



FAQ

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](#)

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.