

United States Coast Guard

Direct Access Multi-Factor Authentication User Guide

**January 2026
v2026.01.05**



Revision History

Date	Author(s)	Version Number	Notes
12/30/2025	C5ISC-MSSPL	v2025.12.30	Initial Draft
01/05/2026	C5ISC-MSSPL	v2026.01.05	Added MFA methods and screenshots

DRAFT

Table of Contents

1.	Signing In	1
2.	Multi-Factor Authentication Methods.....	2
2.1	Text Message	2
2.2	Phone Call	4
2.3	Email.....	6
2.4	Authenticator Application	8

DRAFT

1. Signing In

1. In the Employee ID field, type in employee ID.
2. In the Password field, type in password.
3. Click **Sign in**.

Non-CAC Personnel Enter EMPLID

Employee ID

Password

[Forgot your password?](#)

Sign in

4. Read the Direct Access - DHS Security Notice. Ensure **I Accept** is selected in the drop-down menu.



User Details

----- Direct Access - DHS Security Notice -----
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

I Accept

Continue

5. Click **Continue**.

2. Multi-Factor Authentication Methods

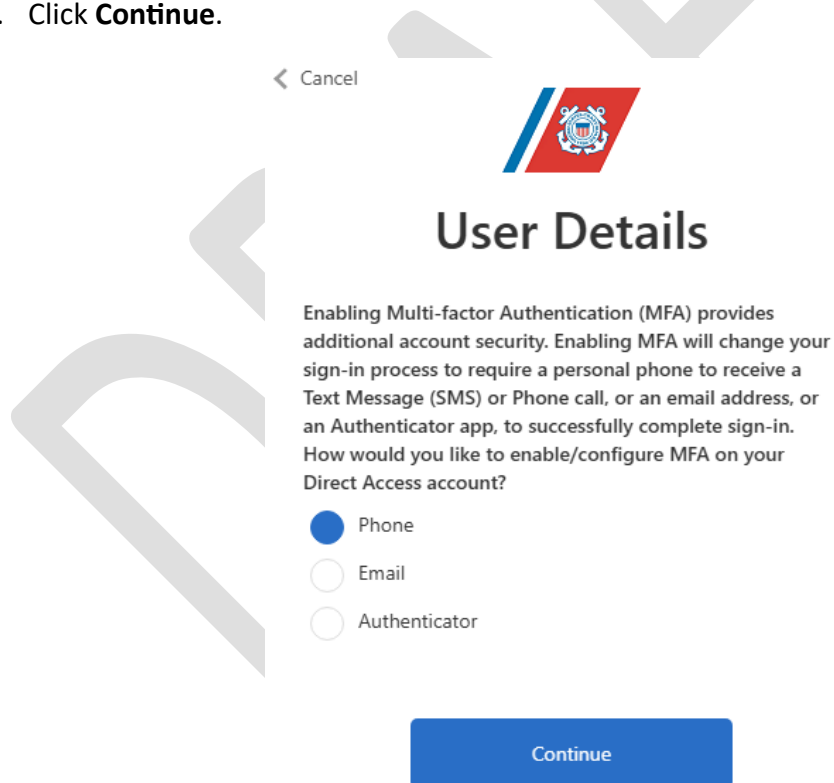
The options for Multi-Factor Authentication (MFA) methods are as follows:

- Text message
- Phone call
- Email
- Authenticator application


To reset an MFA method, contact the Product Support Service Desk (PSSD) by calling 1-800-821-7081 or emailing SMB-USCG-KerWV-ProductSupportSD@uscg.mil.

2.1 Text Message

1. From the list of MFA options, choose **Phone**.
2. Click **Continue**.



< Cancel



User Details

Enabling Multi-factor Authentication (MFA) provides additional account security. Enabling MFA will change your sign-in process to require a personal phone to receive a Text Message (SMS) or Phone call, or an email address, or an Authenticator app, to successfully complete sign-in. How would you like to enable/configure MFA on your Direct Access account?

☒ Phone

☐ Email


☐ Authenticator

Continue

3. From the Country Code drop-down menu, select the appropriate country.

4. In the Phone Number field, type the phone number.

[← Cancel](#)



Enter a number below that we can send a code via SMS or phone to authenticate you.

Country Code

Country/Region ▼

Phone Number


Phone number

Send Code

Call Me

5. Click **Send Code**.

[← Cancel](#)



Enter a number below that we can send a code via SMS or phone to authenticate you.

Country Code

United States (+1) ▼

Phone Number

8888888888

Send Code

Call Me

6. Type the verification code in the box, or if the code has expired or was not received, click **send a new code**. Click **Verify Code**.

Enter your verification code below, or [send a new code](#)

Verify Code

2.2 Phone Call

1. From the list of MFA options, choose **Phone**.
2. Click **Continue**.

< Cancel



User Details


Enabling Multi-factor Authentication (MFA) provides additional account security. Enabling MFA will change your sign-in process to require a personal phone to receive a Text Message (SMS) or Phone call, or an email address, or an Authenticator app, to successfully complete sign-in. How would you like to enable/configure MFA on your Direct Access account?


- ☒ Phone
☐ Email
☐ Authenticator

Continue

3. From the Country Code drop-down menu, select the appropriate country.


4. In the Phone Number field, type the phone number.

 Cancel



Enter a number below that we can send a code via SMS or phone to authenticate you.

Country Code

Country/Region 


Phone Number


Phone number

Send Code

Call Me


5. Click **Call Me**.

 Cancel



Enter a number below that we can send a code via SMS or phone to authenticate you.

Country Code

United States (+1) 

Phone Number

8888888888

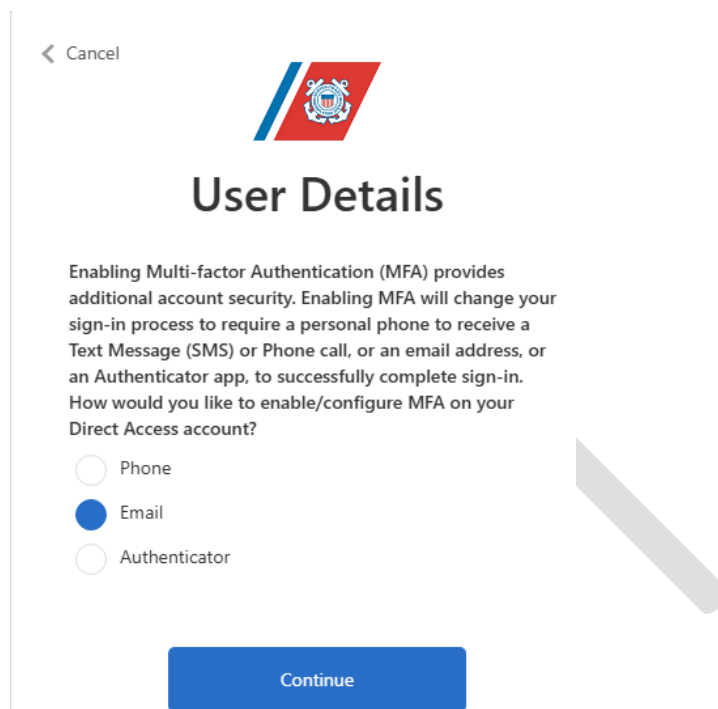
Send Code

Call Me

6. Follow the voice instructions and press the # key on the phone to sign in.


2.3 Email

1. From the list of MFA options, choose **Email**.



This screenshot shows the 'User Details' screen. At the top left is a '< Cancel' link. In the center is a logo consisting of a red rectangle with a white circular emblem and a blue diagonal stripe. Below the logo is the title 'User Details'. A paragraph of text explains that enabling MFA provides additional security and lists options: Text Message (SMS), Phone call, email address, or an Authenticator app. It asks the user how they want to enable MFA. There are three radio buttons: 'Phone' (unselected), 'Email' (selected), and 'Authenticator' (unselected). At the bottom is a blue 'Continue' button.

< Cancel



User Details

Enabling Multi-factor Authentication (MFA) provides additional account security. Enabling MFA will change your sign-in process to require a personal phone to receive a Text Message (SMS) or Phone call, or an email address, or an Authenticator app, to successfully complete sign-in. How would you like to enable/configure MFA on your Direct Access account?

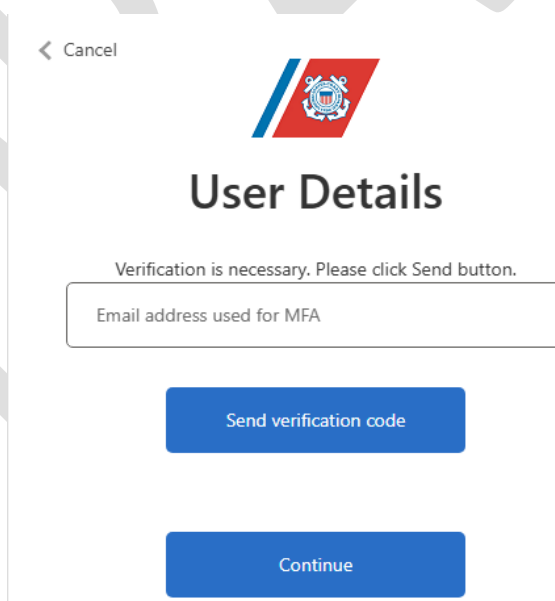
☐ Phone

☒ Email

☐ Authenticator


Continue

2. Click **Continue**.
3. Type in email address in the box. Click **Send verification code**.



This screenshot shows the 'User Details' screen after clicking 'Continue'. It features the same logo and title as the previous screen. Below the title, a message states 'Verification is necessary. Please click Send button.' There is a text input field with the placeholder text 'Email address used for MFA'. Below the input field are two blue buttons: 'Send verification code' and 'Continue'.

< Cancel



User Details

Verification is necessary. Please click Send button.

Email address used for MFA

Send verification code

Continue

4. Type the verification code that was sent to the email, or if the code has expired or was not received, click **Send new code**.

< Cancel



User Details

Verification code has been sent to your inbox. Please copy it to the input box below.

hannah.m.goode@uscg.mil

Verification code

Verify code

Send new code

Continue

5. Click **Verify code**.
6. Click **Continue**.

< Cancel



User Details

E-mail address verified. You can now continue.

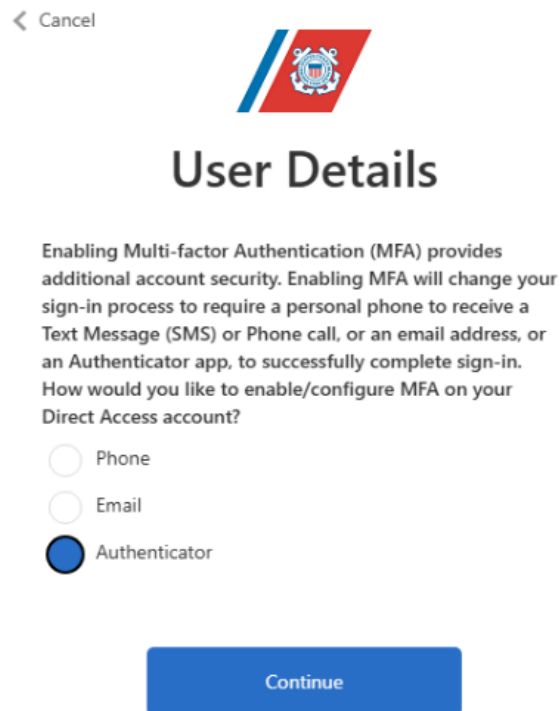
hannah.m.goode@uscg.mil

Change e-mail

Continue

2.4 Authenticator Application

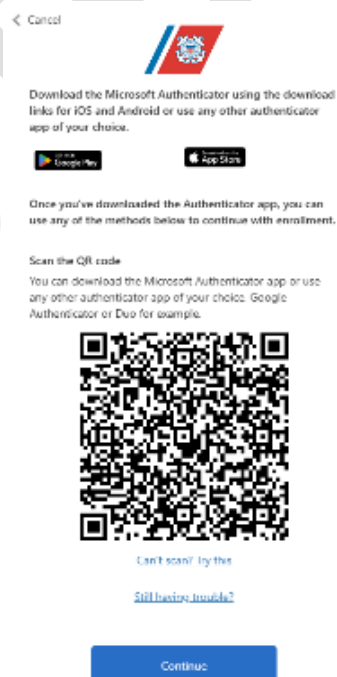
1. From the list of MFA options, select **Authenticator**.



2. Use phone to scan the QR code and add account to Authenticator app.

NOTE

The Microsoft Authenticator app or another authorized app must be downloaded on phone to receive code.



3. Click **Continue**.
4. In the box, type the verification code displayed in the app.

< Cancel



Enter the verification code from your authenticator app.

Enter your code.

Verify

5. Click **Verify**.

DRAFT