

# Multi-Factor Authentication

**Multi-Factor Authentication (MFA)** is an added layer of security that goes beyond a password to perform a second level check to verify a user's identity before they can access protected applications. This extra layer of security protects all Personal Identifying Information (PII) and Protected Health Information (PHI) stored in the applications.

## Where do I go to enroll in MFA or update my MFA option?

1. Login to the HCS <https://commerce.health.state.ny.us> with your User ID and Password
2. Click **MFA Management** from **My Applications**
3. Choose one:
  - A. [I have a NYS driver's license or Non-driver Photo ID](#)
  - B. [I do not have a NYS driver's license or Non-driver Photo ID.](#)

**Change your authentication method anytime.**

## If you selected option A: [I have a NYS driver's license or Non-driver Photo ID](#)

4. Enter your DMV ID number, Date of Birth (MMDDYYYY), Gender and Zip Code from your ID
5. Click **Next**
6. Confirm [State ID/License information has been verified with NY State Department of Motor Vehicles \(NYSDMV\)](#)
7. Select **Type of Authentication**
8. Enter verified security email address, business email address for RSA, scan QR code for authenticator app or enter phone number for voice or SMS
9. Click **Submit**
10. Confirm **Congratulations!! You have successfully updated your MFA information**

## If you selected option B: [I do not have a NYS driver's license or Non-driver Photo ID](#)

4. Enter your Date of Birth, Gender, Non NYS ID and Non NYS ID Value
5. Select **Type of Authentication**
6. Enter verified security email address, business email address for RSA, scan QR code for authenticator app or enter phone number for voice or SMS
7. Click **Submit**
8. Confirm **Congratulations!! You have successfully updated your MFA information**

See page 2 for details about the authentication types

## What is needed to enroll in MFA or update my MFA option?

You will need either a valid NYS DMV Driver's License, NYS DMV Non-driver Photo ID, Passport, Unexpired Foreign Passport, US Driver's license (out-of-state users), or other acceptable form of photo identification.

## How do I use the MFA option?

1. Open the HCS application that requires MFA
2. Authentication page will appear with instructions to enter a **Verification Code**
  - **Security Email**
  - **Use code from authenticator app**
  - **RSA Token (State DOH/ITS):** Enter the number from your State issued RSA hard or soft token
  - **\* SMS (Text Message):** Enter the number you see in your text message
  - **\* Voice (Automated Phone Call):** Enter the number you hear upon answering your phone "your verification code for Health Commerce is..."
3. If desired, check the box to "Remember this browser.." to avoid entering an MFA code for 30 days.  
Do **NOT** check the box if the device is shared.
4. Click **Authenticate.** *\*For external HCS Users Only*

## TIPS:

- Your name in the HCS and on your DMV ID must be an exact match.
- User MFA info can be set up anytime.
- Previously submitted MFA info does not display on screen.
- User receives email notification for all MFA updates.
- **Need help?** Send an email to the Commerce Accounts Management Unit (CAMU) [camu@health.ny.gov](mailto:camu@health.ny.gov) or call **866-529-1890** option 1.
- **I locked my account!** Users will have three chances to enter the MFA validation code successfully in an application. After three failed attempts, you will be logged out of the HCS and your account will be locked. Call the CAMU, verify your identity and your account will be unlocked.

# Multi-Factor Authentication

## MFA Authentication Methods

Upon opening an HCS application protected by MFA, you must enter a one-time code.

If the five minute limit expires to enter the one time code, then you can click  .

Your five options to receive the code are:

1. **Security Email** - Receive a one-time code sent to your *verified* security email address within five minutes or code will expire. Your secure email address is unique to all other HCS users and was verified by clicking the confirmation link sent to that address.
2. **Use code from authenticator app** - Receive the one-time code from the browser extension or smartphone app, like Google or Microsoft Authenticator, you must first scan the Quick Response (QR\*) Code.

*NOTE: This is the preferred option for non-DOH/ITS user because it is faster and more secure.*

Once scanned, enter the number, provided from the Authenticator app, in the One-time Code field.

*You can download Authenticator apps on your smart phone from the Google Play Store or Apple App Store to read the QR code. The QR Code is a type of matrix barcode (or two-dimensional barcode).*

3. **RSA Token (NYS DOH & ITS employees only)** - Receive the MFA code by RSA token, enter the email address you registered with your RSA token. Enter the code from your hard/soft RSA token in the Verification Code field.

*NOTE: This is the preferred option for NYS DOH/ITS user because it is faster and more secure.*

RSA SecurID, LLC consists of a token – either hardware (e.g. a key fob) or software (soft token). To request an RSA Token, go to <https://mytoken.ny.gov/console-selfservice/SelfService.do>.

4. **SMS (Text Message)** - *For external HCS Users Only* Receive the one-time code by Short Message Service (SMS) text message, enter the phone number you wish to receive the text message on. Once you receive the text message, enter the code provided from the text in the One-time Code field within five minutes.
5. **Voice (Automated Phone Call)** - *For external HCS Users Only* Audibly hear the one-time code, enter the phone number you wish to receive the code on. Once you receive the phone call, enter the number provided from the call in the One-time Code field.

**Note: You can check the box to "Remember this browser.." to avoid entering an MFA code for 30 days. Do NOT check the box if the device is shared.**

**You can change your authentication method anytime using MFA Management.**

