



Login and Recovery Codes

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](#)

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.

This is a demo store. No orders will be fulfilled.

Demo expiry: 2025-12-31

Default welcome msg!

LUMA

Search entire store here...

What's New Women Men Gear Training Sale

Two-Factor Authentication

Enter Verification Code
Please enter your two-factor authentication code.

Verification Code

☐ Use recovery code instead

[Verify and Login](#)

[Compare Products](#)
You have no items to compare.

[My Wish List](#)
You have no items in your wish list.

[About us](#)
[Customer Service](#)

[Privacy and Cookie Policy](#)
[Search Terms](#)
[Advanced Search](#)
[Contact Us](#)

Enter your email address [Subscribe](#)

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 'My Account' page of a LUMA store. 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 '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' (You have no items to compare.), and 'My Wish List' (You have no items in your 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.