Getting Started with Multi-Factor Authentication (MFA)

Mobile App

Updated as of 12/17/2019 10:58 AM

Welcome to the State of Nebraska Multi-Factor Authentication (MFA) solution provided by Microsoft.

MFA technologies were introduced to 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 are only allowed when you approve the request via a third factor.

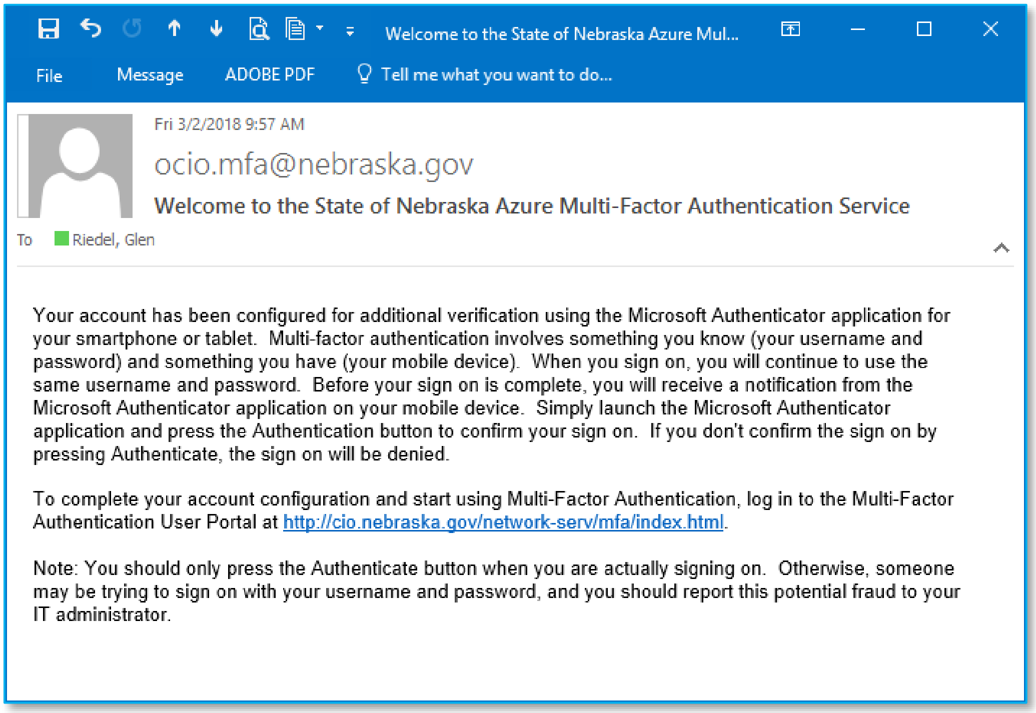
Depending on your security requirements, the third factor may be via:

- phone call
- text message
- app installed on a smartphone
    - push Deny-Approve notification (Mobile App)
    - rotating 6-digit code (OATH Token)
- key-fob style device
    - rotating 6-digit code (OATH Token)

As you can see above, there are several options available to use as the third factor. These ***Mobile App*** instructions will guide you through the setup and use of the “push Deny-Approve notification” option that will appear on your smartphone.

New User Notification

When your account is enabled for MFA you may receive a Welcome email.


Welcome to the State of Nebraska Azure Mul...
File
Message
ADOBE PDF
Tell me what you want to do...

Fri 3/2/2018 9:57 AM

ocio.mfa@nebraska.gov

Welcome to the State of Nebraska Azure Multi-Factor Authentication Service

To 🟩 Riedel, Glen

Your account has been configured for additional verification using the Microsoft Authenticator application for your smartphone or tablet. Multi-factor authentication involves something you know (your username and password) and something you have (your mobile device). When you sign on, you will continue to use the same username and password. Before your sign on is complete, you will receive a notification from the Microsoft Authenticator application on your mobile device. Simply launch the Microsoft Authenticator application and press the Authentication button to confirm your sign on. If you don't confirm the sign on by pressing Authenticate, the sign on will be denied.

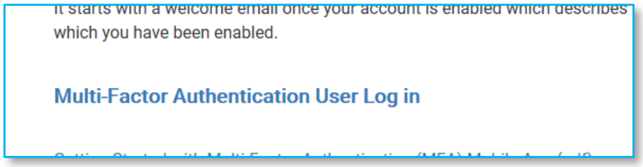
To complete your account configuration and start using Multi-Factor Authentication, log in to the Multi-Factor Authentication User Portal at http://cio.nebraska.gov/network-serv/mfa/index.html.

Note: You should only press the Authenticate button when you are actually signing on. Otherwise, someone may be trying to sign on with your username and password, and you should report this potential fraud to your IT administrator.

Setup Your Account for Mobile App Use

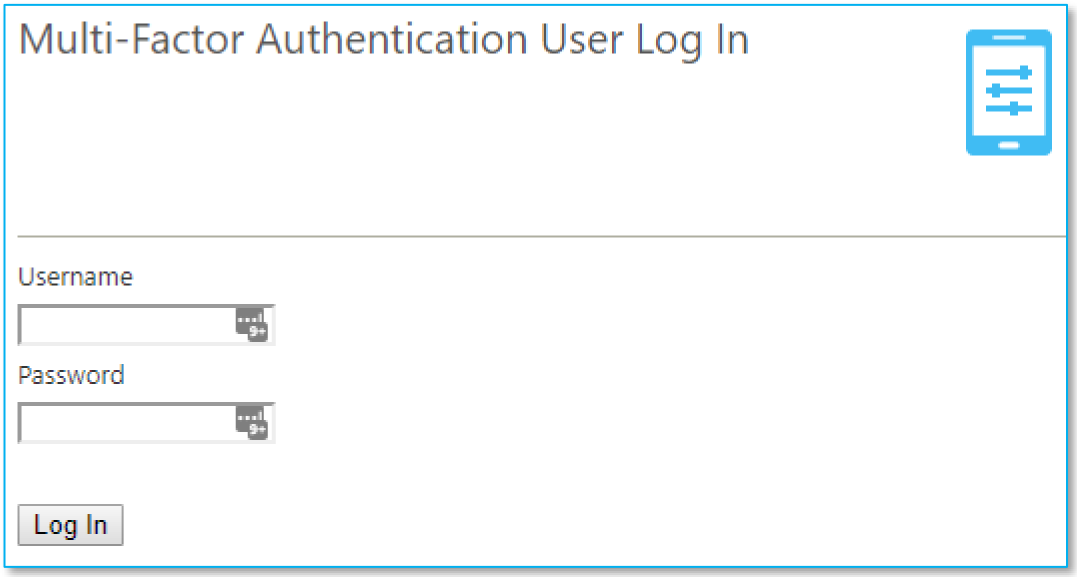
1. Visit the OCIO Network Services / Multi-Factor Authentication site at https://cio.nebraska.gov/network-serv/mfa/index.html and follow these steps.

2. Scroll down to the lower half of the page and click on the bold link “Multi-Factor Authentication User Log in”



It starts with a welcome email once your account is enabled which describes which you have been enabled.

Multi-Factor Authentication User Log in



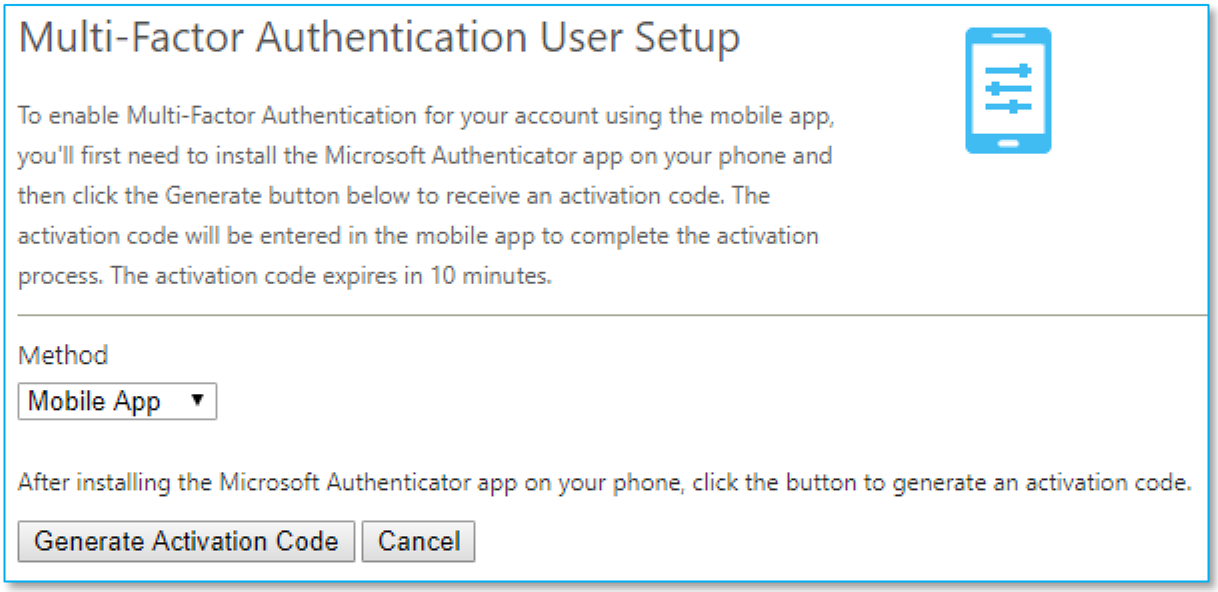
Multi-Factor Authentication User Log In

Username

Password

3. Login with your Windows AD account and password

For First-Time MFA users, you will be prompted with the User Setup screens



Multi-Factor Authentication User Setup

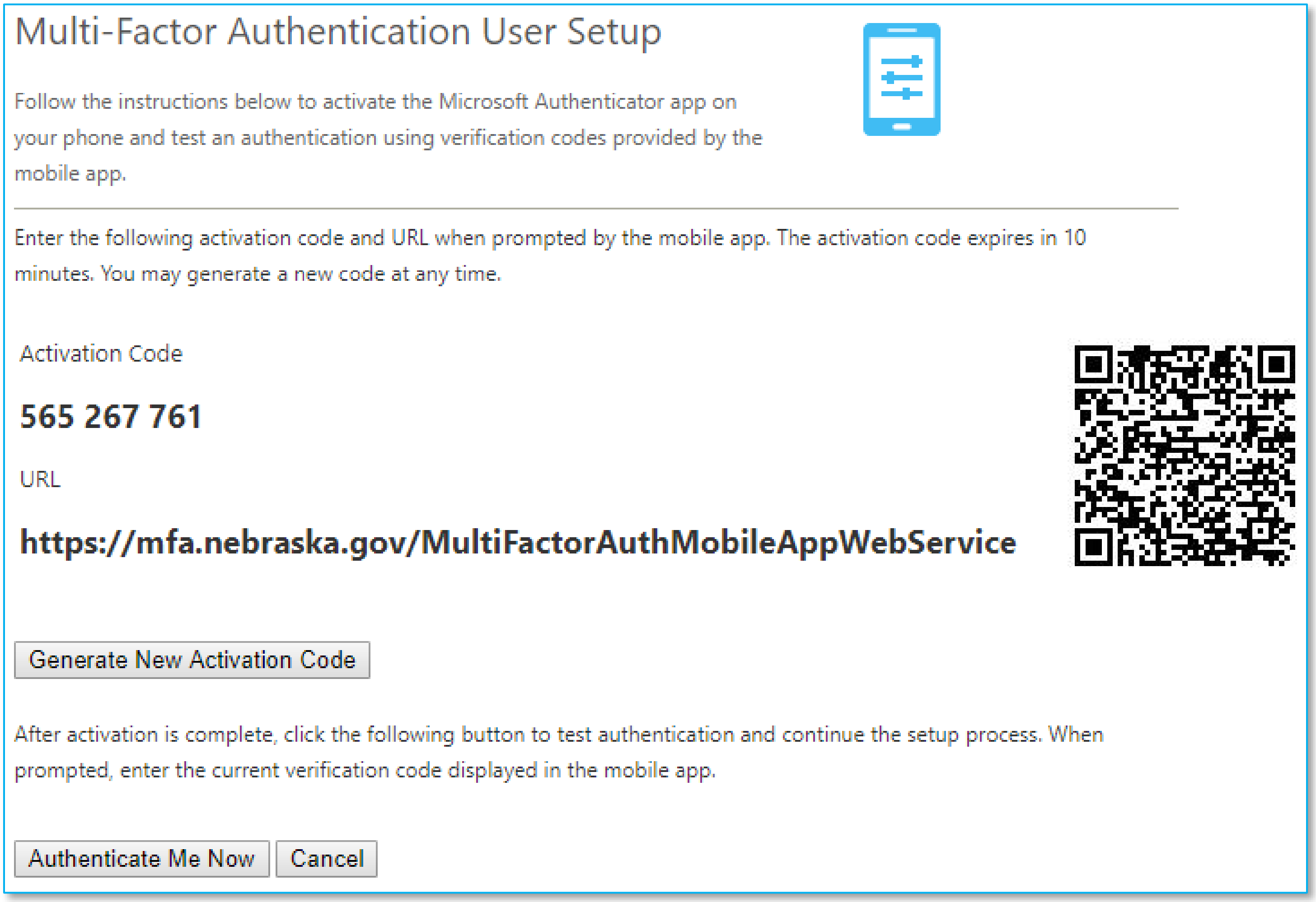
To enable Multi-Factor Authentication for your account using the mobile app, you'll first need to install the Microsoft Authenticator app on your phone and then click the Generate button below to receive an activation code. The activation code will be entered in the mobile app to complete the activation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

Method

Mobile App ▼

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

4. If not already displayed, change the Method to display Mobile App
5. Select the [Generate Activation Code] button



Multi-Factor Authentication User Setup

Follow the instructions below to activate the Microsoft Authenticator app on your phone and test an authentication using verification codes provided by the mobile app.

Enter the following activation code and URL when prompted by the mobile app. The activation code expires in 10 minutes. You may generate a new code at any time.

Activation Code

565 267 761

URL

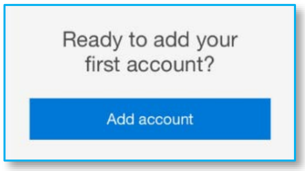
https://mfa.nebraska.gov/MultiFactorAuthMobileAppWebService

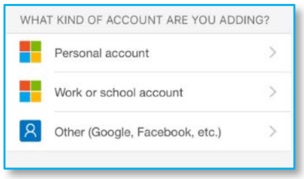
Generate New Activation Code

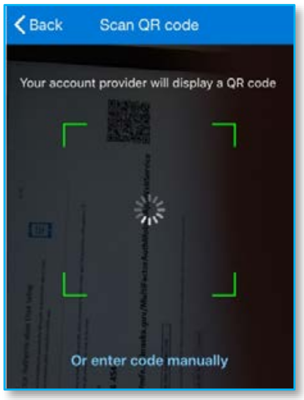
After activation is complete, click the following button to test authentication and continue the setup process. When prompted, enter the current verification code displayed in the mobile app.

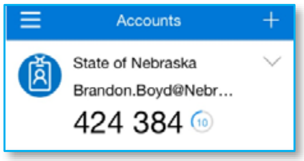
Authenticate Me Now Cancel

6. Setup on your smartphone:
   a. Install and run the Microsoft Authenticator app available from your app store
   b. Add a “Work or School Account”
   c. Scan the QR Code or Enter Activation Code and URL manually
   d. Successful installation will display a 6-digit Token.
      a. The 6-digit Token can be used with the *OATH Token* method of authentication.

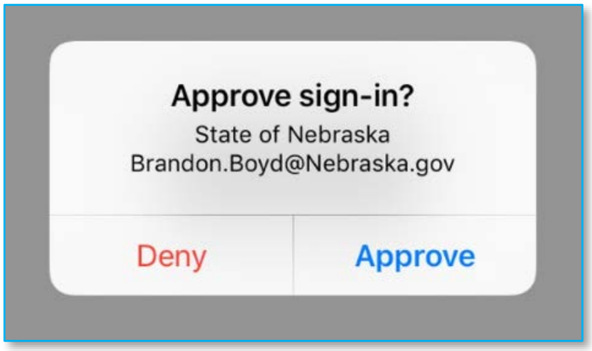



WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)





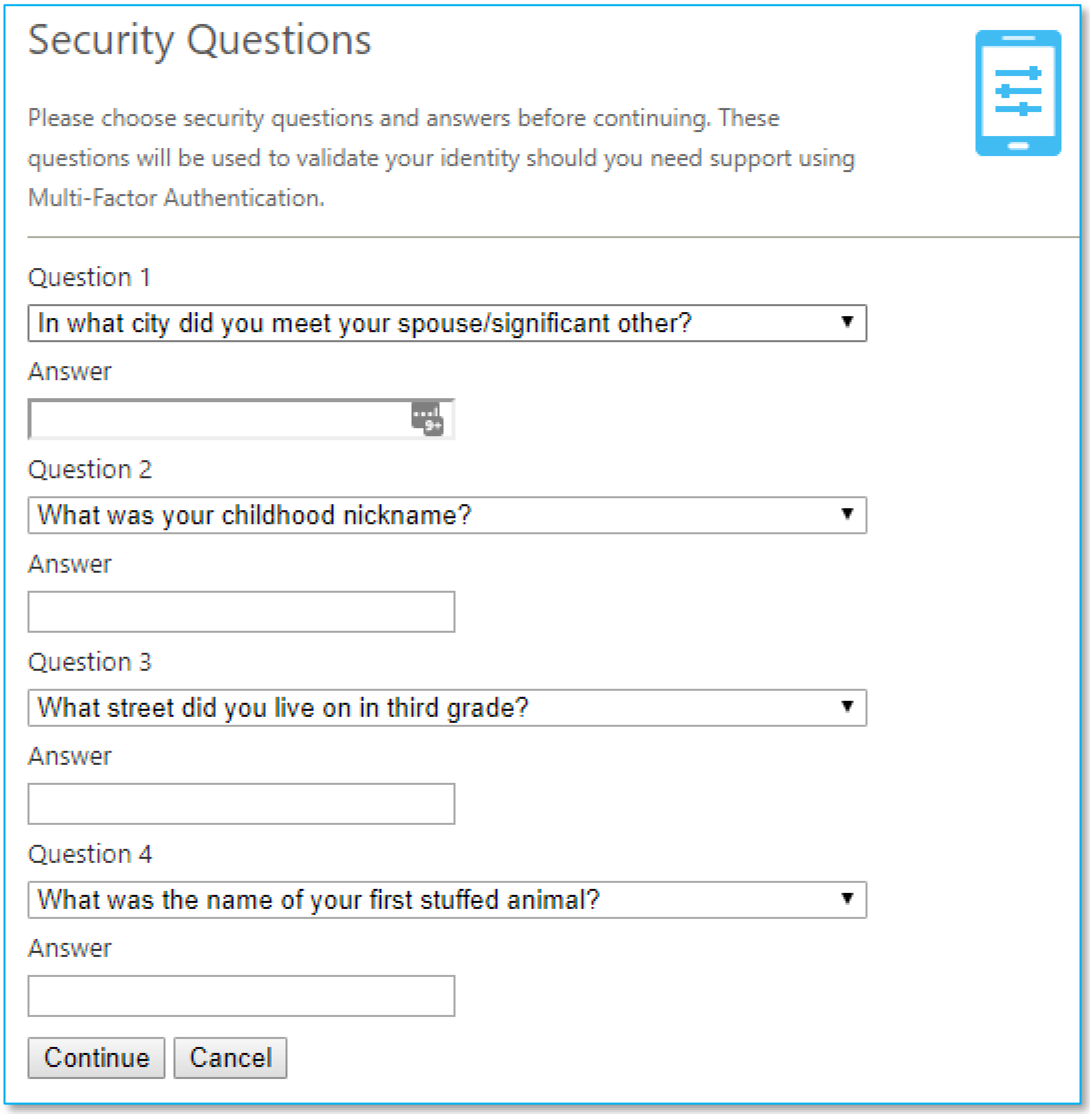
7. Back to the web page: Selecting the [Authenticate Me Now] button should generate a “push Deny-Approve notification” on your smartphone.



Approve sign-in?

State of Nebraska
Brandon.Boyd@Nebraska.gov

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



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

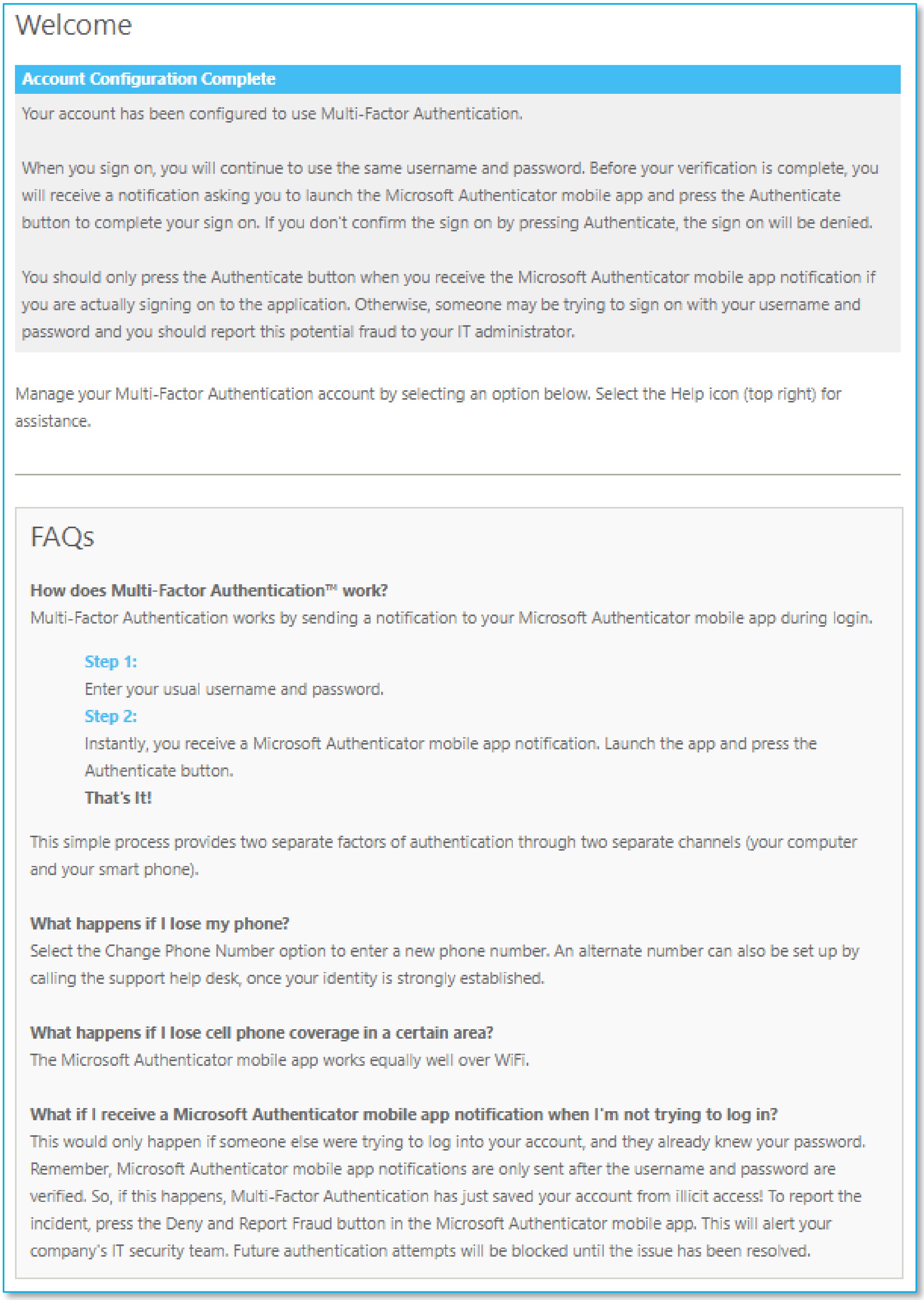
Question 4

What was the name of your first stuffed animal? ▾

Answer

9. Complete the Security Questions and select the [Continue] button

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 receive a notification asking you to launch the Microsoft Authenticator mobile app and press the Authenticate button to complete your sign on. If you don't confirm the sign on by pressing Authenticate, the sign on will be denied.

You should only press the Authenticate button when you receive the Microsoft Authenticator mobile app notification if you are actually signing on to the application. Otherwise, someone may be trying to sign on with your username and password and you should report this potential fraud to your IT administrator.

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 sending a notification to your Microsoft Authenticator mobile app during login.

Step 1:
Enter your usual username and password.
Step 2:
Instantly, you receive a Microsoft Authenticator mobile app notification. Launch the app and press the Authenticate button.
That's It!

This simple process provides two separate factors of authentication through two separate channels (your computer and your smart phone).

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?

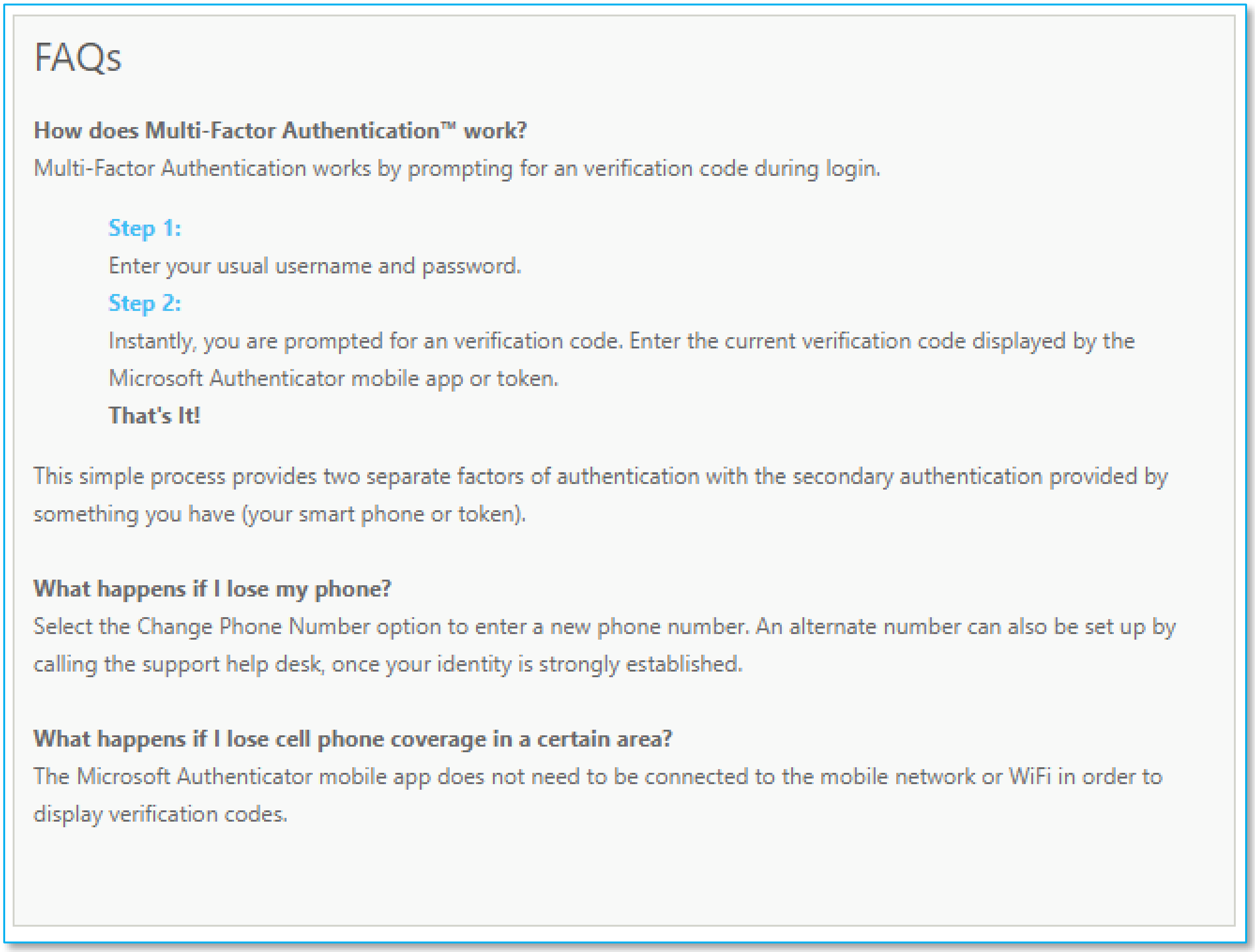
The Microsoft Authenticator mobile app works equally well over WiFi.

What if I receive a Microsoft Authenticator mobile app notification when I'm not trying to log in?

This would only happen if someone else were trying to log into your account, and they already knew your password. Remember, Microsoft Authenticator mobile app notifications are only sent after the username and password are verified. So, if this happens, Multi-Factor Authentication has just saved your account from illicit access! To report the incident, press the Deny and Report Fraud button in the Microsoft Authenticator mobile app. This will alert your company's IT security team. Future authentication attempts will be blocked until the issue has been resolved.

Additional Notes:

If you have decided to use the Mobile App for authentication, another alternative would be to use the OATH Token on your mobile device. To try out this feature, access your MFA account (via Step 1 above), *Change Method* to **OATH Token**, and be sure to *Activate Mobile App*. Below are some FAQ's when this Method is chosen.



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.