DS Logon (DSL)
Frequently Asked Questions (FAQs)

TIP: To search our FAQs, press Control+F

- **What is DSL?** DSL makes it easy for you to access your information contained across DoD and VA partner websites. By signing up for a free account, you can view your financial and benefits information; Personally Identifiable Information (PII); Personal Health Information (PHI); claim statuses and records.

- **Who is Eligible for an Account?** You must be affiliated with the DoD or VA, and listed in the Defense Enrollment Eligibility Reporting System (DEERS) in one of the following roles to get a DSL account: Service Members (Active, Guard, Reservist, Retirees), Veterans; Eligible Family Members (over 18 years old); Spouses (current and former w/DoD Benefits); DoD Civilians and Contractors.

- **How DSL validates a user's identity?** DSL validates a user's identity by allowing a user to use their CAC; remote and/or in-person proof. In-person proofing requires a user to bring I-9 documents to a Veteran Affairs Regional Office or RAPIDS office. Acceptable I-9 documents are listed in **"Adding, Updating, or Correcting Your Records"** section. Remote proofing is the ability to verify your identity using a data vendor and by supplying information that you are in possession of and have knowledge of.

- ***IF YOU ARE REMOTE PROOFING, PLEASE READ ALL OF THE FOLLOWING AS THE PROCESS HAS CHANGED:***
  - In order to protect your PII and PHI in partner applications, *Remote Proofing* is a multiple step process with various workflows where the system automatically selects which workflow a user will remote proof. Remote proofing process consists of successfully uploading documentation (e.g., driver's license), taking a selfie, typing select digits of a credit card/loan, and/or answering knowledge based questions. All information sent to the data vendor is encrypted and protected.
  - **The user cannot choose which workflow is used for remote proofing**
  - The data vendor provides information that helps the DoD verify a user's identity. The information used in remote proofing is pulled using a soft inquiry on your credit report and is not used for any other purpose except to verify your identity at a single point in time.
  - **IMPORTANT**: The data, your identity documents, and information you provide are not used in data mining or for any other purpose except identity verification
  - If you have reported identity theft and your credit report is frozen, you will need to temporarily unfreeze your credit report to remote proof.
  - You **MUST** complete all the steps at a single time in the time limit provided. If you do not complete the process, you timeout, or you provide information that cannot be verified, your ability to access DSL and partner sites may be impacted

- The total time should take approximately 10 minutes. Please have driver licenses, computer or cell phone with a camera, phone to receive an OTP, credit cards, and/or loan documents available **BEFORE** you start the process.
- If you have unsuccessfully tried to remote proof multiple times and are now receiving an error, your ability to remote proof has been suspended for 30 days. If you try again, the 30 day timelines starts over again. DMDC CCC, VA, and DSL cannot remove the suspension on your ability to remote proof as it occurs at the data vendor site

- **REMOTE PROOFING TASKS**:
  - **Two-Factor Authentication (2FA)**
    - You will be provided a one-time PIN (OTP) via a text or voice line that will be sent to you by text or phone call. The number used for OTP is pulled from DEERS so please ensure your contact information is accurate
    - After you receive the message, enter the 5-digit code
    - The code expires in 5 minutes. If the code expires or is invalid, you can request a new code
    - Message and data rates may apply
  - **Multi-Factor Authentication (MFA)**
    - To additionally protect your protect, you can set-up MFA using an authenticator app
    - IMPORTANT: If you do not wish to set-up MFA, press 'SKIP' each time it is presented
    - Cookies must be enabled for MFA set-up
    - You will need to download an authenticator app (e.g., Authy or Microsoft Authenticator) on your smart device (e.g., mobile phone, tablet, etc.)
    - You will be required to enter a 16-digit code to set-up the MFA.
    - Each time you sign-in to your account you will be prompted to enter the OTP 5-digit code AND the MFA 6-digit code from your authenticator app
    - REMINDER: Once MFA has been set-up on your account, this security feature can only be removed by contacting the CCC and request your account be deactivated. You will then be required to either logon with your CAC or establish a new account by verifying your identity and completing the account set-up process
  - **Knowledge Based Questions**
    - Users may be prompted to answer questions regarding their background or information that only they may know, dependent on the workflow.
    - Questions that contain in the quiz must be answered within 3 minutes
    - The data vendor already has the answers to the questions being requested. If the data vendor is able to match the answers completely, this step of the workflow will be complete

- **Financial Account Identity Information**
  - Users may be prompted to verify a financial account, dependent on the workflow
  - Users can select the account type that they would like to be used
  - Users will enter the part of the account number identified by the system
  - The data vendor already has the financial information that is being requested. If the data vendor is able to match the financial information completely, this step of the workflow will be complete
  - American Express and debt cards are not accepted
  - Loan and credit card numbers will NOT be stored. The expiration date or CVV # is not required for verification
- **Document Upload**
  - Users may be prompted to upload an identity verification document and take a selfie (picture of one's self), dependent on the workflow
  - If prompted to upload documents and a selfie, follow the instructions
  - Users on a non-mobile device may be prompted to select an image stored on their device instead of taking a picture with their camera during the 'Selfie' capture process
  - A selfie is self-portrait capturing one's entire face without anything on it or beside it that can be used for identity proofing purposes
  - **Document Upload Tips**:
    - Only 'jpg' images are supported
    - Some devices may need to have default photo settings restored
    - Size 480x640 or greater, 24 bit color and at least 250 dpi
    - If you are having difficulty uploading documents, use either a solid-dark background (recommended) or solid-white background. Do not place on lap or patterned couch
    - If your photo is taking several minutes to upload and is timing out, your photo may be too large
    - Make sure there is no glare or reflection caused by sunlight or lighting. Indirect sunlight is best
    - Recommend not holding your documents, place document on flat surface and take a picture directly above it and not on an angle
    - Ensure the photos are sharp and clear. The documents cannot be blurry and must be easy to read
    - Your document should fill as much of the screen as possible and cannot be cut off or parts not captured in the photo
    - When taking a selfie, it is recommended to have a solid background. Do not wear hats, glasses, distractive clothing unless your state license, driver's license, or other photo ID's also include glasses. Face masks must be removed
    - Do not use blurring or other filters. The photo needs to be a true picture of you

- Use a high-resolution camera or web-cam, if possible. The better the quality, the more likely your document and/or photo will be verified successfully
- Depending on your device, some users may want to seek assistance from a friend or family member to capture a selfie
- Do not hold your camera above your head looking up. Have a picture straight on to your face
- Documents CANNOT be expired, altered or photocopies

- **EXAMPLES OF WHY USERS FAIL REMOTE PROOFING WHEN SUBMITTING DOCUMENTS:**
  - Poor Quality Photos – Document or Selfie is very blurry
  - Holding Documents and Fingers – Fingers covering important parts of the documents such as user's photo, address, etc.
  - Backgrounds: Documents that have been placed on:
    - Multi-colored patterned couches and/or chairs
    - Glass tables that reflect the camera flash
    - Multi-colored carpets
    - Bookshelves with tons of books
    - In front of pictures of the family
    - In a picture frame
    - In the leaves of plants and/or flowers
    - On top of clothing a person is wearing or on their shoes
  - At an angle so id's top appears significantly larger than the bottom
  - Wearing a large brim hat with sunglasses holding a margarita glass
  - Wearing a hat that covers half the face, laughing, at the beach
  - Baseball caps that shade the face
  - Hair covering all of the face, half the face, and/or having both sides of the face covered except for the nose
  - Side capture of the face
  - Fingers covering half the face as if covering their mouth from laughing
  - Pictures while driving with the seat belt on, steering wheel and blurry cars going past in background (this is unsafe too)
  - Sunglasses in a variety of shapes
  - Images standing in front of a mirror with flash glare
  - Family portraits or more than 1 person at a party
  - Only from the nose down
  - Putting a driver's license in front of the face or beside the face
  - Severely damaged ID's that were unreadable
  - Filters used in social media

- **EXAMPLES OF WHY USERS PASS REMOTE PROOFING WHEN SUBMITTING DOCUMENTS:**

  - ID is placed on a dark surface such as a kitchen table or countertop with good lighting
  - No flash glare
  - Selfie captures the full face front on with no sunglasses, hats, hair, or anything else that would take away from the image
  - Selfie that mimics photo on a person's driver's license

- **Best Practices on Protecting Your Account:**
  - Do not give your username/password information to anyone
  - Be sure your phone and computer's software and malware/virus protection are up-to-date
  - Only install software from the software provider's official website
  - Do not click on any emailed links that says you need to install something
  - Again, go directly to a software provider's website to install software
  - Be cautious of messages, links and ads on social media as they may contain viruses. When in doubt, do not click on them
  - **IMPORTANT: Close your web browser and all tabs after you have logged out of DSL. If you do not close all tabs and your web browser, your PII and PHI may still be accessed due to individual computer caching**
  - Check your accounts and data (e.g., eBenefits, bank accounts, credit reports, DSL) on a monthly basis to ensure your information is still accurate
  - If you think your account has been compromised or hacked:
    - Change your password immediately
    - Change your challenge questions
    - Freeze your credit report
    - Check banking account information associated with your benefits. You may need to in-person proof if a compromise has occurred

- DMDC (e.g., Call Centers or DSL team) will not initiate contact with beneficiaries via email or telephone to request private personal (Name, SSN, DOB) or sensitive DSL account information (username, password, challenge questions). If you think you provided personal or account information in response to a fraudulent email, website or phone call, log into your DSL account and immediately change your password and challenge questions immediately
- You must login and reset your passwords every 180 days (6 months)
- You are responsible for keeping your information (e.g., name, address, phone, email) current on your DEERS record. Your contact information (e.g., email and phone numbers) will be used to authenticate you on login and allow you to remote proof

How to sign-up for a DSL account?

Service Members:

- Use your CAC
  1. Select "Create Account" button

2. Select “I have my Common Access Card (CAC) with access to a card reader” during registration process
3. Follow the steps to get an account within the application

- Email Registration
  1. Select “I am one of the following”
  2. Follow the steps to get an account within the application
  3. **NOTE:** In order to use this method, you must have a registered valid email address on your DEERS record to get an account
- RAPIDS
  1. While you are getting a new ID card, you can notify the Verifying Official that you want a DSL account
  2. Provide the RAPIDS Operator with your email address and follow the steps the RAPIDS Operator provides. RAPIDS site locations can be found here https://idco.dmdc.osd.mil/idco
  3. You will receive an email with the activation steps within 24 hours. This email is only good for 7 days
- Sign-up your eligible family members for a DSL account on their behalf while you are logged into DSL. (Family members must be eligible and **have unique email addresses on file**)

Retirees:

- Register for a DSL by selecting “Create Account”
  1. Follow the DSL registration procedures
  2. Registration can take up to 10 minutes to verify your identity. Individuals will be consenting to a soft-inquiry on their credit report and receive a one-time PIN (OTP) to the phone number on file. Prior to starting this, ensure you have time and access to your phone
- RAPIDS
  1. While you are getting a new ID card, you can notify the Verifying Official that you want a DSL account
  2. Provide the RAPIDS Operator with your email address and follow the steps the RAPIDS Operator provides. RAPIDS site locations can be found here https://idco.dmdc.osd.mil/idco
  3. You will receive an email with the activation steps within 24 hours. This email is only good for 7 days
- Remote Proofing
  1. To complete the registration for a DSL account, users must successfully Remote Proof. Read all of the Remote Proofing section at the beginning of this document prior to beginning the process.

Veterans:

- Veterans, their family members and/or dependents have the option to contact the Department of Veterans Affairs (VA) by phone, web page, or in-person in a VA Regional Office to have their identity vetted and added to DEERS, if they are not in DEERS already
- VA Regional Office

1. You will need to complete the in-person identity proofing process by bringing the necessary I9 documentation to a VA Regional Office
2. For more information and instructions, go to http://www.benefits.va.gov/benefits/offices.asp
3. **NOTE:** Ensure your correct mailing address is on your DEERS record (if you have one) as an activation letter will be sent to the address within 7-12 business days

- Call the VA at 800-827-1000
  1. Say eBenefits when prompted for reason for your call
  2. You MUST have the following information PRIOR to calling:
     - Your Full Name (Last name used while in service may be different than what it is today)
     - SSN
     - Checking or Savings Account Number
     - Dollar amount of the most recent electronic fund transfer
- Remote Proofing
  1. To complete the registration for a DSL account, users must successfully Remote Proof. Read all of the Remote Proofing section at the beginning of this document prior to beginning the process.

Military Family Member/Dependents:

- Your Military Sponsor using their CAC
  1. Your military sponsor requests you a DSL account after they have logged into their account
  2. After their request, you will receive an activation email with 24 hours or a letter within 7-12 business days and follow the steps within the letter
- Email Registration
  1. Select “Create Account” → Select “I have an active DoD ID card and an email on file in DEERS”
  2. Follow the steps to get an account within the application
  3. **NOTE:** In order to use this method, you must have a registered valid email address on your DEERS record to get an account. Family members must have unique email addresses on file
- Remote Proofing
  1. Read the Remote Proofing section at the beginning of the document prior to beginning the remote proofing process.
  2. Select “Create Account” to start the registration process or “Activate Account” if you have an activation letter
  3. Follow the steps to get an account within the application
- RAPIDS
  1. While you are getting a new ID card, you can notify the Verifying Official that you want a DSL account
  2. Provide the RAPIDS Operator with your email address and follow the steps the RAPIDS Operator provides. RAPIDS site locations can be found here https://idco.dmdc.osd.mil/idco
- If you have more than 1 Sponsor

- If you are a dependent under more than one sponsor, you can select your preferred sponsor to change sponsors and the associated benefits with that sponsor

- **PLEASE READ IMPORTANT INFORMATION:** Sponsors can see their information and any spouse or dependent's information. For example, Wife is an Active Duty Service Members, who is the sponsor. Husband is the dependent along with the couple's 3 children. Depending on the partner application a user accesses, the wife (sponsor) can view the husband's full medical records along with the children's.

After you have created an account

- **Recommended browser for optimal user experience**
  1. Chrome
  2. Edge
  3. **Note:** Internet Explorer is no longer supported
- **Login with DSL**
  1. Select DSL tab
  2. Enter username and password

- **CAC Login**
  1. Select the CAC tab and select Login

- **Two Factor Authentication (2FA) One Time PIN (OTP):**
  1. When you log in, change your password and/or create a DSL account, you will be asked to input an OTP that will be sent to your landline or text to your cell phone.
  2. Once you have selected methodology (text or phone call), you will
     - Receive a OTP via text or phone call
     - Input the OTP into the box provided
     - If you did not receive the OTP, you can request to resend the OTP to the number selected

     NOTE: Message and data rates may apply. If you are using an international number, not all countries support receiving text and/or voice authentication codes

- **Multi Factor Authentication (MFA) One Time PIN (OTP):**
  1. If you have set-up the MFA option, you will be prompted to enter the 6-digit code from the authenticator app
  2. If you have not set-up the MFA option, you will be prompted to set-up or will need to SKIP

- **Activation Code:**
  1. After setting up your DSL account and requesting an Activation code by email with instructions, select "Activate My Account"
  2. If you did not receive or accidently deleted the email, you can register for a

new account without the activation code
3. If there is no email, current email, current mailing address, you will need to go to:
    - Go to IDCO (https://idco.dmdc.osd.mil/idco/) and update your contact information
    - Visit a VA Regional Office
    - Update during card issuance at a RAPIDS station
    - Call the DMDC Contact Center if the options above cannot be done

- **Challenge Questions:**
    1. Challenge questions are used to reset passwords. Select questions/answers that you can remember to use to reset your password
    2. Avoid odd answers. Answer questions that you CAN remember. Ask yourself if you will remember the answer in a year prior to typing the answer
    3. Ensure that none of your social media accounts contain the answers to your challenge questions
    4. You can change your challenge questions
        - Log into DSL
        - Select Change Challenge Questions

- **Document Upload Identity Verification:**
    1. If prompted to upload documents or a selfie, it is recommended using a smart device (e.g., cell phone) with access to cameras
    2. When finishing uploading documents, click on Verification Status button after one (1) minute to monitor the status of the request
    3. Only .jpg images are supported when selecting an image
    4. Documents are only used for identity purposes and will not be stored nor used after identity verification has occurred

- **Manage Relationships:**
    1. There are several available options such as people who can act on YOUR behalf or people you can act on for THEIR behalf
    2. **PLEASE READ IMPORTANT INFORMATION:** Sponsors can see their information and any spouse or dependent's information. For example, Wife is an Active Duty Service Members, who is the sponsor. Husband is the dependent along with the couple's 3 children. Depending on the partner application a user accesses, the wife (sponsor) can view the husband's full medical records along with the children's.
    3. Be mindful that these authorizations remain active until the authorizing individual revokes them within the DSL application.
    4. If you have a surrogate on file, you can view who the surrogate has access to and what information
    5. **IMPORTANT:** Clinical access authorizes full access to medical records for that individual
    6. You can manage your relationships by
        - Log into DSL

- Select Manage Relationships
- Select Add Relationships
- Select option that applies

- **Account Suspended**
  1. To un-suspend your DSL account
     - Log into DSL
     - Select Un-suspend My Account
     - Answer Challenge Questions
     - Change Password
     - Follow instructions

- **Password Information**
  1. You can change your password at any time, but it MUST be changed at least every 180 days. To change your password,
     - Log into DSL and go to
       a. Manage DSL Account
       b. Change Password
     - Forgot your Password, go to
       a. DSL login screen
       b. Click Forgot Password?
       c. Follow the remaining steps
  2. Passwords must:
     - be between 15 and 20 characters in length
     - contain at least 1 uppercase letter (A-Z)
     - contain at least 1 lowercase letter (a-z)
     - contain at least 1 number (0-9)
     - special characters allowed but not required (i.e. @_#!&$'%*+().,;~:{}|?>=<^[]-)
     - contain at least 2 characters that are different than your previous password
  3. Passwords cannot:
     - have spaces
     - be 1 of your last 10 previous passwords
     - have user names, email address, zip code, Social Security Number (SSN) or date of birth
     - have been changed within the last 24 hours

- **Adding, Updating, or Correcting Your Records**
  1. Using your DSL account or CAC, you can update your address, email address and/or phone number by going to
     - Log into DSL
     - Update Contact Information
  2. Go to IDCO to update your address, email address and/or phone number by going to
     - Log into IDCO (https://idco.dmdc.osd.mil/idco/)

- Under "My Profile"
- Click on "Continue"
- Go to the bottom of screen after updating your information and click "Submit."

3. Contacting the DMDC Customer Contact Center at (800) 368-3665 for the hearing impaired Monday through Friday 5 am to 5 pm PT.
   - Documents may be requested to be submitted via mail or fax.
   - Follow the instructions the Contact Center Representative gives you for updating your information
4. In-person proofing can update your records.
   - You will need to bring in I-9 documents to verify your identity.
   - Ensure you call ahead and make any necessary appointments at the appropriate facilities (e.g., RAPIDS Station, VA Regional Office)
5. Acceptable I-9 documents that may be requested are:
   - Primary: Picture ID issued from Federal or State Government (e.g., valid Passwords, ID card, Military Dependent card, DoD ID card, Permanent Resident Card, State DMV issued ID card, etc.)
   - Secondary: SSN card, non-picture ID card, birth certificate, citizenship or naturalization certificate, driver's license, ID card by local government with DOB, gender, height, eye color, and address.

- **Account Locks, Deactivations, & Suspensions**
  - A user can deactivate their account at any time. An account can be re-established by registering for a new account and completing the identity verification process
  - DSL accounts can be locked for a variety of reasons to include unusual activity. Account locks can only be unlocked by DMDC. Account locks are not the same as account suspended or an account that has been deactivated.
  - An account can be suspended due to incorrect password attempts or inactivity.
  - An account can be removed due to inactivity
  - If you have unsuccessfully tried to remote proof multiple times and are now receiving an error, your ability to remote proof has been suspended for 30 days. If you try again, the 30 day timelines starts over again. DMDC CCC, VA, and DSL cannot remove the suspension on your ability to remote proof as it occurs as the data vendor site

- **Error codes**
  Note: All references to FAQ's, refer to Need Support?
  - Error Code [3] – A username and password is required when logging into DS Logon. Enter your username and password. If you do not remember your username/password, go to Forgot username or Forgot password.
  - Error Code [4] - The DS Logon password is required. You did not enter password when attempting to log on. Fill out all required items when logging in. This includes username and password.
  - Error Code [5] - If you do not remember your username/password, go to Forgot Username or Forgot Password. If you do not have an account, go to "Create Account".

- Error Code [7] - Your request for an account is being processed. You will receive an activation letter to your mailing address. Once you have received, follow the instructions on the letter.
- Error Code [8] - Your account has been suspended due to excessive failed logon attempts. Go to Unsuspend Your Account if you still need to access your account.
- Error Code [9] - This account is locked. Go to the FAQs for what actions are available to you.
- Error Code [10] - The DS Logon username or password you entered is INVALID. Do you need to register for a DS Logon?
- Error Code [11] - The DS Logon username or password you entered is incorrect. Use Forgot Username or Forgot Password for recovery methods or if you do not have an account, register for one.
- Error Code [12] - Your password needs to be reset. Go to Forgot Password to reset your password.
- Error Code [13] - You are not eligible for a DS Logon Account. If you are a Veteran or believe you are eligible for an account, visit the simplified FAQs for what actions are available to you to get a DS Logon account.
- Error Code [14] - The one-time password has expired. You will need to restart the logon process to be able to log into DS Logon.
- Error Code [31] - Unable to read your Common Access Card (CAC). Try again after ensuring your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.
- Error Code [32] - There was a problem reading your Common Access Card (CAC). Make sure your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.
- Error Code [33] - DS Logon is unavailable. Try again later or you can visit the simplified FAQs for further options.
- Error Code [34] - There was a problem reading your Common Access Card (CAC). Make sure your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.
- Error Code [35] - There was a problem reading your Common Access Card (CAC). Make sure your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.
- Error Code [36] - There was a problem reading your Common Access Card (CAC). Make sure your CAC is valid, fits tightly in your smart card reader, and the reader is connected to your machine.
- Error Code [37] - The system is unavailable. Try again later. If this problem continues you may contact the DMDC Support Center (DSC) at 800-477-8227. To best assist you, call when you are at a computer if possible.
- Error Code [38] - There is an issue with your CAC. It may be invalid, revoked, expired or an issue with the certificates. If you believe you have received this message in error, call the DMDC Customer Contact Center at 800-368-3665 for further assistance.
- Error Code [39] - Your digital certificate on your Common Access Card (CAC) is not unique in our system. If you believe you have received this message in error you may contact the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.
- Error Code [40] - There was a problem with your digital certificate on your Common Access Card (CAC). If you believe you have received this message in error you may the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.

- Error Code [41] - The system is unavailable. Try again later. If this problem continues you may contact the DMDC Support Center (DSC) at 800-477-8227. To best assist you, call when you are at a computer if possible.
- Error Code [42] - The information you provided was not found or there may be an error on the record in Defense Enrollment Eligibility Reporting System (DEERS). Ensure you are using your legal first and last name. If you are using your legal name or your name has changed, go to the simplified FAQs for what actions a user must take to update their information or you can contact the DMDC Customer Contact Center at 800-368-3665 for assistance.
- Error Code [43] - We are unable to locate your record based on the information you entered. If this continues contact the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.
- Error Code [44] - We are unable to locate your record based on the information you entered. Try again. If this continues contact the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.
- Error Code [45] - We are unable to locate your record based on the information you entered. Try again. If this continues contact the DMDC Customer Contact Center at 800-368-3665 for further assistance. To best assist you, call when you are at a computer if possible.
- Error Code [46] - The system is currently unavailable. Try again later. If this problem continues, you may contact the DMDC Support Center (DSC) at 800-477-8227 for assistance. To best assist you, call when you are at a computer if possible.
- Error Code [47] - The system is currently unavailable. Try again later. If this problem continues, you may contact the DMDC Support Center (DSC) at 800-477-8227 for assistance. To best assist you, call when you are at a computer if possible.
- Error Code [50] - We have located your Defense Enrollment Eligibility Reporting System (DEERS) record; however, it appears there may be invalid information on file. You may contact the DMDC Customer Contact Center at 800-368-3665 for assistance. To best assist you, call when you are at a computer if possible.
- Error Code [53] - Your Common Access Card (CAC) certificates are invalid and access is revoked. If you believe you have received this message in error you may contact the DMDC Customer Contact Center at 800-368-3665. To best assist you, call when you are at a computer if possible.
- Error Code [54] - Your Common Access Card (CAC) is expired and access is revoked. Visit your nearest ID card facility to obtain a new card. You can locate the nearest ID facility at RAPIDS Site Locator.
- Error Code [55] - Your Common Access Card (CAC) is reported as lost and access is revoked. Visit your nearest ID card facility for assistance with obtaining a new card. You can locate the nearest ID facility at RAPIDS Site Locator.
- Error Code [56] - Your Common Access Card (CAC) is terminated and access is revoked. Visit your nearest ID card facility to obtain a new card. You can locate the nearest ID facility at RAPIDS Site Locator.
- Error Code [57] - The system is currently unavailable due to an outage within another internal system. We hope to have the issue resolved soon, so try again in a few hours. If this problem continues after that time period, you may contact the DMDC Support Center (DSC) at 800-477-8227 for assistance. To best assist you, call when you are at a computer if possible, and be prepared to provide your Personal Identifiable Information if asked to research your specific record.

- Error Code [62] - Your CAC has been identified as having excessive access which has been flagged as potential fraudulent access. In order to protect your PII and PHI, please contact the DMDC Customer Contact Center (CCC)
- at (800)-368-3665 to go through their identity verification process which includes submitting state or federal issued identity documents.
- Person Error Code [p1] - The personal information you provided was not found in Defense Enrollment Eligibility Reporting System (DEERS). Try again.
- Ensure that you enter your personal information accurately, using your legal first and last name. If your name has changed since you or your sponsor served, contact the DMDC Customer Contact Center at 800-368-3665 for assistance with changing your name in DEERS. Veterans (and their family members/dependents) may contact the Department of Veterans Affairs (VA) to have your identity validated and added to DEERS. You may also call the VA at 800-827-1000 for assistance directly, and say "eBenefits" when you are prompted for the reason for your call. You are responsible for keeping your information current in your DEERS record. You must take action to register your family members/dependents and ensure they are correctly entered into DEERS. Once registered in DEERS it is important to keep your DEERS records updated when personal eligibility information changes. This includes contact information and family member status (marriage, divorce, birth, adoption, etc.).
- Person Error Code [p2] or [p3] or [p10] - We have located your Defense Enrollment Eligibility Reporting System (DEERS) record; however, it appears there may be invalid information on file. You may contact the DMDC Customer Contact Center at 800-368-3665 for assistance. To best assist you, call when you are at a computer if possible.
- Person Error Code [p4] or [p5] - The personal information you provided was not found in Defense Enrollment Eligibility Reporting System (DEERS). Try again. If this problem persists, you may contact the DMDC Customer Contact Center at 800-368-3665 for assistance. To best assist you, call when you are at a computer if possible.
- Person Error Code [p6] - Based on the information you provided, your Defense Enrollment Eligibility Reporting System (DEERS) record reflects that you are ineligible to obtain a DS Logon. Veterans (and their family members/dependents) may contact the Department of Veterans Affairs (VA) to have your identity validated and added to DEERS. You may also call the VA at 800-827-1000 for assistance directly, and say "eBenefits" when you are prompted for the reason for your call.
- Person Error Code [p7] or [p8] or [p9] - The personal information you entered does not match the information found in Defense Enrollment Eligibility Reporting System (DEERS). If this problem persists, you may call the DMDC Customer Contact Center at 800-368-3665 for assistance. If you are enrolled in DEERS but your name has changed since you served, contact the DMDC Customer Contact Center at 800-368-3665 for assistance with changing your name in DEERS. To best assist you, call when you are at a computer if possible.
- Identity Proofing Error Code [i1] - We are unable to remotely verify your identity. See the FAQs for alternative methods for identity verification.
- Identity Proofing Error Code [i2] - You have reached the maximum number of attempts to remote proof your identity. You will need to in-person proof to verify your identity
- Identity Proofing Error Code [i3] - DSL is unable to verify your identity remotely. Please use other options (e.g., in-person) to complete the verification process.

- Identity Proofing Error Code [i4] - At this time, we are unable to remotely proof your identity. Pursue our In-Person identity proofing options to verify your identity.
- Identity Proofing Error Code [i5] - The time limit for the remote proofing has expired. You can try again or visit the FAQs for alternative methods for identity verification.
- Identity Proofing Error Code [i6] - The remote proofing service is unavailable. You can wait and try again or visit the FAQs for alternative methods for identity verification.
- Identity Proofing Error Code [i7] - We are unable to remotely proof your identity. Pursue our In-Person identity proofing options to verify your identity.
- Identity Proofing Error Code [i8] - You are only allowed one session at a time to remote proof your identity. Close all your windows and try again.
- Identity Proofing Error Code [i9] - DS Logon is unavailable. Try again later or you can visit the simplified FAQs for further options.
- Identity Proofing Error Code [i10] – At this time, we are unable to remotely proof your identity.
  (Note: this is due to there not being enough credit history on file to verify your credit history. You will not be able to proof your identity online)
- Identity Proofing Error Code [i11] - We are unable to continue to remote proof your identity at this time. If you are initially logging in, please try a different device (e.g., computer, tablet, phone). If you are in the middle of remote proofing your identity, please refer to our FAQs for an alternative option.

I NEED HELP!

First, **READ** the FAQs located in **Need Support?** All of the information for self-help is in the FAQs. If you come across a subject that is not in the FAQs and you still need help, you can contact a call center.

Organization	Contact and operation hours	Helps With
DMDC Customer Contact Center	Phone: 800-368-3665 Hours: Monday-Friday 5am – 5pm PT	DEERS, CAC Issues, identity proofing, and DSL account information. THIS HELPDESK CANNOT HELP A VA USER WITH ID.ME or LOGIN.GOV
RAPIDS Site Locator	https://idco.dmdc.osd.mil/idco/	
Veteran Affairs (eBenefits)	Phone: 800-827-1000 Hours: Monday-Friday 5am – 6pm PT	Veteran adding an identity to DEERS, Benefits Questions, such as GI Bill, Claim Status or Disability Benefits
Veteran Affairs (eBenefits)	Phone: 800-983-0937 Hours: Monday-Friday 5am – 5pm PT	Technical Issues, such as password changes or error codes

Other Partner Helpdesks

Organization	Contact Info

Health Net Federal Services, LLC (TRICARE West Region)	1.844.866.9378
Humana Military (TRICARE East Region)	1.800.444.5445
US Family Health Plan	1.800.748.7347
TRICARE Dental Program (UCCI)	1.844.653.4061
Active Duty Dental Program (UCCI)	1.866.984.2337
TRICARE For Life	1.866.773.0404
TRICARE Mail Order Pharmacy (Express Scripts, Inc.)	1.877.363.1303
Military Health System Help Desk	1.800.600.9332
TRICARE Retail Pharmacy (Express Scripts, Inc.)	1.877.363.1303
Federal Employees Dental and Vision (FEDVIP)	1.877.888.3337
Military Medical Support Office	1.888.647.6676