Remote Access instructions using your Government furnished laptop in conjunction with your Government furnished iPhone

Steps:

1. Turn on Personal Hotspot on your iPhone.
2. Login and connect laptop to your iPhone hotspot.
3. Have PIV PIN available to type into Cisco AnyConnect.
4. Follow the below instructions

Instructions:

For logging into the USA network from a Government Furnished Equipment (GFE) laptop using the Personal Hotspot on your iPhone. This is for when you are not using your home wireless connection.

Prerequisite 1: To successfully log in, you are required to have PIV card and PIN for user authentication and authorization.

Prerequisite 2: If the AnyConnect client software has been installed correctly on the laptop, a **Cisco AnyConnect Secure Mobility Client** folder should be available in the Start/All Apps section.

NOTE: Once you connect the laptop to a wireless signal, Cisco AnyConnect will automatically launch and prompt for your PIV Pin as seen in step 3.

A. Cisco AnyConnect PIV Login procedures

1. Select the **Connect** button on the *Cisco AnyConnect Secure Mobility Client*.

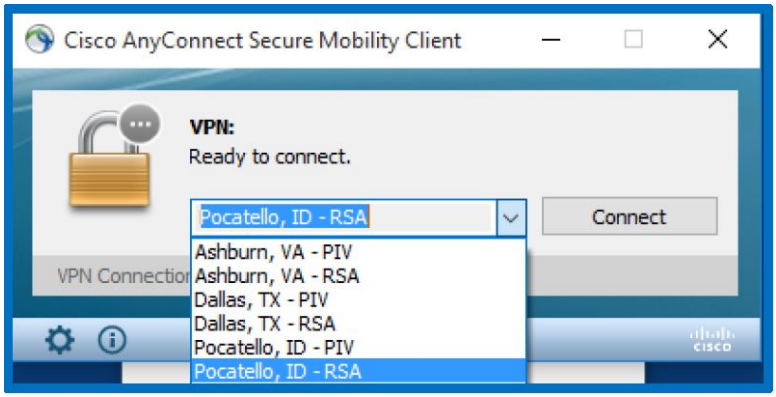


Figure 2.

2. The *AnyConnect Client* contacts the Primary PIV located in the Rockville Data Center. If the Primary connection fails, click on the down arrow and choose one of the other PIV sites.

3. The ASA sends a PIV card certificate request back to the *AnyConnect Client* on the laptop. If a valid PIV card is detected, the *ActivClient Login* window appears. When the window appears, enter a valid PIN and then select the **OK** button.

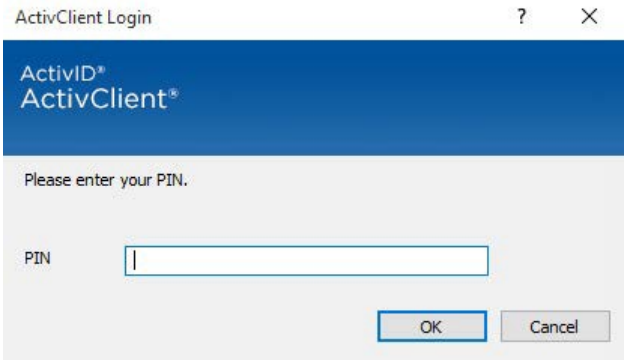


Figure 4.

4. If a valid PIN is not entered, the following message is displayed. Select the **Retry** button and enter a valid PIN for the PIV card.

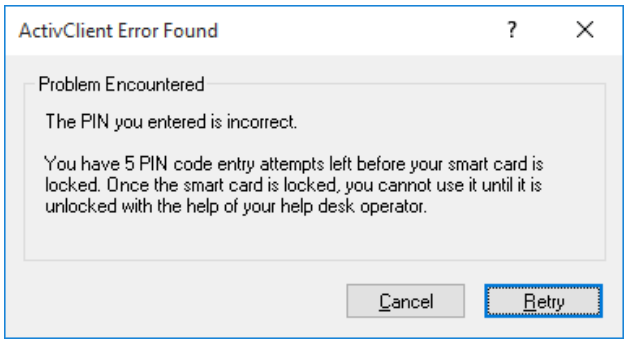


Figure 5.

5. When **Posture Assessment** appears, the PIV card login is being validated, which is the first part of the two- factor Authentication process.

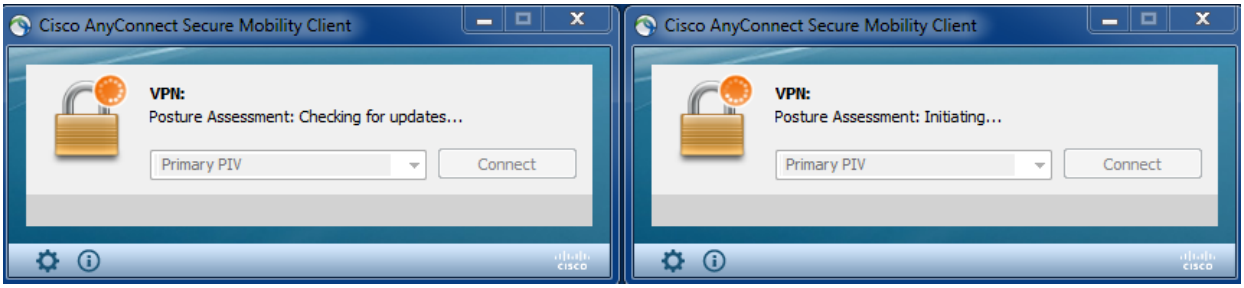


Figure 6a and 6b.

6. The **Hostscan** process downloads two files to scan the laptop for the certificate and present it back to the ASA. This is the second requirement of the two-factor Authentication process.

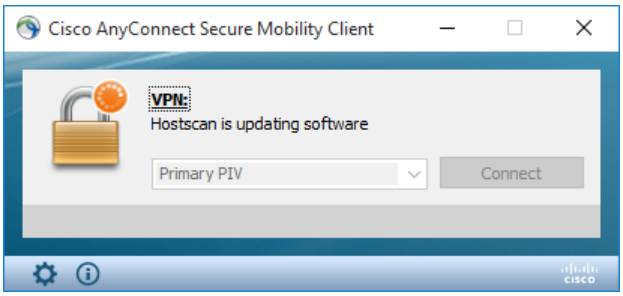


Figure 7.

7. Cisco AnyConnect presents an *Agreement* banner informing the user that s/he is accessing a US DOJ system. If the user agrees to the terms, s/he selects the **Agree** button and the process continues. If the **Disconnect** button is selected, the *AnyConnect* process is terminated.

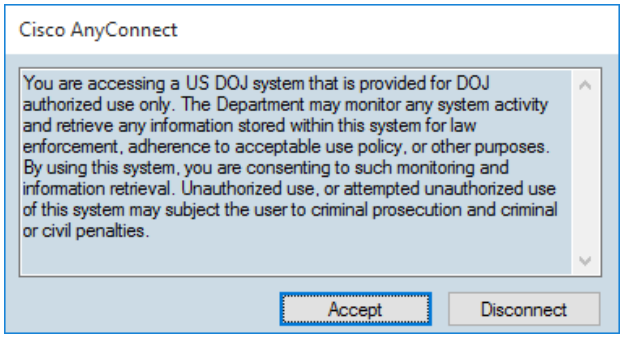


Figure 8.

8. If both certificates presented meet the validation approval process then the *AnyConnect* session will connect, and the following figure is displayed.

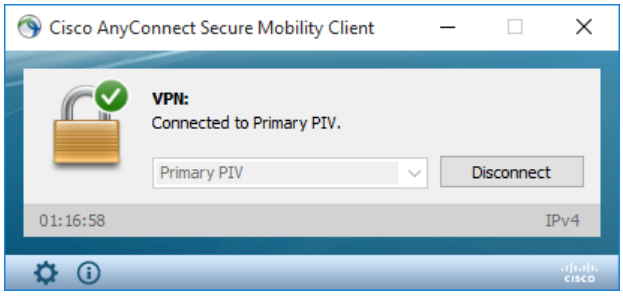
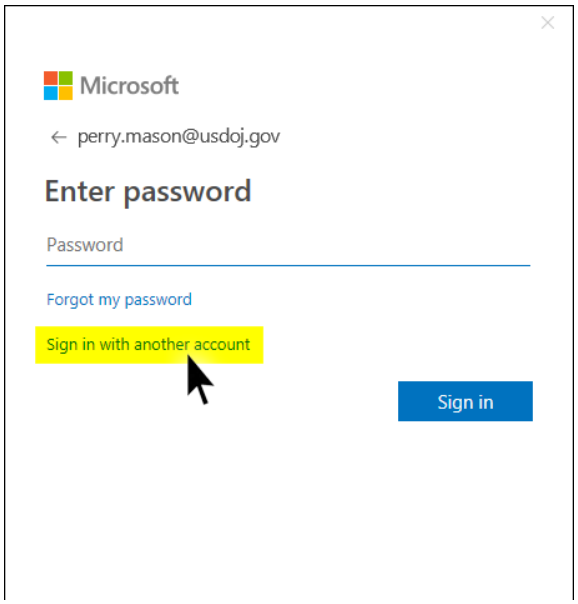


Figure 9.

9. When completed with this requirement you will be connected to the Network.

Note: If using a loaner laptop, the first time you launch Outlook, you will have to create your Office 365 profile. You will get the following prompt:



DO NOT ENTER YOUR PASSWORD. Click on the Sign in with another account link. At the next screen, remove your external email address and replace it with your internal email address as shown in the image below:

Click the Next button and your Outlook profile will load and populate all of your emails. This may take a while depending on the amount of emails that you have.

Outlook, Internet Explore and other network resource should work normally. However, to connect to your files on the network you will have to map to a network drive. To do this complete the following:

Navigate to your Windows Desktop, locate the Map My Drives – GR 

icon and double click it. Wait about 10 seconds and then launch Windows Explorer and the network drives should be mapped.

1. Disconnecting from Cisco AnyConnect Secure Mobility Client

To disconnect, select the Cisco AnyConnect Secure Mobility Client Icon from the bottom right hand corner of the taskbar. The icon will look like a globe with a locked padlock on top of it. You may have to click on the Up Arrow in the taskbar to revel all of the icons to locate the AnyConnect icon.

NOTE: Please always disconnect before shutting down the laptop to release the certificate and prevent problems when connecting to the network upon return to the office. If you leave the connection unattended for more than 4 hours, you will be automatically disconnected.