DS Logon (DSL)
Support Documentation and FAQ

Release 4.05
Document Date: September 5, 2024
Production: August 17, 2024

NOTE: Since the Support Documentation is frequently updated, printing or publishing this document is not recommended.

TIP: To search, press Control and the letter F at the same time. Type in key word(s) to search the document. Users can also use the hyperlinks in the Table of Contents.

Contents

IMPORTANT ACCOUNT SECURITY INFORMATION: Always **close** your web browser and all tabs after logging out of DSL. If not, personal information may still be accessible due to individual computer and browser caching. **This is extremely important when sharing a computer or using a public computer.**

DSL BASICS

DS Logon (DSL) is a single sign-on web application, letting users access their information across multiple DoD partner websites with a single password or login. Users can view personally identifiable information (PII), Personal Health Information (PHI), claim status, and records.

Accessing DSL

Visit the DSL homepage on your computer, tablet, or mobile device. Users with active accounts can log in using username/password, CAC, or DoD-issued PIV.
Recommended browsers are Chrome, Edge and Safari.

DO NOT use any URL starting with webct2. That is an internal test site, not DSL.

Account Eligibility

Per DoD Policy,[1] a user must be:

- 18+ years old, affiliated with the DoD or VA and listed in the Defense Enrollment Eligibility Reporting System (DEERS) as a **Service Member** (Active, Guard, Reservist, Retiree), **Veteran**, **Dependent** (e.g., spouse, ex-spouse, surviving spouse, and/or adult child receiving DoD Benefits), **DoD Civilian**, or **Contractor**.

Login Options

- CAC – Log in with CAC if you have a smart card reader
- Username/password – All users have the ability to log in using a password and the unique username assigned at registration
- PIV – Log in using your DoD-issued PIV card and smart card reader
    - Note: When first logging in, select the PIV tab on the DSL homepage and register your PIV by entering your name, date of birth, person identifier, and DSL username/password. After this one-time PIV registration, you can use your PIV to log into DSL. You will need to re-register the PIV if your DSL account is deactivated. To log in with your PIV, your DSL account must be active.

Creating an Account

DSL allows users to create an account in several ways:

- **CAC registration** requires an active CAC card and smart card reader.
- **Email registration** requires a unique email address on file in DEERS (meaning no other person or family member has the same email listed in DEERS).

[1] DoDM 1341.02 Vol 1

- **In-person proofing** requires a user to bring I-9 documents and photo ID to a Veteran Affairs Regional Office or RAPIDS office; used only when issuing a new ID.
- **Remote identity proofing** requires the user to answer personally identifying questions and/or upload identification documents.

At least one phone number is required. Users cannot register for an account or two-factor authenticate without a valid phone number on file.

Detailed information on creating an account is provided in our Registration Tips & Support section. Visit that section before trying to create an account to have everything you need.

MAINTAINING YOUR ACCOUNT

Requirements to Keep Your Account Active

- Login at least once every 180 days (6 months)
  - Users will receive an email reminder to sign in before the account is deactivated
- Reset the password every 60 days (2 months)
  - Users will be prompted to change the password before it expires
- Update information (e.g., name, address, phone numbers, email) on your DEERS record as needed

Changing Your Password

To change a password, log into your account and select Change Password from your Profile page. The Change Your Password screen lists the criteria that your new DSL password must meet. Passwords can only be changed once every 24 hours and MUST be changed every 60 days. If you forgot your password, visit the DSL homepage and select Forgot Password?

The DMDC Customer Contact Center (CCC) cannot create or change passwords.
Temporary one-time use passwords are not provided.

Updating Your Challenge Questions

Challenge questions are used in the event of a forgotten password or account suspension.

Under Change DS Logon Account on the Profile page, select Change Challenge Questions. You will be prompted to update all five questions. The DMDC Customer Contact Center (CCC) cannot create, change or remove challenge questions.

Tips for choosing challenge questions:

- Be sure that none of your social media accounts contain the answers.
- Ask yourself, “Will I remember this answers a year from now?”

Adding, Updating and Correcting Information

- Users can update their address, email address and/or phone number(s) by logging into DSL and selecting Update Contact Information.
- Users can also update home address, email address and/or phone number by logging into ID Card Office Online (IDCO). Go to "My Profile" and select "Continue." Then, go to the bottom of the screen after updating the information and click "Submit."
- If the above options do not work, contact the DMDC Customer Contact Center (CCC) to update information. Verification documents may be requested and can be submitted via mail or fax. Note: Dependents over 18 must update their own information.
- For in-person updates, make an appointment at a RAPIDS station.

Restoring Access If Your Account Is Deactivated, Suspended, or Locked

- **Deactivated:** You can register for a new account and will need to complete the identity verification process again. Users can choose to deactivate their account at any time by choosing “Deactivate Account.”
  Note: Accounts will be deactivated due to inactivity in 180 days (6 months).
- **Suspended:** Log into DSL and select Un-suspend My Account or Forgot Password? Answer the challenge questions correctly. You’ll be prompted to change the password.
  - Note: An account can be suspended due to incorrect password attempts. The DMDC Customer Contact Center (CCC) cannot unsuspend a user’s account.
- **Locked:** DSL accounts can be locked for a variety of reasons, including unusual activity. Accounts cannot be unlocked by the user. Account locks can only be unlocked by the CCC if the account was locked by DMDC. Contact the CCC to request your account be unlocked. If your account was locked by the Veteran Affairs Office, the CCC may advise you to contact the VA if the CCC is unable to remove the lock.
  Note: DSL can lock and re-lock an account at any time, without notice, if there is suspected fraudulent or unusual activity. DSL has measures to ensure the protection of users’ accounts, such as locking an account from additional access.

ACCOUNT SECURITY OPTIONS

Two-Factor Authentication (2FA)

- Users logging in with a username/password will be prompted to confirm their phone number and select either a text or voice message. A one-time PIN (OTP) will be provided to the selected phone number. Enter the 5-digit PIN into the DSL login screen and click “Submit.” Message and data rates may apply.
- The code expires in 5 minutes. You can request a new code after 30 seconds. A user has 2 attempts to enter the OTP correctly or a lock-out for 1-hour will occur.

- IMPORTANT: DMDC Customer Call Center (CCC), VA call centers, and DSL are not able to remove the 1-hour lock-out.

Multi-Factor Authentication (MFA)

- For additional security, users have the option to setup MFA using an authenticator app (e.g., Authy or Microsoft Authenticator), which must be downloaded on the user's device. Cookies must be enabled on the device; follow the app's instructions for setup on your device.
- Users can choose to set up MFA for DSL anytime from the Profile page after successful login and can also remove MFA after successful login.
- If the user no longer has the device the app is installed on, they can contact the CCC to request MFA be removed.
- If MFA is set-up, the user will not be required to 2FA.

Tips for Keeping Your DSL Account Secure

- **Do not** give username/password information to anyone, not even family.
- Be sure your device's software and malware/virus protection are up-to-date, and only install software from the software provider's official website. Do not click on any emailed links to install something.
- Proactively verify accounts and data (e.g., eBenefits, bank accounts, credit reports, DSL) on a monthly basis to ensure information is still accurate.
- Users who suspect their account has been compromised or hacked should change the password and challenge questions immediately, verify banking information is still accurate, and consider freezing their credit report.
- Be cautious of messages, links and ads on social media, as those can contain viruses. When in doubt, do not click on them.
- The CCC and DSL team will NEVER initiate first contact with users via email or telephone to request PII or sensitive DSL account information (username, password, challenge questions). If you think there is a fraudulent email, website or phone call, log into your DSL account and immediately change the password and challenge questions.

ACCESS FOR DEPENDENTS AND FAMILY MEMBERS

Users can both grant and be granted access to eligible family members' information. If a user has more than one sponsor, the user can select the preferred sponsor by selecting Change Sponsor on the Profile page, as benefits may vary under different sponsors.

> **IMPORTANT:** DSL allows you to authorize individuals to act on YOUR behalf. Others can authorize you to act on THEIR behalf. Sponsors can view their information as well as any dependent information. Clinical Access authorizes full access to medical records for that individual. Be mindful that these authorizations remain active until the authorizing individual revokes them within the DSL application. The user can manage their

relationships by logging into DSL, selecting Manage Relationships, then selecting Add Relationships, and selecting the option that applies. Refer to Need Support? on the Home page for more information.

Granting Access

Within your profile, you can select eligible family members to act on your behalf. These authorizations remain active until you remove them.

- Under Relationships, select Change Relationships.
- Select Add Permission under "People who can act on my behalf."
- You can select eligible family members and the permission type to be granted.
- Select a date range for the permission, "Save," then "Finish" to save the update.
- **Note:** Clinical access authorizes full access to medical records for that individual.

Families with a Military Sponsor

Sponsors can see their own information and any spouse's or dependent's information.

Example: one spouse is an Active Duty Service Member (the Sponsor). The other spouse is the Dependent, along with the couple's 3 children. Depending on the partner application being accessed, the Sponsor can view the dependent spouse's full medical records along with the children's.

Families with Dual Sponsors

In order to view Dependents, the Sponsor who is receiving the benefits must log in, go to Relationships, and give permission to their spouse. Note that the spouse will also need to have an active DSL account. Currently, a dual sponsor spouse must log into DSL with username/password and not their CAC to see the other dependents' (e.g., children's) information.

Surrogate DSL Accounts

Surrogacy is a legal status that allows an individual to act on behalf of another individual for specific purposes, even if they are not family. It is a legally established status, not something established by DSL. Users who require a surrogate can have their surrogate create a DSL account to manage the user's needs. Surrogate accounts will only be established after an individual has been legally deemed a surrogate to a DoD Beneficiary.
The individual will need to:

- Be added to DEERS by going to local military issuing Identification (ID) card facility (RAPIDS Site Locator).

- Contact the facility to make an appointment and communicate that the appointment is to establish surrogacy. The facility will advise what documents are required. These identity documents are for the surrogate, not the DoD Beneficiary.
- Fill out the DD Form 3005 "Application for Surrogate Association for DoD Self-Service (DS) Logon" (find DD 3005 here) and bring the completely filled out form to the appointment. The form will need to contain all required signatures such as a certifying official: Staff Judge Advocate (SJA), Judge Advocate General (JAG), legal representation, or Service Project Officer (SPO). If the form does not have all signatures prior to going to the facility, the form will be rejected.
- Bring all supporting court documentation to the appointment.
- Confirm with the RAPIDS operator that your phone number is on file and current; at least one phone number is required. Users cannot register for an account or two-factor authenticate without a valid phone number on file.
- After the surrogate identity is added to DEERS, an email will be sent to the surrogate that contains account activation instructions if an email is on file.
- The surrogate's account will remain active no longer than 4 years. If the DoD beneficiary is no longer eligible for a DSL account, the surrogate's account will automatically be deactivated.
- Note: Not all DMDC partner websites allow surrogate access.

REGISTRATION TIPS AND SUPPORT

What Method of Registration Should I Use?

User Type	Preferred Registration Method	Alternate Registration Methods
Service Members	CAC	• Email Registration • In Person at a RAPIDS station (only when new ID card is being issued)
Military Family Member/Dependent	Email Registration	• In Person at a RAPIDS station (only when new ID card is being issued) • Remote Identity Proofing • Sponsor Request
Retirees Retiree Family Member/Dependent	Email Registration	• In Person at a RAPIDS station (only when new ID card is being issued) • Remote Identity Proofing
Veterans Veteran Family Member/Dependent	Remote Identity Proofing	• Remote Identity Proofing • DS Logon • login.gov • ID.me • My HealtheVet
Other		Choose the applicable option: • In-person • CAC • Email • Remote Identity Proofing

Register with a CAC

- On the DSL homepage, select the CAC tab and log in.
- After you've successfully authenticated, select "Register for a DS Logon Account" (next to your name) and follow the steps within the application.

Register Using Email

- Confirm you have a unique email address on file in DEERS (meaning no other family member has the same email address in DEERS). You will not be able to register if you do not have a unique email address on file.
- On the DSL homepage, select the "Create New Account" button.
- Choose "Email Registration" and follow the steps within the application.
- You will receive an activation code via email within 24 hours.
    - **Note:** If you do not receive the email, check your junk/spam folder.
- Use the link provided in the email or go directly to the DSL homepage and click the "Activate Account" button.
- Enter the required personal information and requested activation code.
- The system will display your unique username assigned to you.
- Select "Continue" to activate your account.

Register In-Person

IMPORTANT: This option can ONLY be used when a DoD ID card is being issued.

- Make an appointment at a RAPIDS station **(**RAPIDS station locator).
- Bring all necessary identifying documents. Typically two I-9 documents are required. Contact the site to confirm what documents are needed. Documents cannot be expired. Acceptable I-9 documents that may be requested are:
    - **Primary:** Picture ID issued from Federal or State Government (e.g., driver's license, valid passport, 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, ID card by local government with DOB, gender, height, eye color, and address
- At your appointment, notify the Verifying Official (VO) that you would like a DSL account.
- Provide the VO with your unique email address and follow the steps they provide.
- Users will receive an activation code via email with 24 hours.
    - **Note**: If you do not receive the email, check your junk/spam folder.
- Use the link provided in the email or go directly to the DSL homepage and click the "Activate Account" button.
- Enter the required personal information and requested activation code.
- The system will display the unique username assigned to you.

- Select “Continue” to activate your account.

Register with Remote Identity Proofing

IMPORTANT: Do not remote identity proof unless email registration and card issuance at RAPIDS are unavailable. Remote identity proofing should be your last option.

- Read the entire Remote Identity Proofing Procedures and Support section before starting the registration process.
- On the DSL homepage, select the “Create New Account” button.
- Choose “Remote Identity Proofing” and follow the steps within the application.
- Complete the required steps **all at one time**. You may need to upload photos of identity documents, answer knowledge-based questions, take a selfie, and provide credit card and/or loan account information.
- If the identity verification is successful, you will receive a username and an active DSL account.
- The system will display the username assigned to you.
- Select “Continue” to activate your account.

  Note: DO NOT USE your Retiree or Military Dependent card for the documentation upload. All documents must be non-military, U.S. issued and cannot be expired.

Register a Family Member with a Sponsor Request

- For the Military Sponsor:
  - Log into DSL using your CAC.
  - Under Relationships, select “Register DS Logon for my Dependents.”
  - Select the dependent that needs a DSL account (only eligible dependents will appear as options).
  - An activation email will be sent within 24 hours to the dependent’s email on file in DEERS. Once this option has been selected, the dependent must wait for the activation code or 20 days before trying any other registration method.

- For the dependent:
  - Use the link provided in the email or go directly to the DSL homepage and click the “Activate Account” button.
  - Enter the required personal information and requested activation code.
  - The system will display the username assigned to you.
  - Select “Continue” to activate your account.
  - Users who have more than one sponsor can select the preferred sponsor. There may be different benefits associated with different sponsors. To change sponsors, select Change Sponsor from the Profile screen, then select the desired sponsor and click “Finish.”

REMOTE IDENTITY PROOFING SUPPORT

READ ALL OF THIS SECTION BEFORE BEGINNING THE PROCESS

The remote identity proofing process involves uploading specific documentation, submitting a selfie, entering partial credit card/loan account numbers, and/or answering knowledge-based questions. The process takes approximately 10 minutes and must be completed at a single time, within the time limit provided.

Remote Identity Proofing FAQS

- **What items and information do I need to complete the process?** Be sure to have the following items available BEFORE the process begins:
  - Driver's license
  - Computer with a web camera or cell phone with a camera
  - Phone associated with the phone number on your DEERS record (to receive a one-time PIN)
  - Accepted credit cards and/or loan documents (**Note:** Not all credit cards can be verified by the proofing vendor. Refer to the full list in the Financial Account Information section below.) You are not required to enter the full credit card number, expiration date, or CVV. You will not be charged.

- **What devices can be used?** If using a mobile device, it is recommended the device be no older than 5 years old, for example:
  - iPhone 8 on iOS 12 or above
  - Android OS9 or above

- **Is there an expedited process if I need access for enrollments?** To maintain the level of security mandated, there is not an expedited process. If you have a limited timeframe to enroll or submit documents on a partner website, be sure to read the entire identity proofing section so you can be prepared with everything you need. DSL is not responsible for users that miss partner deadlines.

- **How is my credit information used?** The information used in remote identity proofing is pulled using a soft inquiry on a user's credit report. This means it does not impact your credit score and is not used for any other purpose except to verify identity at a single point in time. The data, identity documents, and information provided are not used in data mining or for any other purpose except one-time identity verification.

- **Will my information be secure during registration?** DSL has implemented the required policies, procedures and regulations from the National Institute of Standards and Technology (NIST) which provides instruction and standards for remote verification. All information sent to the data vendor is encrypted.

Remote Identity Proofing Procedure

You may be asked to complete one or more of the following identity proofing steps.

Knowledge-Based Questions

- During the registration process, users may be prompted to answer multiple choice questions regarding their background or information that only the user will know.
- If the data vendor is able to verify answers are correct, the user will successfully pass this step.

Financial Account Information

- Users may be prompted to enter the last 8 digits of a credit card or the entire loan account number for verification of a credit card or loan in their name.
- Credit card expiration date and security code are NOT required and there is NO hold or charge placed on the credit card. This is for identity verification only.
- If the data vendor is able to verify answers are correct, the user will successfully pass this step.
- The following cards are **NOT accepted**: American Express, Debit, Barclays, Kohl's, Utility, Cash Back, Student, Balance Transfer, and Travel Rewards Cards.
- The credit card cannot be in dispute, suppressed, frozen or expired, and must be in the user's name and on the user's credit report. If you need to unfreeze a credit card for verification, you are responsible for reestablishing the credit card freeze.

Document Upload

- Users may be prompted to upload a U.S. identity verification document and take a selfie (a selfie is a picture of one's full face with nothing else in it or beside it).
- Users on a computer may be prompted to select an image stored on their device instead of taking a picture, or may need to seek assistance from a friend or family member when capturing documents and/or selfies.
- Default settings are recommended. Only .jpg format images are supported, with size 480x640 or greater, 24-bit color and at least 250 dpi. If the photo takes several minutes to upload, the photo may be too large.
- When finishing uploading U.S. documents, click on Verification Status after one (1) minute to monitor the status of the request.
- The following documents **cannot be uploaded** for verification: Military ID, Veteran/DAV, Dependent ID card, PIV card, expired ID card and/or foreign-issued documents. (The data vendor is unable to verify these documents.)

Accepted Document Uploads	NOT Accepted
• U.S. Issued • Valid (Unexpired) • Clear, easy to read • Entire document is visible • Document is on a solid color surface • Original copy	• Military or VA Issued • Photocopy • Damaged or altered • Expired • Foreign Issued • Poor photo capture (glare, parts cut off, or partially hidden)

Identity Document Upload Tips

- Use a smart device (e.g., cell phone) with a camera.
- Lay the document on a flat surface with a dark, solid background. Don't hold the document when taking the picture or place the document on your lap.
- Take the pictures from directly above and not at an angle.
- Avoid glass tables or mirrors that reflect camera flash.

Selfie Do's and Don'ts

- ✓ Use a solid background – similar to a driver's license or passport photo
- ✓ Look straight into the camera
- ✓ Include your face only
- ✓ Ensure your face fills most of the photo
- ✓ Check that the photo is clear and not blurry before uploading

- **X** Don't wear glasses, hairstyles that cover the face, hats, or face masks
- **X** Don't use a "busy" background (posters, framed photos, bookcases with lots of items)
- **X** Don't use a filter
- **X** Don't use a mirror due to glare issues
- **X** Don't turn your head sideways
- **X** Don't upload a photo of a photo or a professional portrait
- **X** Don't take a picture of a phone screen or upload a photo of an ID saved on a phone
- **X** Don't include pets or other people – even partial faces or framed photos in the background can result in a failing submission

Remote Identity Proofing Troubleshooting

Issue	Action to Take
Received an Error	Refer to the Error Codes in this document. The error code will include information on what to do next.
Credit Report Is Frozen	Unfreeze your account temporarily, then re-add the freeze when proofing is completed successfully.
Address Isn't Being Accepted	Ensure your address is updated on your DEERS record. Update your address on your credit card(s) so accurate information is being reported to credit agencies.

Received an Identity Proofing ("i") Error	If you are not able to remote identity proof, you may still be able to register via email or complete in-person proofing. See the Registration Tips and Support section to review the requirements. Too many failed attempts at remote identity proofing will result in a 31-day lockout that cannot be removed by the CCC. Additional attempts will restart the 31-day period.

ADDITIONAL SUPPORT

All the information needed for self-help is in this Support Documentation. If you still need assistance, contact the CCC or relevant partner helpdesk.

VETERANS: For issues with non-DSL credentials on VA websites, contact the helpdesk for the credential being used, i.e. DS Logon, login.gov, ID.me, and My HealtheVet.

Contact Centers

Organization	Contact and Operation Hours	Helps With
DMDC Customer Contact Center (CCC)	Phone: 800-368-3665 Hours: Mon-Fri 5am – 5pm PT	DEERS data, CAC issues, DSL account information The CCC does **not** help with ID.me, login.gov, or MyHealtheVet
RAPIDS Site Locator	https://idco.dmdc.osd.mil/idco/	Locating ID Facilities

Other Partner Helpdesks

Organization	Contact Info
TRICARE West (previously Health Net Federal Services, LLC)	1.844.866.9378 (WEST)
VA (Data issues)	1.800.827.1000
VA (Technical issues)	1.800.983.0937
Humana Military (TRICARE East Region)	1.800.444.5445
US Family Health Plan	1.800.748.7347
TRICARE Dental Program (UCCI) United Concordia	1.844.653.4061
Active Duty Dental Program (UCCI)	1.866.984.2337
TRICARE For Life (TFL)	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

Error Codes

- **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 your 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 New 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 the letter, ensure you 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. For additional information, refer to our Support Documentation and FAQ located in Need Support? on the Home page.
- **Error Code [10]** - The DS Logon username or password you entered is INVALID. Do you need to register for a DS Logon? Refer to our Support Documentation and FAQ located in Need Support? on the Home page prior to registering.
- **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. Refer to our Support Documentation and FAQ located in Need Support? on the Home page prior to registering.
- **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 our Support Documentation and FAQ located in Need Support? on the Home page to verify 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 refer to our Support Documentation and FAQ located in Need Support? on the Home page.

- **Error Code [34-35-36]** - 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 and 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. The DMDC Customer Contact Center (CCC) cannot assist when systems are unavailable.
- **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 (CCC) 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 (CCC) 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 (CCC) at 800-368-3665 for further assistance. 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, refer to our Support Documentation and FAQ located in Need Support? on the Home page for what actions a user must take to update their information or you can contact the DMDC Customer Contact Center (CCC) at 800-368-3665 for assistance.
- **Error Code [43-44-45]** - We are unable to locate your record based on the information you entered. If this continues contact the DMDC Customer Contact Center (CCC) 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] or [49] -** 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. The DMDC Customer Contact Center (CCC) cannot assist when systems are unavailable.
- **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 (CCC) 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 (CCC) 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. The DMDC Customer Contact Center (CCC) cannot assist when systems are unavailable.
- **Error Code [61]** – We couldn't access your DEERS record, possibly due to a data error on your record. Try again later. If this problem continues, you may contact the DMDC Customer Contact Center (CCC) at 800-368-3665 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 and request approval to be unlocked.
- **Error Code [63]** - There was a problem reading your PIV. Make sure your PIV is valid, fits tightly in your smart card reader, and the reader is connected to your machine.
- **Error Code [64]** - You do not have a DS Logon account. Refer to our Support Documentation and FAQ located in Need Support? on the Home page prior to registering. Select 'Create New Account' and complete registration.
- **Error Code [65]** - You do not have an active DS Logon account. Refer to our Support Documentation and FAQ located in Need Support? on the Home page prior to registering. Select 'Create New Account' and complete registration.
- **Error Code [66]** - Your PIV is not registered. You will now be redirected to complete your PIV registration.
- **Error Code [67]** - Your PIV cannot be registered with the current DS Logon credential.
- **Error Code [68]** - Select the CAC tab to login using your CAC.
- **Error Code [69]** - Your account has been deactivated. You can create a new account by selecting Create New Account.
- **Error Code [70] -** There was an issue with your request. Press Continue to try again. If the problem persists, clear your cookies, cache, and close your browsers on all devices you may have used to access this site.
- **Error Code [71] -** An active session has been detected. Clear your cookies, cache, and close your browsers on all devices you may have used to access this site.
- **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 (CCC) at 800-368-3665 for assistance with changing your name in DEERS. Refer to our Support Documentation and FAQ located in Need Support? on the Home page for more information.

- **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 (CCC) 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 (CCC) 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. Refer to our Support Documentation and FAQ located in Need Support? on the Home page for more information.
- **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 (CCC) 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 (CCC) 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. Refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative methods for identity verification.
- **Identity Proofing Error Code [i2]** - You have reached the maximum number of attempts to remote proof your identity and must wait 31 days. You may be able to in-person proof to verify your identity. Refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.
- **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. Refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.
- **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 or refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.
- **Identity Proofing Error Code [i5]** - The time limit for the remote proofing has expired. You can try again in 1 hour or refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.
- **Identity Proofing Error Code [i6]** - The remote proofing service is unavailable. You can wait and try again or refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.

- **Identity Proofing Error Code [i7]** - We are unable to remotely proof your identity. Pursue our In-Person identity proofing options to verify your identity or refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.
- **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 in 30 minutes.
- **Identity Proofing Error Code [i9]** - DS Logon is unavailable. Try again later or you can visit our Support Documentation and FAQ located in Need Support? on the Home page for alternative 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.) Refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.
- **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, refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.
- **Identity Proofing Error Code [i12]** - You have reached the maximum number of attempts to remote proof your identity and cannot remote proof again for 31 days. The DMDC Customer Call Center (CCC) cannot re-establish the capability to remote proof again prior to the 31 days. For additional information or alternative options, refer to our Support Documentation and FAQ located in Need Support? on the Home page for alternative options.
- **One-Time PIN Error Code [otp3]** - You have exceeded the number of times allowed to enter your PIN. In order to protect your account, the account has been locked for 1 hour. Try again in 1 hour. The DMDC Customer Call Center (CCC) cannot remove this 1 hour lock out.