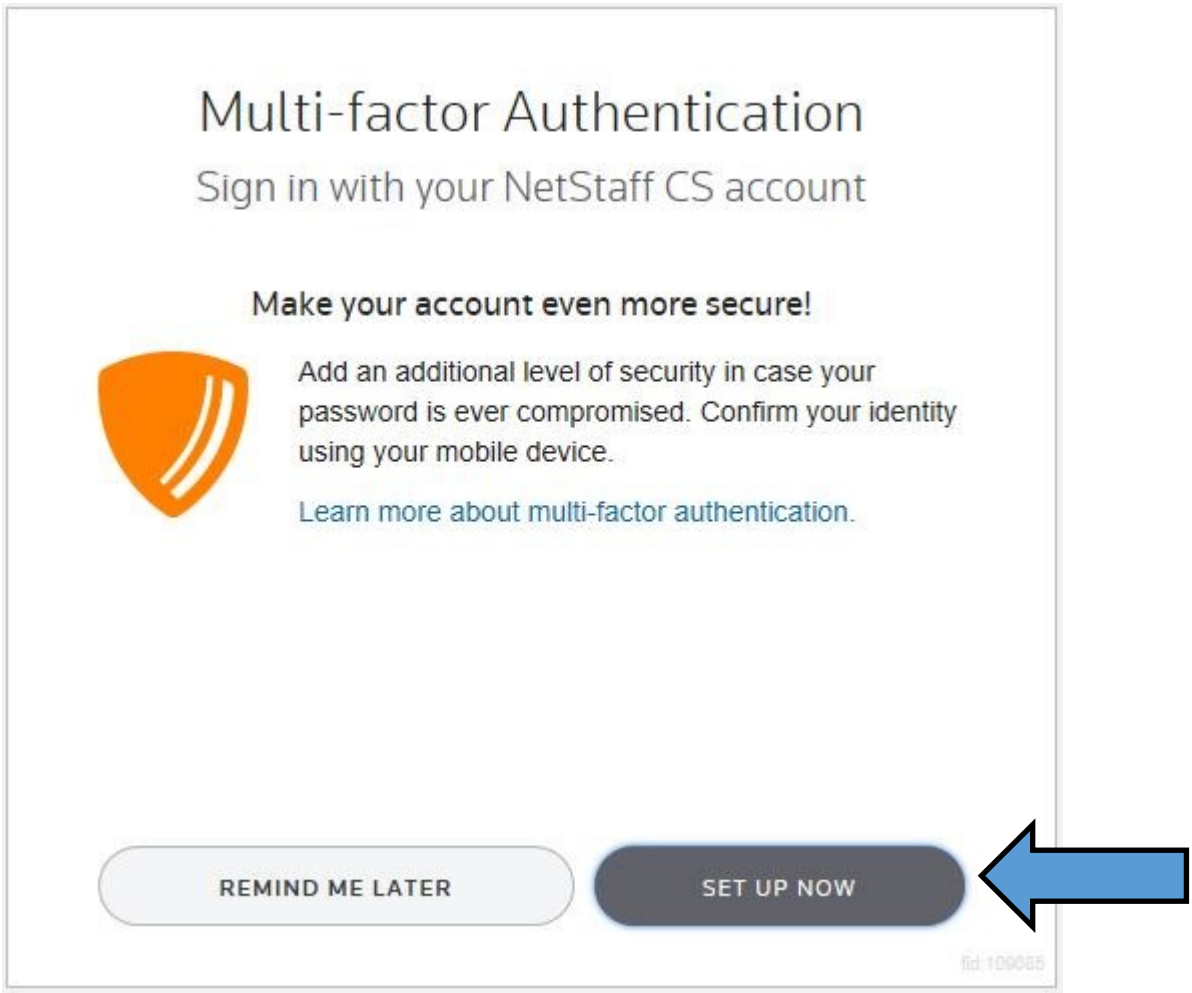
Multi-Factor Authentication

Multi-factor authentication provides an additional layer of security that helps protect confidential data. Many online accounts or software applications are currently protected by a login and password. That password is the single factor in the authentication process — the way that those applications or services confirm identity.

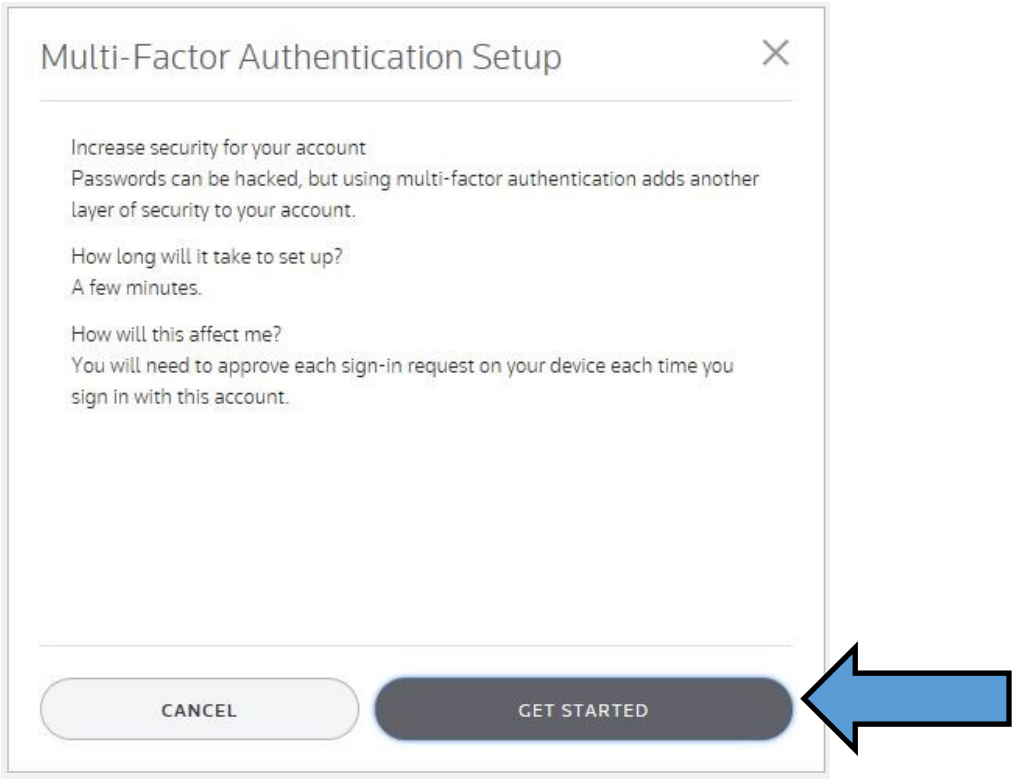
Multi-factor authentication adds at least one more layer of identity verification to that process so protection against hacking and fraud attempts is stronger and more secure than a simple password. That additional layer can take many forms, such as a physical ID card, a digital confirmation code, or even a fingerprint. Multi-factor authentication is in use every time a transaction is paid using a debit card or cash is withdrawn from an ATM: the debit card is one factor and the PIN is another.

Enabling Multi-Factor Authentication

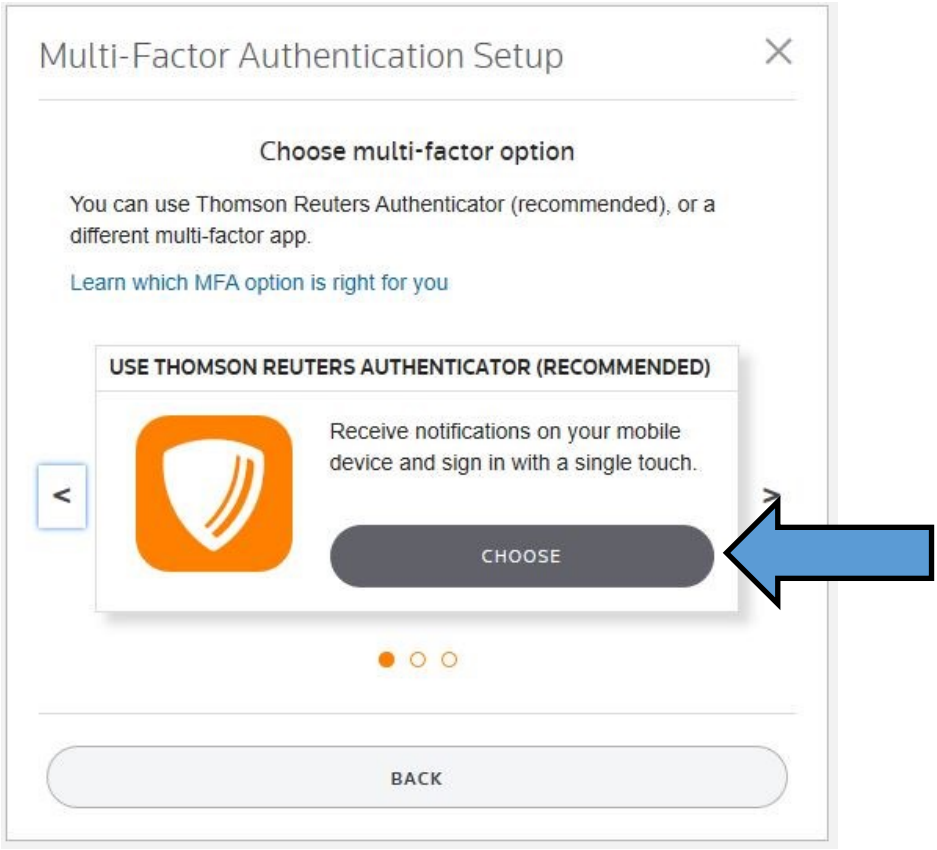
Upon signing into the NetClient account, an option will be presented to enable multi-factor authentication or to skip multi-factor setup. Choose “Set Up Now” to enable multi-factor authentication.



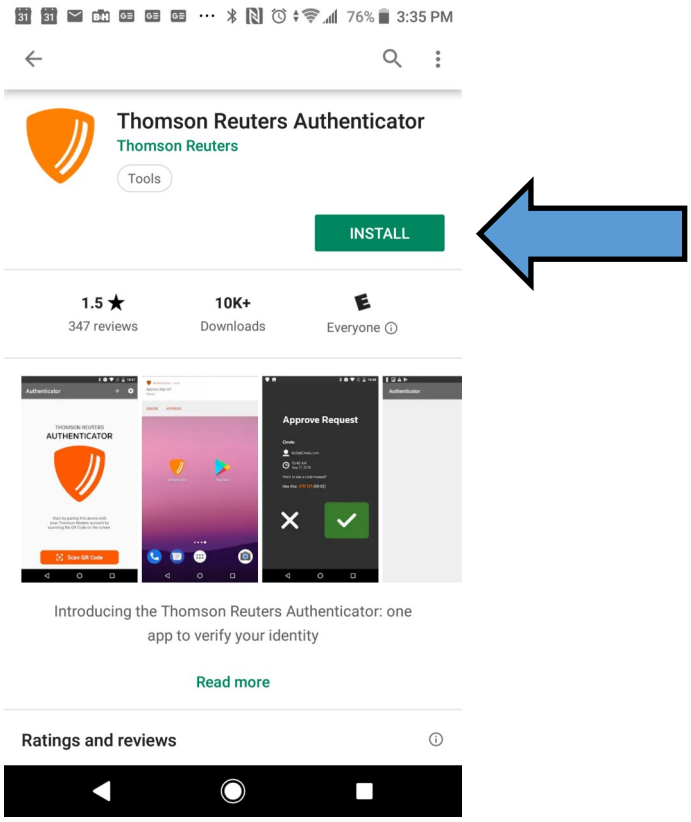
On the next tile click “Get Started” to continue the enabling process.



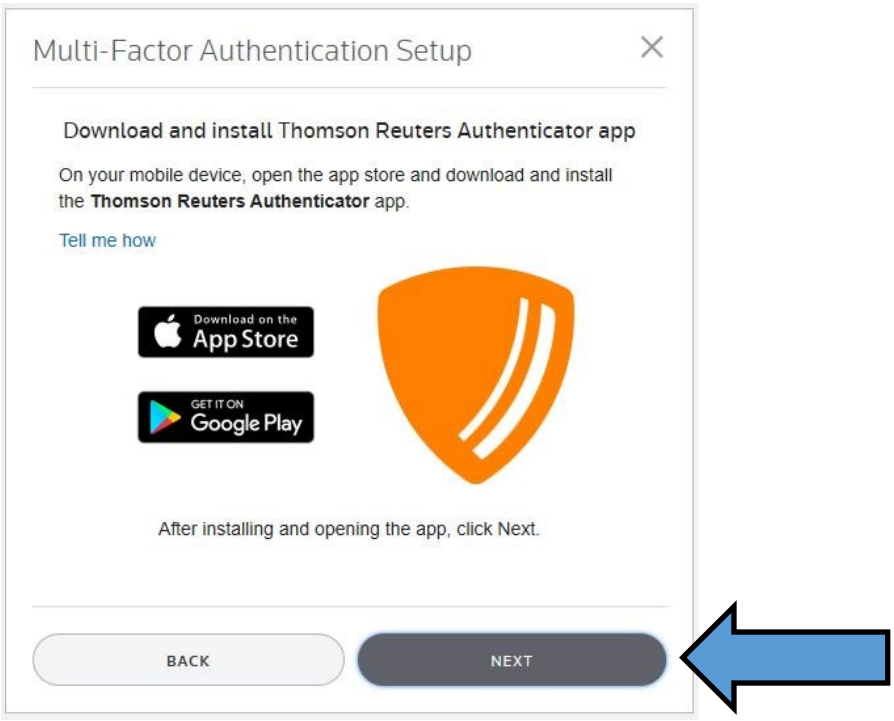
There is the option of using the official Thomson Reuters Authenticator, which is recommended, a third-party authenticator, or a card. This tutorial will only present the recommended Thomson Reuters Authenticator. Click “Choose” on the Thomson Reuter option.



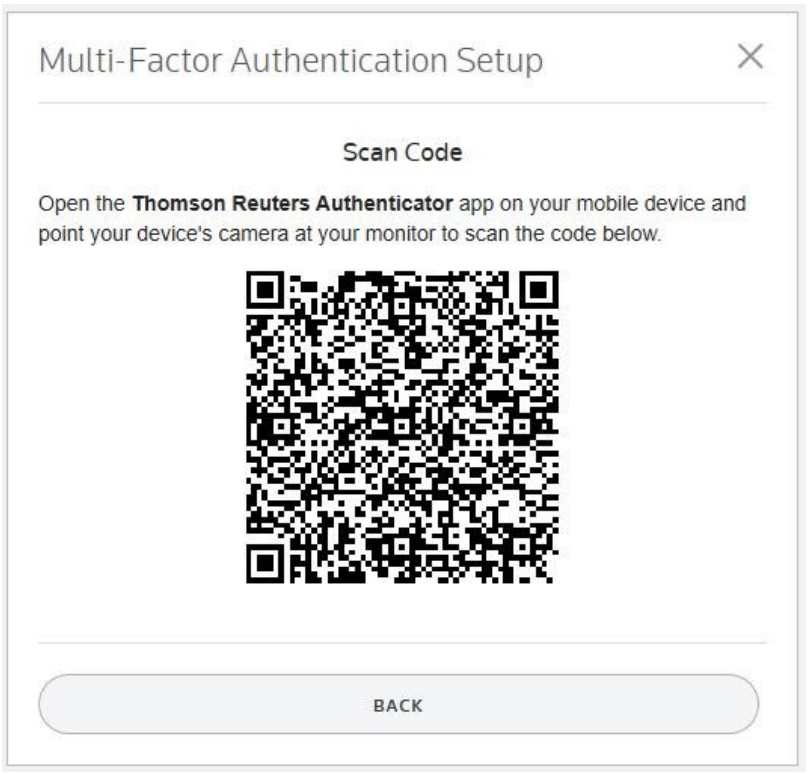
The Thomson Reuters Authenticator is available from both the Android Google Play Store and the Apple App Store. Download the application before proceeding.



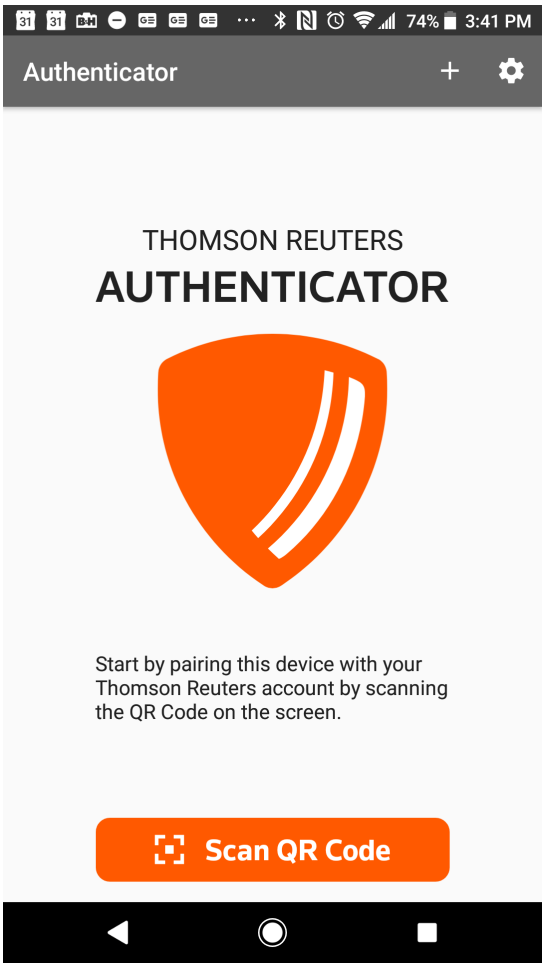
When the application has completed the installation on the mobile device, click the “Next” button to proceed.



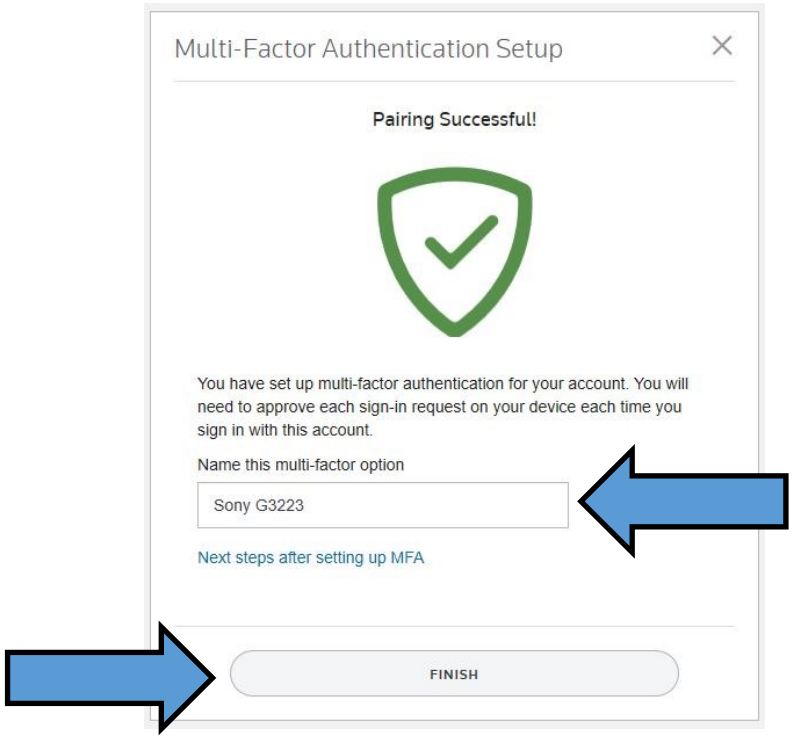
A QR code will be produced which should be scanned using the mobile device.



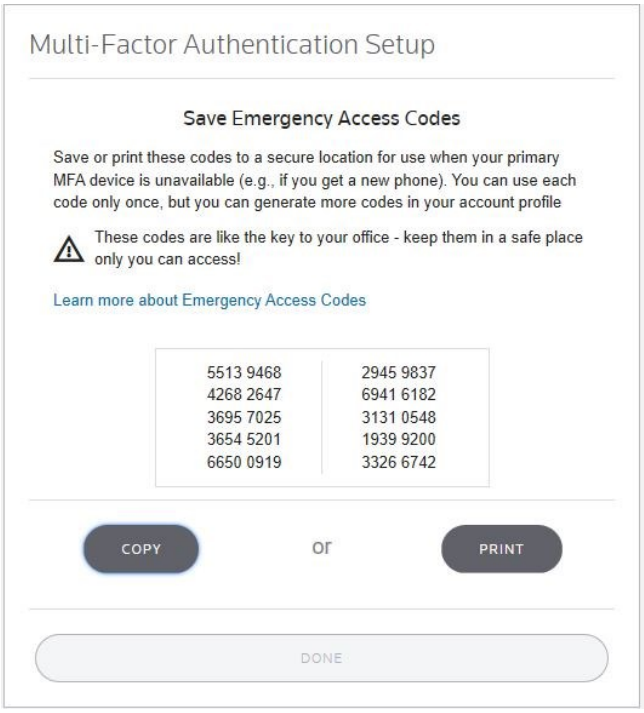
Launch the Thomson Reuters Authenticator and click the “Scan QR Code” button to scan the code.



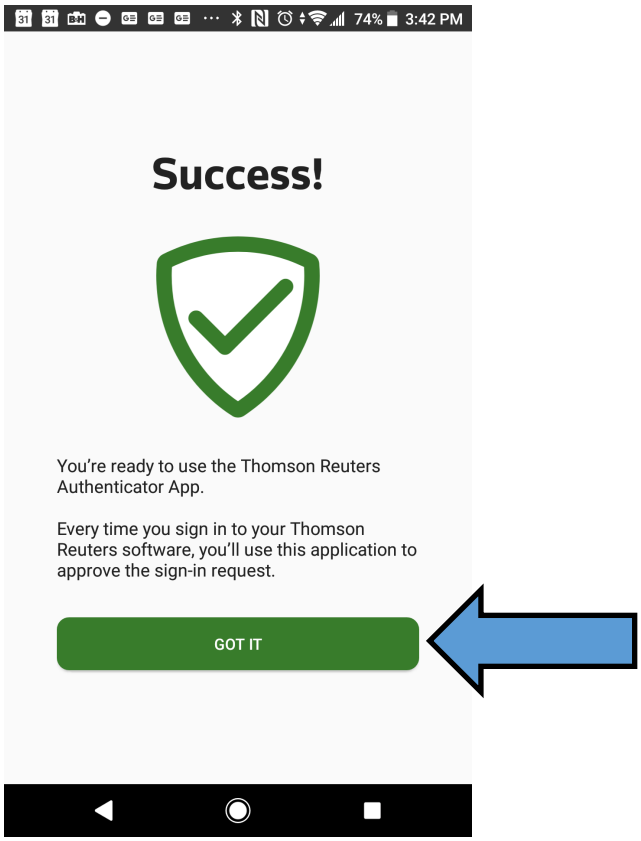
Scanning the code will pair the mobile device with the account, and a confirmation will be presented. There will also be a field in which the multi-factor option can be given a friendly name. The name of the mobile device will be pre-filled in the field, but this can be changed. Once any changes are made click “Finish”.



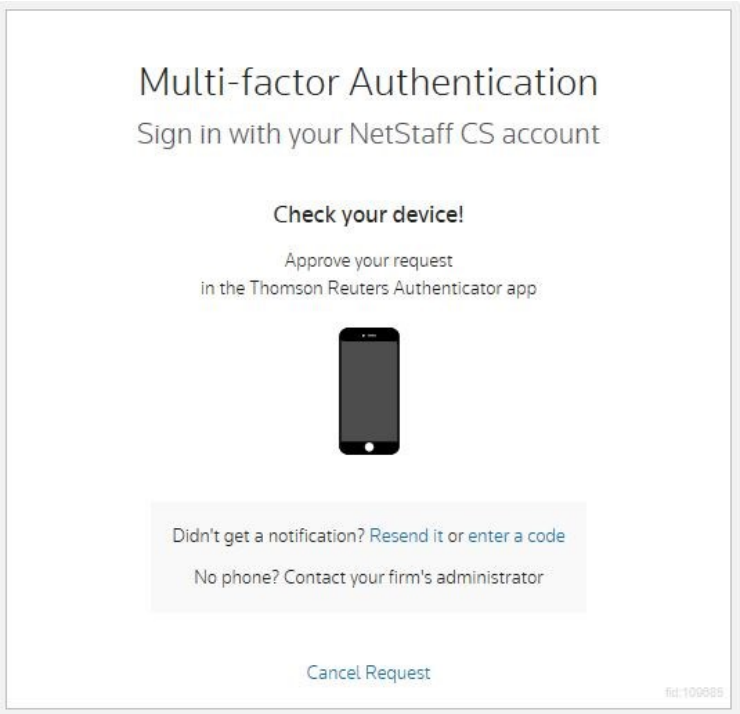
Ten codes will be presented at this time. Save these codes in the event that the paired device is not present. These codes can also be used when pairing the account to a new device.



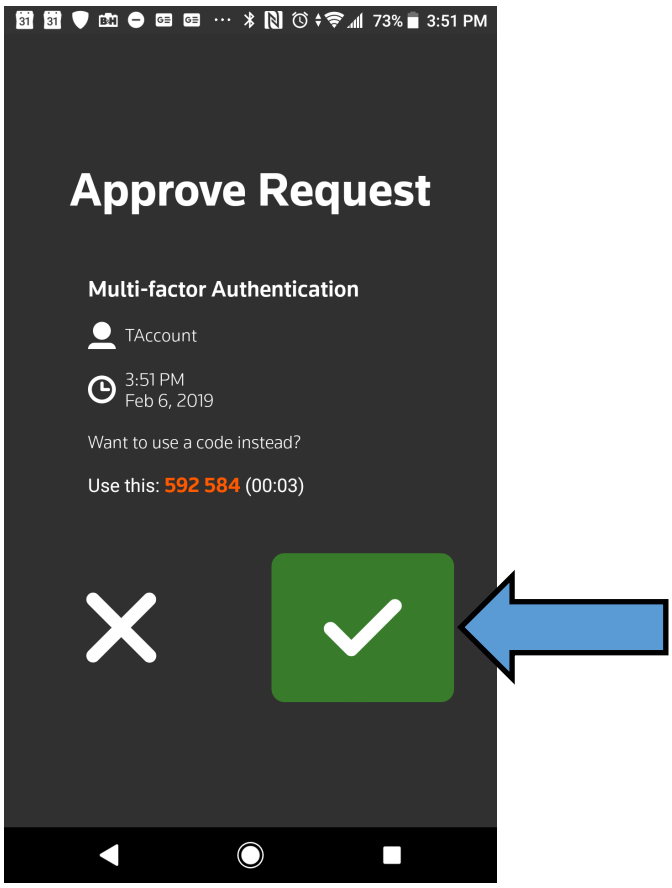
The mobile device will also confirm the pairing. Click “Got It” to proceed.



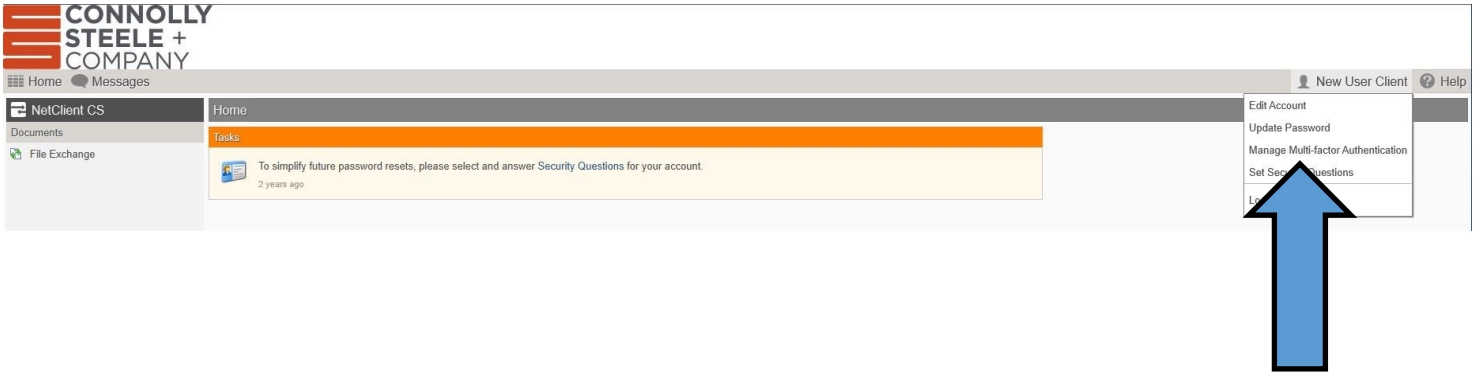
At this point, and after the username and password are entered on future logins, NetClient will prompt to check the mobile device for an approval request.



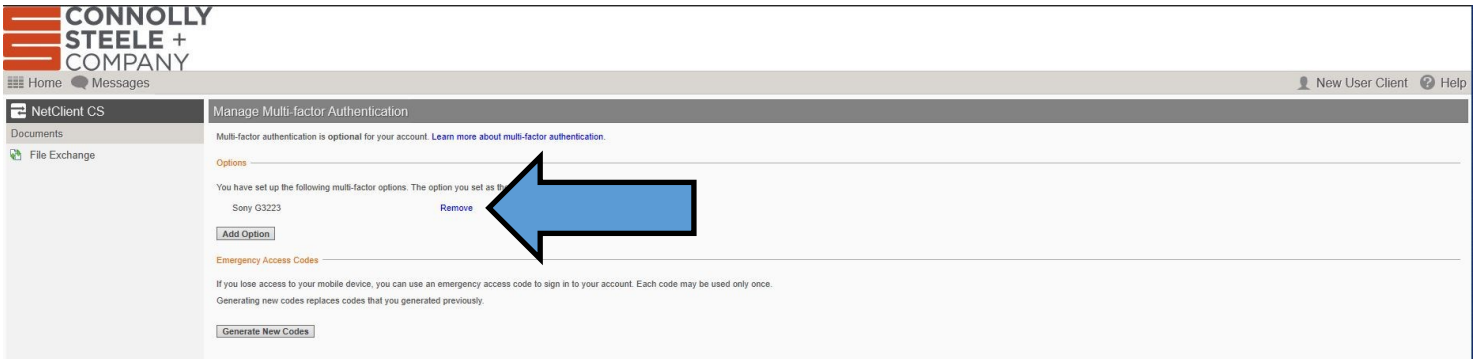
Open the Thomson Reuters Authenticator and click the green box with a white checkmark to approve the sign in request and enter the account.



To deactivate MultiFactor Authentication sign into the NetClient web portal. Click on the account name on the right side of the screen. On the drop down menu click on “Manage Multifactor Authentication.

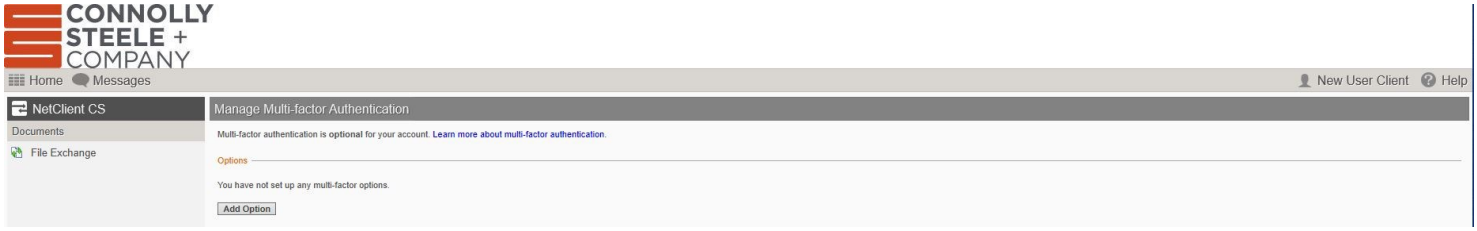


Under the “Options” heading the mobile device paired to the account is listed. Click on “Remove” to the right of the device to

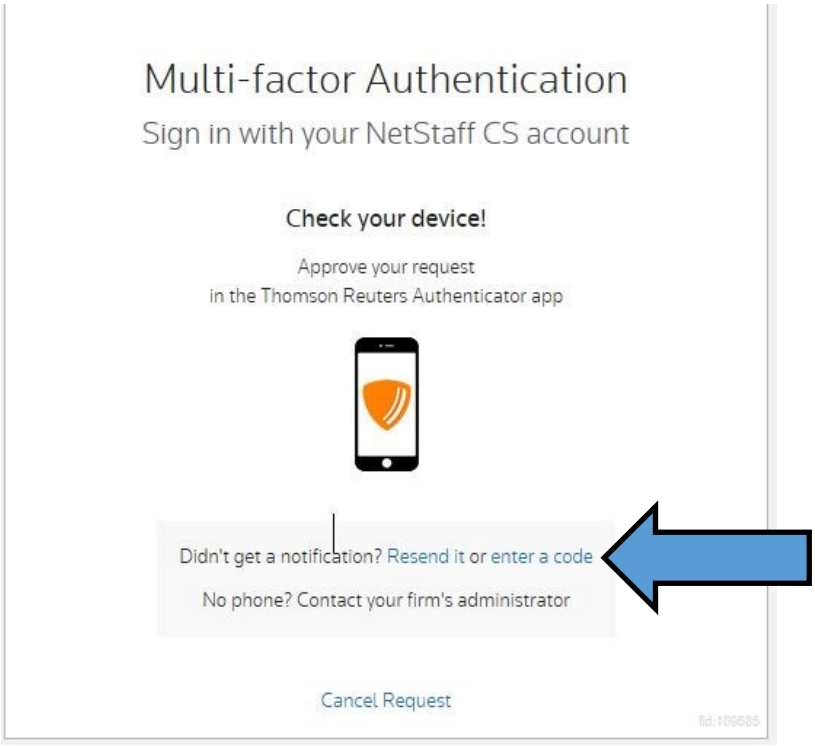


Enter the account password to confirm the deactivation of MultiFactor Authentication.

The account now shows that no MultiFactor Authentication options are activated.



If the mobile device that is paired with the NetClient account is not available, or if it is not receiving the notification, a code will be required to access the account. On the prompt to check the mobile device near the bottom is the option to enter a code. This code can be obtained by calling Connolly, Steele & Co., or you can use one of the codes generated when originally activating multi-factor authentication. When the code is in hand click the "Enter a Code" option.



A field in which the code can be entered will be presented. Enter the code, including any spaces, and click "Go"

Access to the account will be granted.