What is CAC Modernization, and why do I need to take action?

The Coast Guard will transition to a new authentication method for the Common Access Card (CAC), to align with the rest of the federal government. To prepare for this transition, all personnel must have the new “Authentication” certificate on their CAC, so if you were notified, you must follow this guidance. In mid-March 2020, CG-6 will release an ALCOAST to provide guidance and directions for logging into CG workstations, systems, and applications using the new authentication certificate. The CAC is the Coast Guard’s primary means for authentication to access unclassified networks, information systems, and applications.

Activating the PIV-Auth (“Authentication”) Certificate (Adding the Certificate to the CAC)

IMPORTANT NOTICE: 1.) Most users should NOT need to replace their CAC or visit a RAPIDS/DEERS (ID office) to complete this action. 2.) It is HIGHLY preferred to access the website below using Internet Explorer from a Coast Guard workstation (remote-VDI does NOT work). 3.) If you receive an error stating JAVA needs to be installed, submit a ticket to CGFIXIT requesting JAVA be repaired and/or attempt these steps from another workstation.

1) Highlight the link below, copy and paste into another window (Internet Explorer) to be directed to the DMDC site:
   https://www.dmdc.osd.mil/self_service/rapids/unauthenticated?execution=e1s1

2) Click **Sign In**

![Sign In Image](https://www.dmdc.osd.mil/self_service/rapids/unauthenticated?execution=e1s1)
3) The DEERS Self-Service Consent to Monitor window appears. Click OK.

4) Click the CAC tab.

5) The Common Access Card (CAC) window appears. Click Login.
6) The Select a Certificate window appears. Select the ‘DOD email’ certificate which is the current authentication certificate accepted. Select OK.

7) Enter your PIN
8) The RAPIDS Self Service window appears. Select Activate PIV Certificate.
9) The PIV Update window appears. In the PIV Information section, click **Proceed**.

**NOTE:** If presented with the “Java Update Needed” window, click **Later** (Continue and you will be reminded to update again later.)
The Reading data from CAC Window appears.
NOTE: If your CAC has the PIV-Auth ("Authentication") certificate activated by default, or you have previously manually activated the PIV-Auth certificate, then you will receive the following: If you don’t receive the following screen, proceed to 10.

10) The *ID Card Office Online Applet* window appears. Click **Run**.

11) The PIV Update window appears. Click **Update CAC**.
12) The PIV Update window displays “Your CAC has been successfully updated”. Click Log Out.
Great, your PIV-Auth (Authentication) Certificate is now activated (added to your CAC)!

**No further action is required at this time.** Further guidance for using the new Authentication certificate will be announced via ALCOAST in mid-March 2020.

Thank you for your cooperation!

---

**Experiencing Issues Updating your CAC?**

If you have any complications throughout this process, you should submit a CGFIXIT request via the CGFIXIT icon on your desktop and proceed to:

I NEED HELP WITH > MY CAC OR LOGIN > REQUEST NOW > I AM HAVING OTHER CAC ISSUES NOT IDENTIFIED ABOVE.

If unable to log in to a Coast Guard workstation contact the Centralized Service Desk Branch (CSDB) at 1-855-CG-Fixit (1-855-243-4948) (option 1, 1, 3).

---

Do you have questions about CAC Modernization? Please refer to the Frequently Asked Questions (FAQ’s) at [https://www.dcms.uscg.mil/CAC/](https://www.dcms.uscg.mil/CAC/)

---

09-Mar-20