Google Authenticator User Guide

User Guide - V1.01

Version Control

Version	Date	Update information
1.01	26/05/2021	Updated formatting and added FAQ section

Table of Contents

Introduction

This guide goes through the steps required to set up the Google Authenticator app. This app allows you to use two-factor authentication (2FA) with the Merchant Management System (MMS). Logging in using 2FA is required to change specific settings within the MMS.

Once configured, you can use the Google Authenticator app to receive codes. You can set up Google Authenticator or another app that creates one-time verification codes when you do not have an internet connection or mobile service. Once you have received the code, enter it on the sign-in screen to confirm it is you.

Alternatively, you can consider using other applications like Authy, LastPass Authenticator etc. NB: this is a one-time registration process, and only one 2FA authenticator can be used per user account.

Step 1: Download the Google Authenticator app to your device

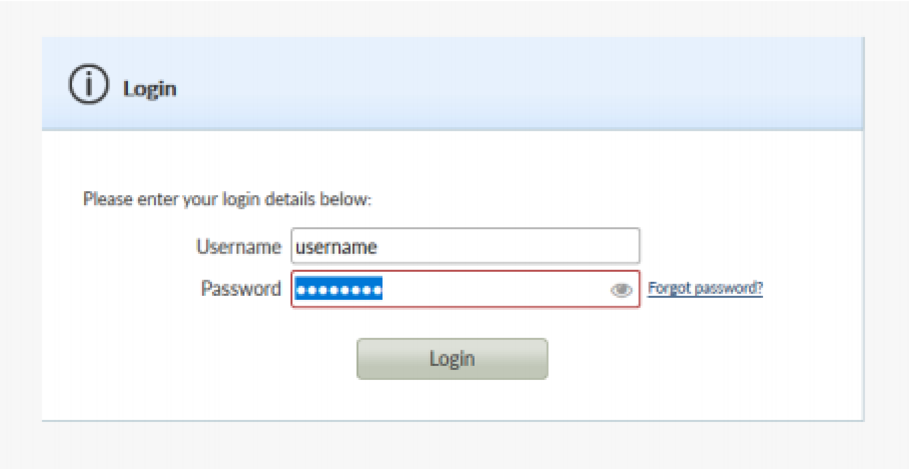
You will need to have the mobile device you want to use at hand. Install the Google Authenticator app to your device. You can download the app below:

iPhone and iPad
Android

Note: make sure the time on your device is set correctly.

Step 2: Log into the Merchant Management System (MMS)

Open the MMS and log in with your user credentials:



Login

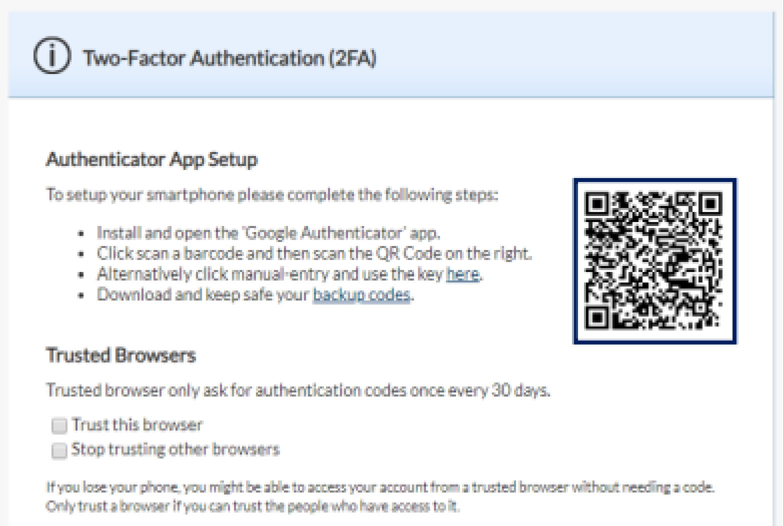
Please enter your login details below:

Username: username

Password: ●●●●●●●●●

Step 3: Link your Device with your MMS account

Open the Google Authenticator App on your device and select '+' in the top right. Select 'Scan barcode and point your mobile device at the PC Screen to scan the QR Code from the MMS.



Two-Factor Authentication (2FA)

Authenticator App Setup

To setup your smartphone please complete the following steps:

- Install and open the 'Google Authenticator' app.
- Click scan a barcode and then scan the QR Code on the right.
- Alternatively click manual-entry and use the key here.
- Download and keep safe your backup codes.

Trusted Browsers

Trusted browser only ask for authentication codes once every 30 days.

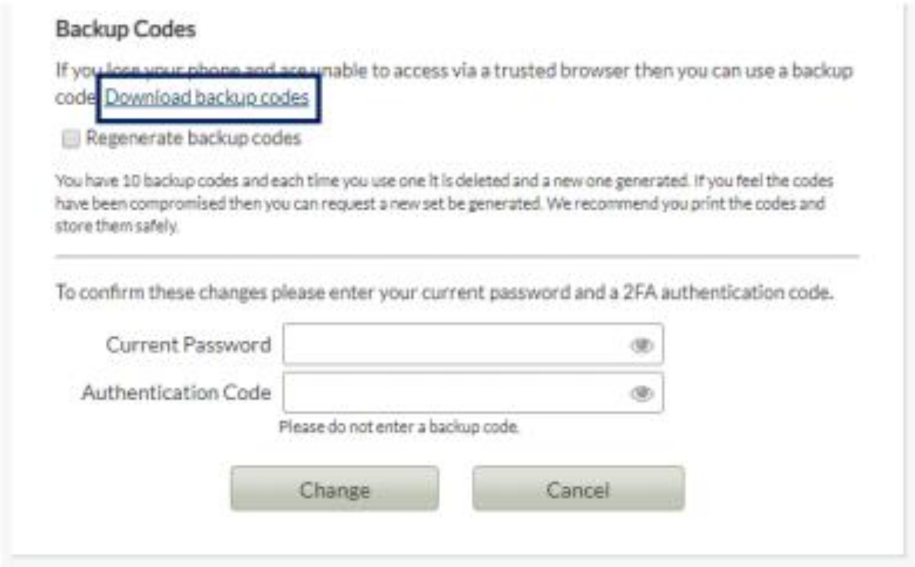
□ Trust this browser
□ Stop trusting other browsers

If you lose your phone, you might be able to access your account from a trusted browser without needing a code. Only trust a browser if you can trust the people who have access to it.

Step 4: Finishing the set-up

Your smartphone will now generate a six-digit number which you will need to enter into the 'Authentication Code' field on the MMS, along with your current MMS Password.

Ensure you download and safely store your backup codes.



Backup Codes

If you lose your phone and are unable to access via a trusted browser then you can use a backup code Download backup codes

□ Regenerate backup codes

You have 10 backup codes and each time you use one it is deleted and a new one generated. If you feel the codes have been compromised then you can request a new set be generated. We recommend you print the codes and store them safely.

To confirm these changes please enter your current password and a 2FA authentication code.

Current Password

Authentication Code

Please do not enter a backup code.

Frequently Asked Questions

How can I transfer Google Authenticator codes to a new device?

You need:

- Your old phone with Google Authenticator codes
- The latest version of the Google Authenticator app installed on your old phone
- Your new phone

1. On your new phone, install the Google Authenticator app.
2. In the app, tap Get Started.
3. At the bottom, tap Import existing accounts?
4. On your old phone, create a QR code:
    1. In the Authenticator app, tap More ⋮ › Transfer accounts › Export accounts.
    2. Select which accounts you want to transfer to your new phone, and then tap Next.
        - If you transfer multiple accounts, your old phone may create more than one QR code.
5. On your new phone, tap Scan QR code.
6. After you scan your QR codes, you get a confirmation that your Google Authenticator accounts have been transferred.

Tip: If your camera cannot scan the QR code, it may be that there is too much info. Try to export again with fewer accounts.

What can I do if my phone is lost or stolen?

You have several ways you can get back into your account, depending on your circumstances:

1. **Use backup options**

If you have lost access to your primary phone, you can verify it’s you with:

- Another phone signed into your Google Account.
- Another phone number you’ve added in the 2-Step Verification section of your Google Account.
- A backup code you previously saved.
- A security key you’ve added in the 2-Step Verification section of your Google Account.

2. **Sign in from a trusted device**

If you previously signed in from a device and checked the box next to “Don’t ask again on this computer,” you might be able to sign in from that device without a second verification step. After you sign into your Google Account, you can manage your verification methods.

3. Get a new phone from your carrier

If you lose your phone, you can ask your carrier to transfer your phone number to a new phone or SIM card.

4. Recover your account

If you can’t sign in, follow the steps to recover your account. If you are having trouble, try the tips to complete account recovery steps.