

Texas Digital Identity Solution (TDIS) Portal – MFA Registration

Last Updated: 2/21/2024



Table of Contents

1	Introduction.....	3
1.1	Procedure Purpose.....	3
1.2	Scope.....	3
1.3	Prerequisites	3
2	MFA Registration Guide	4
2.1	Accessing the MFA Registration Screen.....	4
2.2	Phone Number Registration.....	5
2.3	Microsoft Authenticator App Registration.....	6
2.3.1	Microsoft Authenticator Registration for New App Users	7
2.3.2	Microsoft Authenticator Registration for Existing App Users.....	9
2.4	Google Authenticator App Registration	12
2.4.1	Google Authenticator Registration for New App Users.....	13
2.4.2	Google Authenticator Registration for Existing App Users	16
2.5	Security Key Registration.....	18
3	Appendices	21
3.1	Advanced Security Devices Information	21
3.2	Phone Number Information	21

1 Introduction

1.1 Procedure Purpose

This guide provides an overview of how to register MFA methods in the Texas Digital Identity Solution Portal.

1.2 Scope

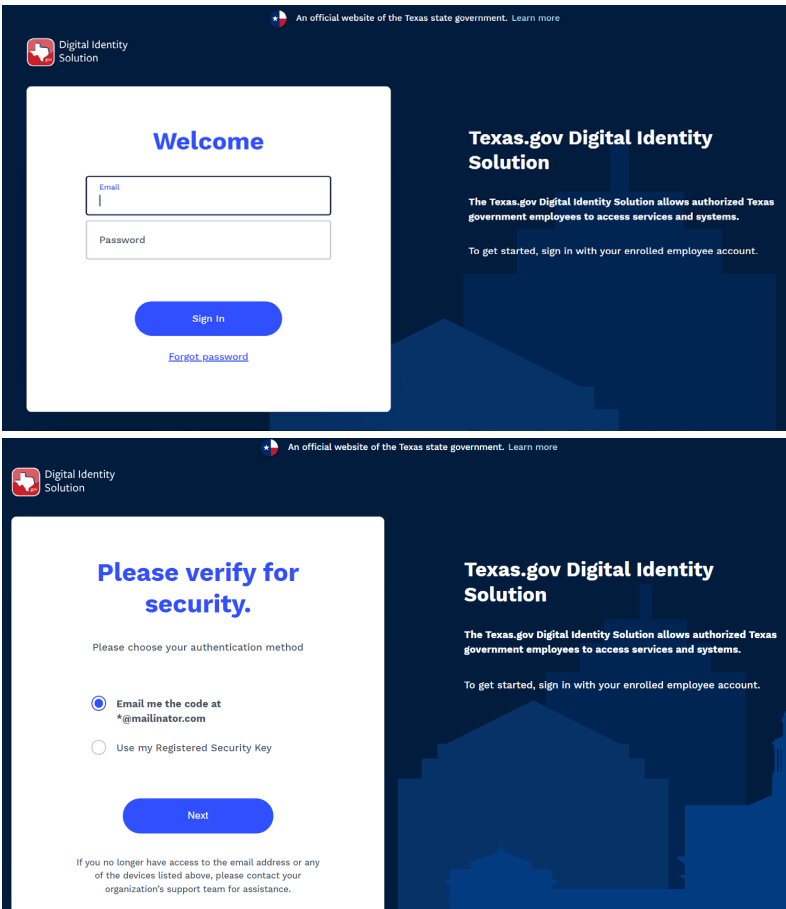
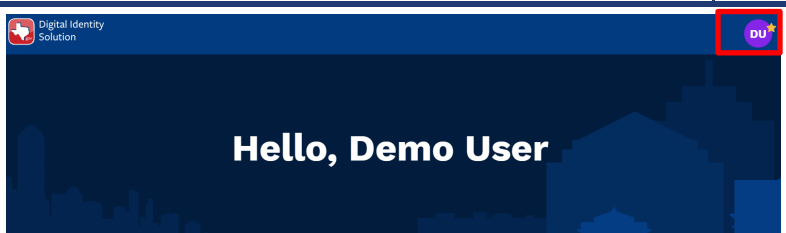
This guide is written for customers of the Texas Digital Identity Solution. It explains how to add additional MFA methods to a user's profile in the [TDIS Portal](#).

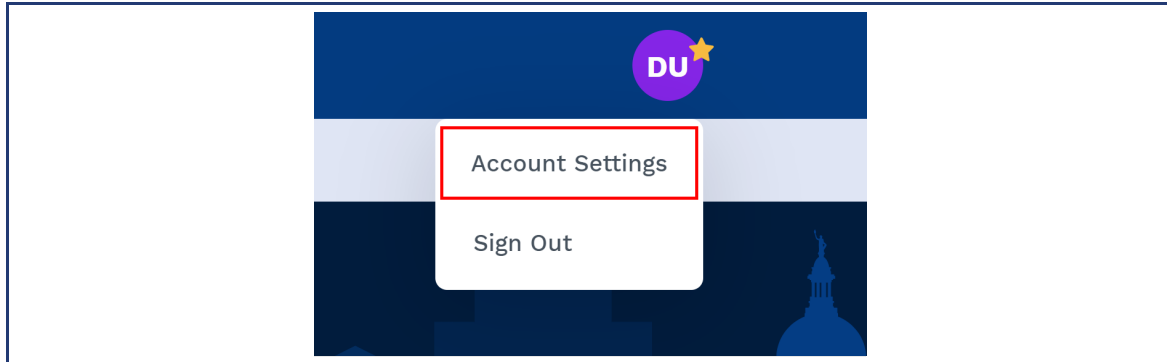
1.3 Prerequisites

Currently, the Texas Digital Identity Solution Portal supports the Microsoft Authenticator App and Google Authenticator App. These apps can be found on a mobile phone's app store by searching "Microsoft Authenticator App" or by searching "Google Authenticator App." There should be no cost associated with downloading either of these applications. An organization might have requirements on which Authenticator App should be used. Please check with the Organization Help Desk to verify.

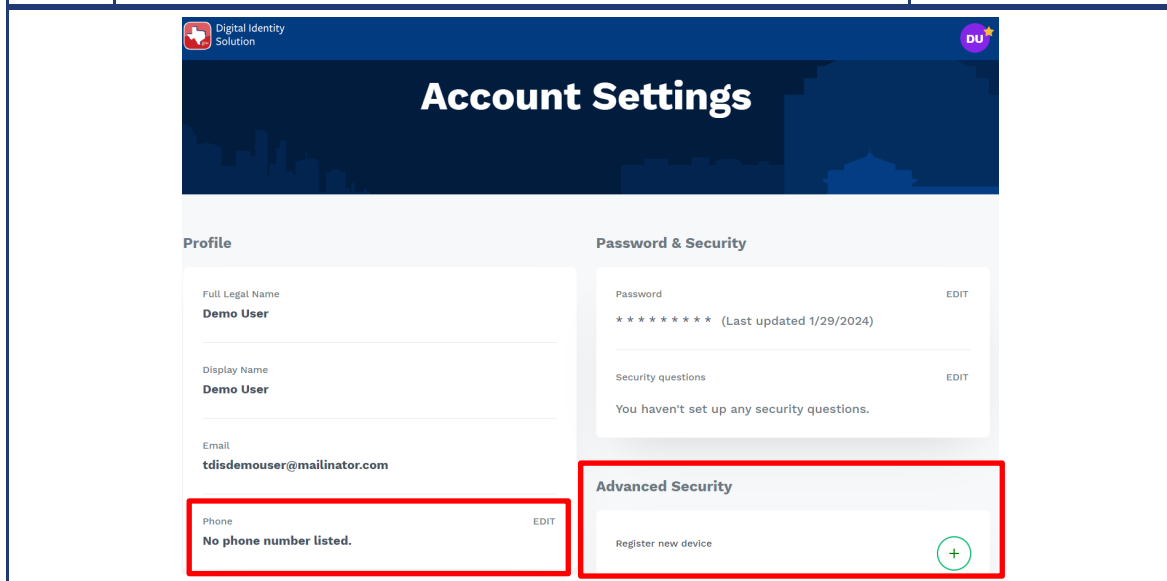
2 MFA Registration Guide

2.1 Accessing the MFA Registration Screen

Step	Description	Owner
1.	Login to the TDIS Portal .	User
		
2.	To navigate to the Self-Service Dashboard, select your avatar (purple circle with initials) in the upper right-hand corner of the Employee Dashboard.	User
		
3.	A submenu will display. Select Account Settings .	User

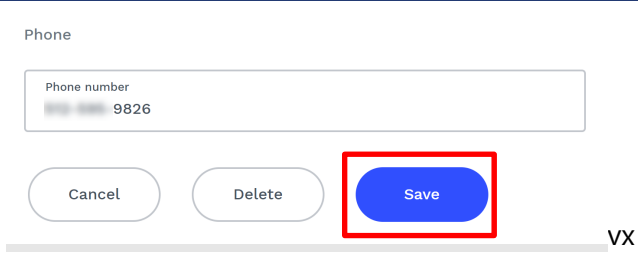


4.	From the Account Settings screen, you can add and/or update your phone number and Advanced Security devices.	User
----	---	------



2.2 Phone Number Registration

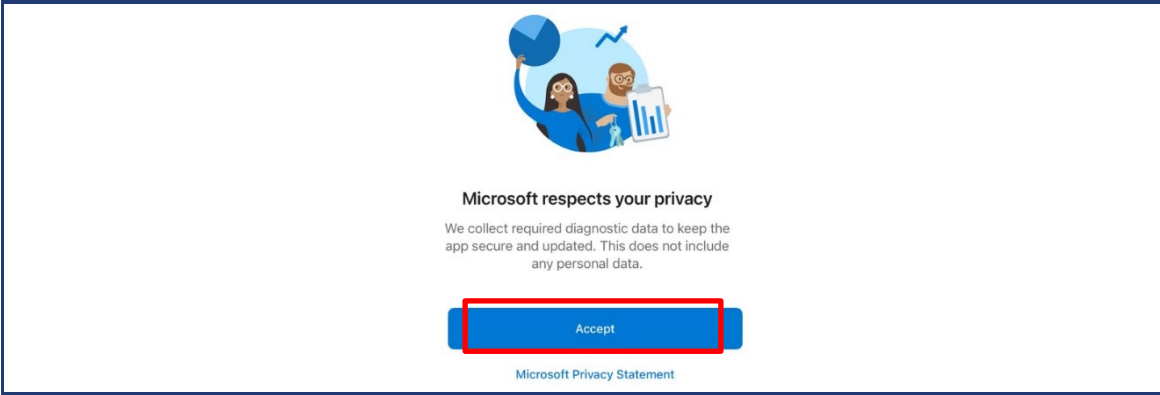
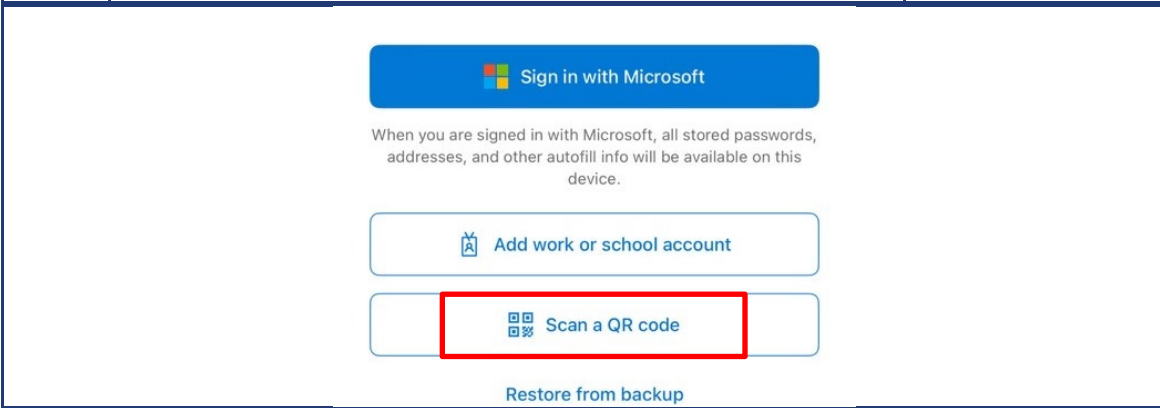
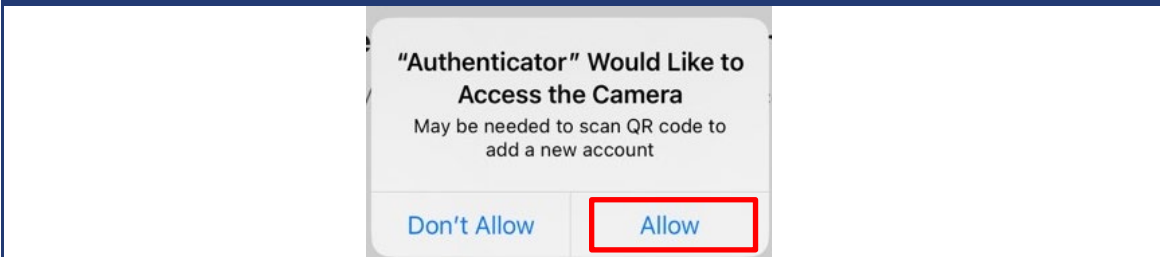
Step	Description	Owner
	Login to TDIS Portal . Proceed to your Account Settings page. Under Profile , select the Edit button in the section labeled Phone .	User

		
5.	Enter your 10-digit phone number into the phone number field (e.g., XXX-XXX-XXXX). Select Save to proceed.	User
		
6.	Next, enter the One-Time Passcode (OTP) into the One-Time Passcode field. Select Submit to proceed.	User
		
7.	Your phone number is added to your account.	User

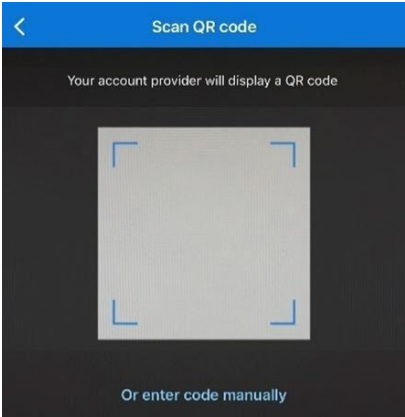
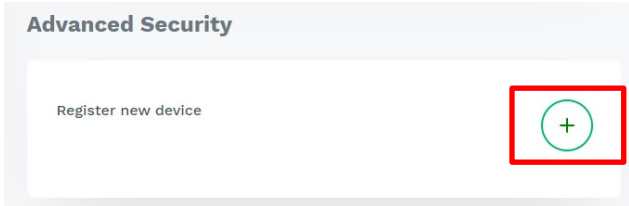
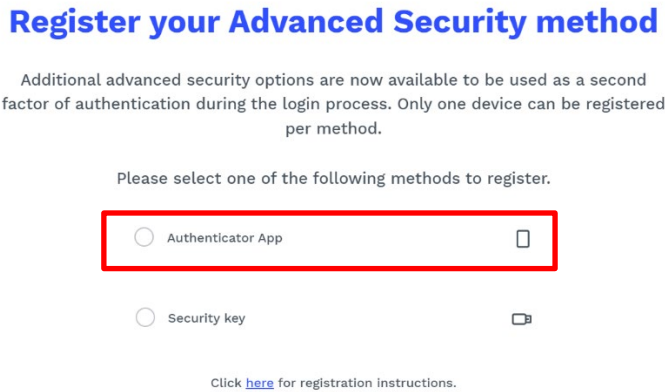
2.3 Microsoft Authenticator App Registration

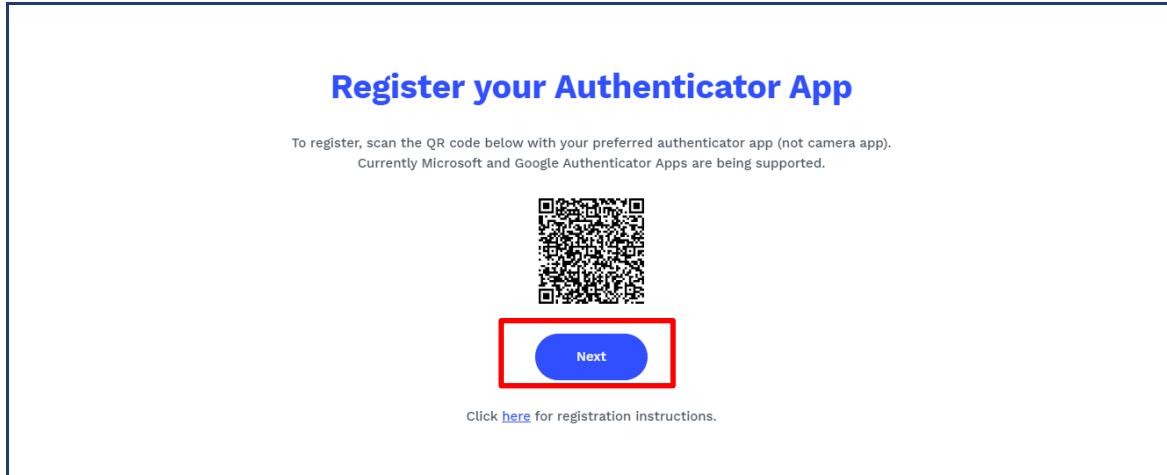
2.3.1 Microsoft Authenticator Registration for New App Users

Please use the following steps if this is your first time downloading Microsoft Authenticator. If you already have the Authenticator App set up for another website’s MFA purposes, skip to 2.3.2 Microsoft Authenticator Registration for Existing App Users.

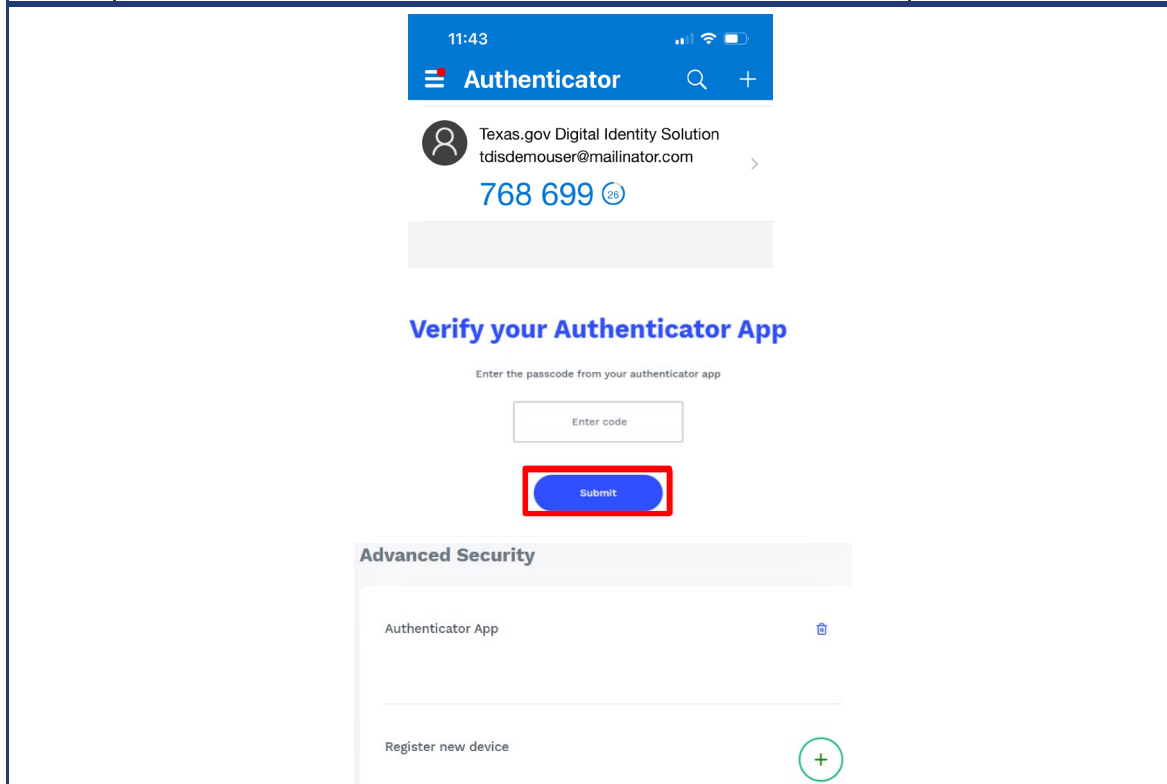
Step	Description	Owner
	<p>After opening your newly downloaded Microsoft Authenticator App, you may be asked to agree to a privacy statement. Once you have read the privacy statement, select I agree.</p>	User
 <p>The screenshot shows a privacy statement from Microsoft. At the top, there is an illustration of two people looking at a screen. Below the illustration, the text reads: "Microsoft respects your privacy. We collect required diagnostic data to keep the app secure and updated. This does not include any personal data." At the bottom, there is a blue button labeled "Accept" which is highlighted with a red rectangular box.</p>		
8.	<p>Select Scan a QR Code.</p>	User
 <p>The screenshot shows the Microsoft sign-in screen. At the top, there is a blue button labeled "Sign in with Microsoft". Below it, there is a text block: "When you are signed in with Microsoft, all stored passwords, addresses, and other autofill info will be available on this device." Below the text, there are three buttons: "Add work or school account", "Scan a QR code", and "Restore from backup". The "Scan a QR code" button is highlighted with a red rectangular box.</p>		
9.	<p>After selecting the QR code option, you will be asked to provide access to the Microsoft Authenticator App for your phone’s camera. Select OK.</p>	User
 <p>The screenshot shows a system dialog box titled "Authenticator Would Like to Access the Camera". The text inside reads: "May be needed to scan QR code to add a new account". At the bottom, there are two buttons: "Don't Allow" and "Allow". The "Allow" button is highlighted with a red rectangular box.</p>		

Texas Digital Identity Solution (TDIS) Portal – MFA Registration

10.	A window will pop up ready for you to scan a QR code.	User
		
11.	Proceed to your Account Settings page on TDIS Portal . Under Advanced Security , select the green '+' .	User
		
12.	Select Authenticator App.	User
		
13.	Scan the QR code provided on the TDIS Portal . Select Next .	User



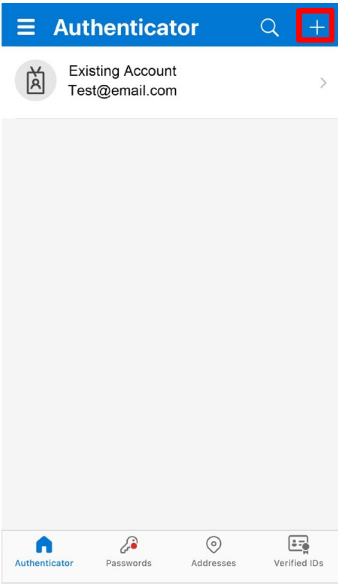
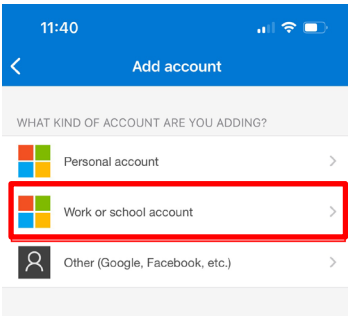
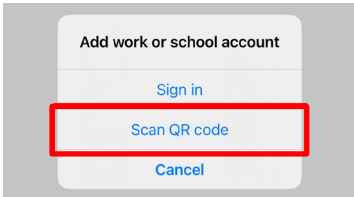
14.	After selecting next on the TDIS Portal , type in your Time-Based Passcode from your Authenticator App into the code prompt on the portal and select Submit . You will then be able to see your device under the Advanced Security Settings in Account Settings .	User
-----	--	------

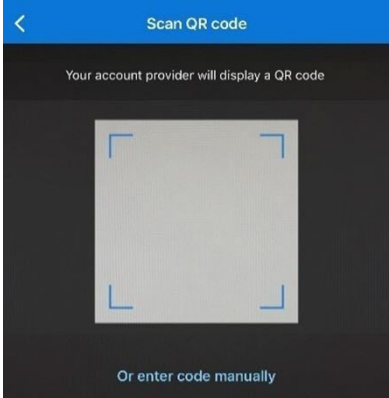
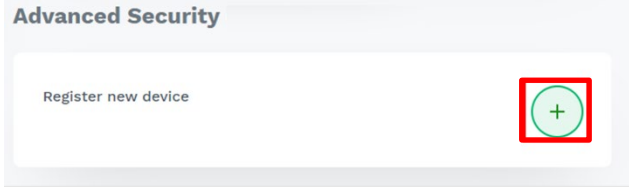
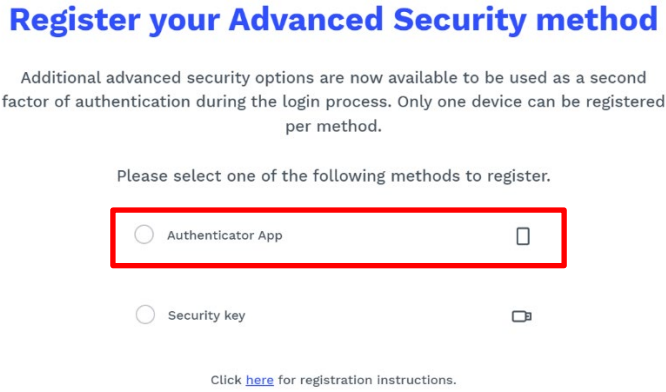



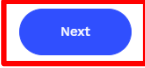
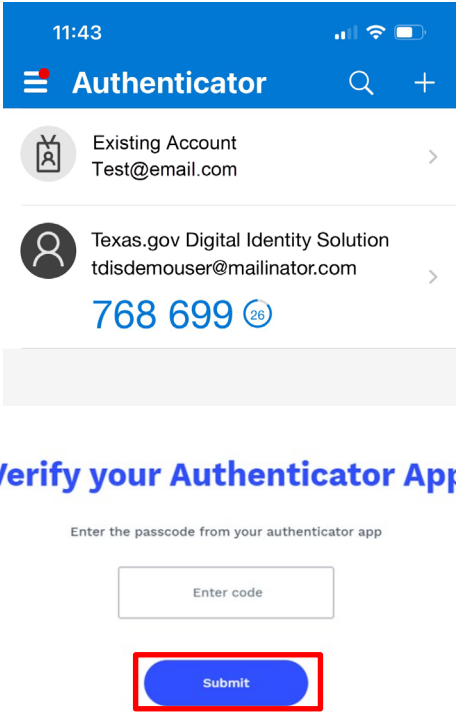
2.3.2 Microsoft Authenticator Registration for Existing App Users

Please use the following steps if you already have the Authenticator App set up for another website’s MFA purposes. **Note:** You can only have one [TDIS Portal](#) account.

Texas Digital Identity Solution (TDIS) Portal – MFA Registration

Step	Description	Owner
	To add an account to your Authenticator App, select the “+” sign in the upper right-hand corner.	User
		
15.	This will prompt you to choose what kind of account you are adding. We recommend selecting Work or School Account .	User
		
16.	Select Scan QR Code .	User
		
17.	A window will pop up ready for you to scan a QR code.	User

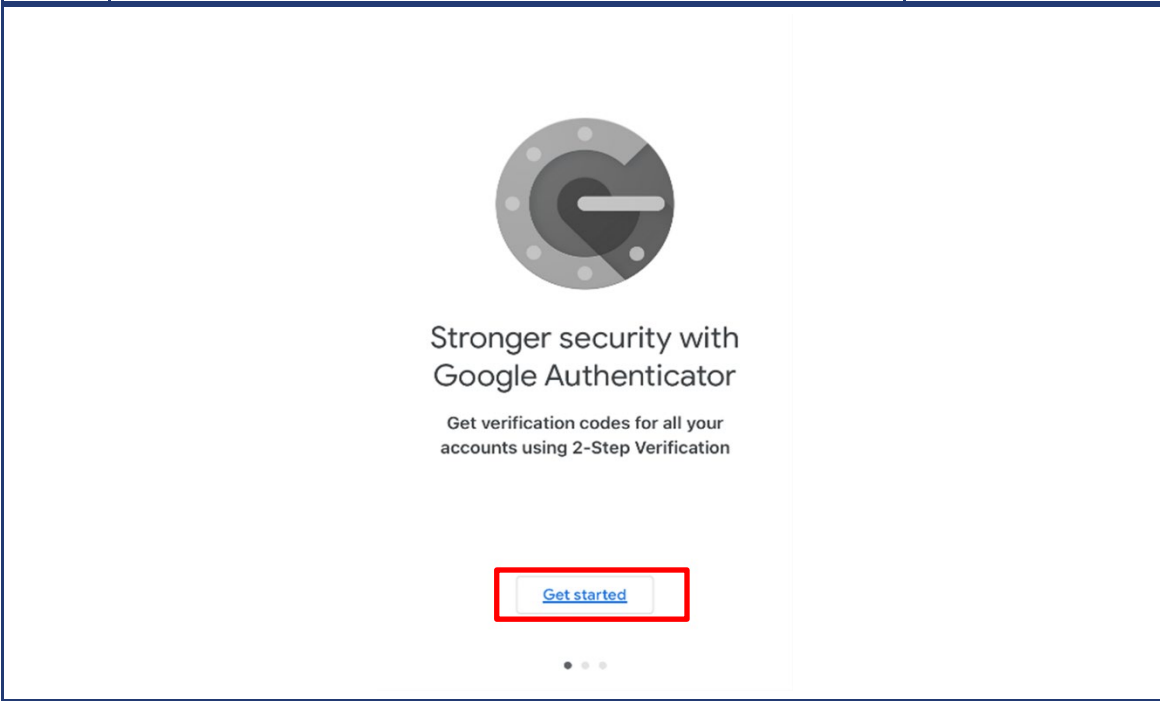
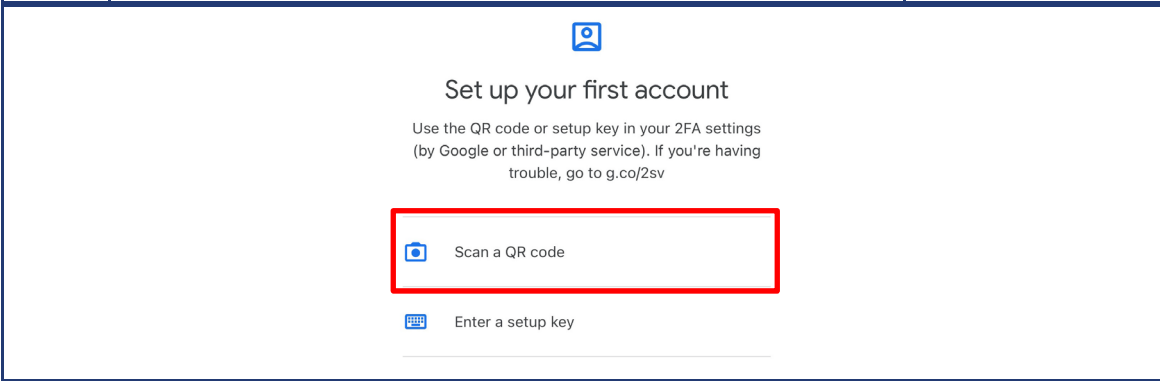
Step	Description	Owner
		
18.	<p>Proceed to your Account Settings page on TDIS Portal. Under Advanced Security, select the green '+'.</p>	User
		
19.	<p>Select Authenticator App.</p>	User
		
20.	<p>Scan the QR code provided on the TDIS Portal. Select Next.</p>	User

Step	Description	Owner
	<p style="text-align: center;">Register your Authenticator App</p> <p style="text-align: center;">To register, scan the QR code below with your preferred authenticator app (not camera app). Currently Microsoft and Google Authenticator Apps are being supported.</p> <div style="text-align: center;">   </div> <p style="text-align: center;">Click here for registration instructions.</p>	
21.	<p>After selecting next on the TDIS Portal, type in your Time-Based Passcode from your Authenticator App into the code prompt on the portal and select Submit. You will then be able to see your device under the Advanced Security Settings in Account Settings.</p>	User
		

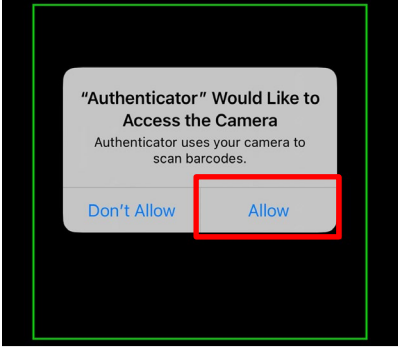
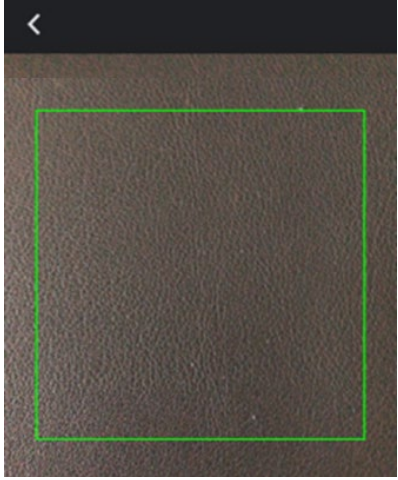
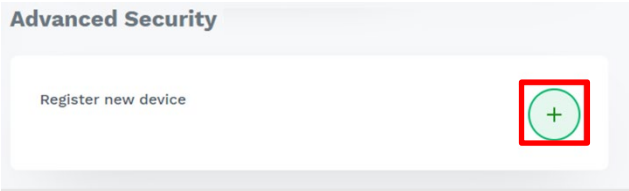
2.4 Google Authenticator App Registration

2.4.1 Google Authenticator Registration for New App Users

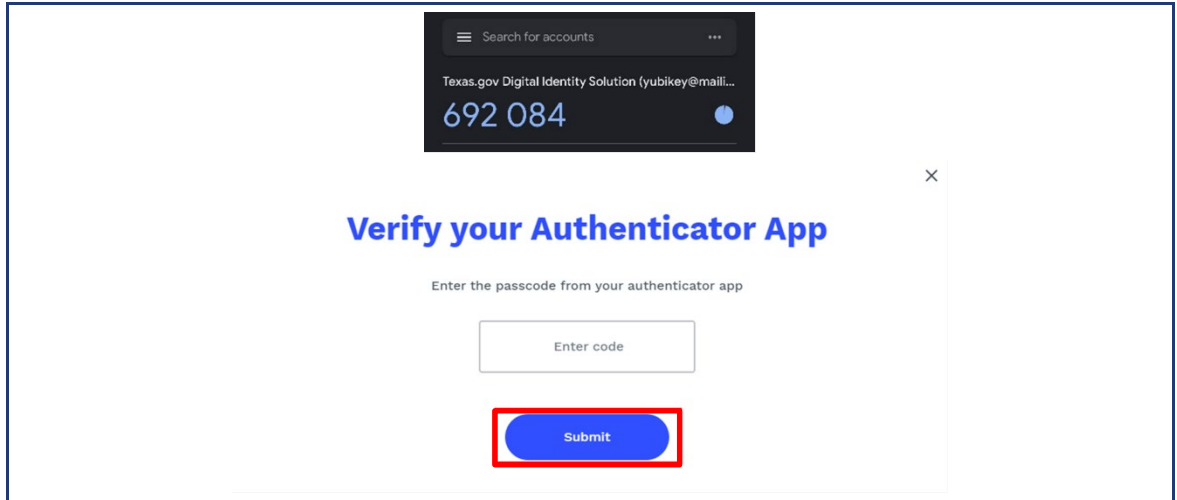
Please use the following steps if this is your first time downloading Google Authenticator. If you already have the Authenticator App set up for another website’s MFA purposes, please skip to 2.4.2 Google Authenticator Registration for Existing App Users.

Step	Description	Owner
	After opening your newly downloaded Google Authenticator App, select Get Started to begin configuring your app.	User
		
22.	Select Scan a QR code.	User
		
23.	After selecting the QR code option, you will be asked to provide access to Google Authenticator App for your phone’s camera. Select Allow .	User

Texas Digital Identity Solution (TDIS) Portal – MFA Registration

		
24.	A window will pop up ready for you to scan a QR code.	User
		
25.	Proceed to your Account Settings page on TDIS Portal . Under Advanced Security , select the green '+' .	User
		
26.	Select Authenticator App .	User

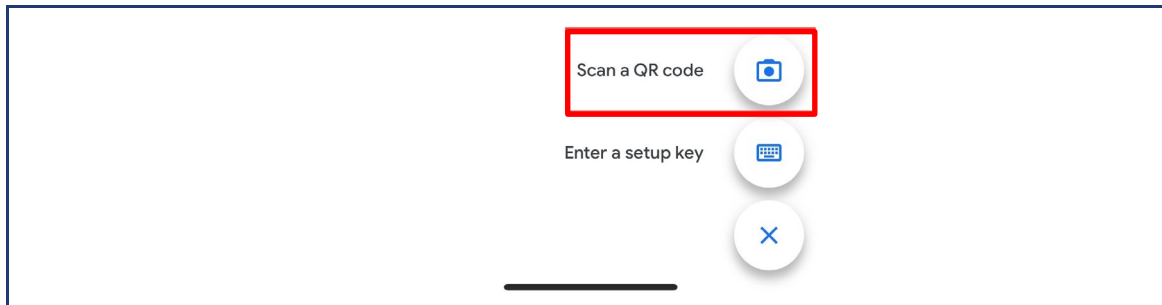
<div style="text-align: center;"> <h3>Register your Advanced Security method</h3> <p>Additional advanced security options are now available to be used as a second factor of authentication during the login process. Only one device can be registered per method.</p> <p>Please select one of the following methods to register.</p> <div style="border: 2px solid red; padding: 5px; display: inline-block; margin-bottom: 10px;"> <input type="radio"/> Authenticator App </div> <input type="radio"/> Security key </div> <p style="text-align: center; font-size: small;">Click here for registration instructions.</p>		
27.	Scan the QR code provided on the TDIS Portal . Select Next .	User
<div style="text-align: center;"> <h3>Register your Authenticator App</h3> <p>To register, scan the QR code below with your preferred authenticator app (not camera app). Currently Microsoft and Google Authenticator Apps are being supported.</p> <div style="border: 2px solid red; padding: 5px; display: inline-block; margin-top: 10px;"> Next </div> <p style="text-align: center; font-size: small;">Click here for registration instructions.</p> </div>		
28.	After selecting Next on the TDIS Portal , type in your Time-Based Passcode from your Authenticator App into the code prompt on the portal and select Submit . You will then be able to see your device under the Advanced Security Settings in Account Settings .	User



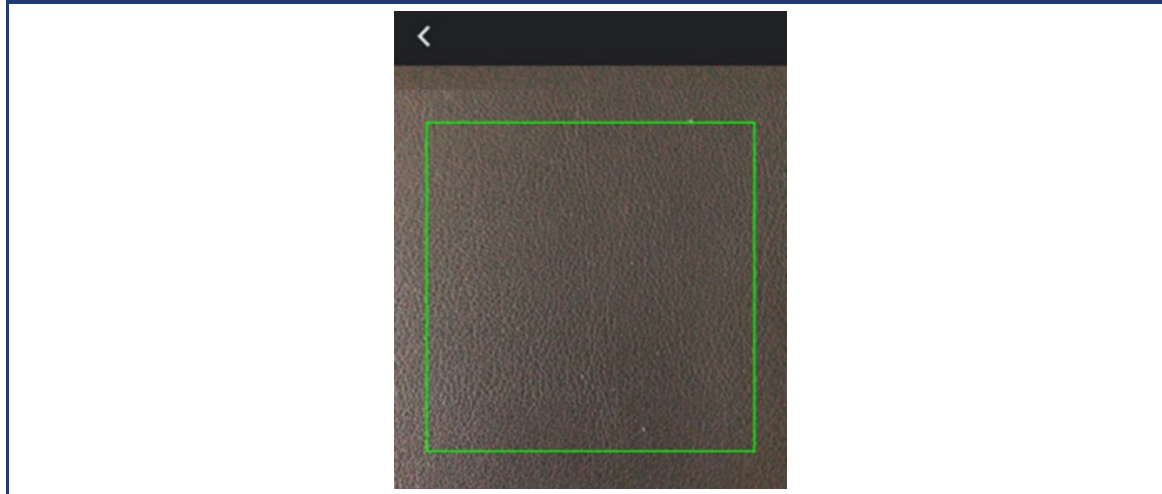
2.4.2 Google Authenticator Registration for Existing App Users

Please use the following steps if you already have the Authenticator App set up for another website’s MFA purposes.

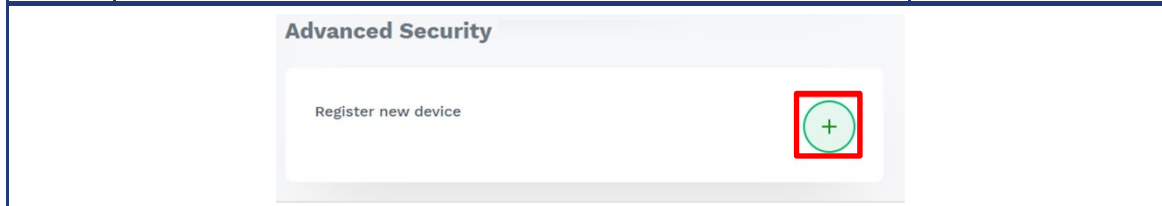
Step	Description	Owner
	To add an account to your Authenticator app, select the multi-colored '+' at the bottom of your screen.	User
29.	Select Scan a QR code.	User



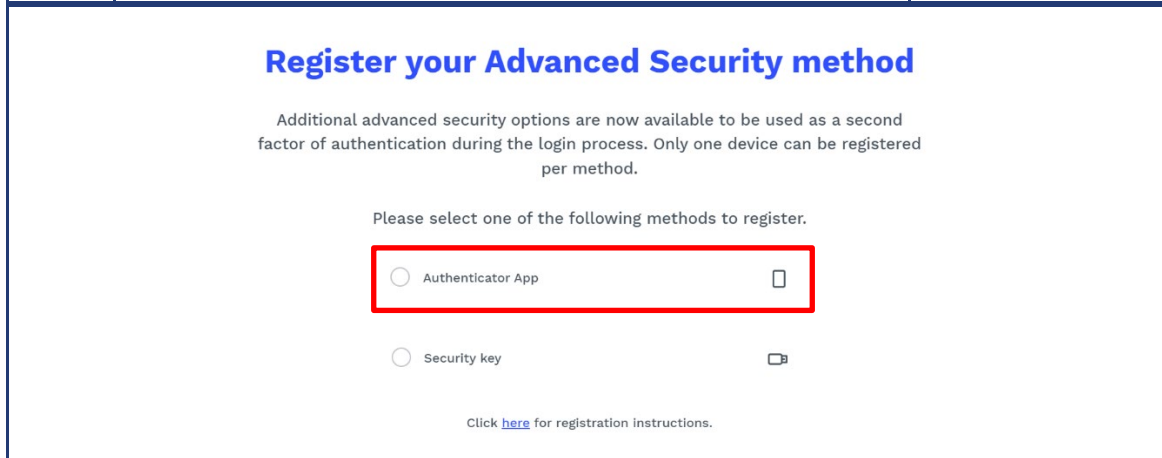
30.	A window will pop up ready for you to scan a QR code.	User
-----	---	------



31.	Proceed to your Account Settings page on TDIS Portal . Under Advanced Security , select the green '+' .	User
-----	--	------




32.	Select Authenticator App .	User
-----	-----------------------------------	------



33.	Scan the QR code provided on the TDIS Portal . Select Next .	User
-----	---	------

Register your Authenticator App

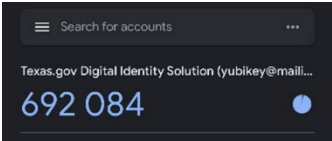
To register, scan the QR code below with your preferred authenticator app (not camera app).
Currently Microsoft and Google Authenticator Apps are being supported.



Next

Click [here](#) for registration instructions.

34.	After selecting Next on the TDIS Portal , type in your Time-Based Passcode from your Authenticator App into the code prompt on the portal and select Submit . You will then be able to see your device under the Advanced Security Settings in Account Settings .	User
-----	---	------



Verify your Authenticator App

Enter the passcode from your authenticator app

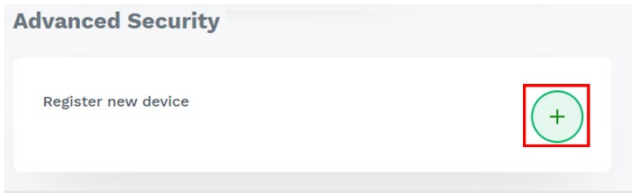
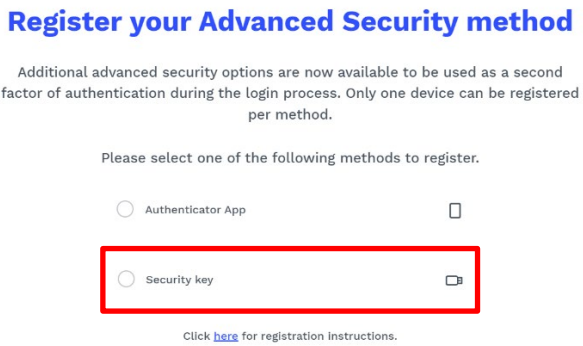

Enter code

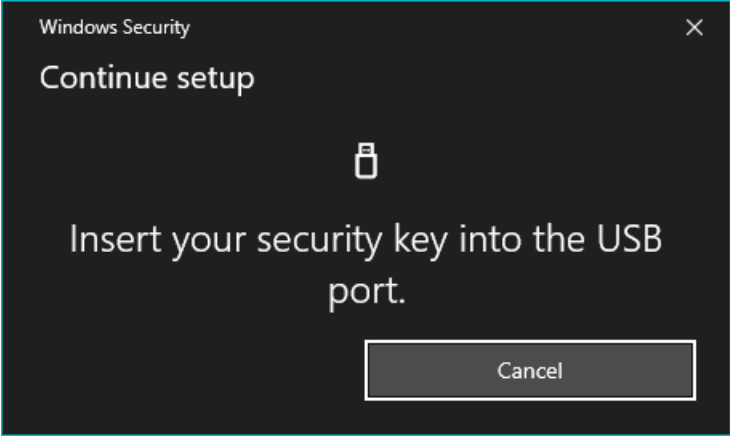
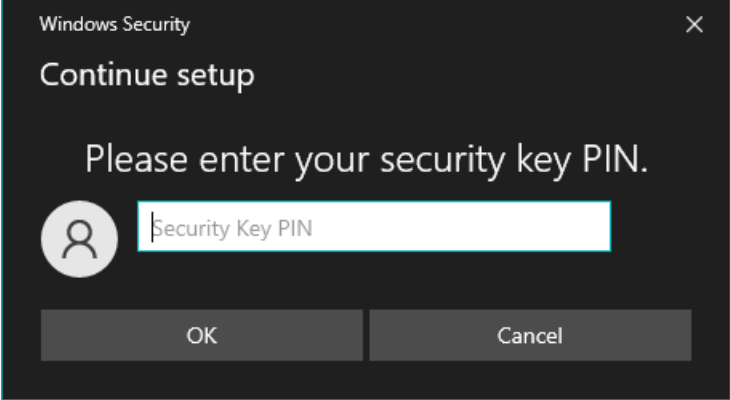
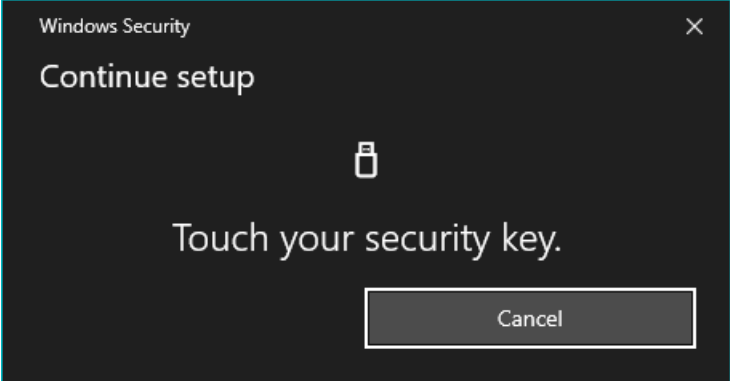
Submit

2.5 Security Key Registration

Step	Description	Owner
	Login to TDIS Portal . Proceed to your Account Settings page. Under Advanced Security , select the green '+' . Note: TDIS is compatible with both USB and USB-C Security Keys.	User

Texas Digital Identity Solution (TDIS) Portal – MFA Registration

Step	Description	Owner
		
35.	Select Security Key .	User
		
36.	A dialogue box should appear asking you to confirm security key setup. Select OK .	User
		
37.	A dialogue box should appear instructing you to insert the security key into the USB port of your laptop or computer.	User

Step	Description	Owner
		
38.	<p>Once the device is detected, you may be prompted to enter a security pin. Choose any pin number that you will remember. This will not be used during MFA and is prompted from the device itself. Select OK after entering.</p>	User
		
39.	<p>Another dialogue box should appear instructing you to touch the security key. You will then be able to see your device under the Advanced Security Settings in Account Settings.</p>	User
		

3 Appendices

3.1 Advanced Security Devices Information

- A user can only have up to one (1) Security Key (e.g., Yubikey) and one (1) Authenticator App registered to their account.
- TDIS currently supports Microsoft and Google Authenticator Apps.
- A user can only delete an Advanced Security device if they are logged into TDIS with the same advanced security device for that login period. For instance, if a user uses their Authenticator App to login to TDIS, they will be able to delete that device from their account.
- If a user loses access to their device, they will need to contact their Delegated Admin to have it removed from their account.
- Advanced Security devices extend across the entire TDIS Platform.
- Any issues concerning the physical security keys or a user's app will need to be redirected to the proper third-party (i.e., Microsoft, Google, Yubico, etc.).
- Advanced Security devices are only available for login, the user cannot use them for Forgot Password self-service.

3.2 Phone Number Information

- Users must use a device that can receive SMS messages; a landline cannot be used.