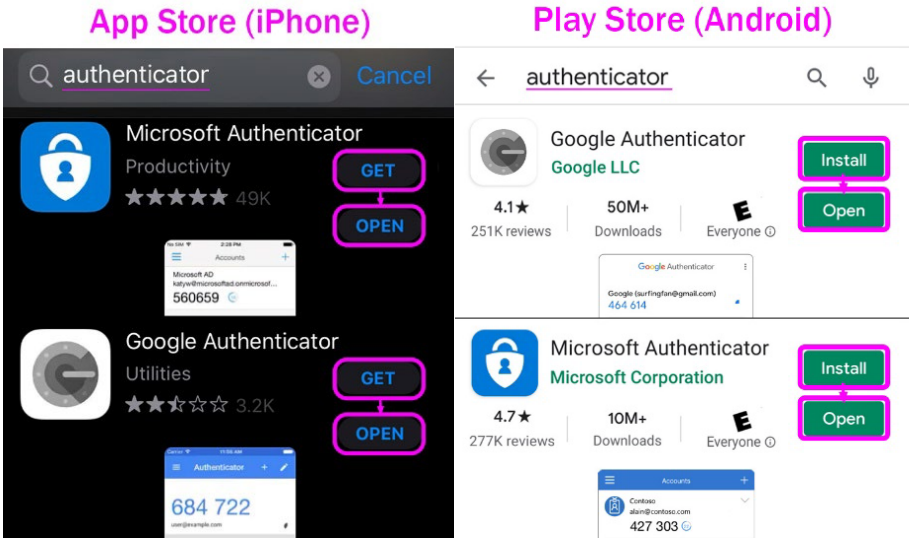
Intermountain 2-Factor Google / Microsoft Authenticator Configuration Guide

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 smartphone app and add it to your account.

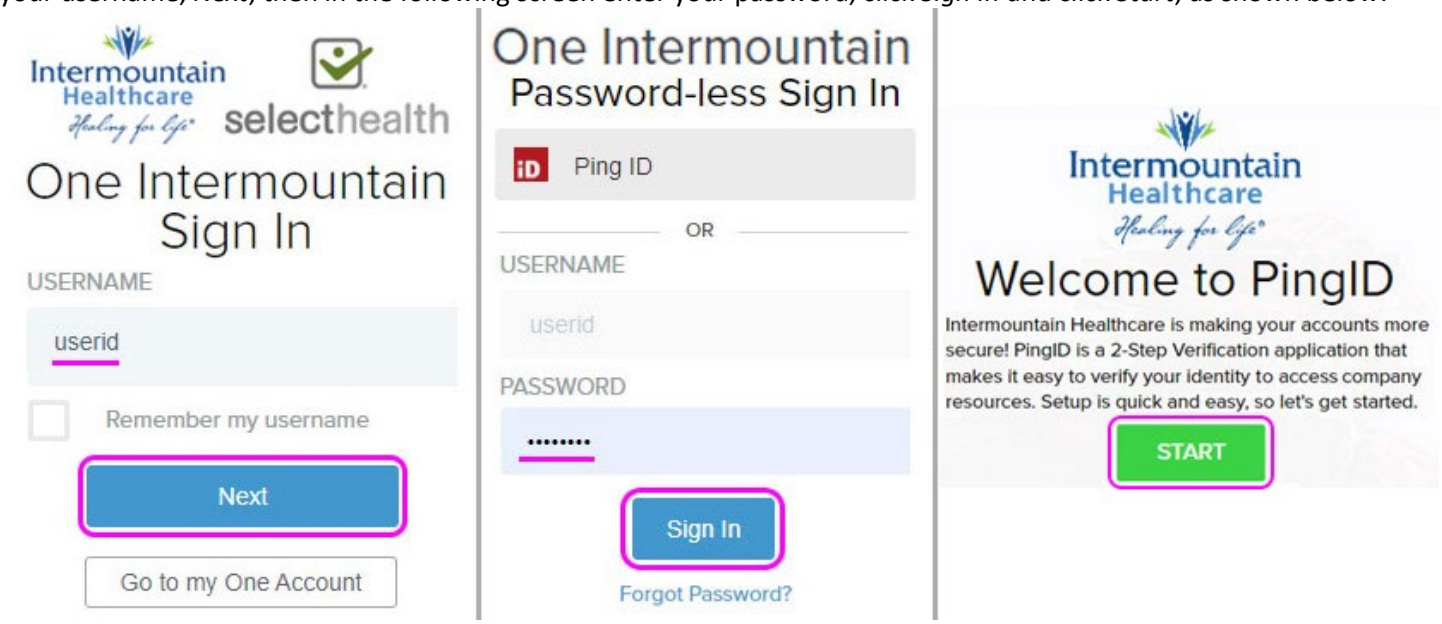
1. *Before stepping through this tutorial:* Although Authenticator requires no additional configuration on your account, you will want to assure that the Physician Portal, DSA Portal, SecureAccess (Remote), Citrix VDI and/or imail2 access has been added to your account.

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:

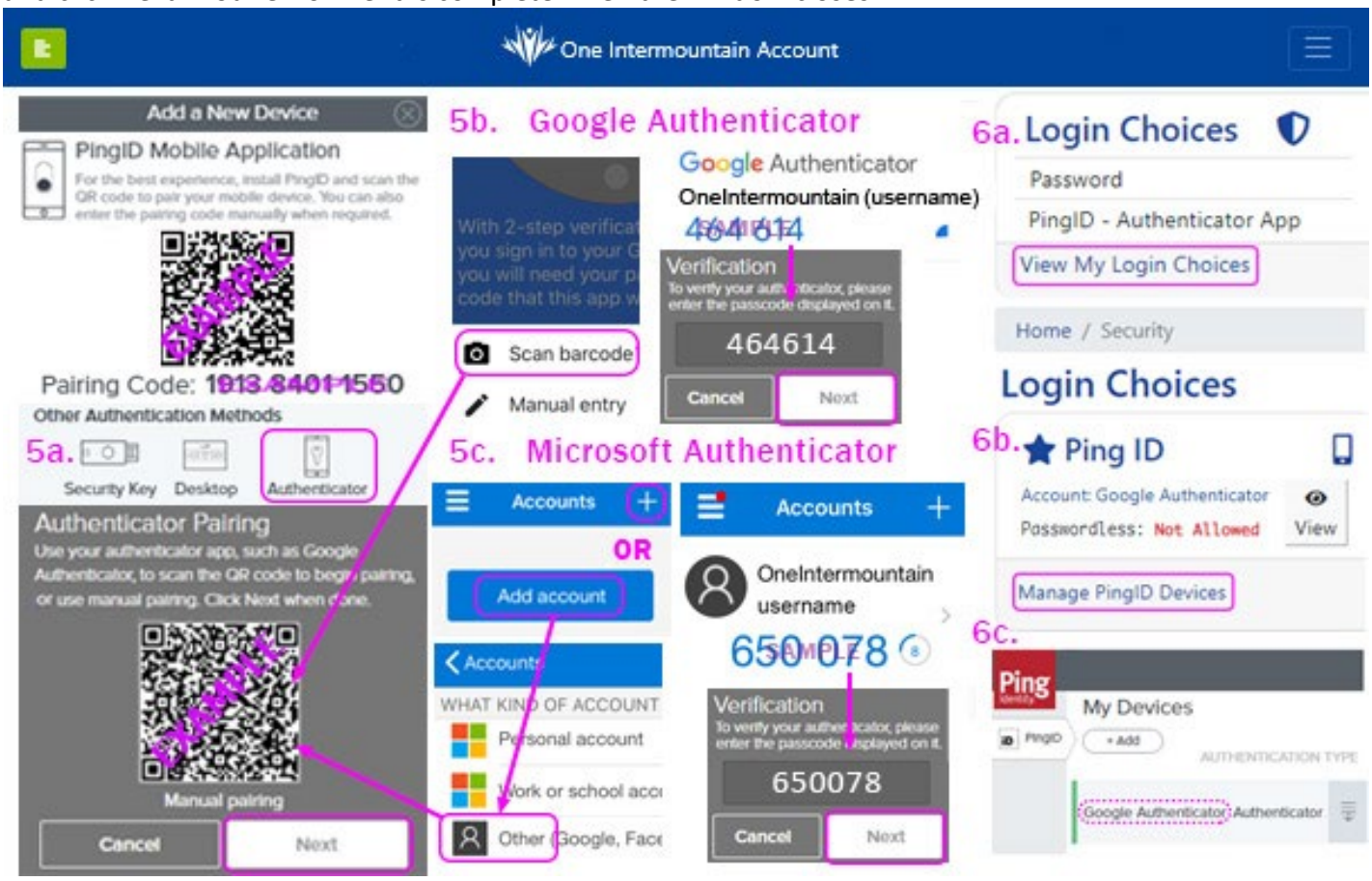


3. Click *Get* or *Install* to start the download and then *Open*.

4. *On a computer or device other than your smartphone*, go to https://account.intermountain.net and sign in by entering your username, *Next*, then in the following screen enter your password, click *Sign In* and click *Start*, as shown below:



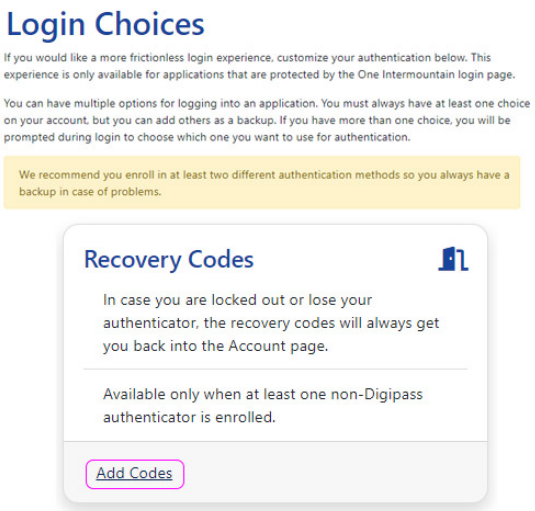
5a. The *Add a New Device* window will appear. Click *Authenticator* which will open the *Authenticator Pairing* window. Per your preference, follow the instructions for EITHER Google OR Microsoft Authenticator:
5b. Google Authenticator: Select *Scan barcode* in the app on your phone, allow the app to access your phone's camera (if prompted), then scan the QR Code showing on your computer screen, like what is shown under 5a. Once the phone app starts generating 6-digit codes, click *Next* on your computer/device, below the QR Code. In the following window, enter the 6-digit code from the phone app and click *Next.* Your enrollment is complete when the window closes.
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, like what is shown under 5a. Once the phone app starts generating 6-digit codes, click *Next* on your computer/device, below the QR Code. In the following window, enter the 6-digit code from the phone app and click *Next.* Your enrollment is complete when the window closes.

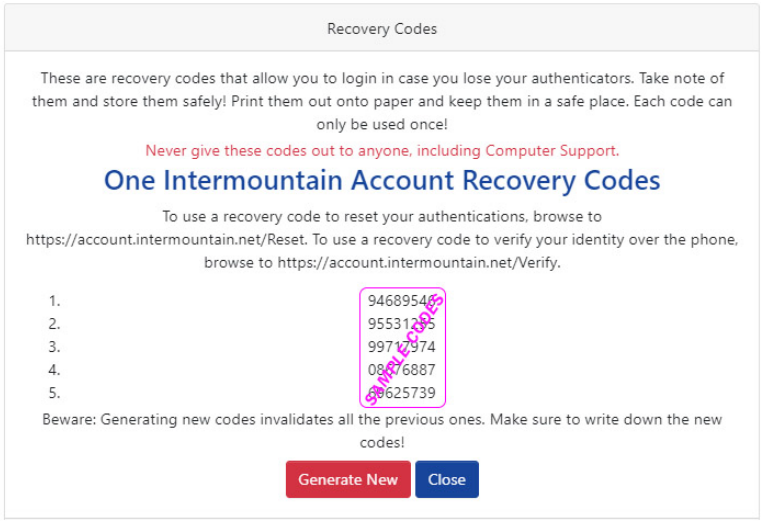


6a. Back at the One Intermountain dashboard, if you click *View My Login Choices,* you can see your Authenticator device under Ping ID, which is also the management tool used for all authenticator options.
6b. If you need to make changes to your Authenticator device, on the *Login Choices* page, find the *Ping ID* section and click *Manage PingID Devices* to open the PingID device management page.
6c. The PingID device management window should open and you should see your Authenticator under *My Devices*, which confirms that you have successfully enrolled your authenticator for 2-Factor authentication. Changes can be made by clicking the gray menu (3 lines with a down arrow) on the right side.

7. Once you have added 2-Factor Authentication (Authenticator, in this case), it is suggested that you go to **Login Choices** -> Recovery Codes, click *Add Codes* then follow the instructions on the page and click *Close*.

(Visual on following page)


Login Choices
If you would like a more frictionless login experience, customize your authentication below. This experience is only available for applications that are protected by the One Intermountain login page.
You can have multiple options for logging into an application. You must always have at least one choice on your account, but you can add others as a backup. If you have more than one choice, you will be prompted during login to choose which one you want to use for authentication.
We recommend you enroll in at least two different authentication methods so you always have a backup in case of problems.
Recovery Codes
In case you are locked out or lose your authenticator, the recovery codes will always get you back into the Account page.
Available only when at least one non-Digipass authenticator is enrolled.
Add Codes


Recovery Codes
These are recovery codes that allow you to login in case you lose your authenticators. Take note of them and store them safely! Print them out onto paper and keep them in a safe place. Each code can only be used once!
Never give these codes out to anyone, including Computer Support.
One Intermountain Account Recovery Codes
To use a recovery code to reset your authentications, browse to https://account.intermountain.net/Reset. To use a recovery code to verify your identity over the phone, browse to https://account.intermountain.net/Verify.
1. 94689548
2. 95531285
3. 99717974
4. 08876887
5. 96625739
SAMPLE CODES
Beware: Generating new codes invalidates all the previous ones. Make sure to write down the new codes!
Generate New
Close