MFA Registration Quick Reference Guide

Contents

1   Managing Your 2nd Factor Authentication Method

The MFA User Portal allows users to enroll in Multi-Factor Authentication and maintain their account. A user may change their phone number, authentication method, or security questions.
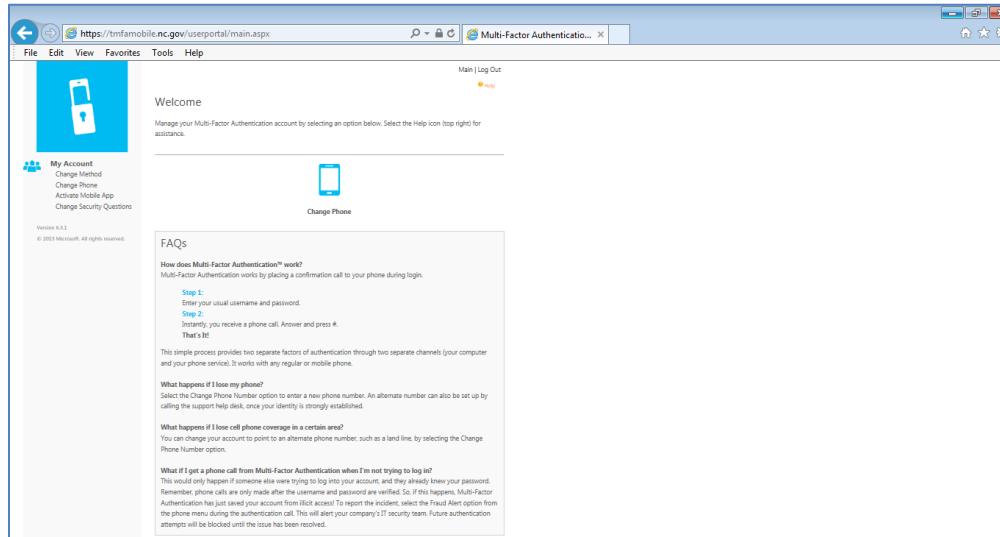
1.1   Change Method

This can be used to select your MFA method. Select Phone Call method to receive a phone call to authenticate. Select Text Message method to receive a text message to authenticate. Select Mobile App method to authenticate using the Multi-Factor Authentication mobile app. Select OATH Token method to authenticate using an authentication code from the Multi-Factor Authentication mobile app.
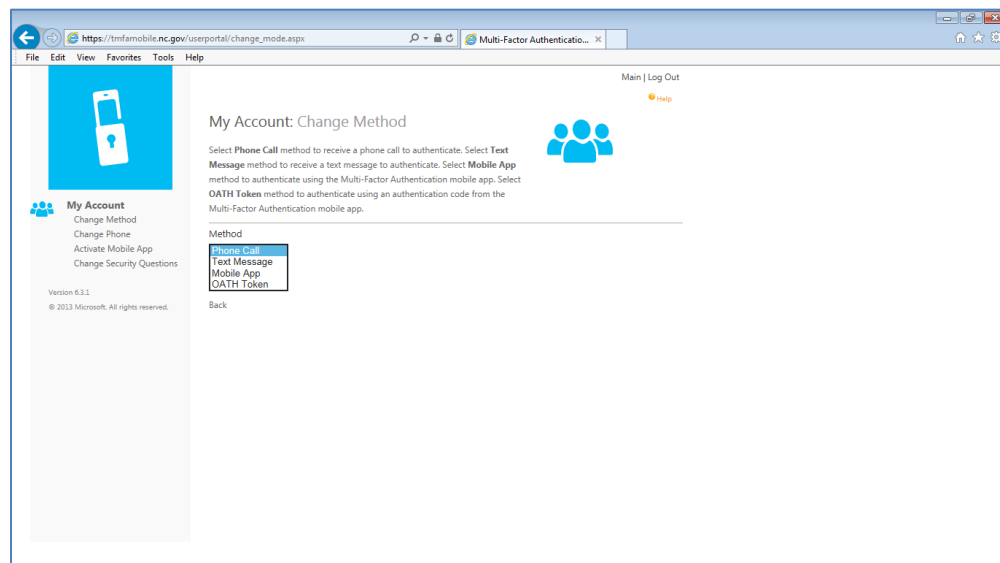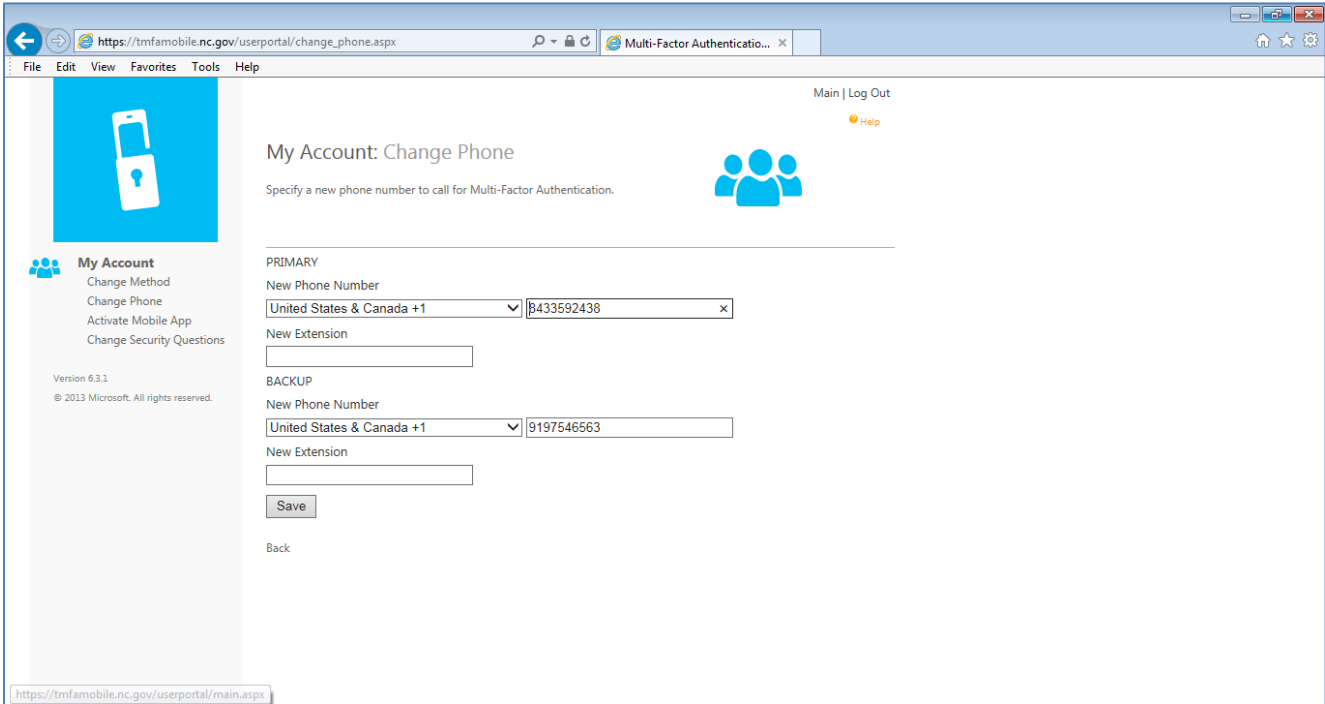
1.2   Change Phone

If you select the Voice Call authentication method or have been pre-configured to use that method, the page will prompt you to enter your primary phone number and extension if applicable. You may also enter a backup phone number (optional).

If you are required to use a PIN when you authenticate, the page will also prompt you to enter a PIN. After entering you phone number(s) and PIN (if applicable), click the Call Me Now to Authenticate button. Azure Multi-Factor Authentication will perform a phone call authentication to your primary phone number. You then must answer the phone call and enter their PIN (if applicable) and press # to move on to the next step of the self-enrollment process.

Figure – Change Phone

If you select the SMS Text authentication method or have been pre-configured to use that method, the page will prompt you to enter your mobile phone number. If you are required to use a PIN when you authenticate, the page will also prompt you to enter a PIN. After entering your phone number and PIN (if applicable), click the Text Me Now to Authenticate button. Azure Multi-Factor Authentication will perform an SMS authentication to your mobile phone. You must receive the SMS which contains a one-time-passcode (OTP) and enter the code field below.
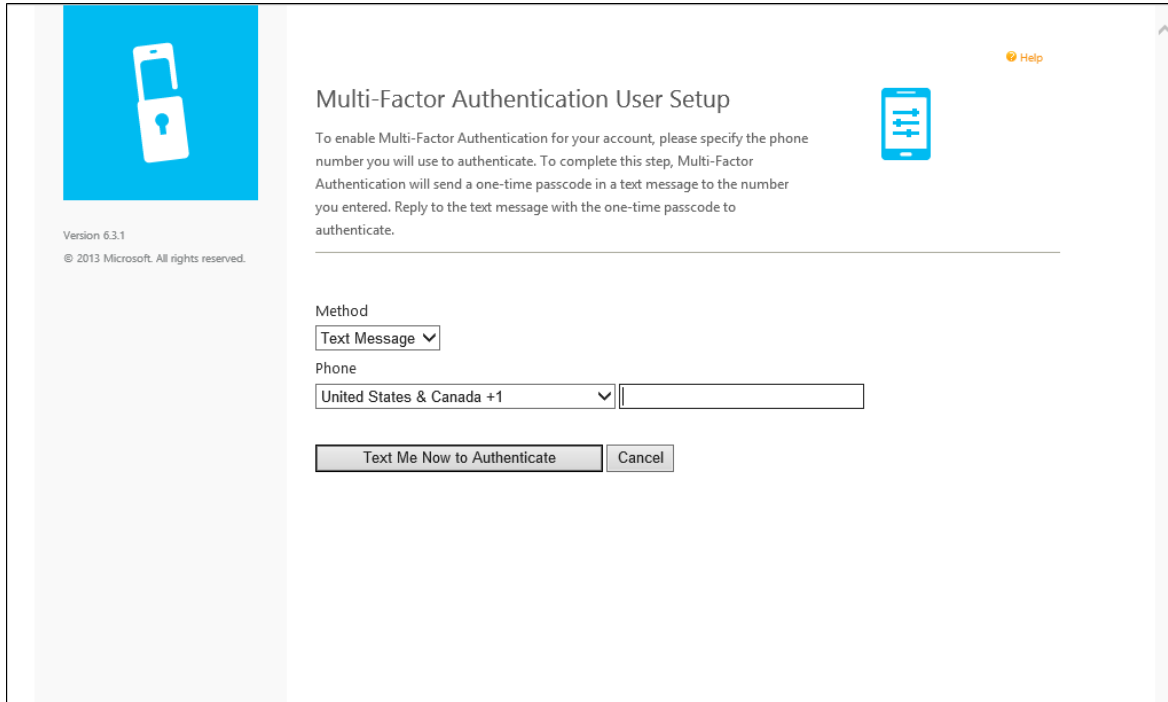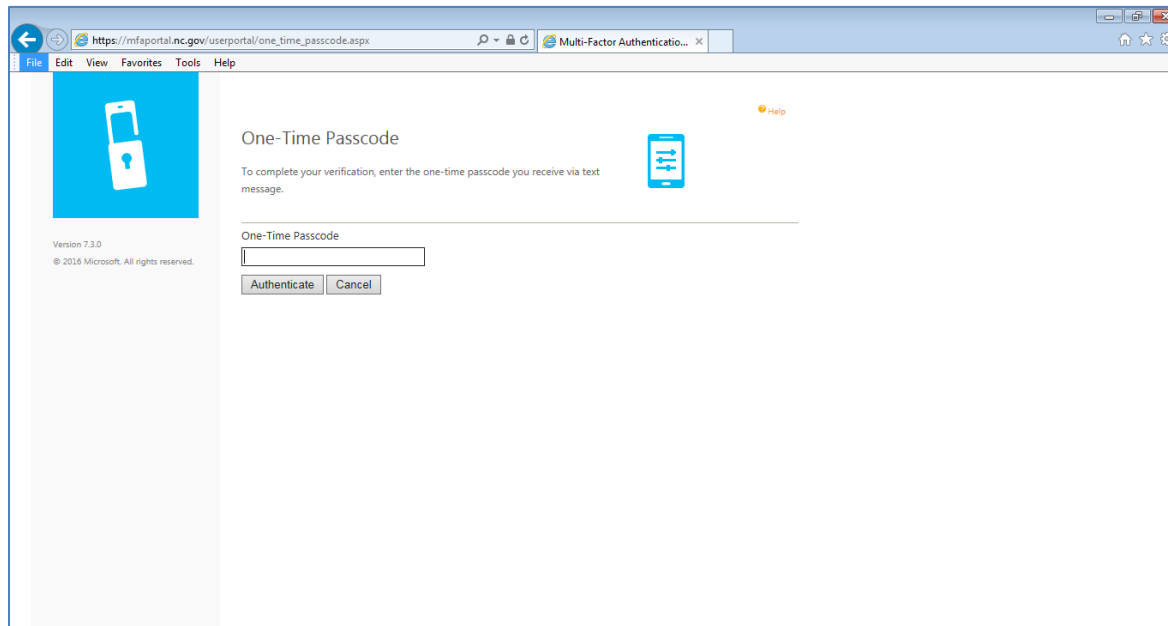

Figure – Enter One-Time Passcode

1.3   Install Mobile App

The Microsoft Authenticator lets you quickly and securely verify your identity. It must be downloaded to your smart phone from the provider's app store

- Android: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en
- iOS: https://itunes.apple.com/us/app/microsoft-authenticator/id983156458?mt=8
- Windows: www.microsoft.com/en-us/store/p/microsoft-authenticator/9nblgggzmcj6
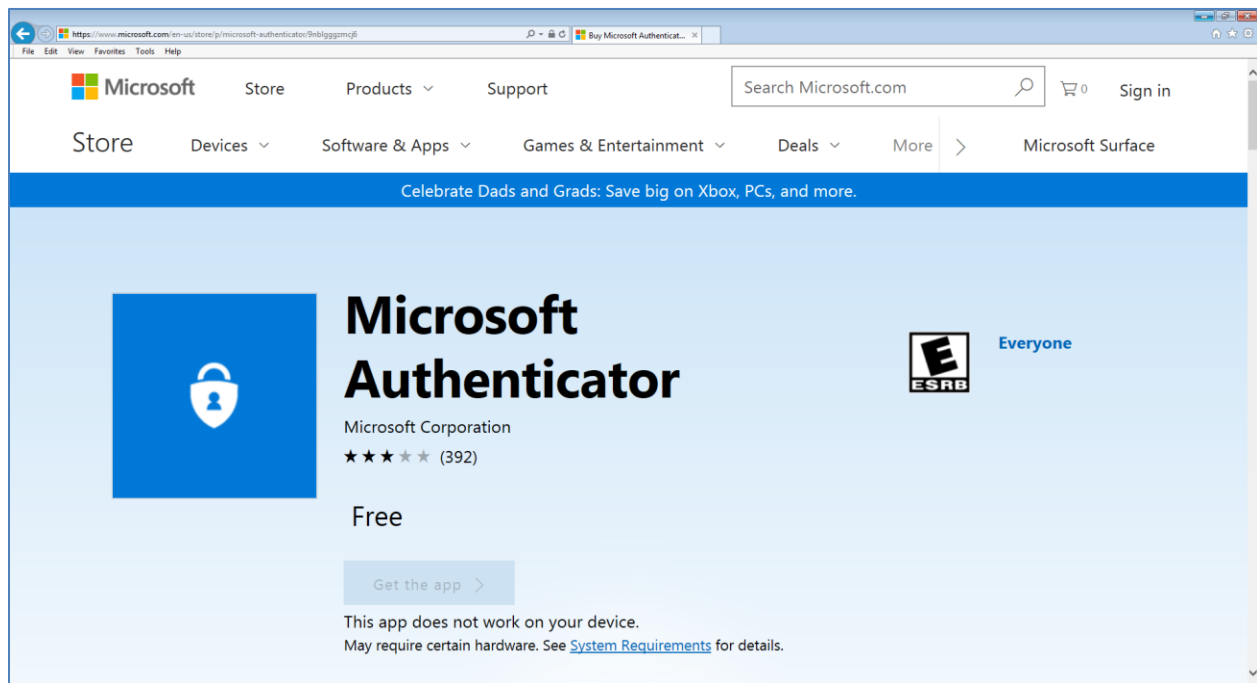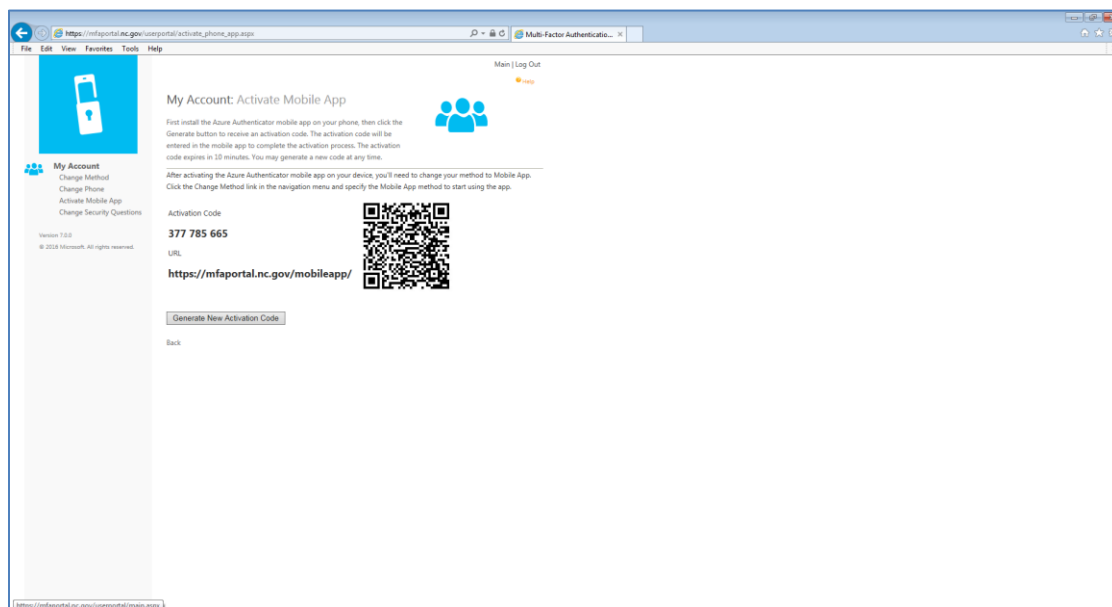
1.4   Activate Mobile App

If you select the Mobile app authentication method or have been pre-configured to use that method, the page will prompt you to install the Azure Multi-Factor Authentication app on your device and generate an activation code. After installing the Azure Multi-Factor Authentication app, click the Generate Activation Code button.
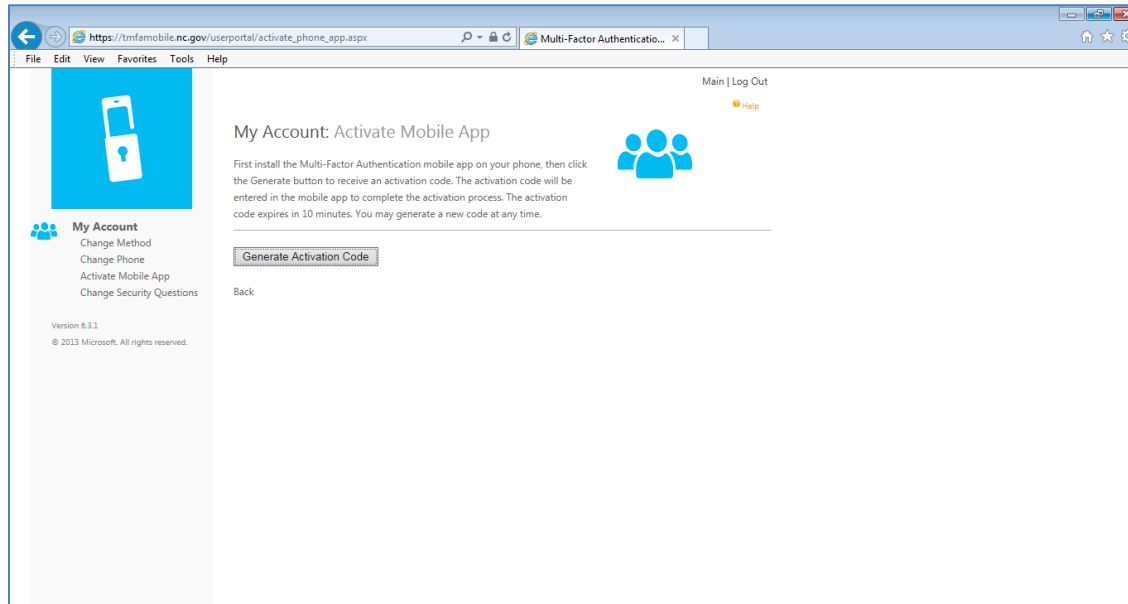
The page then displays an activation code and a URL along with a barcode picture. If you are required to use a PIN when you authenticate, the page will also prompt you to enter a PIN. You may enter the activation code and URL into the Azure Multi-Factor Authentication app or use the barcode scanner to scan the barcode picture and clicks the Activate button.

After the activation is complete, click the Authenticate Me Now button. Azure Multi-Factor Authentication will perform an authentication to your mobile app. You must enter your PIN (if applicable) and press the Authenticate button on your mobile app to move on to the next step of the self-enrollment process.
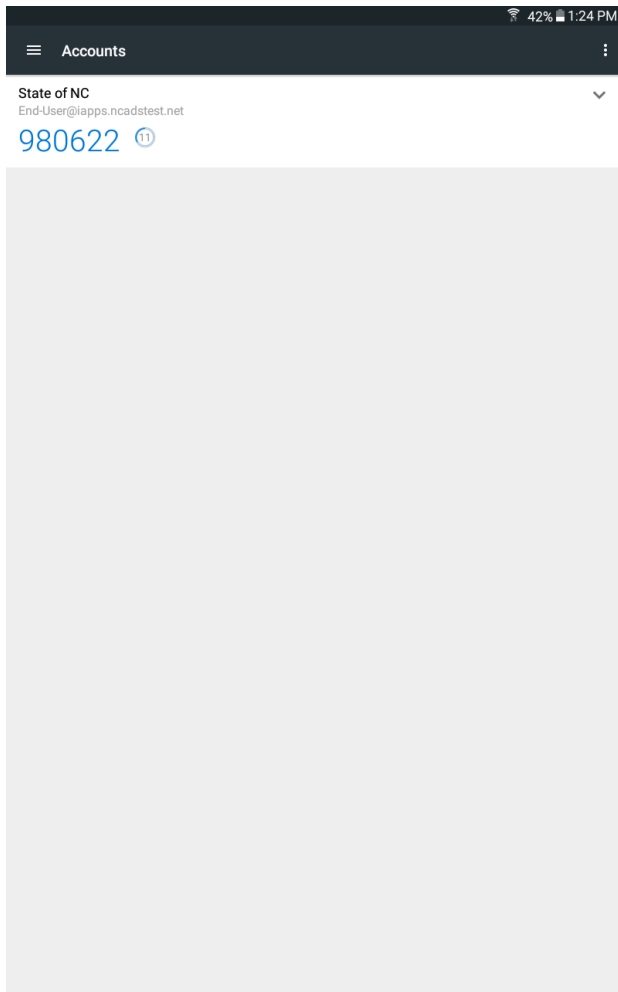
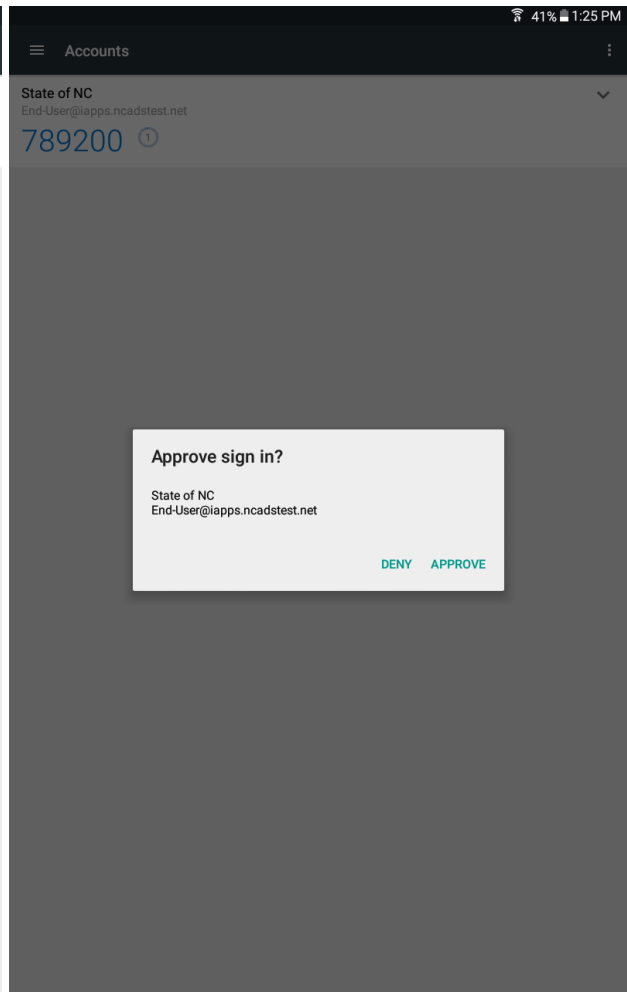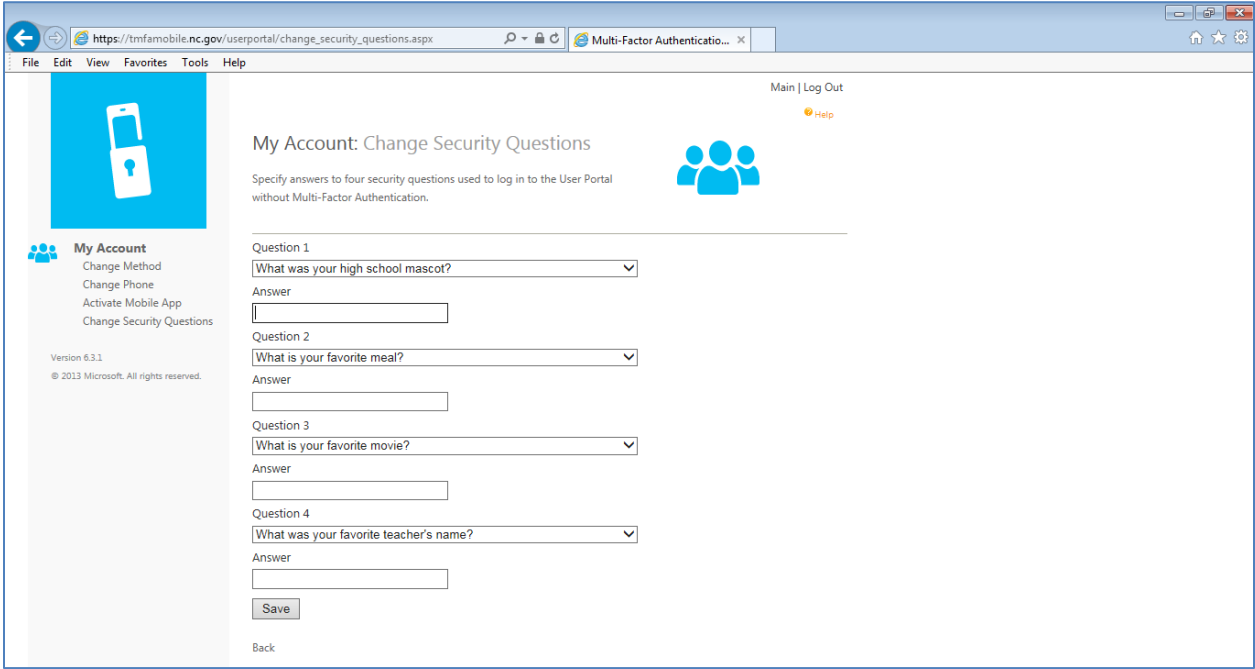Figure – Mobile App Idle   Figure – Mobile App Active

1.5   Change Security Questions

If, at any time, you are required to change your security questions or answers, click Change Security Questions and re-enter desired information, then click save. You must select four security questions and provide answers to the selected questions.

2   Frequently Asked Questions

Q: How can I get help with application access?

A: Contact the application/service owner who supports the application.

Q: How can I get help with the MFA registration process?

A: Contact the application/service owner who requested your enrollment.

Q: How can I get help with changing my MFA method?

A: Contact the application/service owner who requested your enrollment.

Q: What do I do if I don't receive a response on my phone or if I forgot my phone?

A: If you previously configured a backup phone, try again by selecting that phone when prompted from the sign in page. If you have not configured a backup phone, you may:

a) Browse to the MFA user portal page and sign in using your security questions. Once signed in, you may change your 2nd factor method.
b) Contact your admin and ask them to update your 2nd factor method, and/or the number assigned to your primary phone – mobile or office.

Q: Why am I receiving an MFA call from an anonymous caller after setting up caller ID?

A: Sometimes, when MFA calls are placed through the public telephone network, they are routed through a carrier that doesn't support caller ID. Therefore, caller ID is not guaranteed even though the MFA system always sends it.

Q: What if my 2nd factor device (mobile phone/tablet) is lost or stolen?

A: If your 2nd factor method is lost or stolen, you should immediately:

a) Browse to the MFA user portal page and sign in using your security questions. Once signed in, you may change your 2nd factor method.
b) Contact your admin and ask them to update your 2nd factor method, and/or the number assigned to your primary phone – mobile or office.