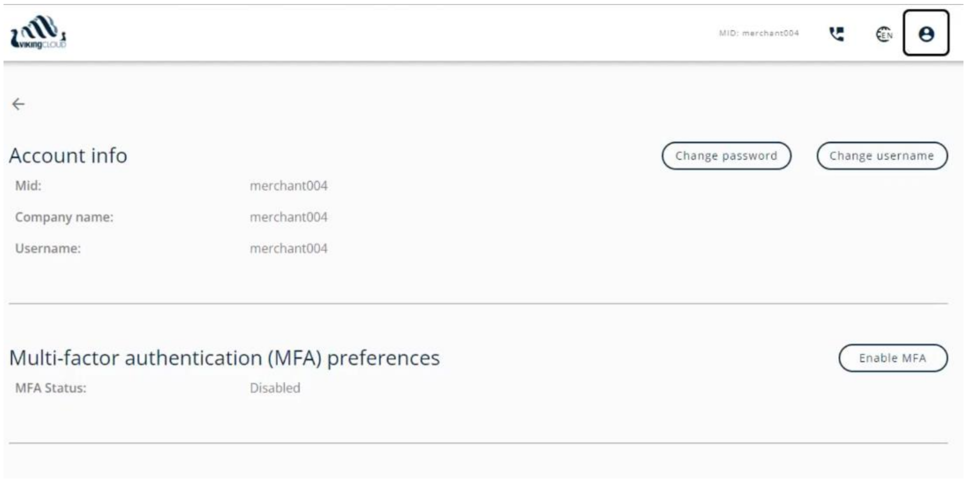
Multi-factor Authentication Guide

The purpose of this document is to provide information about multi-factor authentication (MFA) feature on the compliance portal.

MFA is an authentication method that adds a layer of protection to the sign-in process. In addition to the username and password, once enabled, MFA will require the user to input a one-time passcode (OTP) before entering the portal.

How to enable MFA

Go to the Account Preferences screen, scroll down to the “Multi-factor authentication (MFA) preferences” section.



MID: merchant004

Account info

Mid: merchant004

Company name: merchant004

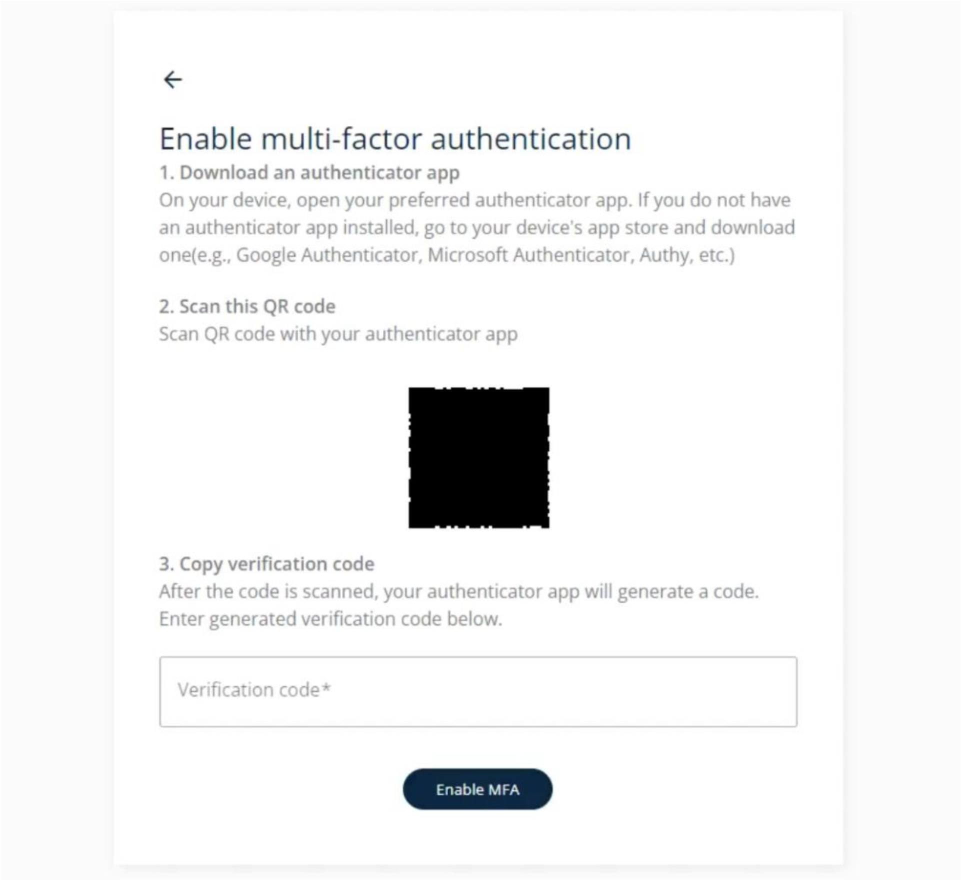
Username: merchant004

Multi-factor authentication (MFA) preferences

MFA Status: Disabled

Click “**Enable MFA**” and follow the instructions on the screen.

Open the authenticator app, scan the QR code.



Enable multi-factor authentication

1. Download an authenticator app

On your device, open your preferred authenticator app. If you do not have an authenticator app installed, go to your device's app store and download one(e.g., Google Authenticator, Microsoft Authenticator, Authy, etc.)

2. Scan this QR code

Scan QR code with your authenticator app

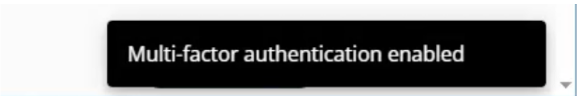
[redacted]

3. Copy verification code

After the code is scanned, your authenticator app will generate a code. Enter generated verification code below.

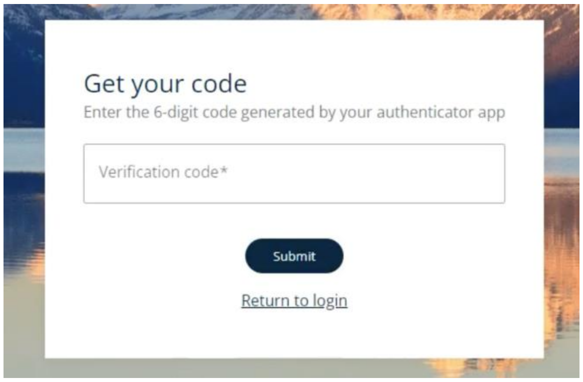
Verification code*

Type in the verification code, and click “**Enable MFA**” to enable the feature. A portal message will be displayed as well.



Multi-factor authentication enabled

You will be required to input the verification code on all subsequent logins (until MFA is disabled).



Get your code

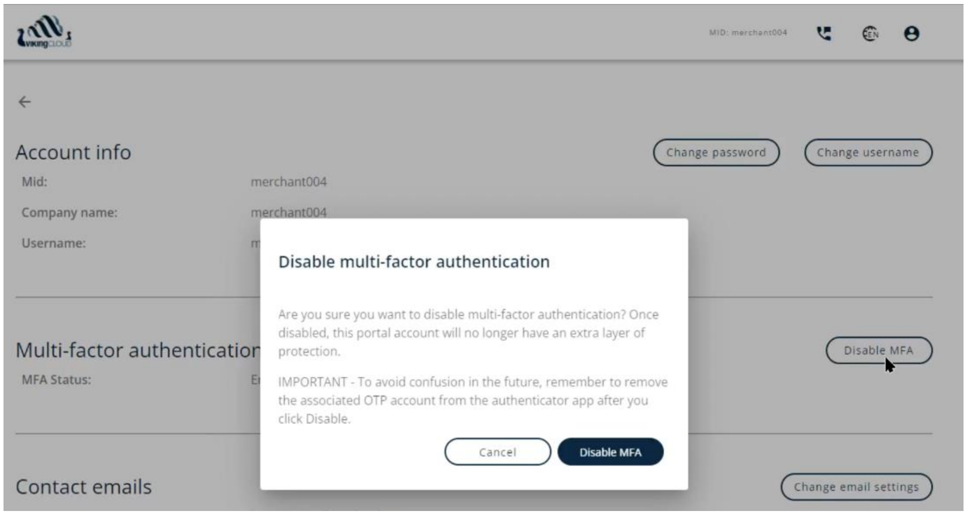
Enter the 6-digit code generated by your authenticator app

Verification code*

How to disable MFA

Go to the Account Preferences screen, scroll down to the “Multi-factor authentication (MFA) preferences” section.

Click “**Disable MFA**” and follow the instructions on the screen.



Account info

Mid: merchant004

Company name: merchant004

Username:

Multi-factor authentication

MFA Status:

Contact emails

Disable multi-factor authentication

Are you sure you want to disable multi-factor authentication? Once disabled, this portal account will no longer have an extra layer of protection.

IMPORTANT - To avoid confusion in the future, remember to remove the associated OTP account from the authenticator app after you click Disable.

System Requirements

The SAIR MFA implementation requires:

- User to download and install an authenticator app of their choice onto a system or device that can detect or scan a QR code.

FAQ

1. *Can I receive the verification code via text message, email or push notification?*

   Currently only time-based one-time password (TOTP) via authenticator app is supported.

2. *What if I no longer have access to my verification device or system?*

   Please contact the compliance portal support team for further assistance. You will be required to provide additional authentication information for security purposes.

3. *I am already a compliance portal user, can I enable MFA?*

   Yes, all merchant users of the system will be able to enable MFA.

4. *I am registering on the compliance portal for the first time, can I enable MFA?*

   Yes. Please register your compliance portal account as usual. After you complete registration, go to your Account Preferences screen to enable MFA.

5. *If I use single-sign-on (SSO) to access the compliance portal, will I be able to also use MFA?*

   For users that use single-sign-on (SSO), you will be able to enable MFA if you choose (but it is not required). If MFA is enabled for a SSO user, SSO will continue to work as usual.

Additional Resources

Some available third-party resources to assist with configurating MFA on some popular devices and apps (made available for convenience only; not an endorsement):

- Automatically fill in one-time verification codes on iPhone - Apple Support
- Set up temporary verification codes in the Microsoft Authenticator app - Microsoft Support

Accessibility Update (Compliance) - Nov. 23

- Get verification codes with Google Authenticator - Android - Google Account Help
- Add a New Two Factor Authentication (2FA) Account Token in the Authy App – Authy
- Use 1Password as an authenticator for sites with two-factor authentication