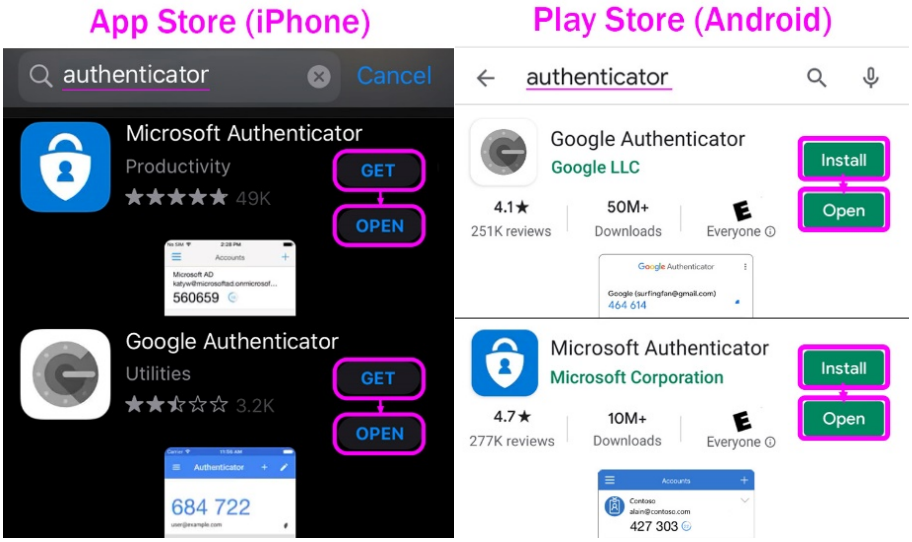
Intermountain 2-Factor Google / Microsoft Authenticator Configuration Guide

2-Factor Authentication is currently an option for many types of online account types e.g. Google, Microsoft, Facebook, Amazon and others. Because you may already be using either the Google or Microsoft Authenticator app for other accounts and because the setup of either is very similar, this guide covers both. Each time you log into certain Intermountain applications, you have the option to use either **Authenticator** app to generate a 6-digit code as the last step of the login process. This setup guide covers how to configure the app on your smartphone.

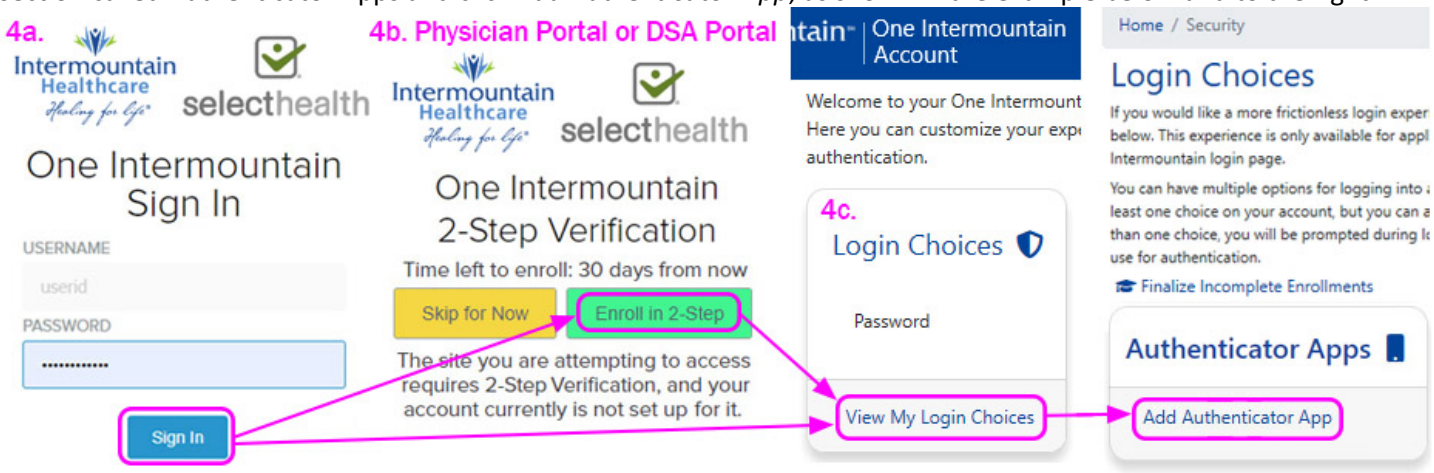
1. *Before stepping through this tutorial:* Although Authenticator requires no additional configuration on your account, you will want to assure that the Physician Portal, DSA Portal, SecureAccess (Remote), Citrix VDI and/or imail2 access has been added to your account.

2. Based on your phone type, open the Apple App Store (iPhone) or Google Play Store (Android) then search for ***authenticator*** and choose either the Google or Microsoft version from the search results, as shown below:

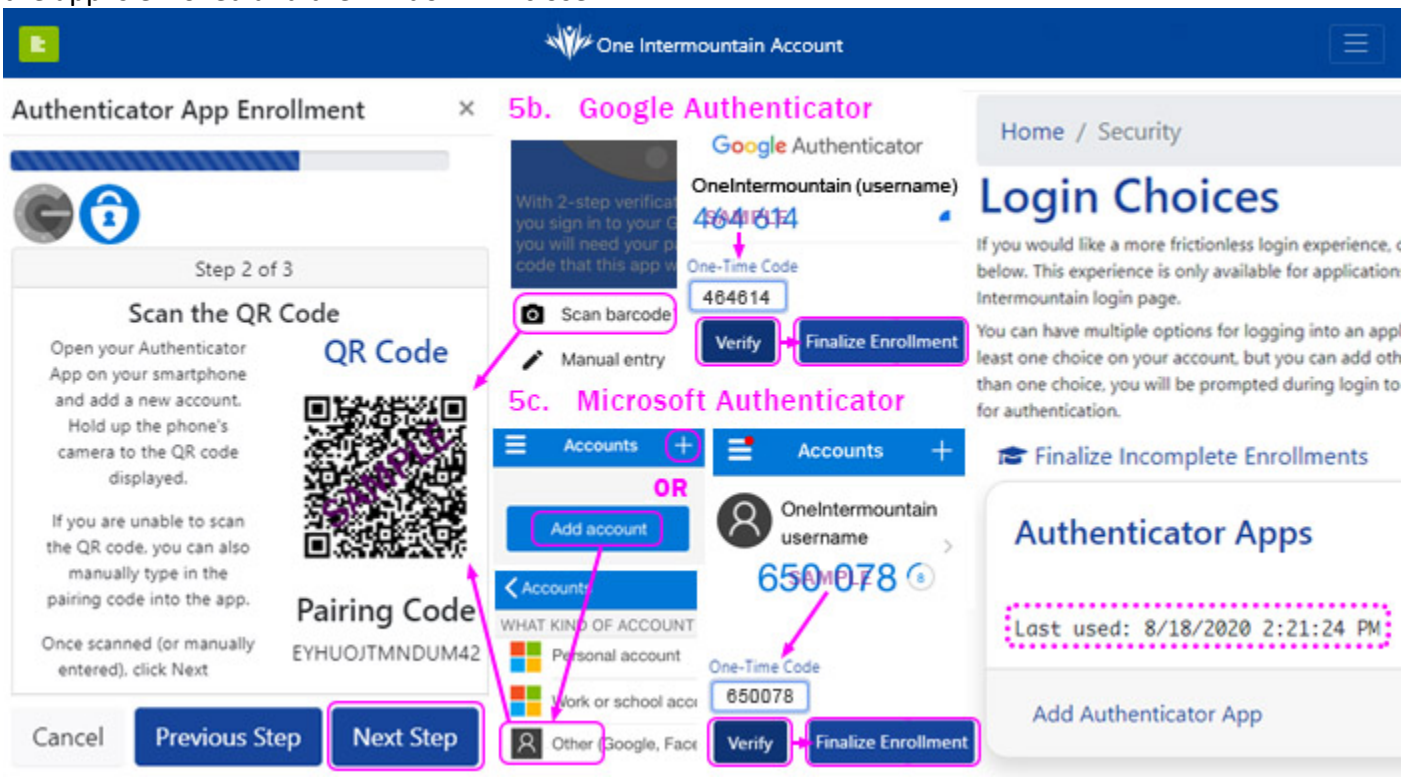


3. Click *Get* or *Install* to start the download and then *Open*.

4a. *On a computer or device other than your smartphone*, go to https://account.intermountain.net and sign in using your typical Intermountain credentials.
4b. If you are logging into the Physician Portal or DSA Portal sites directly and haven't already set up 2-Factor Verification, you will likely see the warning (as shown below) and you should click *Enroll in 2-Step*.
4c. Both 4a. and 4b. will take you to the One Intermountain Account page where you should immediately see the *Login Choices* section. Click *View My Login Choices*, which will take you to the *Login Choices* page. Scroll down to find the section called Authenticator Apps and click *Add Authenticator App*, as shown in the example below and to the right:



5a. The *Add Authenticator Enrollment* window will appear. Since you already installed an Authenticator app, you can click *Next Step* until you are at *Step 2 of 3*, as shown on the left below.
5b. Google Authenticator: Select *Scan barcode* in the app on your phone, allow the app to access your phone's camera (if prompted), then scan the QR Code showing on your computer screen, similar to the example below and to the left. Once the phone app starts generating 6-digit codes, click *Next Step* on your computer/device (below the QR Code) to proceed to Step 3. Enter the 6-digit code from the phone app and click *Verify*. Select *Click to Finalize Enrollment* and you should then see a message confirming the app is enrolled and the window will close.
5c. Microsoft Authenticator: In the app on your phone, select *Add Account* or the **+** symbol in the upper right corner then choose *Other* as the account type. Select *Continue* on the message related to backup, allow the app to access your phone's camera (if prompted), then scan the QR Code showing on your computer screen, similar to the example below and to the left. Once the phone app starts generating 6-digit codes, click *Next Step* on your computer/device (below the QR Code) to proceed to Step 3. Enter the 6-digit code from the phone app and click *Verify*. Select *Click to Finalize Enrollment* and you should then see a message confirming the app is enrolled and the window will close.



6. With enrollment finalized, return to the *Login Choices* page to confirm that it shows a recent date and time under the *Authenticator Apps* section, as shown in the example above and to the right. In rare cases, if enrollment doesn't work the first time and a recent date and time are NOT showing under the *Authenticator Apps* section, you will need to click *Finalize Incomplete Enrollments* and step through the last part of the process again until you see a recent date and time under the *Authenticator Apps* section.