Two-Factor Authentication Setup

Google Authenticator is a widely used and trusted option for enabling two-factor authentication. Due to this, we've enabled support for it in our system. Google Authenticator generates a 6-digit code to type in after properly authenticating with their username and password.

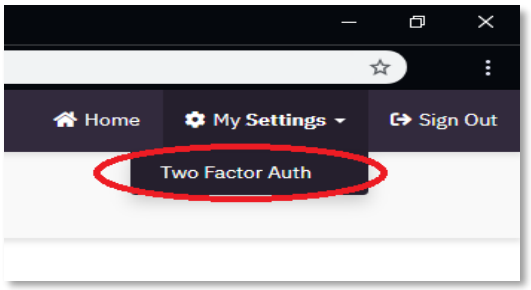
To set up Google Authenticator, you first need to download the official Google Authenticator app on your mobile phone (for Android or iOS).

- iOS: App Store link
- Android: Play Store link

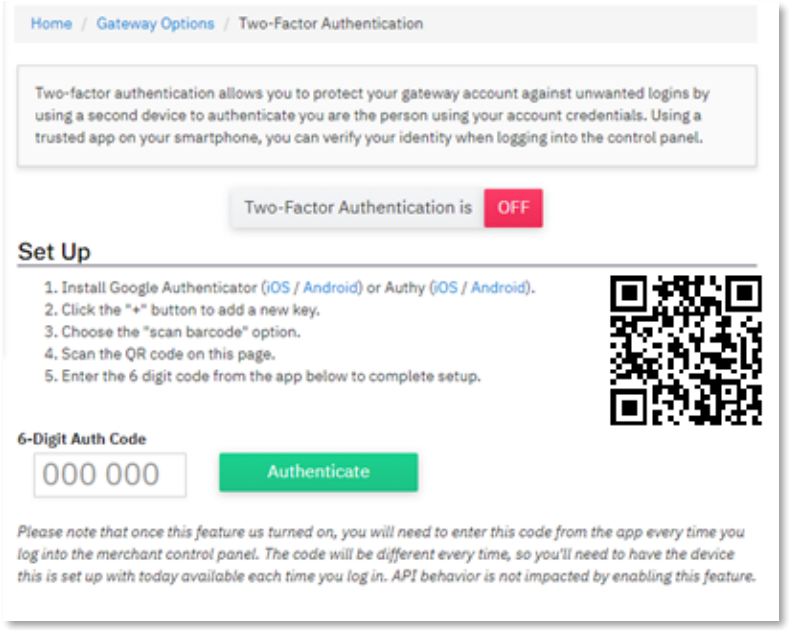
You can also search in your respective device's app store for 'Google Authenticator'.

Setup/Functionality Instructions

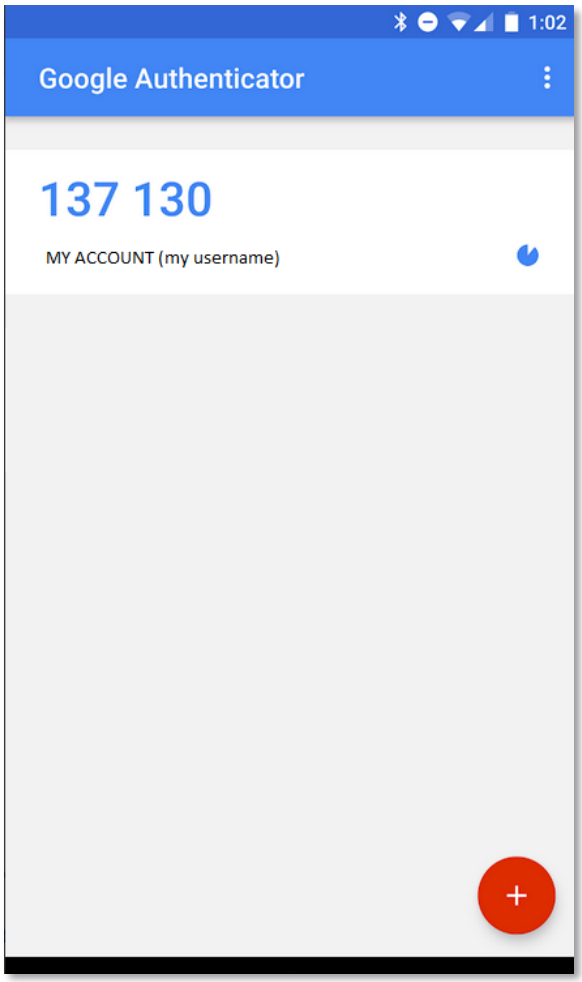
After logging into your user, click the "My Settings" dropdown from the top right-hand corner of the Control Panel, then click the "Two Factor Auth" option.



This will bring you to the screen to configure Two Factor Authentication for your user.

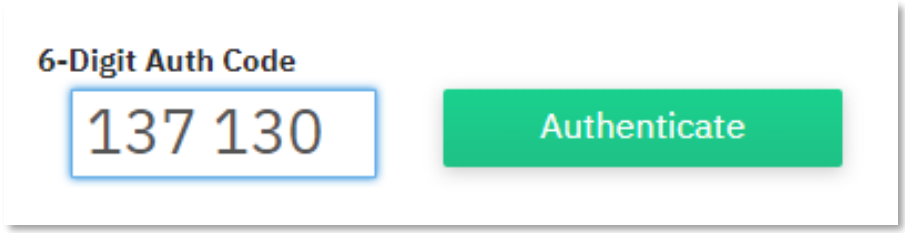


Launch the Google Authenticator application on your smart phone, click the “+”, and choose “Scan a Barcode” to add a new two-factor authentication key to the app.

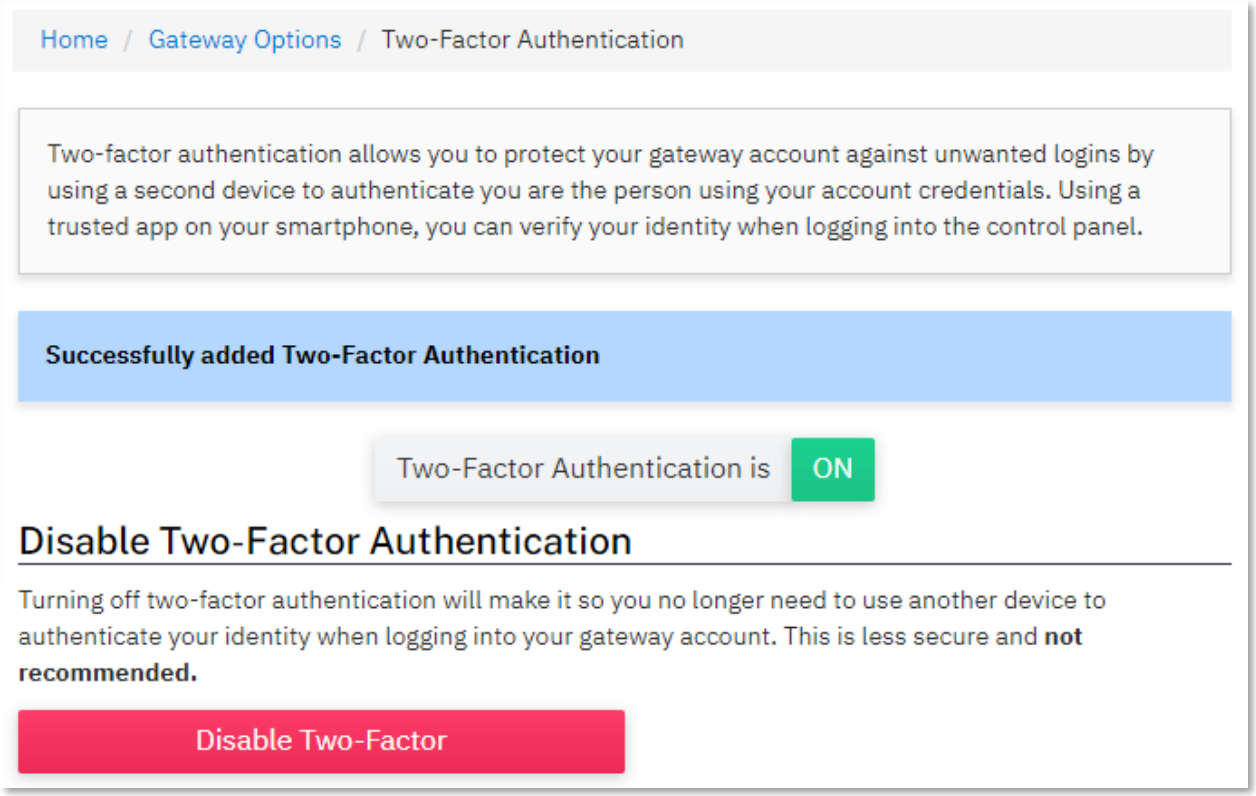


After scanning the QR code displayed on the Control Panel, a new cycling code will appear in your Google Authenticator app, along with an auto-generated title to help remember what account the code is used for.

To finalize setup for your user, enter the 6-digit code displayed in the Google Authenticator app into the box under “6-Digit Auth Code” and click “Authenticate”

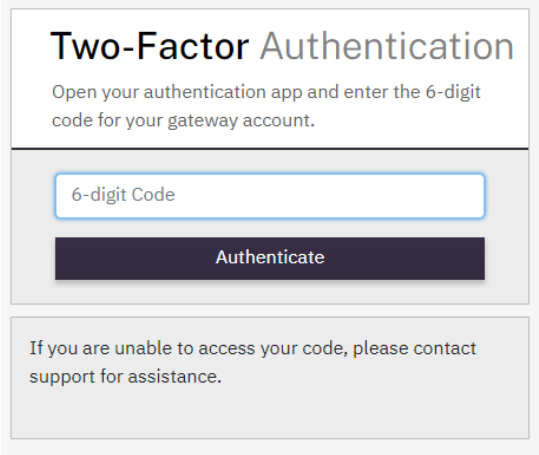


You will be presented with the following screen confirming your two-factor authentication has been successfully configured.



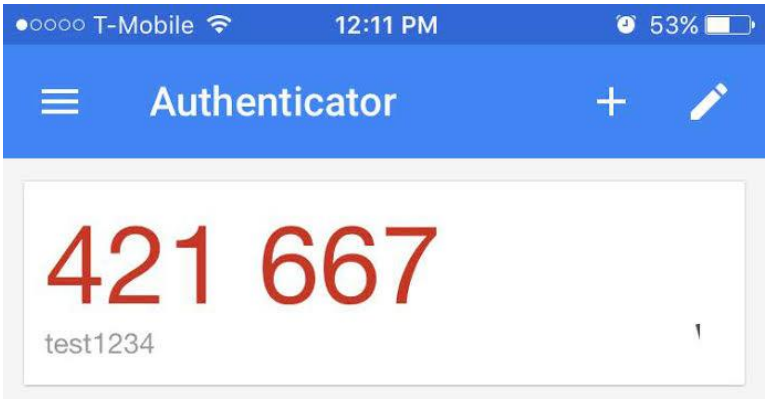
To use Google Authenticator when signing into a Merchant Account:

1. Successfully authenticate with your regular Username and Password
2. You will be prompted to enter in the two-factor authentication code. Launch the Google Authenticator app, enter the current 6-digit code associated with the account name, and click “Authenticate”



Notes

- Google Authenticator codes are available for 30 seconds and are unusable after that time has expired. Codes with 5 seconds left to use will turn red. There is also a small countdown clock icon to the right of each code that will get smaller as time ticks down.



- If a user inputs the wrong Secret Key/Passphrase, enters an expired code, or (after release) attempts to use a code generated from a Key/Passphrase previous to the currently set Key/Passphrase, they will receive ‘Authentication Failed’ when attempting to input their one-time password.