



OneLogin User Guide

Version 1.0

Updated 06/04/2025

<https://wvoasis.onelogin.com/portal>

For Questions:

wvOASIS HelpDesk

1-855-666-8823 (Mon -Fri 7am to 5pm)

helpdesk@wvoasis.gov





TABLE OF CONTENTS

- 1. Setting Up Entry Into OneLogin 4
- 2. Choosing /Setting Up the Authentication Factor 10
 - a. Email..... 10
 - b. SMS (Text Message) 10
 - c. Authenticator Application 11
 - d. OneLogin Protect 11
- 3. The Main Menu 13
 - a. Frequents Menu..... 13
 - b. wvOASIS Applications Menu 13
- 4. The Profile Settings..... 15
 - a. Profile 15
 - b. Change Password 15
 - c. Security Factors 16
 - d. Recent Activity..... 18
- 5. Logging In to One Login..... 20
 - a. Multiple Security Factors 20

Confidential and proprietary material of West Virginia and CGI. Documents contain material for West Virginia’s internal use only

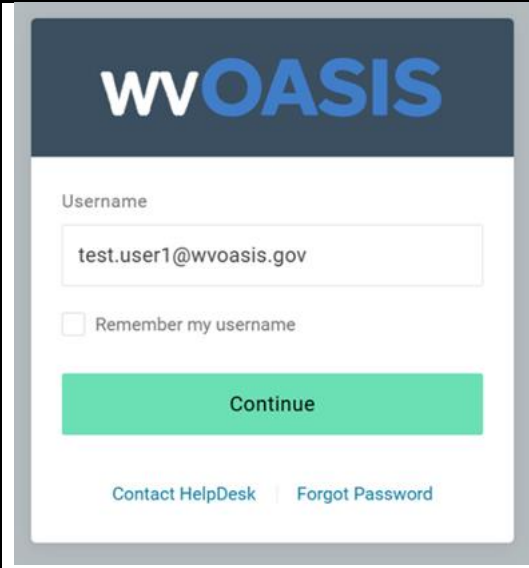
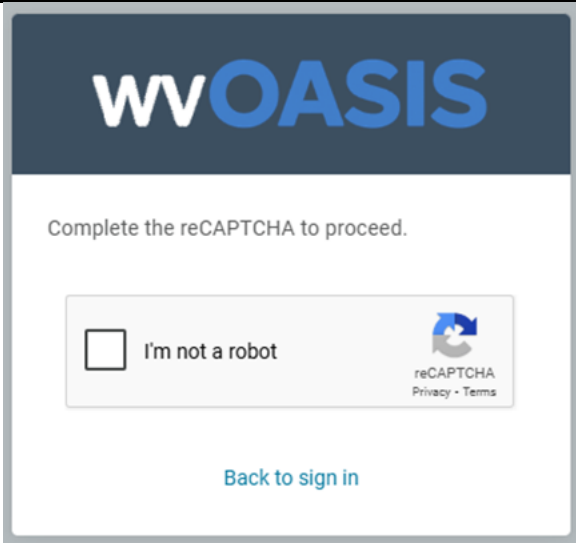
wvOASIS is transitioning from myApps to a new single sign on application called OneLogin. OneLogin will be used to access wvOASIS applications previously in myApps. Users who have Pcard training, Notices and/or Vista will have a myApps icon under OneLogin to allow access to these applications.

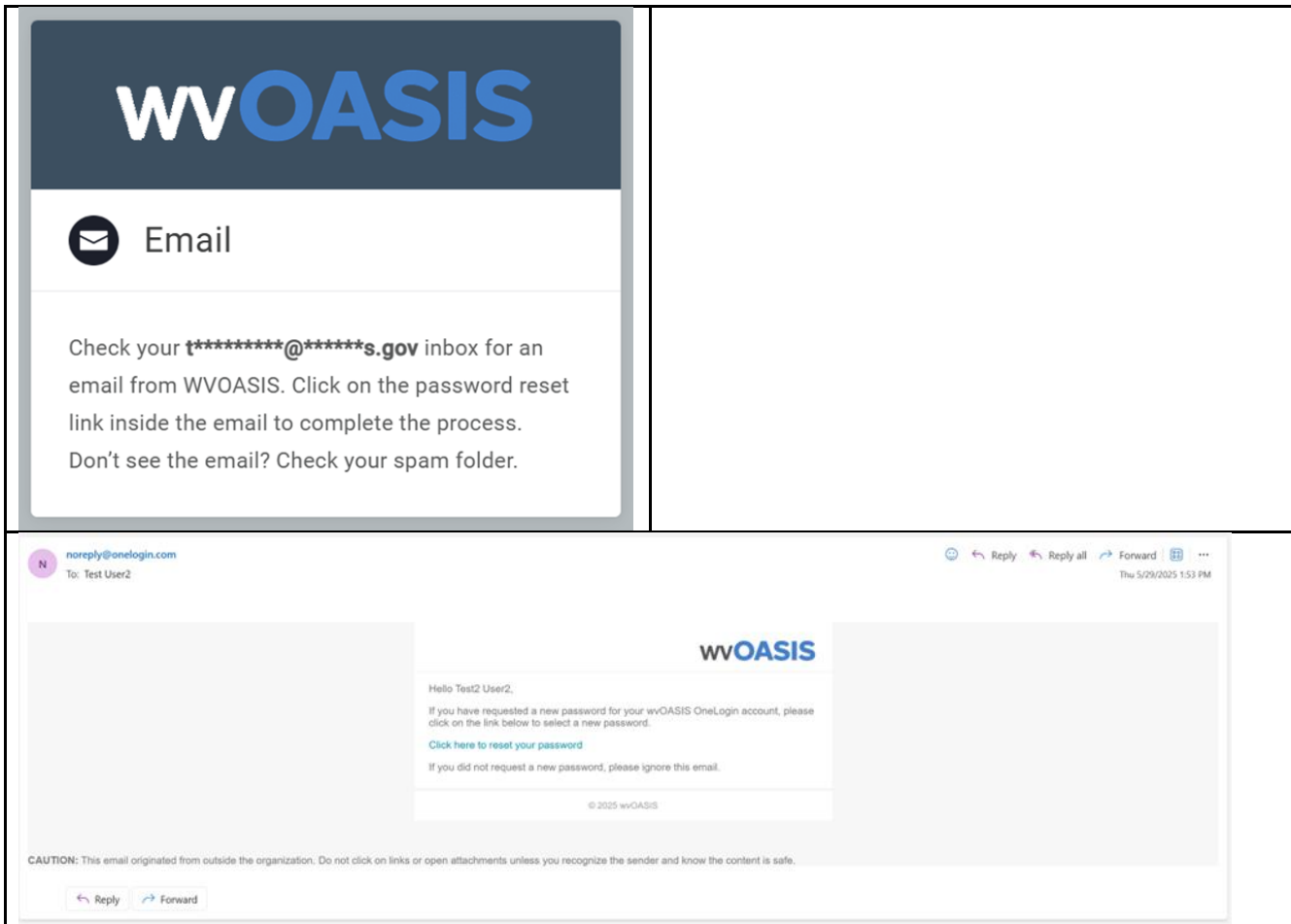
1. Setting Up Entry Into OneLogin

- a. Please navigate to the following URL: <https://wvoasis.onelogin.com/portal>

NOTE: You may want to bookmark this URL for future access to OneLogin.

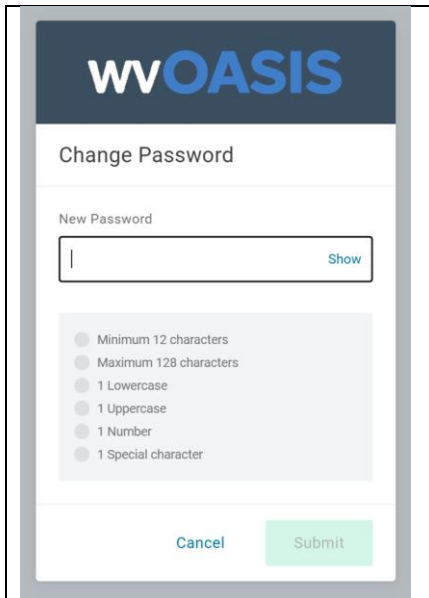
- b. At the sign in screen, do not click Continue.
- c. **You must click “Forgot Password”** and you will enter your existing email address from MyApps. Now you can click Continue.
- d. If you are presented with the reCAPTCHA instructions, please complete this screen (Optional – may show up / may not)
- e. You will then be notified that you have received an email with a Password Reset Link.

 The sign-in screen for WVOASIS. It features the WVOASIS logo at the top. Below it is a "Username" label and a text input field containing "test.user1@wvoasis.gov". There is a checkbox labeled "Remember my username". A green "Continue" button is below the input field. At the bottom, there are two links: "Contact HelpDesk" and "Forgot Password".	 The reCAPTCHA screen for WVOASIS. It features the WVOASIS logo at the top. Below it is the text "Complete the reCAPTCHA to proceed." There is a checkbox labeled "I'm not a robot" and a reCAPTCHA logo with links for "Privacy" and "Terms". A blue "Back to sign in" link is at the bottom.
---	---



- f. Click the Link in the email to begin. You will next see a pop-up screen that will prompt you to create a password.

The password must adhere to the following criteria in the radio buttons as shown in the picture below:

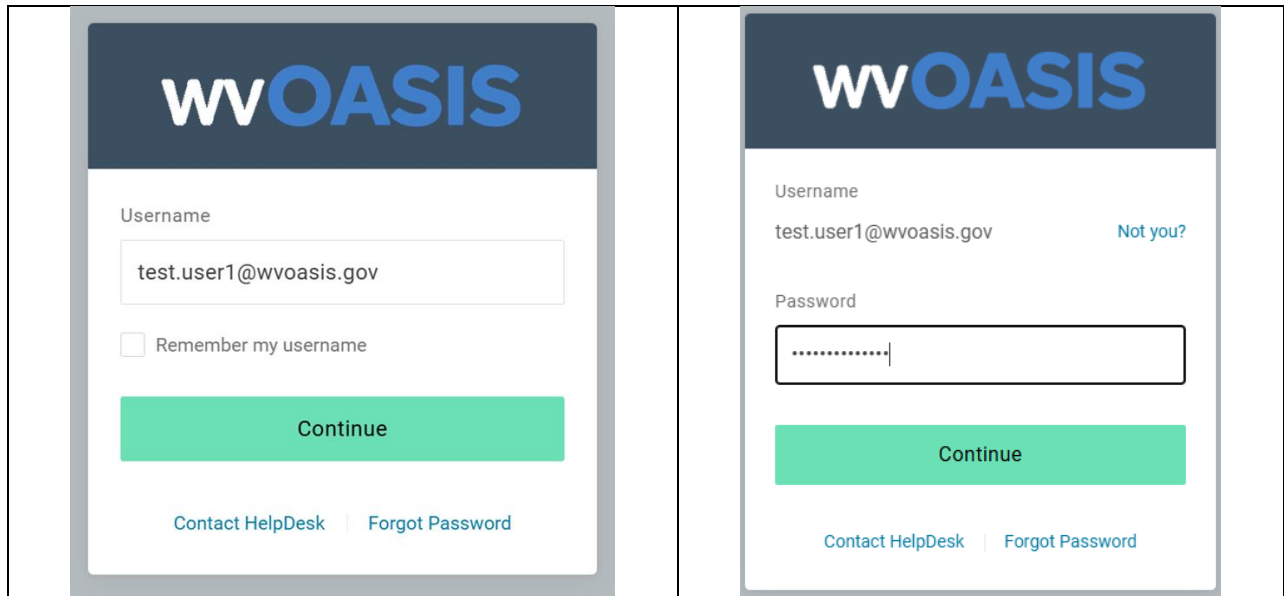
A screenshot of the wvOASIS 'Change Password' interface. At the top is the wvOASIS logo. Below it is the title 'Change Password'. A section labeled 'New Password' contains a text input field with a 'Show' link to its right. Below the input field is a list of password requirements, each with a radio button: 'Minimum 12 characters', 'Maximum 128 characters', '1 Lowercase', '1 Uppercase', '1 Number', and '1 Special character'. At the bottom are two buttons: 'Cancel' and 'Submit'.

NOTE: You will not be able to re-use the LINK in the email to log in again to wvOASIS.Onelogin.com/portal

USE THIS LINK GOING FORWARD: <https://wvoasis.onelogin.com/portal>

(It may be helpful to bookmark this link in your browser)

- g. Once you set up the password, you will again see a login screen. Enter your email address and click the Continue Button. Next enter your newly created password.

Two side-by-side screenshots of the WVOasis login interface. The left screenshot shows the login page with a dark blue header containing the "WVOasis" logo. Below the header is a white form with a "Username" label, a text input field containing "test.user1@wvoasis.gov", a checkbox labeled "Remember my username", a green "Continue" button, and two links at the bottom: "Contact HelpDesk" and "Forgot Password". The right screenshot shows the same login page but with the "Username" field pre-filled with "test.user1@wvoasis.gov" and a "Not you?" link to its right. The "Password" field is now visible, showing a masked password "....." with a cursor. The "Continue" button and bottom links remain the same.

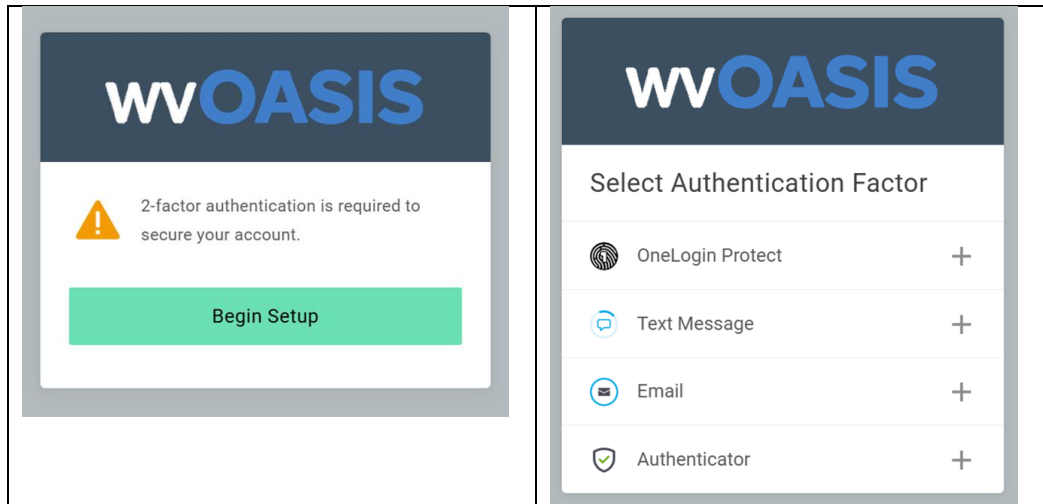
- h. After you log in, you will be required to select your Authentication Factors. You should setup at least two. One primary and one backup.

If you pick your primary to be a phone-based authentication factor (Text, Authenticator, OneLogin Protect), you may want to choose Email as your backup. Click Begin Setup to start.

Once you create the first Authentication Factor, you must navigate to the Profile menu to set up additional Authentication Factors.

Please use Section 4.c of this document for additional details on how to access the Security Factors menu and to choose your Primary designation.

NOTE: We strongly recommend that you set up **TWO Authentication Factors.**









You can set up as many Authentication Factors as you want. Here are some guidelines:

1. You may already use an Authenticator app on your phone for other apps. (Microsoft or Google are popular). If so, you can add an Authenticator for this application as one of your Authentication Factors.
2. Something new for OneLogin is the OneLogin Protect mobile app. If you choose to use this app, you will need to install this app on your mobile device. You will also need to enable biometric (face ID). The OneLogin Protect app provides the convenience of having a “push” notification to log into OneLogin come from your mobile device.

Each time you login, using your primary or a backup authentication factor, you will receive a code to enter into the login screen.

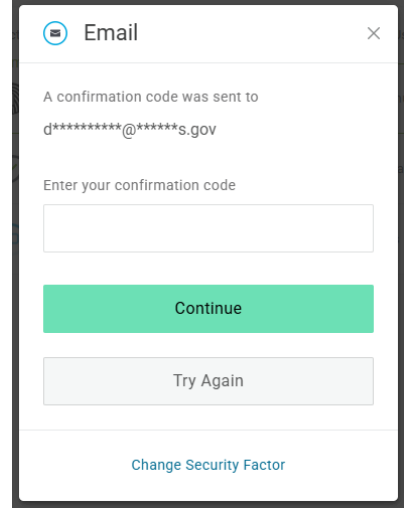
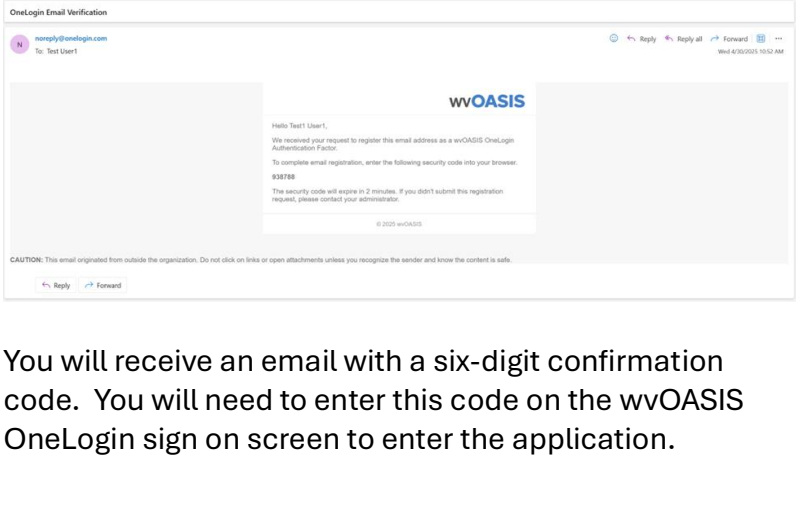
Refer to Section 5, for screenshots on having the ability to choose from multiple Authentication Factors on the sign in process.

Note: Having **Email** as a secondary/backup Authentication Factor is ideal because the other three methods (SMS / Authenticator / OneLogin Protect) require you to have access to your phone. Email can be retrieved from your workstation/laptop.

<div><h3>Text Message</h3><p>Enter your code</p><div><input type="text"/>Show</div><div>Continue</div><p>Having trouble? Resend SMS code</p><p>Change Authentication Factor</p></div>	<div><h3>Select Authentication Factor</h3><div><div></div>OneLogin Protect</div><div><div></div>Authenticator</div><div><div></div>OneLogin SMS</div><div><div></div>Email</div></div>
--	--

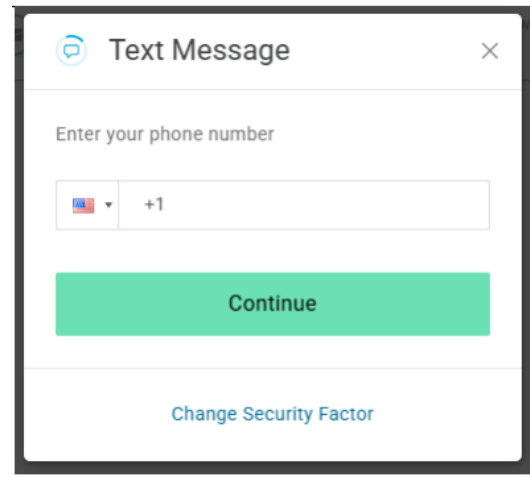
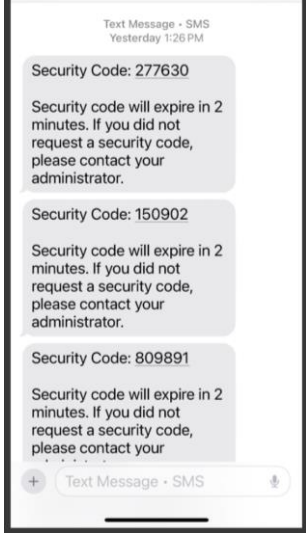
2. Choosing /Setting Up the Authentication Factor

- a. **Email** – If you choose email as your 2-Factor Authentication, you see this screen pop-up.

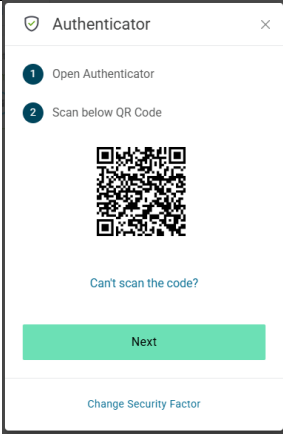
 <p>Email</p> <p>A confirmation code was sent to d*****@*****s.gov</p> <p>Enter your confirmation code</p> <input type="text"/> <p>Continue</p> <p>Try Again</p> <p>Change Security Factor</p>	 <p>OneLogin Email Verification</p> <p>Hi Test User1,</p> <p>We received your request to register this email address as a wvOASIS OneLogin Authentication Factor.</p> <p>To complete email registration, enter the following security code into your browser:</p> <p>838788</p> <p>The security code will expire in 2 minutes. If you didn't submit this registration request, please contact your administrator.</p> <p>© 2025 wvOASIS</p> <p>CAUTION: This email originated from outside the organization. Do not click on links or open attachments unless you recognize the sender and know the content is safe.</p>
---	--

You will receive an email with a six-digit confirmation code. You will need to enter this code on the wvOASIS OneLogin sign on screen to enter the application.

- b. **SMS (Text Message)** -- this option sends a code to your phone each time you request to login.

 <p>Text Message</p> <p>Enter your phone number</p> <p>+1</p> <p>Continue</p> <p>Change Security Factor</p>	 <p>Text Message - SMS Yesterday 1:26 PM</p> <p>Security Code: 277630</p> <p>Security code will expire in 2 minutes. If you did not request a security code, please contact your administrator.</p> <p>Security Code: 150902</p> <p>Security code will expire in 2 minutes. If you did not request a security code, please contact your administrator.</p> <p>Security Code: 809891</p> <p>Security code will expire in 2 minutes. If you did not request a security code, please contact your administrator.</p>
---	---

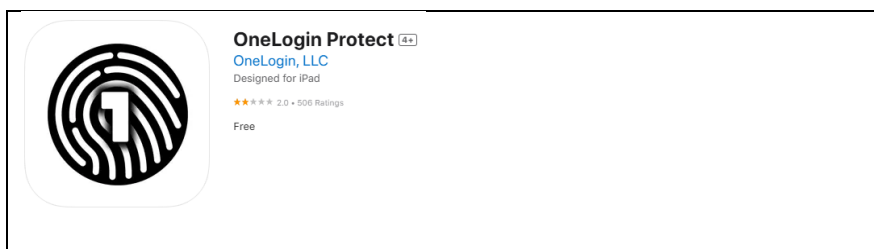
- c. **Authenticator Application** – You can use Google Authenticator or Microsoft Authentication. This option allows you to open the Authenticator App on Your Phone and Scan the QR Code.

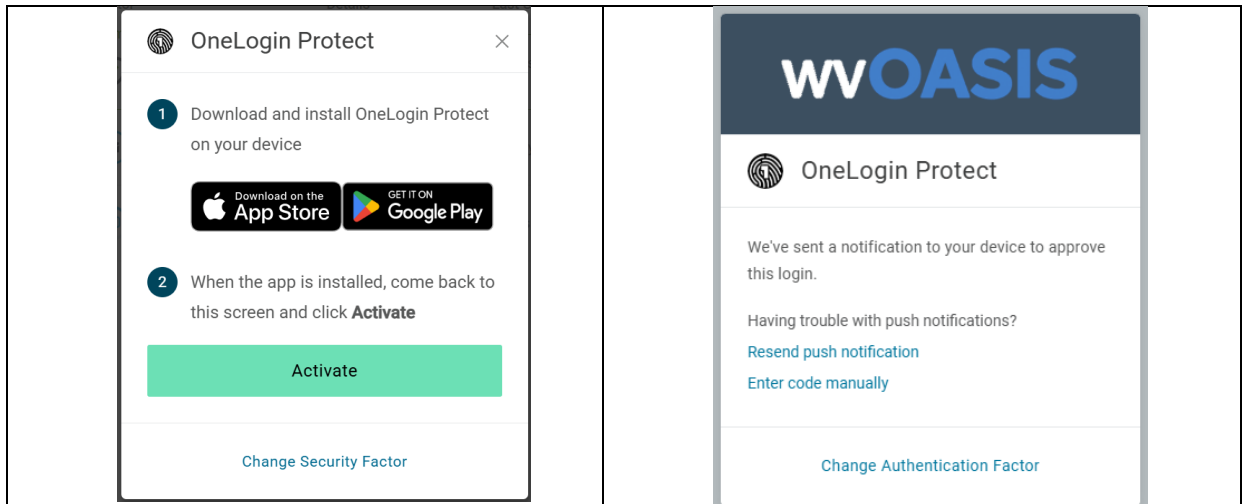
	<ol style="list-style-type: none"> 1. Open the Authenticator application on your phone. Click the “+” in the top right corner. 2. Select “work or school account” 3. Select “Scan QR Code” 4. Use your phone to scan the QR code as shown (left) by the OneLogin application. 5. Your phone will add the OneLogin entry for you as long as it can recognize the QR code.
---	---

- d. **OneLogin Protect** – If you choose this option, you will need to install the OneLogin Protect app to your phone. You will also need to enable Biometrics (Face ID). The app on your phone will register your phone ID by having you scan the QR code in the OneLogin application when this option is chosen. Each time you login to OneLogin and use the OneLogin Protect authentication method, you will confirm with a tap on your phone (Apple Watch) to login.

The OneLogin Protect app provides the convenience of having a “push” notification coming from your phone, to allow you to log into OneLogin. It will also generate a random code each time in case your wireless network / cellphone provider does not enable push notifications. Follow the prompts on the screen on the right, to login.

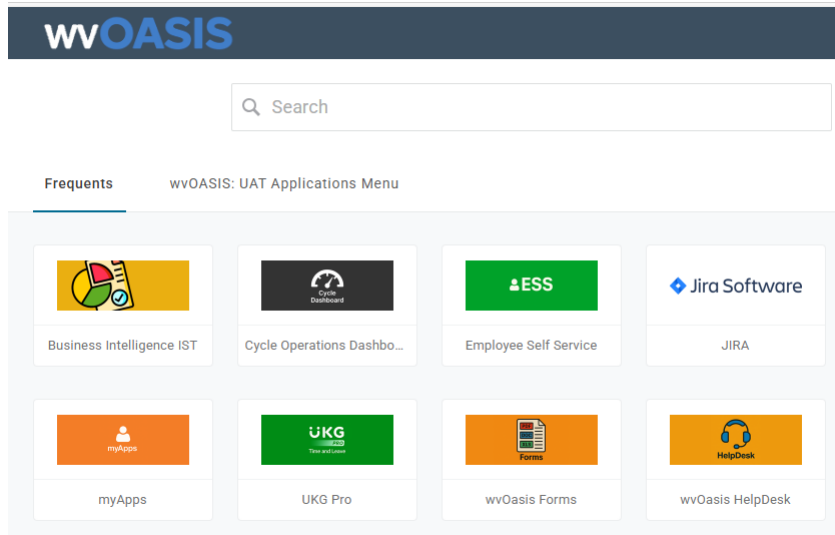
Look for These Symbols for the Correct App to Download:





3. The Main Menu

a. **Frequents Menu.** You will be defaulted to the **Frequents** menu. This displays the most commonly used applications. You may see applications that you have never used. Over time, you will see the most commonly used applications.



b. wvOASIS Applications Menu

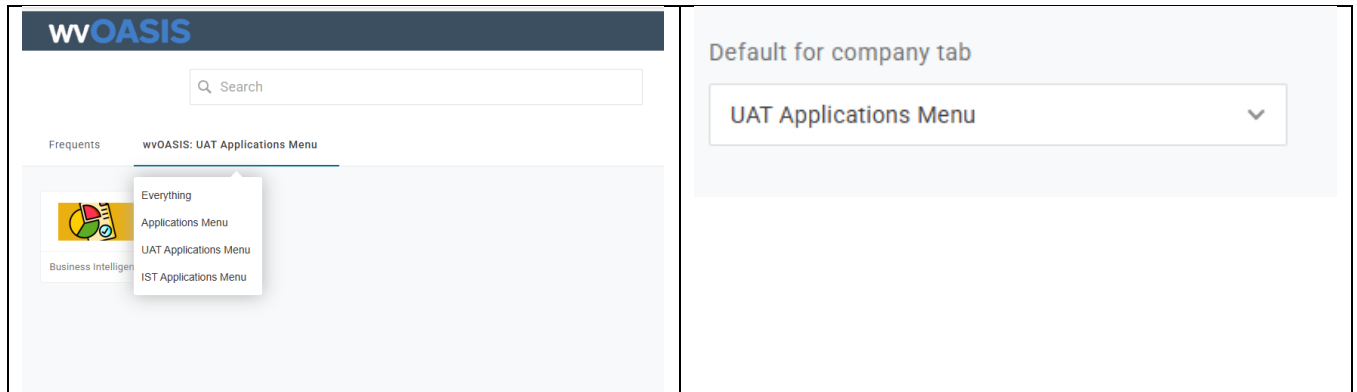
The wvOASIS Applications Menu will be customized according to your security settings.

You will need to click it once to change from “Frequents” to this Application Menu. A second click will display the dropdown menu.

In OneLogin you can set the default Application menu you wish to display. Everyone will have “Everything” and “Applications Menu”. For most people these are the same. A select few will have specific applications on the second menu.

To change the default, visit the Profile section of this document for specific details.

NOTE: The links take you to the same locations (ESS, UKG, etc.) as the current My Apps.

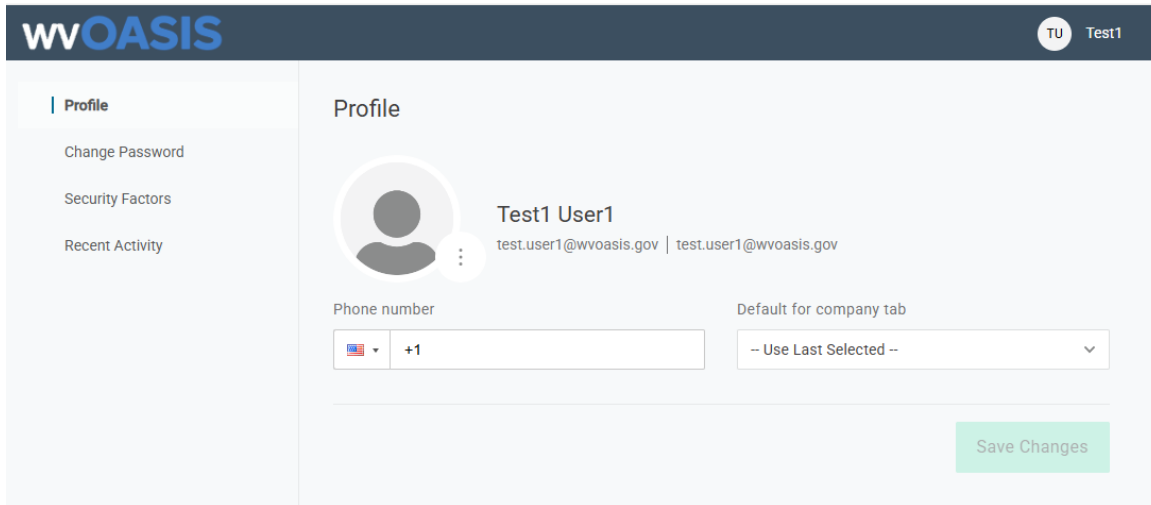


Depending on your role these may have different links.

NOTE: The links take you to the same locations (ESS, UKG, etc.) as the current My Apps.

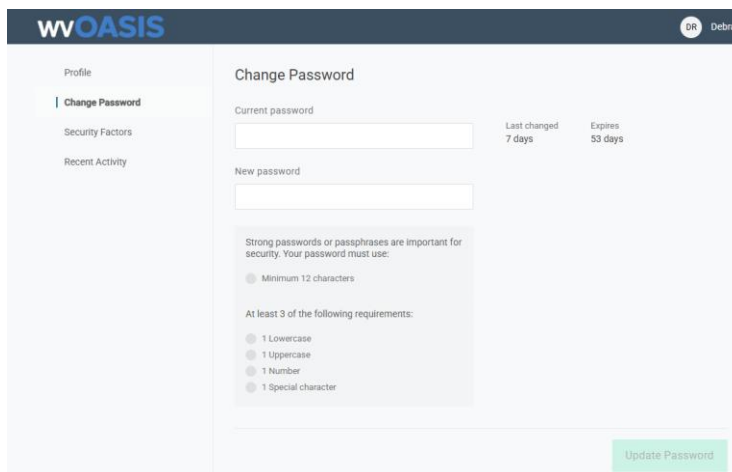
4. The Profile Settings

a. Profile – you can confirm the information is correct (email and phone). You can add a profile picture. You can also choose which menu to always display by setting the “Default for company tab”. Click the green button to save your changes. **Note:** The “wvOASIS” at the top will return you to the main application menu. Click it once. It is a hyperlink.



The screenshot shows the wvOASIS application interface. At the top, the wvOASIS logo is on the left, and a user profile icon with 'TU' and 'Test1' is on the right. The left sidebar contains a 'Profile' section with links to 'Change Password', 'Security Factors', and 'Recent Activity'. The main content area is titled 'Profile' and displays a user profile for 'Test1 User1' with email addresses 'test.user1@wvoasis.gov' and 'test.user1@wvoasis.gov'. Below the profile information, there are two input fields: 'Phone number' with a country code dropdown (showing '+1') and a 'Default for company tab' dropdown (showing '-- Use Last Selected --'). A green 'Save Changes' button is located at the bottom right of the main content area.

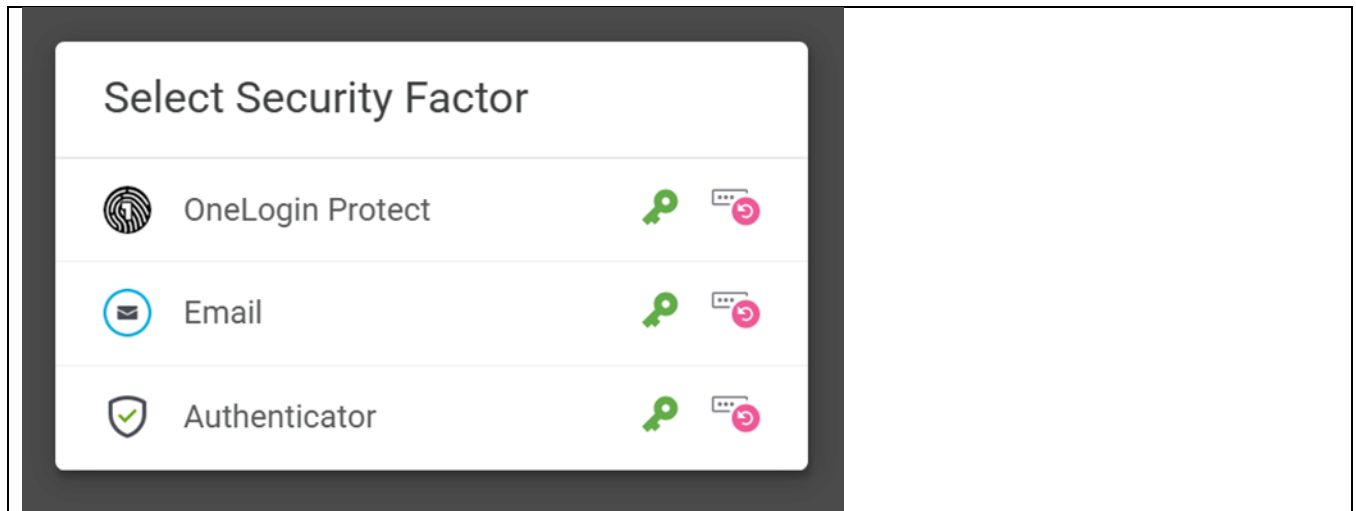
b. Change Password – here you are able to change your OneLogin password. Use the password guidelines for your new password. Click the green button to save your changes. The wvOASIS at the top will return you to the application menu.



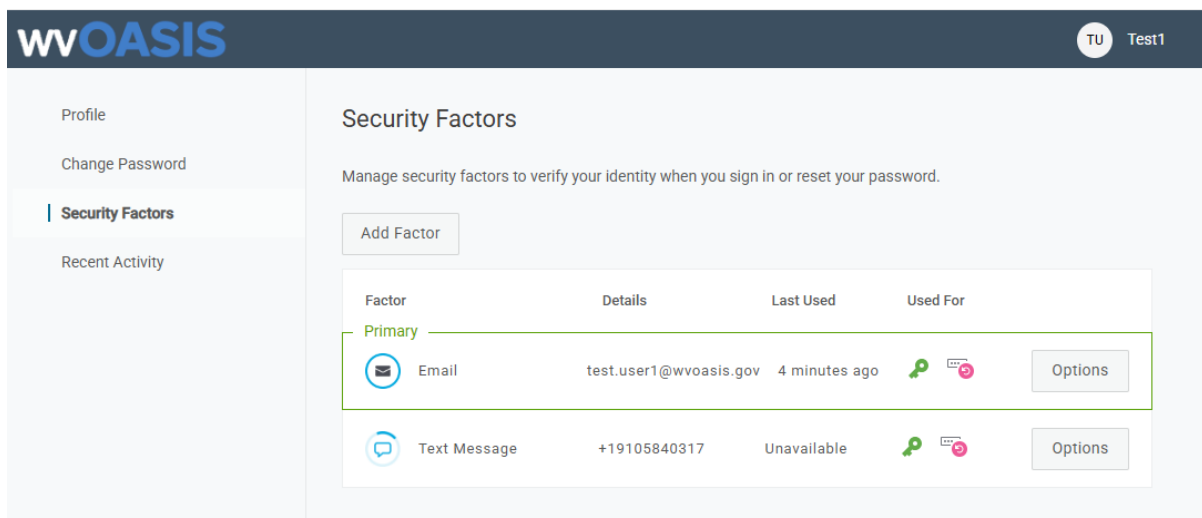
The screenshot shows the wvOASIS application interface for the 'Change Password' section. The top header shows the wvOASIS logo and a user profile icon with 'DR' and 'Debra'. The left sidebar contains a 'Change Password' section with links to 'Profile', 'Security Factors', and 'Recent Activity'. The main content area is titled 'Change Password' and displays two input fields: 'Current password' and 'New password'. To the right of the 'Current password' field, it shows 'Last changed 7 days' and 'Expires 53 days'. Below the input fields, there is a section for password requirements: 'Strong passwords or passphrases are important for security. Your password must use:' followed by a list of requirements: 'Minimum 12 characters', 'At least 3 of the following requirements:', '1 Lowercase', '1 Uppercase', '1 Number', and '1 Special character'. A green 'Update Password' button is located at the bottom right of the main content area.

c. Security Factors – the next item will allow you to manage your authentication factors. Here you can add an authentication factor. You can change your primary authentication factor.

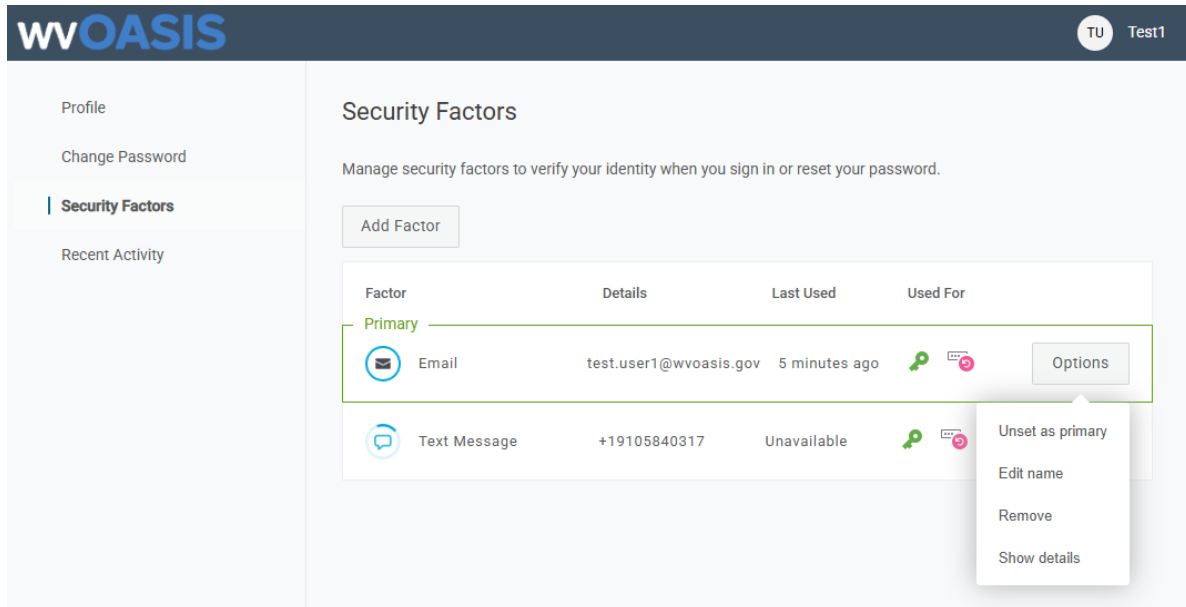
Click the Add Factor button to begin setting up a new factor.



A green outline with the word Primary is around the factor that is your primary authentication factor. The wvOASIS at the top will return you to the application menu.



For each item the Options button provides additional information.



WVOASIS TU Test1

Profile
Change Password
Security Factors
Recent Activity

Security Factors

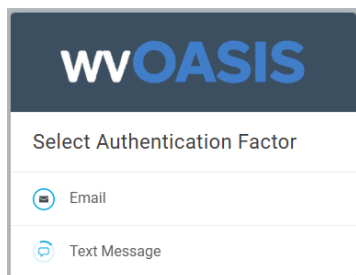
Manage security factors to verify your identity when you sign in or reset your password.

Add Factor

Factor	Details	Last Used	Used For
Primary Email	test.user1@wvoasis.gov	5 minutes ago	Options
Text Message	+19105840317	Unavailable	Options

- Unset as primary
- Edit name
- Remove
- Show details

If you chose “Unset as primary”, and you do not choose and set another Security Factor as your primary, you will be prompted at your next login to choose an Authentication Factor. You may actually prefer this to be the case if you want to choose the authentication method at the time of login. This screen shows you what you will see at Login if you do not set a Primary Authentication Factor.

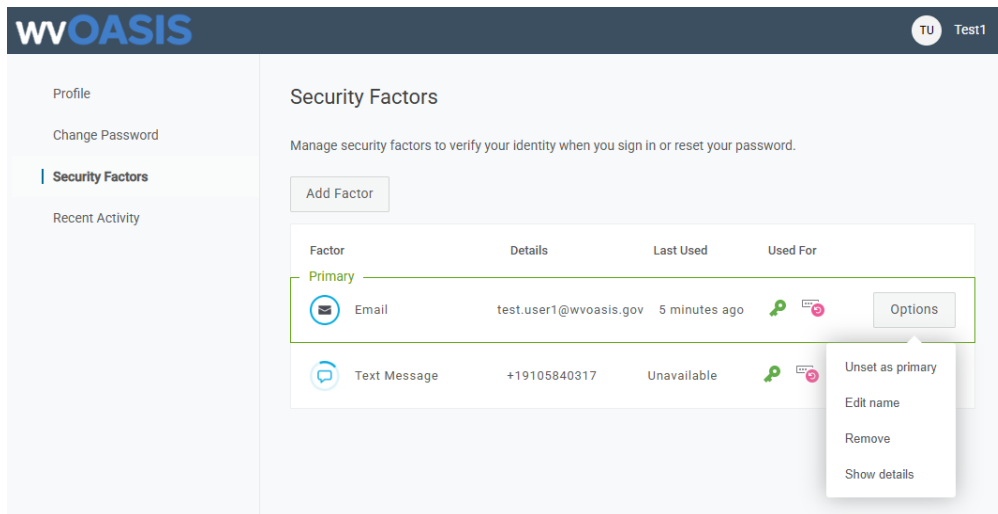


WVOASIS

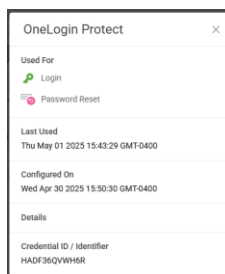
Select Authentication Factor

- Email
- Text Message

From this screen again Security Factors, if you select Show Details:



It brings up this view:



d. Recent Activity – the next item on the left side menu will allow you to view the history of activity within your OneLogin access. The top row has four tabs (All / Login / Password / Factors). If you want to only see login details, click the login tab. Otherwise the All tab has all log entries. For each specific entry you can click on the > at the right side of each row to display more details as shown in the second image. The details for each type of activity will vary.

Profile

Change Password

Security Factors

Recent Activity

Recent Activity

All	Login	Password	Factors
Event	Browser/Device		Location/Time
Login	Chrome Windows 10	129.71.11.68 3 minutes ago	>
Login	Chrome Windows 10	129.71.11.68 8 days ago	>
Logged Out	Unknown Unknown	129.71.11.68 8 days ago	>
Login	Chrome Windows 10	129.71.11.68 8 days ago	>
Login	Chrome Windows 10	129.71.11.68 8 days ago	>
Security Factor Added	Email	129.71.11.68 8 days ago	>
Login Failed	Unavailable	74.195.4.45 8 days ago	>
Password Changed	Unavailable	74.195.4.45 8 days ago	>

Recent Activity

Browser/Device

Chrome

Windows 10

Location

173.80.123.62

Time

Fri Apr 25 2025 08:59:40 GMT-0400 (4 hours ago)

Event Type

USER_LOGGED_INTO_ONELOGIN

Event UUID

a5b50aef-00c8-4bc0-82eb-6b18321036d4








Event Useragent

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 Edg/135.0.0.0

5. Logging In to One Login

a. Multiple Security Factors – once you have more than one Security Factor set up, your initial log on screen to One Login, will appear differently. At the bottom you will be able to change your authentication factor by clicking on the Change Authentication Factor link.

It is very important to set up at least two Authentication Factors, so that you have a backup method for gaining access. Suppose you have misplaced your phone and need to get in. By having email as your secondary authentication factor, you can change to it as your temporary authentication factor.

  Text Message Enter your code <input type="text"/> Show Continue Having trouble? Resend SMS code Change Authentication Factor	 Select Authentication Factor  OneLogin Protect  Authenticator  OneLogin SMS  Email
--	---

For Questions:

wvOASIS HelpDesk

1-855-666-8823 (Mon -Fri 7am to 5pm)

helpdesk@wvoasis.gov