



NHTSA

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Multi-factor Authentication (MFA) for NHTSA Portals

Quick Reference Guide
November 2023

Quick Reference Guide - Table Of Contents

- ✓ What is multi-factor authentication (MFA)?
- ✓ What is this quick reference guide for ?
- ✓ What is Login.gov and why is DOT/NHTSA using it ?
- ✓ Authentication Method Setup
- ✓ How to Create Login.gov Account

What is Multi-Factor Authentication (MFA)?

- MFA is an authentication method that requires users to present two or more credentials to gain access to a website. Typically, a password is the first credential. A user must then choose a second authentication method. Authentication methods are also called factors. There are several options that users can choose for their second factor (password being the first factor). A common example is a one-time code sent via email, phone call or SMS text message.
- During login, **after** the user has entered their user ID and password, the user must also enter the code for the second factor to complete a successful login.



What is this Quick Reference Guide for ?

- NHTSA is implementing MFA for the following NHTSA portals:
 - ❑ **VISTA Portal**
- Throughout this slide deck, the term “NHTSA portal” refers to the VISTA portal..

** This is also a NHTSA portal. However, for the context of this slide deck, “NHTSA Portal” will only refer to the three portals above which have not yet been MFA-enabled.*

What is Login.gov and why are we using it?

- For better protection of user accounts, all federal agencies are now required to implement MFA to login to federal websites.
- Login.gov is a federal government sign-in service that facilitates MFA by allowing users to access participating federal websites with a single Login.gov account.
- When you try to sign into a participating federal government website, Login.gov will prompt you to sign in or create an account before you can access the secure website.
- Login.gov supports multiple authentication factors (see next slide) and many federal websites within NHTSA are now using Login.gov to implement MFA
- Login.gov is free to users



Login.gov Authentication Methods

Login.gov provides the following second factor authentication options:

- **Face or touch unlock:** You can only use face or touch unlock on a device that supports this feature. You will not see this option in the list of authentication options if your device does not have this capability. Since face or touch unlock is specific to the device and browser, you'll need to use the same device and browser in the future to sign in using this authentication method.
- **Authentication Application:** Authentication applications are downloaded to your device and generate secure, six-digit codes you use to sign in to your accounts.
- **Security key:** A security key is typically an external physical device, like a USB, that you plug into your computer. The key is linked to your accounts and will only grant access to those accounts once the key is plugged in and activated.
- **Text Message / Phone Call:** Login.gov will send a unique security code to that phone number each time you sign in to your Login.gov account. Each security code expires after ten minutes and can only be used once. If you don't enter the security code within ten minutes, request a new code.
- **Backup Codes:** Backup codes are an accessible option for users who do not have access to a phone. However, backup codes are the least secure option for two-factor authentication. Backup codes must be printed or written down which makes them more vulnerable to theft and phishing.

DOT/NHTSA recommends that you use either the **Authentication Application or Text/Phone call** for Authentication

To learn more about the authentication method, visit <https://login.gov/help/get-started/authentication-options/>



How to Create a Login.gov Account and Setting up a Phone Authentication Method

Login.gov Account Registration- First time

Step 1) :

VISTA Portal: <https://vista.nhtsa.dot.gov/conformity>

Click Login



Welcome!

A place where you can easily submit Conformity Packages.

** Only the screenshot for MSP is shown on this slide. MRP and MCP login screen will look similar.*

Login.gov Account Registration- First time

Step 2) :

Click VISTA Login.gov



Register for Login.gov Account

- System will automatically forward you to Login.gov's Create your account page
- Enter your email address and check the rules of use box
- Click on the Submit button

Remember! Registering for your Login.gov account is a one-time task. You **must** use the same email address that you use for your **NHTSA portal approved account.**

LOGIN.GOV NHTSA

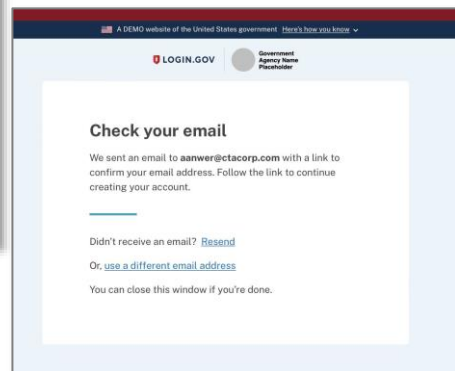
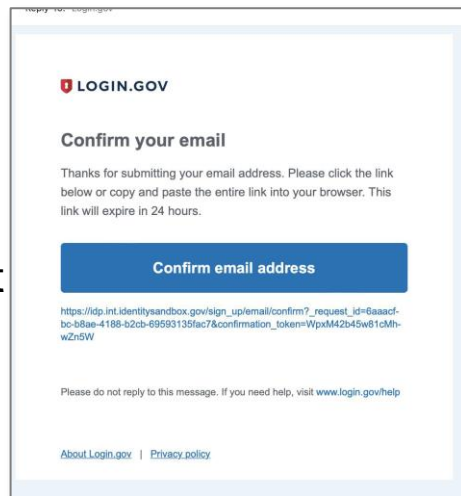
NHTSA Incident Report - SGO 2021-01 Portal is using Login.gov to allow you to sign in to your account safely and securely.

Email address

Password ☐ Show password

Create Login.gov Account

- Next, Login.Gov will promptly send you an email to confirm your email
- Check your inbox for the “Confirm your Email” email from login.gov (if you did not receive it, check your junk/spam email just in case)
- Click on confirm the email address/URL provided in the email



Create Login.gov Account

- After you have clicked the confirm your email address button/URL provided in the email, you will be redirected back to Login.gov to finish setting up your account
- System will display a screen to setup the password
- Create a strong password (***Passwords must be at least 12 characters***)
- Next, click on Continue button. **Remember the password, this will be your password going forward to log into NHTSA portals everytime.**

The screenshot shows the 'Create a strong password' step of the Login.gov account creation process. At the top, a green confirmation message states 'You have confirmed your email address'. Below this, the heading 'Create a strong password' is followed by instructions: 'It must be at least 12 characters long and not be a commonly used password. That's it!'. A 'Show password' checkbox is located to the right of the password input field. The password field itself is empty. Below the field, a 'Password strength' indicator shows four bars, with the first two being filled. A dark grey 'Continue' button is positioned below the strength indicator. At the bottom, there is a 'Password safety tips' link with a plus icon, and a 'Cancel account creation' link.

Authentication Methods

- After you have set up a strong password, the authentication method setup screen will be displayed.
- Select an authentication method. Not all Authentication methods can be used for NHTSA Portals. We recommend that you choose **text message/phone** or the **authentication application**. Backup codes are written down and are easily lost.
- You can visit the following page to learn more about each type of authentication method <https://login.gov/help/get-started/authentication-options/>

Remember, the authentication method that you choose now **will be used in addition to your user ID and password** every time you log into the NHTSA portal.

Authentication method setup

Add another layer of security by using one of the multi-factor authentication options below.

- ☐ **Face or Touch Unlock**
Use your device to verify your identity. We do not store your fingerprints or images. Recommended since it prevents phishing.
- ☐ **Security key**
A physical device, often shaped like a USB drive, that you plug in to your device.
- ☐ **Government Employee ID**
PIV/CAC cards for government and military employees. Desktop only.
- ☐ **Authentication Application**
Download or use an authentication app of your choice to generate secure codes.
- ☐ **Text or Voice Message**
Receive a secure code by (SMS) text or phone call to your device. Do not use web-based (VOIP) phone services or premium rate (toll) phone numbers.
- ☐ **Backup Codes**
A list of 10 codes you can print or save to your device. When you use the last code, we will generate a new list. Keep in mind backup codes are easy to lose.

[Continue](#)

[Cancel account creation](#)

Authentication Methods - Phone

- For example, for the demo purposes we will use the Text or Voice message option. If you choose to use this method, select the Text or Voice Message radio button and click on the Continue button

Remember! If you choose Text or Voice Message, you will be required to enter the security code received via text or phone call as your second form of authentication

Authentication method setup
Add another layer of security by using one of the multi-factor authentication options below.

- ☐ **Face or Touch Unlock**
Use your device to verify your identity. We do not store your fingerprints or images. Recommended since it prevents phishing.
- ☐ **Security key**
A physical device, often shaped like a USB drive, that you plug in to your device.
- ☐ **Government Employee ID**
PIV/CAC cards for government and military employees. Desktop only.
- ☐ **Authentication Application**
Download or use an authentication app of your choice to generate secure codes.
- ☒ **Text or Voice Message**
Receive a secure code by (SMS) text or phone call to your device. Do not use web-based (VOIP) phone services or premium rate toll phone numbers.
- ☐ **Backup Codes**
A list of 10 codes you can print or save to your device. When you use the last code, we will generate a new list. Keep in mind backup codes are easy to lose.

[Continue](#)

[Cancel account creation](#)

Authentication Methods - Phone/Text Setup

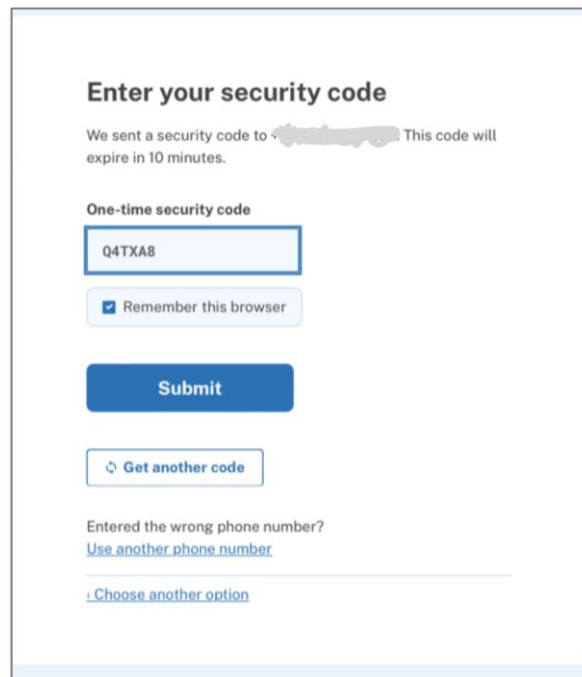
- You must provide a cell phone number where you will want to receive a security code.
- Additionally, the phone method also has a phone call option.
- Make your selection by clicking on the radio button for either text message or phone call
- Click on the Send code button

Remember to provide the phone number that is accessible to you

The screenshot shows a mobile app interface for setting up authentication. At the top, there is a green speech bubble with a black telephone handset icon and five asterisks. Below this, the text reads: "Send your security code via text message (SMS) or phone call". A note states: "We'll send you a security code each time you sign in." Another note says: "Message and data rates may apply. Do not use web-based (VOIP) phone services or premium rate (toll) phone numbers." There is a section for "Phone number" with an example "(201) 555-0123" and a text input field with a US flag icon. Below that, a question asks "How should we send you a code?" with two radio button options: "Text message (SMS)" (which is selected) and "Phone call". A link for "Mobile terms of service" is present. At the bottom, there is a blue "Send code" button and a link for "Choose another option".

Authentication Methods - Text security code

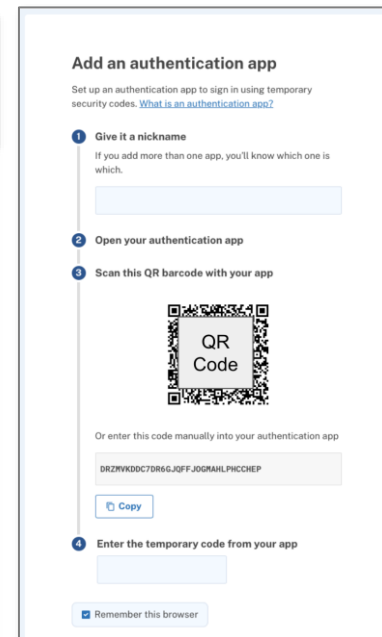
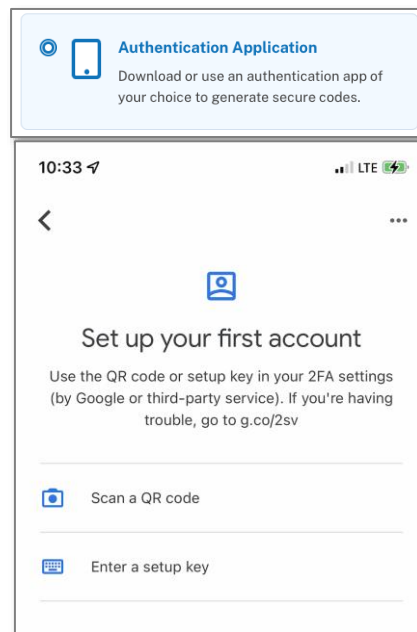
- If the text message option was chosen on the previous screen, a unique security code gets sent to your phone. If the phone call option was chosen, you will receive a phone call containing the security code
- Each security code expires after ten minutes and can only be used once
- After you have entered the code, click on the Submit button
- If it is more than 10 minutes, you can always request another code by clicking on the Get another code button



The screenshot shows a web form titled "Enter your security code". Below the title, it says "We sent a security code to [redacted] This code will expire in 10 minutes." There is a text input field containing "Q4TXA8". Below the input field is a checkbox labeled "Remember this browser" which is checked. A blue "Submit" button is below the checkbox. At the bottom, there is a link "Get another code" with a refresh icon. Below that, it says "Entered the wrong phone number?" followed by two links: "Use another phone number" and "Choose another option".

Authentication Methods - Application

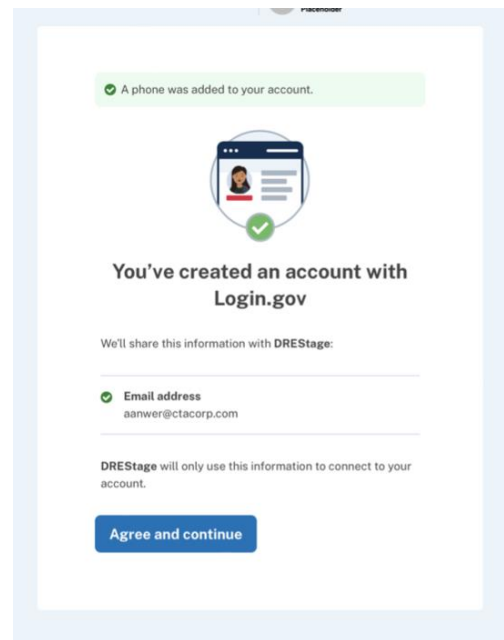
1. Choose a device, such as a computer or mobile device (phone or tablet), on which you can install apps.
2. Download and install an authentication app to your device. Some popular options include:
 - a. Android options: Google Authenticator, Authy, LastPass, 1Password.
 - b. iOS options: Google Authenticator, Authy, LastPass, 1Password.
 - c. Windows apps: 1Password, OTP Manager.
 - d. Mac apps: 1Password, OTP Manager.
 - e. Chrome extensions: Authenticator.
3. Open the app and use the QR code to establish a new account and associated token.



Authentication Methods - Account Created

- Next, if this is your first time setting up, you will see a message to agree and continue
- This message is a confirmation that an account has been created for the NHTSA portal you were trying to access and a second authentication method has been set up
- Click on the Agree and continue button

Remember! This screen is only displayed when you are setting up your account for the first time



Successful Account Setup & Login

- After successfully setting up your new Login.gov password and your choice of second authentication method, you will have to authenticate using this method going forward.
- After successfully authenticating with Login.gov, you will be automatically redirected back to the application you are trying to access and will be able to continue business as normal.



FAQs

Frequently Asked Questions (1 of 2)

Question	Answer
What is my password to login.gov?	Once you have confirmed your email address, set up a strong password. If you have done so and forgotten your password, go to this link: https://secure.login.gov/users/password/new
What is an authentication method ?	An authentication method is another verification factor to secure a user's account: 1. After you have created a password, you will be prompted to choose a second authentication method 2. The following methods are the <i>suggested</i> options for you to use: a. Text message/Phone call b. Authentication App

Frequently Asked Questions (2 of 2)

Question	Answer
How do I reset my password?	Visit the Login.gov sign in page and click on “Forgot your password” link to reset the password
How do I access my account if I do not have access to my chosen authentication method anymore? Example: I cannot access my phone or backup codes.	You will have to request to delete your existing account, please reach out to login.gov for help https://login.gov/help/manage-your-account/delete-your-account/
Can I change my second authentication method?	Yes, you can. Please follow the link below: https://login.gov/help/manage-your-account/add-or-change-your-authentication-method/
I have created my account on Login.gov, but I do not see an account created?	You must confirm your email address. Check your inbox and look for the email to confirm.