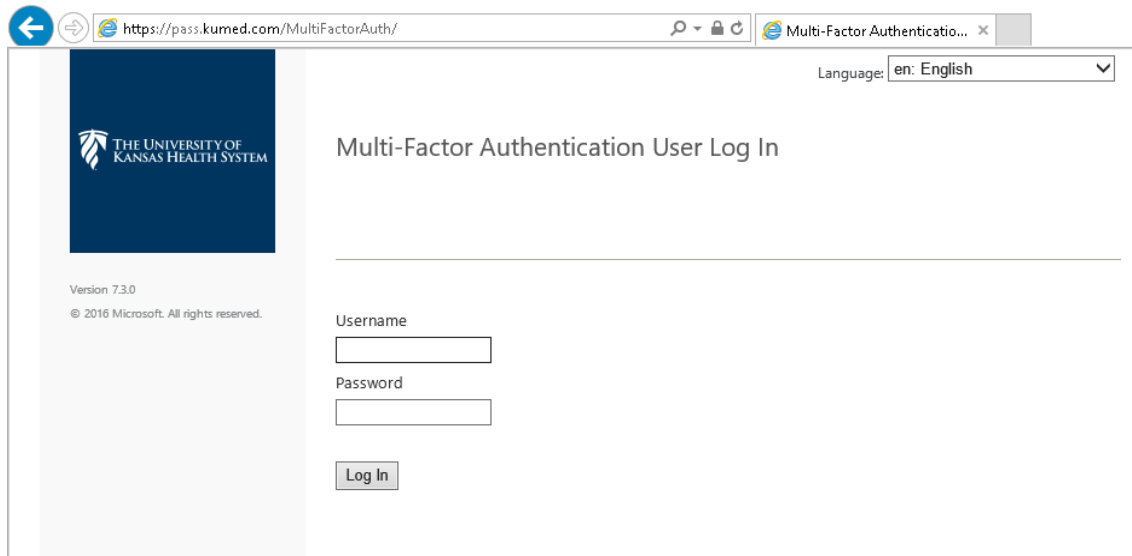


Multi-Factor Authentication Enrollment

LOGIN

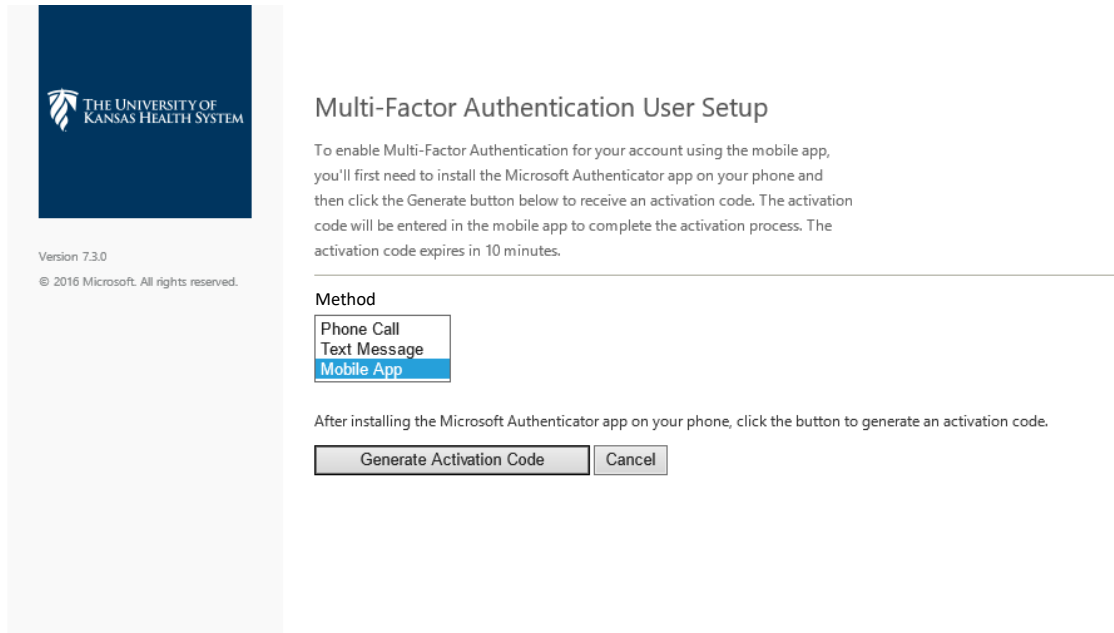
From a desktop PC visit <https://pass.kumed.com/MultiFactorAuth>. Log in with your health system username and password.



SELECT AUTHENTICATION METHOD

Use the "Method" drop-down menu to choose how you prefer to provide a second factor used to confirm your identity. You may choose the phone call or text message options to receive a one-time code that you will enter to confirm your identity, or you can use the Microsoft Authenticator mobile app to log in automatically. We review the instructions to set up each option in the pages that follow.

Multi-Factor Authentication Enrollment



Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account using the mobile app, you'll first need to install the Microsoft Authenticator app on your phone and then click the Generate button below to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes.

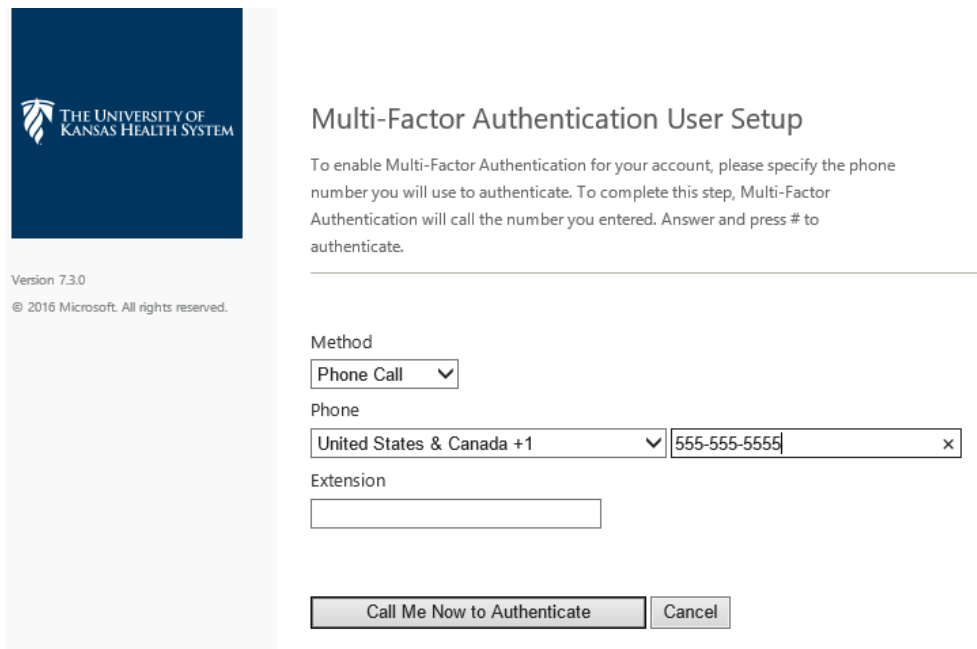
Method

- Phone Call
- Text Message
- Mobile App**

After installing the Microsoft Authenticator app on your phone, click the button to generate an activation code.

PHONE CALL

To use the phone call method, enter a number at which you can be reached when using applications requiring Multi-Factor Authentication. You may return to the MFA site any time to update this number as needed.



Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account, please specify the phone number you will use to authenticate. To complete this step, Multi-Factor Authentication will call the number you entered. Answer and press # to authenticate.

Method

Phone Call

Phone

United States & Canada +1 555-555-5555

Extension

Multi-Factor Authentication Enrollment

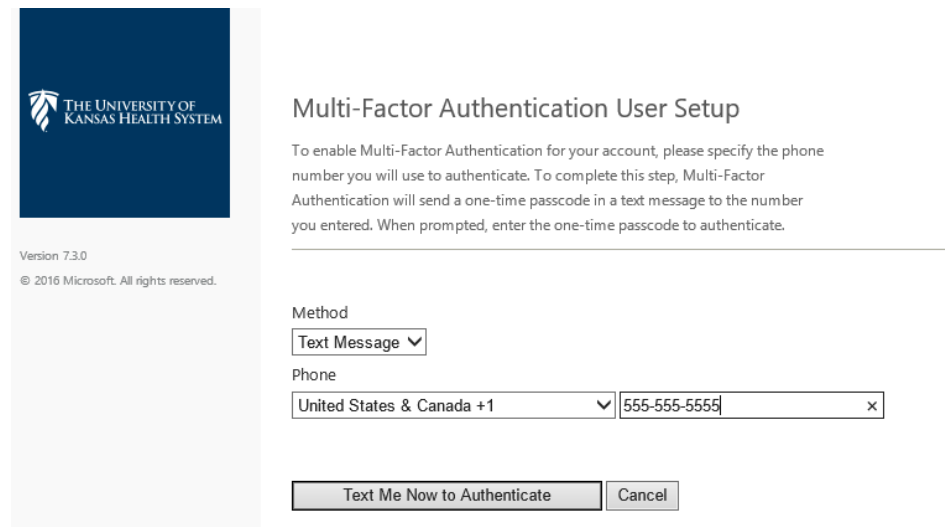
After entering your phone number, click Call Me Now to Authenticate. You will then receive a call from an automated service with this message: “Thank you for using the Microsoft sign in verification system. Please press the # key to finish your verification.”

After pressing the # key on your phone, you will be directed to set up [security questions](#). After completing these questions, your account will be configured to use Multi-Factor Authentication.

Future logins to applications enhanced with Multi-Factor Authentication will prompt a phone call to this number before allowing access to the application. Pressing # will complete the verification and allow access to the application. If you do not press # in the time allowed, enhanced security will be required to either: generate a new call, text a passcode or answer the security questions you established.

TEXT MESSAGE

To use the text message method, enter a number at which you can receive messages when using applications requiring Multi-Factor Authentication. You may return to the MFA site any time to update this number as needed.



Version 7.3.0
© 2016 Microsoft. All rights reserved.

Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account, please specify the phone number you will use to authenticate. To complete this step, Multi-Factor Authentication will send a one-time passcode in a text message to the number you entered. When prompted, enter the one-time passcode to authenticate.

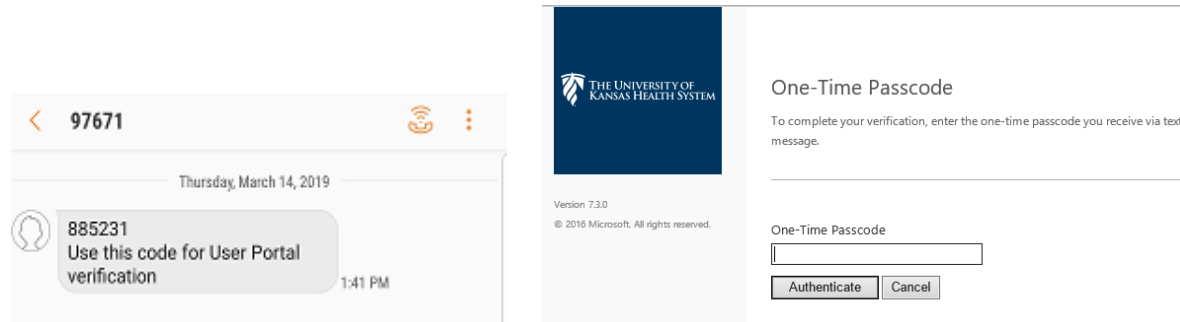
Method
Text Message

Phone
United States & Canada +1 555-555-5555

Text Me Now to Authenticate Cancel

Click: Text Me Now to Authenticate. You will then receive a text message with a 6-digit code. Enter this in the One-Time Passcode field as shown.

Multi-Factor Authentication Enrollment



After entering the passcode and clicking Authenticate, the authentication page will be automatically redirected to set up your [security questions](#). After completing these questions, your account will be configured to use Multi-Factor Authentication.

Future logins to applications enhanced with Multi-Factor Authentication will prompt a text message to this number before allowing access to the application. Entering the passcode received in the text message will complete the verification and allow access to the application. If the passcode is entered incorrectly, enhanced security will be required to either: generate a new call, text a new passcode or answer the security questions you established.

MOBILE APP

Begin by installing Microsoft Authenticator from either Google Play or the Apple App Store.



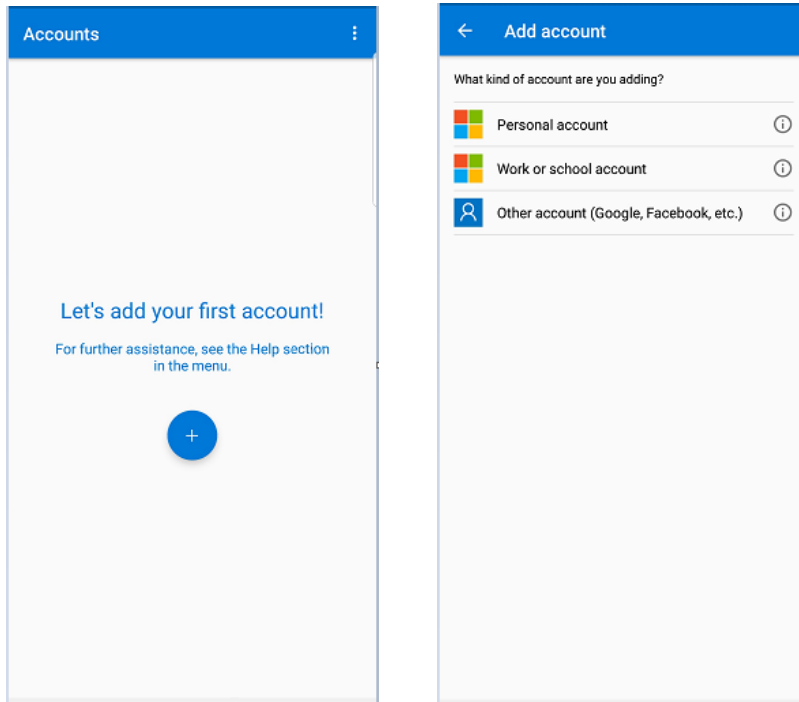
The app will appear in Google Play or the App Store with this icon:



Microsoft Authenticator
Microsoft Corporation Business

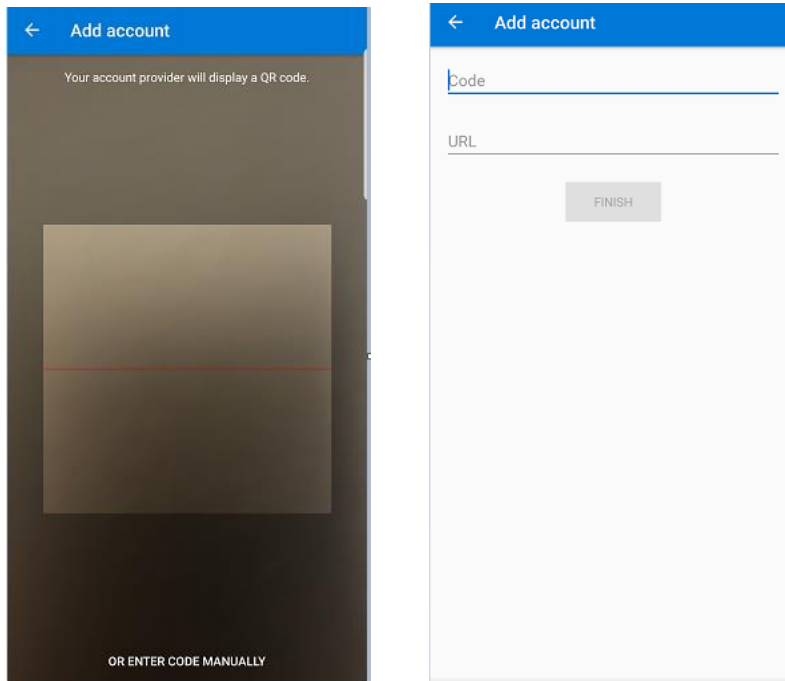
Tap the + to add your account and choose Work or school account. Allow any permissions requested.

Multi-Factor Authentication Enrollment

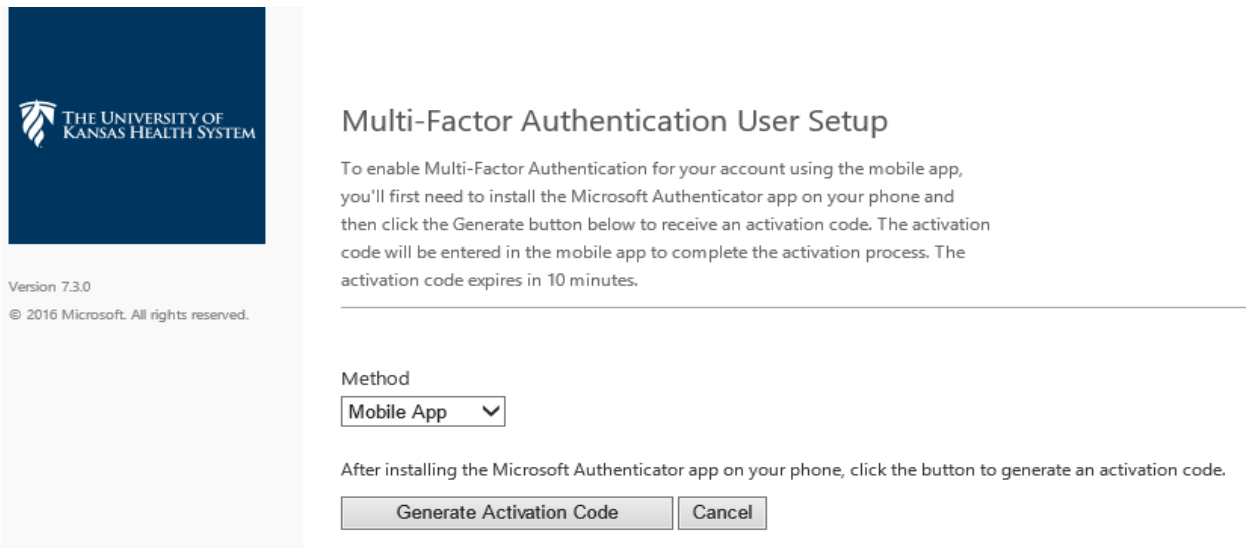


Your mobile device will open a screen ready to scan a QR code. You also may enter the code manually.

Multi-Factor Authentication Enrollment



With the app installed and ready to scan, select Mobile App and click Generate Activation Code from the Multi-Factor Authentication User Setup page.



You will then see a page like the example below. ****Note, if viewing this page from a mobile device the activation code and QR will not display. Please access this page from a desktop or laptop device. The**

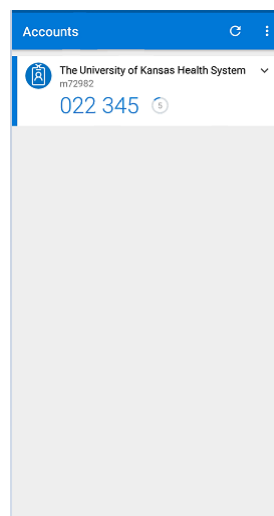
Multi-Factor Authentication Enrollment

Activation code and QR is unique to each user and instance where a new activation code is requested. This code cannot be reused or shared. Scan the QR code using your device camera or enter the code and URL manually if you are unable to scan the QR.



After entering the passcode and clicking Authenticate, the authentication page will be automatically redirected to set up your [security questions](#). After completing these questions, your account will be configured to use Multi-Factor Authentication.

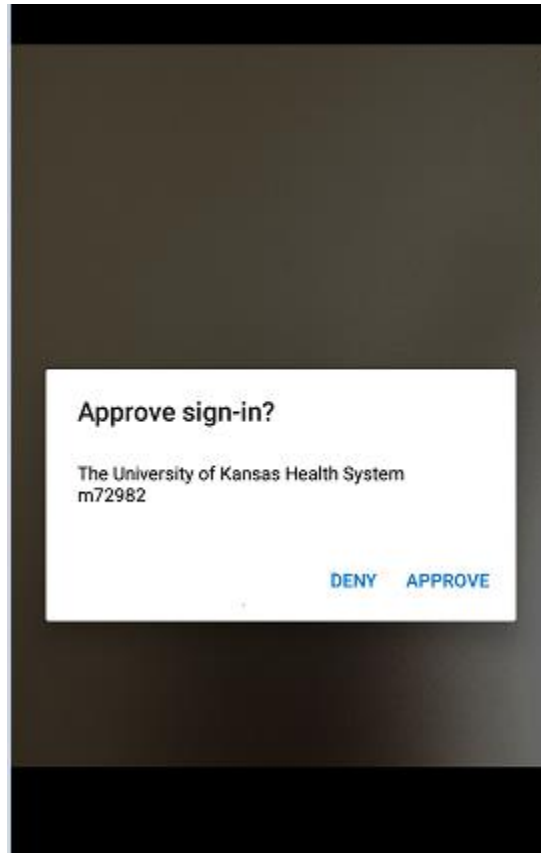
The Microsoft Authenticator app will open a page displaying your username and an activation code that refreshes every 30 seconds.



Multi-Factor Authentication Enrollment

When logging into an application enhanced with Multi-Factor Authentication, you will receive a push notification asking you to approve or deny the sign-on.

- Clicking Approve will allow you access to the application.
- Clicking Deny will prompt enhanced security to require resending the notification to the mobile app, generating a new call, texting a new passcode or answering the user supplied security questions.



Multi-Factor Authentication Enrollment

SECURITY QUESTIONS

After completing setup of your preferred Multi-Factor Authentication method, you will be prompted to set up security questions as shown below.



Version 7.3.0

© 2016 Microsoft. All rights reserved.

Security Questions

Please choose security questions and answers before continuing. These questions will be used to validate your identity should you need support using Multi-Factor Authentication.

Question 1

What was your high school mascot?

Answer

Question 2

What was your favorite pet's name?

Answer

Question 3

What is your favorite movie?

Answer

Question 4

What was your favorite teacher's name?

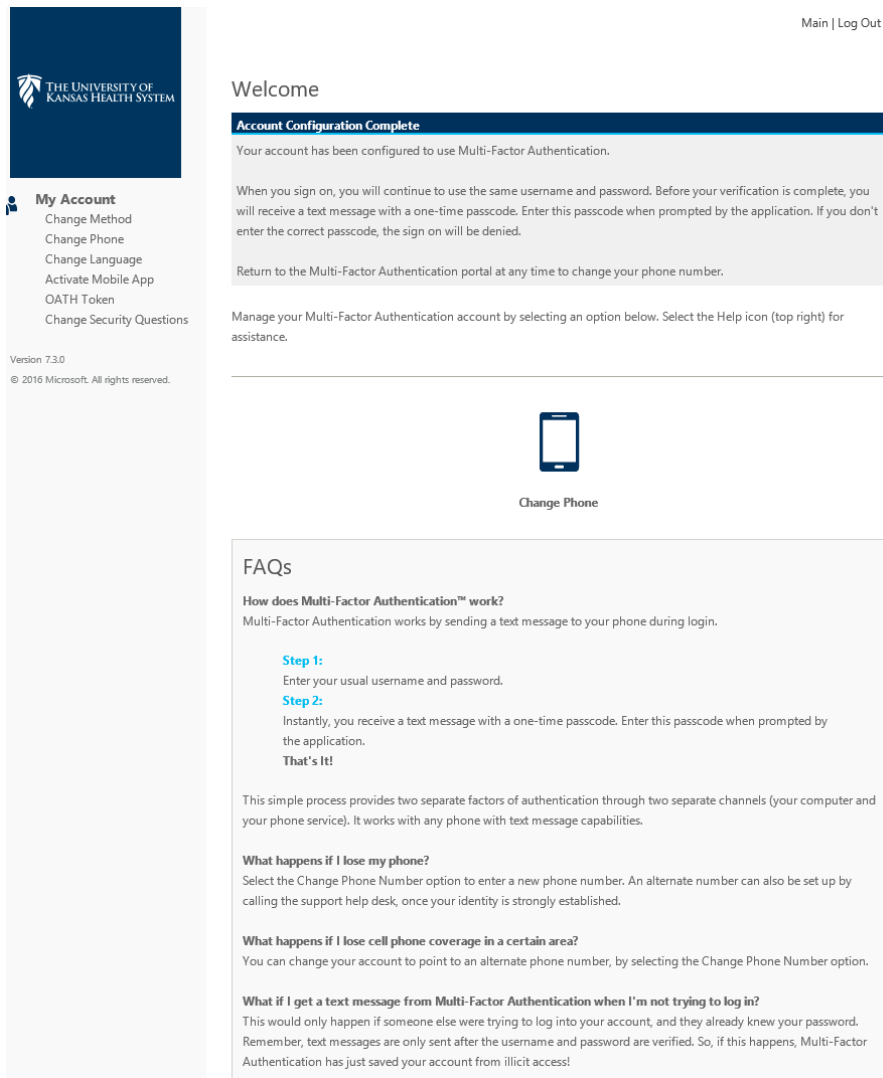
Answer

Multi-Factor Authentication Enrollment

ACCOUNT

After completing the security questions and clicking continue your account will be configured to use Multi-Factor Authentication. You will automatically be redirected to your account page.

From this page you can update your preferred authentication method to use any of the other methods, update your phone number and change your security questions.



The screenshot shows a web interface for Multi-Factor Authentication enrollment. On the left is a sidebar with the University of Kansas Health System logo and a 'My Account' menu containing options like 'Change Method', 'Change Phone', 'Change Language', 'Activate Mobile App', 'OATH Token', and 'Change Security Questions'. The main content area has a 'Welcome' message and a 'Account Configuration Complete' notification stating that the account is configured for MFA. Below this, there is a 'Change Phone' button with a mobile phone icon. A 'FAQs' section follows, with questions such as 'How does Multi-Factor Authentication™ work?', 'What happens if I lose my phone?', 'What happens if I lose cell phone coverage in a certain area?', and 'What if I get a text message from Multi-Factor Authentication when I'm not trying to log in?'. The top right corner of the page has links for 'Main | Log Out'.

FOR MORE INFORMATION CONTACT:

Hospital Help Desk 913-945-9999, Select #1 for Health System | Click **MyIT** icon on desktop

3.11.2019 | Produced by HITS | This material contains confidential and copyrighted information.

Multi-Factor Authentication Enrollment