USER INSTRUCTIONS FOR PIV AUTHENTICATION CERTIFICATE CONVERSION

***** Ensure you have fully read and understand these instructions before you begin. Please print or have the instructions available to assist you. *****

PROCESS:
You will be notified by your IMO of your migration date. The below instructions **MUST** be followed during your **FIRST** Windows login on your migration date.

Make sure to DISCONNECT from VPN and SHUTDOWN the computer at the end of the day PRIOR to your migration date.

Pay *careful attention* to the instructions below based on your telework status during your migration date. Failure to follow these instructions may require remote users to bring their computer on-post to connect to the network.

AFTER migration you will always logon to the network using your 16-digit authentication certificate. You will also always logon to VPN using the profile "PIV.apgmd.ra.army.mil" and your authentication certificate.

***** DO NOT PERFORM THESE STEPS PRIOR TO YOUR MIGRATION DATE *****

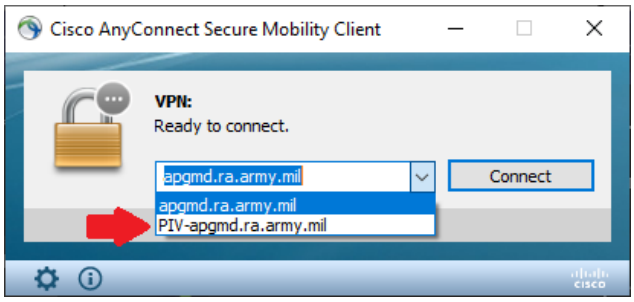
INSTRUCTIONS (Click the link based on telework status):

Telework (VPN) User – Method 1 ***PREFERRED METHOD – USE THIS FIRST***
Telework (VPN) User – Method 2
On-Site User
Notes/Troubleshooting

Telework (VPN) User – Method 1 *PREFERRED METHOD – USE THIS FIRST*

1. Turn on the computer.
2. At the login screen press Ctrl+Alt+Delete to login to windows.
3. Select Cisco AnyConnect VPN Pre-Connect Icon in the lower right corner.

4. You will be presented the Cisco AnyConnect VPN Client with a drop down menu. Verify that you have two profiles. Select "PIV-apgmd.ra.army.mil" and click Connect.



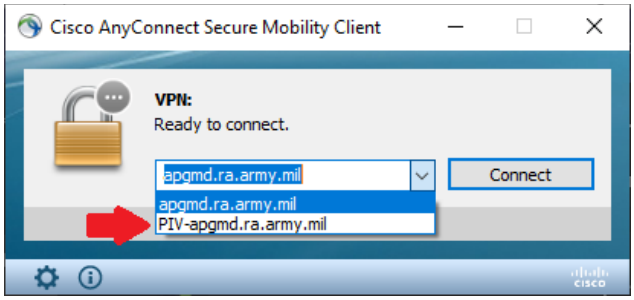
5. Click Ok at the next popup.
6. Click Accept at the next popup.
7. Click on "Other User" in the bottom left of the screen.

8. Click on "Sign in Options" in the middle of the screen.
9. In the middle of the screen, select the smart card icon that corresponds to your sign on that shows a 16 digit EDIPI number.

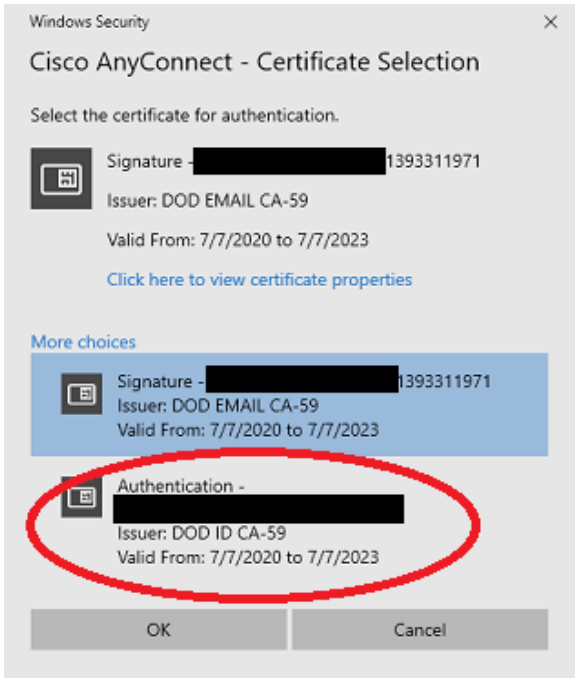
10. Enter your CAC pin.
11. Press Enter.

Telework (VPN) User – Method 2

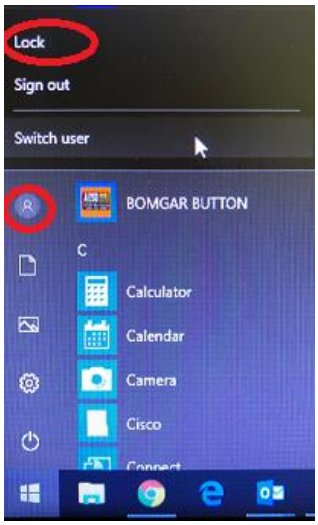
1. Turn on the computer.
2. Log into Windows using normal process/certificate (10 digit EDIPI).
3. Connect to Cisco AnyConnect VPN. Verify that you have two profiles. Select "PIV-apgmd.ra.army.mil" and click Connect.



4. When prompted use your <u>authentication</u> certificate.



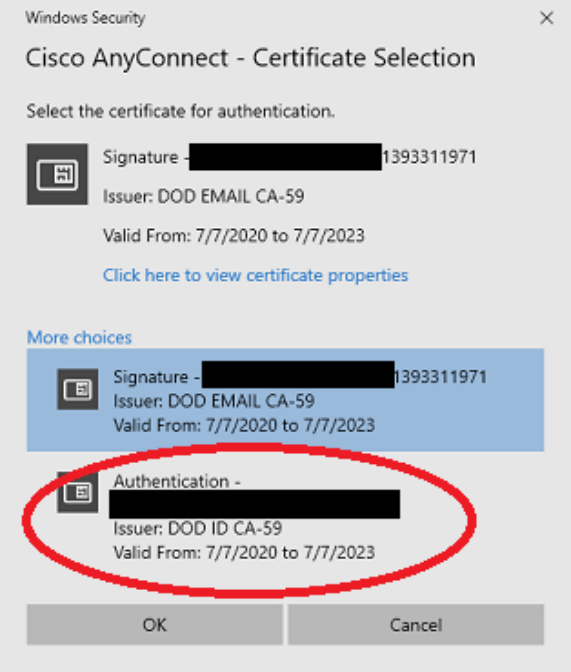
5. Once logged into VPN, click the Windows icon in the lower left of the screen on the taskbar, click the user icon, and click on "lock" to lock the computer. Alternatively, you can press Ctrl+Alt+Delete then click on "Lock"



6. Press Ctrl+Alt+Delete.
7. Click on “Other User” in the bottom left of the screen.

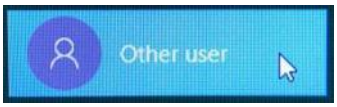
8. Click on “Sign in Options” in the middle of the screen.
9. In the middle of the screen, select the smart card icon that corresponds to your sign on that shows a 16 digit EDIPI number.

10. Enter your CAC pin.
11. Disconnect from Cisco AnyConnect VPN.
12. Re-connect to Cisco AnyConnect VPN using the same profile “PIV-apgmd.ra.army.mil” and click Connect. Again, use your authentication certificate when connecting.


Windows Security
Cisco AnyConnect - Certificate Selection
Select the certificate for authentication.
Signature - [redacted]1393311971
Issuer: DOD EMAIL CA-59
Valid From: 7/7/2020 to 7/7/2023
Click here to view certificate properties
More choices
Signature - [redacted]1393311971
Issuer: DOD EMAIL CA-59
Valid From: 7/7/2020 to 7/7/2023
Authentication - [redacted]
Issuer: DOD ID CA-59
Valid From: 7/7/2020 to 7/7/2023
OK
Cancel

On-Site User

1. Turn on/restart your machine.
2. Press Ctrl+Alt+Delete to login to windows.
3. Click on “Other User” in the bottom left of the screen.



3. Click on “Sign in Options” in the middle of the screen.
4. In the middle of the screen, select the smart card icon that corresponds to your sign on that shows a 16 digit EDIPI number.

5. Enter your CAC pin.
6. Test your Cisco AnyConnect VPN connection now using the **authentication certificate** instead of email certificate.

Notes/Troubleshooting

- **After you log in with your PIV certificate once, you will continue to use the PIV certificate to login to Windows from now on.**
- Windows may not default to your PIV certificate right away. Please double check you signed in using the method above and make sure you are using the PIV certificate with the 16 digit EDIPI.
- If you login to a "visitor account" this means you signed in with the wrong certificate. Visitor accounts have a black background, have limited access/connectivity, and will not look like your normal profile. Logout and follow the directions above again based on your telework status, making sure to login using the PIV certificate with the 16 digit EDIPI.
    - If you get a visitor account using both your regular certificate (10 digit EDIPI) and the PIV certificate (16 digit EDIPI) please contact AESD (Army Enterprise Service Desk) at 1-866-335-ARMY.
- If you get the message "Domain specified is not available" please check the following:
    - Check to make sure you are using the PIV certificate with the 16 digit EDIPI.
    - Complete the instructions for "Telework (VPN) Users – Method 1" (preferred method).
    - If you were unable to do the "Telework (VPN) Users – Method 1" instructions and receive this message while performing "Telework (VPN) User – Method 2" instructions, double check your internet connection and make sure you are still connected to VPN.
    - If you still receive the message, you will need to bring your computer on site, plug into the network, and complete the instructions for on-site user.
- You may need to sign back into Microsoft Teams after logging in into the Windows with your PIV certificate. Log back into Teams with your @cvr.mil login.
- Please contact AESD (Army Enterprise Service Desk) at 1-866-335-ARMY if you have followed all instructions and troubleshooting steps above and are still unable to login.