Frequently Asked Questions (FAQ) for Direct Access Multifactor Authentication (MFA) Enrollment

---

General Questions

Q: What is Multifactor Authentication (MFA)?
A: Multi-factor Authentication (MFA) is a security process in which you provide a code sent to you to verify your identity after logging in. Think of it as a second lock on the door. The first is your username and password, and the second is the code sent to your phone.

Q: Why is MFA required?
A: MFA enhances security by preventing unauthorized access to systems and accounts, even if your password is compromised. It is a critical step in safeguarding sensitive information and ensuring compliance with security policies.

Q: Who needs to enroll in MFA?
A: Effective January 5, 2026, ALL LOCAL ACCOUNT USERS OR NON-CAC users accessing DIRECT ACCESS are REQUIRED to enroll in MFA.

NOTE: If you do not use MFA, you will not be able to login to Direct Access.

Policy and Compliance

Q: Is MFA enrollment mandatory?
A: Yes, MFA enrollment is mandatory for all users accessing Direct Access to comply with security policies. Again, failure to enroll will result in failure to access Direct Access.

Q: How often will I need to authenticate using MFA?
A: Every time you log in to Direct Access or when prompted due to security policies (e.g., after a password reset).
After you select your preferred method of MFA (text or phone call) that will be used every time.

Enrollment Process

Q: How do I enroll in MFA?
A: Follow these steps to enroll in MFA:

1. LOGIN TO DIRECT ACCESS
    a. In the Employee ID field, type in employee ID.
    b. In the Password field, type in password.

Non-CAC Personnel Enter EMPLID

Employee ID

> Employee ID

Password

> Password

Forgot your password?

Sign in

    c. Click **Sign in**.

2. Follow the on-screen instructions to complete the setup process. Read the Direct Access - DHS Security Notice. Ensure **Agree** is selected. Click **Continue**.
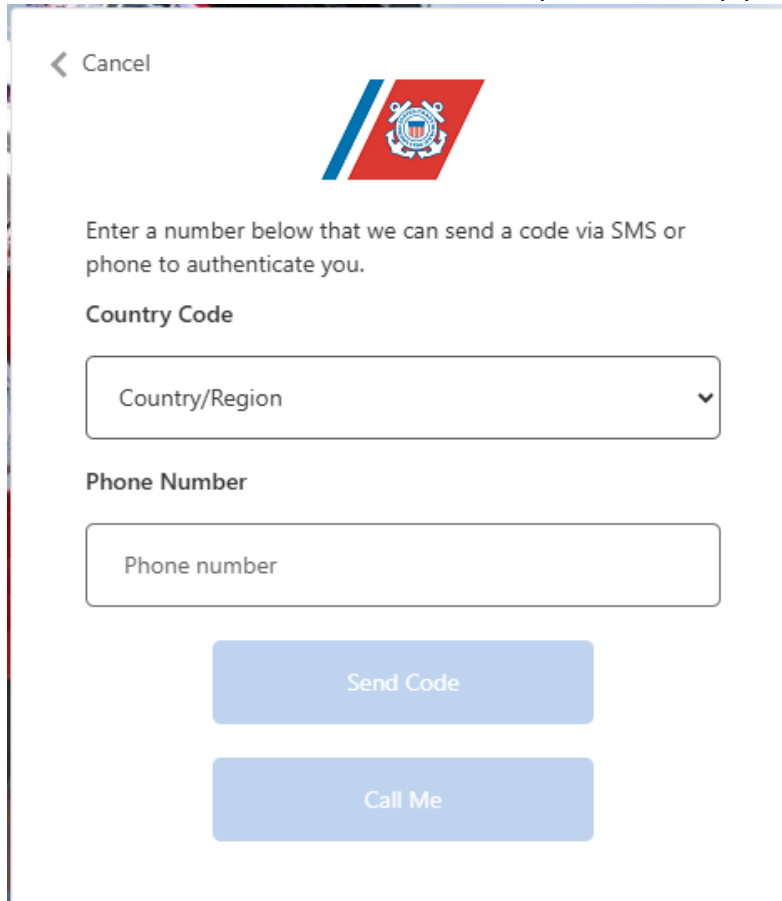
User Details

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 to successfully complete sign-in.

● Agree

Continue

3. Follow the on-screen instructions to complete the setup process.

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

Q: What authentication methods can I use for MFA?
A: You can use one or more of the following methods:

- Phone call
- Text message

Q: Can I enroll multiple devices for MFA?
A: No, you can only have one number or device enrolled with DA MFA login at a time. If you wish to reset your phone number, Product Support Service Desk can be reached by calling 1 800 821 7081 or by emailing SMB-USCG-KerWV-ProductSupportSD@uscg.mil.

Q: Is it better to call or email the Product Support Service Desk?
A: It is better to CALL 1-800-821-7081 than to email, but if you cannot call for any reason then email is an option.

Troubleshooting and Support

Q: What if I don't have a smartphone?
A: If you don't have a smartphone, you can use other authentication methods, such as a phone call by landline.

Q: I didn't receive the MFA code. What should I do?
A: If you didn't receive the code:

1. Ensure your device has a stable internet or cellular connection.
2. Verify that your device is correctly enrolled in MFA.
3. Call helpdesk for further assistance if nothing else works.

Q: Can I change my authentication method after enrollment?
A: Yes, you can change your authentication method by calling the help desk. Product Support Service Desk can be reached by calling 1 800 821 7081 or by emailing SMB-USCG-KerWV-ProductSupportSD@uscg.mil.

Q: If I have additional questions or issues, who can I contact for help?
A: For assistance with Direct Access login or technical issues please call 1-800-821-7081 (option 1).
If you cannot use a phone, send an email to SMB-USCG-KerWV-ProductSupportSD@uscg.mil for the Product Support Service Desk.