Department of Defense COVID-19 Response

Guide for Cardholders to Use Temporary Capability for CAC/VoLAC Certificate Update

To ensure DoD ID card offices are postured to maintain continuity of operations and to minimize the number of non-essential visits to DoD ID card offices, the Department has enabled a temporary capability to allow cardholders to update their certificates on soon-to-expire Common Access Cards (CACs) and Volunteer Logical Access Credentials (VoLACs).

This guide provides step-by-step instructions for cardholders to use the temporary capability to update their certificates.

Summary

Am I eligible? ........................................................................................................................................... 1

What is the process? .................................................................................................................................. 2

Who do I contact if I have problems? ....................................................................................................... 10

____________________________________

Am I eligible?
To be eligible to update your certificates on your CAC or VoLAC, all of the following must be true:

1. **The CAC or VoLAC must expire within 30 days.**
   - For example, you can update a CAC that expires on 30 May 2020 no sooner than 1 May 2020.

2. **The CAC or VoLAC must be unexpired when attempting to update the certificates.**

3. **The CAC or VoLAC holder must have an active Affiliation which extends beyond the ID card expiration date.**

4. **The CAC or VoLAC holder must use a computer that is properly configured to support IDCO certificate updates.**
   - All operations that update your CAC or VoLAC require ActivClient 7.1 or higher, Java 8 update 144 or higher, and Internet Explorer version 7 or higher. Please ensure your computer meets these minimum requirements.
What is the process?

1. Open Internet Explorer (version 7 or higher).


3. Login with your CAC.
   - Click through the prompts to login with your CAC.
     - You must login to IDCO using your CAC (VoLAC will also be accepted under CAC login). If your card or certificates have already expired, you will not be able to login.
     - If you login using DS Logon, you will not be able to update the certificates on your CAC or VoLAC.

4. Confirm that your “Affiliation” exists beyond your current card end date.
- If IDCO indicates your “Affiliation” end date is beyond the expiration date printed on your card, proceed to STEP 5.
- If you are a Uniformed Service member or civilian employee with no defined Affiliation end date (e.g., “UNKNOWN”), proceed to STEP 5.
- If you are a Uniformed Service member (e.g., enlisted Service members) or civilian employee with a defined Affiliation end date that coincides with your card end date, contact your Human Resources (HR) personnel.
  - HR personnel must first update your affiliation with DoD in DCPDS or MILPDS before you can use IDCO to update your certificates.
  - You must wait one business day following the date of the HR update. If your affiliation end date is not updated in IDCO after one business day, contact your HR personnel.
- If you are a contractor and other personnel sponsored via the Trusted Associate Sponsorship System (TASS) with a defined Affiliation end date that coincides with your card end date, contact your TASS Trusted Agent (TA) or Contracting Officer (CO)/Contracting Officer Representative (COR).
  - The TASS TA must first update your affiliation with DoD by creating a new TASS application before you can use IDCO to update your certificates.
    - This is the same process the TASS TA would follow to sponsor you for a new CAC. TASS TAs should use the new contract end date (including unfunded contract options) for the new TASS application.
  - You must wait one business day following the date your TASS application was approved. If your affiliation end date is not updated in IDCO after one business day, contact your TASS TA.
5. **Confirm that your “Card Expires” date is beyond the expiration date printed on your CAC or VoLAC.**
   - If IDCO indicates your “Card Expires” date is beyond the expiration date printed on your card, proceed to STEP 6.
   - If IDCO indicates your “Card Expires” date is **NOT** beyond the expiration date printed on your card and you are a Uniformed Service member or civilian employee:
     - Wait one business day following the date of the HR update before using IDCO.
   - If IDCO indicates your “Card Expires” date is **NOT** beyond the expiration date printed on your card and you are a contractor and other personnel sponsored via TASS, contact your TASS TA or CO/COR.
     - Wait one business day following the date of the approval of the TASS application before using IDCO.

6. Select “Change CAC Email” to begin the email certificate update process.
• IDCO will replace your expiring email signing and email encryption certificates with certificates valid through the updated expiration date.
• IDCO will read contents of the chip to validate the current email certificates.
7. **Authorize the IDCO applet to run on your PC.**
   - Click “Run”.

8. **Wait for IDCO to read the contents of the CAC chip.**
   - IDCO will display progress monitors for various processes including reading the data from the card and checking the certificate status.

9. **Confirm email address.**
   - IDCO will display the “Current email address” which was used to create the current email certificates, and the “Email address provided by your organization” which is based on standards provided by your DoD Component.
   - If the “current email address” and “email address provided by organization” are the same and you do not need to change your email address:
     - Click “Next” without checking either box to proceed with certificate update.
   - If the “Current email address” and “Email address provided by organization” are the same, and you need to change your email address:
- Check the box to “Change from email provided by your organization to another email address”.
- Click “Next”.
- Enter your preferred email address. Most organizations prescribe the required email address format, which (in most cases) is the email on the CAC; however, some individuals are permitted to use non-standard email formats. IDCO allows this update but restricts the email to approved email extensions. For questions about your organization’s email formats, contact your Service Helpdesk.

- If the “Current email address” and “Email address provided by organization” are different, and you would like to keep the current email address or change to a new email address:
  - Check the box to “Change from email provided by your organization to another email address”.
  - Click “Next”.
  - Enter your preferred email address. Most organizations prescribe the required email address format, which (in most cases) is the email on the CAC; however, some individuals are permitted to use non-standard email formats. IDCO allows this update but restricts the email to approved email extensions. For questions about your organization’s email formats, contact your Service Helpdesk.

- If the “Current email address” and “Email address provided by organization” are different, and you would like to keep the “Email address provided by organization”:
  - Click “Next” without checking either box to proceed with certificate update.
10. Confirm the changes to proceed with certificate update.
   • Before replacing the email certificates on your CAC, IDCO will confirm the changes and require you to acknowledge.
   • Click “Yes” to proceed with certificate updates.

11. Follow on-screen prompts to complete certificate update.
   • You may be requested to acknowledge running the IDCO applet again.
   • Various progress monitors will be displayed as the update continues.
12. IDCO will confirm that your certificates have been updated.

13. After certificates have successfully updated, follow all Service-specific requirements that are typically required after getting a new CAC.
   - Contact your Service IT helpdesk for assistance. Your Service Helpdesk, which can be found using [https://public.cyber.mil/pki-pke/help](https://public.cyber.mil/pki-pke/help), under the section “Combatant Command/Service/Agency Helpdesks.”
   - U.S. Coast Guard Helpdesk: 1-855-CG-Fixit (1-855-243-4948) (option 1, 1, 3) or [https://cgfixit.osc.uscg.mil](https://cgfixit.osc.uscg.mil)
   - NOAA Helpdesk: [NSDesk@noaa.gov](mailto:NSDesk@noaa.gov) or 1-855-673-3751 (Hours of Operation 7:00am - 7:00pm ET M-F (excluding Holidays))
   - USPHS Helpdesk: [cchelpdesk@hhs.gov](mailto:cchelpdesk@hhs.gov)
Who do I contact if I have problems?

- If ID Card Office Online (IDCO) indicates your affiliation end date does not extend beyond your CAC or VoLAC expiration date, you should contact:
  - Your HR representative, if you are a military member or civilian.
  - Your DoD sponsor (i.e., COR or TASS Trusted Agent), if you are a contractor or other population type who has been sponsored through TASS.

- If you plan to change your email address at the same time as updating your certificates and have a question about your organization’s requirements for email addresses, you should contact:
  - Your Service Helpdesk, which can be found using https://public.cyber.mil/pki-pke/help, under the section “Combatant Command/Service/Agency Helpdesks.”
  - U.S. Coast Guard Helpdesk: 1-855-CG-Fixit (1-855-243-4948) (option 1, 1, 3) or https://cgfixit.osc.uscg.mil
  - NOAA Helpdesk: NSDesk@noaa.gov or 1-855-673-3751 (Hours of Operation 7:00am - 7:00pm ET M-F (excluding Holidays))
  - USPHS Helpdesk: cchelpdesk@hhs.gov

- If ID Card Office Online (IDCO) gives you an error message when trying to rekey your certificates, you should contact:
  - Your Service Helpdesk, which can be found using https://public.cyber.mil/pki-pke/help, under the section “Combatant Command/Service/Agency Helpdesks.”
  - U.S. Coast Guard Helpdesk: 1-855-CG-Fixit (1-855-243-4948) (option 1, 1, 3) or https://cgfixit.osc.uscg.mil
  - NOAA Helpdesk: NSDesk@noaa.gov or 1-855-673-3751 (Hours of Operation 7:00am - 7:00pm ET M-F (excluding Holidays))
  - USPHS Helpdesk: cchelpdesk@hhs.gov