

CAC PIN Reset Frequently Asked Questions

What is CPR?

The Common Access Card (CAC) Personal Identification Number (PIN) Reset system (CPR) was developed to provide a portable, flexible, single purpose system, capable of providing timely PIN reset capability to the field in a myriad of operating environments. The system was designed to securely solve the PIN reset problem, using Commercial off the Shelf (COTS) hardware over a client/server network.

Benefits of CPR –

- Provides timely and secure PIN resets
- Minimal time away from duty station
- Can be made available 24 hours a day

What is the CPR process?

CTA logs onto the CPR application, asks the customer to insert the CAC into the reader. Next, the customer places their finger on the fingerprint reader. If the fingerprint matches the fingerprint stored in the DEERS database, a picture of the card holder appears on the screen. The CTA verifies the individual on the screen is the individual presenting the locked CAC. The final step is to have the customer enter a 6-8 digit PIN twice. If the fingerprint doesn't match, the CTA sends the customer to a DEERS/RAPIDS station.

What are the acronyms TASM and CTA?

TASM – Trusted Agent Security Manager for the CPR workstation. Two individuals may be named as primary and alternate TASMs for each site. Their responsibilities are to manage the CPR workstation and include assigning CTAs who will run the CPR application. The TASM is responsible for maintaining the required CTA registration forms.

CTA - Certified Trusted Agent for the CPR workstation. The CTA is the day-to-day operator of the CPR workstation/application. There may be any number of CTAs as determined by local Leadership and TASMs, but should be within the scope of control of the primary & alternate TASMs. The CTAs are assigned to perform the actual PIN resets. Resetting PINs is the only function that a CTA will be able to perform.

Can we have several TASMs?

No. DMDC has restricted the assignment of one Primary and one Alternate TASM for each site.

Is there a lock out of the TASMs or CTAs?

If a TASM or CTA does not log on to the applications for 45 days, the account is locked by an automatic DMDC sweep.

What is required for TASM registration?

Three forms are required for each TASM.

1. Trusted Agent Security Manager (TASM)/ CPR Trusted Agent (CTA) Registration/Revocation Request
2. CPR User Qualifications Affidavit
3. TASM & CTA Acknowledgement of Responsibilities Form

The CTAs can only log onto the CPR application after the TASM has logged on.

The CTA's should be able to be configured as local "User" provided that they are also granted the additional privilege to read the single registry key "HKEY_LOCAL_MACHINE/Software/DMDC/CPR/Timers/13". The local network administrator should have the access required for this task.

Are there any firewall settings?

It is suggested that both Ports 80 and 443 be opened for all of the following IP addresses: 214.3.117.51, 214.3.117.53, 214.3.117.46, & 214.3.117.10.

Trouble connecting?

Try the following sites from Internet Explorer.

cac-cpr-1.dmdc.osd.mil
wasp-ae.dmdc.osd.mil

214.3.117.46
214.3.117.53

If you are able to access these sites using Internet Explorer, but not using the CPR console (Tools, the Test Communications options) contact the CPR helpdesk for replacement hosts file.

My CTA's are having trouble connecting. They're getting a "Java.Lang.nullpointer" error. Is there any solution to this problem?

The DMDC Tier 2 resolution is to refresh each CTA account by having the TASM log into Security Online and:

- 1) Remove the "01" access code and click submit to update the record.
- 2) Logout and then login again
- 3) Update the user account and select the "01" access code again and click submit.
- 4) Logout

I'm getting a "Java Lang error" when trying to connect to DMDC. Is there a solution for this problem?

The firewall is probably blocking the connection to DMDC. Recommend try using an internet connection not connected to their network (Dialup) to see if you can successfully connect.