

Multi-Factor Authentication Changes Quick Reference Guide

Version 1.24

Last Updated November 2024

© 2024 Verizon. All Rights Reserved. The Verizon names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.



Version History

Version	Date	Description of Changes
1.24	November 2024	Initial Document

Table of Contents

Version History	2
Table of Contents	3
Proprietary Statement	4
Introduction.....	5
Frequently Asked Questions (FAQs)	5
Request Yubikey	6
Order Yubikey.....	7
Register Yubikey	10
Request DUO Mobile	15
DUO Mobile Setup.....	16
Request PIV/CAC.....	20
Customer Support.....	22
WITS 3 Help Desk	22

Proprietary Statement

VERIZON CONFIDENTIAL: The enclosed material is PROPRIETARY AND CONFIDENTIAL and exempt from public release pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552(b)(4). Notify Verizon prior to responding to any FOIA request for this material.

These materials, whether provided to you in writing or verbally, are the sole property of Verizon and are not to be used other than as described in these materials or to evaluate Verizon's services or both. Do not circulate these materials throughout your organization to your employees unless they have a need for this information or to any third parties without Verizon's express written permission.

Introduction

To increase security and compliance with GSA POAM Verizon OSS-C-2021-055 changes are being made to the multi-factor authentication/sign-in process for the WITS 3 portal.

Verizon has a requirement to migrate from email-based one-time passcodes (OTP). OTP is no longer compliant with NIST 800-63 Digital Identity guidelines. With a migration from OTP, Verizon has chosen to implement Yubikeys, DUO and PIV cards. OTP is deprecated and not compliant. If an agency chooses to accept the security risk of continuing to use email-based OTP, Verizon will continue to support the agency's desires with documented acceptance of risk.

Link the the FAQ for 800-63 requirements: pages.nist.gov/800-63-FAQ/#q-b11

Current authentication requires the use of a One Time Passcode (OTP) via email. Starting the week of **February 17, 2025**, the new authentication process requires the selection of one of the following:

- **Yubikey** – Yubikey is a USB hardware-based security device that inserts into the computer. You have the option to choose either a USB-A (YubiKey 5 NFC FIPS), USB-C (YubiKey 5C NFC FIPS) or USB-C (YubiKey 5C FIPS) device to be provided by Verizon.
- **DUO Mobile** – The free DUO application can be downloaded to your mobile device from your Android Play Store, Apple App Store, etc. DUO uses one time codes that expire when used. As an option, generate multiple codes to be used throughout the day. Use the DUO codes in the order they were generated; any codes created previously will expire.
- **PIV** (Personal Identity Verification) / **CAC** (Common Access Card) – PIV/CAC is issued by your agency. It inserts into the computer and requires a valid certificate name selection. Agency coordination will be required to use this method.

Until PIV/CAC is set up, agency users can proceed signing in to the WITS 3 portal using One Time Passcode (OTP) via email temporarily.

For questions or to change your selection, contact the WITS 3 Help Desk at 1-800-381-3444, option 6, or ServiceAtOnceSupport@verizon.com.

After making a selection, use the instructions in the corresponding sections below to complete the setup for Yubikey, DUO Mobile, or PIV/CAC.

Frequently Asked Questions (FAQs)

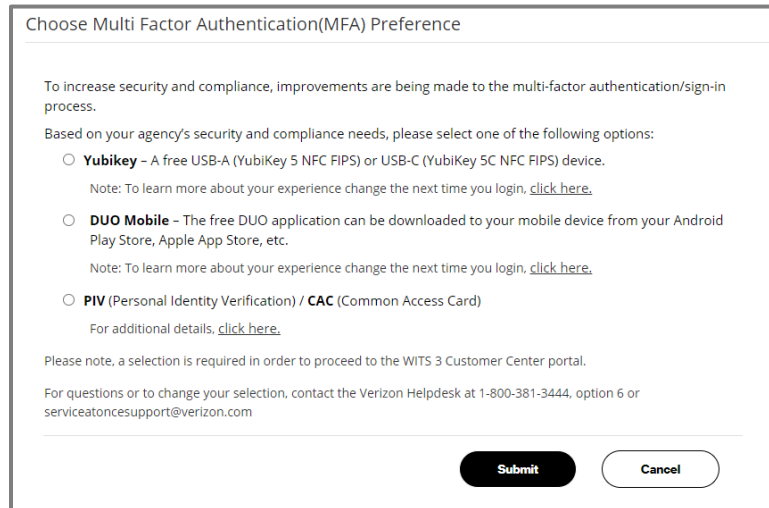
1. Where can I find the technical details for Yubikey?
 - Yubikey technical details can be viewed here: <https://docs.yubico.com/hardware/yubikey/yk-tech-manual/yk5-intro.html#yubikey-5-fips-series>
2. Where can I find the technical details for DUO Mobile?
 - DUO Mobile technical details can be viewed here: <https://duo.com/docs/duoweb-v2#overview>

Request Yubikey

Use the instructions in this section to request, order and register a Yubikey device.

1. Go to the WITS 3 portal, and sign in.

The Multi-Factor Authentication (MFA) pop-up message displays.



Choose Multi Factor Authentication(MFA) Preference

To increase security and compliance, improvements are being made to the multi-factor authentication/sign-in process.

Based on your agency's security and compliance needs, please select one of the following options:

- ☐ **Yubikey** – A free USB-A (YubiKey 5 NFC FIPS) or USB-C (YubiKey 5C NFC FIPS) device.
Note: To learn more about your experience change the next time you login, [click here](#).
- ☐ **DUO Mobile** – The free DUO application can be downloaded to your mobile device from your Android Play Store, Apple App Store, etc.
Note: To learn more about your experience change the next time you login, [click here](#).
- ☐ **PIV (Personal Identity Verification) / CAC (Common Access Card)**
For additional details, [click here](#).

Please note, a selection is required in order to proceed to the WITS 3 Customer Center portal.

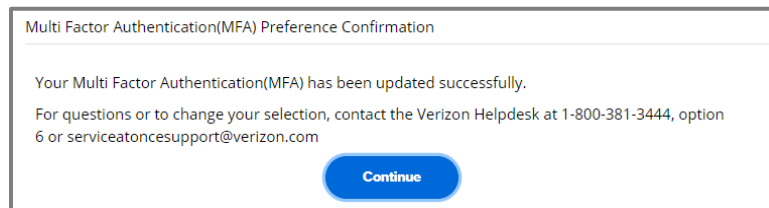
For questions or to change your selection, contact the Verizon Helpdesk at 1-800-381-3444, option 6 or serviceatoncesupport@verizon.com

Submit **Cancel**

Figure 1: MFA Message

2. Select *Yubikey*.
3. Click **Submit**.

Success message displays.



Multi Factor Authentication(MFA) Preference Confirmation

Your Multi Factor Authentication(MFA) has been updated successfully.

For questions or to change your selection, contact the Verizon Helpdesk at 1-800-381-3444, option 6 or serviceatoncesupport@verizon.com

Continue

Figure 2: Success Message

4. Click **Continue**.

The WITS 3 portal home page displays.

Order Yubikey

Use the following instructions to order a Yubikey device.

1. Go to the WITS 3 portal, and sign in.


Select yubikey screen displays.

You have chosen Yubikey as your Multi Factor Authentication (MFA) method. Please complete the shipment request below.


New shipment request

1. Select yubikey 2. Shipment address 3. Summary


Please Select Your Product



YubiKey 5 NFC FIPS
Keychain for wearing on a standard keyring. USB-A connector for standard 1.0, 2.0 and 3.0 ports. Near Field Communication (NFC) for mobile communication
- Compatible on modern Android and iOS devices.



YubiKey 5C NFC FIPS
Keychain for wearing on a standard keyring. USB-C connector for standard 1.0, 2.0 and 3.0 ports. Near Field Communication (NFC) for mobile communication
- Compatible on modern Android and iOS devices.



YubiKey 5C FIPS
Keychain for wearing on a standard keyring. USB-C connector for standard 1.0, 2.0 and 3.0 ports.

Figure 3: Select Yubikey

2. Select a Yubikey device:
 - USB-A (YubiKey 5 NFC FIPS)
 - USB-C (YubiKey 5C NFC FIPS)
 - USB-C (YubiKey 5C FIPS)

3. Click **Next**.

Shipment address screen displays.

Welcome, [redacted]

You have chosen Yubikey as your Multi Factor Authentication (MFA) method. Please complete the shipment request below.

New shipment request

1. Select yubikey **2. Shipment address** 3. Summary

Please enter shipment address

Email address *

EISAnalystTrain@gmail.com

Company name *

Verizon

First name *

[redacted]

Last name *

Training

Street line 1 *

22001 Loudoun County Pkwy

Street line 2

Street line 3

Country *

United States of America (the) ▼

State/Province *

Virginia ▼

City *

Ashburn

ZIP/Postal code *

20147

Phone number *

+1 5712662101

Back Next

Figure 4: Shipment Address

4. Enter the following required information:

- Email Address
- Company Name
- First Name
- Last Name
- Street Line 1
- (Optional) Street Line 2
- Country
- State/Province
- City
- Zip/Postal Code
- Phone Number

5. Click **Next**.


Summary page displays.

You have chosen Yubikey as your Multi Factor Authentication (MFA) method. Please complete the shipment request below.

New shipment request

1. Select yubikey 2. Shipment address **3. Summary**

Please verify selected product and shipment address below.

**YubiKey 5 NFC FIPS**
Keychain for wearing on a standard keyring. USB-A connector for standard 1.0, 2.0 and 3.0 ports. Near Field Communication (NFC) for mobile communication - Compatible on modern Android and iOS devices.

Email: [redacted]@gmail.com

First name: [redacted] Last name: **Training**

Company Name: **Verizon** Phone number: +1 [redacted]

Street line 1: [redacted]

Street line 2: [redacted] Country: **United States of America (the)**

State: **Virginia** City: [redacted]

Zip code: [redacted]

Figure 5: Summary


6. Confirm information is correct.
7. Click **Submit**.

Confirmation screen displays.

New shipment request

1. Select yubikey 2. Shipment address **3. Summary**

Please verify selected product and shipment address below.

**YubiKey 5 NFC FIPS**
Keychain for wearing on a stand and 3.0 ports. Near Field Communication (NFC) for mobile communication - Compatible on modern Android and iOS devices.

Email: [redacted]@verizon.com

First name: [redacted] Last name: [redacted]

Company Name: **Verizon** Phone number: +1 [redacted]

Street line 1: [redacted]

Street line 2: [redacted] Country: **United States**

State: [redacted] City: [redacted]

Zip code: [redacted]

Confirmation!

Do you want to place this Order?

Figure 6: Order Confirmation

8. Click **Yes**.

Confirmation message with shipment details displays.

Note: For questions or to change your selection, contact the WITS 3 Help Desk at [1-800-381-3444](tel:1-800-381-3444), option 6, or ServiceAtOnceSupport@verizon.com.

9. Click **Go to Homepage**.

The WITS 3 portal home page displays.

Note: Agency users can proceed signing in to the WITS 3 portal using One Time Passcode (OTP) via email temporarily. Once your Yubikey is delivered, use the instructions in the *Register Yubikey* section below to complete the setup process.

Register Yubikey

After your Yubikey has been ordered and you receive it in the mail, use the following instructions to complete the setup process.

1. Go to the WITS 3 portal, and sign in.

Yubikey message displays.

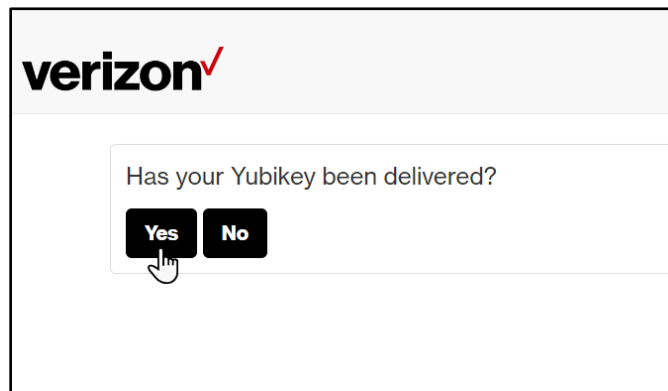


Figure 7: Yubikey Delivery

2. Has your Yubikey been delivered?
 - a. If yes, click **Yes**. Then, proceed to Step 3 below.
 - b. If no, click **No**. Users can proceed temporarily using the OTP via email while awaiting the Yubikey device delivery.

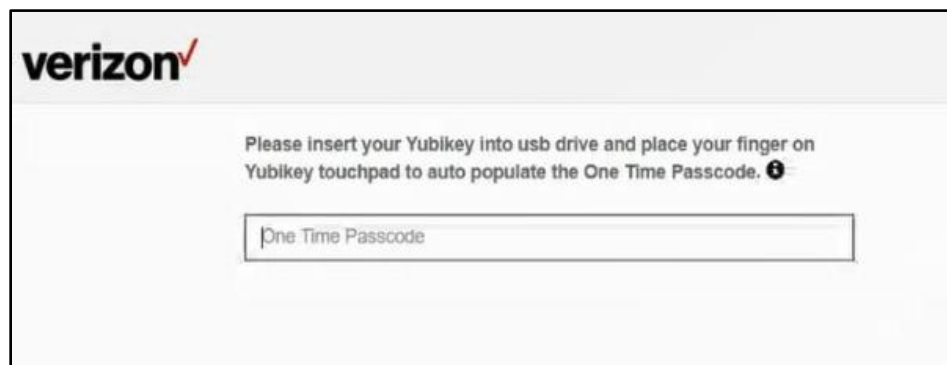


Figure 8: One Time Passcode

3. Insert the Yubikey into your computer.

Note: Inserting a Yubikey into a mobile device is not authorized.

The Yubikey will flash once inserted.

4. Touch the Yubikey touchpad with your finger to auto-populate the One Time Passcode.

Yubikey registration screen displays.

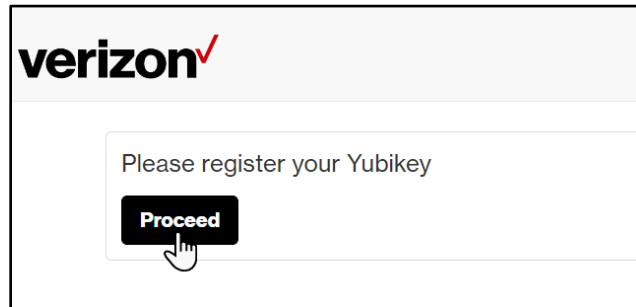


Figure 9: Yubikey Registration

5. Click Proceed.

Choose where to save this passkey screen displays.

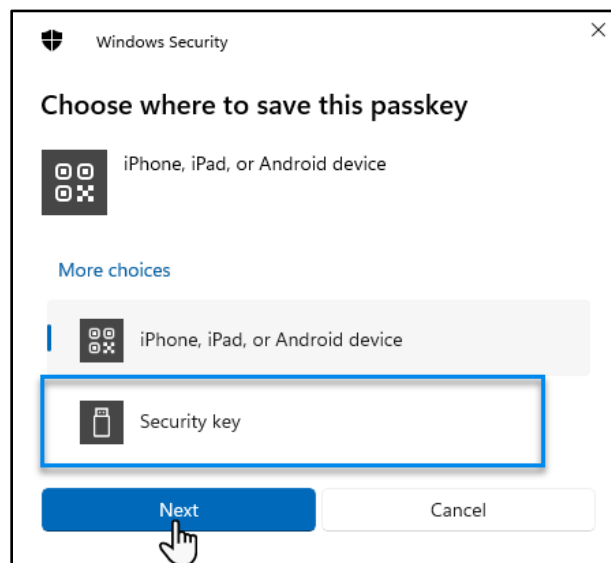


Figure 10: Save This Passkey

6. Select *Security key*.

7. Click **Next**.

Security key setup screen displays.

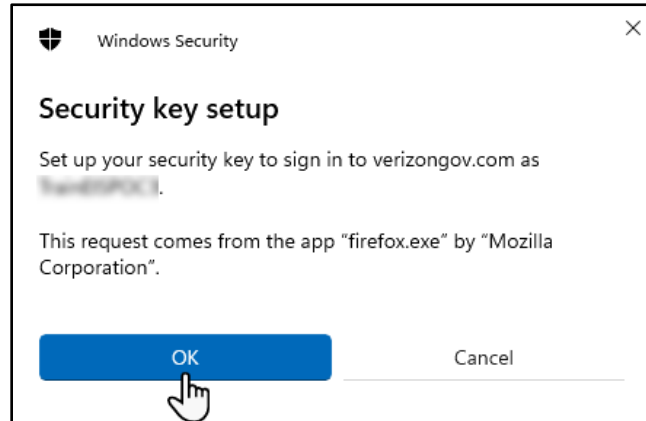


Figure 11: Security Key Setup

8. Click **OK**.

Create PIN screen displays.

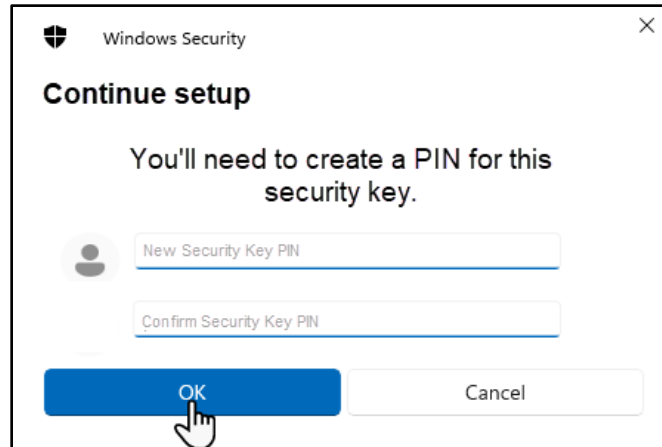


Figure 12: Create PIN

9. Create your security key PIN. Note: PINs must be at least 6 digits long.
10. Enter your security key PIN again.
11. Click **OK**.

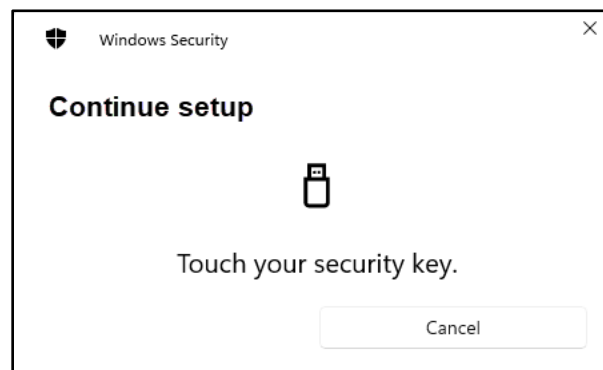


Figure 13: Continue Setup

12. Touch the Yubikey touchpad with your finger.

Passkey saved message displays.

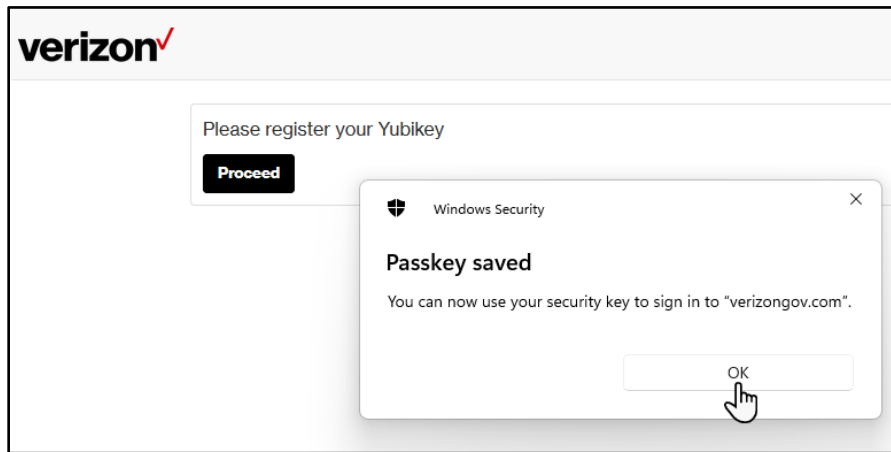


Figure 14: Passkey Saved

13. Click **OK**.

Note: Your Yubikey has been registered. Use the steps below to complete the initial sign in process.

Choose where to save this passkey screen displays.

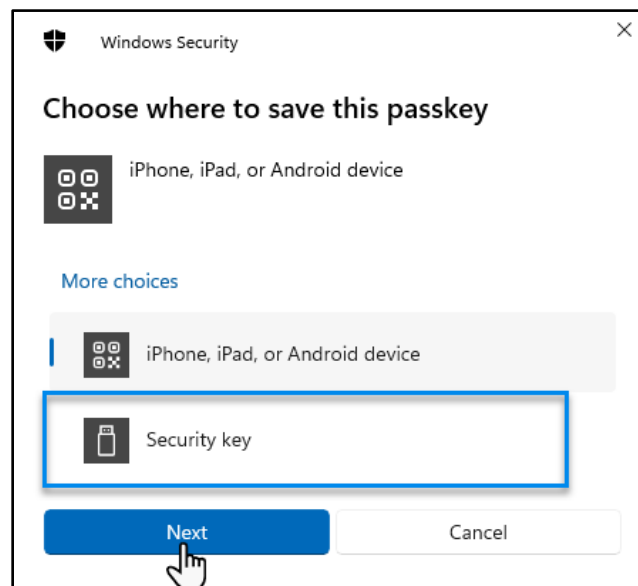


Figure 15: Save This Passkey

14. Select *Security key*.

15. Click **Next**.

Security key PIN screen displays.

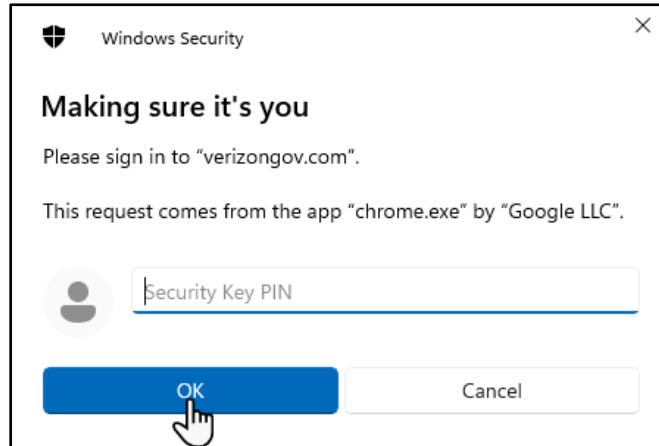


Figure 16: Enter PIN

16. Enter your security key PIN.

17. Click **OK**.

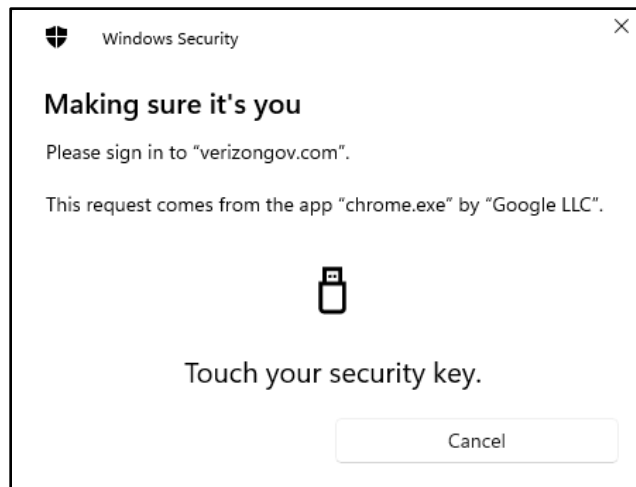


Figure 17: Yubikey Touchpad

18. Touch the Yubikey touchpad with your finger.

Government Warning displays.

19. Click **Continue**.

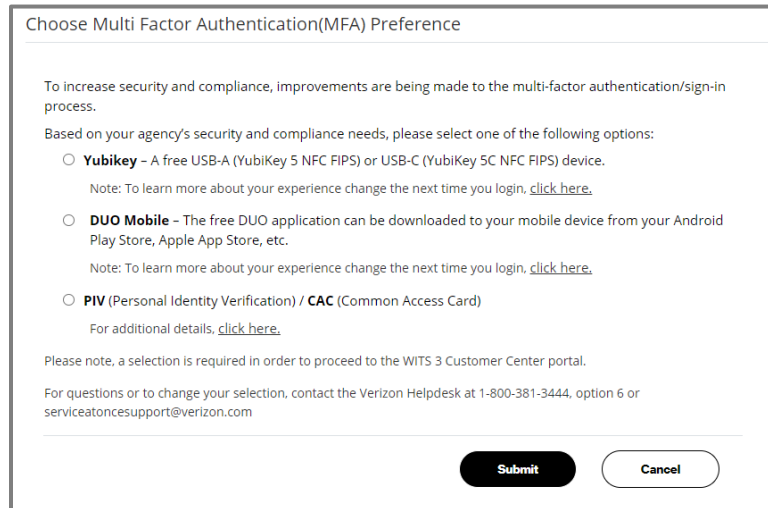
The WITS 3 portal home page displays.

Request DUO Mobile

Use the instructions in this section to request and complete the setup process for DUO Mobile.

1. Go to the WITS 3 portal, and sign in.

The Multi-Factor Authentication (MFA) pop-up message displays.



Choose Multi Factor Authentication(MFA) Preference

To increase security and compliance, improvements are being made to the multi-factor authentication/sign-in process.

Based on your agency's security and compliance needs, please select one of the following options:

- ☐ **Yubikey** – A free USB-A (YubiKey 5 NFC FIPS) or USB-C (YubiKey 5C NFC FIPS) device.
Note: To learn more about your experience change the next time you login, [click here](#).
- ☐ **DUO Mobile** – The free DUO application can be downloaded to your mobile device from your Android Play Store, Apple App Store, etc.
Note: To learn more about your experience change the next time you login, [click here](#).
- ☐ **PIV** (Personal Identity Verification) / **CAC** (Common Access Card)
For additional details, [click here](#).

Please note, a selection is required in order to proceed to the WITS 3 Customer Center portal.

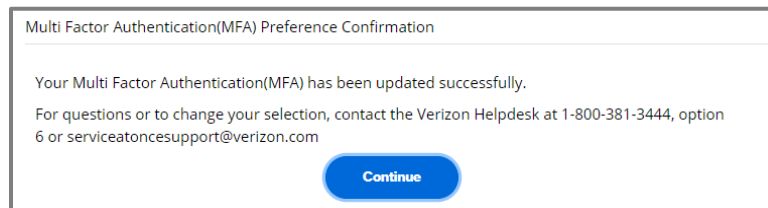
For questions or to change your selection, contact the Verizon Helpdesk at 1-800-381-3444, option 6 or serviceatoncesupport@verizon.com

Submit **Cancel**

Figure 18: MFA Message

2. Select *DUO Mobile*.
3. Click **Submit**.

Success message displays.



Multi Factor Authentication(MFA) Preference Confirmation

Your Multi Factor Authentication(MFA) has been updated successfully.

For questions or to change your selection, contact the Verizon Helpdesk at 1-800-381-3444, option 6 or serviceatoncesupport@verizon.com

Continue

Figure 19: Success Message

4. Click **Continue**.

The WITS 3 portal home page displays.

DUO Mobile Setup

Use the following instructions to complete the setup process for DUO Mobile.

1. Go to the WITS 3 portal, and sign in.

DUO setup screen displays.



Figure 20: DUO AUTH Setup

2. Click **Start setup**.

Add a device page displays.

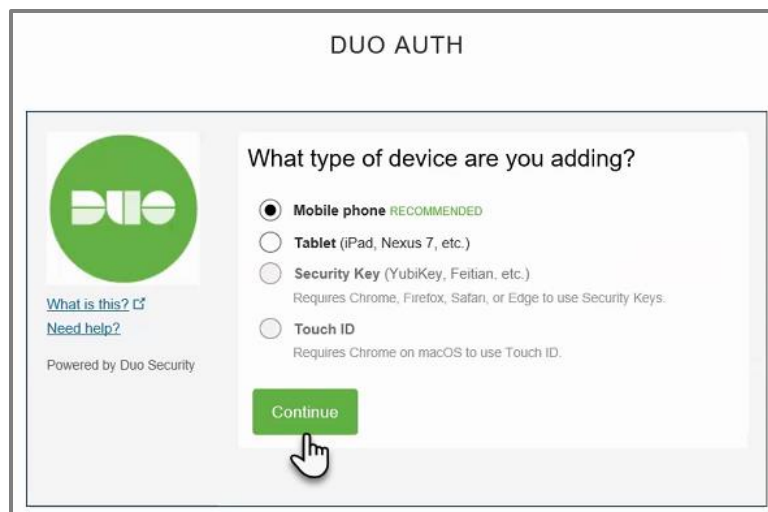
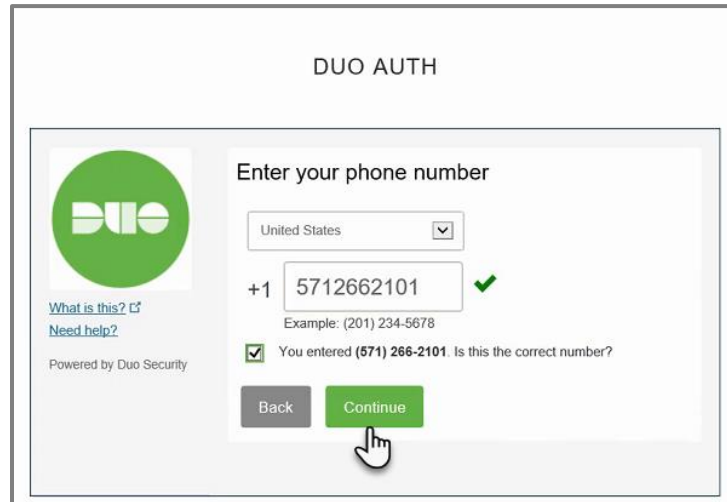


Figure 21: Add a Device

3. Click to select which type of device to add:

- **Option 1, Mobile phone:** Select if using the Duo Mobile application on a mobile phone.
- **Option 2, Tablet (iPad, Nexus 7, etc.):** Select if Duo Mobile application has been previously downloaded to be used with other accounts. Then, skip to Step 6.



The image shows a web interface titled "DUO AUTH". On the left is a green circular logo with the word "DUO" in white. Below the logo are links for "What is this?" and "Need help?", and the text "Powered by Duo Security". The main content area is titled "Enter your phone number". It features a dropdown menu for "United States", a text input field containing "+1 5712662101" with a green checkmark to its right, and an example "(201) 234-5678". Below this is a checkbox that is checked, with the text "You entered (571) 266-2101. Is this the correct number?". At the bottom are "Back" and "Continue" buttons. A hand cursor is pointing at the "Continue" button.

Figure 22: Enter Phone Number

4. Select the Country Code from the drop-down menu.
5. Enter your phone number.
6. Click to select **Is this the correct number?**
7. Click **Continue**.

Type of phone page displays.



The image shows a web interface titled "DUO AUTH". On the left is the same green circular logo and links as in Figure 22. The main content area is titled "What type of phone is 571-266-2101?". It features two radio button options: "iPhone" (unselected) and "Android" (selected). Below these are "Back" and "Continue" buttons. A hand cursor is pointing at the "Continue" button.

Figure 23: Type of Phone

8. Click to select the type of phone:
 - iPhone
 - Android
9. Click **Continue**.

Install Duo Mobile page displays.

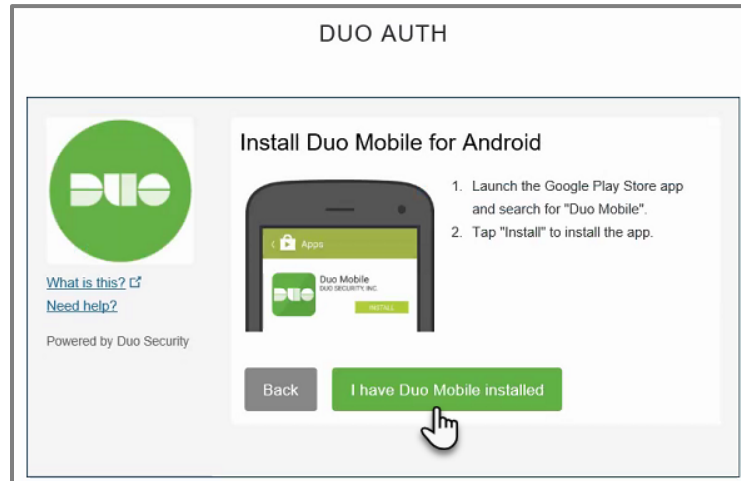


Figure 24: Install Duo Mobile

10. Follow the on-screen instructions to install the Duo Mobile application.

11. Click **I have Duo Mobile installed**.

Activate Duo Mobile page displays.

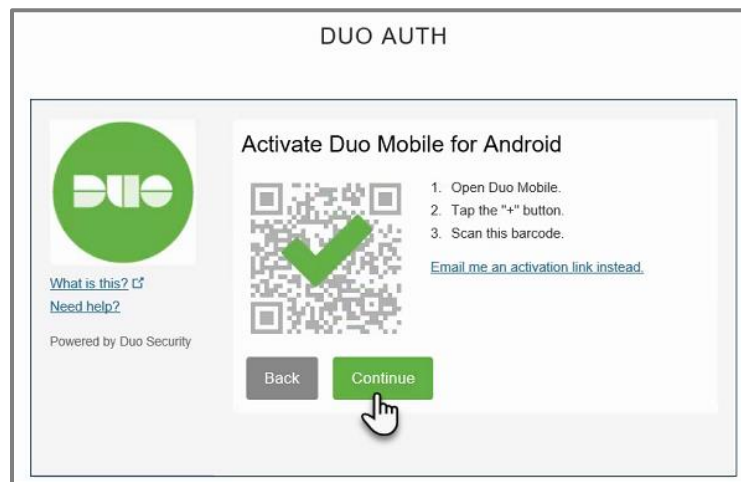


Figure 25: Activate Duo Mobile

12. Follow the on-screen instructions to activate the Duo Mobile application.

13. Click **Continue**.

My Settings & Devices displays.

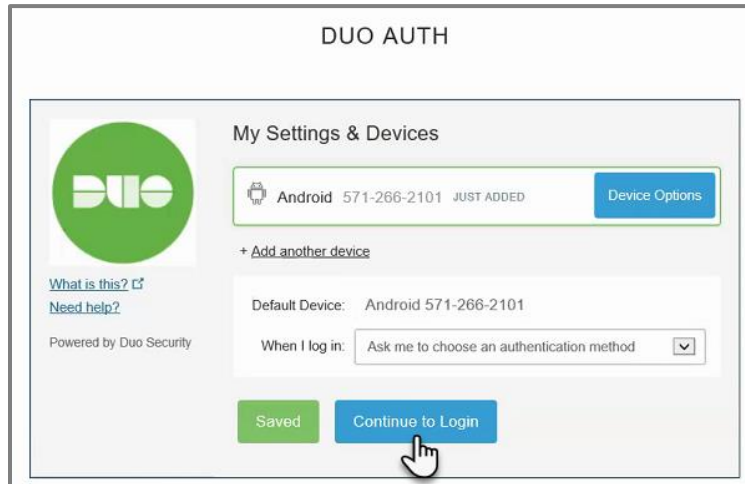


Figure 26: My Settings & Devices

14. From the *When I log in* drop-down menu, select one the following two options:

- Ask me to choose an authentication method
- Automatically send this device a Duo Push

15. Click **Continue to Login**.

Authentication methods page display.

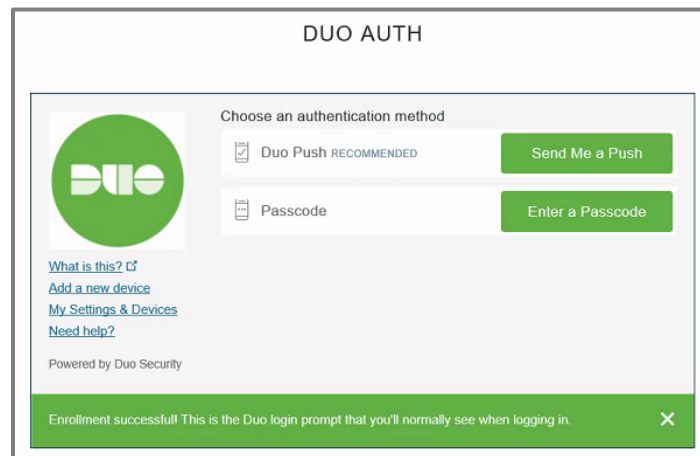


Figure 27: Authentication Methods

16. Click one of the following two options:

- **Send Me a Push:** Open your Duo Mobile application and click **Approve**.
- **Enter a Passcode:** Generate a code on your Duo Mobile application and enter it on the authentication methods screen. Click **Log In**.

Government Warning displays.

17. Click **Continue**.

The WITS 3 portal home page displays.

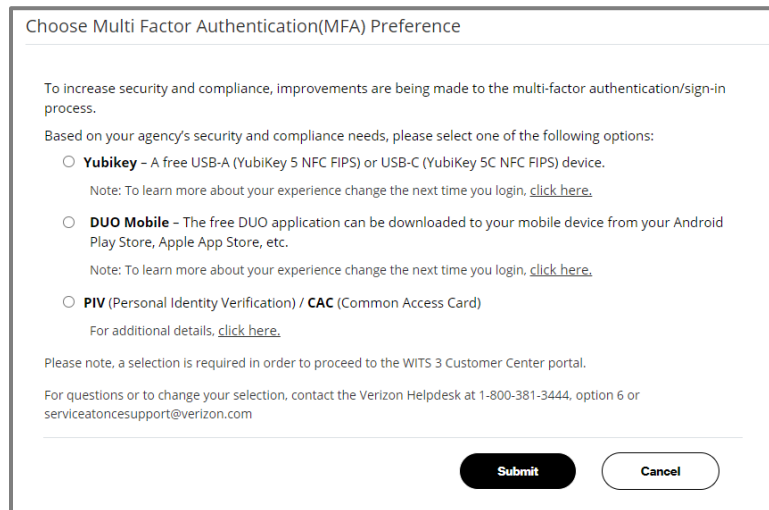
Request PIV/CAC

Use the following instructions to request Personal Identity Verification (PIV) / Common Access Card (CAC). Agency coordination will be required to use this option.

Until PIV/CAC is set up, agency users can proceed signing in to the WITS 3 portal using One Time Passcode (OTP) via email temporarily.

1. Go to the WITS 3 portal, and sign in.

The Multi-Factor Authentication (MFA) pop-up message displays.

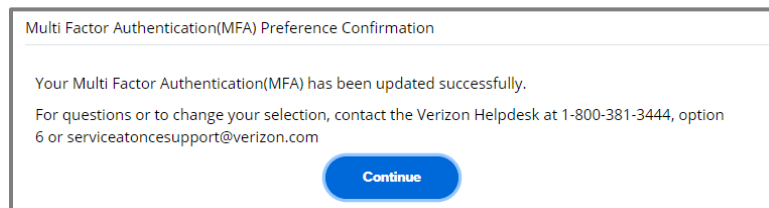


The screenshot shows a dialog box titled "Choose Multi Factor Authentication(MFA) Preference". The text inside reads: "To increase security and compliance, improvements are being made to the multi-factor authentication/sign-in process. Based on your agency's security and compliance needs, please select one of the following options:" followed by three radio button options: "Yubikey", "DUO Mobile", and "PIV (Personal Identity Verification) / CAC (Common Access Card)". Each option has a descriptive note and a "click here" link. At the bottom, there are "Submit" and "Cancel" buttons.

Figure 28: MFA Message

2. Select *PIV (Personal Identity Verification)* / *CAC (Common Access Card)*.
3. Click **Submit**.

Success message displays.



The screenshot shows a dialog box titled "Multi Factor Authentication(MFA) Preference Confirmation". The text inside reads: "Your Multi Factor Authentication(MFA) has been updated successfully. For questions or to change your selection, contact the Verizon Helpdesk at 1-800-381-3444, option 6 or serviceatoncesupport@verizon.com". At the bottom, there is a "Continue" button.

Figure 29: Success Message

4. Click **Continue**.

The WITS 3 portal home page displays.

Verizon will contact you/your agency to confirm selection and initiate next steps. Please be prepared to provide the following:

- Agency Name
- Agency Technical Contact
- Agency Security Contact
- Other agency contacts to be included
- Confirmation of the agency's root Certificate to Authenticate (CA) is publicly listed
| <https://www.idmanagement.gov>
- Or provide agency root CA
- Do you have a process in place to proactively inform us when your Certificate Revocation List endpoints expire/change?
- If so, can you share the contact person to discuss obtaining an alert?
- Does your agency only support Online Certificate Status Protocol (OCSP) for certificate validation?
- Identify 1-2 agency users to test

Customer Support

WITS 3 Help Desk

Email: ServiceAtOnceSupport@verizon.com

Phone: 1- 800-381-3444, Option 6