Two-Factor Authentication

Sales Staff Documentation

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

LAST UPDATED
2026-09-26

SOURCE
Open this article online

EXTENSION
Magento 2 Extension Sales Staff

Two-Factor Authentication

The Staff TFA add-on adds a second step to the Staff storefront login. After the password is accepted, a representative enters a six-digit code from an authenticator app. A single-use recovery code can be used when the authenticator device is unavailable.

Staff TFA and Staff SAML cannot be installed together. The `mageb2b/staff-tfa` package declares a Composer conflict with `mageb2b/staff-saml`. Choose TFA for password-based Staff accounts that need an authenticator step, or choose SAML when an identity provider controls Staff sign-in.

Requirements and installation

Staff TFA requires the Staff base extension (`mageb2b/staff`).

```
composer require mageb2b/staff-tfa:*
php bin/magento module:enable MageB2B_StaffTFA
php bin/magento setup:upgrade
php bin/magento setup:di:compile
php bin/magento setup:static-content:deploy
php bin/magento cache:flush
```

Run the static-content command with the locales and deployment strategy used by the store. Install and test the add-on in staging before enabling mandatory TFA.

If Composer reports a conflict with `mageb2b/staff-saml`, decide which login method the project will use. Do not bypass the conflict or copy either module into `app/code`.

Configure TFA

Open **Stores > Configuration > MageB2B > Staff > Two-Factor Authentication**.

Setting	What it controls	Default
Enable TFA for Staff	Makes TFA setup and verification available to Staff accounts	No
Mandatory TFA for All Staff	Sends every Staff account without a configured secret through setup after password login	No
Issuer Name	Name shown next to the account in the authenticator app	Staff Portal

Configuration can be set at default, website or store-view scope. Use a recognizable issuer name so representatives can distinguish this account from other entries in their authenticator app.

Start with TFA enabled but not mandatory. Complete setup and recovery testing with one

representative, then enable the mandatory setting if every Staff account should use it.

Enrol a Staff account

When TFA is optional, the representative opens **Setup Two-Factor Authentication** from the Staff account navigation. When it is mandatory, the module sends an unconfigured representative to the setup page immediately after a successful password login.

The setup flow is:

1. Scan the QR code with a compatible authenticator app. The secret is also shown for manual entry.
2. Enter the current six-digit code to confirm that the app and Magento use the same secret.
3. Save the ten recovery codes shown after confirmation. They can be printed or downloaded as a text file.
4. Continue to the Staff dashboard.

The recovery-code screen is shown as part of setup. Store the codes outside Magento and do not send them through a shared chat or ticket.

Sign in with TFA

The normal Staff email and password are checked first. Magento then opens the verification page and does not establish the authenticated Staff session until the second step succeeds.

Enter the six-digit code currently displayed by the authenticator app. If the device is unavailable, select **Use recovery code instead** and enter an unused recovery code. Each recovery code is removed after a successful login and cannot be used again.

Authenticator codes depend on the current time. If a valid-looking code is rejected, confirm that the phone and Magento server clocks are synchronized before resetting the account.

Manage recovery codes

The Staff account page shows whether TFA is enabled and how many recovery codes remain. A representative can generate a new set from the TFA account block. The new set replaces all previous recovery codes.

When TFA is optional, a representative can disable it after entering the current Staff password. Mandatory TFA cannot be disabled from the Staff account or through the Admin disable action.

Reset a locked account

An administrator needs the **TFA Management** permission for the relevant actions. Open

the Staff record in Magento Admin and use **Reset TFA** when the representative has lost both the authenticator device and all recovery codes.

Resetting TFA removes the saved authenticator secret and recovery codes. At the next login, the representative must enrol again when TFA is mandatory. If TFA is optional, the account remains without TFA until it is set up again.

Treat a reset request as an account-recovery request. Verify the representative's identity through an agreed internal process before resetting the second factor.

The package defines these Admin permissions:

- TFA Management
- Reset Staff TFA
- Disable Staff TFA

Grant them only to roles responsible for Staff account recovery.

Stored security data

The add-on extends the Staff account record with the enabled state, the authenticator secret and the remaining recovery codes. Magento encrypts the secret and recovery-code data before saving them. Recovery codes are compared as exact, single-use values.

Do not include QR codes, manual secrets, authenticator codes or recovery codes in screenshots or support requests.

Troubleshooting

Setup keeps returning to the QR code

Use the newest code from the same authenticator entry that scanned the displayed QR code. Confirm that cookies and the Staff session persist between the setup page and form submission.

A representative is redirected to setup after every login

Check that setup was completed with a valid code and that the Staff record now shows TFA as enabled. Mandatory TFA continues to require setup until Magento has saved a confirmed secret.

Authenticator codes are rejected

Check the phone and server time, then try the newest code. Do not regenerate the authenticator entry repeatedly, because each new setup produces a different secret.

No recovery codes remain

Generate a new set while the representative can still sign in. If access is already lost, an authorized administrator must reset TFA and the representative must enrol again.

Composer will not install TFA beside SAML

This is expected. Staff TFA conflicts with Staff SAML because they provide alternative Staff login methods. Remove the unneeded authentication add-on through the project's tested Composer deployment process before installing the other one.

Related: Installation and Setup, SAML Single Sign-On and Common Issues.