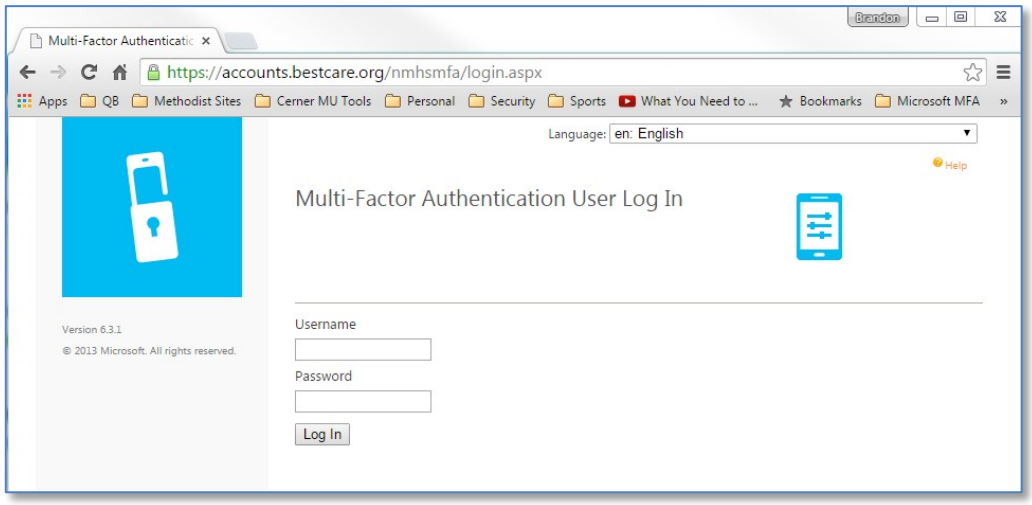
Two-Factor Authentication Options

Manage your two-factor authentication options through the https://accounts.bestcare.org website. This website is available internally and externally of the organization. Like other services, if you connect while external of Methodist Health System, you will be required to use the two-factor authentication process to connect.

Step 1

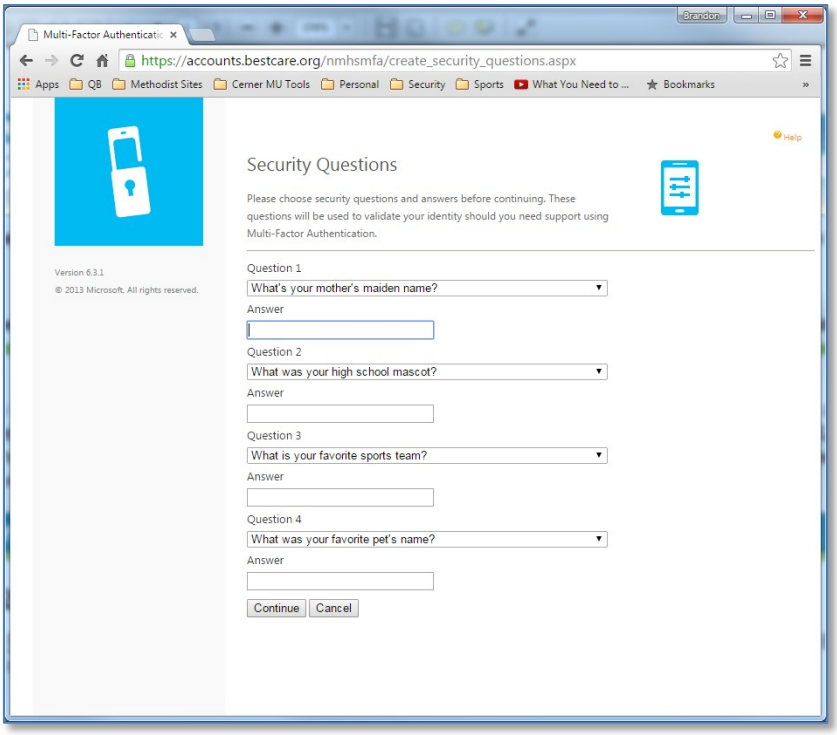
Open your browser and go to https://accounts.bestcare.org. You will be presented with the logon screen shown below. Log in with your network Username and Password.



Step 2

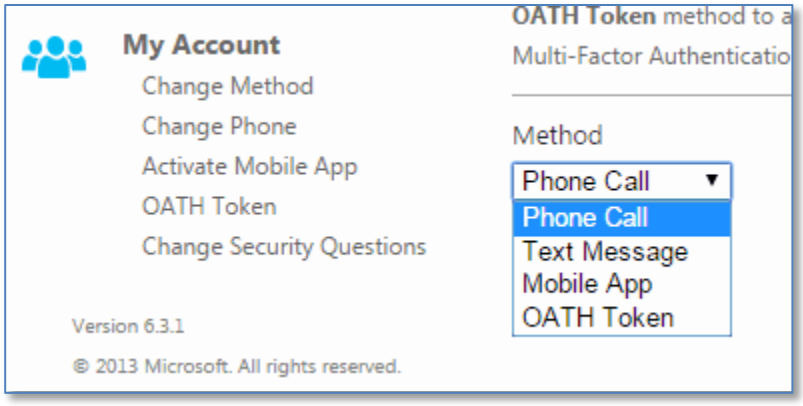
The first time you access this site you must answer 4 security questions about yourself. You can click the drop down arrow on the right to select the questions you want to answer. When complete, click Continue.

Note: You must choose 4 unique questions.



Step 3

After you answer the security questions you will be allowed to manage your account and change options for how you want to be notified for two-factor authentication. We will review the options that are available below.



Change Method – Options for two-factor authentication

(Details for setting up each method below are shown on the next page.)

1. **Phone Call** – the phone call option is the default option set for most accounts. The system will call you on the number you have provided to our system. When you authenticate externally with the correct username and password, the system will make a voice call to that number, asking you if you want to authenticate by pressing the # sign. This should complete the authentication process and allow you in.
    a. Benefits of this method include the ability to have up to two numbers it calls to authenticate.
    b. Ability to use a voice line such as a home phone or office number and extension.

    The system will call back three times if it doesn't get the correct response of #. If you have two numbers defined it will rotate between both numbers making three attempts at each number before it stops.

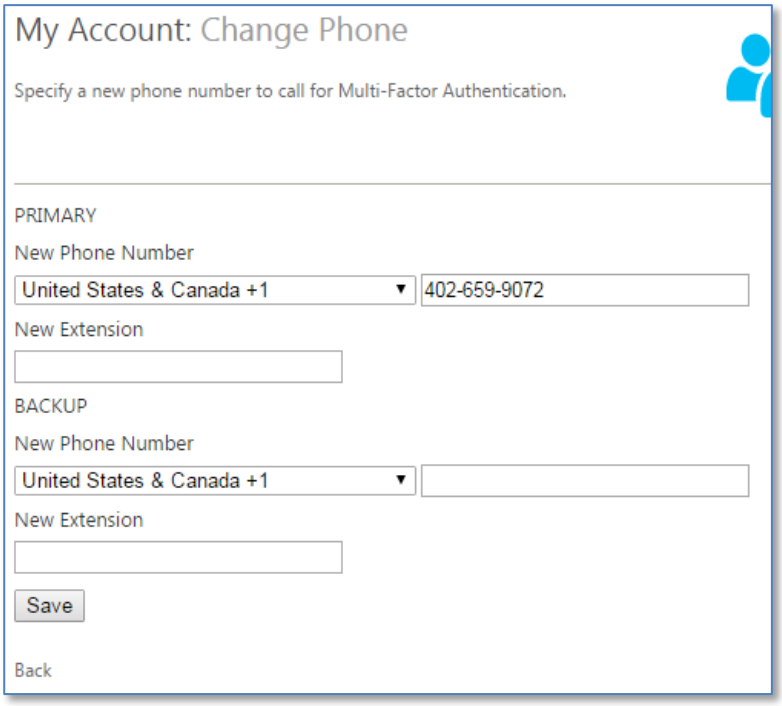
2. **Text Message** – the text message option works well if you have a text plan on your cellular phone. You will receive a text message from our system. You just reply to that text message with the 6-digit code it sent which will complete the authentication process.

3. **Mobile App** – Setting up the mobile app is a two-step process and requires a smart phone or tablet device capable of running the application. Instructions on how to set this up are included below:
    a. Benefits of this method are that it runs over Wi-Fi and works well for users that do not have a strong Cellular connection.
    b. It can be setup to receive a push notification or you can use it like a token where you type in the number that is displayed. The number randomly changes each minute while the application is live.

4. **OATH Token** – Used for either the Mobile App or a hard token that is distributed to you upon request.
    a. This method can be used with the Mobile App or with a hard token provided by Methodist. The process varies depending on which option you are using, however, they both will present a screen for you to fill in a code at the time of authentication.
    b. Benefits of this method include being able to authenticate while you are not accessible for text or phone calls. Perhaps on a plane where you have Wi-Fi, but not cellular coverage.

Phone Call

1. You may change the phone numbers used to contact you with this option by clicking the Change Phone option on the left of the screen. It will present a similar window as shown below. You can use a Primary and Secondary number such as a cellular phone as primary and home or work phone number as secondary. The system will dial the numbers listed exactly as they are put in so be sure you double-check the number before clicking the Save button.



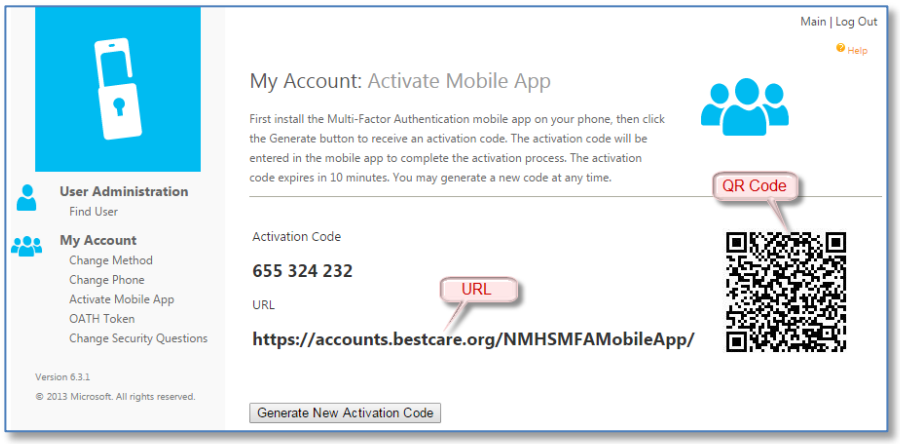
The screen will look different if you choose the **text option** under the **Change Method** section. That screen shot is below. When setup for text, it can only use one number so your primary number will be used. Ensure that number is capable of receiving text messages for this process to work.

Mobile App

Before you can change your method to use the Mobile App, you first have to install and activate the Mobile App so it is linked to your account as described below.

Android Device: Installing the Microsoft Authenticator Application

1. From a device other than your mobile phone, log into the https://accounts.bestcare.org website with your network credentials, if you haven't already.
2. Under the My Account heading, click on Activate Mobile App.
3. In the Activate Mobile App window, click on Generate Activation Code and leave this window open. This will display a QR code which you will scan once you have installed the mobile app with the instructions below.
4. Download the Microsoft Authenticator Application from Google Play Store. The icon is shown to the right:
5. Install the Microsoft Authenticator Application:
    - Tap Install and allow access to any necessary features, if asked.
    - When asked to activate an account, choose Scan Barcode. (Alternatively you could choose Enter Manually and manually type in the URL from the website page.)
6. If a barcode app is not found on your device, you should be prompted to download one. Download and install the recommended barcode app. Rather than Open the barcode scan app, tap the Back button to return to the Microsoft setup process.Tap Select Scan QR code.
7. Scan the QR code you opened from the website in Step 3 above.

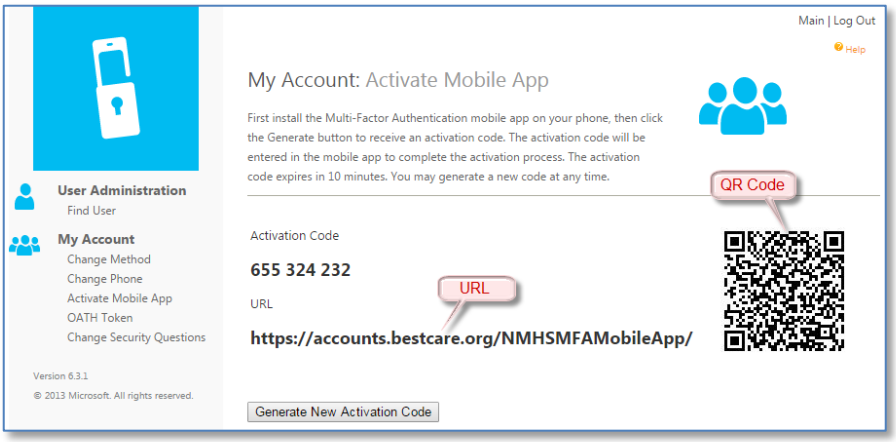


8. Once you are successful, you can now use the **"Change Method"** option on the left of the website screen to setup your two-factor authentication to use the **Mobile App** or **OATH Token**.
    - Mobile App Method requires that cellular service is available to your phone at the time you are logging in.
    - OATH Token Method allows you to generate a code from the Mobile App when needed, whether cellular service is available at that moment or not.

9. When you click Save, text above the Method dropdown will confirm that "Your method has been changed."

iPhone Device: Installing the Microsoft Authenticator Application

1. From a device other than your mobile phone, log into the https://accounts.bestcare.org website using your network credentials, if you haven't already.
2. Under the My Account heading, click on Activate Mobile App.
3. In the Activate Mobile App window, click on Generate Activation Code and leave this window open. This will display a QR code which you will scan once you have installed the mobile app with the instructions below.
4. From your mobile phone, download the Microsoft Authenticator Application from the App Store. The icon is shown to the right:
5. Install the Microsoft Authenticator Application:
   a. You may be asked during installation if you want to **Allow Push Notifications**. If asked, say yes.
   b. If asked, accept to allow access to various device features as well as notifications.
   c. When asked to activate an account either by scanning a barcode or entering manually. Choose Scan Barcode.
   d. In the next Activate Account window, again tap Scan Barcode.
6. Scan the QR code you opened in Step 3 above.



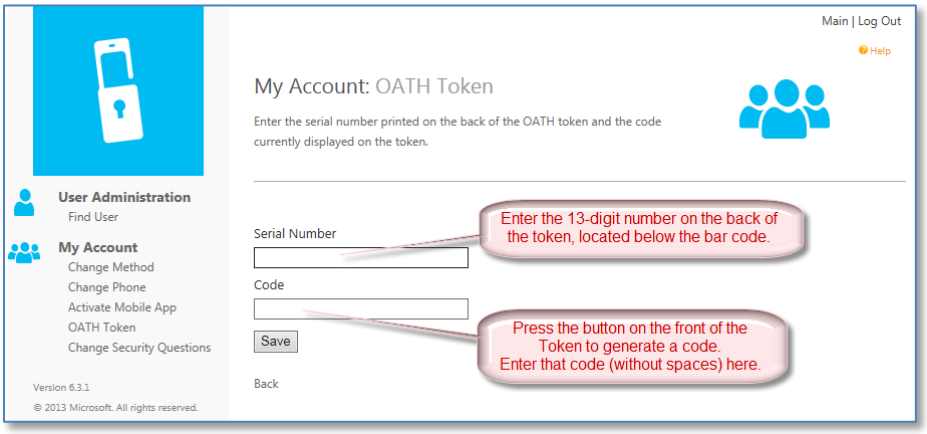
7. Once you are successful, you can now use the **"Change Method"** option on the left of the website screen to setup your two-factor authentication to use the **Mobile App** or **OATH Token**.
   - Mobile App Method requires that cellular service is available to your phone at the time you are logging in.
   - OATH Token Method allows you to generate a code from the Mobile App when needed, whether cellular service is available at that moment or not.

8. When you click Save, text above the Method dropdown will confirm that "Your method has been changed."

OATH Token

(fits on a key ring)

1. Obtain a Token by calling the I.T. Services Desk at 402-354-2280.
2. Under My Account, select OATH Token.
3. Register your Token as indicated below, then click **Save**.



4. Go to Change Method, select OATH Token from the dropdown, and then click Save.
5. Text above the Method dropdown will confirm that “Your method has been changed.”
6. Your Token setup is now complete.
7. Push the Token button whenever you need to generate a code.

FAQs

How does Multi-Factor Authentication™ work?

The default Multi-Factor Authentication works by placing a confirmation call to your phone during login.

Step 1:

Enter your usual username and password.

Step 2:

Instantly, you receive a phone call. Answer and press #.

That's It!

This simple process provides two separate factors of authentication through two separate channels (your computer and your phone service). It works with any regular or mobile phone.

What happens if I lose my phone?

Select the Change Phone Number option to enter a new phone number or an alternate number can also be set up.

What happens if I lose cell phone coverage in a certain area?

You can change your account to point to an alternate phone number, such as a land line, by selecting the Change Phone Number option. Alternately, you can choose to setup the Mobile App on a smart phone or tablet. This application can use Wi-Fi in addition to cellular networks to communicate.

What if I get a phone call from Multi-Factor Authentication when I'm not trying to log in?

This would only happen if someone else was trying to log into your account, and they already knew your password. Remember, phone calls are only made after the username and password are verified. So, if this happens, Multi-Factor Authentication has just saved your account from illicit access! To report the incident, select the Fraud Alert option from the phone menu during the authentication call by pressing 0#. This will alert your company's IT security team. Future authentication attempts will be blocked until the issue has been resolved.