



Multi-Factor Authentication User Guide



Table of Contents

Document Overview	3
Scope	3
Purpose	3
Registration for Multi-Factor Authentication	4
Registration for Oracle Mobile Authenticator	6
User Log-in Using One-Time Access Code From Email	9
User Log-in Using One-Time Access Code From Oracle Mobile Authenticator	12
Using the Resend Option	15
Self Service—Remove Oracle Mobile Authenticator	19
Self Service—Update Email Account	23

Document Overview

Scope

The scope of this Multi-Factor Authentication (MFA) User Guide is to provide in-depth information to the end user on the MNsure application's multi-factor authentication solution. Multi-factor authentication is a security mechanism used by applications requiring an increased level of security. Generally, authentication security is broken down into three categories: something you know (password, pin); something you have (hard token, badge, ATM cards); something you are (fingerprint, other biometric). This standard mandates the use of two or more of the above authentication mechanisms to gain access to a system.

This document includes the following major components of the multi-factor authentication functionality:

- I. Registration
- II. Registration for Oracle Mobile Authenticator
- III. User log-in using access code from email
- IV. User log-in using access code from Oracle Mobile Authenticator
- V. Using resend access code option
- VI. Self service remove Oracle Mobile Authenticator
- VII. Self service update email account

Purpose

The purpose of this document is to provide information and step-by-step instructions so that end users can use multi-factor authentication security to access MNsure. This solution will support the use of a one time access code delivered to users via email or the Oracle Mobile Authenticator application.

Registration for Multi-Factor Authentication

After signing in the user will be redirected to the MFA registration page if they have opted themselves in to the MFA solution (consumers only) or if they are required to use the MFA solution (administrators).

- a) Multi-factor authentication registration page is displayed.
- b) Enter a valid email account.
- c) Accept the terms and conditions by clicking on “I Agree”.
- d) Click “Submit”.

MNsure offers the highest level of security for protecting consumer information. Multi-factor authentication is an additional layer of security to ensure that MNsure information remains secure and protected from fraud and identity theft.

This is an important tool for managing security and preventing unauthorized access to state systems.

You will now be required to sign in to your account by entering your one-time access code, which is sent via email each time you sign in to MNsure. You will have an opportunity to update the email address associated with your account through the following registration process.

Please ensure that the email address listed below is correct, or update it if you would like to receive your one-time access code at a different email address. Please complete your registration below by agreeing to the terms and conditions before submitting your information.

Email*

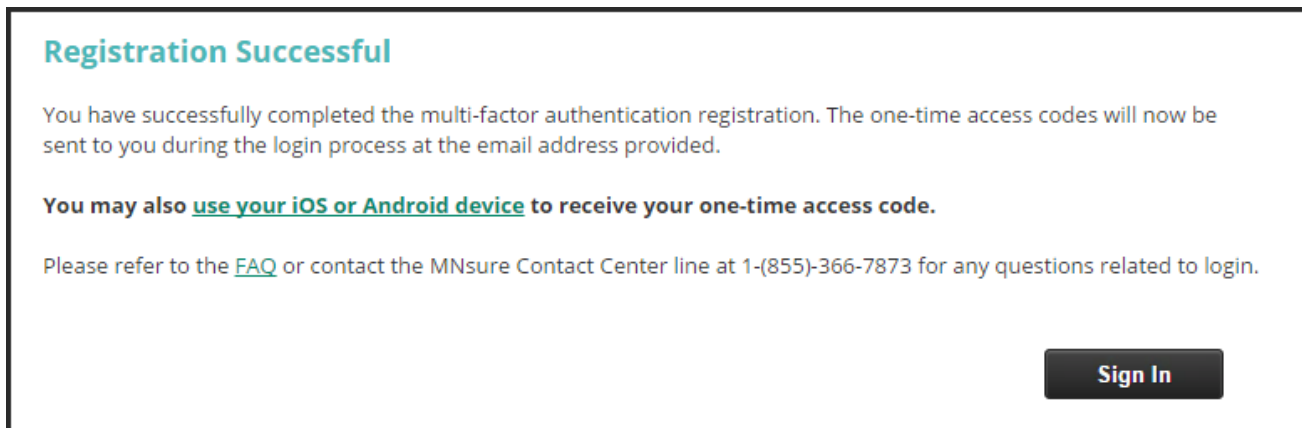
Terms and Conditions.
The MNsure system is the property of the State of Minnesota and is subject to the Minnesota Government Data Practices Act. By using this system, you are representing yourself as an authorized user, and as such, you agree to use the system for authorized purposes only and in compliance with state and federal law. Users of the system who have the ability to see the personal information of participants, including state employees, contractors, community assistance partners, and other system users, must adhere to rules of behavior for protection of private participant information as defined in the [MNsure Privacy Policy](#). These rules are consistent with and in addition to state and federal laws and the privacy and security policies and procedures for MNsure, including the Minnesota Department of Human Services (DHS) Information and Technology Policies and Procedures, and the Appropriate Use of Electronic Communication and Technology Policy (applicable only to state employee users). Non-compliance with the rules and associated security policies may be cause for disciplinary actions including suspension and/or termination of access privileges, employment consequences, and/or civil and criminal legal action.

Enrollment in multi-factor authentication requires validation of the user credentials as well as providing an accurate email address

I Agree that I have read and accepted the terms and conditions. The information provided is accurate to the best of my knowledge *

****Please note that access code will be sent to this email address.***

- e) Once the user clicks submit, a registration successful message will be displayed as shown in the screenshot below.



This completes the registration for multi-factor authentication. Once the user is successfully registered, the user can proceed to log in.

Registration for Oracle Mobile Authenticator

After registering for MFA a user can then register their Android or Apple device to receive one time access codes through the Oracle Mobile Authenticator (OMA) application.

- a) Navigate to www.mnsure.org/mfa/oma-registration-instructions.jsp on your computer. This will display the following steps:
- b) Download the Oracle Mobile Authenticator (OMA) application for Android or Apple using the appropriate links below.



**Android Google Play
QR Code**

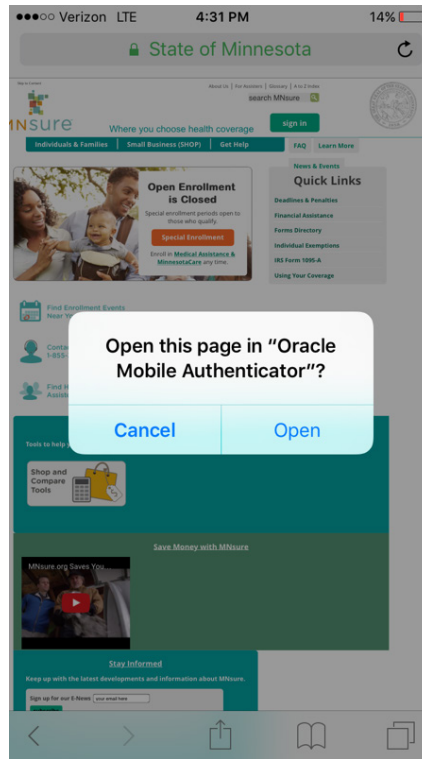


**Apple iOS
QR Code**

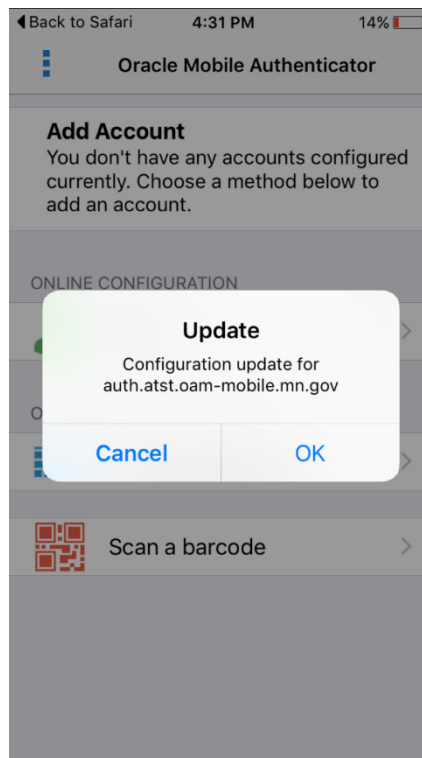
- c) After the OMA download and installation is complete, please navigate to <https://www.mnsure.org/mfa/oma.jsp> on your mobile device using an internet browser, or scan the QR code below.



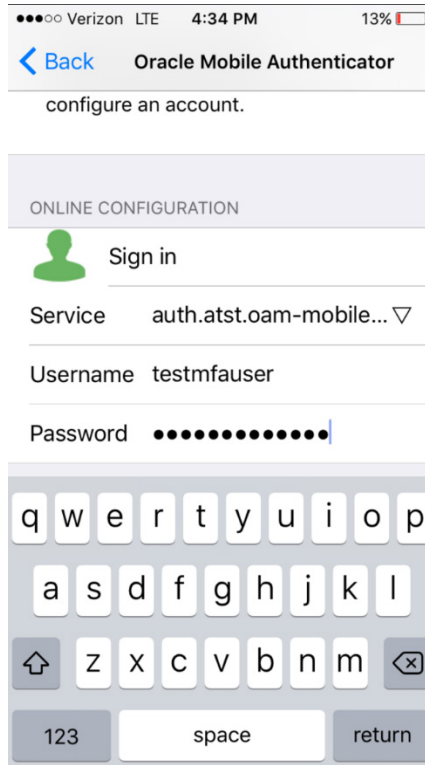
- d) Apple devices may ask if they may open the OMA application. Allow the phone to open the OMA application.



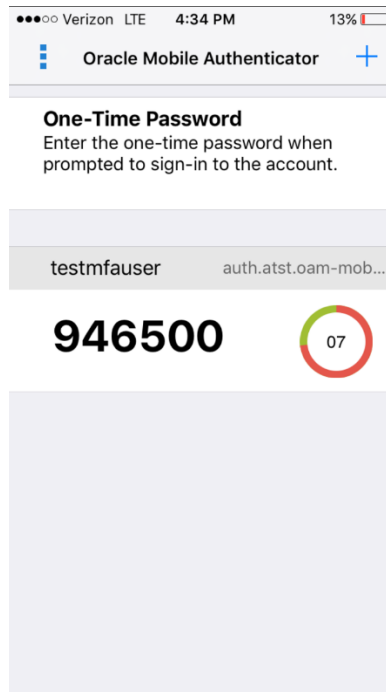
- e) Your device will ask if it can update your OMA application settings. Please allow your device to update the OMA application settings.



- f) Log in to the OMA application by providing your MNsure username and password.

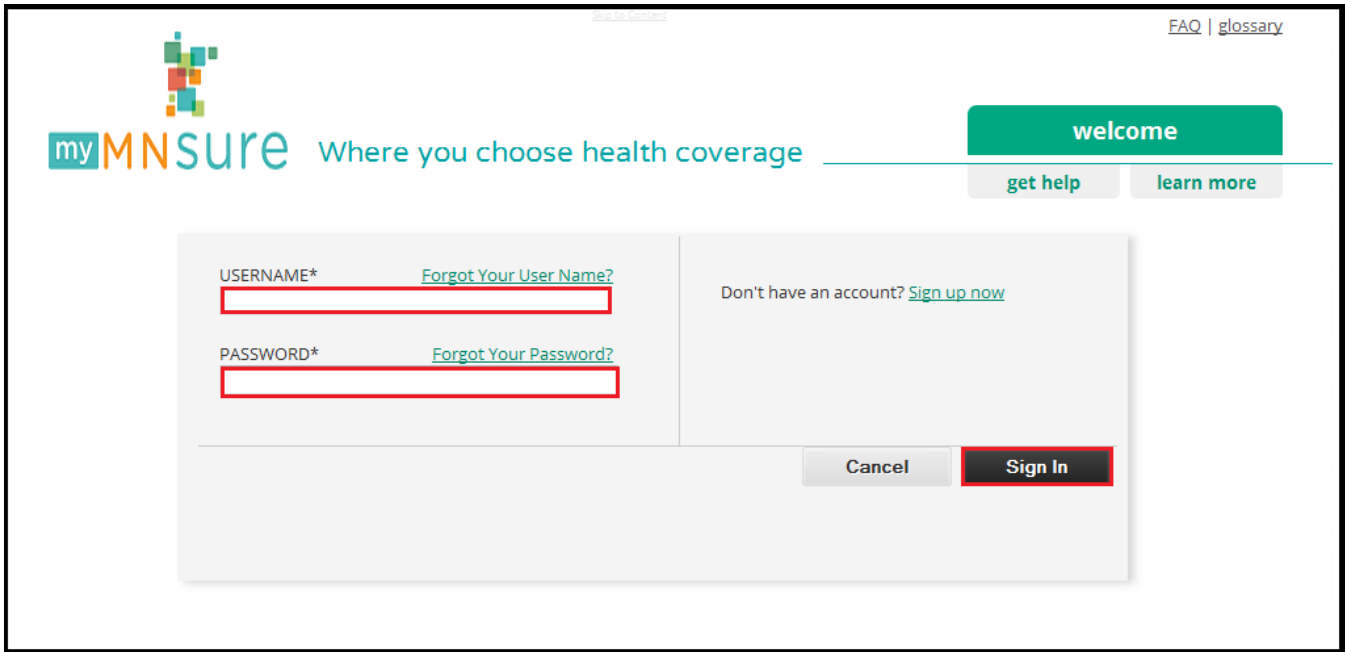


- g) You are now successfully registered for use of the Oracle Mobile Authenticator application. The next time you log in you will be presented with the delivery option for your one-time access code.

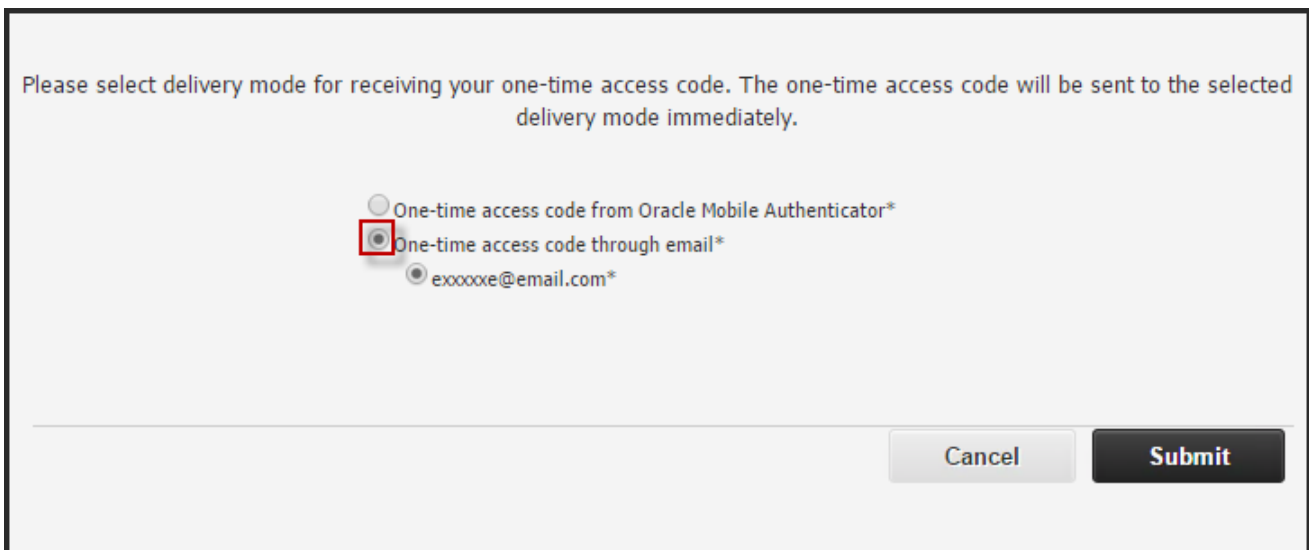


User Log-in Using One-Time Access Code From Email

- a) Navigate to the MNsure sign-in page.
- b) Enter username and password.
- c) Click on “Sign In” button as shown in the screenshot below.



- d) Radio button for selection of email will be displayed on the next screen.
- e) Select “One Time access code through Email” Radio Button as displayed in the screenshot



- f) Click on the partially hashed email account where the one-time access code will be sent.

Please select delivery mode for receiving your one-time access code. The one-time access code will be sent to the selected delivery mode immediately.

One-time access code from Oracle Mobile Authenticator*

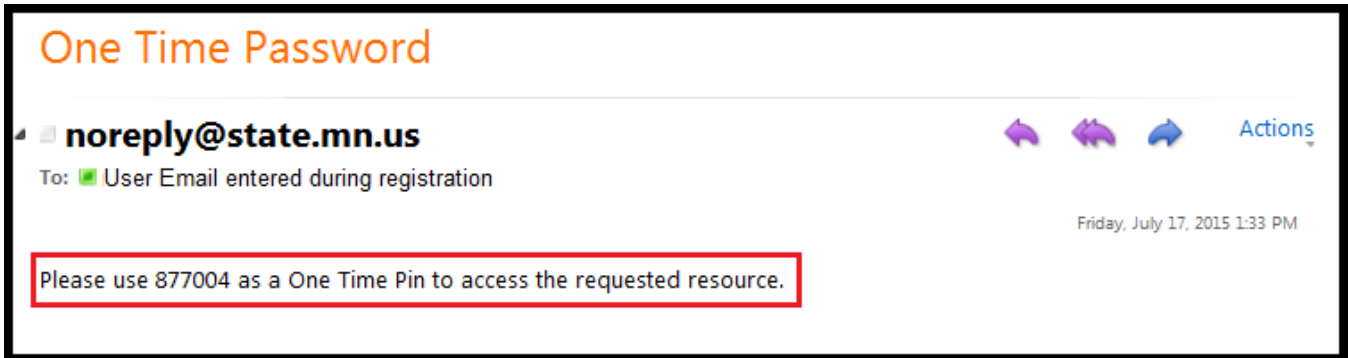
One-time access code through email*

exxxxxe@email.com*

g) Click on "Submit". The user will be redirected to enter the one-time access code.

****Once the user clicks submit the one time access code will be sent to the user's email account and the application will redirect the user to the next page as shown in step (i) below.***

h) Sign in to the email account which was used for registration and check the email for the one-time code.



- i) Enter the one-time access code that you have received in the email.
- j) Click on “Submit” Button.

Please do not close this browser. You are required to enter the one-time access code on this page.

Your one-time access code has been sent to you via the delivery mode selected. Please enter your one-time access code below.

Enter your one-time access code*:

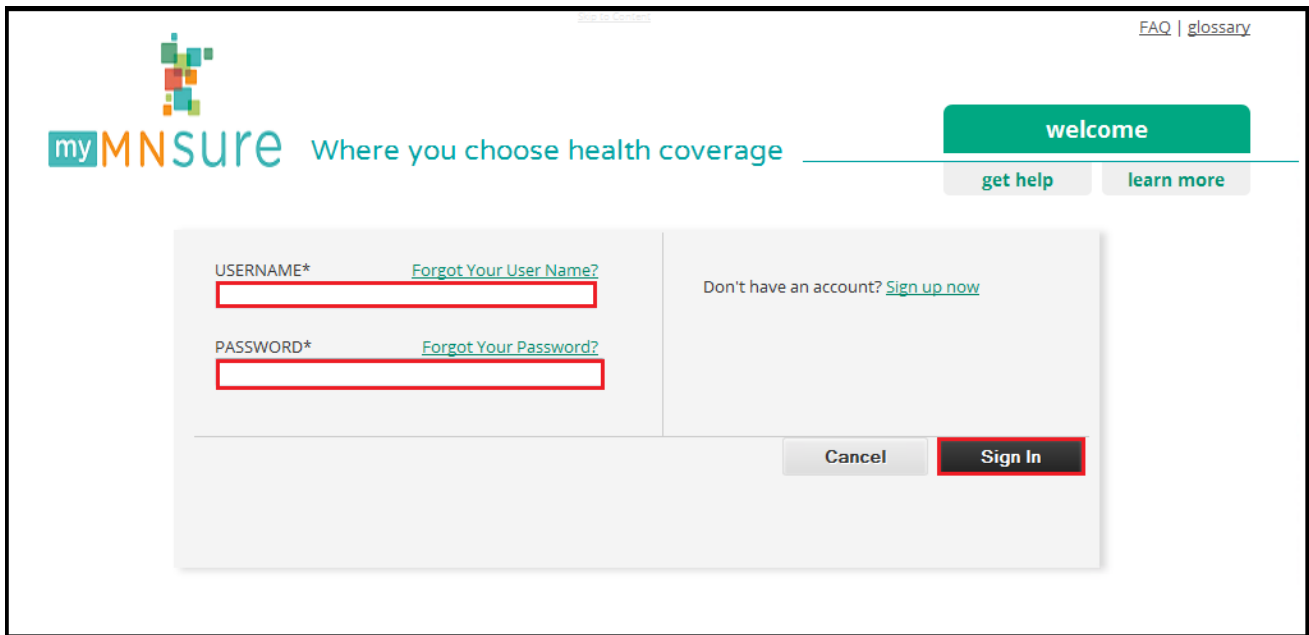
Cancel Resend **Submit**

- k) The user will be successfully logged in.

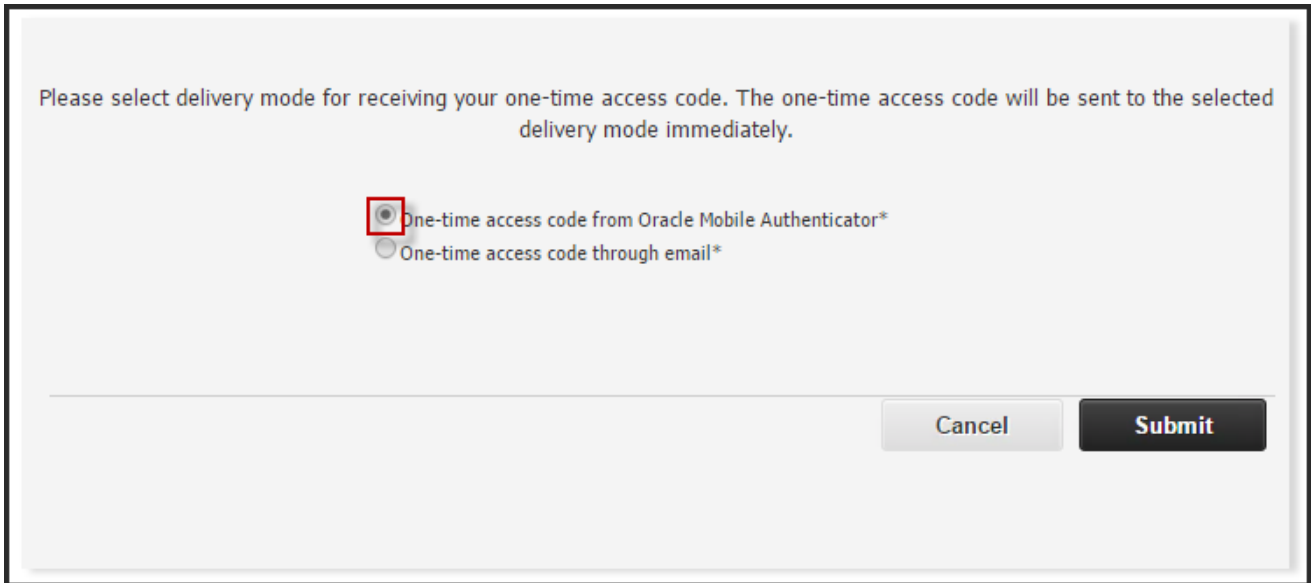
User Log-in Using One-Time Access Code From Oracle Mobile Authenticator

Before a user can use the Oracle Mobile Authenticator solution they must first register for Multi-Factor Authentication and follow the setup steps found on the [Oracle Mobile Authenticator Registration Instructions](#) page.

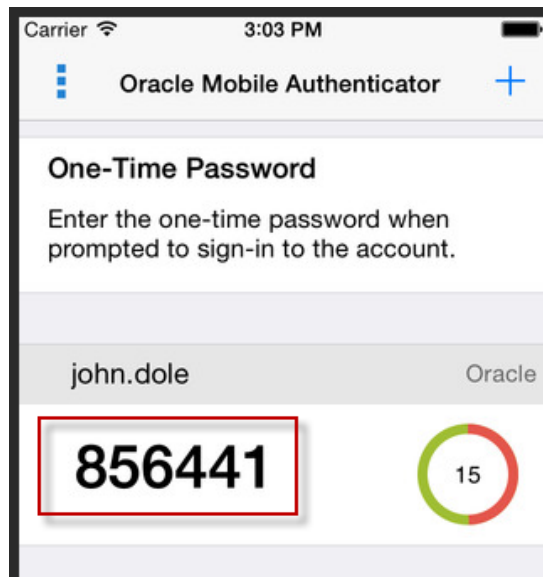
- a) Navigate to the MNsure sign-in page.
- b) Enter username and password.
- c) Click on “Sign In” button as shown in the screenshot below.



- d) Select “One time access code from Oracle Mobile Authenticator” radio button as displayed in the screenshot and click Submit.



- e) Open the Oracle Mobile Authenticator application on your registered device.
- f) Enter the one-time access code displayed in the Oracle Mobile Authenticator app.



- g) Click on the “Submit” button.

Please do not close this browser. You are required to enter the one-time access code on this page.

Your one-time access code has been sent to you via the delivery mode selected. Please enter your one-time access code below.

Enter your one-time access code*:

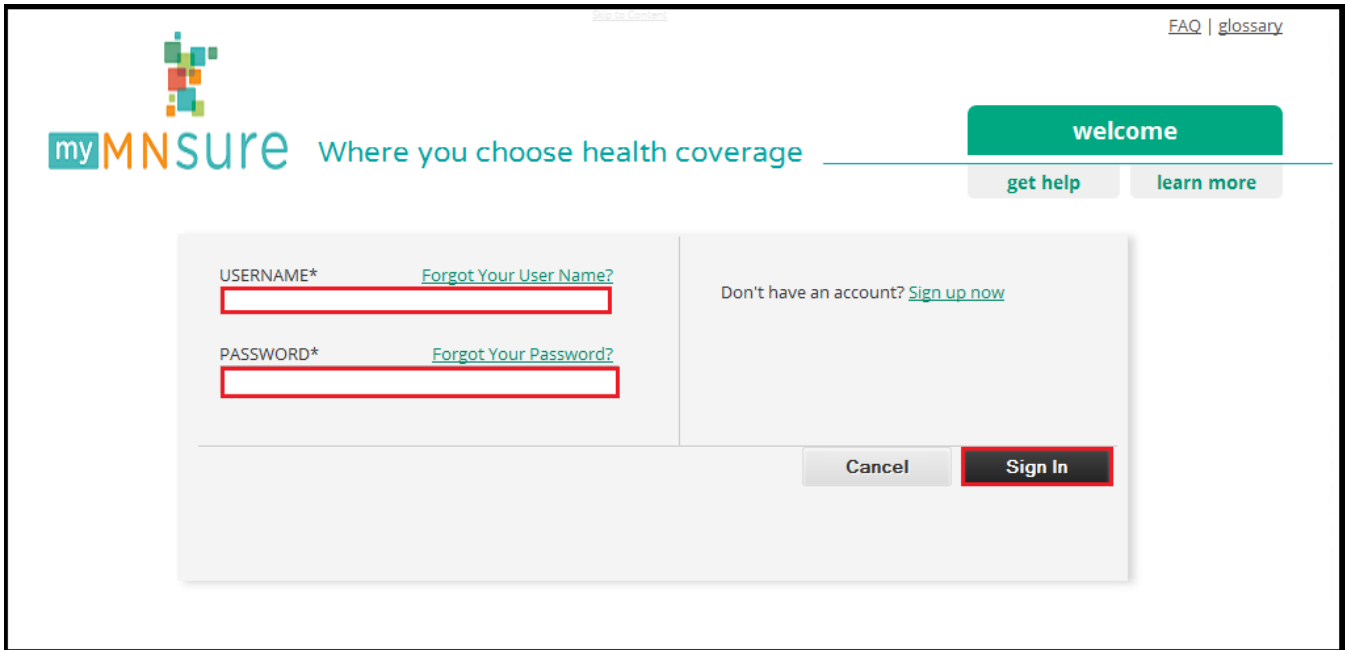
Cancel Resend **Submit**

h) The user will be successfully logged in.

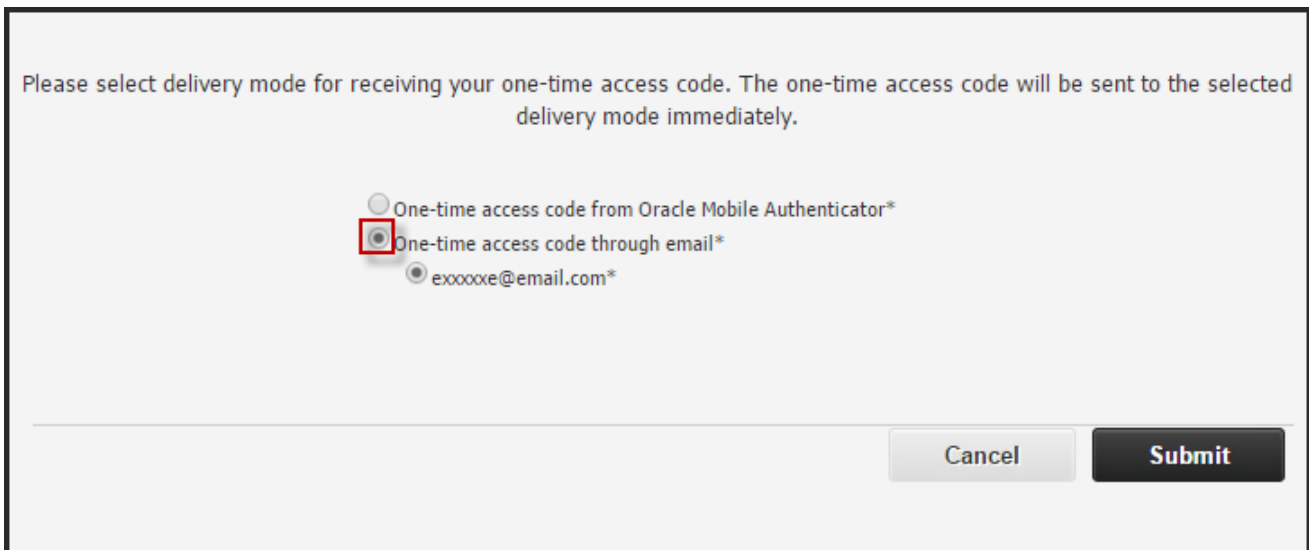
Using the Resend Option

If a user decides they want to resend a new one time access code or select a different delivery method they can use the Resend option.

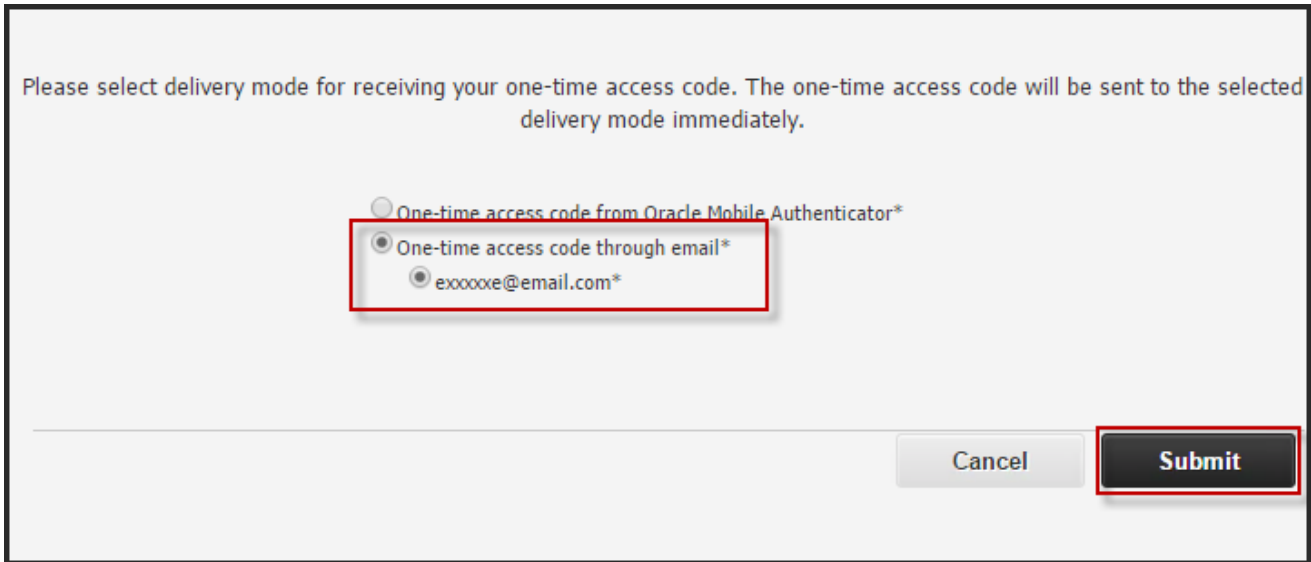
- a) Navigate to the MNSure sign-in page.
- b) Enter username and password.
- c) Click on “Sign In” button as shown in the screenshot below.



- d) Radio button for selection of email will be displayed on the next screen.
- e) Select “One time access code through Email” radio button as displayed in the screenshot.



f) Click on the email account where the one time access code will be sent.

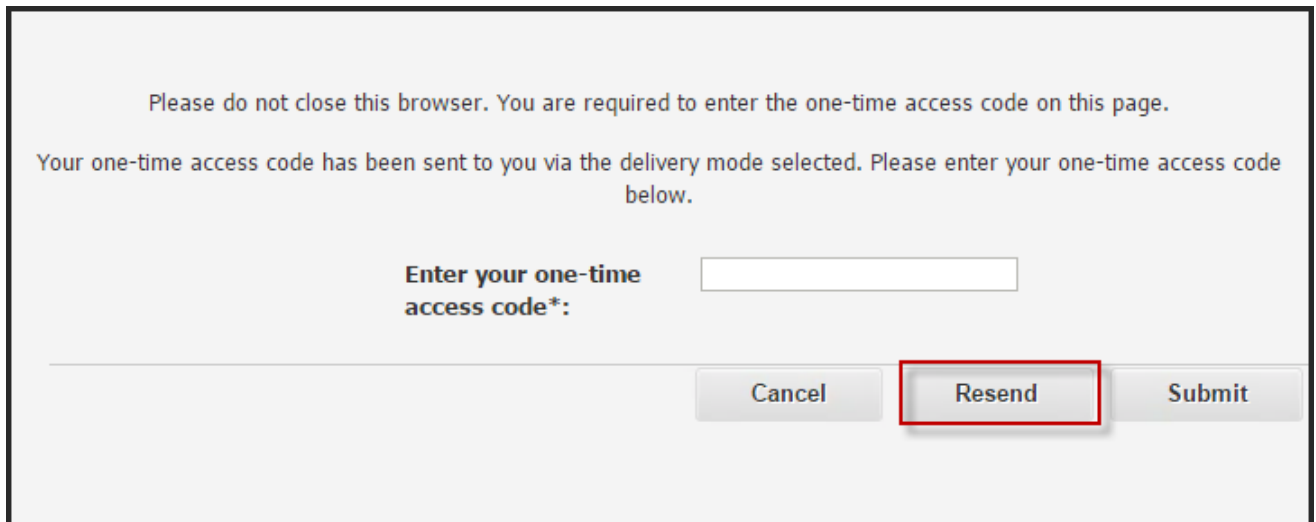


g) Click on "Submit". The user will be redirected to enter the one-time access code.

****Once the user clicks submit the one-time access code will be sent to the user's email account and the application will redirect the user to the next page.***

If required, the user can receive a new one-time access code by using the "Resend" button.

h) Click on Resend OTP button, as shown in screenshot below. This will take you back to the mode selection page.



i) Radio button for selection of email will be displayed on the next screen.

- j) Select the “one-time access code through Email” radio button as displayed in the screenshot.

Please select delivery mode for receiving your one-time access code. The one-time access code will be sent to the selected delivery mode immediately.

One-time access code from Oracle Mobile Authenticator*

One-time access code through email*

exxxxxe@email.com*

Cancel Submit

- k) Click on the email address where the one-time access code will be sent.

Please select delivery mode for receiving your one-time access code. The one-time access code will be sent to the selected delivery mode immediately.

One-time access code from Oracle Mobile Authenticator*

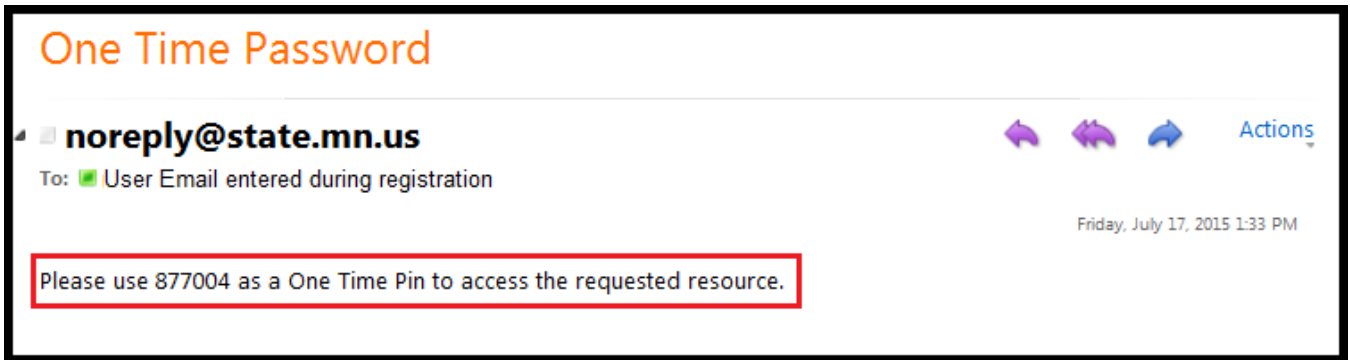
One-time access code through email*

exxxxxe@email.com*

Cancel Submit

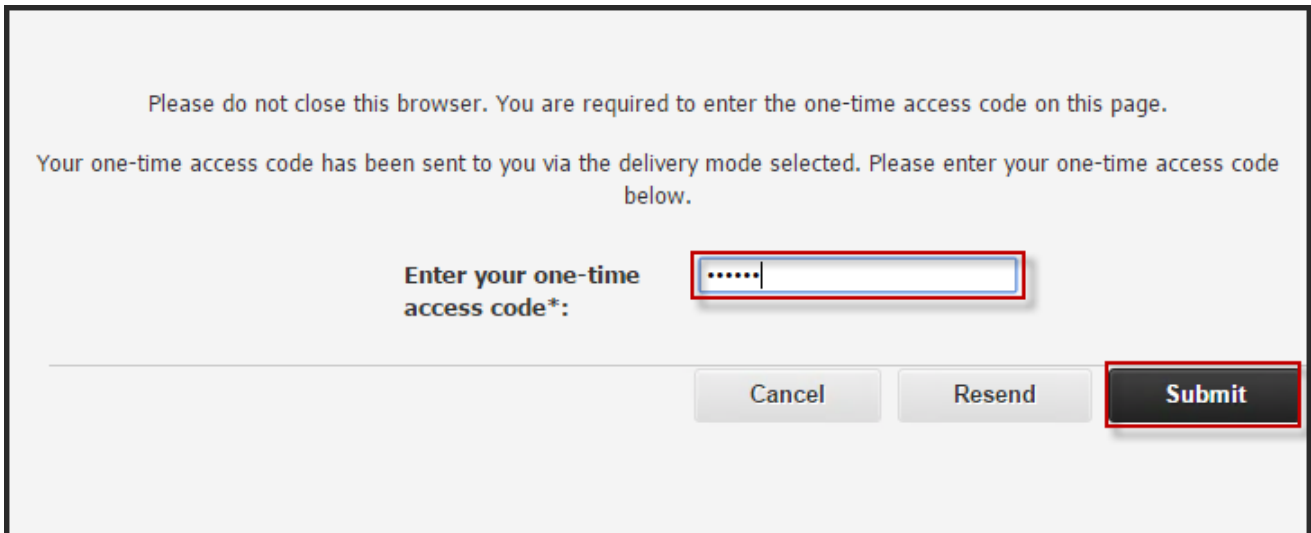
- l) Click on “Submit”. The user will be redirected to enter the one-time access code.

m) Sign in to the email account which was used for registration and check the email for the one-time access code.



n) Enter the one-time access code that you have received in the email.

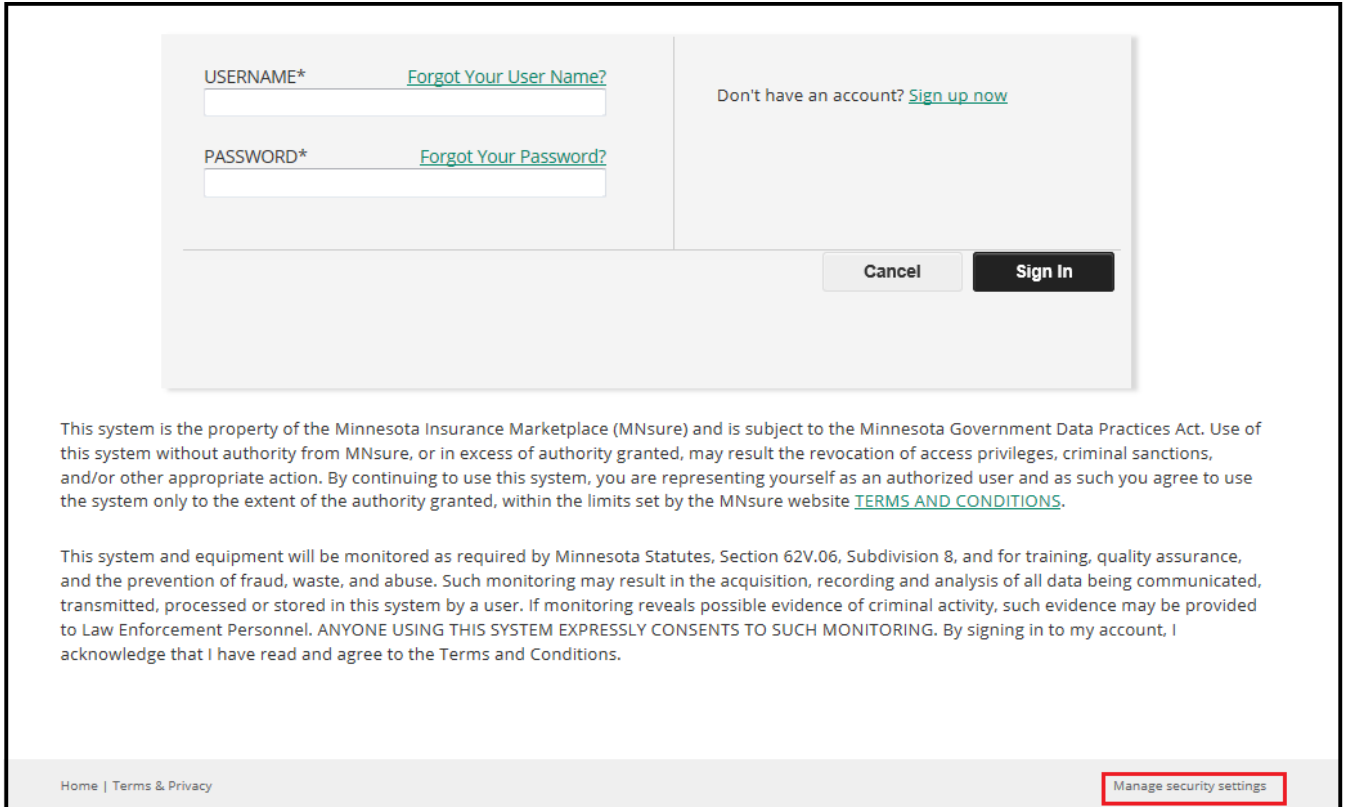
o) Click on the "Submit" button.



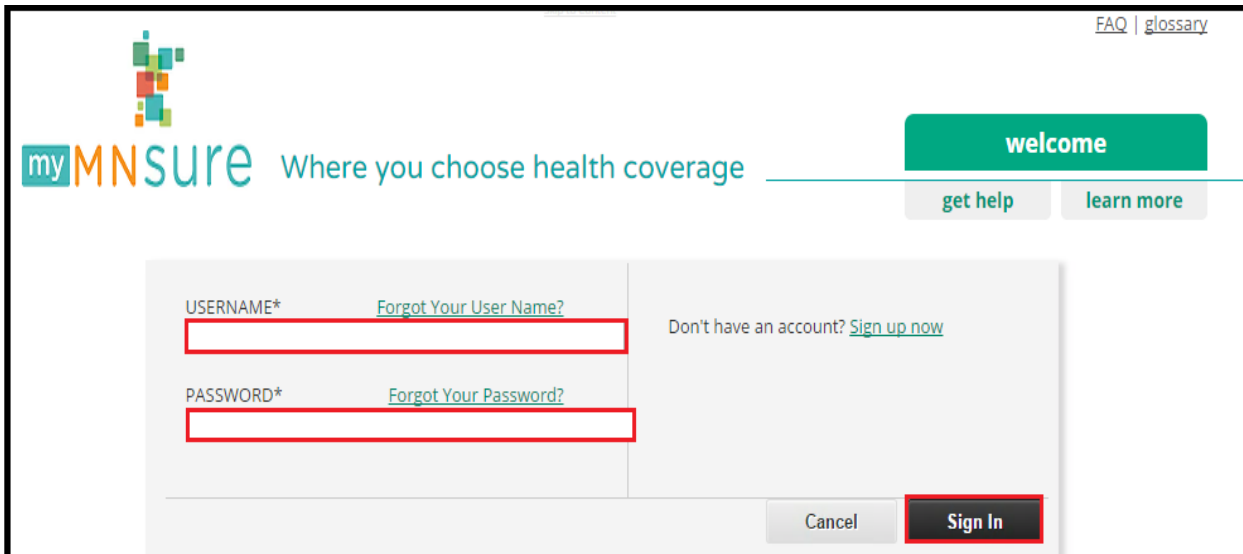
p) The user will be successfully logged in.

Self Service—Remove Oracle Mobile Authenticator

- a) Navigate to the MNsure sign-in page.
- b) Click on the Manage Security Link at the bottom of the page as shown below in the screenshot.

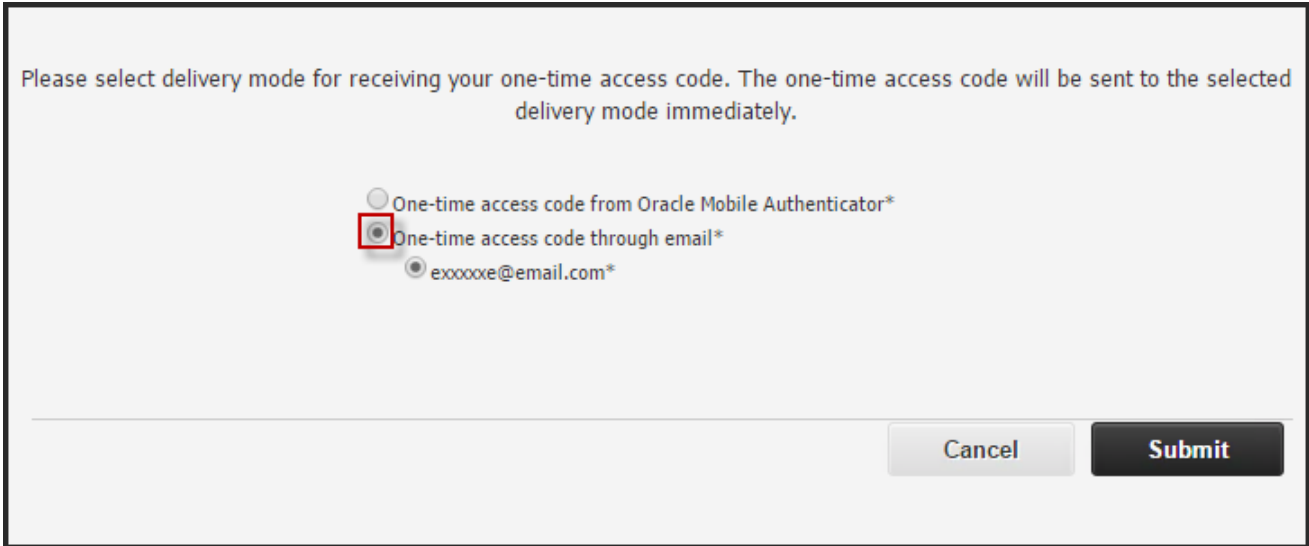


- c) Enter username and password.

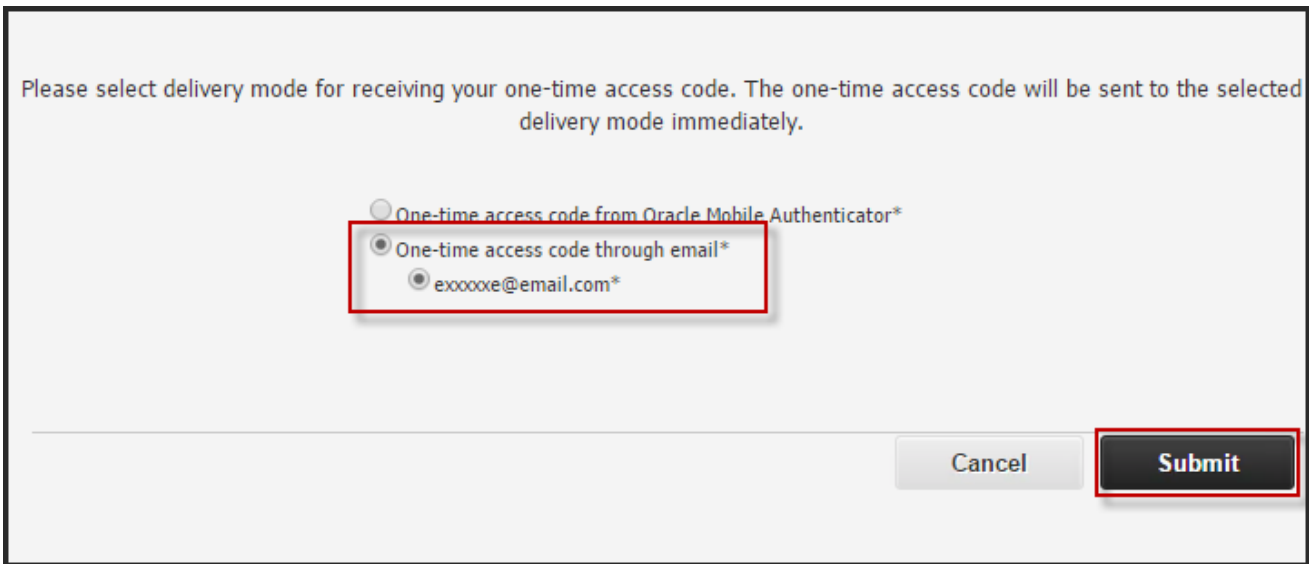


- d) Radio button for selection of email will be displayed on the next screen.

e) Select the “one-time access code through Email” radio button as displayed in the screenshot.



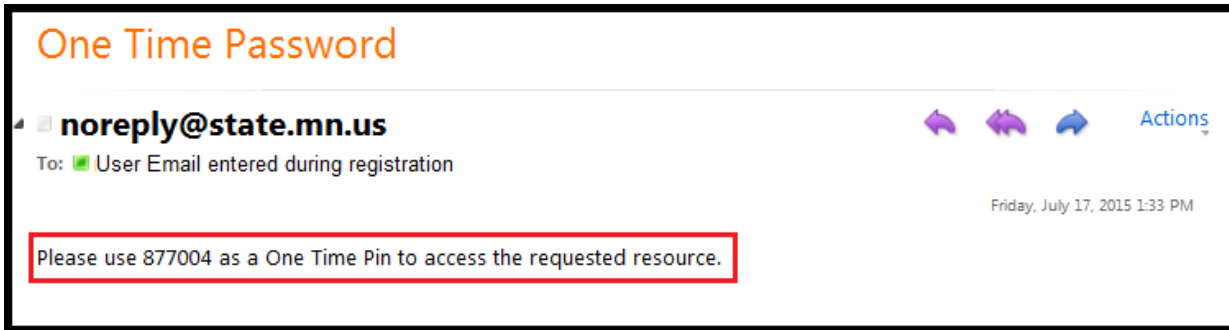
f) Click on the email account where the one-time access code will be sent.



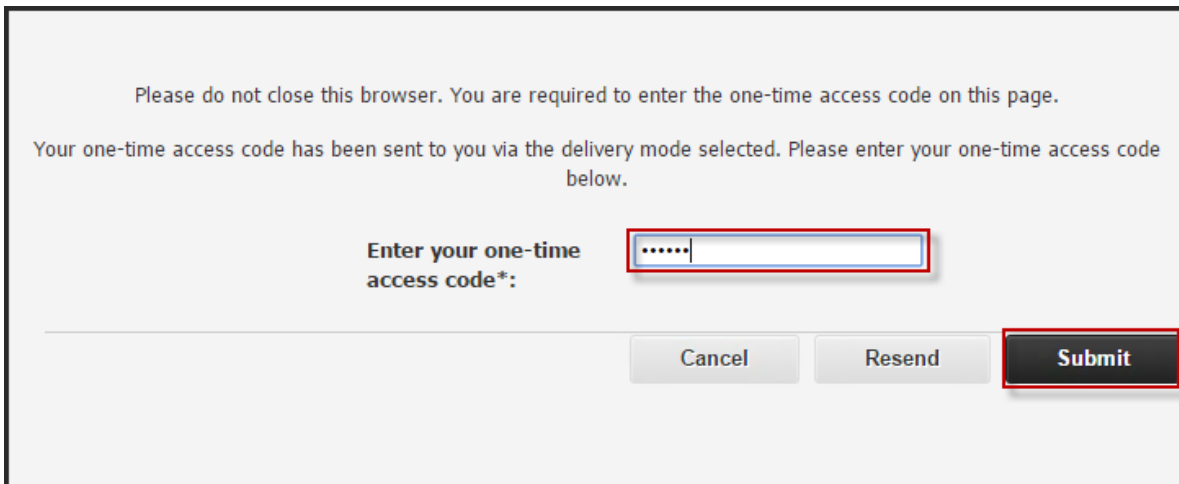
g) Click on “Submit”. The user will be redirected to enter the one-time access code.

****Once the user clicks submit the one-time access code will be sent to the user’s email account and the application will redirect the user to the next page as shown in step (j) below.***

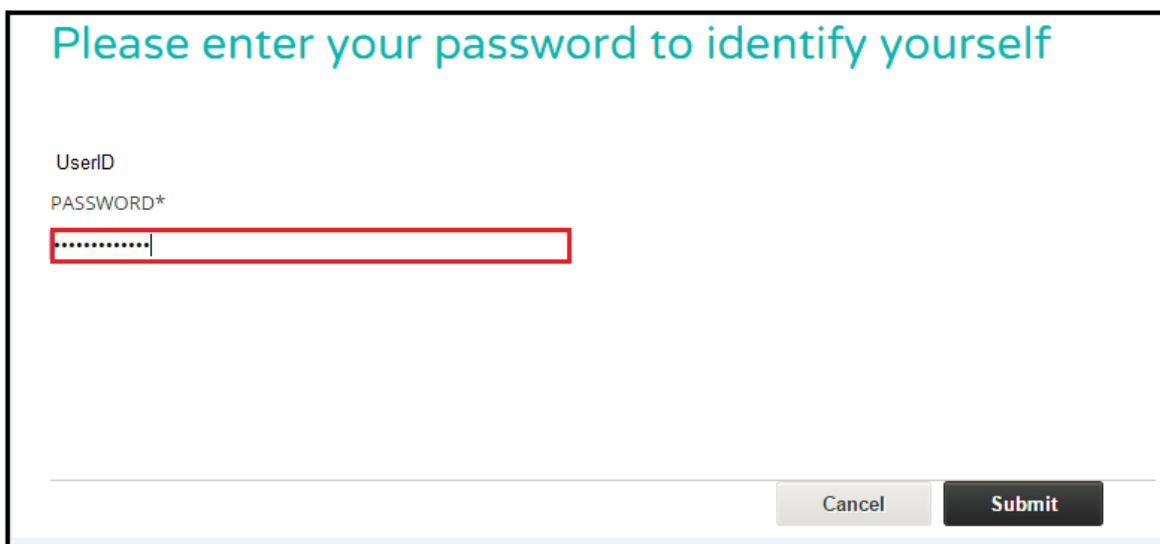
- h) Sign in to the email account which was used for registration and check the email for the one-time access code.



- i) Enter the one-time access code that you have received in the email.
- j) Click on the "Submit" button.



- k) Re-enter your password.



- l) Click on the "Change multi-factor settings" tab at the top.

[Change contact information](#) | [Change password](#) | [Change security questions & answers](#) | [Change multi-factor settings](#)

Change contact information

Your email address, phone number, or shared secret can be changed here. This email address will receive notifications related to your MNsure login account. Your email can also receive one-time

m) To remove Oracle Mobile Authenticator from your account click where instructed on the page.

You are currently registered to use Oracle Mobile Authenticator for delivery of your one-time access code to your mobile device. To remove the use of Oracle Mobile Authenticator from your account please [click here](#).

n) Click on “Remove Device” to un-link your device from your account. You will no longer be able to receive one-time access codes on your device through the Oracle Mobile Authenticator application.

You are currently using the Oracle Mobile Authenticator to deliver one time access codes to your smartphone. If you chose to remove this device from your account you will no longer be able to receive one time access codes via the Oracle Mobile Authenticator app unless you re-register your device.

Are you sure that you wish to remove this device from your account?

o) The user will be presented with a success page informing them that Oracle Mobile Authenticator has been removed.

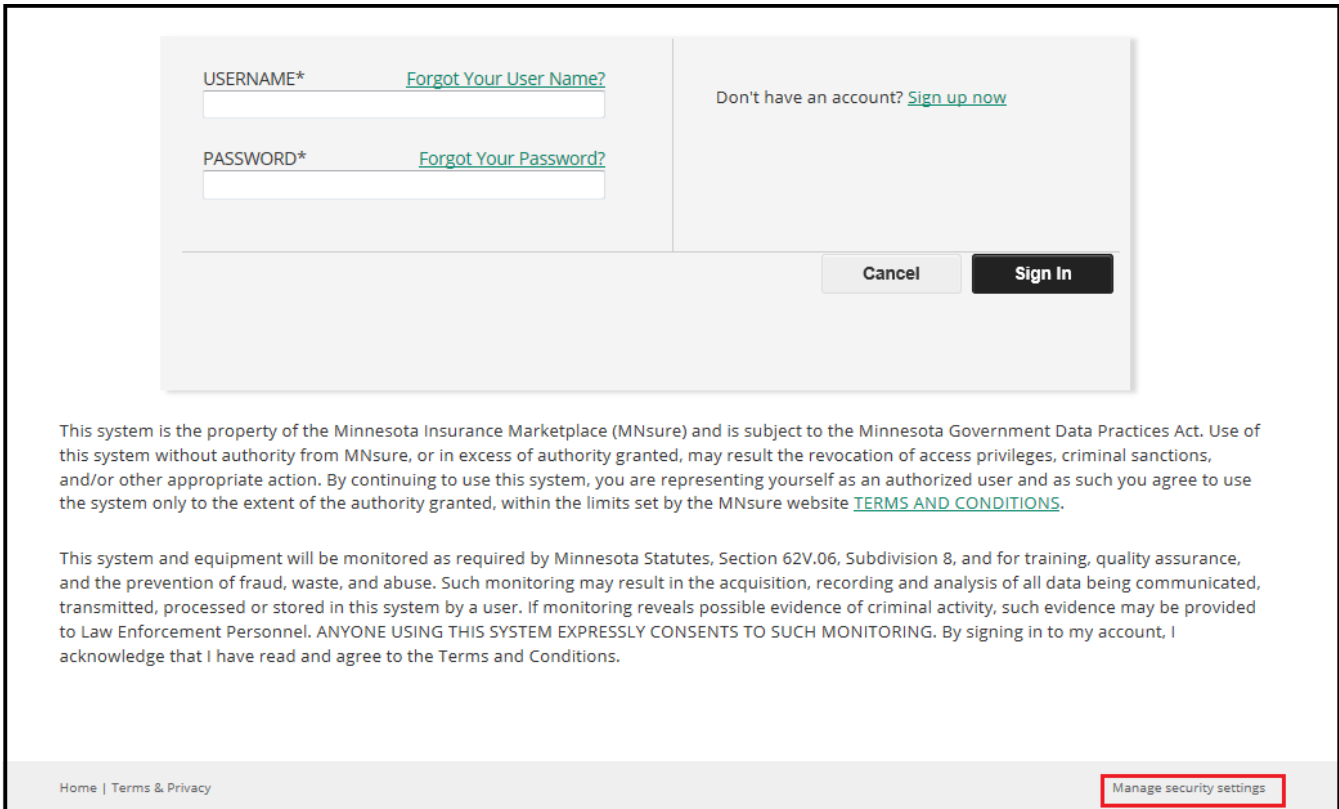
Oracle Mobile Authenticator has been removed

You have successfully unregistered Oracle Mobile Authenticator from your account.
You will no longer be able to deliver one-time access codes via Oracle Mobile Authenticator.

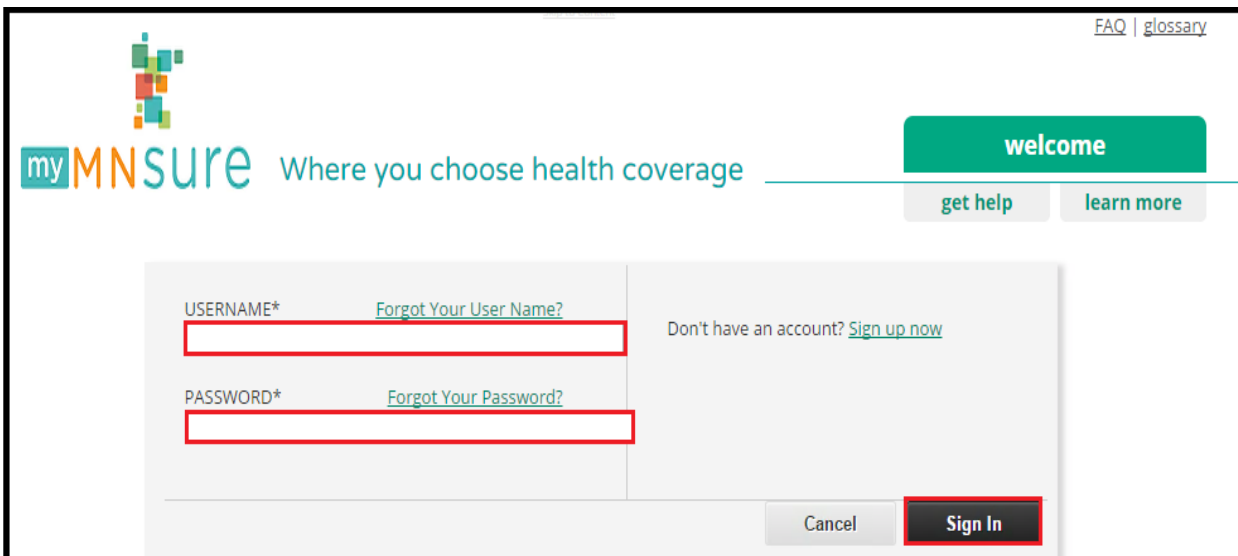
p) We strongly suggest removing the account from inside the Oracle Mobile Authenticator application on your device. To do this you must tap and hold the account inside the application until the ribbon at the top is displayed. From there you can click on the trash can icon to remove the account from the Oracle Mobile Authenticator application.

Self Service—Update Email Account

- a) Navigate to the MNsure sign-in page.
- b) Click on the Manage Security Link at the bottom of the page as shown below in the screenshot.

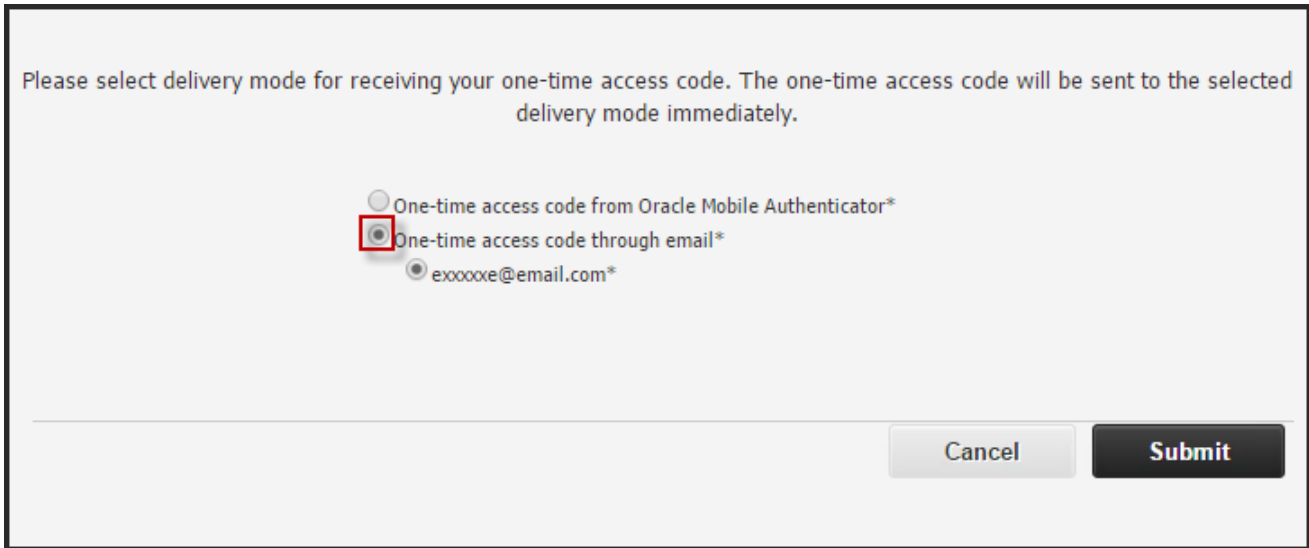


- c) Enter username and password.

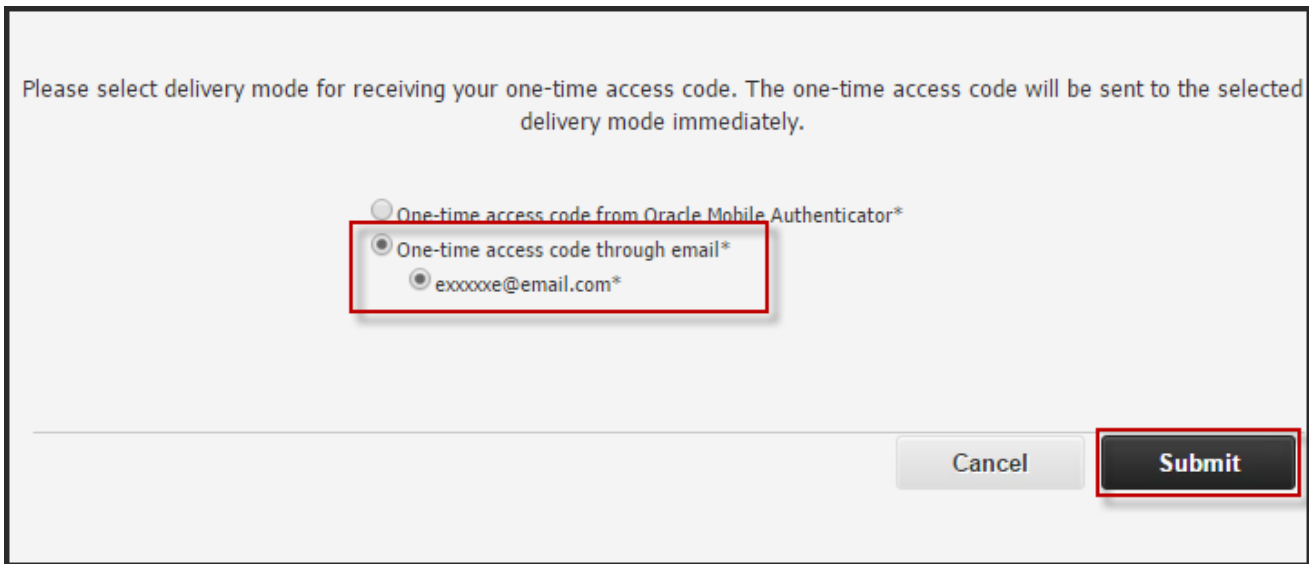


- d) Radio button for selection of email will be displayed on the next screen.

e) Select the “one-time access code through Email” radio button as displayed in the screenshot.



f) Click on the email account where the one-time access code will be sent.



g) Click on “Submit”. The user will be redirected to enter the one-time access code.

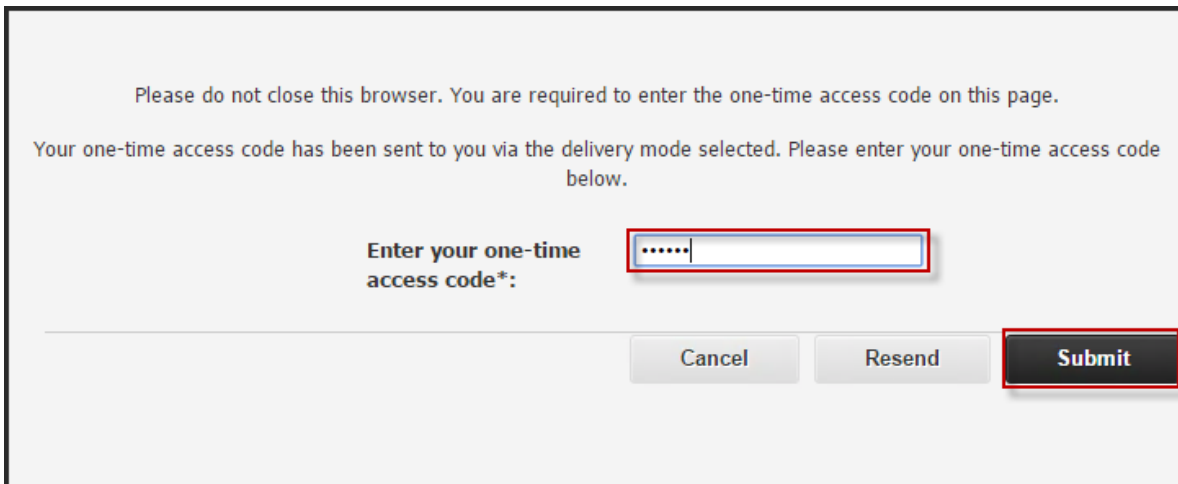
****Once the user clicks submit the one-time access code will be sent to the user’s email account and the application will redirect the user to the next page as shown in step (j) below.***

h) Sign in to the email account which was used for registration and check the email for the one-time access code.

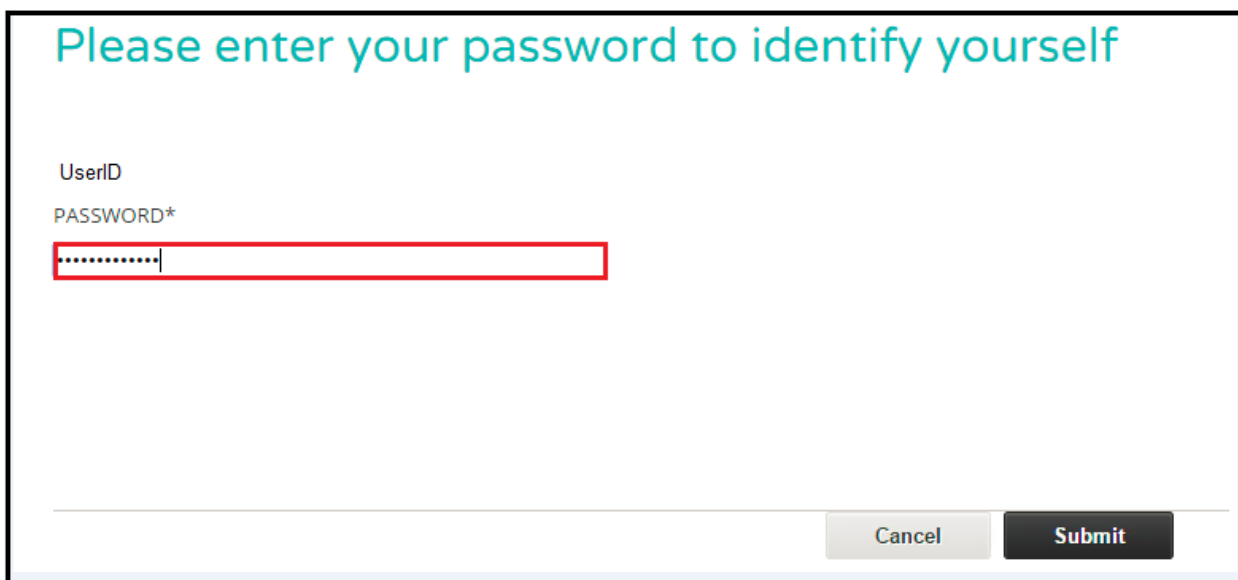


i) Enter the one-time access code that you have received in the email.

j) Click on the "Submit" button.



k) Re-enter your password.



- l) Update the email account that will be used to receive the one-time access code.

[Change contact information](#) | [Change password](#) | [Change security questions & answers](#) | [Change multi-factor settings](#)

Change contact information

Your email address, phone number, or shared secret can be changed here. This email address will receive notifications related to your MNsure login account. Your email can also receive one-time access codes if you are using multi-factor authentication. Your shared secret is used to help the contact center identify you over the phone.

EMAIL ADDRESS
new@email.com

RE-ENTER EMAIL ADDRESS
new@email.com

PHONE NUMBER (###)###-####

SHARED SECRET

[Click here for directions to set up your shared secret](#)

Apply

- m) Click on Apply.
- n) A message as shown in screenshot below appears which confirms that changes have been successfully applied.

[Change contact information](#) | [Change password](#) | [Change security questions & answers](#) | [Change multi-factor settings](#)

Manage Security Settings

Changes to your security settings have been successfully applied.

Ok

- o) The email account is successfully updated and the user will now receive the one-time access code via the updated email account.