

Enabling your MFA account for Use

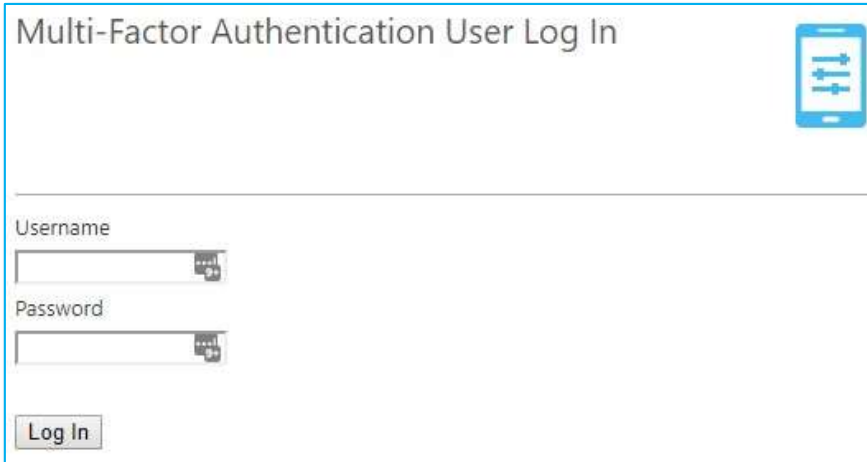
Welcome to the State of Nebraska Multi-Factor Authentication (MFA) solution, provided by Microsoft. MFA technologies provide enhanced security—on top of the standard username/password authentication mechanisms. When MFA is enabled for a service or an application, you can rest assured that any login attempts using your credentials will only be allowed when you approve the request with an additional form of authentication, something you have.

When logging into certain applications such as email, with your MFA account enabled, you will be asked to provide additional 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 a Smartphone 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.

Setup your MFA Account in 9 Steps

1. Begin by navigating to the OCIO Network Services Multi-Factor Authentication website:
<https://cio.nebraska.gov/network-serv/mfa/index.html>
2. Scroll down to the lower half of the page, click “Multi-Factor Authentication User Portal”

A screenshot of a web portal titled "Multi-Factor Authentication User Log In". The page has a light blue header with a smartphone icon on the right. Below the header, there are two input fields: "Username" and "Password", each with a small "mail" icon to its right. At the bottom left, there is a "Log In" button.

3. Login with your Windows AD account and password

For First-Time MFA users: You will be prompted with the User Setup dialogue box



Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account using the OATH Token method, 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
OATH Token ▼

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

Generate Activation Code Cancel

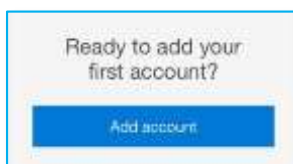
4. Set the Method

- a. Push Notification Users Select: **Mobile App ▼**
Select "Generate Activation Code"
- b. Soft Token Users Select: **OATH Token ▼**
Select "Generate Activation Code"
- c. Text Message Users Select: **Text Message ▼**
Enter 10 digit phone number and Select "Text Me Now to Authenticate"

5. **For Hard Token users:** Press the button to display the 6-Digit Code

For Soft Token or Push Notification users:

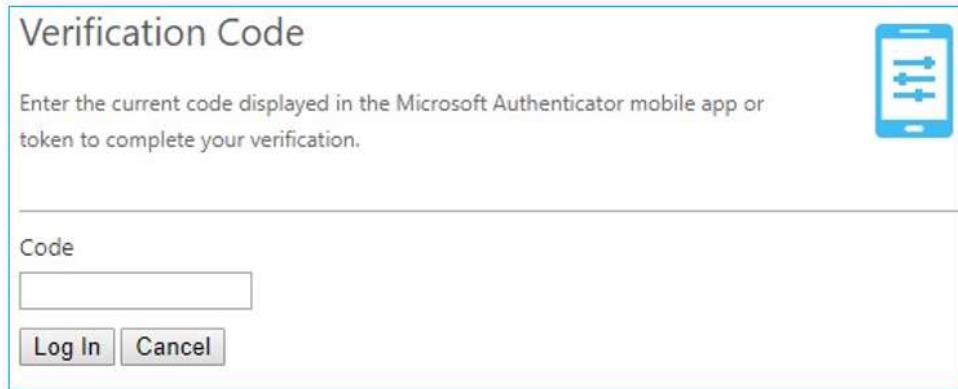
- d. Install and run the Microsoft Authenticator app available from your app store
 - i. Allow app to access Camera so you can Scan the QR Code
- e. Add a "Work or School Account"
- f. Scan the QR Code or Enter Activation Code and URL manually
- g. Successful installation will display the Soft Token (6-digit code)



6. Select "Authenticate Me Now"

7. For Hard Token, Soft Token, and Text Message users:

- a. You should see the Verification Code Screen

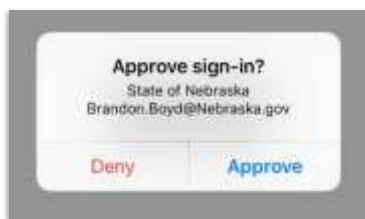
A screenshot of a web-based verification screen. At the top, the title "Verification Code" is displayed. Below the title, a message reads: "Enter the current code displayed in the Microsoft Authenticator mobile app or token to complete your verification." To the right of this message is a small icon of a smartphone. Below the message is a text input field labeled "Code". At the bottom of the screen are two buttons: "Log In" and "Cancel".

- b. In the Code box, enter the 6-digit number that is being displayed on your smartphone app

- c. Select "Log In", which should take you to the Security Questions screen

8. For Push Notification users:


- a. A Pop-Up notification on your smartphone should appear



- b.
- c. Selecting the Approve option on your smartphone will take you to the Security Questions screen in your browser

9. Complete the Security Questions and select "Continue"

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

In what city did you meet your spouse/significant other? ▼

Answer

Question 2

What was your childhood nickname? ▼

Answer

Question 3

What street did you live on in third grade? ▼

Answer

Question 4

What was the name of your first stuffed animal? ▼

Answer

When you are presented with the Welcome screen, your MFA User Account is complete.

Welcome

Account Configuration Complete

Your account has been configured to use Multi-Factor Authentication.

When you sign on, you will continue to use the same username and password. Before your verification is complete, you will be prompted by the application to enter the current verification code from the Microsoft Authenticator mobile app or token to complete your sign on. If you don't enter the correct verification code, the sign on will be denied.

Manage your Multi-Factor Authentication account by selecting an option below. Select the Help icon (top right) for assistance.

FAQs

How does Multi-Factor Authentication™ work?

Multi-Factor Authentication works by prompting for an verification code during login.

Step 1:

Enter your usual username and password.

Step 2:

Instantly, you are prompted for an verification code. Enter the current verification code displayed by the Microsoft Authenticator mobile app or token.

That's It!

This simple process provides two separate factors of authentication with the secondary authentication provided by something you have (your smart phone or token).

What happens if I lose my phone?

Select the Change Phone Number option to enter a new phone number. An alternate number can also be set up by calling the support help desk, once your identity is strongly established.

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

The Microsoft Authenticator mobile app does not need to be connected to the mobile network or WiFi in order to display verification codes.