Setting up MFA in the Cloud

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 using 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.

   ![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.

   ![Add Method]

   Select the Authenticator App

   ![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. **Do not remove any previous/existing authenticator account(s), if present.**

       Select Work or School Account.
11. Select “Scan a QR code”.

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

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.
Setting up MFA in the Cloud

Authorizing your New MFA Account

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


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.

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.
Setting up MFA in the Cloud

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

Return to the +Add Method link.

16. Select the Phone option

17. Enter your mobile phone number into the appropriate box and then click Next.
Setting up MFA in the Cloud

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

![Image of MFA setup interface](image)

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

![Image of MFA setup notification](image)

Authorizing your New MFA Account

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

Setting up MFA in the Cloud

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

23. 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.

24. 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.