**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 for partners to type in after properly authenticating with their username and password.

To set up Google Authenticator, you need to download the official Google Authenticator app on your mobile phone (for Android or iOS), turn on Two-factor for the desired username, and manually enter the Secret Key provided during setup.

* iOS: [App Store link](https://itunes.apple.com/us/app/google-authenticator/id388497605)
* Android: [Play Store link](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)

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

**Setup/Functionality Instructions**

An account without Two-factor enabled will look as it does today, with unchecked boxes.



After checking the box to “Require Two-factor authentication”, “Use Google Authenticator” will be selected by default.

Upon saving (or creating) the User Account settings, a pop-up window will appear with direct links to download the Google Authenticator apps for iOS and Android, and will display the User’s Secret Key which is required to configure Google Authenticator.

You have the option to create your own Secret Key instead of the one generated; however, it must use only Base32 characters (letters A-Z and digits 2-7).

At this point, you should launch the Google Authenticator app on your mobile phone and set up a new entry within the app before clicking Ok. Google Authenticator does not require linking to a Gmail account.

**Upon Google Authenticator app launch, follow these steps:**

**For New Users of Google Authenticator:**

1. Choose ‘Begin Setup’.
2. Choose ‘Manual entry’ or ‘Enter a provided key’.
3. Enter an Account name. The Account name can be your username, or something else identifiable. It is not tied to the username on the Gateway, this is only for identification in the app.
4. Enter the Secret Key in the ‘Key’ or ‘Your key’ field. It is not case sensitive.
5. Time based is ON (toggled to the right) by default. Users should NOT change this.
6. Click the Check-mark icon in the upper right-hand corner or the ‘ADD’ button to complete.

**For Users who already use Google Authenticator:**

1. Choose the + symbol in the app (The position of this button varies based on phone OS version).
2. Choose ‘Manual Entry’ or ‘Enter a provided key”
3. Follow steps 3-6 above.

Note: Google Authenticator supports a ‘bar-code scan’ setup method, but we do not support that feature currently.

**To use Google Authenticator when signing into a Partner 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 and enter the current 6-digit code associated with the ‘Account name’ (configured in the previous step).

**Notes**

* Partners that wish to use legacy two-factor apps can click ‘Cancel’ when the Google Authenticator pop-up appears. This will cause the legacy Two-factor setup to display.
* If a partner switches between using the legacy Two-factor and Google Authenticator, they will see a warning pop up that they must confirm before proceeding. They can choose ‘Cancel’ to continue using their currently set form of Two-factor Authentication.

**Switching to Google Authenticator**

**Switching to Legacy Authenticator**

* When you switch from legacy two-factor to Google Authenticator, or vice versa, the previous Secret Key or Passphrase (as applicable to the switch) will be unusable. If you want to switch back, you will need to set up the app again using a new Secret Key or Passphrase.
* To generate a new Google Authenticator Secret Key (if a user’s current one isn’t working), click ‘Click to Set’ in their username settings next to Generate Secret Key, and re-set up their app. It is best to delete the old one by clicking the pencil icon in the Google Authenticator app and deleting the entry.

* 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.

* Users cannot edit the secret key entered after setup is complete. If it was not entered properly, they will need to delete the bad entry and start over.
* When a user sets a new Passphrase OR Secret Key (depending on Authentication Method) a warning will appear to notify them that their previous Key/Passphrase will not be usable.

* 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.