Multi-Factor Authentication: User

Table of Contents

Introduction

To better protect data security and customer information, Total Expert allows you to set up multi-factor authentication (MFA) for your account (if your organization makes it available). This requires you to provide a securely generated code in addition to your user name and password to log in. This extra proof of identity makes it much less likely that a compromised password can be used to access sensitive information stored in your account.

Note
If you use a single sign-on (SSO) service to log in to Total Expert, then that service uses its own authentication steps and bypasses Total Expert's MFA (even if MFA is set up for your Total Expert account).

End User Setup

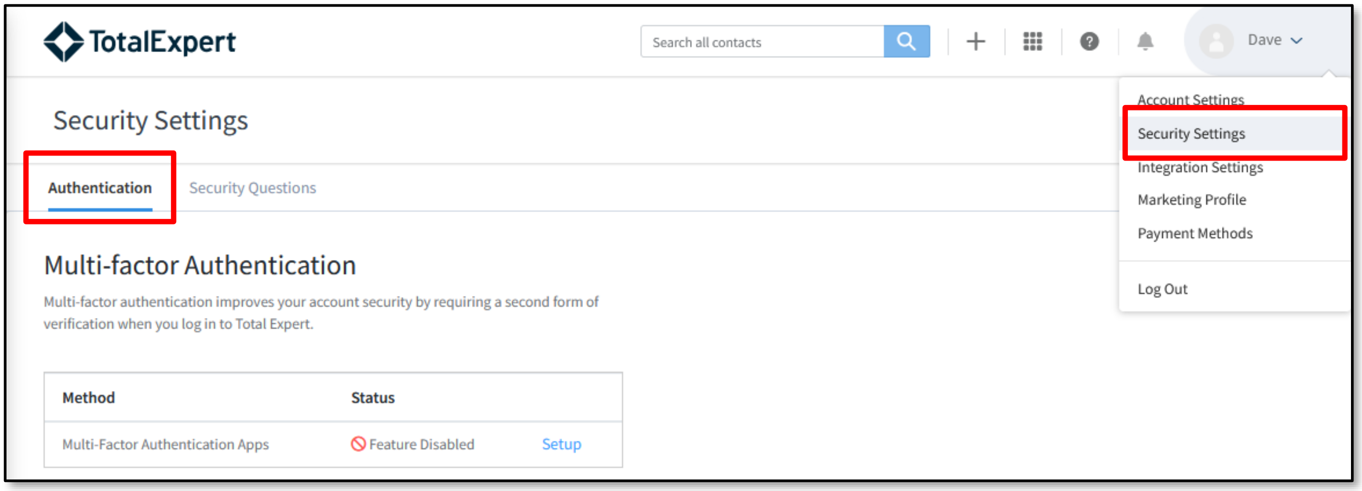
Tip
You should receive an automatically generated email every time the MFA setup in your account changes. This alerts you to take immediate action in the event that your account is compromised. If you made the changes yourself, these emails require no action.

The way you set up MFA for your account depends on whether your organization has made it required or optional.

Setup Inside Your Account (Optional Setup)

If your organization makes MFA available but does not require it for every user, you can set it up after logging in to your account.

1. Navigate to **settings menu → Security Settings**.
2. Click the **Authentication** tab if it is not already selected.



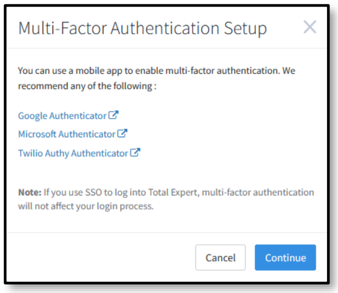
Security Settings

Multi-factor Authentication

Multi-factor authentication improves your account security by requiring a second form of verification when you log in to Total Expert.

Method	Status	
Multi-Factor Authentication Apps	🛇 Feature Disabled	Setup

3. If you have not yet set up an MFA app in your account, the box shows the Ø symbol under Status and shows a Setup link. Click **Setup**.
4. The Multi-Factor Authentication Setup box opens. This box provides links to 3 recommended authenticator apps you can download to your personal device, though you can use any app that supports temporary one-time password (TOTP) setup. Once you have downloaded your preferred app, click the **Continue** button.

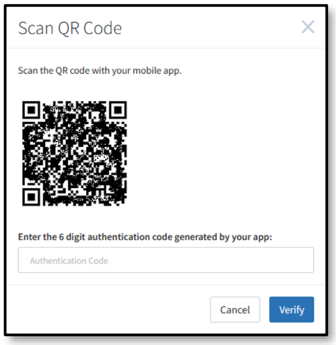


You can use a mobile app to enable multi-factor authentication. We recommend any of the following :

Note: If you use SSO to log into Total Expert, multi-factor authentication will not affect your login process.

Note
Total Expert does not use codes sent by SMS. Authenticator apps are more secure.

5. In your app, use the QR code provided on the next screen to establish a connection with your Total Expert account. (The QR code in the image below has been deliberately obscured.)



Scan the QR code with your mobile app.

Enter the 6 digit authentication code generated by your app:

6. In the provided field, enter the authentication code provided by the app.
7. Click the **Verify** button.

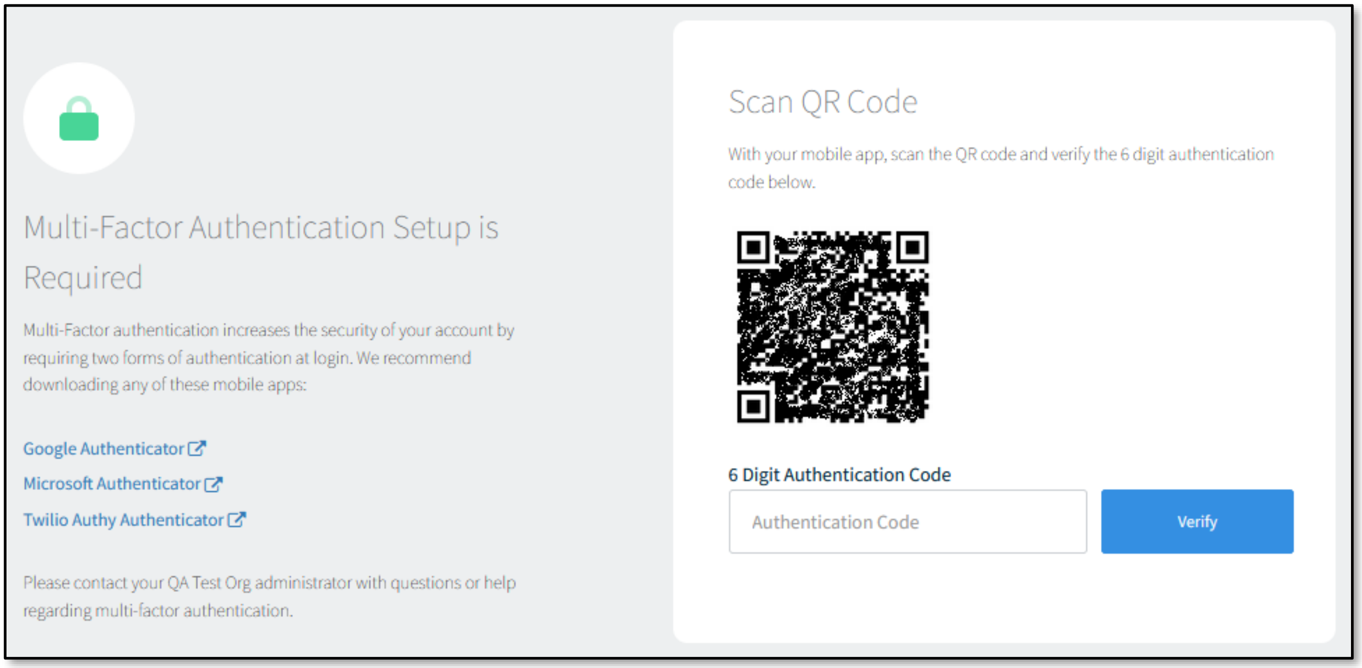
Note
Individual apps may use a different procedure to connect with your account. Follow the app's instructions.

Tip
Your setup is successful when the Status symbol switches to ✓ and the link switches to Disable.

Setup from the Login Screen (Required Setup)

If your organization requires you to set up MFA, you will have to do so during your next login attempt. After entering your user name and password, you are shown a screen with links to 3 recommended authenticator apps you can download to your personal device (though you can use any app that supports temporary one-time password (TOTP) setup) and a QR code. (The QR code in the image below has been deliberately obscured.)

Once you have downloaded your preferred app, use the QR code to establish a connection with your Total Expert account. In the **Authentication Code** field, enter the 6-digit code provided by the app, and click the **Verify** button.



Multi-Factor Authentication Setup is Required

Multi-Factor authentication increases the security of your account by requiring two forms of authentication at login. We recommend downloading any of these mobile apps:

Google Authenticator
Microsoft Authenticator
Twilio Authy Authenticator

Please contact your QA Test Org administrator with questions or help regarding multi-factor authentication.

Scan QR Code

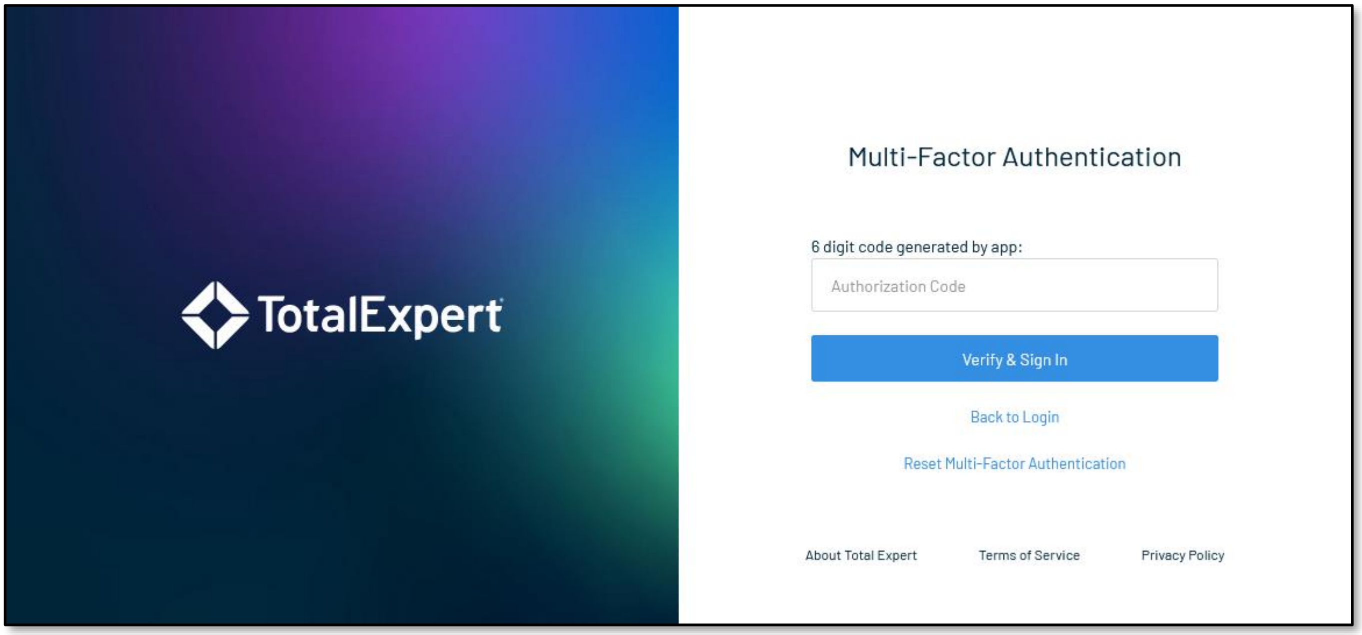
With your mobile app, scan the QR code and verify the 6 digit authentication code below.

6 Digit Authentication Code

The confirmation screen reminds you that you will need this information each time you log in from now on. Click the **Continue to [organization name]** button to finish logging in.

Logging in with MFA

After you set up MFA for your account, you must provide the authorization code each time you attempt to log in. After you enter your user name and password as usual, you are shown the Multi-Factor Authentication screen. On this screen, simply enter the 6-digit code from your app in the **Authorization Code** field, then click the **Verify & Sign In** button.



Multi-Factor Authentication

6 digit code generated by app:

Authorization Code

Verify & Sign In

Back to Login

Reset Multi-Factor Authentication

About Total Expert

Terms of Service

Privacy Policy

Resetting MFA for Your Account

The process for resetting your MFA setup depends on whether or not you still have access to the device you used to set up your MFA. If you still have it, you can use it to log in as usual, then process the change from inside your account. If not, you must request a reset before you can log in.

After Logging In

If you log in with your existing device and MFA setup, but want to reset the MFA for your account (such as when you have a new device), click the **Disable** link on the Security Settings page, then click the **Disable** button in the confirmation box. At this point, 1 of 2 things will happen, depending on your organization settings:

- If your organization allows automatic user reset, the Disable link switches back to Setup, and you can begin the process again from the beginning. See Setup Inside Your Account (Optional Setup) above.
- If your organization does not allow automatic user reset, the Disable link is replaced by the text Reset Pending, which remains until an admin resets the MFA for your account.
  - They should contact you to verify that your reset request was genuine before resetting your MFA.
  - You can continue to log in using the existing setup until then.
  - When the admin has reset your MFA, you will receive an email notification with instructions. Remember to delete the existing setup in your authenticator app.

From the Login Page

If you have lost access to your device:

1. Enter your user name and password on the login page. This opens the Multi-Factor Authentication screen.
2. Click the **Reset Multi-Factor Authentication** link on this page. This takes you to the Multi-Factor Authentication Reset page.

3. Read the information presented and click the **Submit Reset Request** button. The configured administrators are notified. They should contact you to verify that your reset request was genuine before resetting your MFA.

Note
The existing MFA setup remains valid while the request is pending. However, if you have lost access to your device, you cannot log in.

When the admin has reset your MFA, you will receive an email notification with instructions. Remember to delete the existing setup in your authenticator app before proceeding to create a new setup.