Multi-Factor Authentication User Guide

Table of Contents

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

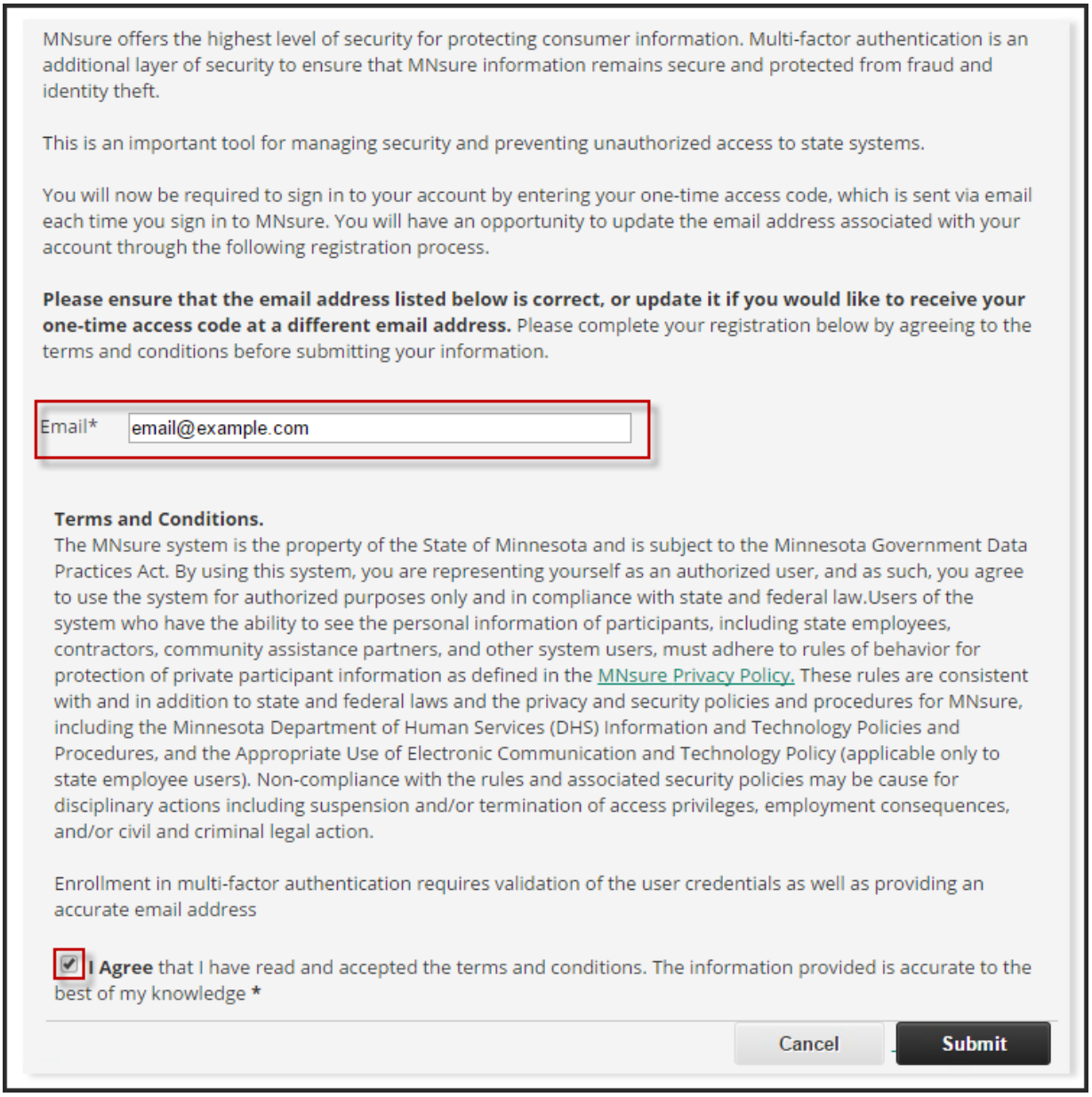
After signing in the user will be redirected to the MFA registration page if they have opted themselves in to the MFA solution (consumers only) or if they are required to use the MFA solution (administrators).

a) Multi-factor authentication registration page is displayed.

b) Enter a valid email account.

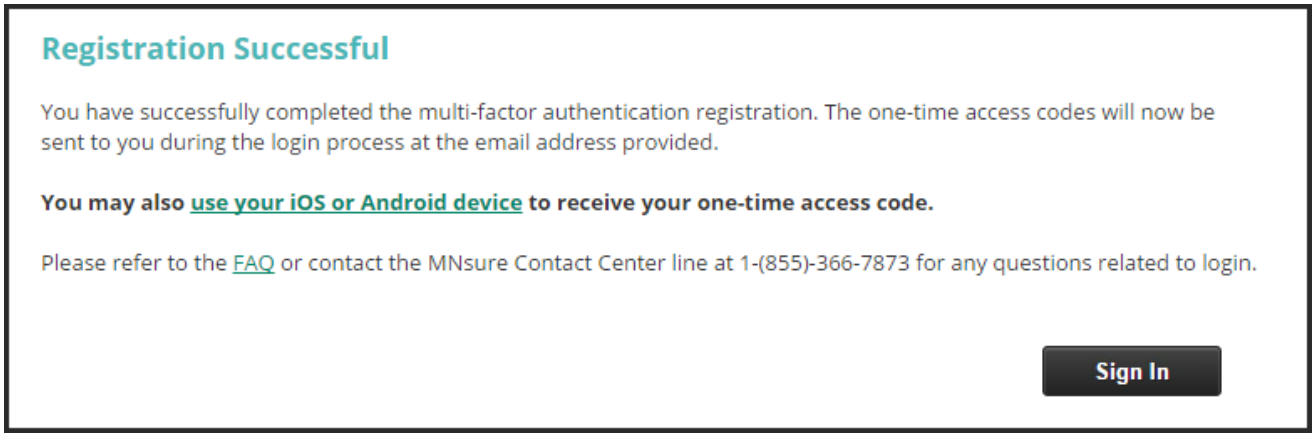
c) Accept the terms and conditions by clicking on “I Agree”.

d) Click “Submit”.



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 than 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:

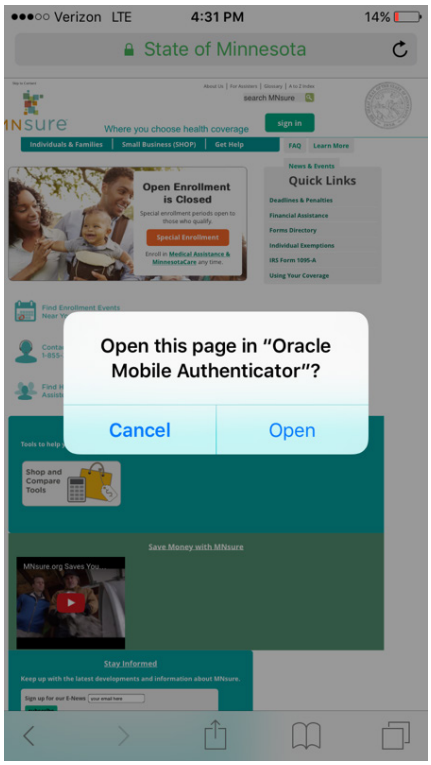
b) Download the Oracle Mobile Authenticator (OMA) application for Android or Apple using the appropriate links below.

Android Google Play QR Code

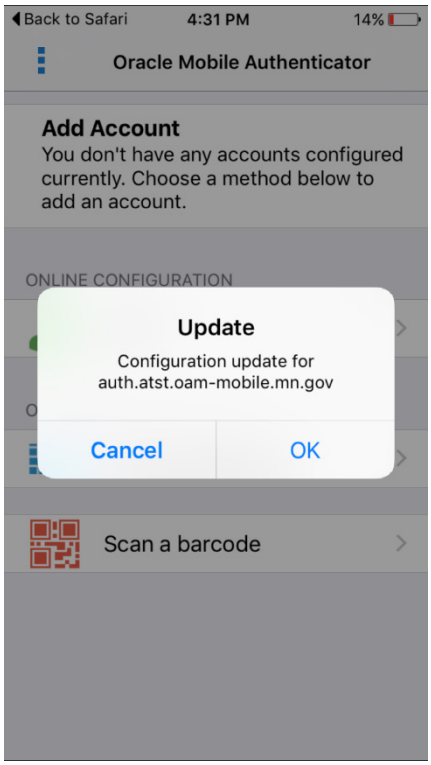
Apple iOS QR Code

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.

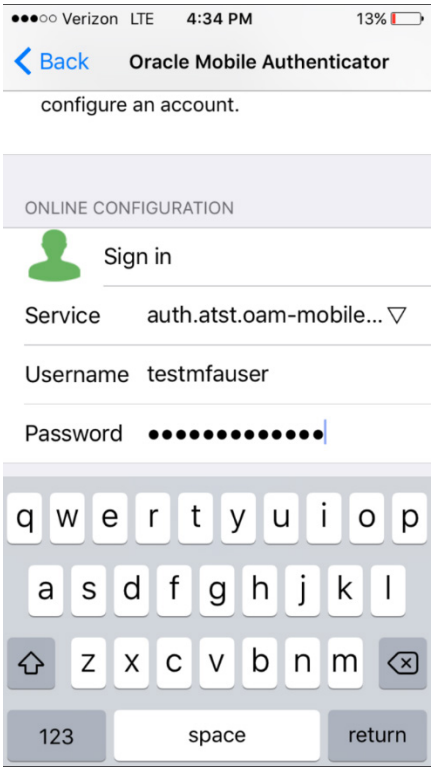
d) Apple devices may ask if they may open the OMA application. Allow the phone to open the OMA application.



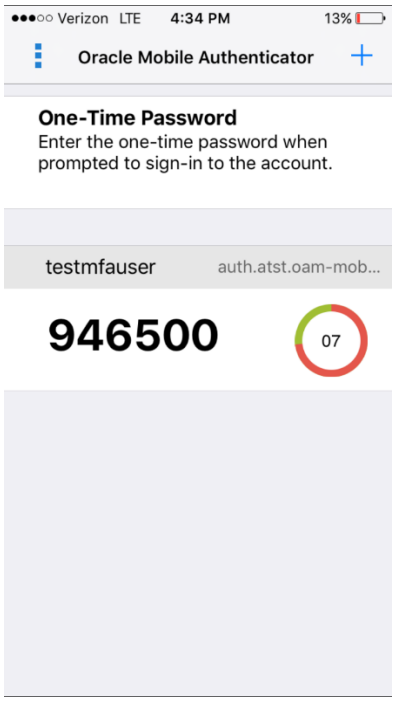
e) Your device will ask if it can update your OMA application settings. Please allow your device to update the OMA application settings.



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.

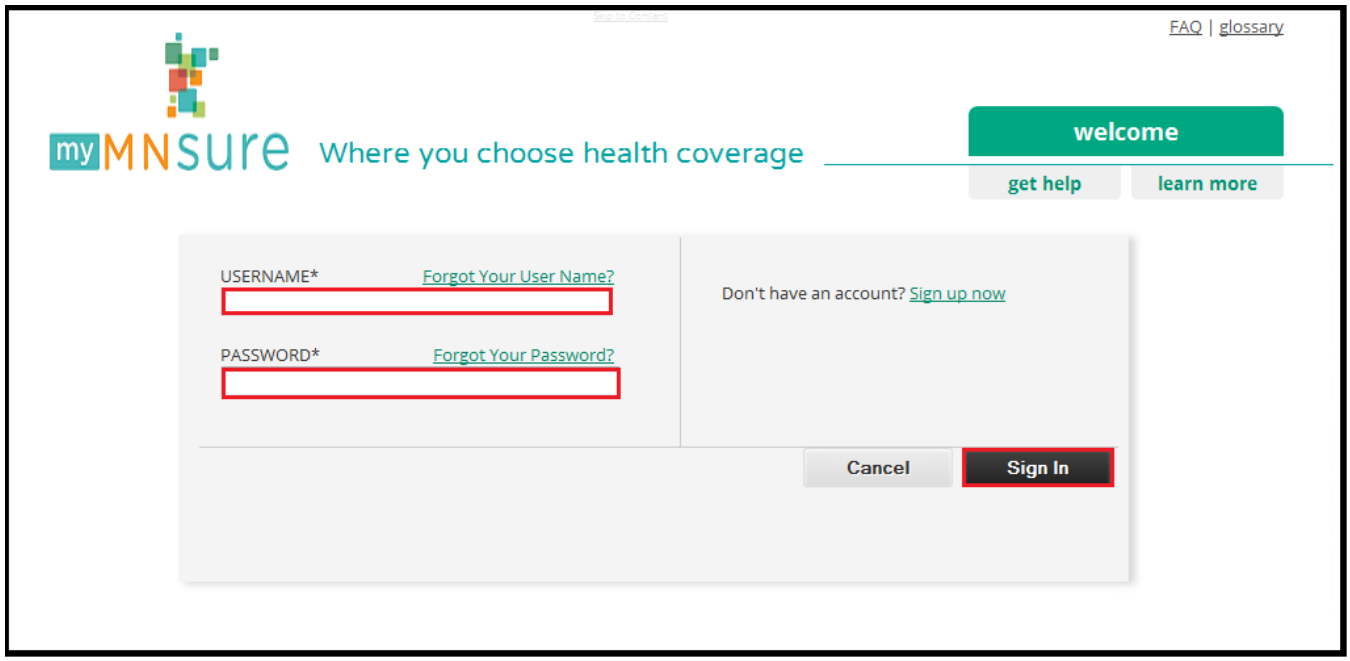


User Log-in Using One-Time Access Code From Email

a) Navigate to the MNsure sign-in page.

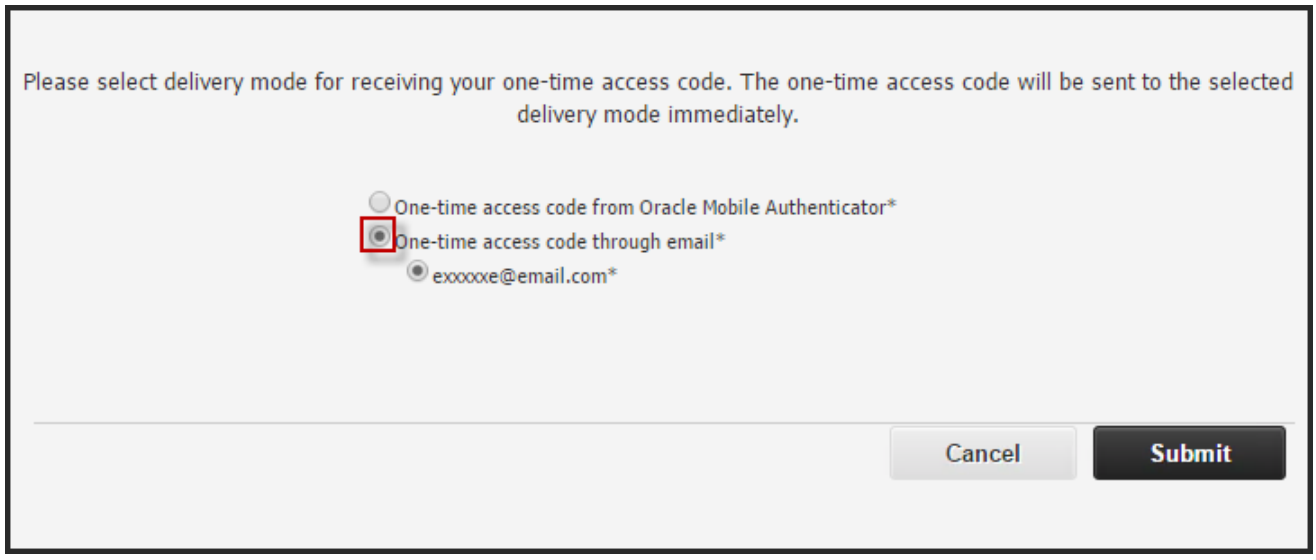
b) Enter username and password.

c) Click on “Sign In” button as shown in the screenshot below.

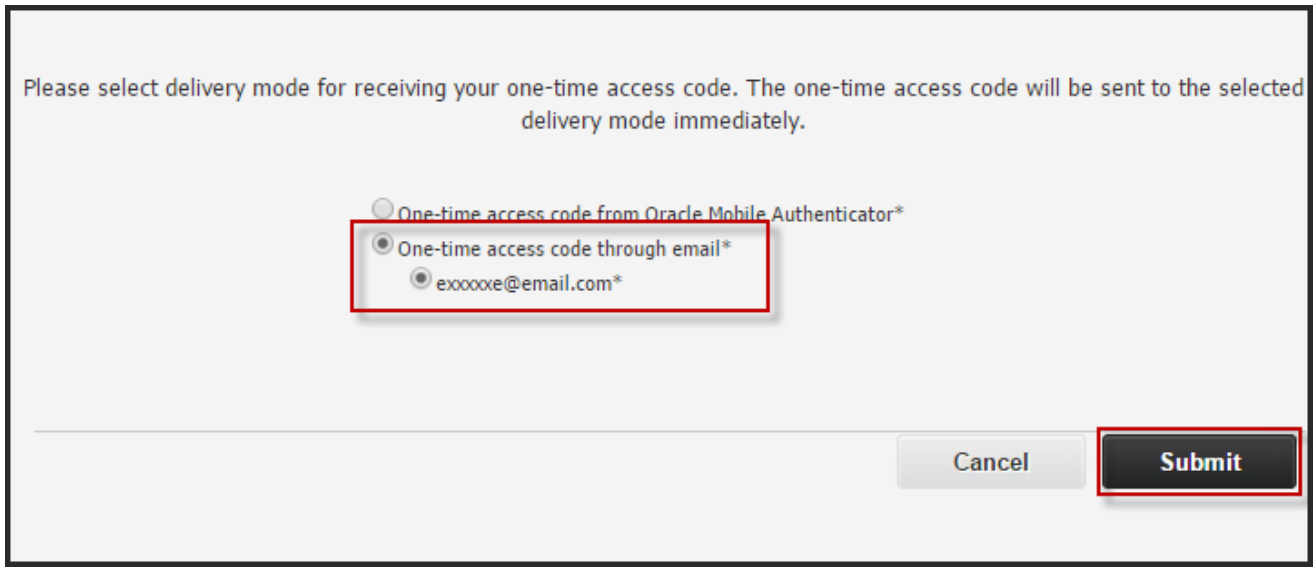


d) Radio button for selection of email will be displayed on the next screen.

e) Select “One Time access code through Email” Radio Button as displayed in the screenshot



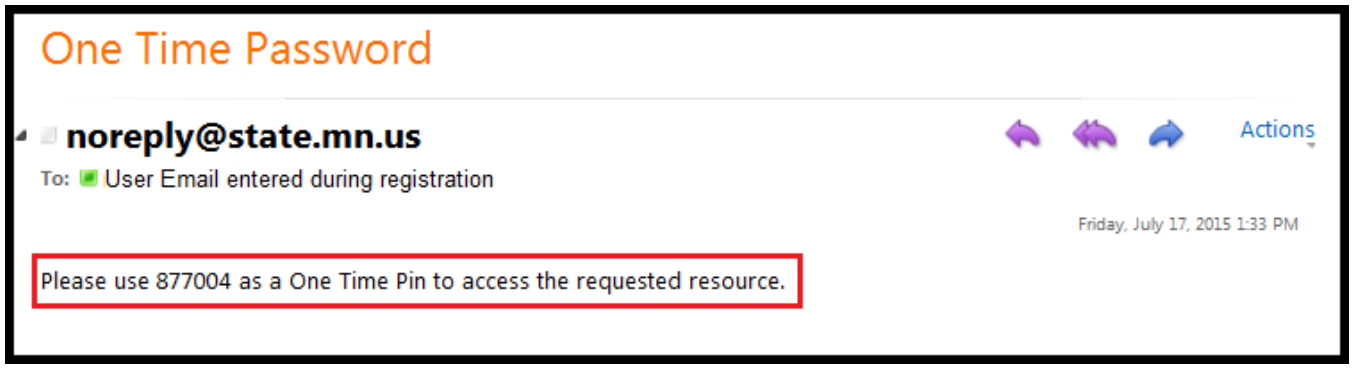
f) Click on the partially hashed email account where the one-time access code will be sent.



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

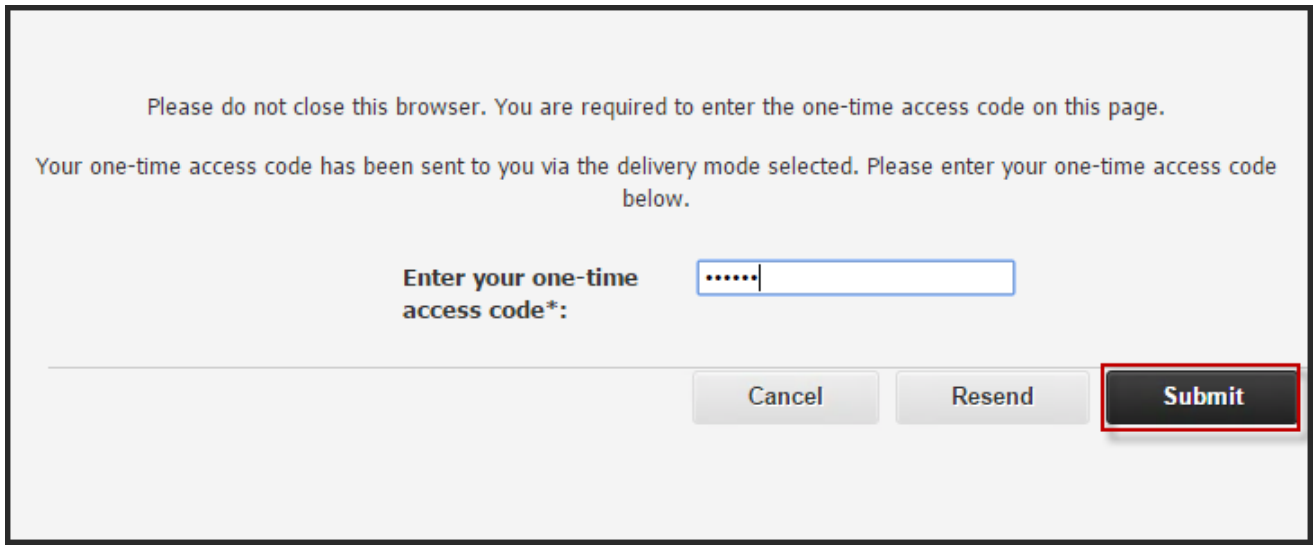
Once the user clicks submit the one time access code will be sent to the user’s email account and the application will redirect the user to the next page as shown in step (i) below.

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.



k) The user will be successfully logged in.

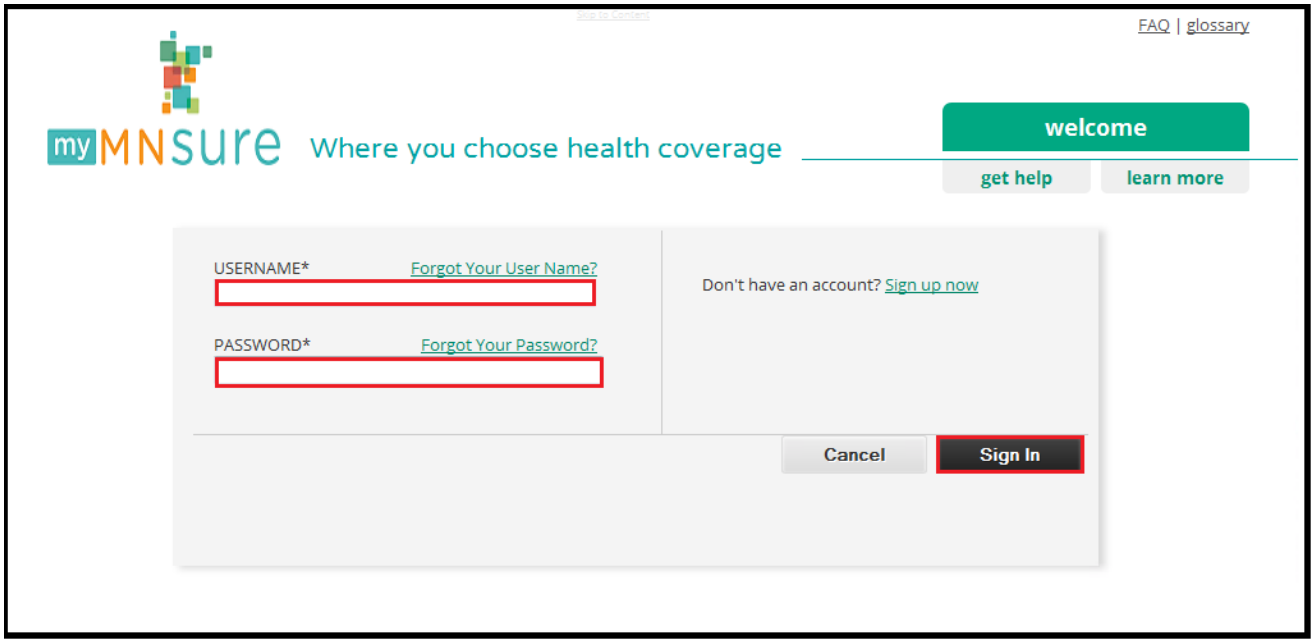
User Log-in Using One-Time Access Code From Oracle Mobile Authenticator

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.

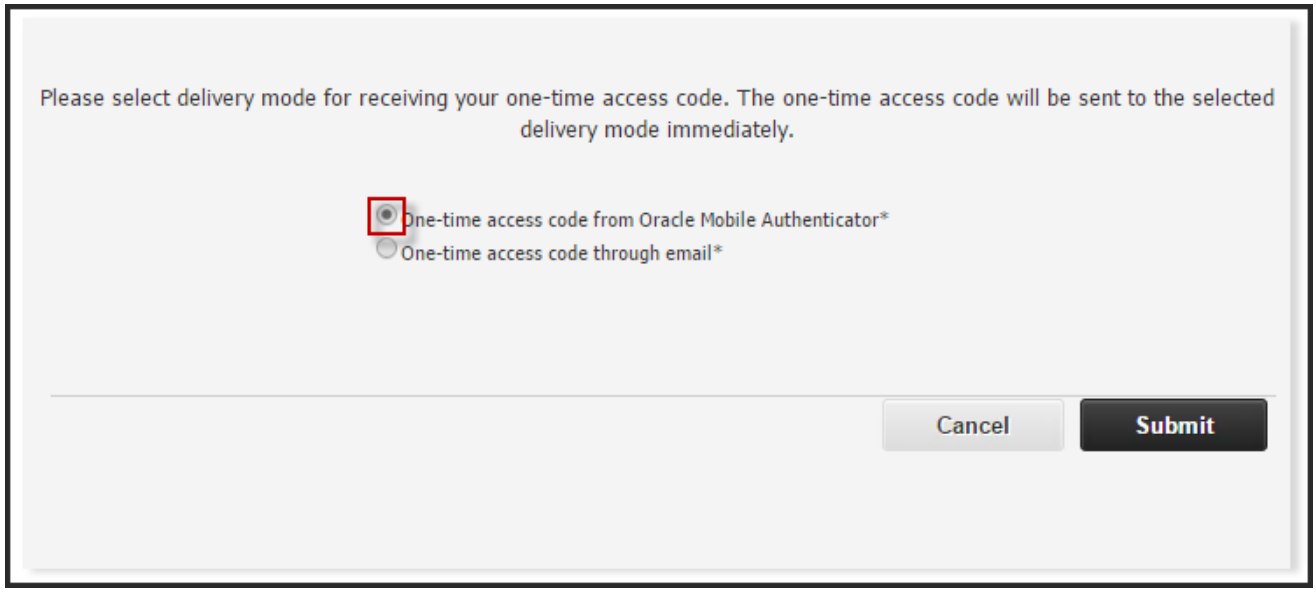
a) Navigate to the MNsure sign-in page.

b) Enter username and password.

c) Click on “Sign In” button as shown in the screenshot below.

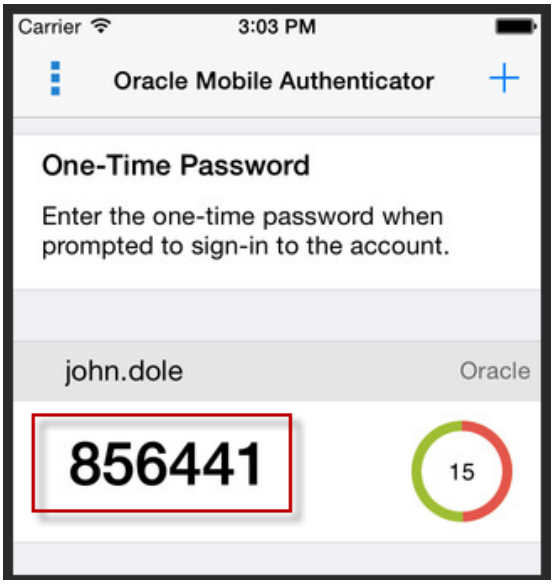


d) Select “One time access code from Oracle Mobile Authenticator” radio button as displayed in the screenshot and click Submit.

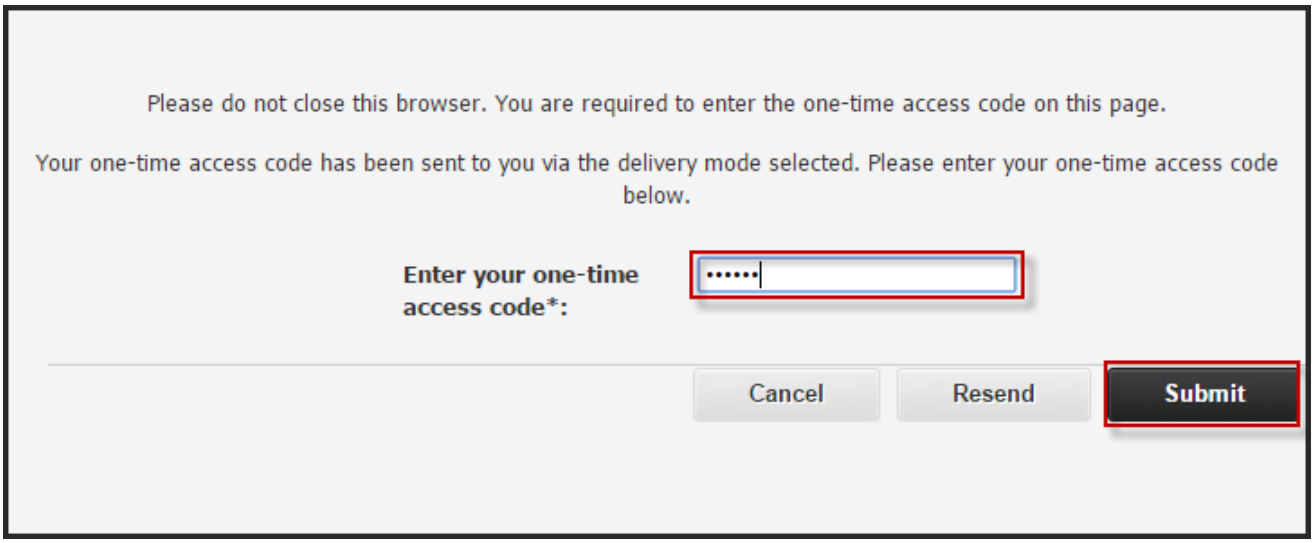


e) Open the Oracle Mobile Authenticator application on your registered device.

f) Enter the one-time access code displayed in the Oracle Mobile Authenticator app.



g) Click on the “Submit” button.



h) The user will be successfully logged in.

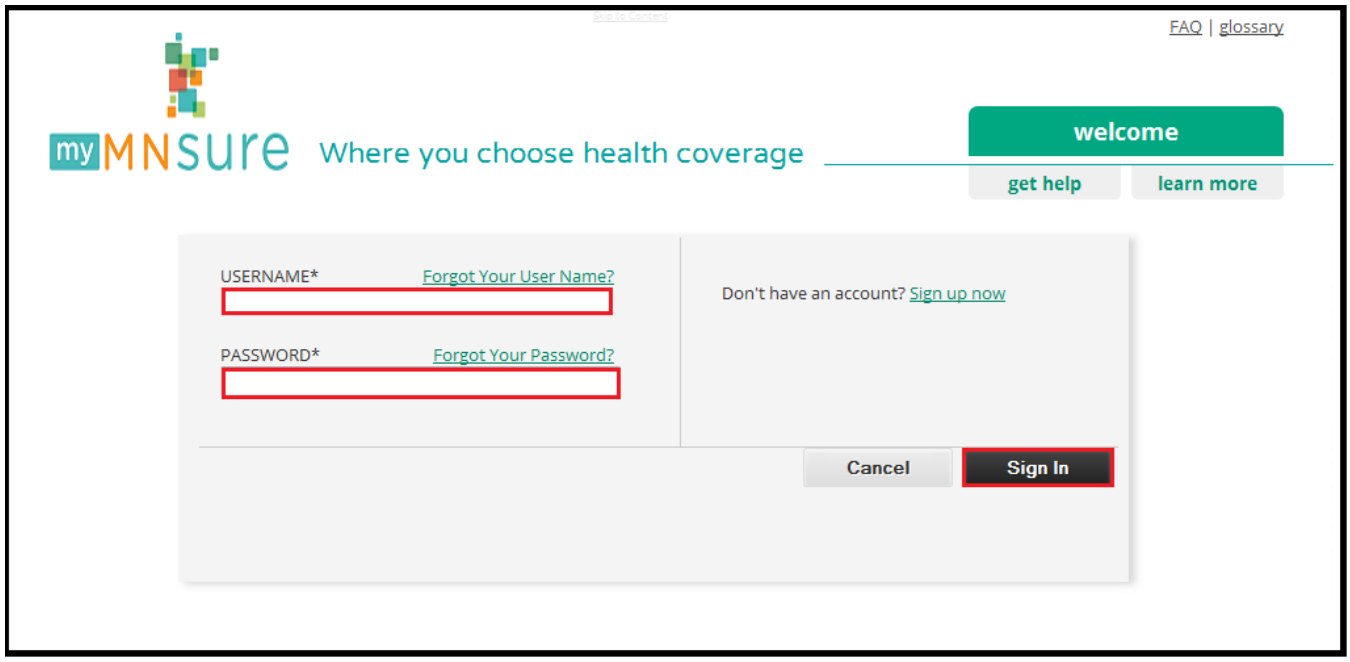
Using the Resend Option

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.

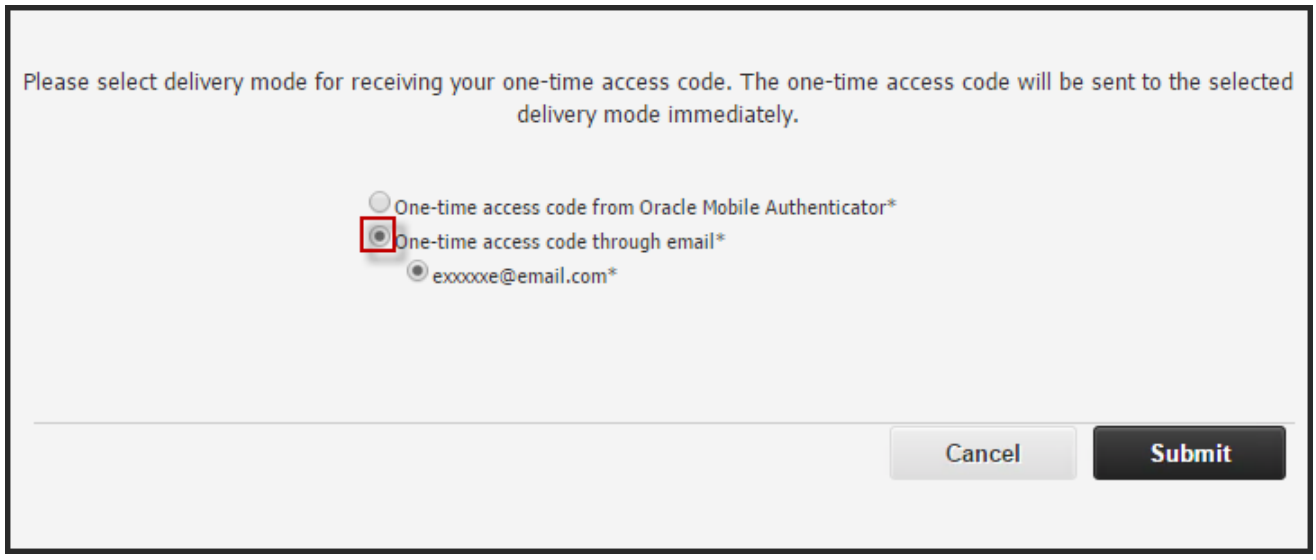
b) Enter username and password.

c) Click on “Sign In” button as shown in the screenshot below.

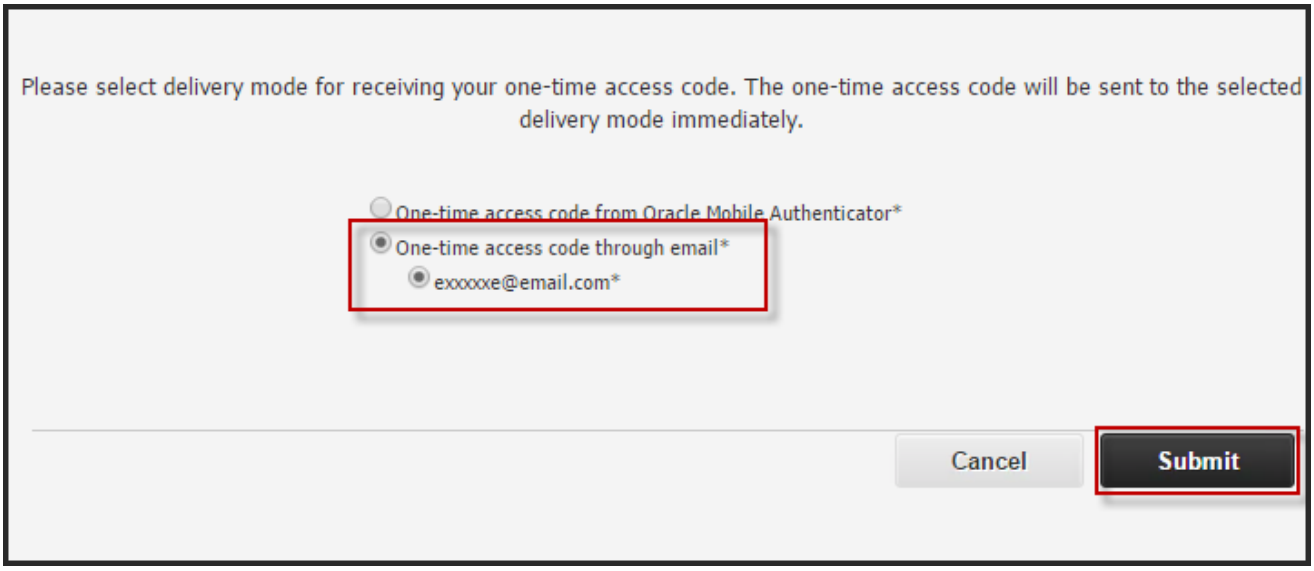


d) Radio button for selection of email will be displayed on the next screen.

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.

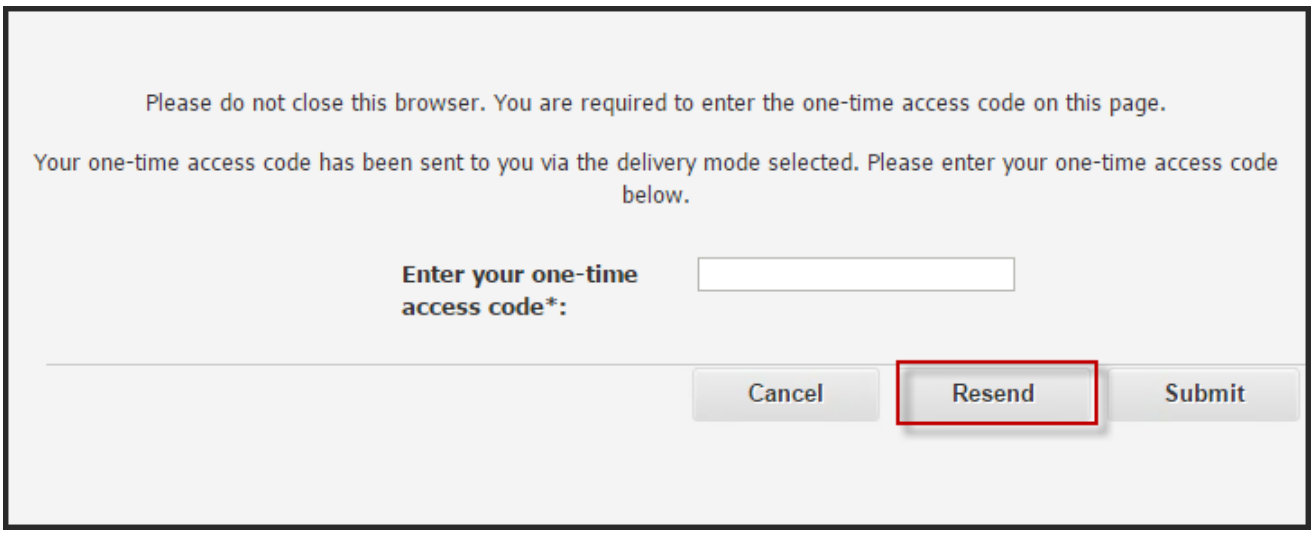


g) Click on “Submit”. The user will be redirected to enter the one-time access code.

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.

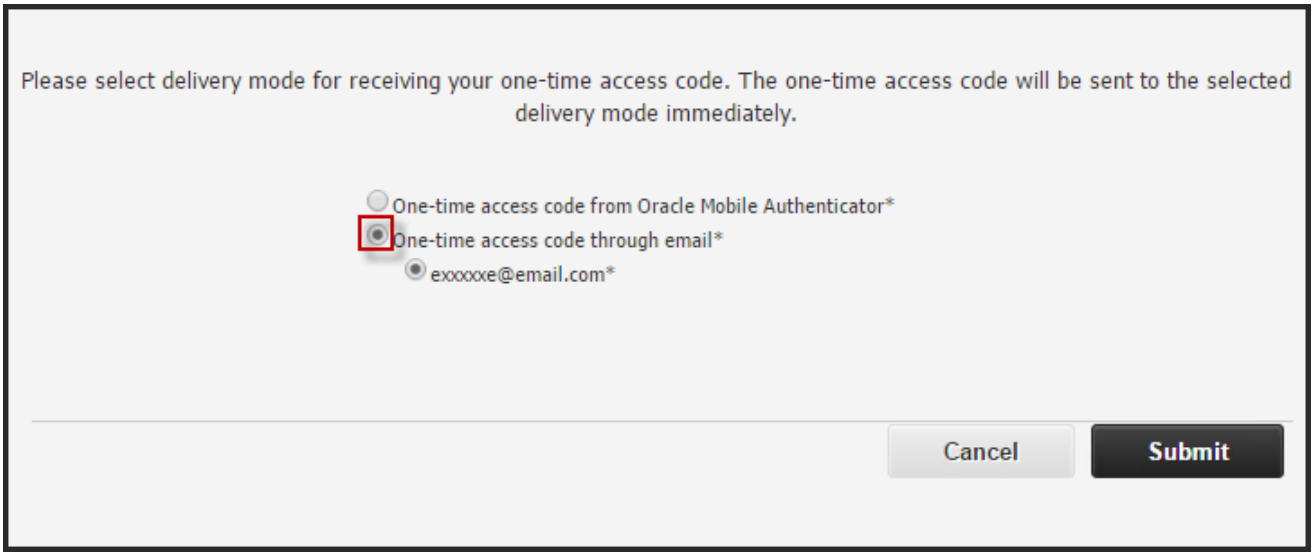
If required, the user can receive a new one-time access code by using the “Resend” button.

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

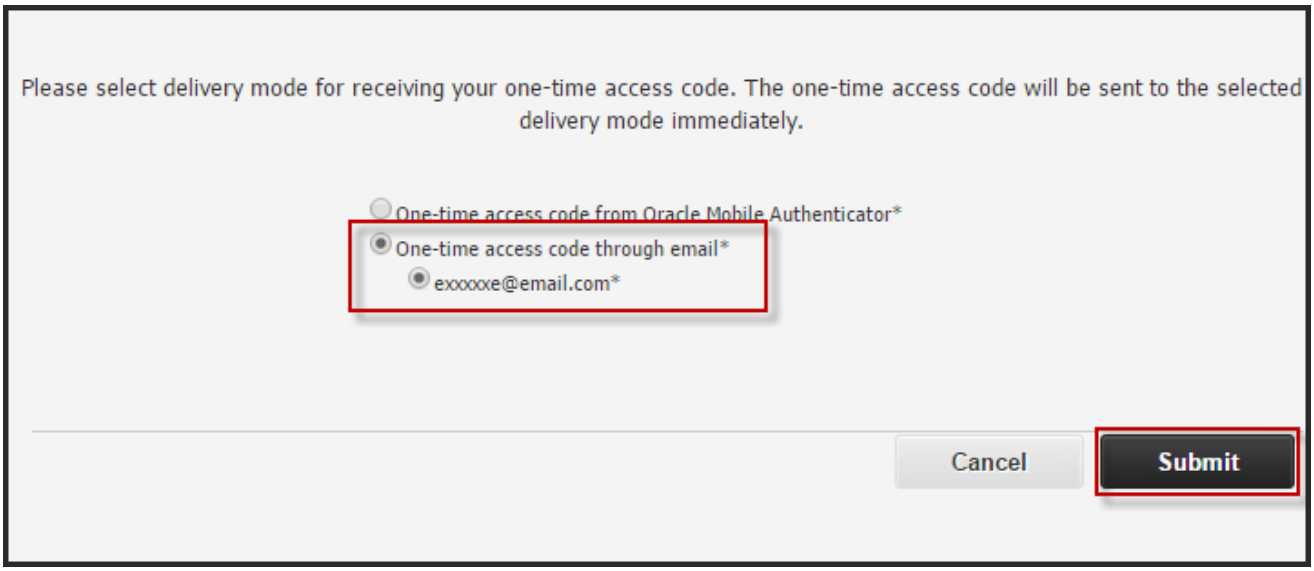


i) Radio button for selection of email will be displayed on the next screen.

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

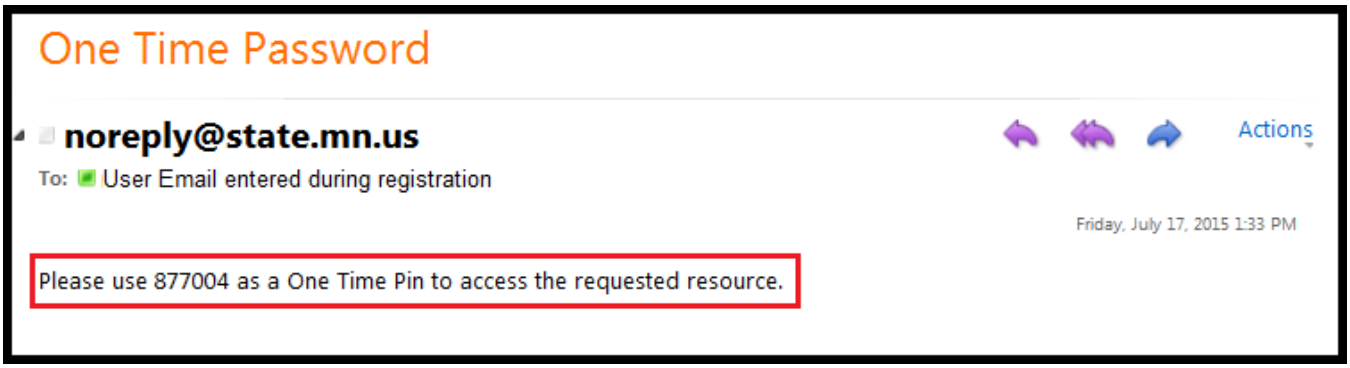


k) Click on the email address where the one-time access code will be sent.



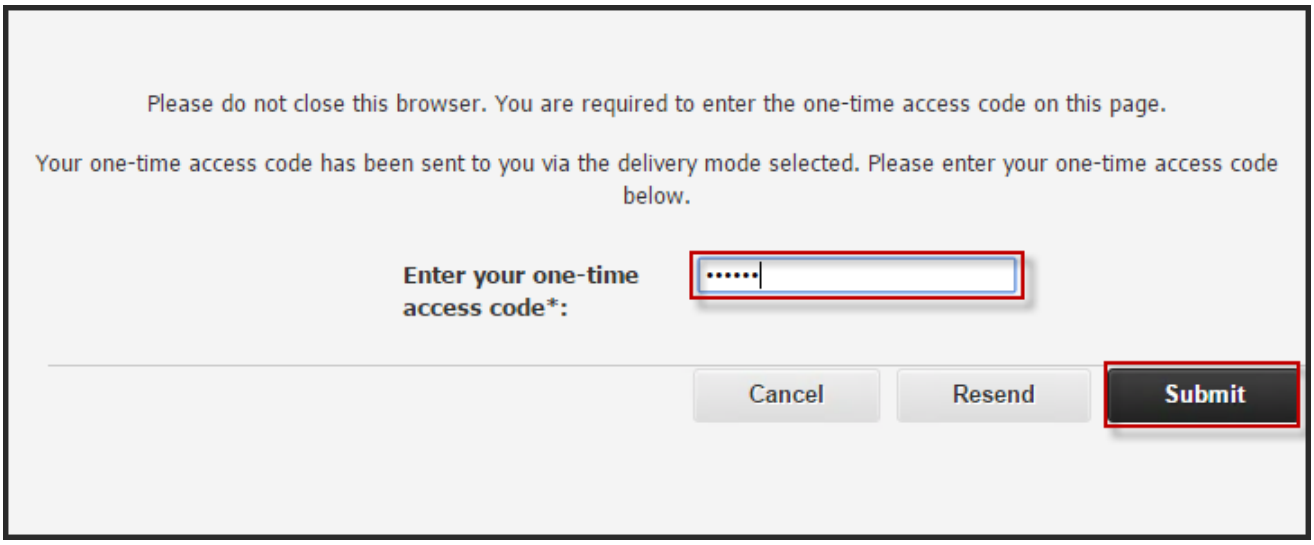
l) Click on “Submit”. The user will be redirected to enter the one-time access code.

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.

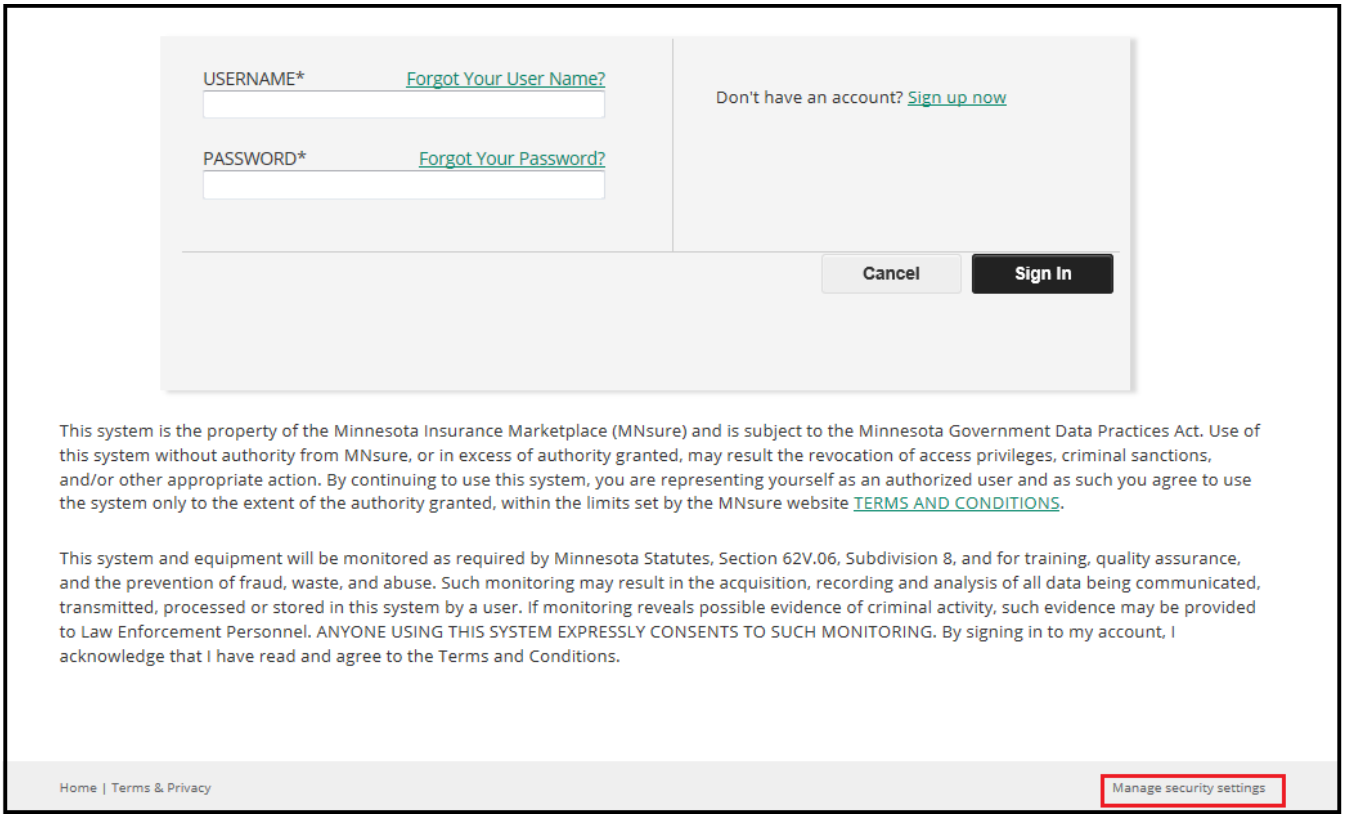


p) The user will be successfully logged in.

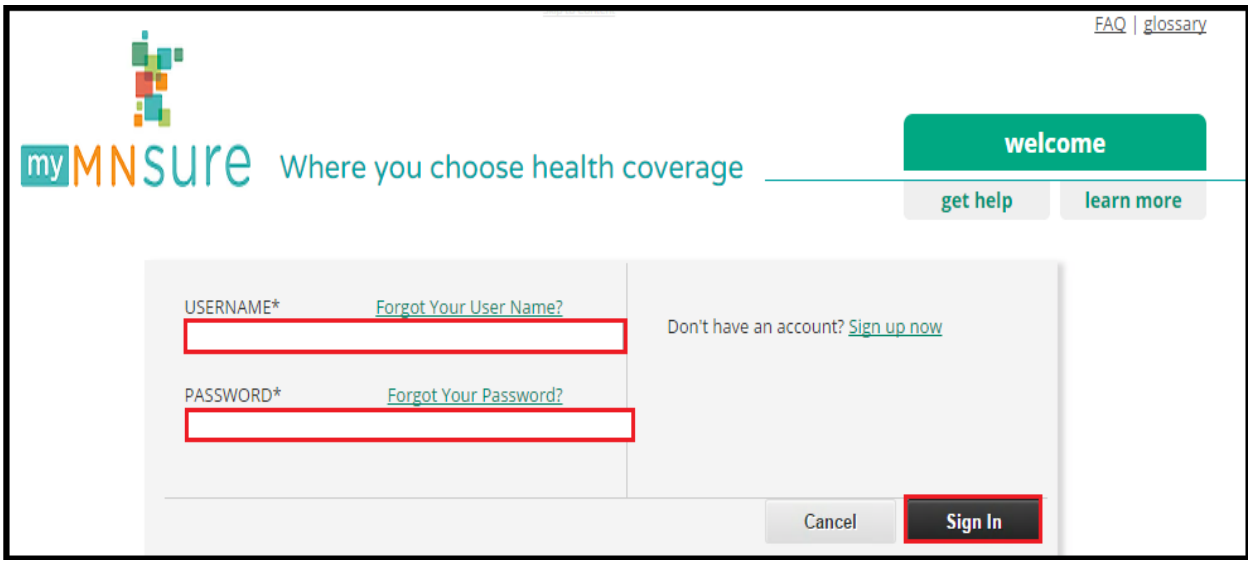
Self Service—Remove Oracle Mobile Authenticator

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.

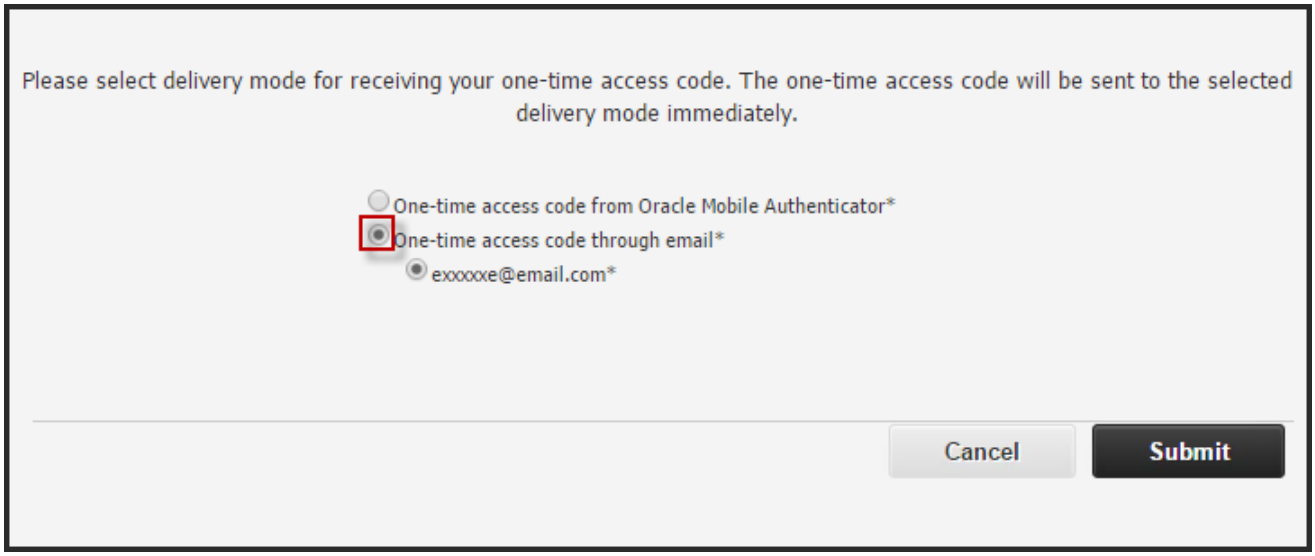


c) Enter username and password.

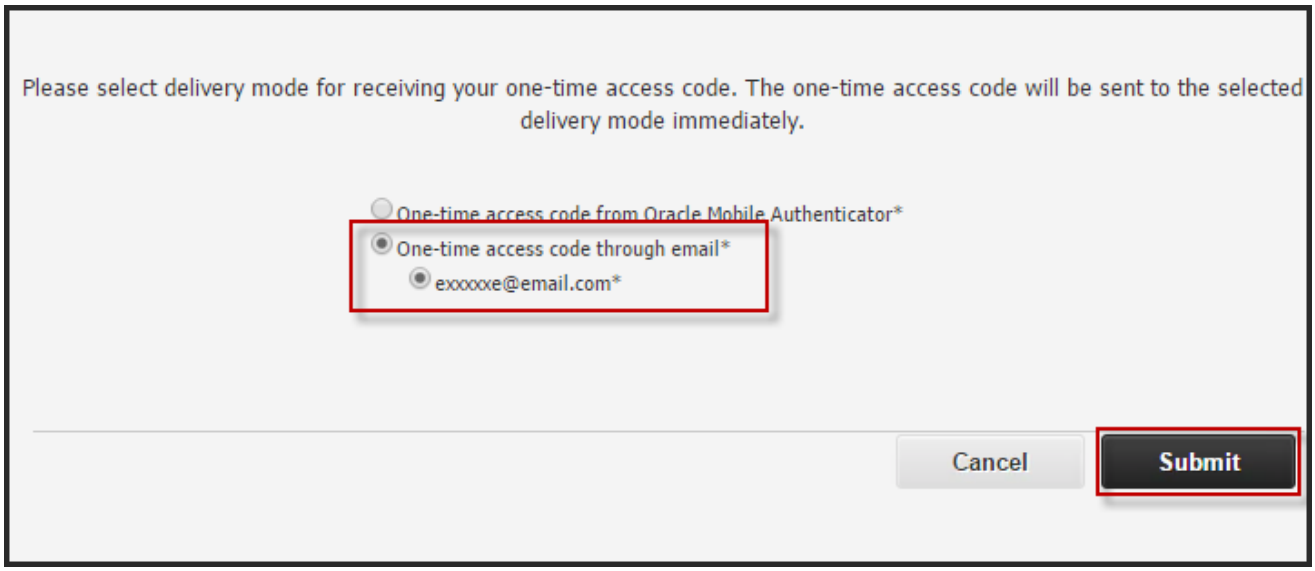


d) Radio button for selection of email will be displayed on the next screen.

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



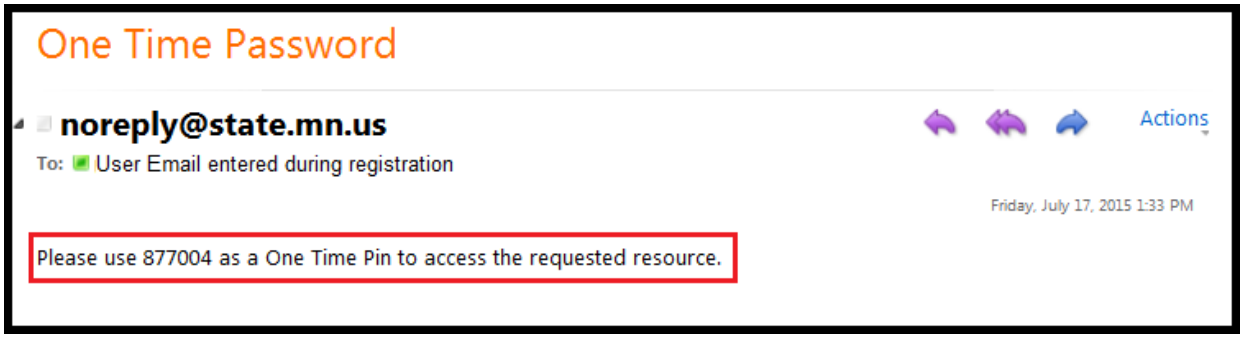
f) Click on the email account where the one-time access code will be sent.



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

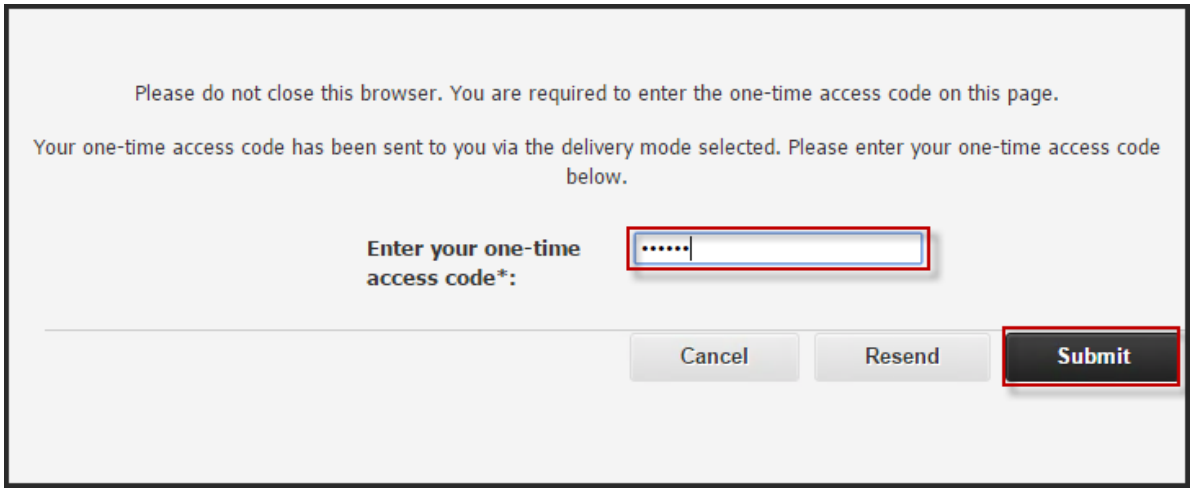
Once the user clicks submit the one-time access code will be sent to the user’s email account and the application will redirect the user to the next page as shown in step (j) below.

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

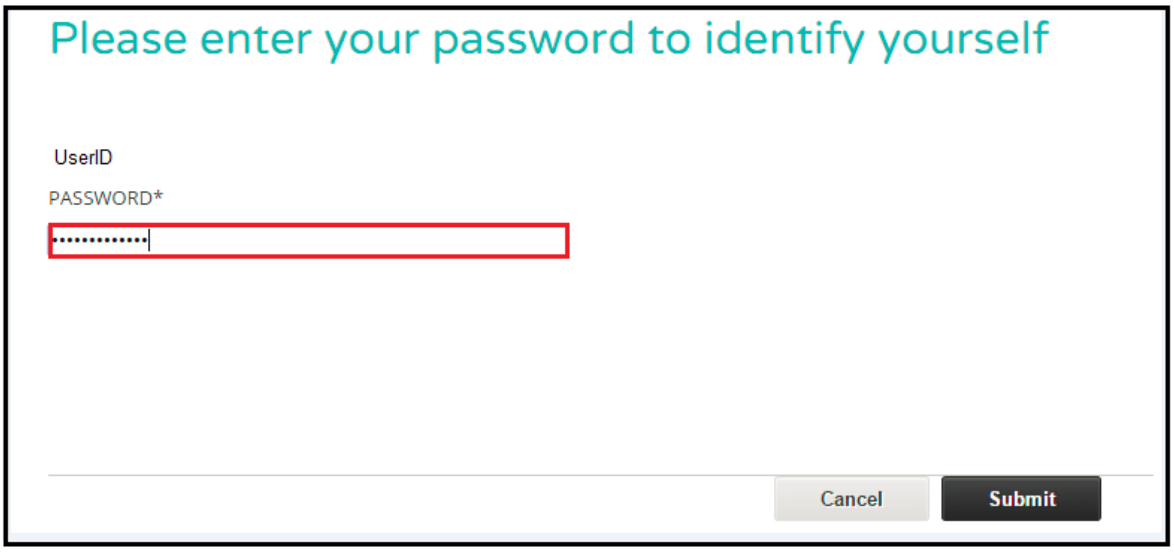


i) Enter the one-time access code that you have received in the email.

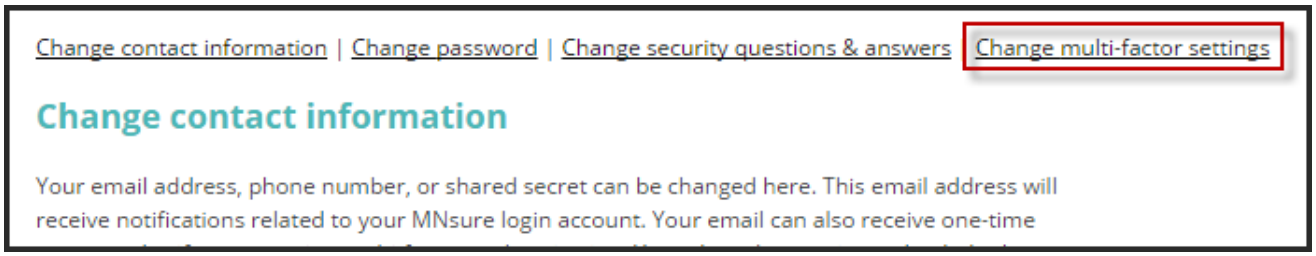
j) Click on the “Submit” button.



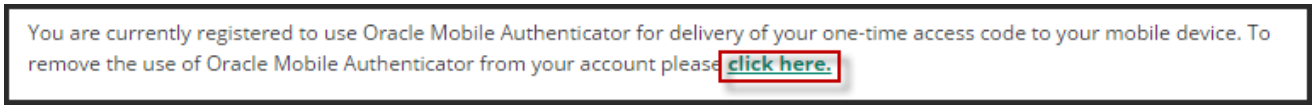
k) Re-enter your password.



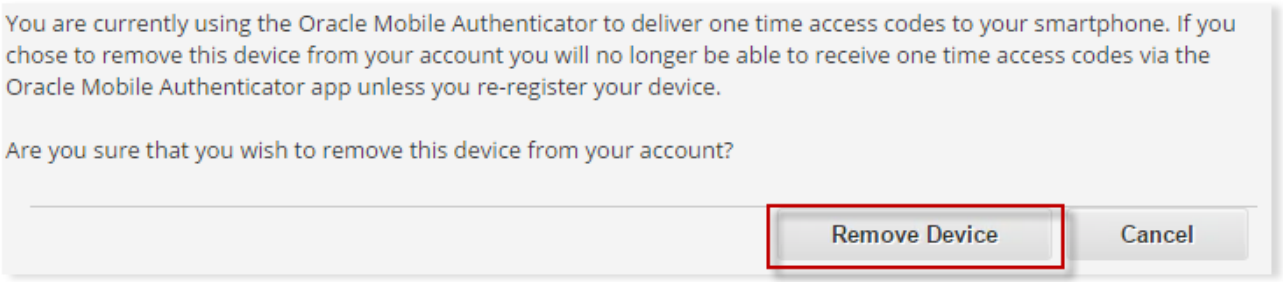
l) Click on the “Change multi-factor settings” tab at the top.



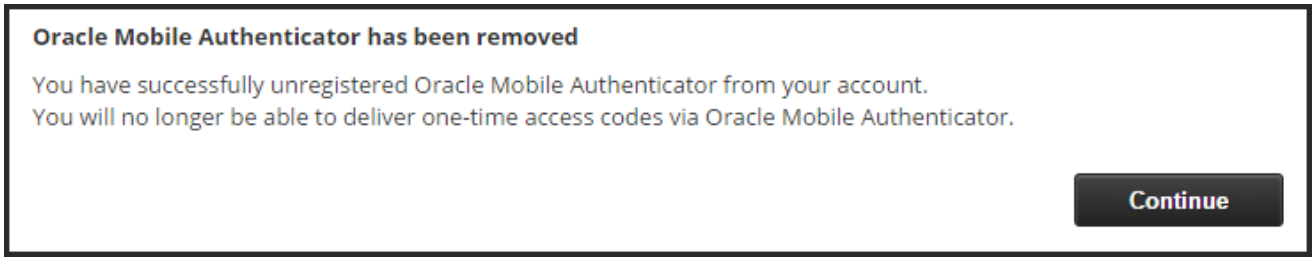
m) To remove Oracle Mobile Authenticator from your account click where instructred on the page.



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.



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

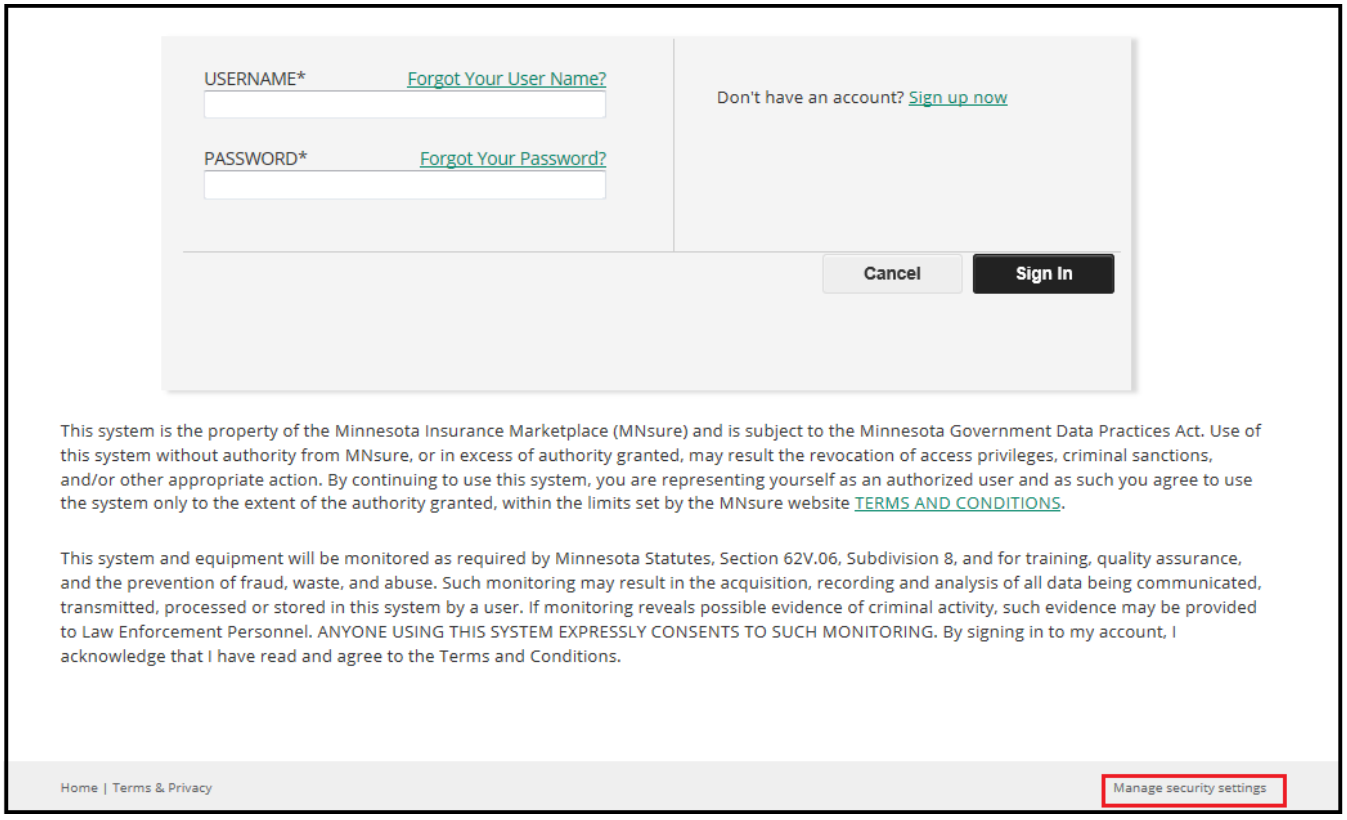


p) We strongly suggest removing the account from inside the Oracle Mobile Authenticator application on your device. To do this you must tap and hold the account inside the application until the ribbon at the top is displayed. From there you can click on the trash can icon to remove the account from the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

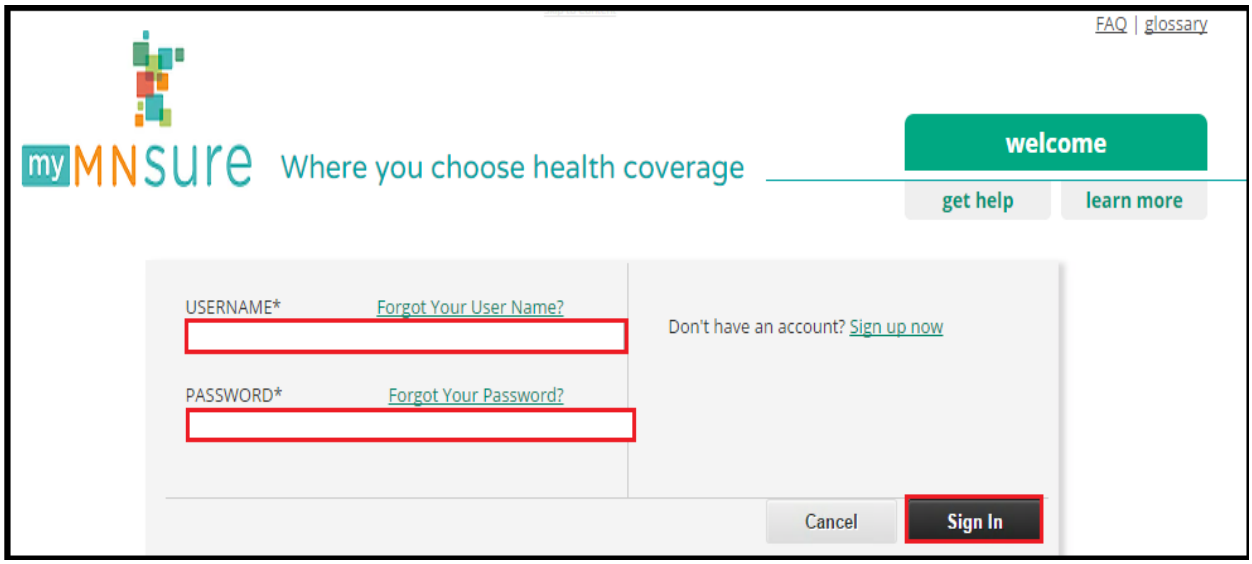
Self Service—Update Email Account

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.

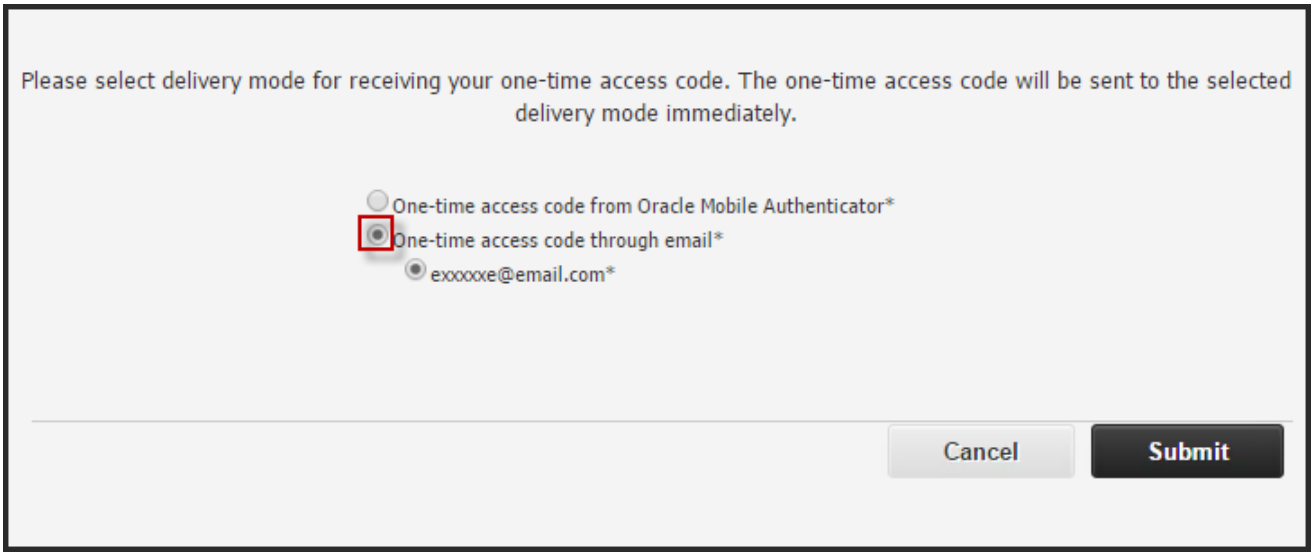


c) Enter username and password.

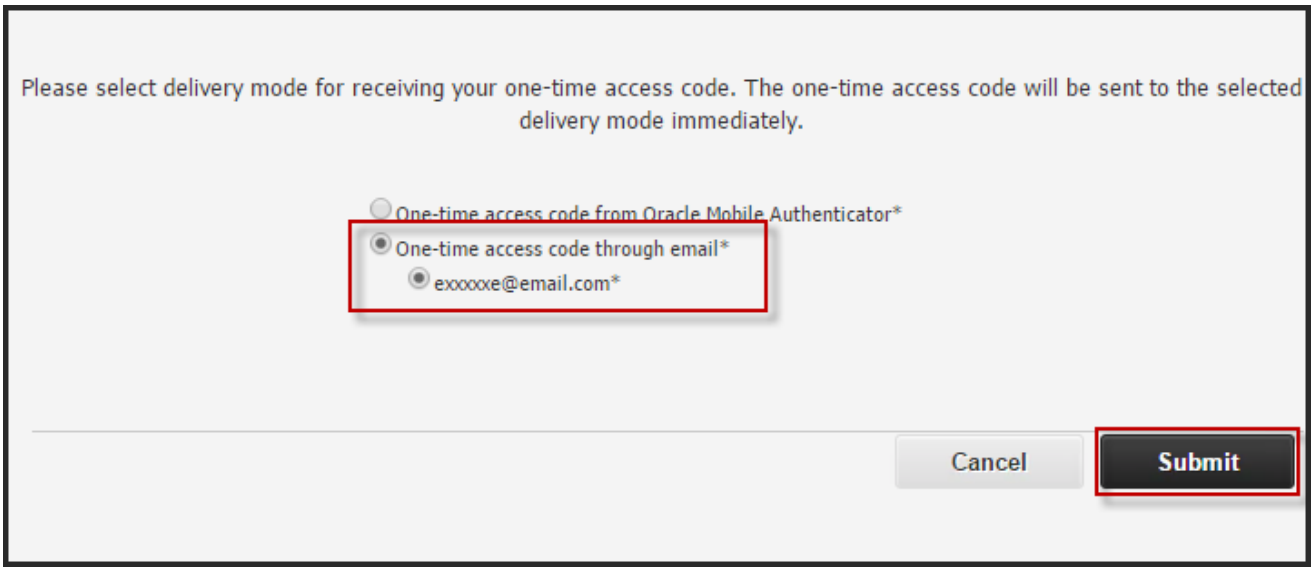


d) Radio button for selection of email will be displayed on the next screen.

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



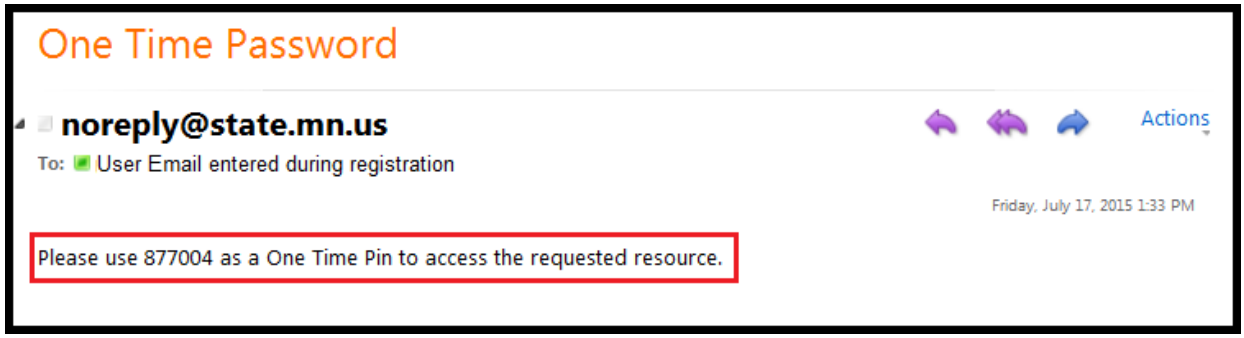
f) Click on the email account where the one-time access code will be sent.



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

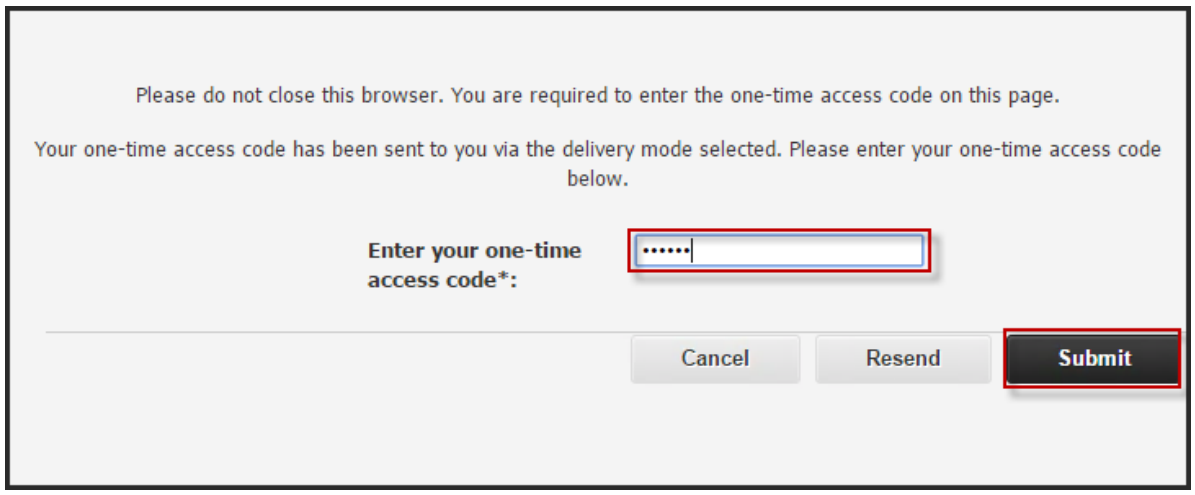
Once the user clicks submit the one-time access code will be sent to the user’s email account and the application will redirect the user to the next page as shown in step (j) below.

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

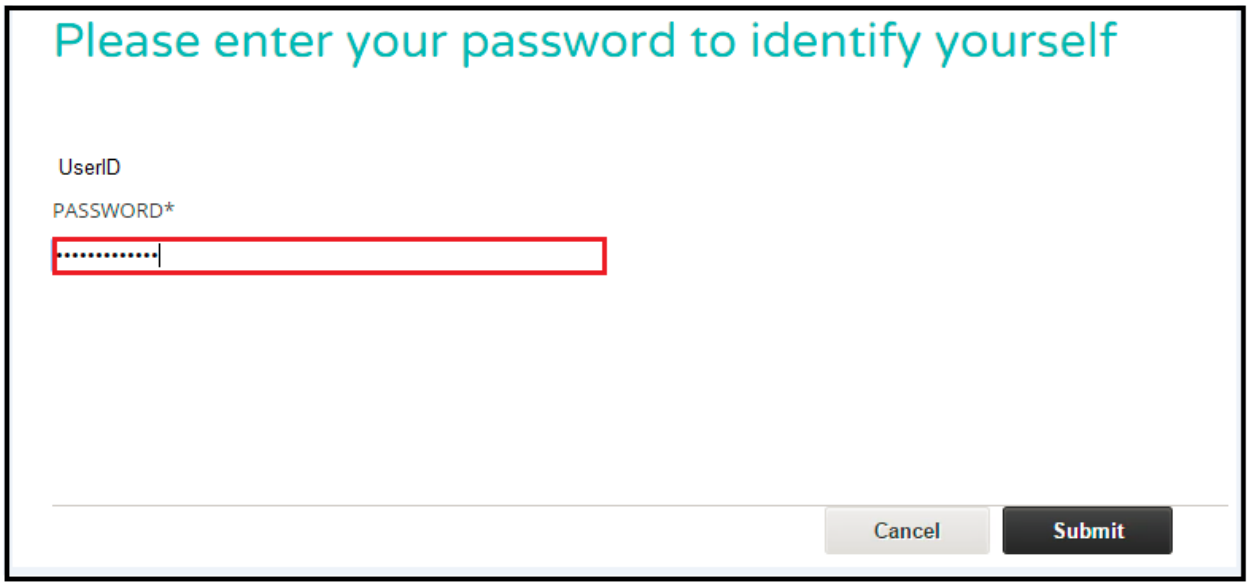


i) Enter the one-time access code that you have received in the email.

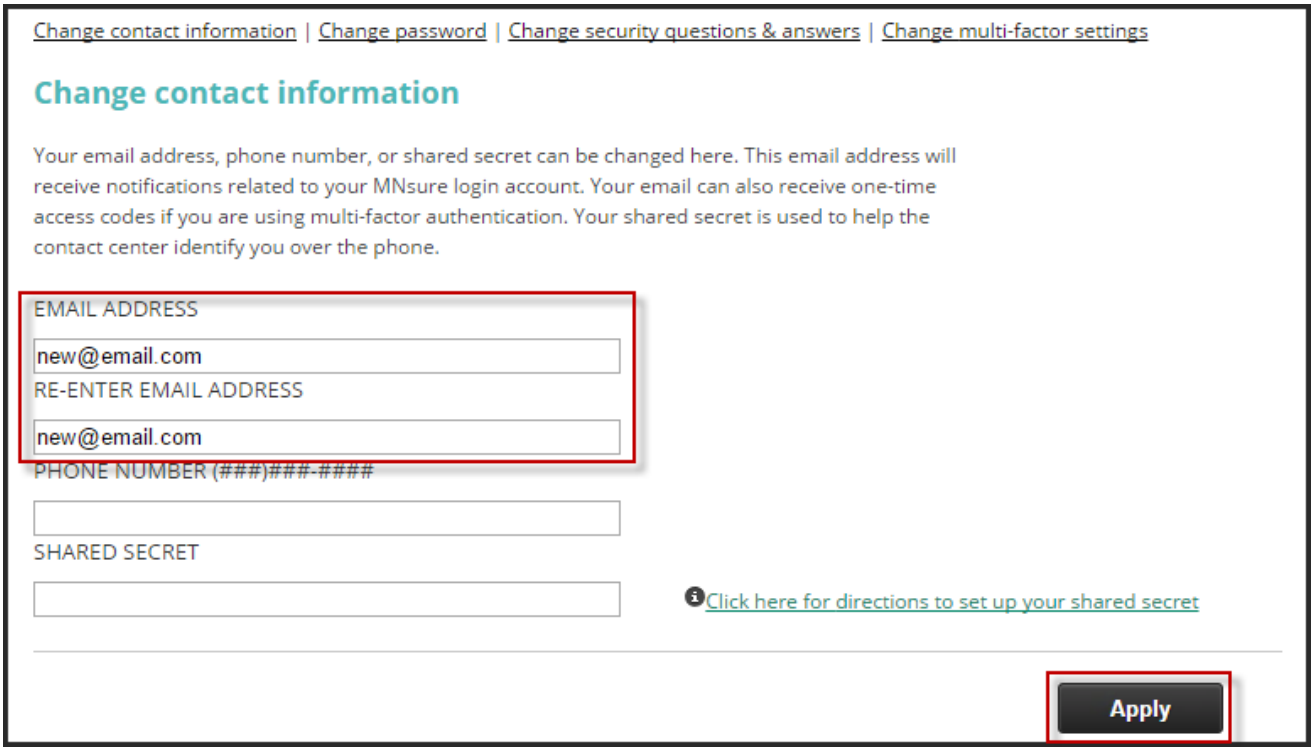
j) Click on the “Submit” button.



k) Re-enter your password.

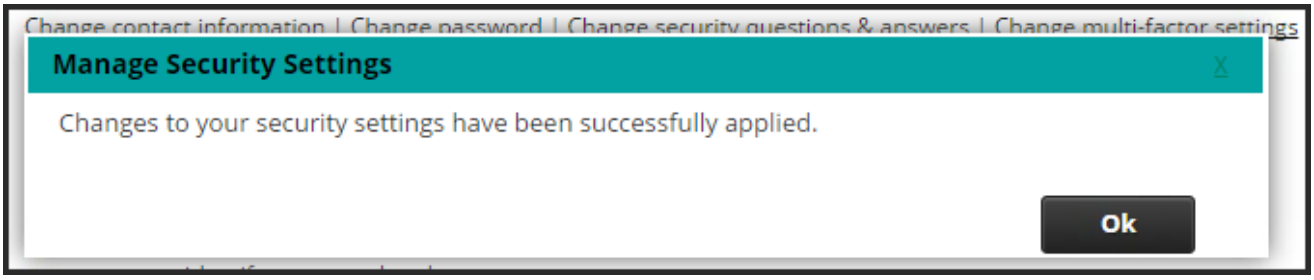


l) Update the email account that will be used to receive the one-time access code.



m) Click on Apply.

n) A message as shown in screenshot below appears which confirms that changes have been successfully applied.



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