Two-factor authentication overview

The Thomson Reuters Account uses two-factor authentication (previously called multi-factor authentication or MFA) to check your identity and help make sure your account isn't compromised. It also adds another layer of protection so your account safety relies on more than a simple password.

Who is required to use two-factor authentication

From August 2025 two-factor authentication will be required for Onvio and Digita Virtual Office for both staff and clients.

Verification options

You can access our products safely and securely using one or more of the methods listed below.

- **Auth0 Guardian mobile app.** The only option that includes push notifications. The app is free on the Apple App Store and on Google Play for Android.
- **Other app.** Use another app from Microsoft, Google, Symantec, Duo, or LastPass. These won't use push notifications and can be used to generate login codes only.
- **Biometrics.** Use a thumbprint or facial recognition feature on your device to approve a sign-in.
- **Security key**: Use a hardware key to enter a code at sign-in.
- **Text message.** Receive a text with a code to enter at sign-in.
- **Phone call.** Receive a phone call with a code to enter at sign-in.

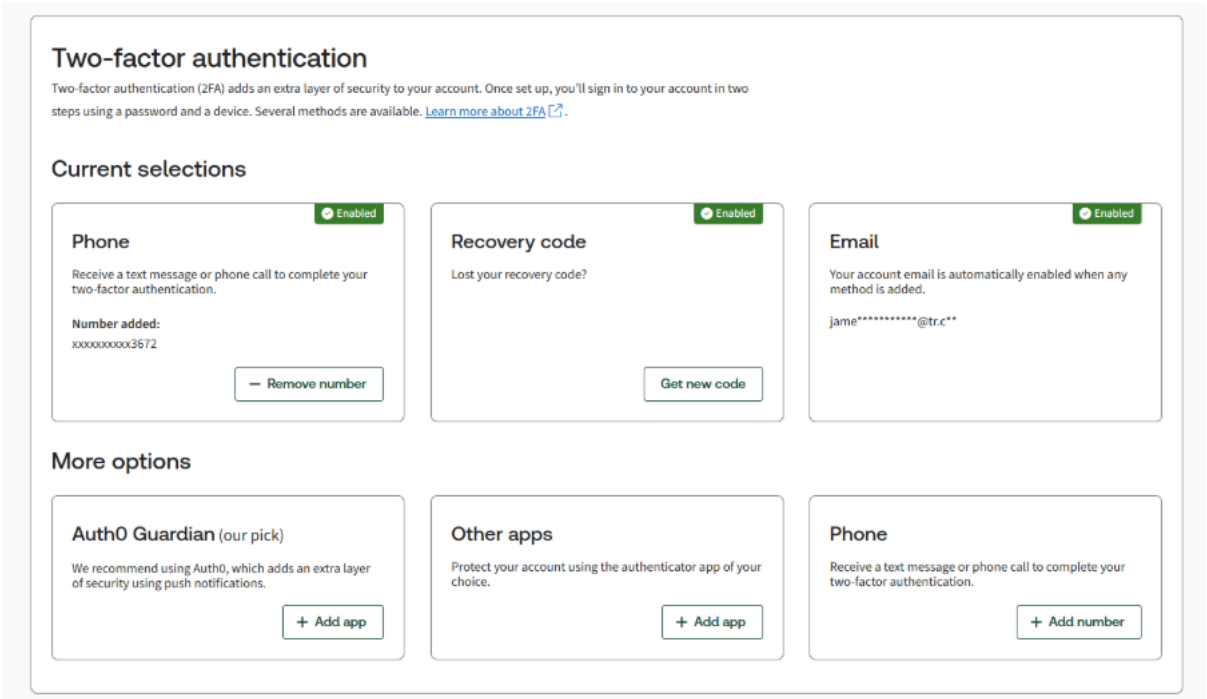
The Auth0 Guardian mobile app is our recommended option for frequent users of Onvio such as staff however infrequent users, such as clients who only access it once a year to sign a tax return, may prefer the text message option.

The Thomson Reuters Account can be linked to an alternative two-factor authentication app if your firm already uses a similar method for accessing internal systems however alternative apps will not send notifications. Select the 'Other app' option to link your Onvio/DVO login to an alternative method.

Manage two-factor authentication

Two-factor authentication can be managed after the initial setup by logging in to Onvio/DVO and selecting Manage Thomson Reuters Account. This option can be located by clicking on your username in the Onvio/DVO home pages.

This can be used to set up a new two-factor authentication method and pair a new device to an existing account.


Two-factor authentication
Two-factor authentication (2FA) adds an extra layer of security to your account. Once set up, you'll sign in to your account in two steps using a password and a device. Several methods are available. Learn more about 2FA.
Current selections
Enabled
Phone
Receive a text message or phone call to complete your two-factor authentication.
Number added:
xxxxxxxxx3672
Remove number
Enabled
Recovery code
Lost your recovery code?
Get new code
Enabled
Email
Your account email is automatically enabled when any method is added.
jame**********@tr.c**
More options
Auth0 Guardian (our pick)
We recommend using Auth0, which adds an extra layer of security using push notifications.
Add app
Other apps
Protect your account using the authenticator app of your choice.
Add app
Phone
Receive a text message or phone call to complete your two-factor authentication.
Add number