CAC Modernization Tips

Please see below for helpful tips that may guide you towards a successful workday on the day your account is converted to enable the **'Authentication'** certificate:

1. If not already completed, download the PIV-Auth (**'Authentication'**) 16-digit certificate to your CAC. This task was due 31 May and is the method for obtaining the certificate. This can be completed by following the guide below: https://www.dcms.uscg.mil/Portals/10/CG-6/CAC/CAC-Modernization-User-Steps_Graphics_27APR.pdf?ver=2020-04-27-134702-687

2. To verify you have the **'Authentication'** 16-digit certificate on your CAC perform the following:

1) Click the ^ arrow to open the System Tray (located to the left of the time/date on your desktop),
2) Double click the "ActivClient Agent" icon (looks like a very small CAC reader),
3) Double click the "My Certificates" icon,
4) Multiple certificates are listed here. The **'Authentication'** certificate is the new certificate everyone must have.

3. For CG-VPN users only; when logging into your laptop, it is **HIGHLY PREFERRED** you sign into VPN **FIRST** (this is called "SBL" (Sign-in Before Log-in)); then log into Windows. Signing into VPN first ensures updates/fixes are pushed to your laptop! Follow the steps below:

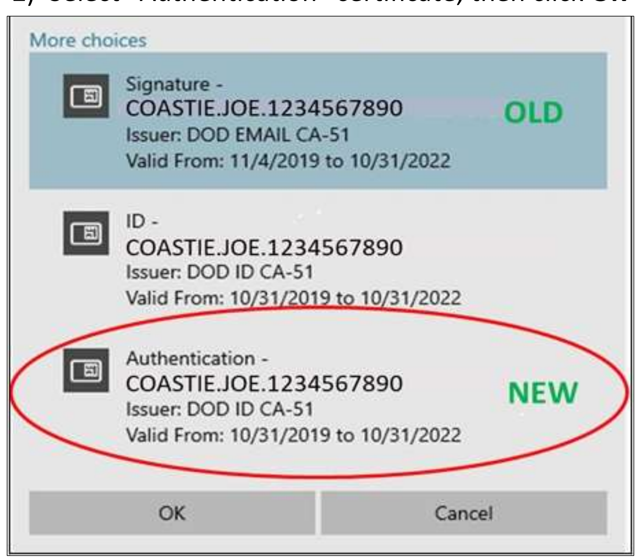
1) Click the  icon located on your Windows log-in screen,
2) Sign (connect) into your preferred VPN server (ensure you select the VPN servers ending in **–PIV**)
3) Log into Windows to access your desktop profile.
   NOTE: When signing into VPN before logging into Windows to access your desktop, you should always receive the Splash Screen (the colorful screen you receive with notifications that requires you to click "I Understand" to proceed. These notifications provide USCG wide alerts you should know!

CG-VPN Users Only: Once your account is converted to enable the "Authentication" certificate, you will begin selected the VPN servers ending in "–PIV".

4. For all USCG CAC-enabled websites during your session, always use your **'Authentication'** 16-digit certificate.

1) Click "More Choices"

2) Select "Authentication" certificate, then click **OK**



5. Please see below for helpful info for different user types:

- **CGOne Enterprise Users (most users):** From your CG workstation connected to CGOne on Ethernet, select the 16-digit certificate. This is different than the 10-digit certificate that you have been using. If you do not see your 16-digit certificate, keep clicking certificate options until you find it. If you do not see it, you missed Step 1 and will need to call 855-CGFIXIT to obtain your certificate.
- **VDI Users:** Follow the same procedure as CGOne enterprise users.
- **CG-VPN Users:** Perform *Start Before Log-on* (SBL). This ensures that if your laptop has an XML file waiting to install, it can install successfully. You should see that your site selections include -PIV in the name (i.e. cgvpnosc.uscg.mil, cgvpnosc.uscg.mil-PIV, etc.). If you do not, call 855-CGFIXIT and prepare to share contents of your C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile directory. All of the VPN pools are available for selection; select your site with a **-PIV** ending. If this is unsuccessful, try another site without the -PIV ending. Keep trying different sites until you get to the log-on screen. Select the 16-digit certificate. This is different than the 10-digit certificate that you have been using. If you do not see your 16-digit certificate, keep clicking certificate options until you find it.
- **Mobility Users (BlackBerry UEM):** Ensure you have downloaded the PIV-Cert (**'Authentication'** 16-digit) prior to Purebred enrollment. Current Purebred users can verify this by selecting, "Settings", "General", "Profiles & Device Management", "Purebred Configuration", "More Details". If your CAC Modernization and Purebred migrations were successful, you will see 4 certificates.

Encountering difficulties? Please try the troubleshooting tips below:

I logged in and all my files are gone, Skype will not connect, and Outlook will not connect.	You selected the 10-digit certificate. Log out, then log in with the 16-digit certificate. If issues persist, contact CSD, 855-CGFIXIT.
I can't connect to any of the VPN choices.	Contact CSD, 855-CGFIXIT.
I connect using SBL (VPN only), use the right certificate, then my Outlook won't open.	Has your mailbox moved to Office 365? Contact CSD, 855-CGFIXIT. Otherwise, try to open Outlook with a brand new profile.
I don't have **-PIV** selections in the VPN drop down.	You may need to visit your Coast Guard facility and plug your workstation in to the Coast Guard enterprise network. Contact CSD, 855-CGFIXIT.
I cannot use my PureBred mobile device to access my usual CG websites and applications.	Contact CSD, 855-CGFIXIT.
I'm nightshift and my email/CGPortal/Files stopped allowing access.	Logoff and log back in. User was transitioned to PIV during implementation. CGPortal and other applications will take time to replicate, however local files and email should remediate within an hour.
I can login, but cannot print to a CAC enabled printer.	Notify local base support to validate local printer is setup for PIV. (Unknown whether printing profile needs to be updated as well.)
I received a new CAC, but I cannot see any certificate but the PIV.	If present, user will need to go to a Coast Guard facility to have ActivClient 7.2 installed. Contact CSD, 855-CGFIXIT.
I can log in and most of my applications work, but there is one or more that do not.	Contact CSD, 855-CGFIXIT.
I logged in with my PIV on the date I was switched, but all my stuff is gone.	Contact CSD, 855-CGFIXIT.

Reference:

USCG CAC Modernization Page (FAQ's/ALCOAST/User Instructions):
https://www.dcms.uscg.mil/CAC/