Two-Factor Authentication Setup

Last Modified on 09/10/2026 10:33 am CDT

Google Authenticator is a widely used and trusted option for enabling two-factor authentication, so support for it has been enabled. Google Authenticator generates a 6-digit code to enter after properly authenticating with a username and password.

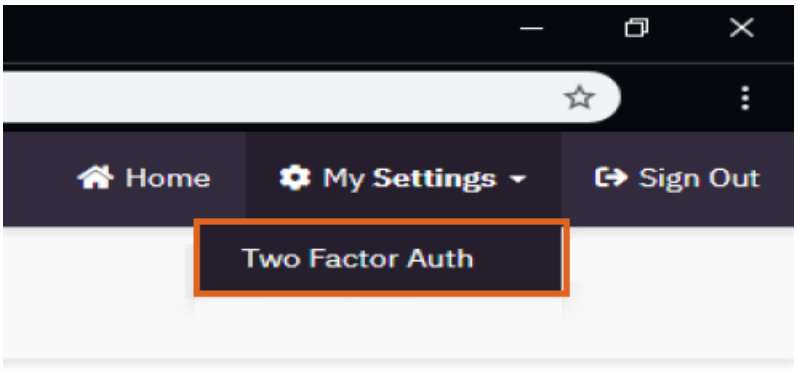
To set up Google Authenticator, download the official Google Authenticator app on a mobile phone (for Android or iOS).

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

Alternatively, search in the device's app store for *Google Authenticator*.

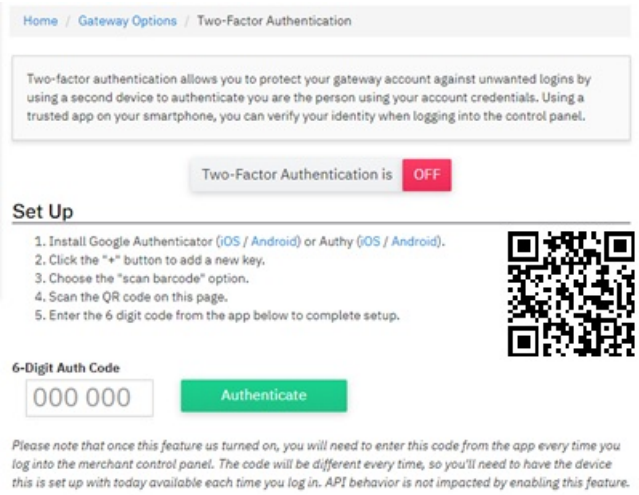
Setup/Functionality Instructions

After logging in, select the *My Settings* drop-down from the top right-hand corner of the *Control Panel*, then select the *Two Factor Auth* option.

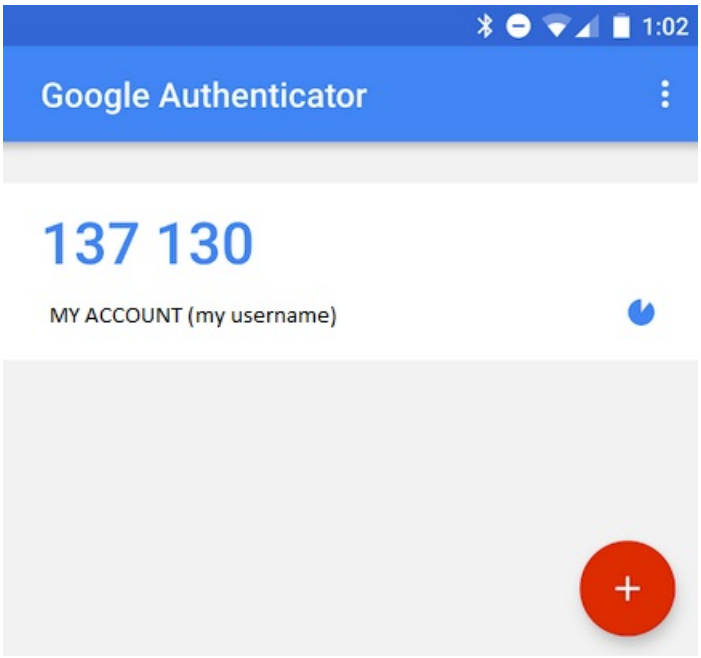


This will navigate to the screen to configure Two Factor Authentication.

Launch the Google Authenticator application, select the **+**, and choose **Scan a Barcode** to add a new two-factor authentication key to the app.

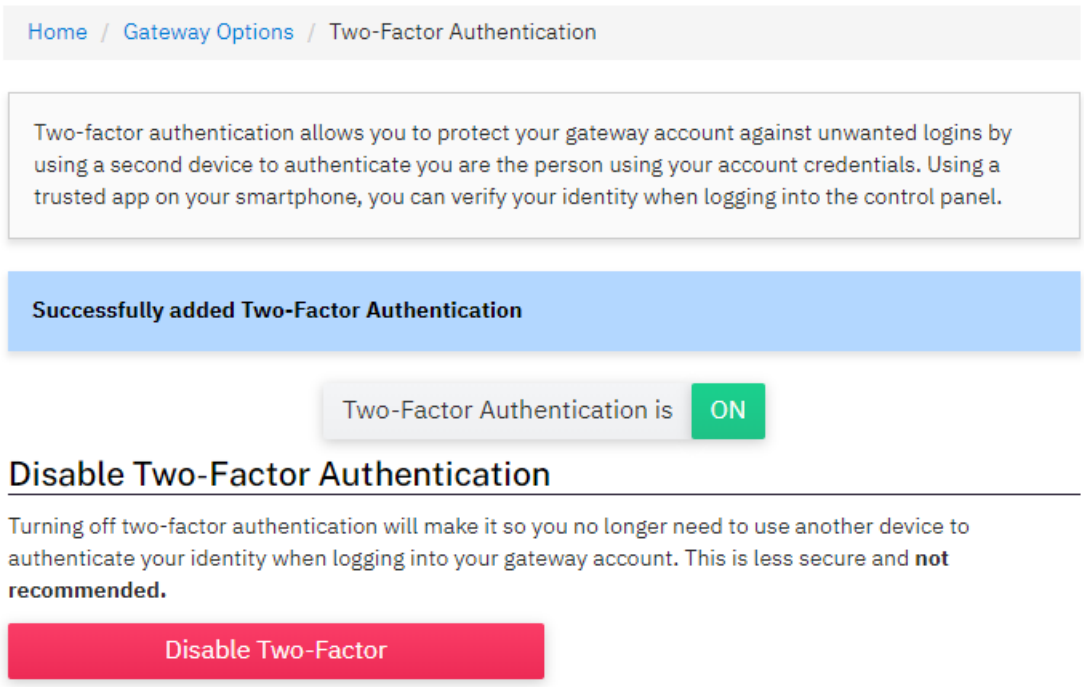


After scanning the QR code displayed on the *Control Panel*, a new cycling code will appear in the Google Authenticator app, along with an auto-generated title to help remember for what account the code is used.



To finalize setup, enter the 6-digit code from the Google Authenticator app into the *6-Digit Auth Code* field and select **Authenticate**.

The following screen will be displayed confirming two-factor authentication has been successfully configured.



Use Google Authenticator when Signing into a Merchant Account

1. Successfully authenticate with the regular *Username* and *Password*.
2. A prompt will display to enter the two-factor authentication code. Launch the Google Authenticator app, enter the current 6-digit code associated with the account name, and select **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 the wrong *Secret Key/Passphrase* is entered, an expired code is used, or (after release) an attempt is made to use a code generated from a *Key/Passphrase* previous to the currently set *Key/Passphrase*, *Authentication Failed* will display when attempting to input the one-time password.