Setting up MFA in the Cloud Ver 3

NEBRASKA
Good Life. Great Vision.
OFFICE OF THE CIO

OCIO Network Services
January 2021

Overview

Multi-Factor Authentication (MFA) enables users to securely access work applications from remote working locations. Logging into the State's secure applications, such as email, with an MFA account enabled requires authentication using one of the following methods:

- Approval via push notification - Deny or approve a login attempt from your Smartphone.
- Soft Token - Enter a rotating 6-digit code provided by the Microsoft Authenticator app.
- Hard Token - Enter a rotating 6-digit code provided by a key-fob device.
- Text Token - Enter a One-Time Passcode provided by a text message.

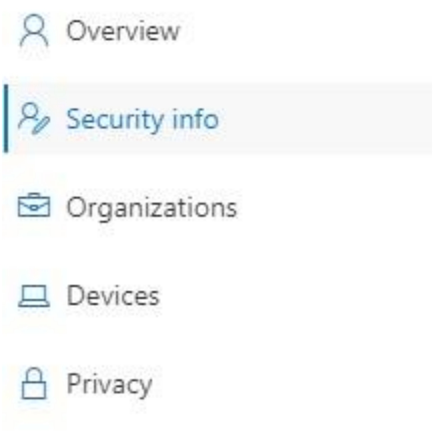
This guide will assist MFA users in setting up their MFA account on a mobile device. To do this, you will need a computer with internet access and your mobile device.

Setting Up Your Account

1. From your workstation, launch a modern browser (Chrome, Edge or Firefox), and go to https://mysignins.microsoft.com
2. If prompted, login to your Microsoft account. Although Microsoft displays Email or phone on the identity entry line, use your Nebraska Azure user account. (first.last@nebraska.gov)
3. Microsoft will direct you to the State of Nebraska's sign in page. Sign in on the State's ADFS page using your STN username (username@nebraska.gov) and password.

> **My Sign-Ins.** Once this page loads, you may see a screen detailing the different places you have logged in from. If you see something that is out of the ordinary (you signed in from Russia for example), contact the OCIO Service Desk immediately.

4. Select Security Info from the home menu to the left side of the screen.

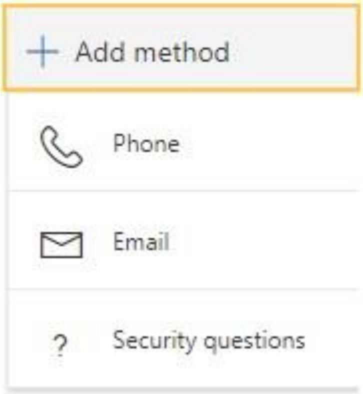


   a. As detailed in Step 5, you will need to setup your security questions.

   b. If the 'Security Questions' field already exists, you're all set. Skip ahead to Step 7.

5. Begin setting up your security questions.

   Select +Add Method.



   From the dropdown menu select Security Question, then Add.

6. For each question, use the dropdown menu to select a question you will easily remember the answer to. Type the answer in the proceeding line. Continue until all three questions are answered.

   Select Done.

Setting up MFA in the Cloud

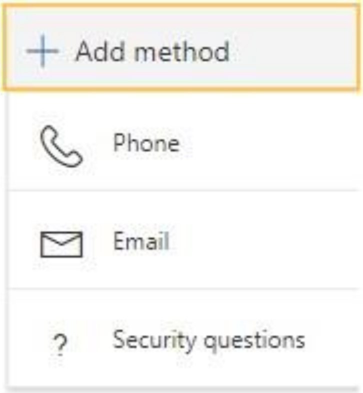
7. The preferred method for MFA is the Microsoft Authenticator app. You can also register to have a code texted to your phone for authentication. **To set up your phone for text MFA instead of using the Microsoft Authenticator app, skip to step 15**.

Before you proceed, the Microsoft Authenticator app must be installed on your mobile device. If you haven't done that yet, you can download and install Microsoft Authenticator from the Google Play Store for Android devices or go to the App Store if you are using an Apple device.

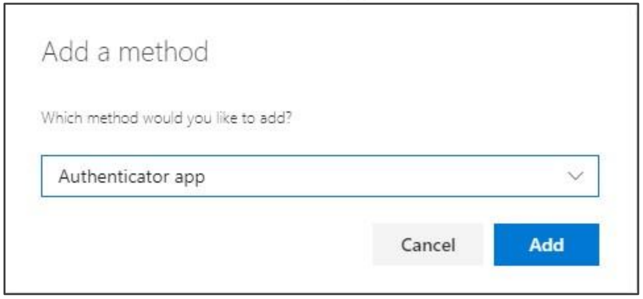
Do not remove the authenticator app if it is already present on your phone.

8. **Setting up MFA using the Authenticator app**

Return to the +Add Method link.



Select the Authenticator App


Add a method

Which method would you like to add?

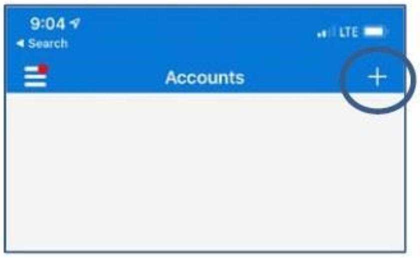
Authenticator app

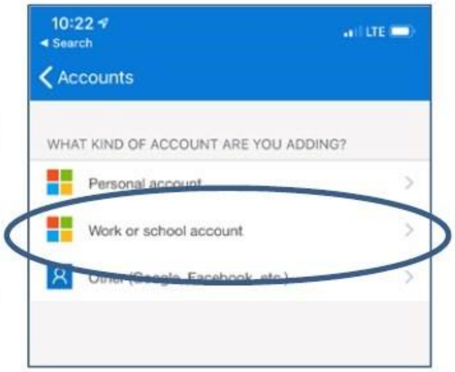
9. On your mobile device, navigate to Authenticator to open/launch the application.

10. Setup your new Authenticator account. Select Add (+) in the top right corner of the screen. *If you are re-registering a new device, then you should remove your old* ***@Nebraska.gov*** *account before setting up the new one. Otherwise, do not remove any previous/existing authenticator account(s), if present.*

Setting up MFA in the Cloud

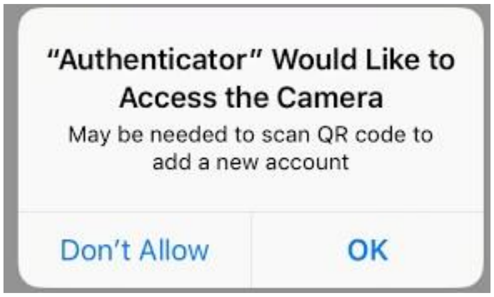
Select Work or School Account.




10:22
Search
LTE
Accounts
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)

11. Select “Scan a QR code”.

Authenticator may prompt you to allow access to your camera. Select OK.



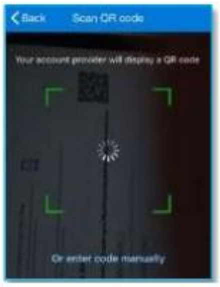
“Authenticator” Would Like to Access the Camera

May be needed to scan QR code to add a new account

12. From your computer browser, select Next.

This will generate your QR code (example shown). Use your phone to scan the QR code.

On your browser, select Next.



Your mobile device will prompt you to approve the initial configuration. Select Approve.

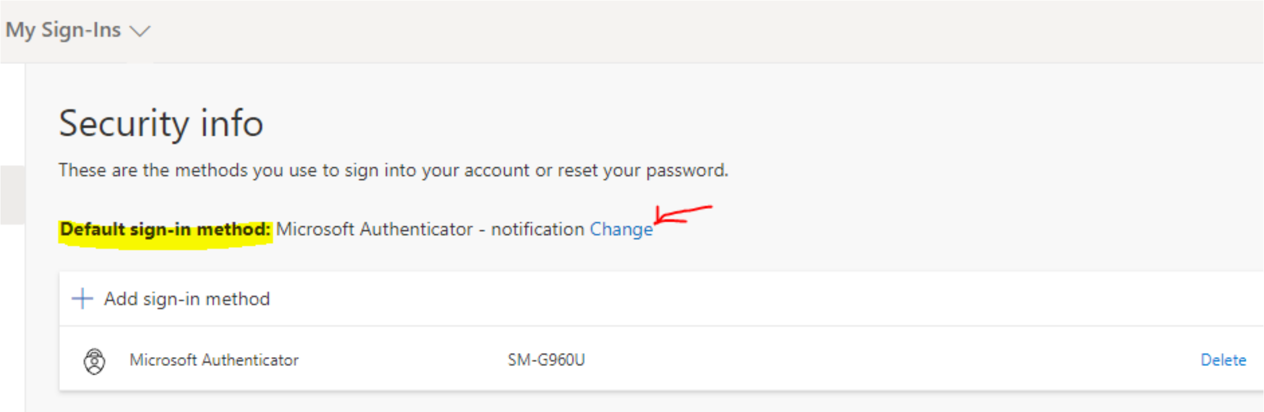
In the browser, select Next.   You may see a notification pop-up in your browser window if the new account was successfully set up.

Preparing Your Account For Use With A Hardware Token

13. If you will be using a hardware token (also referred to as a key fob) **OR** if you want to enter the 6 digit one-time pass code from the Microsoft Authenticator app instead of receiving a push notification, you will need to change your **Default sign-in method.**

> The 6 digit one-time pass code from the Microsoft Authenticator app is NOT the same as the one-time pass code texted to your phone via SMS message if the phone method is set up.

14. In the Security Info tab where you set up Microsoft Authenticator, go to the top of the page and find **Default sign-in method:** Click on Change



My Sign-Ins

Security info

These are the methods you use to sign into your account or reset your password.

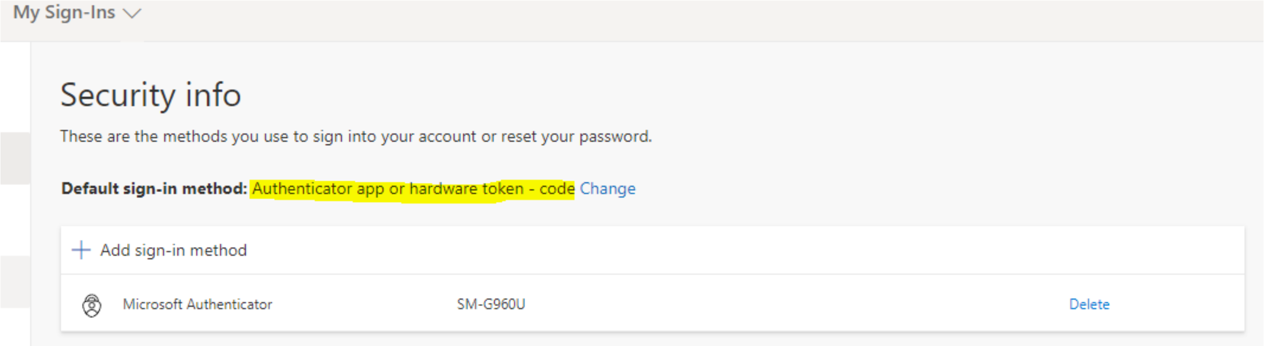
Default sign-in method: Microsoft Authenticator - notification Change

+ Add sign-in method

Microsoft Authenticator	SM-G960U	Delete

15. Select: **Authenticator app or hardware token code** and click **Confirm**

16. Your default sign-in method should look like this in order to use the hard token or the Microsoft Authenticator soft token codes.



My Sign-Ins

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Authenticator app or hardware token - code Change

+ Add sign-in method

Microsoft Authenticator	SM-G960U	Delete

When your account is set up to use this method, you can use either the code from the hard token or the code from the Microsoft Authenticator app. Both are valid and either will work.

Testing Authorization For Your New MFA Account

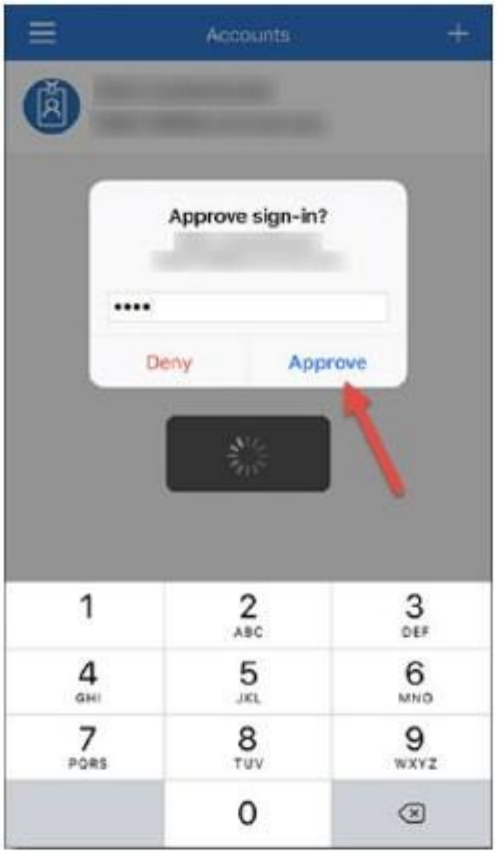
17. Sign Out of My Sign Ins (browser, upper right corner) and close the browser.

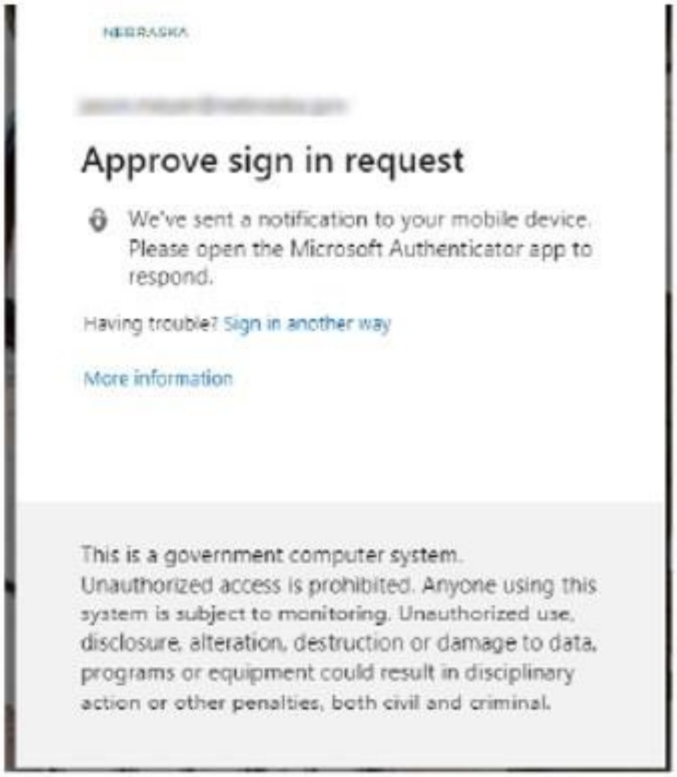
18. Launch a new browser and go back to https://mysignins.microsoft.com.

19. Select Security Info.

    If the account was set up successfully, your mobile device will receive a notification for Approval.

    Select Approve. A confirmation page will load in your computer's browser.





NEBRASKA

[redacted]

Approve sign in request

We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

Having trouble? Sign in another way

More information

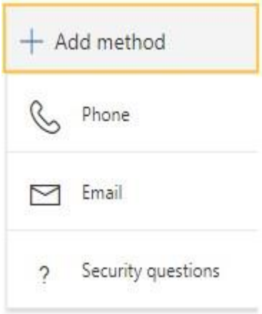
This is a government computer system. Unauthorized access is prohibited. Anyone using this system is subject to monitoring. Unauthorized use, disclosure, alteration, destruction or damage to data, programs or equipment could result in disciplinary action or other penalties, both civil and criminal.

Once you receive confirmation, your new account is all set. You can use your mobile device with the Authenticator app to send push notifications or enter a soft token code when signing in with MFA.

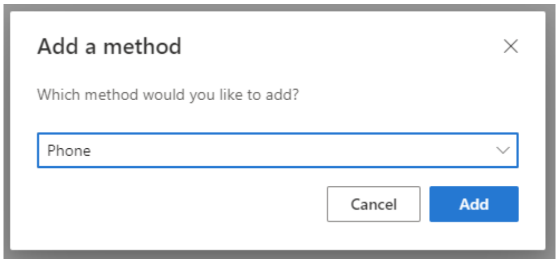
The following pages contain instructions for setting up MFA using text. If your setup with the Microsoft Authenticator app was successful, you can exit the document now.

20. **Setting up MFA using your phone to receive a onetime text code - *Optional***

Return to the +Add Method link.



21. Select the Phone option

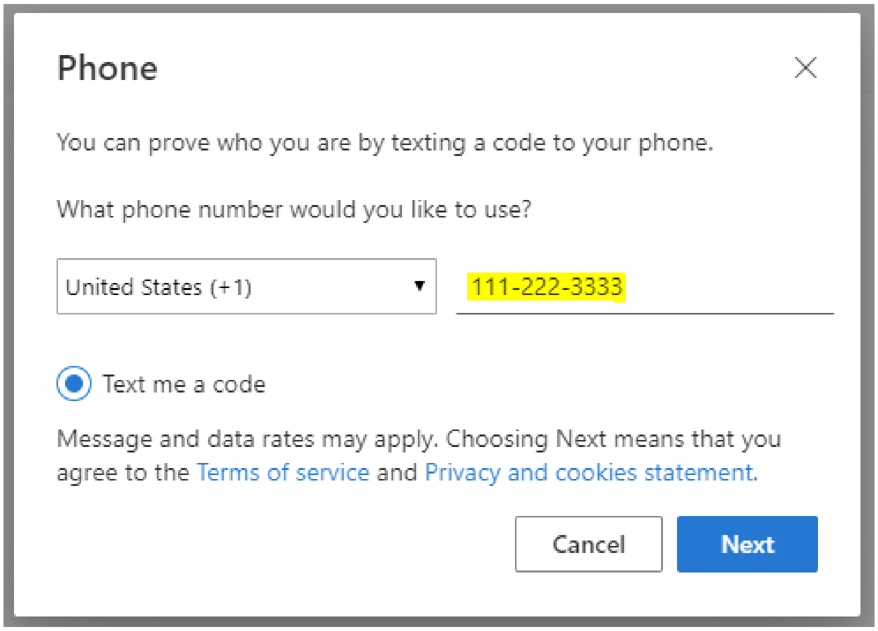


Add a method

Which method would you like to add?

Phone

22. Enter your mobile phone number into the appropriate box and then click Next.



Phone

You can prove who you are by texting a code to your phone.

What phone number would you like to use?

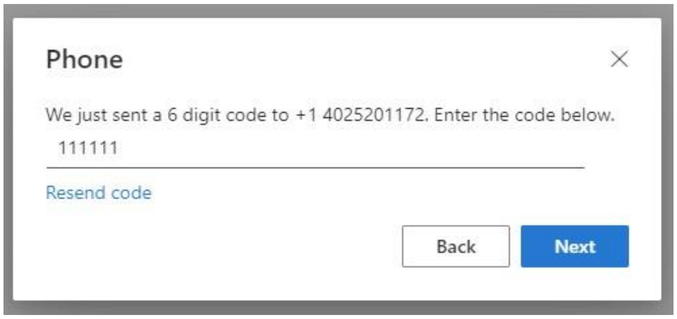
United States (+1) ▾ 111-222-3333

● Text me a code

Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement.

Setting up MFA in the Cloud

23. You will receive a text with a 6-digit code, enter the code and click Next.

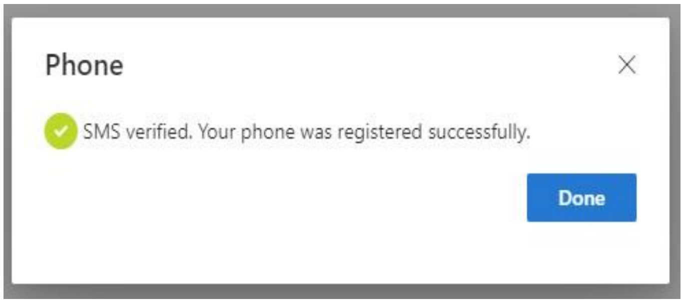


Phone

We just sent a 6 digit code to +1 4025201172. Enter the code below.

111111

24. You will see a notification of successful registration. Click on Done.



Phone

SMS verified. Your phone was registered successfully.

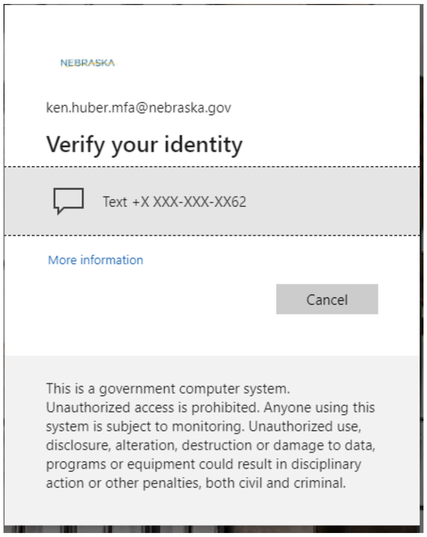
Authorizing your New MFA Account

25. Sign Out of My Sign Ins (browser, upper right corner) and close the browser.

26. Launch a new browser and go back to https://mysignins.microsoft.com.
Select Security info on the left side of the page.

Setting up MFA in the Cloud

27. You will get a pop-up box requesting that you verify your identity. Click on the grayed area.



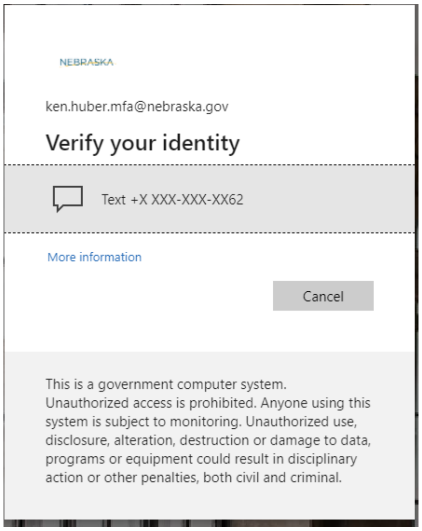
ken.huber.mfa@nebraska.gov

Verify your identity

Text +X XXX-XXX-XX62

This is a government computer system. Unauthorized access is prohibited. Anyone using this system is subject to monitoring. Unauthorized use, disclosure, alteration, destruction or damage to data, programs or equipment could result in disciplinary action or other penalties, both civil and criminal.

28. You will see another pop-up box where you can enter the code that was texted to you. Enter the code and click on Verify.



ken.huber.mfa@nebraska.gov

Verify your identity

Text +X XXX-XXX-XX62

This is a government computer system. Unauthorized access is prohibited. Anyone using this system is subject to monitoring. Unauthorized use, disclosure, alteration, destruction or damage to data, programs or equipment could result in disciplinary action or other penalties, both civil and criminal.

29. When the code is verified you will be taken to the Security Info webpage.

If further assistance is required, please contact the OCIO Service Desk team for support. Contact information is available at: https://cio.nebraska.gov/servicedesk/index.html.