication** does not enable the form by itself.

For a Hyvä storefront, confirm that **MageB2B\_CustomerTFAHyva** is enabled and that the active theme's Tailwind CSS was rebuilt after installation.

---

## Login as Customer skips the challenge

---

Check **Disable TFA During Admin Login as Customer**. It is enabled by default. Disable that bypass when assisted sessions must complete the customer's TFA challenge.

---

## The authenticator shows an unfamiliar name

---

The label uses **Issuer Name** plus the customer email. Update the issuer to a recognizable store name. Existing authenticator entries keep the label they received when scanned; customers must re-enroll to replace it.

## **FAQ**

### **Which authenticator apps work?**

The setup uses standard TOTP provisioning. Apps that support time-based one-time passwords can scan the QR code or accept the secret manually.

### **Does the module send codes by email or SMS?**

No. It supports authenticator-app codes and one-time recovery codes.

### **Is TFA optional or mandatory?**

The store administrator chooses. Optional mode lets each customer enroll and later disable TFA with the current password. Mandatory mode requires setup and prevents customer disablement.

### **When is the customer considered signed in?**

For an enrolled account, only after the password and TFA challenge both succeed. Magento keeps the password result pending until verification.

### **How many recovery codes are created?**

The count is configurable and defaults to 10. Each generated code has ten uppercase letters or digits and works once.

### **Can recovery codes be viewed later?**

No. Their values appear only on the success page immediately after setup or regeneration. The dashboard shows only the remaining count.

### **What invalidates old recovery codes?**

Using a code removes that code. Regenerating the set invalidates every previous recovery code. Disabling or resetting TFA removes the set as well.

### **What happens after too many wrong codes?**

Magento cancels the pending TFA login and returns the customer to normal sign-in. It does not permanently lock the account through this feature.

### **Can an administrator see the secret or recovery codes?**

The customer form shows only whether TFA is enabled. The secret and recovery-code list

are stored encrypted and are not displayed by the Admin UI.

---

## Can an administrator reset TFA?

Yes, with the dedicated ACL permission. Reset clears the customer's TFA state. Your support team should verify account ownership first.

---

## Does Login as Customer require TFA?

That depends on configuration. The default bypass allows the assisted Admin session without customer TFA. Disable the bypass to challenge impersonated sessions too.

---

## Does the module remember trusted devices?

No. A new customer login session requires a fresh authenticator or recovery code.

---

## Does it protect Magento Admin users?

No. It protects storefront customer accounts. Magento Admin authentication is a separate system.

---

## Is there a REST or GraphQL API?

No. The package provides storefront and Admin UI flows and declares no web API or GraphQL schema. The `tfa_enabled` customer attribute is additionally **protected**: customer and guest API tokens cannot toggle it through `custom_attributes` — only admin or integration writes apply.

---

## Can the store hide recovery-code regeneration?

Yes. Set **Allow Customers to Regenerate Recovery Codes** to **No** at the required scope. Customers can continue using existing recovery codes during sign-in, but they cannot replace the set from their account.

---

## Can customers remove TFA themselves?

Only when **Allow Customers to Disable TFA** is enabled and TFA is not mandatory. The customer must confirm the current Magento password. Administrators with the reset permission can still remove an enrollment from the customer record.

---

## Does the base package support Hyvä storefronts?

Install the separate `mageb2b/customer-tfa-hyva` package for Hyvä storefront templates. The base package continues to own enrollment, verification, recovery codes, configuration and Admin reset behavior.