



Configuration

Customer Two-Factor Authentication Documentation

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

LAST UPDATED
2026-10-13

SOURCE
[Open this article
online](#)

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

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 Information

SECURITY Two-Factor Authentication

CATALOG

CUSTOMERS

SALES

MAGEB2B

Customer Two-Factor Authentication

SERVICES

ADVANCED

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

Save Config

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.

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.