



Login Using Google Authenticator

Detailed Instructions on How to
Download and Use Google Authenticator

Multi-Factor Authentication (MFA)

What is Multi-Factor Authentication?

- Multi-Factor Authentication (MFA) adds another layer of security to verify a user's identity by combining factors that identify an individual.
 - What the user knows (such as a username and password)
 - What the user has (such as a phone or tablet device that generates a token)
 - What the user is (such as a fingerprint, iris scan etc.)*
- Not all applications require MFA. Users will be prompted for MFA only when it is required for a specific application.
- OneHealthPort currently offers two ways users can opt to complete their Multi-Factor Authentication
 - One-Time Passcode (OTP) sent to the user's email
 - Google Authenticator Token

What is Google Authenticator?

- Google Authenticator is a free App that is downloaded to a user's mobile or tablet device that generates a six to eight-digit passcode which must be provided in addition to the username and password to login.
 - The App is free and does not use cell phone minutes or data
 - Users do not need to create a Google account

***NOTE: Currently OneHealthPort does not use this type of identity verification to authenticate users.**

Login Using Username and Password



Subscriber ID:

Password:

[Login](#)

This login page requires that you have registered as a OneHealthPort Subscriber.

[I'm not a OneHealthPort Subscriber but would like information on subscribing](#)
[Forgot My Password](#)
[Forgot My Subscriber ID](#)

Login to the Application you are trying to access with your OneHealthPort Single Sign-On (SSO) Subscriber ID (username) and password.

Multi-Factor Authentication



CHOOSE AN AUTHENTICATION METHOD

The application you are trying to access required multi-factor authentication. Please select an authentication method from the list below.

- One Time Password
- Google Authenticator Token
- [? What is this?](#)

Submit



Click on the “what is this?” link to learn more about Multi-Factor Authentication and links to detailed instructions and FAQs

MFA Web Page

OneHealthPort

Multi-Factor Authentication

Multi-factor authentication (MFA) enhances the security of your account by requiring multiple methods to verify your identity. These can include something you know (like your user name and password) plus something you have (like a smartphone app or individual email account) to approve your login. This prevents your account from being accessed by anyone other than yourself, even if they know your password.

Not all OneHealthPort applications require Multi-factor authentication. When you try to access an application, if it requires multi-factor authentication; you will be directed to complete additional login steps.

OneHealthPort provides your organization with 2 options for implementing the Multi-factor authentication:

- One Time Passwords (OTP)

An email will be sent to you with a one time password that you enter in the login screen to proceed with login

- Google Authenticator Token

The Google authenticator app on your smartphone (instructions on how to download the App on your phone and provision it will be emailed to you) will generate a unique code that you enter in the login screen to proceed.

Click on the following guides to learn more about how to use each of the multi-factor authentication methods:

[Click here to download the step-by-step guide to use the One Time Password \(OTP\)](#)

[Click here to download the step-by-step guide to use the Google Authenticator](#)

For answers to our frequently asked questions on Multi-Factor Authentication [click here](#)

For additional questions/concerns please contact [OneHealthPort Support Desk](#)

Google Authenticator Token



CHOOSE AN AUTHENTICATION METHOD

The application you are trying to access required multi-factor authentication. Please select an authentication method from the list below.

- One Time Password
- Google Authenticator Token

 [What is this?](#)

Submit

Select "Google Authenticator Token" and click "Submit."

First Time Using Google Authenticator

Your software token was issued successfully. Please check your email for further instructions.

Ok



MULTIFACTOR AUTHENTICATION

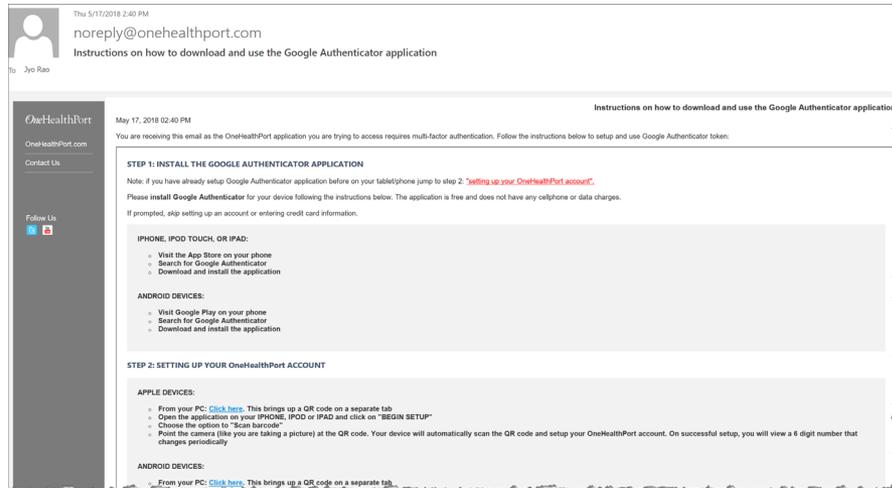
The application you are trying to access requires multi-factor authentication. To verify your identity, enter the code generated by the Google Authenticator application on your smartphone or tablet.

Verify

[Click here to email instructions on how to download the Google Authenticator application](#)

If the user is using Google Authenticator for the first time, click the hyperlink. The system will email detailed instructions to the email affiliated with the user's OneHealthPort SSO account to download the App to a smartphone or tablet device and link the Authenticator to the user's OneHealthPort SSO account.

Emailed Instructions for Installing and Using Google Authenticator



The content in this email gives directions for:

- Downloading the application
- Linking it to the user's OneHealthPort SSO account
- Using the Authenticator passcode

Detailed Instructions to Download Google Authenticator

Step-by-step instructions for downloading the Google Authenticator App and linking it to the user's OneHealthPort SSO account:

- [Instructions for Apple Devices](#) (Slide 10)
- [Instructions for Android Devices](#) (Slide 25)

Instructions for Apple Devices

Access the App Store



Tap on the App Store icon. If it's the first time opening the App Store, the user will be prompted to:

- Login with Apple ID and password
- Enter payment details (this step can be **SKIPPED***)

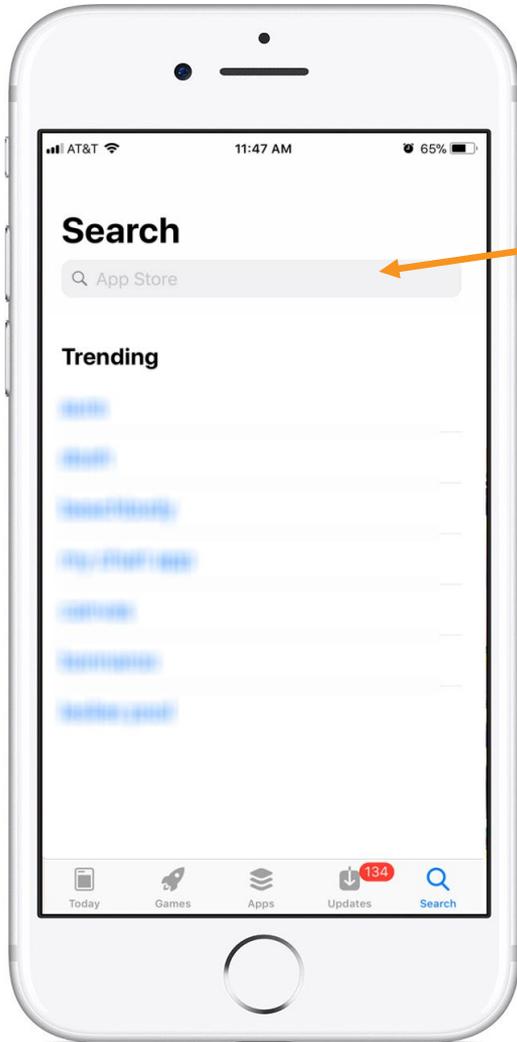
*For more information on how to skip adding payment information see <https://support.apple.com/en-us/HT204034#iOS>

Search for an App in the App Store



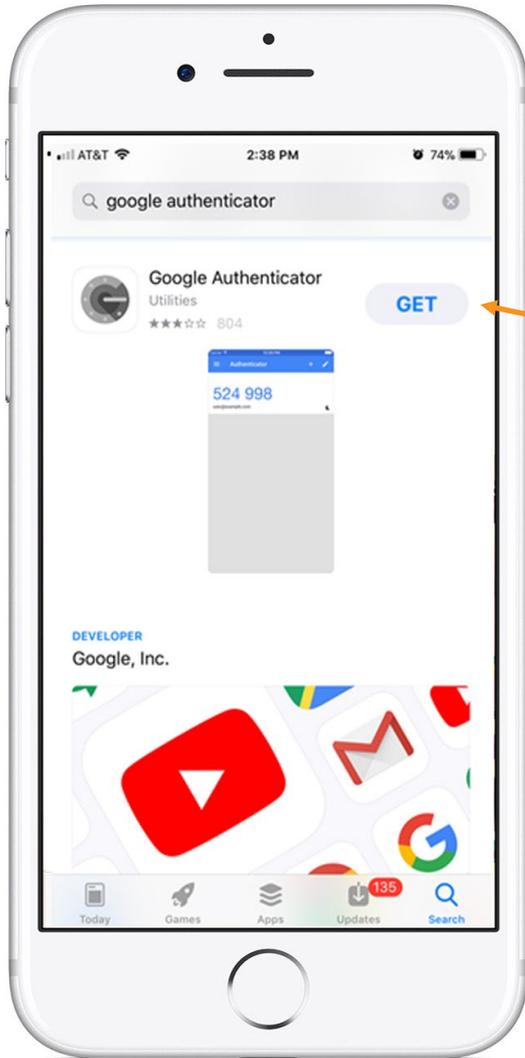
Tap the Search key. It's the key that looks like a magnifying glass at the phone's bottom right corner.

Search for Google Authenticator



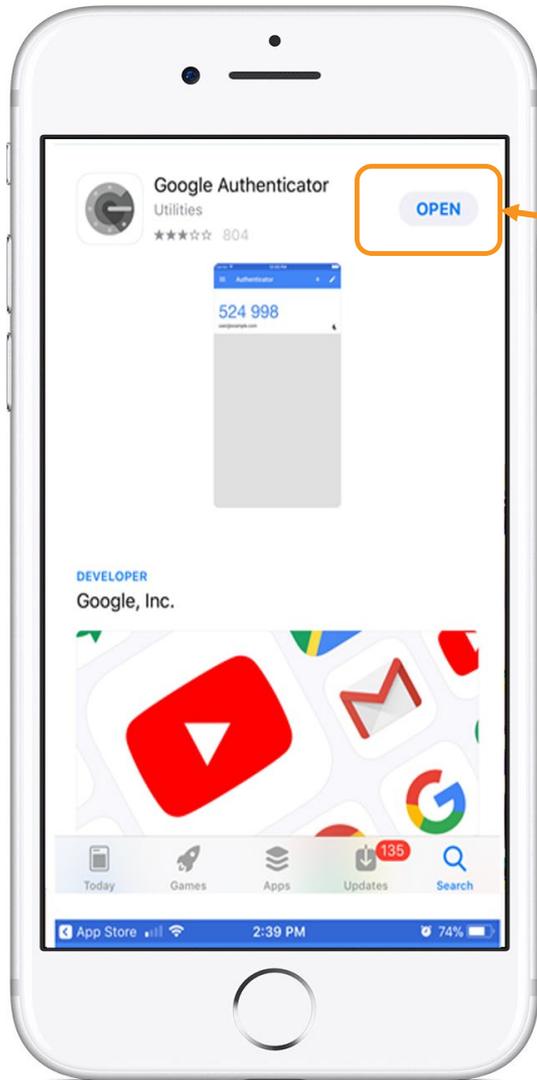
In the Search function, the device brings up the search box. Type “**Google Authenticator**”.

Download Google Authenticator



Once you find the App, tap on **“GET”** to start downloading the App.

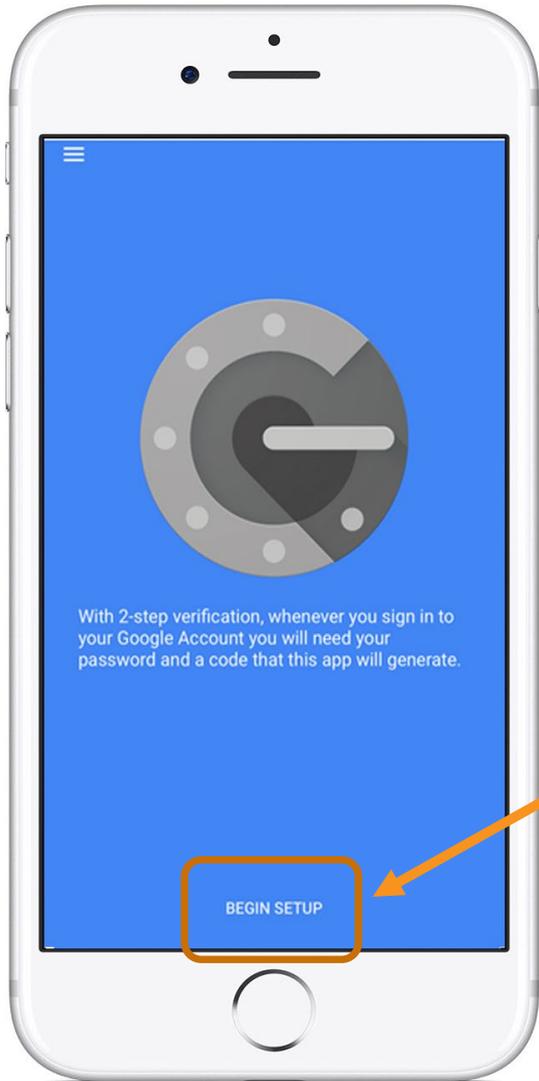
Open the App



Tap on **“OPEN”** once the App has completed the download.

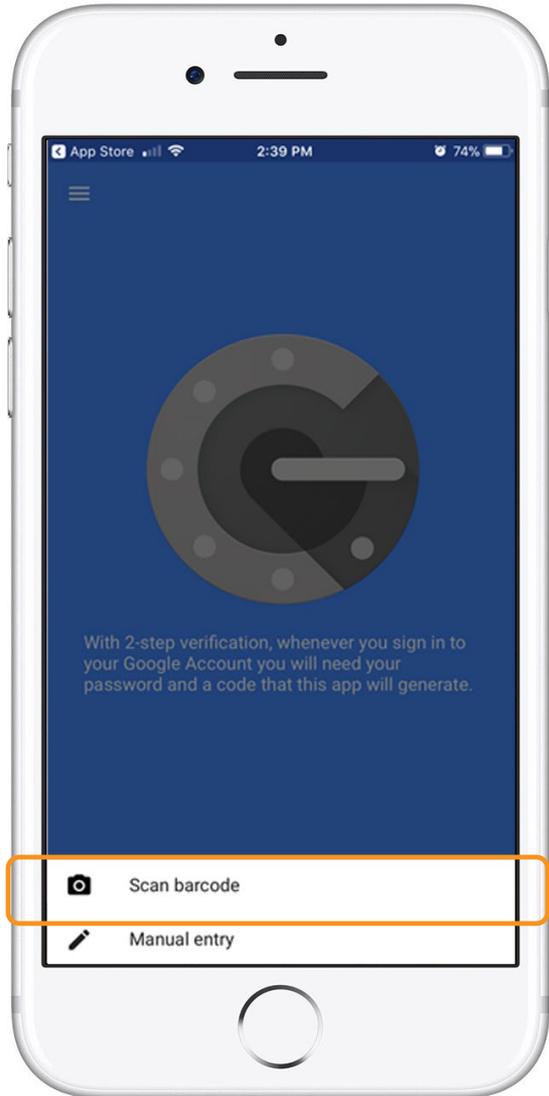
Linking the App to the User's OneHealthPort SSO Account

Setup



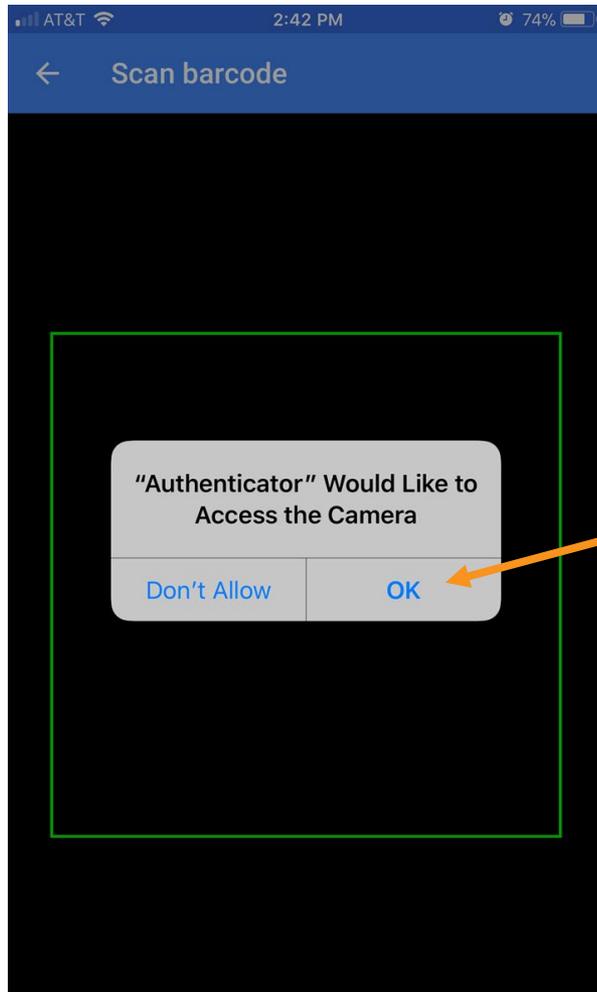
Tap on **“Begin Setup”**.

Scan Barcode



Tap on **“Scan barcode”**.

Authenticator Access to the Camera



The Authenticator requires access to the device camera to complete the linking process with the OneHealthPort SSO account. Tap on "OK".

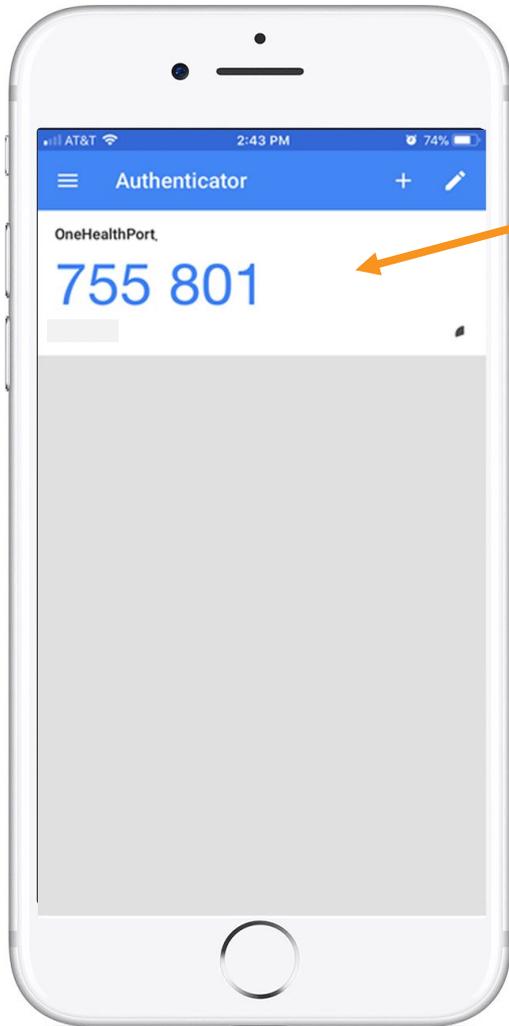
Linking to OneHealthPort SSO Account



STEP 1: From the email (on computer), click on the link to open a QR code.

STEP 2: Using the device camera, scan the QR code **on computer screen** to automatically link the Google Authenticator to the OneHealthPort SSO account.

Successful Link to OneHealthPort Account



Linking is successful to the user's OneHealthPort SSO account when a periodically changing 6-digit number (passcode) displays and "OneHealthPort" is above the passcode.

Using the Passcode

MFA Verification Using The Passcode

When access to applications require MFA, a prompt screen will appear for use in entering the passcode. Enter the passcode from Google Authenticator on your device and click on “**Verify**”.

OneHealthPort



MULTIFACTOR AUTHENTICATION

The application you are trying to access requires multi-factor authentication. To verify your identity, enter the code generated by the Google Authenticator application on your smartphone or tablet.

Enter Verification Code

Verify

[Click here to email instructions on how to download the Google Authenticator application](#)

Successful Login to the Application

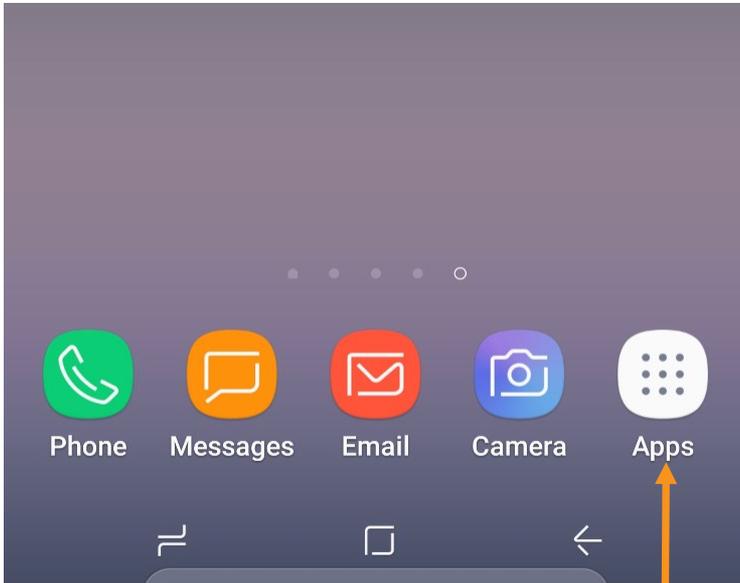
The screenshot displays the OneHealthPort application interface. At the top left is the OneHealthPort logo. To its right is a search bar with a plus sign, the text 'Find Patients', and a magnifying glass icon. Further right is a user profile icon and the text 'Logout'. Below the navigation bar, the interface is divided into two main sections. The left section is titled 'Notifications' and features a dropdown menu set to '10 days' and a table with columns 'Name', 'Subject', and 'Received'. The table content is 'There is no data available'. The right section is titled 'Recent Patients' and shows a list of patient records with star and trash icons for each entry.

Successful entry of the passcode will permit access to the application.*

* Note: The above screenshot is an example of one of OneHealthPort's applications.

Instructions for Android Devices

Access the Play Store



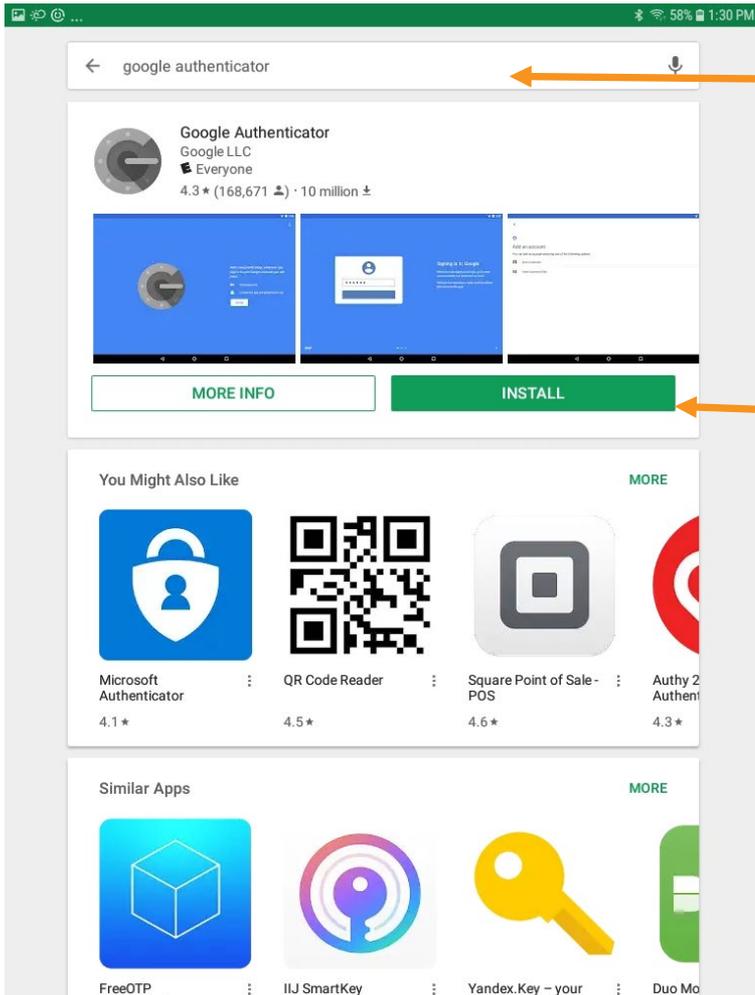
STEP 1: Tap on the “Apps” icon



STEP 2: Tap on the “Play Store” icon

If it's the first time opening the Play Store, the user will be prompted to enter Google account information and payment details. This step can be **SKIPPED**.

Search for Google Authenticator

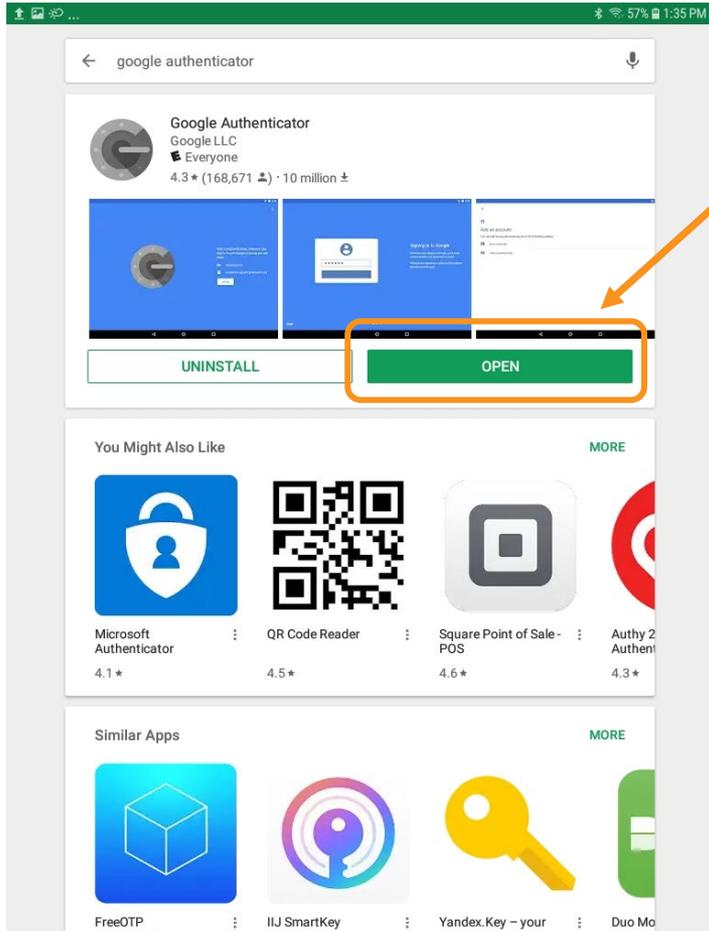


Type “Google Authenticator” in the Search box.

Once the Google Authenticator App is found, tap on “INSTALL” to start downloading the App.

Open the App

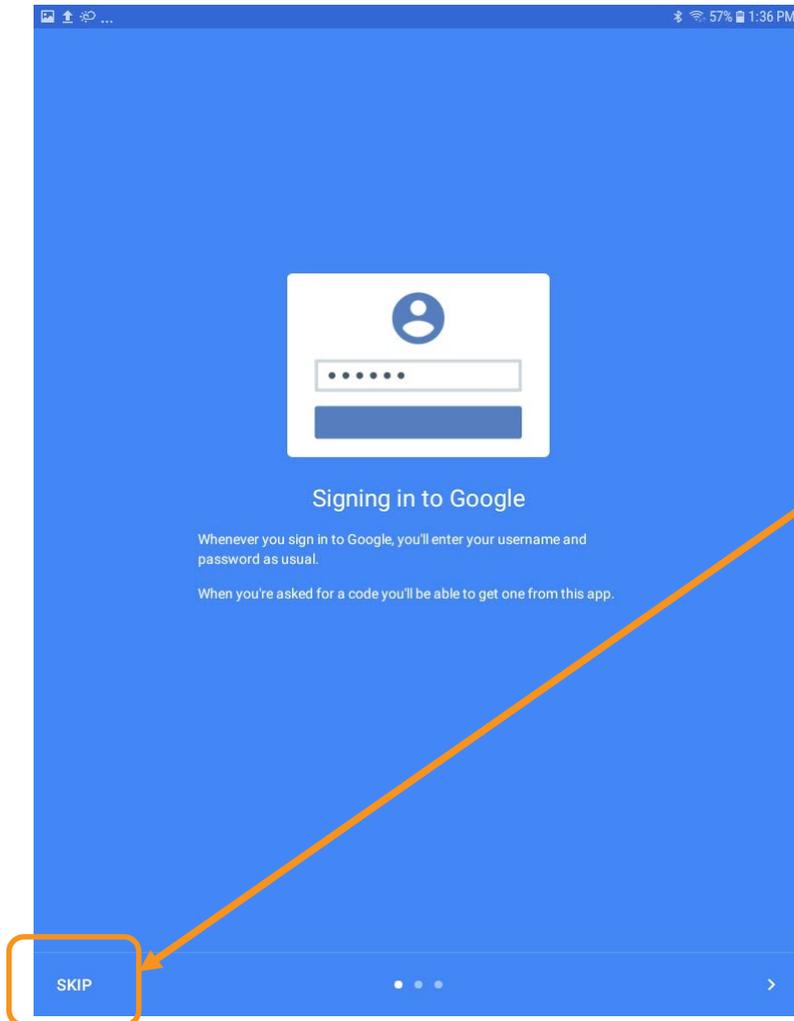
Tap on **“OPEN”** once the App has completed the download. App may also be accessed from the icon on the home screen.



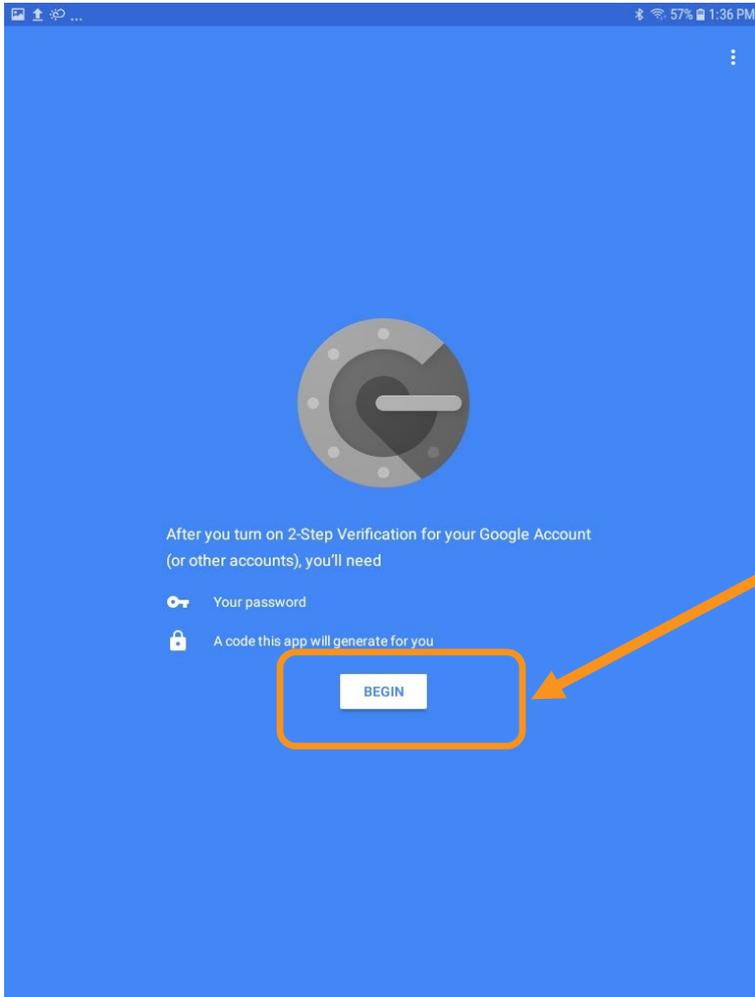
Linking the App to the User's OneHealthPort SSO Account

Setup

Open the Google Authenticator App. **Skip** the Signing in to Google.

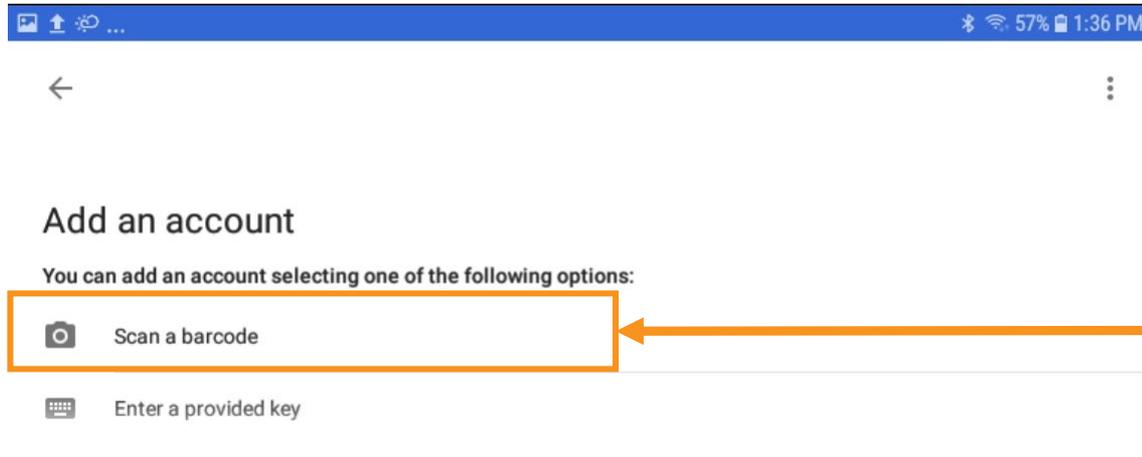


Begin



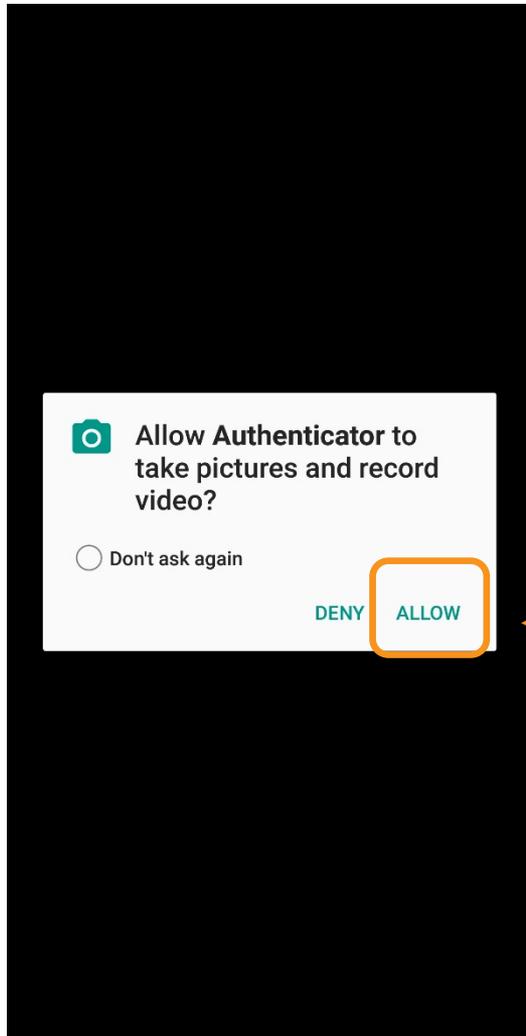
Tap to **Begin** setup.

Scan a Barcode



Tap to **Scan a barcode.**

Authenticator Access to the Camera



The Authenticator requires access to the device camera to complete the linking process with the SSO account. Tap on **“ALLOW”**.

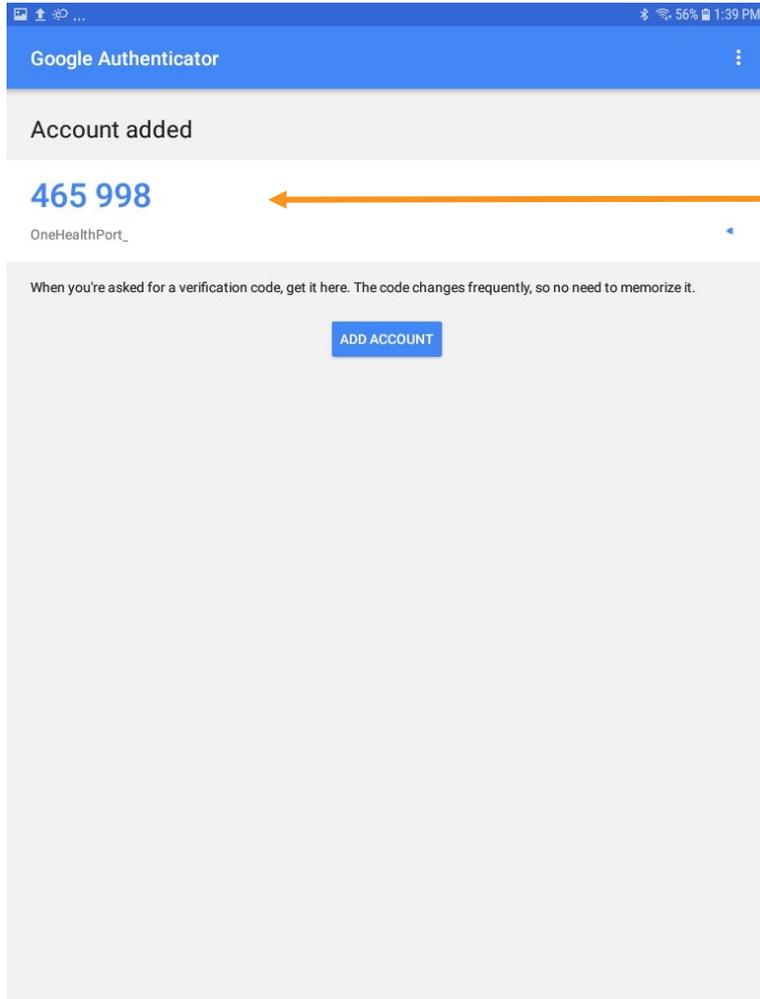
Linking to OneHealthPort SSO Account



STEP 1: From the email (on computer), click on the link to open a QR code.

STEP 2: Using the device camera, scan the QR code **on computer** to automatically link the Google Authenticator to the OneHealthPort SSO account.

Successful Link to OneHealthPort Account

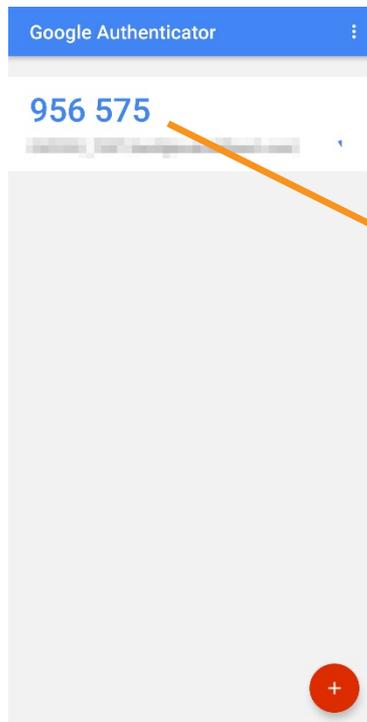


Linking is successful to the user's OneHealthPort SSO account when a periodically changing 6-digit number (passcode) displays and "OneHealthPort" is below the passcode.

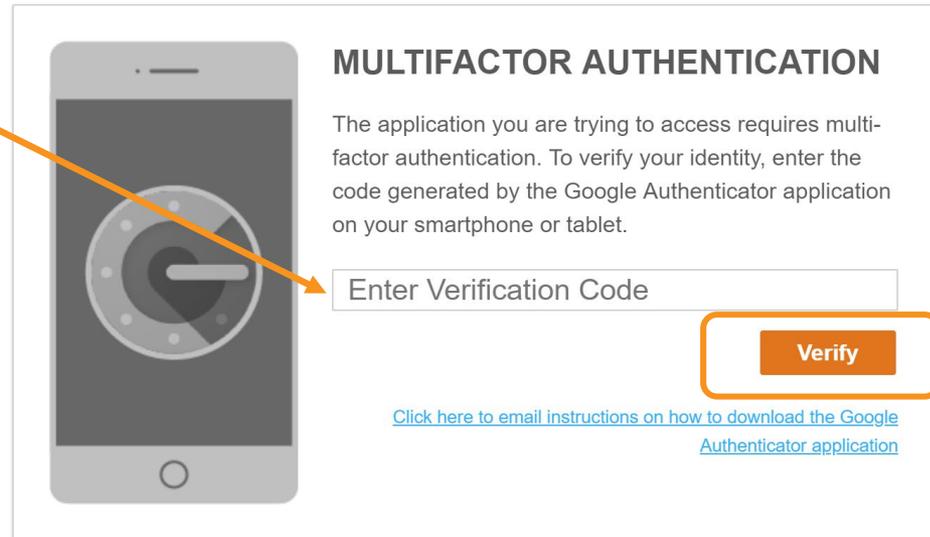
Using the Passcode

MFA Verification Using The Passcode

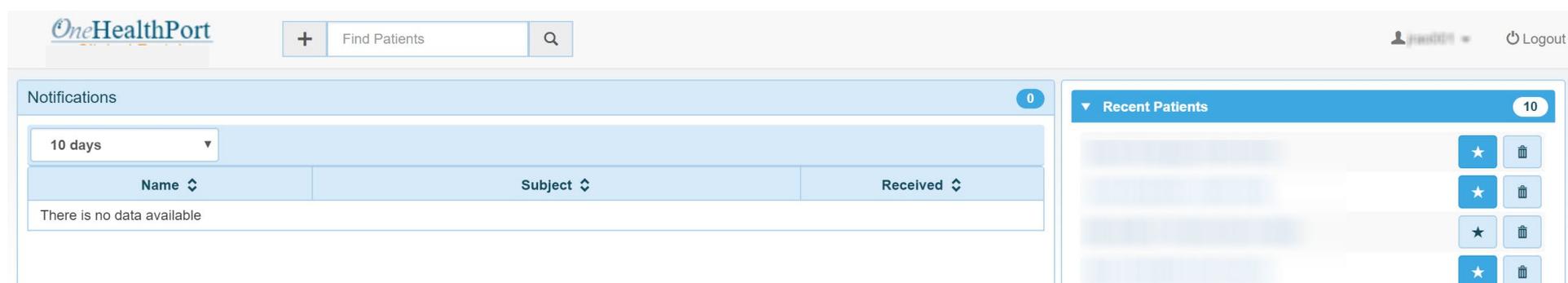
When access to applications require MFA, a prompt screen will appear for use in entering the passcode. Enter the passcode from Google Authenticator on your device and click on “**Verify**”.



OneHealthPort



Successful Login to the Application



Successful entry of the passcode will permit access to the application.*

* Note: the above screenshot is an example of one of OneHealthPort's applications.