Multi-Factor Authentication

Audience

naviHealth External Users (**nH Coordinate** and **nH Access**)

Contents

Overview

Back to Contents

This work instruction provides guidance on how to set up multi-factor authentication (MFA) for external users of naviHealth applications, like **nH Coordinate** or **nH Access**. All users of naviHealth applications are required to set up MFA.

Multi-factor authentication is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application or online account. MFA decreases the likelihood of a successful cyber-attack.

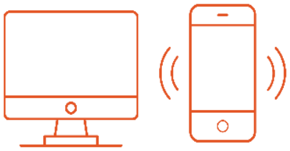
naviHealth set up a two-factor model where the first factor is something the user knows, such as their username and password, and the second factor is something the user has in their possession which is unique to them, such as a onetime password which is sent via email or text.

For any issues or questions, see the Multi-Factor Authentication FAQ at the end of this document or contact the **nH Coordinate** or **nH Access** support team.

Multi-Factor Authentication

If you have naviHealth account credentials you are required to setup MFA.

nH Access
nH Coordinate



Multi-Factor Authentication

How does MFA work?

First factor is your account credentials

Second factor is a onetime password (code) sent via email or text, or a phone call.

Here are the choices of second factors
You only need one of these, but you may have both

Email
Onetime password (code) sent to the email address associated with your naviHealth account

SMS and Voice
Provide your phone number and then have the option to answer a phone call or receive a text

Which sections of the instruction do I need?

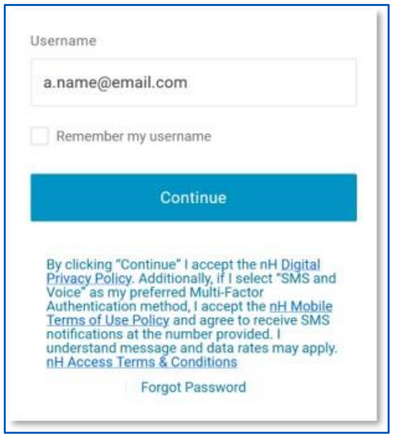
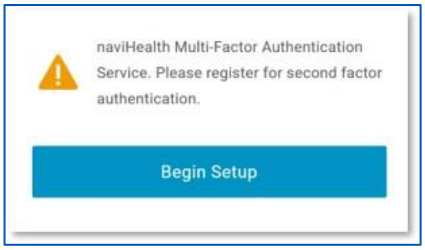
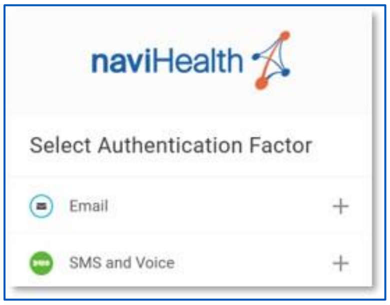
Email only	1. Section 1: First time login 2. Section 2: Email Setup
SMS and Voice only	1. Section 1: First time login 2. Section 4: SMS and Voice Setup
Email and SMS and Voice	1. Section 1: First time login 2. First go to Section 2 or 4 3. Section 3: Link to manage factors 4. Then go to Section 4 or 2

Multi-Factor Authentication

Section 1:
First-time Login

Back to Contents

Follow the steps below if this is the first time logging in to setup multi-factor authentication (MFA)

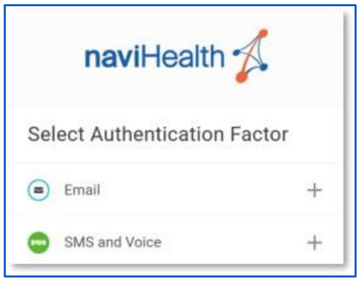
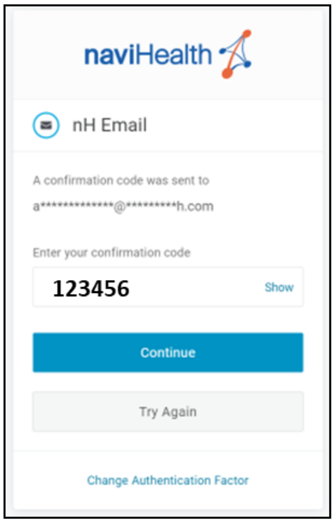
Step	Action
1.	Click or navigate to https://navihealth.onelogin.com to login to your OneLogin account. Enter your username/email address and click **Continue**.  Username a.name@email.com □ Remember my username Continue By clicking "Continue" I accept the nH Digital Privacy Policy. Additionally, if I select "SMS and Voice" as my preferred Multi-Factor Authentication method, I accept the nH Mobile Terms of Use Policy and agree to receive SMS notifications at the number provided. I understand message and data rates may apply. nH Access Terms & Conditions Forgot Password
2.	Click **Begin Setup**.  naviHealth Multi-Factor Authentication Service. Please register for second factor authentication. Begin Setup
3.	Select which factor you would like to setup firs:  naviHealth Select Authentication Factor Email + SMS and Voice + If Email – proceed to Section 2 of this instruction If SMS and Voice – proceed to Section 4 of this instruction

Multi-Factor Authentication

Section 2: Email

[Back to Contents](#)

Follow the steps below to setup **Email** as an authentication factor

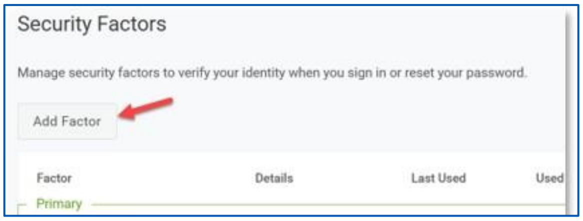
Step	Action
1.	This section assumes you have already logged in with your account credentials and have selected to setup **Email**  naviHealth Select Authentication Factor Email + SMS and Voice +
2.	You will receive an email with a login code. Enter the code and select **Continue**.  naviHealth nH Email A confirmation code was sent to a**************@**********h.com Enter your confirmation code 123456 Show Continue Try Again Change Authentication Factor **NOTE:** If you did not receive the email or the code expired before you had a chance to enter it, select **Try Again** so a new code can be sent.

Section 3:

Link to Manage Factors

Back to Contents

Follow the steps below to setup a second authentication factor.

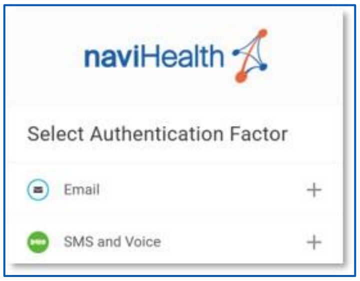
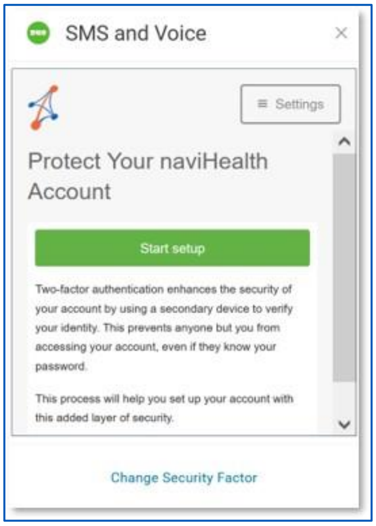
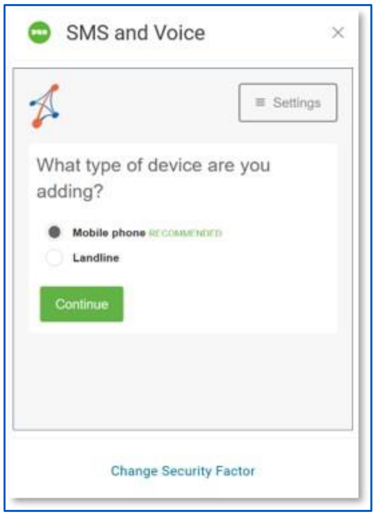
Step	Action
1.	This section assumes that you are logged in with your account credentials, you have already setup Email or SMS and Phone as a factor and you wish to also add the other as a factor
2.	Click or navigate to: https://navihealth.onelogin.com/profile2/mfa
3.	Select **Add Factor**.  Security Factors Manage security factors to verify your identity when you sign in or reset your password. Add Factor Factor Details Last Used Used Primary

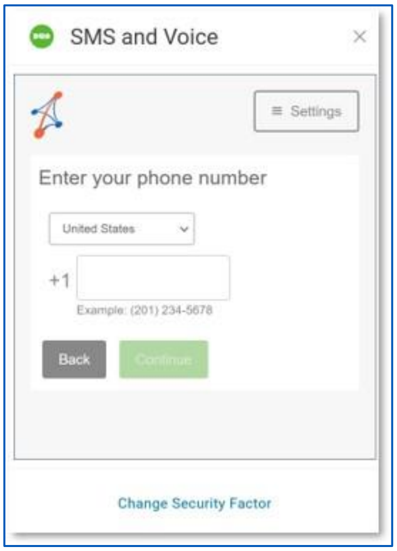
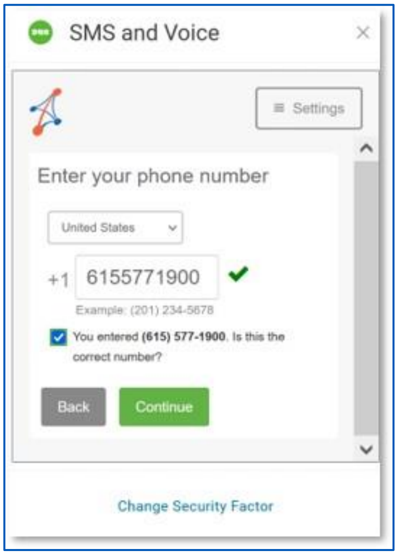
Multi-Factor Authentication

Section 4: SMS and Voice

[Back to Contents](#)

Follow the steps below to setup **SMS and Voice** as an authentication factor. Setting up **SMS and Voice** as an authentication factor is optional.

Step	Action
1.	This section assumes you have already logged in with your account credentials and have selected to setup **SMS and Voice**  naviHealth Select Authentication Factor Email + SMS and Voice +
2.	Select **Start setup**.  SMS and Voice × ≡ Settings Protect Your naviHealth Account Start setup Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password. This process will help you set up your account with this added layer of security. Change Security Factor
3.	Ensure that **Mobile phone** is selected, and then select **Continue**.  SMS and Voice × ≡ Settings What type of device are you adding? ● Mobile phone RECOMMENDED ○ Landline Continue Change Security Factor

4.	Enter your mobile phone number. **NOTE:** Only US-based phone numbers are permitted.  SMS and Voice ≡ Settings Enter your phone number United States +1 Example: (201) 234-5678 Back Continue Change Security Factor
5.	A green check mark will appear to verify a 10-digit number has been entered.  SMS and Voice ≡ Settings Enter your phone number United States Example: (201) 234-5678 Back Continue Change Security Factor +1 6155771900 ✓ ☑ You entered **(615) 577-1900**. Is this the correct number? Check the box to verify the correct phone number has been entered. Click **Continue**.

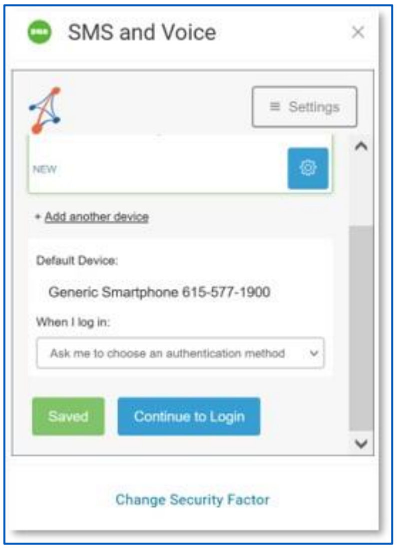
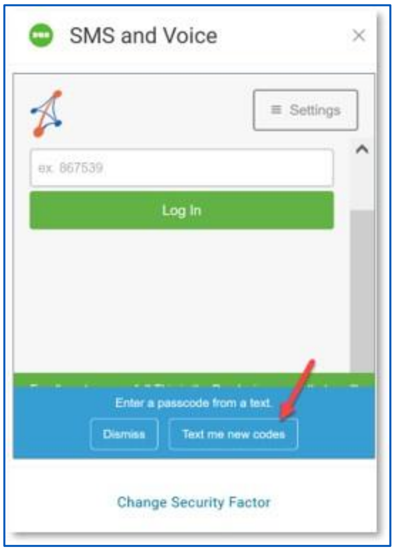
Continued on next page

Multi-Factor Authentication

Section 4: SMS and Voice (continued)

[Back to Contents]

Follow the steps below to setup SMS/text messaging as a second authentication factor.

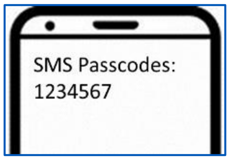
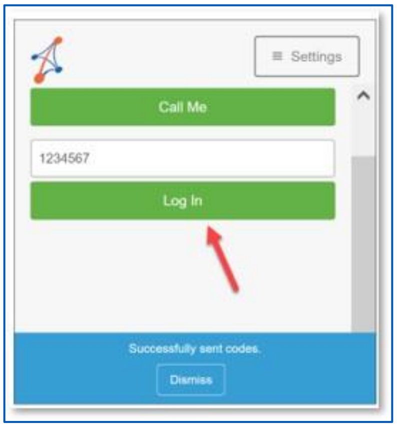
Step	Action
6.	Scroll down until you see the **When I log in** dropdown box.  SMS and Voice ≡ Settings NEW + Add another device Saved Continue to Login Change Security Factor Default Device: Generic Smartphone 615-577-1900 When I log in: Ask me to choose an authentication method
7.	a. Select one of the following options: • Ask me to choose an authentication method (every time I log in). • Default to the Primary Factor (**Recommended**). b. Click **Continue to Login**.
8.	Select **Text me new codes**.  SMS and Voice ≡ Settings ex. 867539 Log In Dismiss Text me new codes Change Security Factor Enter a passcode from a text.

Continued on next page

Section 4: SMS and Voice (continued)

Back to Contents

Follow the steps below to setup SMS/text messaging as a second authentication factor.

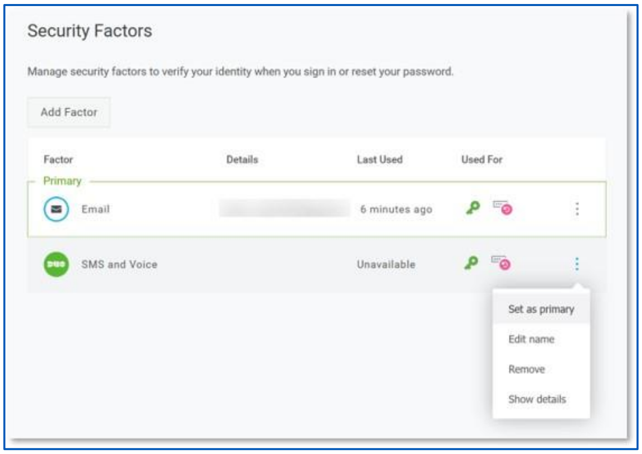
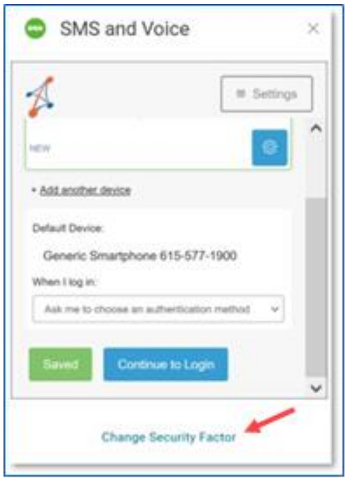
Step	Action
9.	The message in the blue box will change to **Successfully sent codes** and you will receive a text message.  SMS Passcodes: 1234567
10.	Enter the code and select **Log In**.  ≡ Settings Call Me 1234567 Log In Successfully sent codes. Dismiss

Continued on next page

Multi-Factor Authentication

Section 5: Setting a Primary Factor

Back to Contents

Step	Action
1.	**Optional:** To change your primary authentication mode, hover your mouse over the ellipsis (3 dots) on the far right of the table to display the dropdown menu.  Security Factors Manage security factors to verify your identity when you sign in or reset your password. Add Factor Factor | Details | Last Used | Used For Primary Email | [redacted] | 6 minutes ago | SMS and Voice | | Unavailable | **NOTE:** If you have setup SMS and Voice as your primary factor but your phone is not at hand (e.g., lost, mis-placed), begin logging in as usual, but when the MFA screen appears, select **Change Authentication Factor** at the bottom of the screen. A screen will appear which will allow you to select Email as the primary authentication factor.  SMS and Voice Default Device: Generic Smartphone 615-577-1900 When I log in: Ask me to choose an authentication method Settings NEW + Add another device Saved Continue to Login Change Security Factor

Multi-Factor Authentication

Q1 What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application or online account.

The first factor is something the user knows, such as their username and password. The second factor is something the user has in their possession which is unique to them, such as a onetime password which is sent via email or text.

You've probably already experienced this without even noticing it or thinking about it – almost any time a bank or website sends you an email or text message with a code to be entered into a pop-up window – it's MFA.

Q2 Why is naviHealth taking this step?

At naviHealth, we take the protection of data seriously. Cyber criminals are increasingly using advanced techniques to access critical and sensitive business information. The growth of remote work, multiple devices, and public network access increases the risk of unwanted intrusion and disruption to business activity. MFA is one of the easiest, most effective tools for enhancing login security, and safeguarding data against security threats.

Q3 Who is impacted by this change?

All naviHealth platform users will be required to complete this two-step process.

Q4 How will it work?

The main login screen will remain the same with the addition of a verification step of entering a code received by email, text message or phone call.

Q5 What if I have additional questions?

For any issues or questions, please contact the **nH Coordinate** or **nH Access** support team.