Subject: MFA Setup Instructions – Action Required Before March 6th

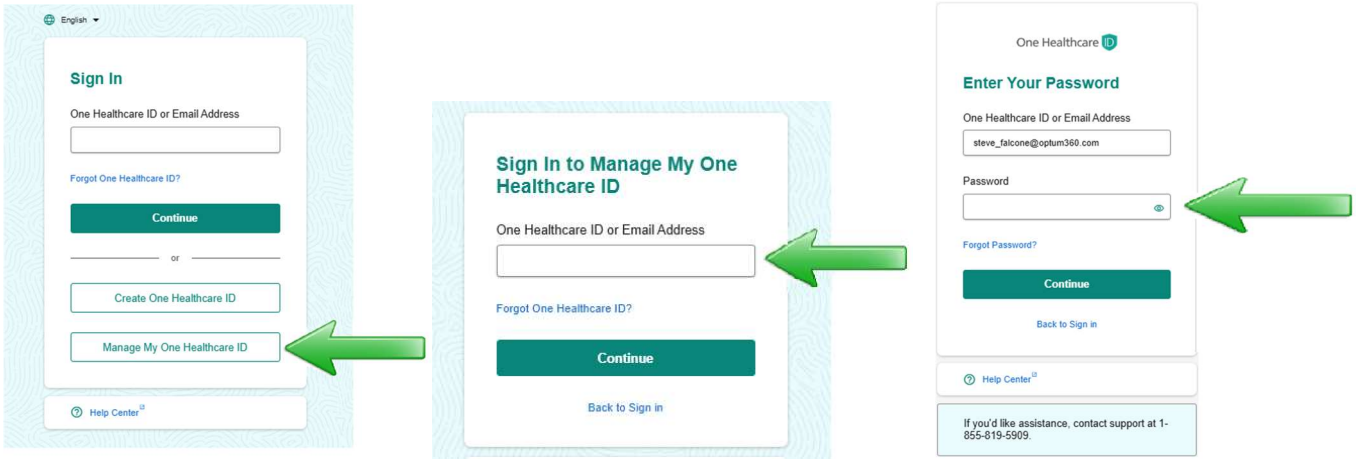
Purpose:
This document provides step-by-step instructions for setting up additional **Multi-Factor Authentication (MFA) methods** before March 6th. After this date, **email verification will no longer be available**, and users will need to authenticate using either a **Phone**, **Passkey,** or an **Authenticator** app.

Two methods of authentication are necessary, password plus one additional method.

Please follow the instructions below to ensure continued access to your account.

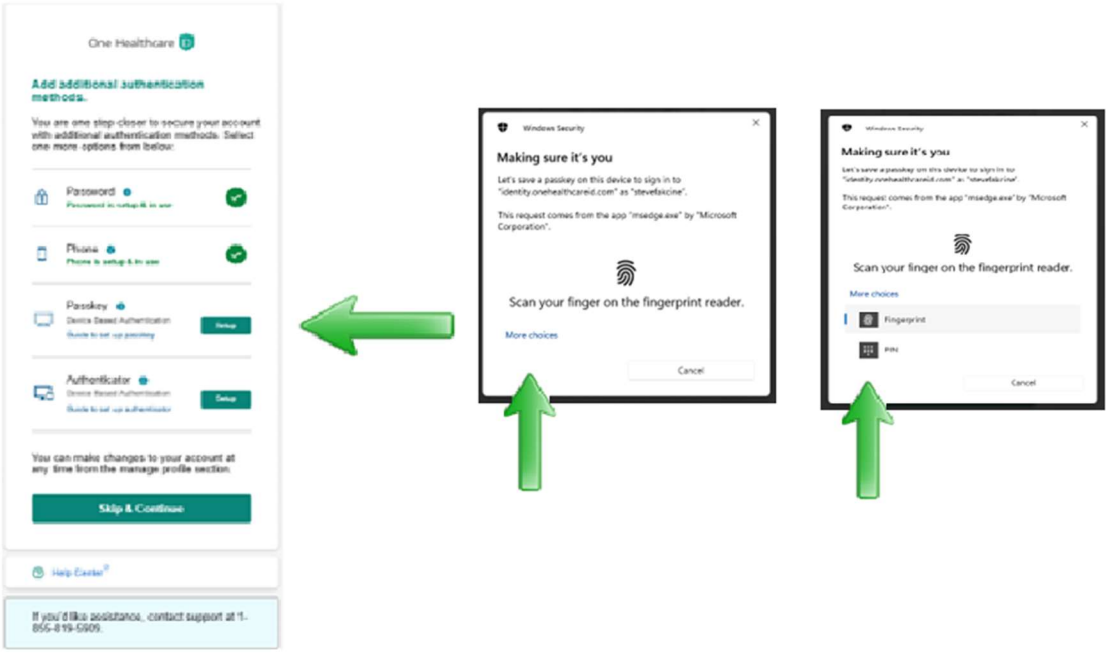
Step 1: Access Your One Healthcare ID

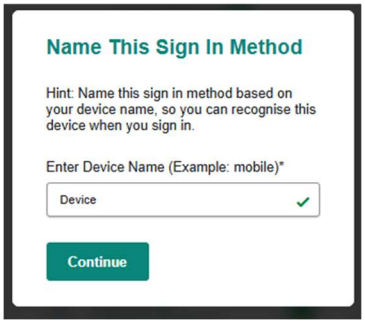
1. Go to the **One Healthcare ID** page: Sign In | One Healthcare ID
2. Click on **"Manage My One Healthcare ID."**
3. Enter your **One Healthcare ID or Email Address.**
4. Enter your **password** and sign in.



Step 2: For Passkey Authentication

1. Select **“Passkey”** as your secondary authentication method.
2. A **Windows Hello** prompt will appear. Use your **fingerprint scanner** to authenticate.
    - If you do not have a biometric reader, select **“More Choices”** and choose to enter your **PIN** instead.
    - If you do not know your PIN, reset it by going to: **Settings > Accounts > Sign-in Options.**
3. Once complete, you will receive confirmation that your **Passkey has been saved.** Enter a **name for your device** when prompted.

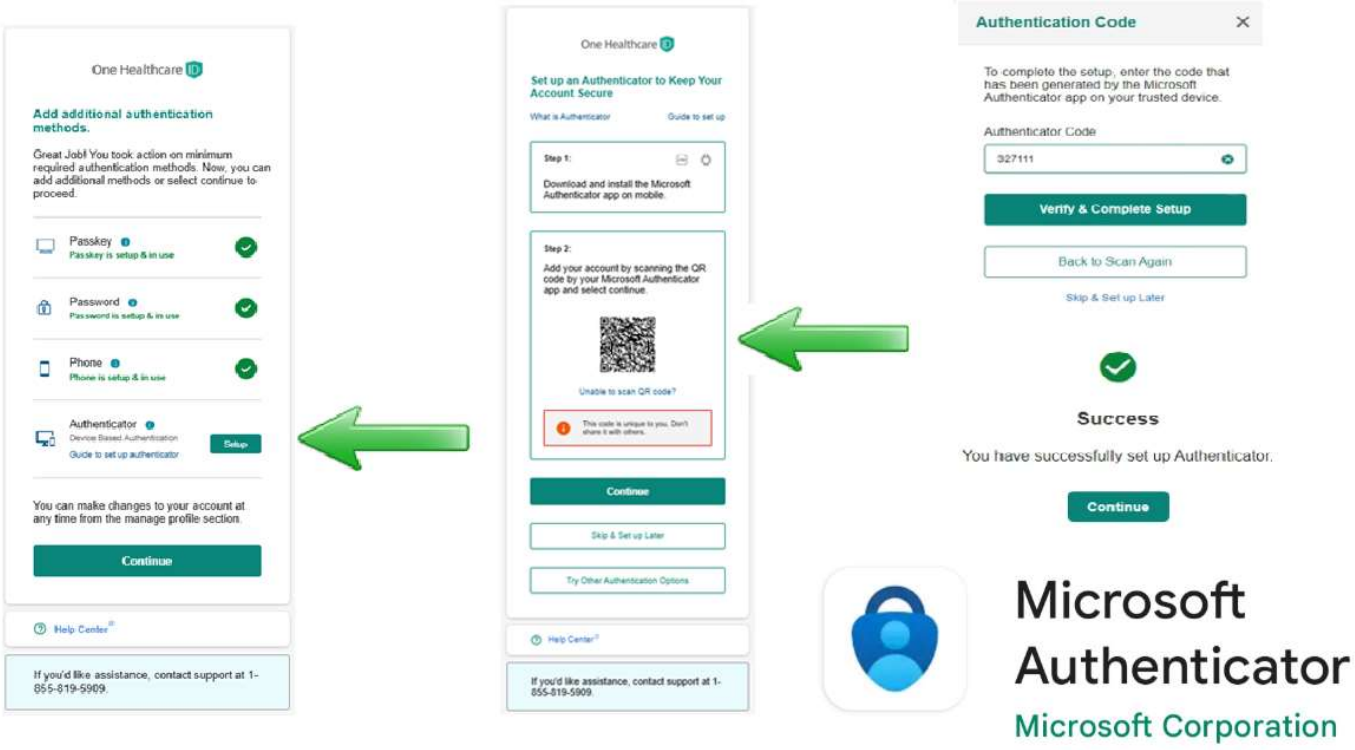




Step 3: For Authenticator App (Recommended for Password-less Login)

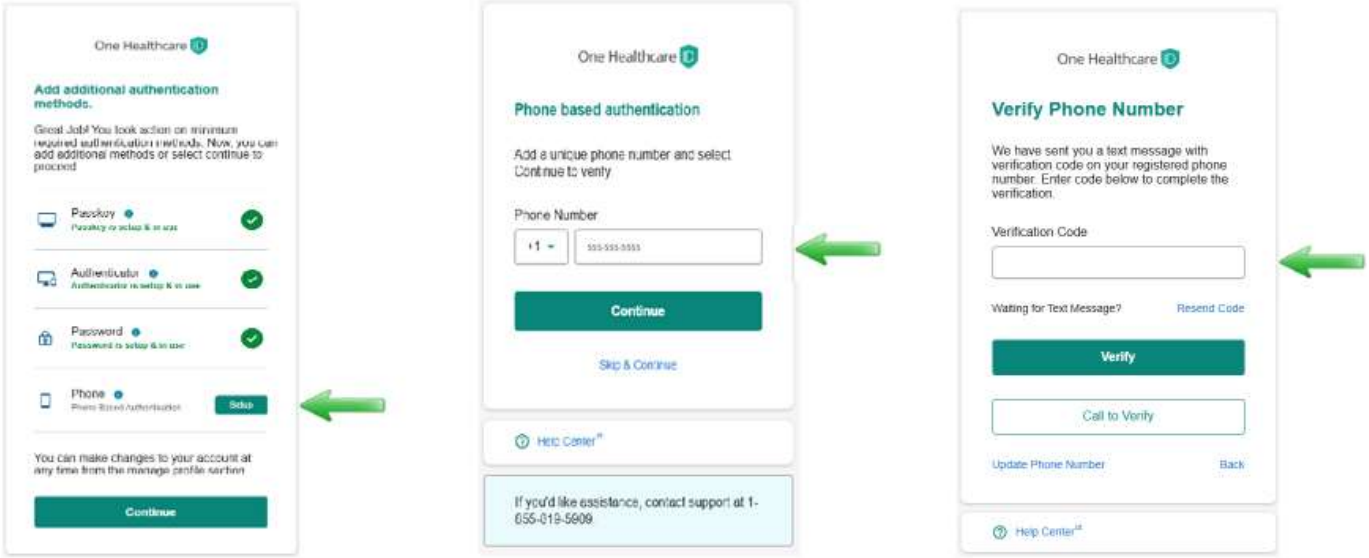
Authenticator offers a password-less method of signing in by using a time-based one-time password generated on the authenticator app (for example, Microsoft Authenticator) of your trusted device. You may configure your authenticator app with your credentials and use the unique 6-digit code generated every 30 secs to verify your identity as well as an MFA option for your account.

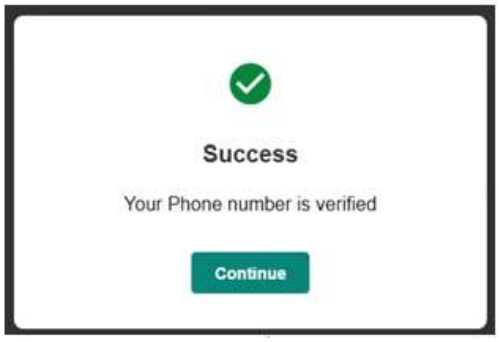
1. Under **"Authenticator,"** click **"Set Up."**
2. A QR code will appear. Open your **Authenticator app** (e.g., **Microsoft Authenticator**) on your phone.
3. Select **“Add Account”** and scan the QR code.
4. A **6-digit code** will be generated every **30 seconds** in your app.
5. Select continue and enter the **6-digit authentication code.**
    - **Please note**- This Bar code is unique to you, do not share it with others.



Step 4: For Phone setup (For Phone Based Authentication)

1. Select “Phone” as your secondary authentication method.
2. Add a unique phone number and select **Continue** to verify.
3. Select one of the following methods to verify your phone number.
    - “Via Text Message”
    - “Via Call”
4. An automated text message or phone call will be sent to the phone number you provide for account confirmation and recovery purposes. If you select text message, messaging and data rates may apply.





One Healthcare ID

Frequently Asked Questions:

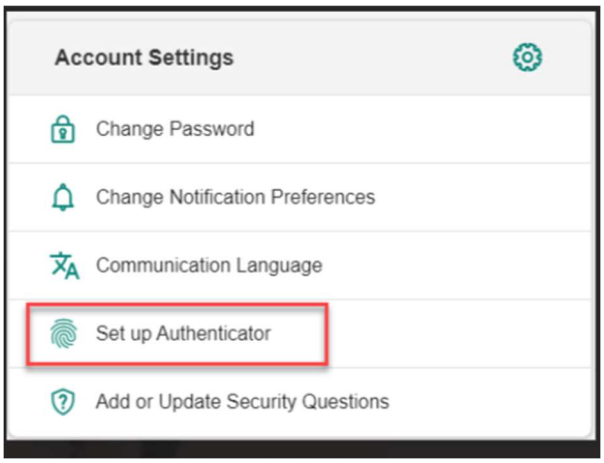
- **Do I need all forms of authentication?**

  No, you only need your password and one additional method of authentication.

  - Recommended that you have three or more methods of authentication in the event one is not available.

- **What if I don't see the same display of the authentication methods?**

  You may see a different view like the below,



  This will work for you as well.

- **I forgot my password. How do I change my password?**

  If you forget your password, you can use self-service to set a new password. Before you can set the new password you must confirm your identity using your email address or other verified information from your profile. To begin select the Forgot Password link on the Sign In page.

- **My account has been locked. How do I unlock my account?**

  Your account is automatically locked if an incorrect password is entered too many times in a short period of time. This prevents unauthorized access to your account. You can unlock your account by verifying your identity and then setting a new password. To begin, select **Continue** on the **Account Locked** page.

One Healthcare ID

Frequently Asked Questions:

- **If you have forgotten your One Healthcare ID. How do I retrieve my One Healthcare ID?**

  If you forget your One Healthcare ID, you can use self-service to retrieve it using your email address or other verified information from your profile. To begin select the Forgot One Healthcare ID link on the Sign In page.

- **Why can't I sign in with my email address?**

  If your email address is associated with two or more One Healthcare IDs, you cannot sign in using the email address. If you are using a shared email address, you must sign in with your One Healthcare ID.

  If you forget your One Healthcare ID you can use self-service to retrieve it using your email address or other verified information from your profile. To begin select the Forgot One Healthcare ID link on the Sign In page.

- **If a customer has a Clean Desk" policy (No phone number to add to authentication) or (an international phone number) what would be the users next action?**

  Clean desk policy users can use Password and Passkey as their way for authentication.

- **For new user registration, what will be the work around if the user does not have a phone number available?**

  User can register and setup password, passkey as their authentication methods and use recovery code for recovery methods like password recovery and passkey recovery.

- **What is a recovery Code?**

  A recovery key is a **randomly generated 20-character code** that helps improve the security of your account by giving you more control over resetting your password to regain access to your account. This gives you more control of your account recovery methods and can help prevent an attacker from gaining access to and taking control of your account.

  However, if you lose your recovery key and can't access one of your trusted devices, you'll be locked out of your account permanently and end up creating new account.

One Healthcare ID

Frequently Asked Questions:

- **What is a passkey?**

  WebAuthn is part of the FIDO2 framework, which is a set of technologies that enable password less authentication between servers, browsers, and authenticators. WebAuthn is supported on Chrome, Firefox, and Edge, and Safari.

  It allows servers to integrate with the strong authenticators now built into devices, like Windows Hello or Apple's Touch ID. Instead of a password, a private-public keypair (known as a credential) is created for a website. The private key is stored securely on the user's device; a public key and randomly generated credential ID is sent to the server for storage. The server can then use the public key to prove the user's identity.

- **Pre-requisite for Passkey for windows OS**

  Windows Hello offers a personal, secure way to sign in to your Windows devices using facial recognition, fingerprint, or a PIN. The setup process for Windows Hello can vary significantly due to differences in devices, operating systems (OS) organizational policies, and other factors. For this reason, it is recommended to consult with your IT department or refer to Microsoft's guidance that specifically matches your setup needs.

- **Technical requirements for Passkey**

  Operating Systems:
  - Windows 10 or later
  - macOS X Sierra (10.12) or later
  - Linux with recent versions of Ubuntu, Fedora, or other distributions that support WebAuthn
  - Android 7.0 (Nougat) or later
  - iOS 13.3 or later (for Safari users)

  Browsers:
  - Google Chrome 67 or later
  - Mozilla Firefox 60 or later
  - Microsoft Edge 18 or later
  - Safari 13 or later
  - Opera 54 or later

  Other Requirements:
  - Devices require a built-in or external biometric sensor for biometric authentication.
  - For security keys, devices need support for USB, NFC, or Bluetooth security keys.

  Additional Notes:
  - Browser updates: Ensure your browser is updated to the latest version for the best WebAuthn support.
  - Device and browser combination: Some features and capabilities might vary depending on your specific device and browser combination.