United States Coast Guard (USCG)

CG CYBER NOSC-AMT

VDI Remote Access for macOS Catalina/Mojave Installation Guide

September 9, 2020

Approved for Internet Release

Revision	Date	Comments
1.0	September 9, 2020	Initial document

Table of Contents

Introduction

This guide provides instructions on how to install and configure VDI Remote Access software on personal macOS computers. This guide is not for standard workstations that connect to CGOne. Standard workstations are automatically configured for VDI Remote Access.

OpenSSL is an open source cryptographic utility that verifies that the downloaded Department of Defense-specific root and intermediate Certificate Authority (CA) certificates are authentic and have not been tampered with.

The Keychain Access utility provides a graphical user interface for managing CA certificates in the operating system's certificate store. All public certificates installed with this application are considered unclassified.

VMware Horizon Client provides secure access to a virtual desktop connected to CGOne. The VMware Horizon Client software isolates the virtual desktop from the computer running the software.

A. Symbols

The following symbols may be used in this document:

Name	Description	Name	Description
	Caution: Exception and/or important direction/information		Note: Need to Know or Helpful Information
	Warning: Read and/or take action is required		Red rectangular and circular shapes are used to highlight an area of the screenshot

B. Prerequisites

For VDI Remote Access to be properly downloaded and installed, ensure you have the following:

1. CAC reader
2. Administrator rights to your mac
3. Internet connection (for Chapter 3)
4. Completely removed all previous CAC software (ActivClient, OpenSC, CACKey, etc), and DoD CA's from Keychain. Instructions can be found at militarycac.com/macuninstall.htm

C. Support

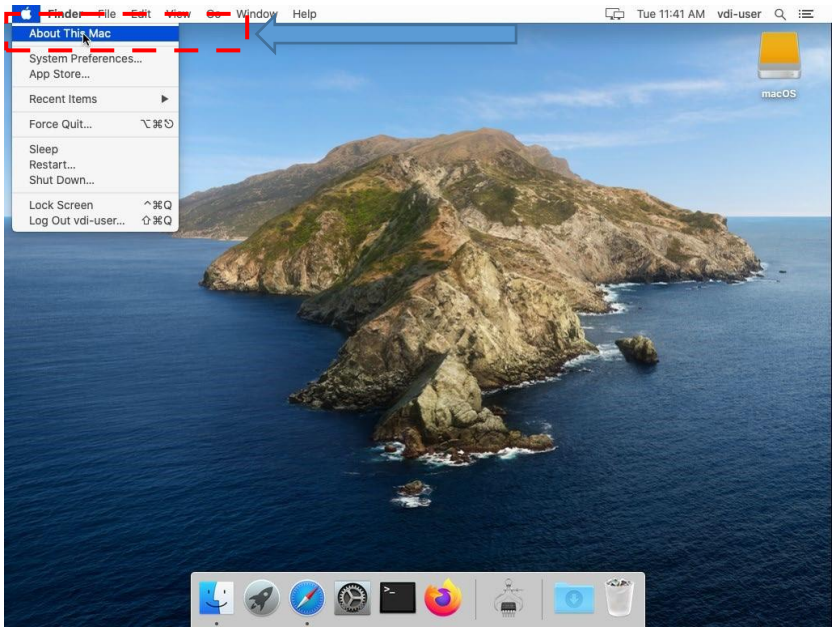
SBU CGOne Support: The Centralized Service Desk can not provide VDI installation support for personal computers. Additional information on installing VDI on personal computers can be found on the CG Portal at: https://cg.portal.uscg.mil/units/tiscom/Services/SitePages_EISI/Virtual_Desktop.aspx

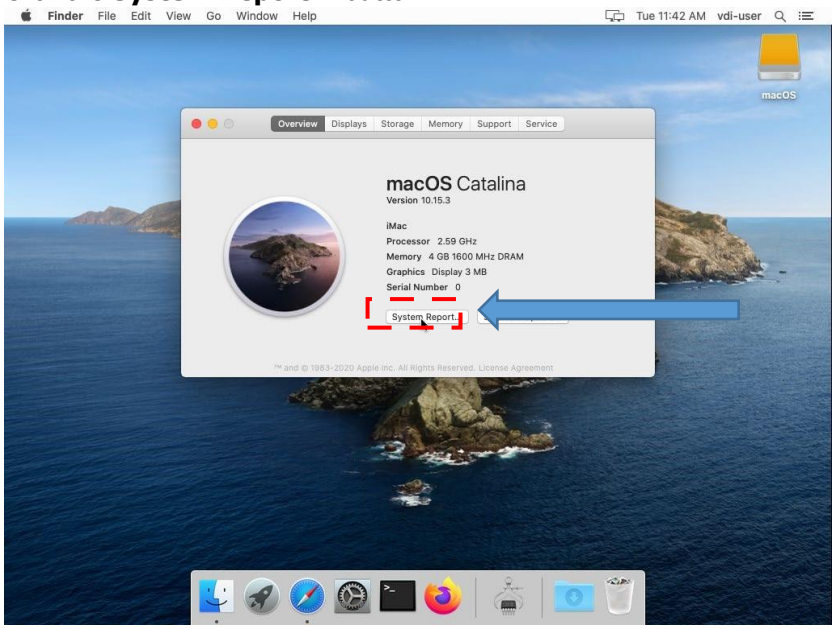
CAC Support: To obtain support for the CAC reader and drivers, users must contact their respective Base C4IT Support Department (BCD)/Electronic Software Distribution. Additionally, the local Supporting Personnel Office will resolve CAC issues (locked card, etc.).

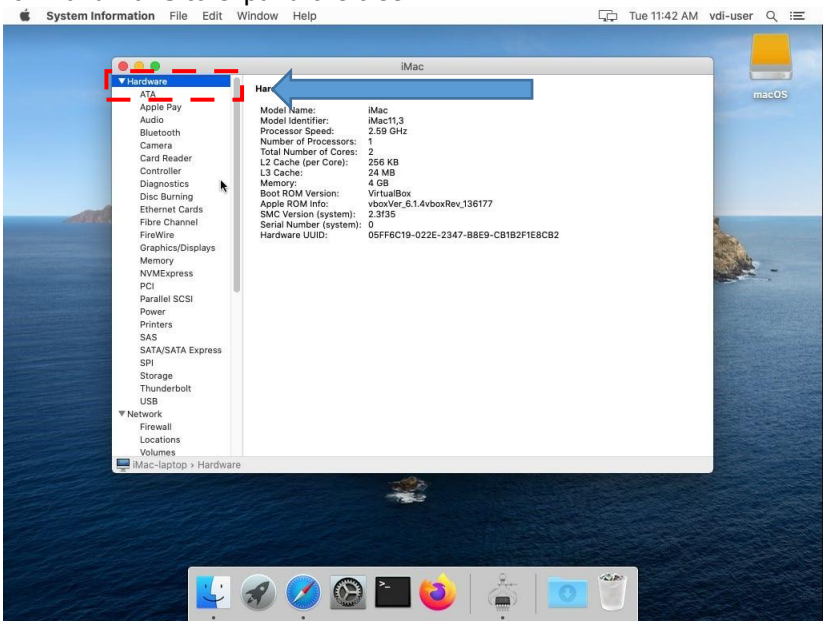
Chapter 1: Verify Smart Card Reader OS Compatibility

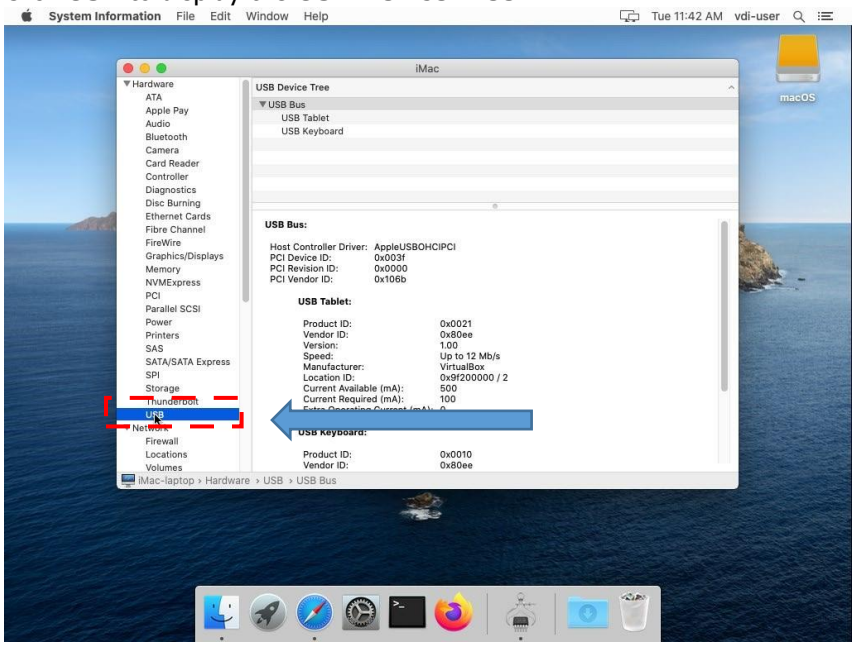
Certain card readers require updated firmware or drivers to function properly with macOS.

Use the following procedure to verify your system and smart card reader are compatible.

Step	Verify Smart Card Reader OS Compatibility
1.	Click the Apple Icon in the upper left corner of the desktop and click **About This Mac**. 

2.	Click the **System Report...** button. 

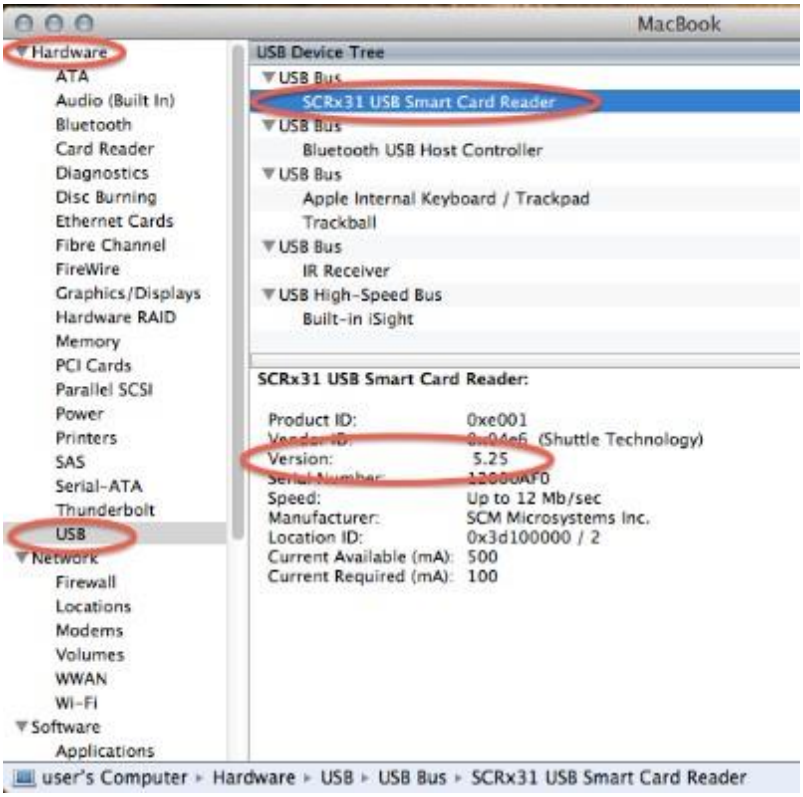
Step	Verify Smart Card Reader OS Compatibility
3.	Click **Hardware** to expand the tree. 

4.	Click **USB** to display the **USB Device Tree**. 

Step	Verify Smart Card Reader OS Compatibility

5.	*** If your reader looks like this, (**SCR-331)**, go to step 6. ***  *** If your reader looks like these (Iogear **GSR-202, 202v, 205 or 205)**, go to step 7. ***  *** If your reader looks like this (**SCR-3500A)**, go to step 8. ***  *** Otherwise, go to step 9. ***

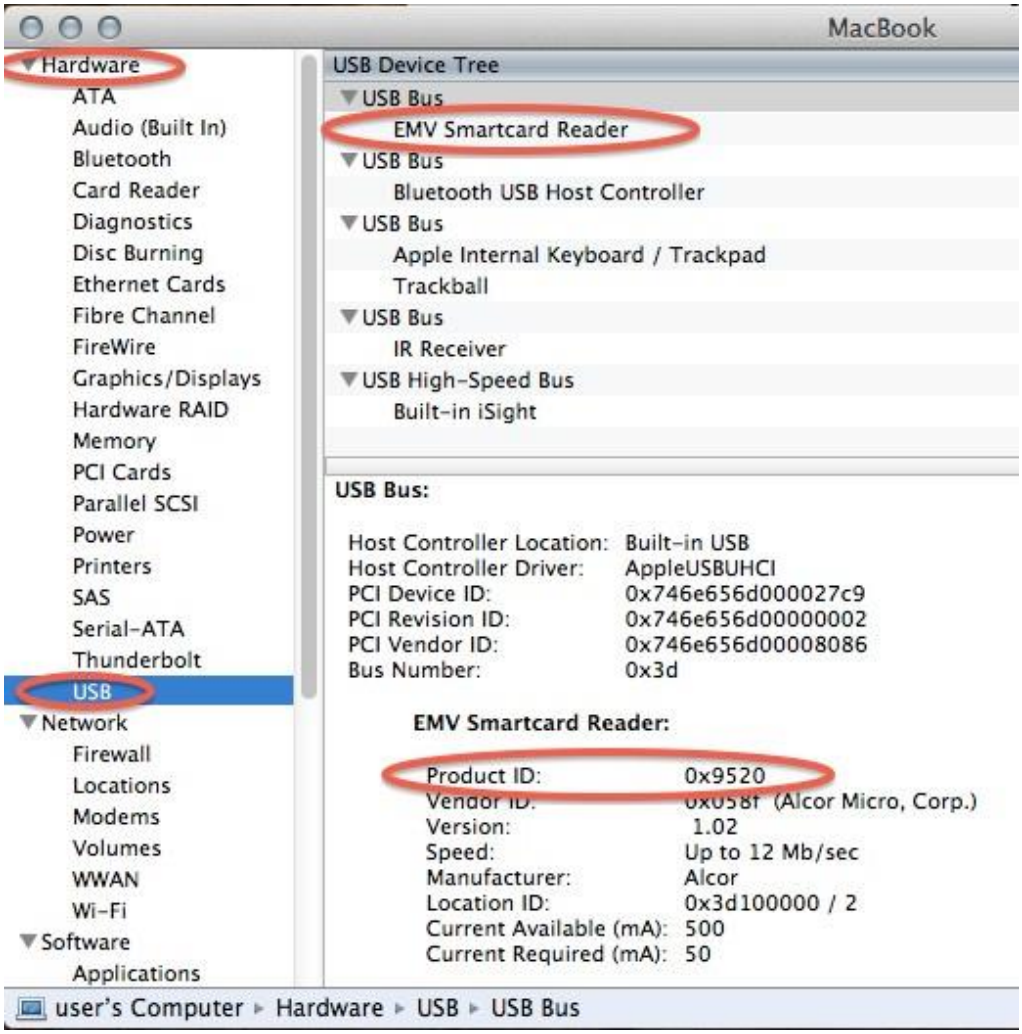
Step	Verify Smart Card Reader OS Compatibility

6.	If your reader does not look like this, go to step 9.  Click **SCRx31 USB Smart Card Reader** to view the details.  Note the value of the **Version** field. If the number is 5.18 or 5.25, proceed to step 9. If the number is below 5.18, then the firmware must be updated to 5.25. Please see militarycac.com/cacdrivers.htm#FIRMWARE_UPDATE.

Step	Verify Smart Card Reader OS Compatibility

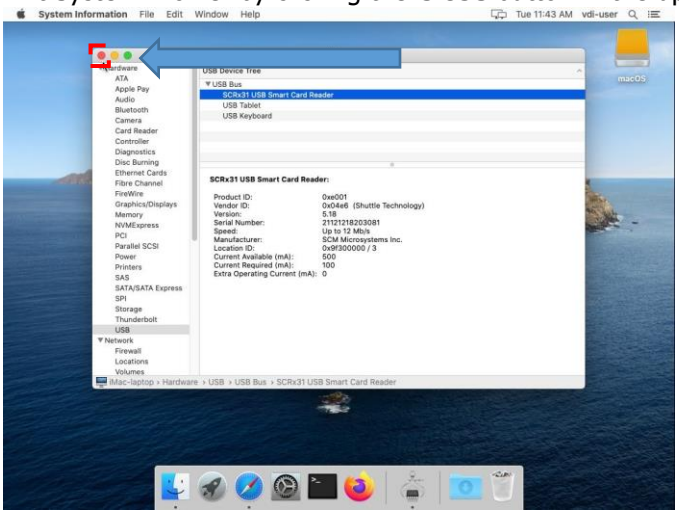
7. If your reader does not look like these, go to step 9.

Click **EMV Smartcard Reader** to view the details.



Note the value of the **Product ID** field. If the value is 0x9520, proceed to step 9. If the value is 0x9540, then the firmware must be downgraded. Please see militarycac.com/iogear.htm

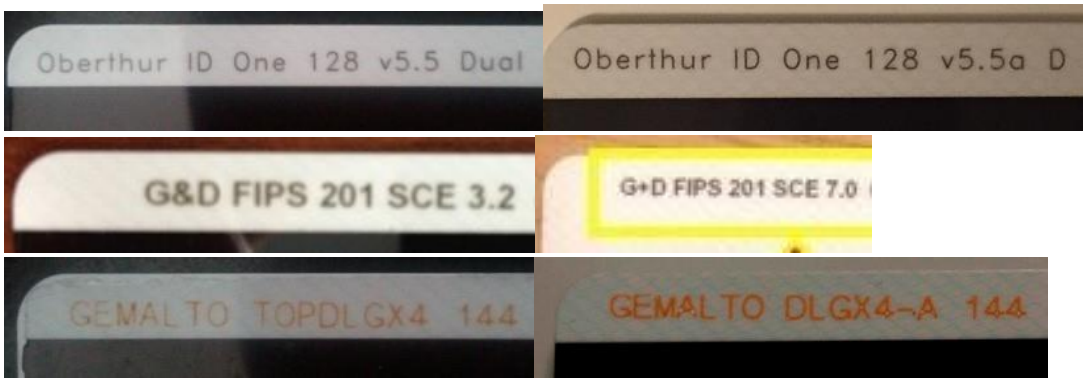
Step	Verify Smart Card Reader OS Compatibility

8.	If your reader does not look like this, go to step 9.  SCR-3500 Smart fold mini USB Smart Card Reader **Mac Friendly [10.4 - 10.15]** **Note: There is another SCR-3500 reader being sold with a Part number different from the original *905141* (sometimes shows as SCR3500A P/N:905430-1). If you are a Mac user, install this updated driver. Hold the *control* key [on your keyboard] when clicking the .pkg file [with your mouse], select [the word] *Open*** Go to the following link and scroll to SCR-3500 https://militarycac.com/usbreaders.htm follow steps in outlined in red. Restart might be required if so continue steps when restart is complete. If these steps do not work or you have a the SCR3500A P/N:9054301-1 reader, you need to update the driver. See Appendix B, and complete the procedures before continuing.
9.	Exit System Profiler by clicking the **Close** button in the upper left corner of the window. 

10.	Exit the About This Mac dialog by clicking the **Close** button in the upper left corner of the window. 
End	The procedure to Verify Smart Card Reader OS Compatibility is complete. Proceed to Chapter 2: Verify Smart Card Stock Version.

Chapter 2: Verify Smart Card Stock Version

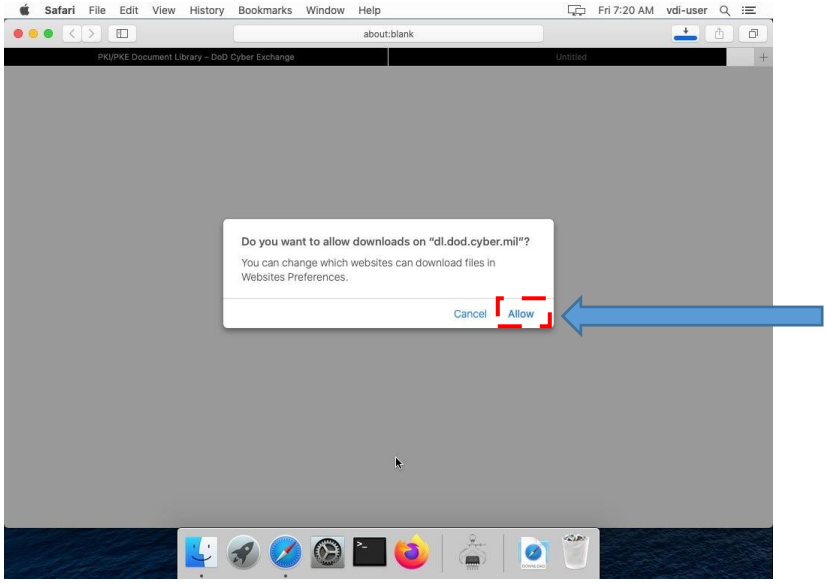
Only newer smart cards are supported for macOS. Use these procedures to verify that a supported smart card is being used

Step	Verify Smart Card Stock Version
1.	Turn over smart card to the back, and observe the card stock version in the upper left corner.
2.	If the version doesn't match one of these, then a new smart card must be obtained from an ID Card Office. 

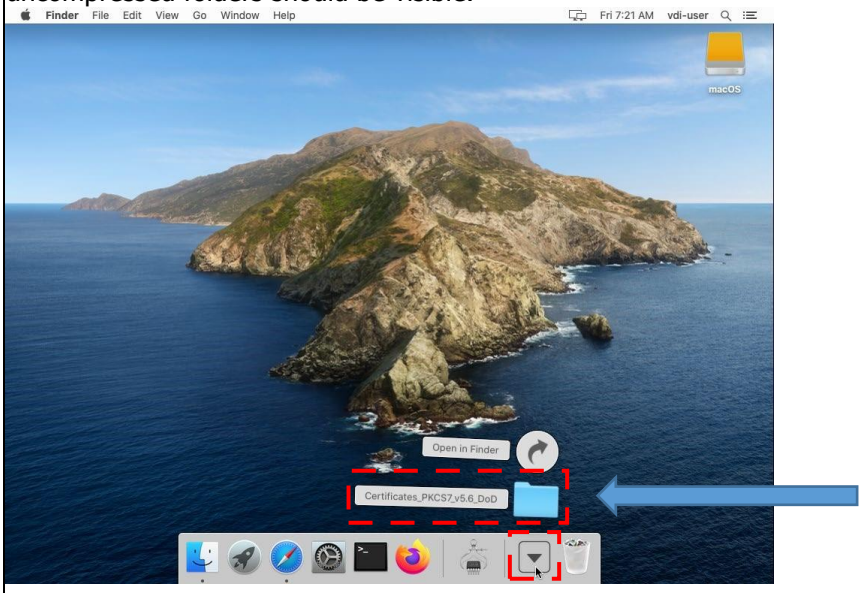
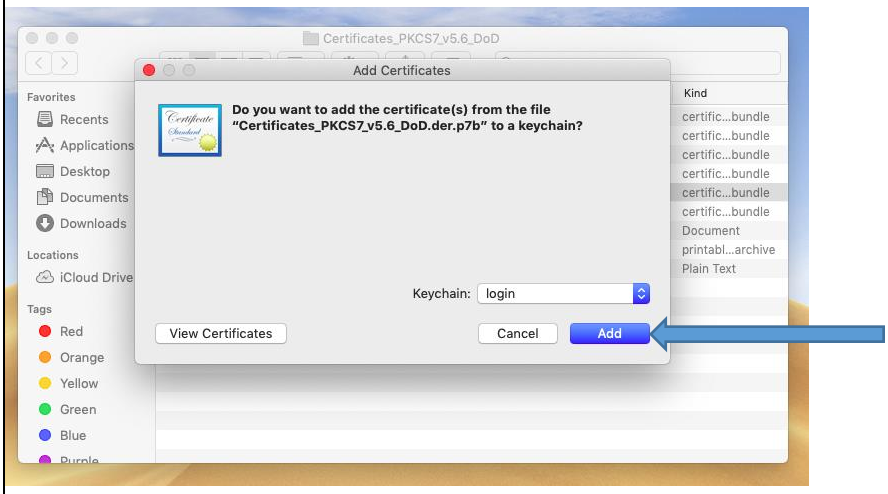
End	The procedure to Verify Smart Card Stock Version is complete. Proceed to Chapter 3: Download Required Software.

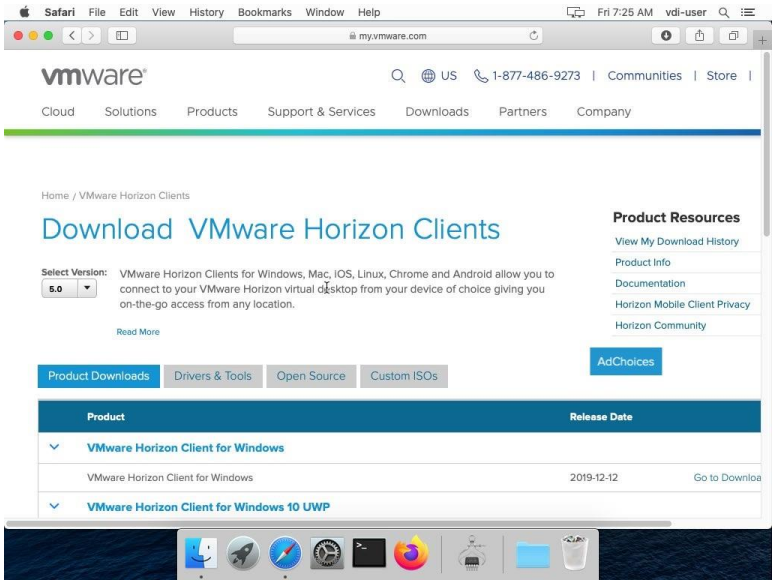
Chapter 3: Download Required Software

Use the following procedure to access the DoD Cyber Exchange and VMware from the computer you will be working remotely with to obtain the certificate and program files to download and install for VDI Remote Access.

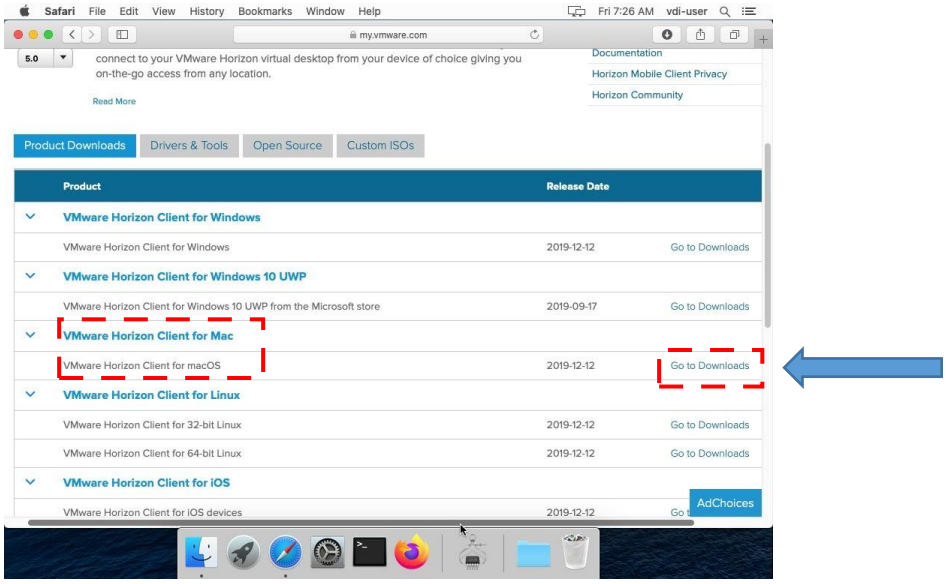
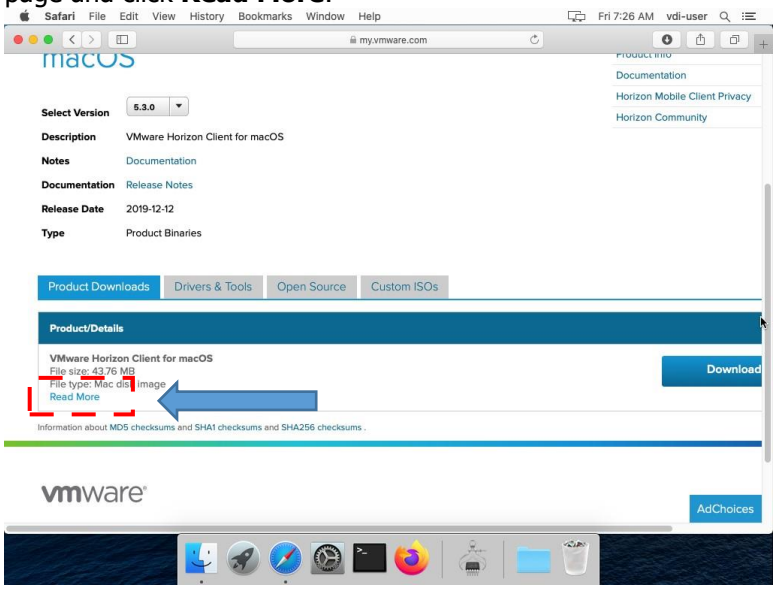
Step	Download Required Software
1.	On your home computer, use the Safari browser to open the following link: https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/zip/unclass-certificates_pkcs7_v56_dod.zip If the direct link is inaccessible go to https://public.cyber.mil/pki-pke/end-users/getting-started/cross-cert-chaining/
2.	The following screen likely appears (unless you've already granted download permissions). Click **Allow.** This will save DoD PKI PKCS#7 CA certificate bundle. 

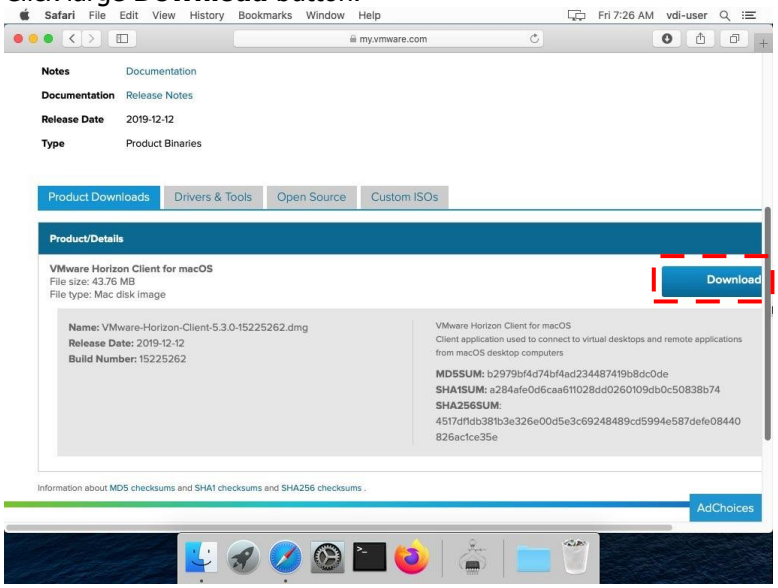
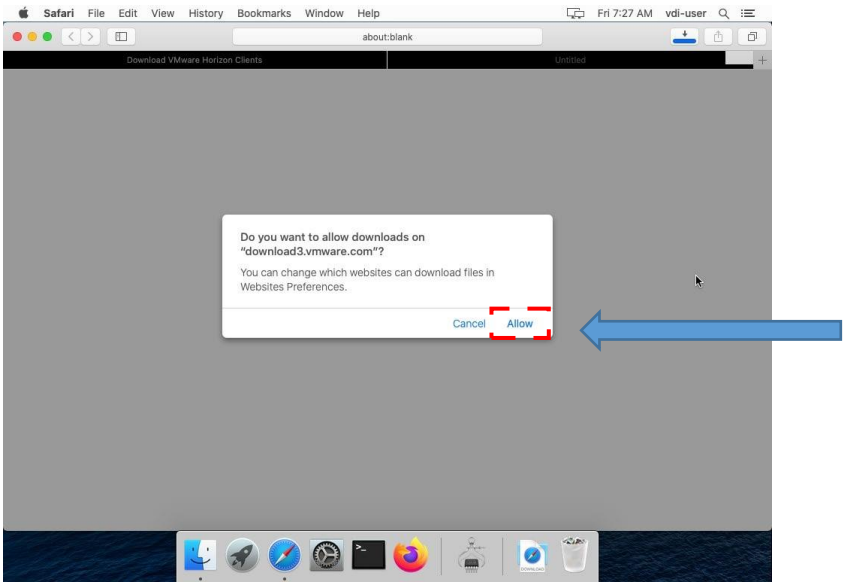
Step	Download Required Software

3.	Confirm the file has successfully downloaded and unzipped by clicking the Download icon on the Dock. The uncompressed folders should be visible. 
4.	Open file location and install the following files double click each certificate bundle and install to login, import all the .pem and .p7b files into the keychain. 
5.	On your home computer, use your preferred browser to open the following link: https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop_end_user_computing/vmware_horizon_clients/5_0

6.	You are now at the VMware **Download VMware Horizon Clients** page, where the VDI software files are located. 

Step	Download Required Software

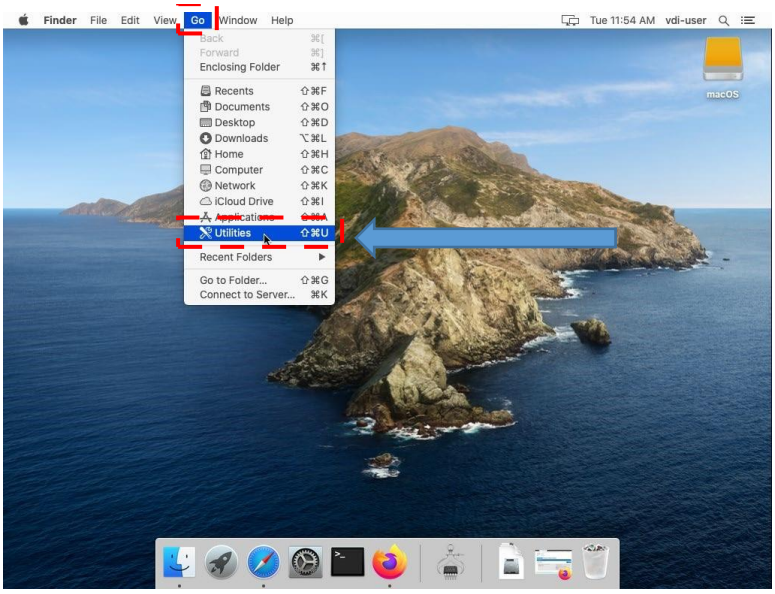
7.	Navigate down the page and expand the **VMware Horizon Client for Mac** section (if not already). Click **Go to Downloads**. 
8.	You are now at the download page for the selected VMWare Horizon Client. Navigate down the page and click **Read More**. 

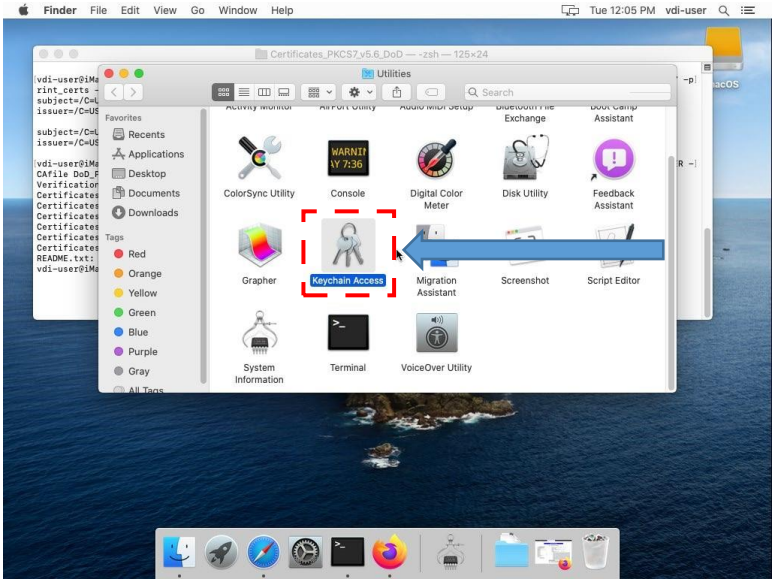
Step	Download Required Software
9.	Click large **Download** button. 
10.	The following screen likely appears (unless you have already granted download permissions). Click **Allow.** 

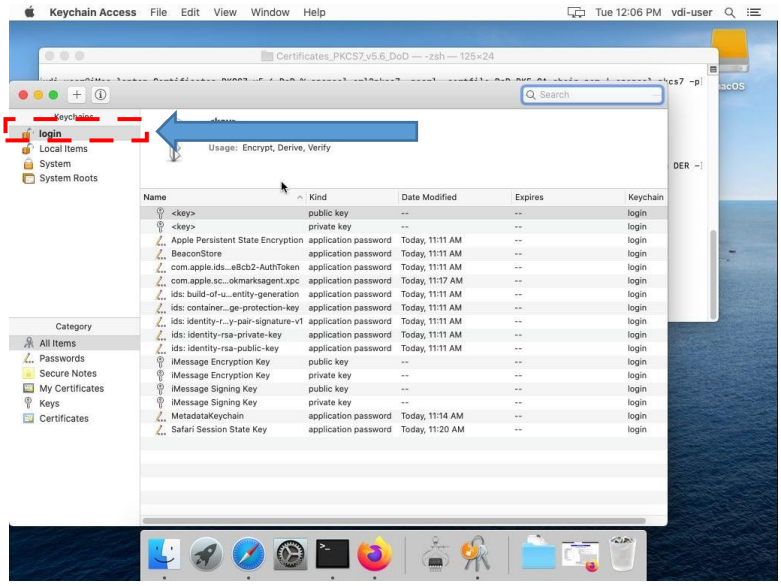
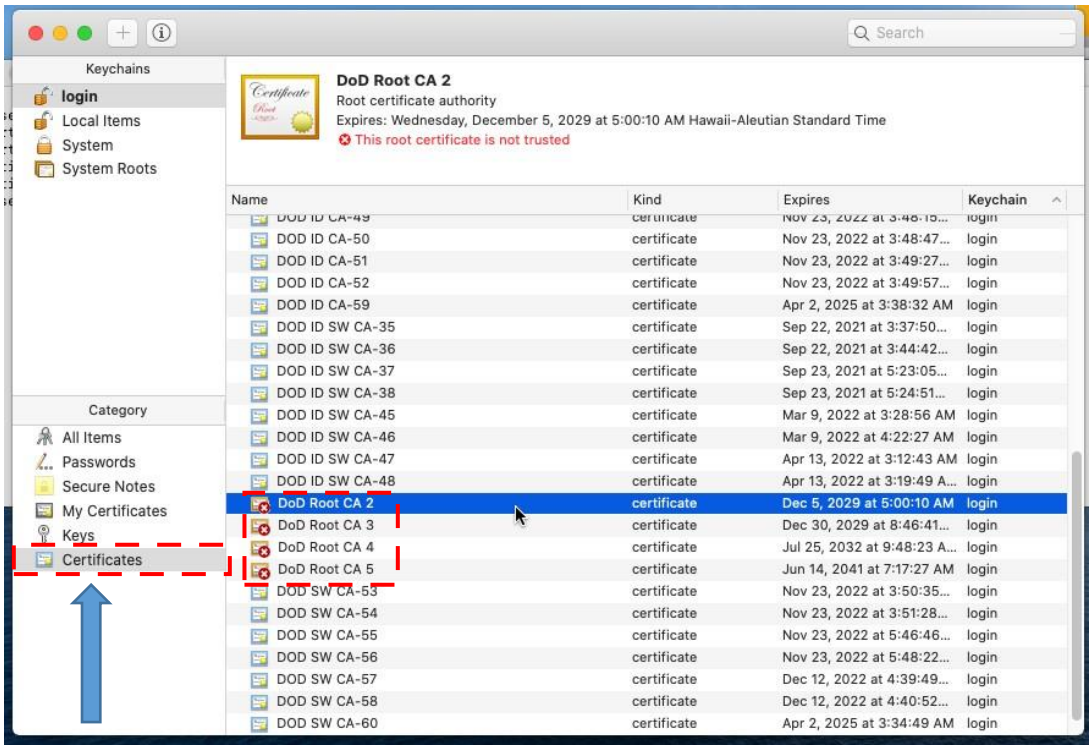
End	The procedure to Download Required Software is complete. Proceed to Chapter 4: Install DoD CA Certificates - OS.

Chapter 4: Trust DoD CA Certificates - OS

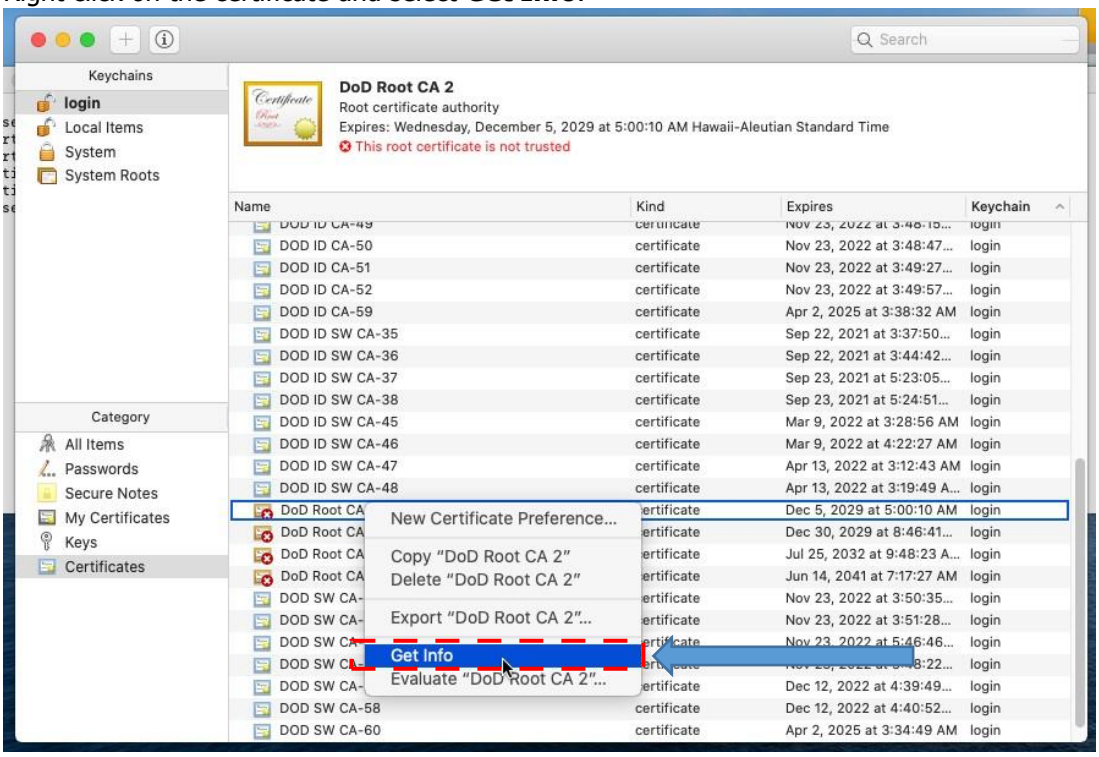
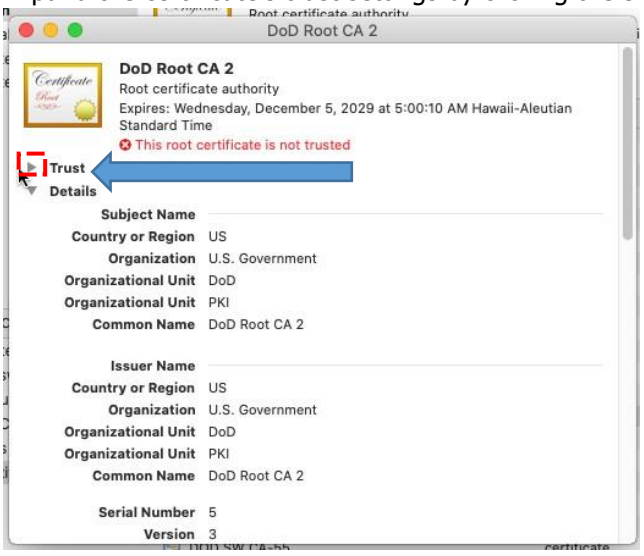
Use the following procedure to install the DoD CA Certificates into the operating system's trusted store.

Step	Trust DoD CA Certificates - OS
1.	 The DoD Root CAs need to be explicitly trusted. Click **Go,** then **Utilities.**

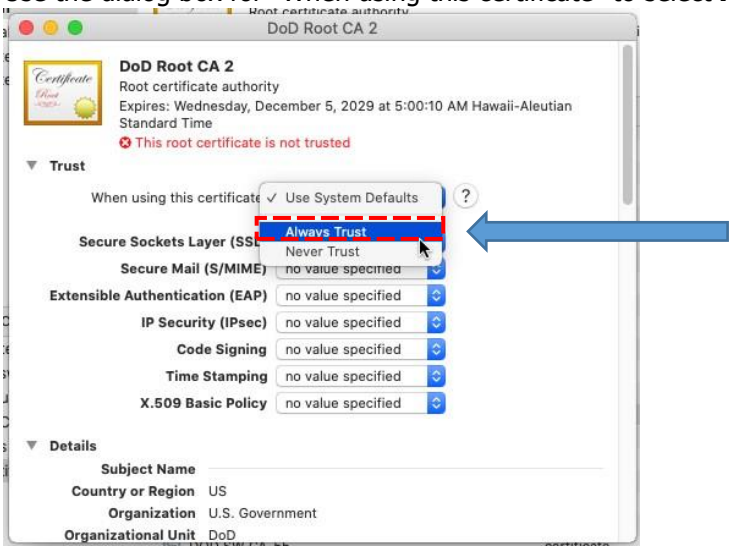
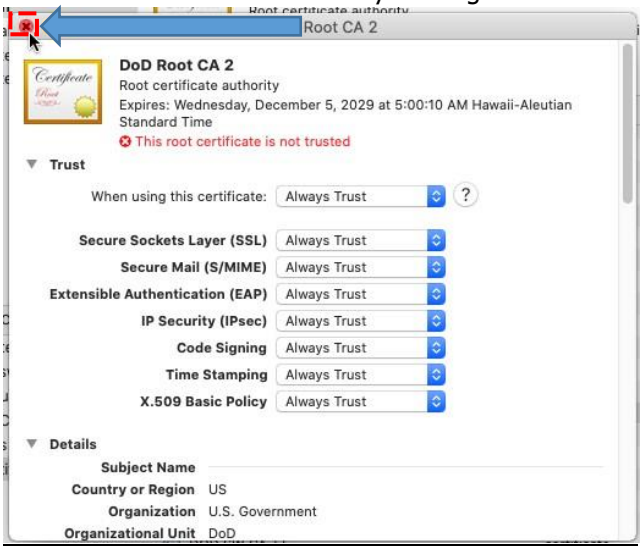
2.	Open the macOS trust application by double-clicking **Keychain Access**. 

Step	Trust DoD CA Certificates - OS
3.	The following screen will appear. Select the **login** keychain. 
4.	Select the **Certificates** category. Scroll down until the DoD Root CAs (2, 3, 4 & 5) are visible. 

| Step | Trust DoD CA Certificates - OS |

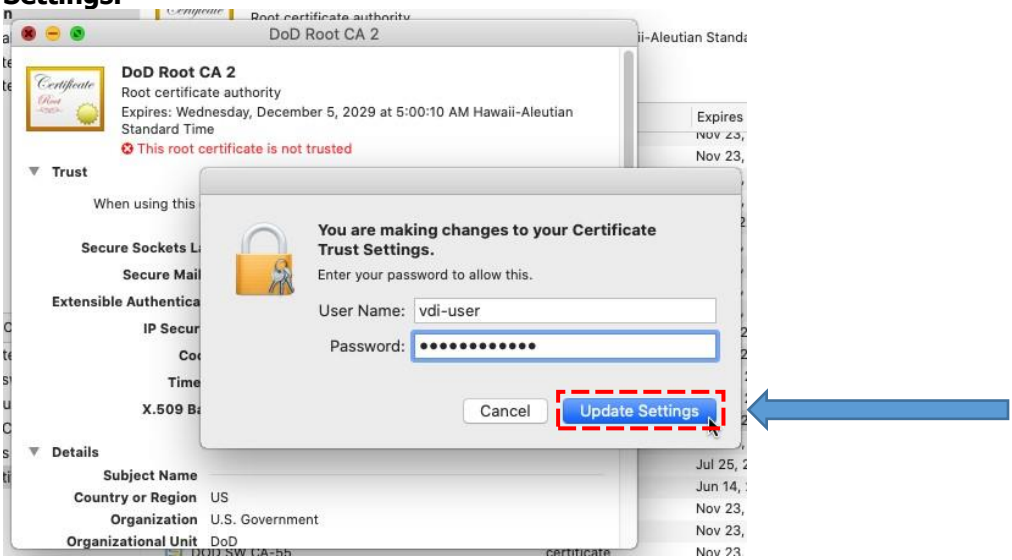
5.	Steps 25 – 28 must be repeated for each DoD Root CA that has a red X icon. Right click on the certificate and select **Get Info**. 
6.	Expand the certificate's trust settings by clicking the small triangle next to **Trust**. 

Step	Trust DoD CA Certificates - OS

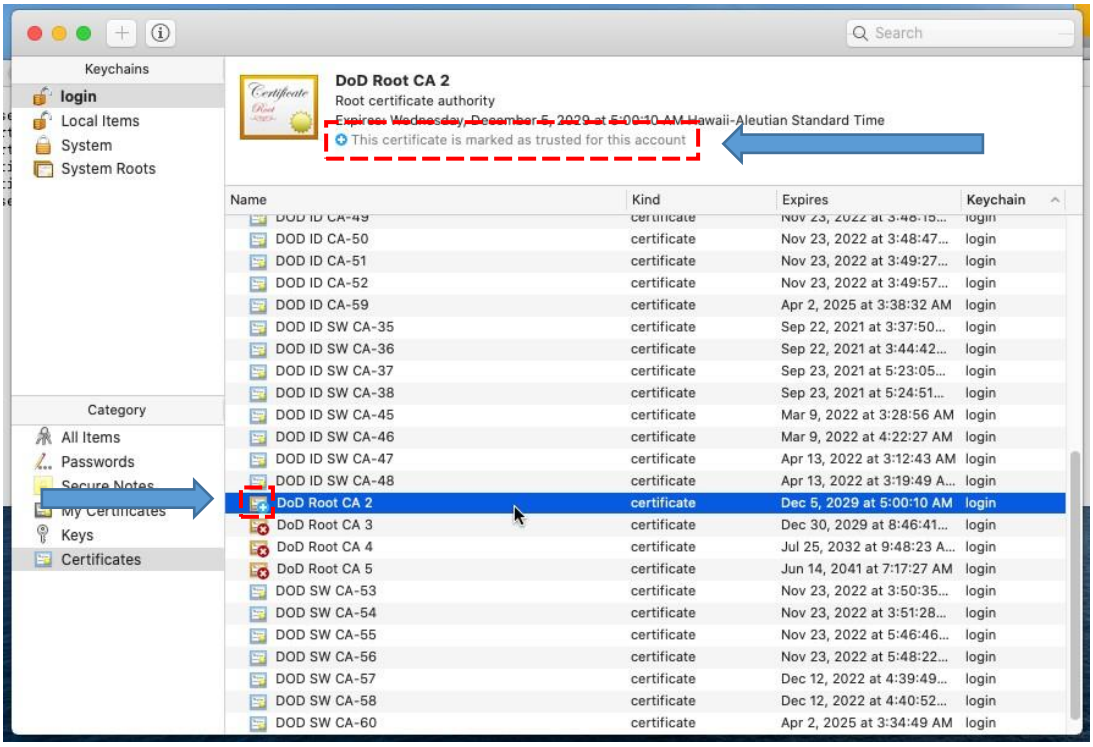
7.	Use the dialog box for "When using this certificate" to select **Always Trust.** 
8.	Close the certificate's window by clicking the red button in the upper left corner. 

Step	Trust DoD CA Certificates - OS

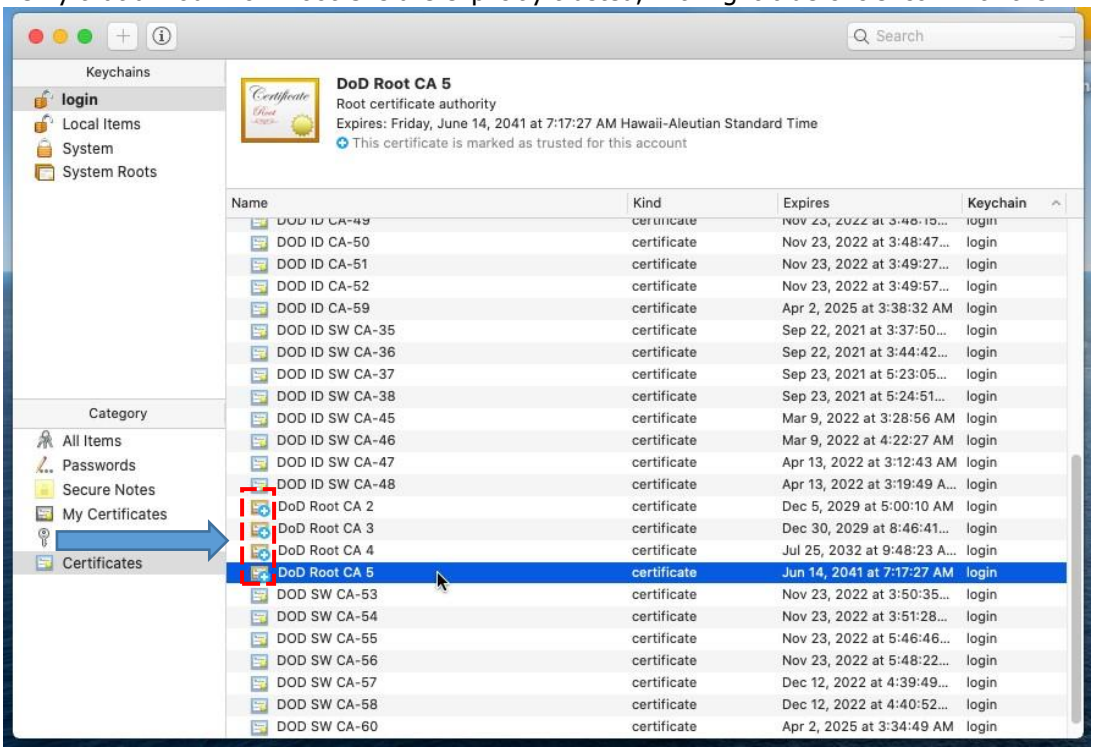
9. The following screen will appear. Enter password to confirm the trust change, and click **Update Settings.**



10. Confirm that the DoD Root CA is now marked as trusted.



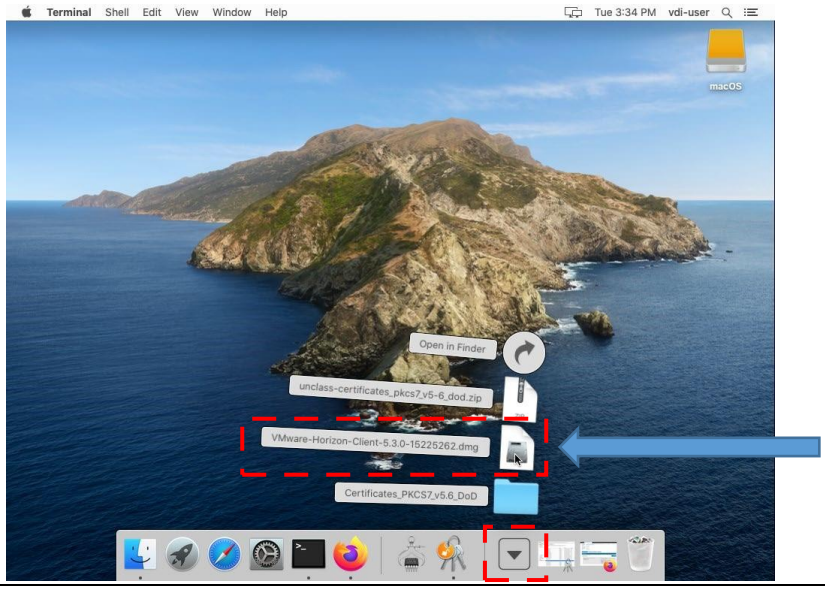
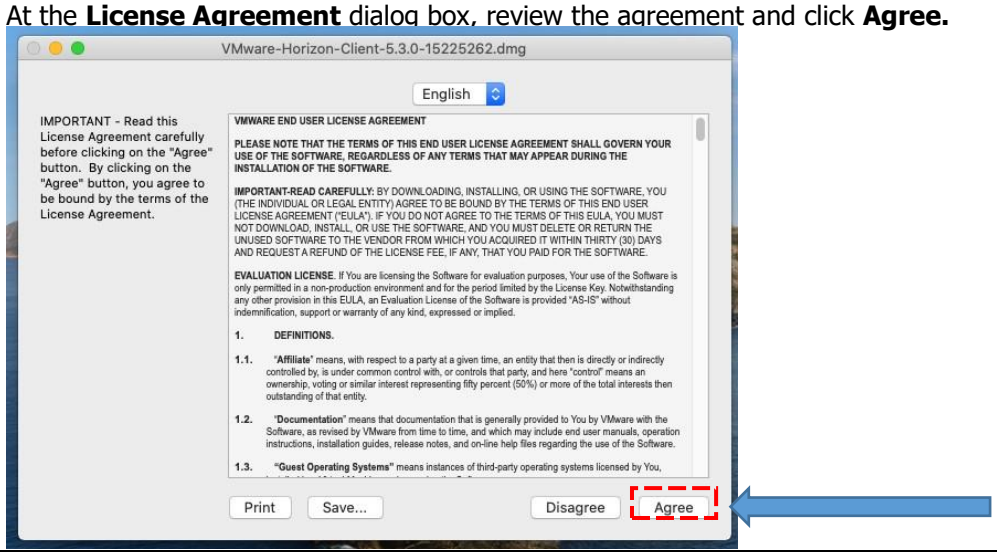
*** Repeat Steps 25 – 30 for DoD Root CA 3, 4 and 5 ***

Step	Trust DoD CA Certificates - OS
11.	Verify that all four DoD Root CAs are explicitly trusted, with light blue circle icon with the white +. 
End	The procedure to Install DoD CA Certificates - OS is completed. Proceed to Chapter 5: Install VDI VMware Horizon Client.

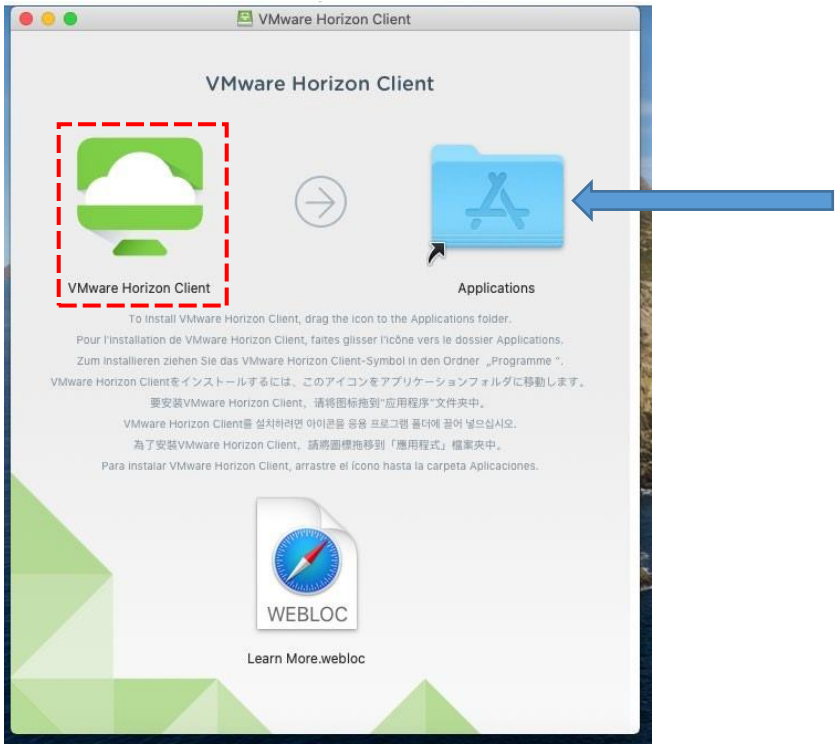
Chapter 5: Install VDI VMware Horizon Client

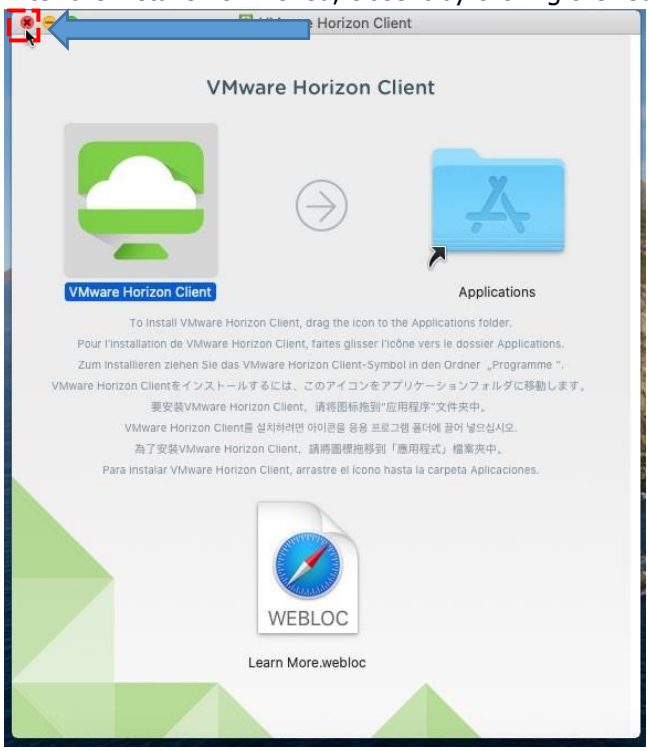
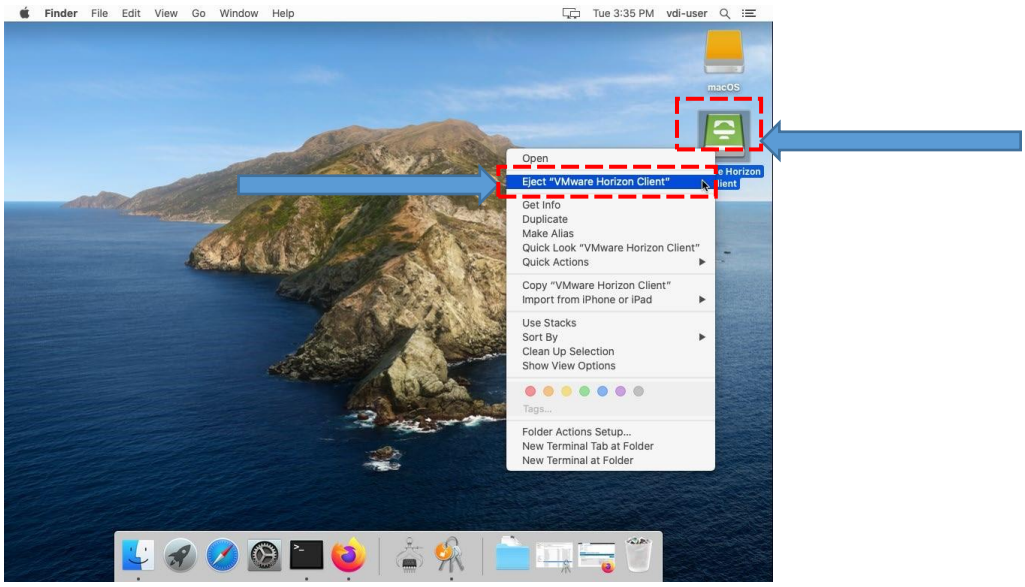
Use the following procedure to update the VMware Horizon Client.

Step	Install VDI VMware Horizon Client

Step	Install VDI VMware Horizon Client
1.	Access the recently downloaded files and click the VMware-Horizon client installer. 
2.	At the **License Agreement** dialog box, review the agreement and click **Agree.** 

Step	Install VDI VMware Horizon Client

9.	The following screen will appear. Drag the **VMware** icon to the **Applications** folder. 

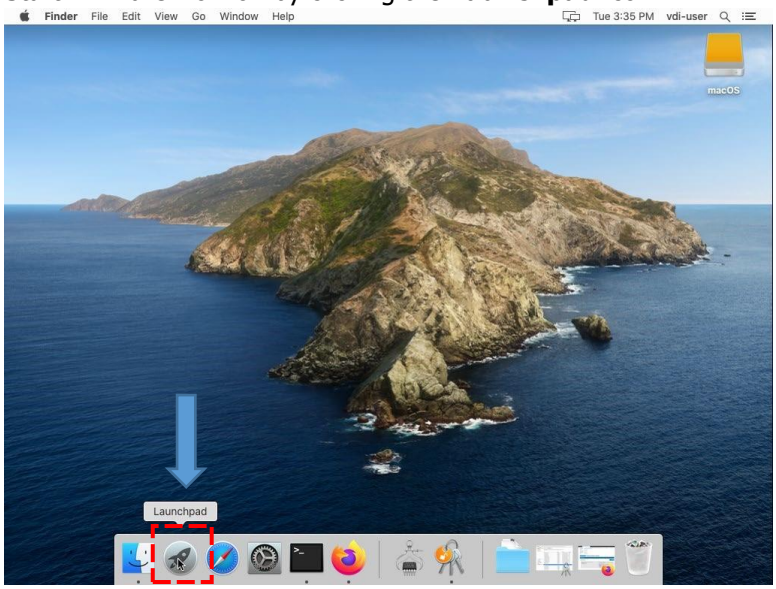
10.	After the installer is finished, close it by clicking the red button in the upper left corner. 
Step	**Install VDI VMware Horizon Client**
11.	Unmount the installer by right clicking on the green disk icon and selecting **Eject "VMware Horizon Client"**. 

End	The process for Installing the VDI VMware Horizon Client is complete. Proceed to Chapter 6: Connecting to VDI.

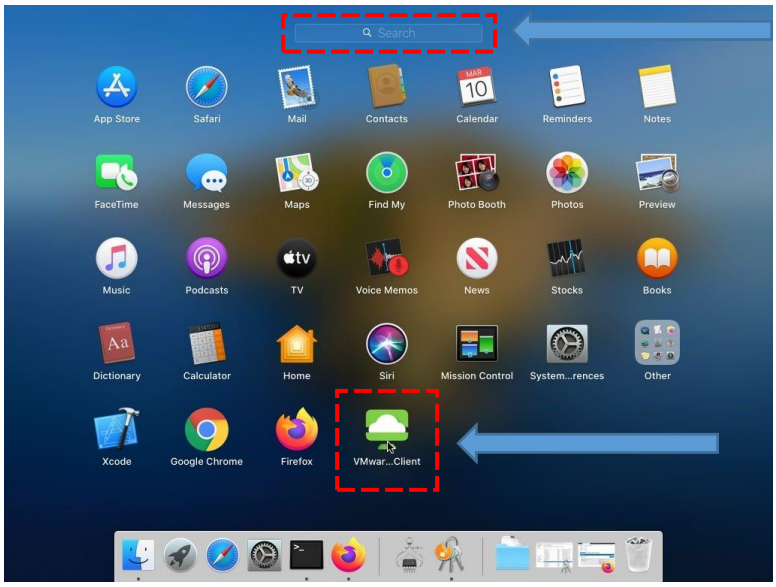
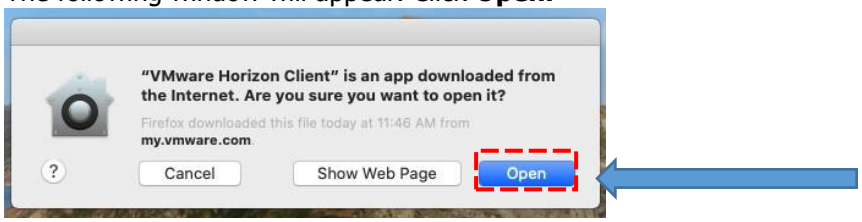
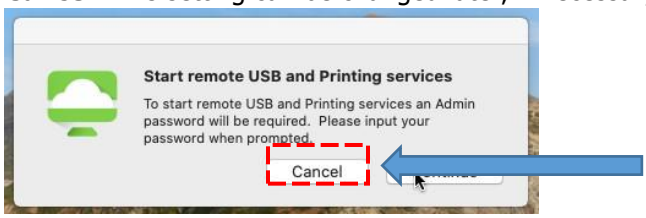
Chapter 6: Connecting to VDI

Use the following procedure to initially access VDI with the VMware Horizon Client. Several steps will only need to be performed the first time the program is run.

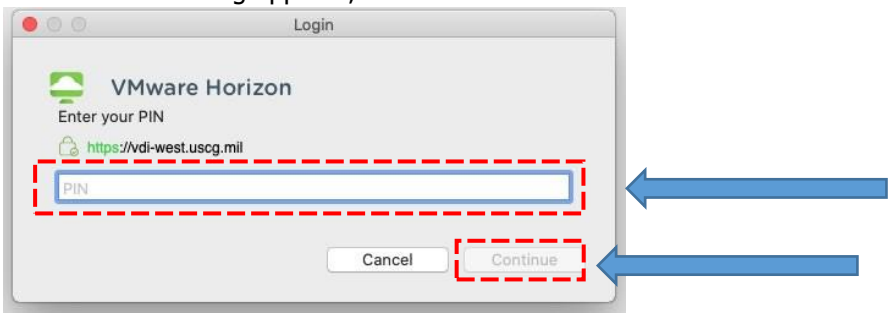
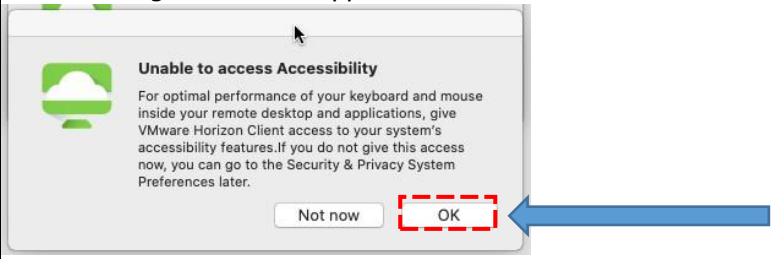
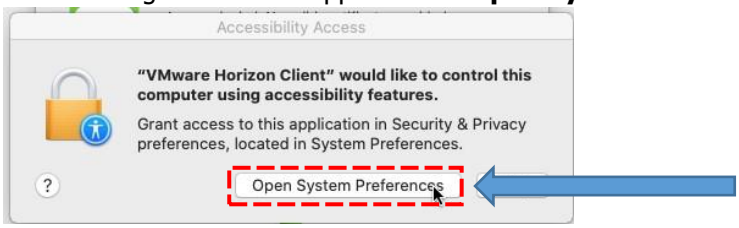
Step	Connecting to VDI
1.	Plug your smart card reader into the computer.
2.	Insert your CAC into the reader.

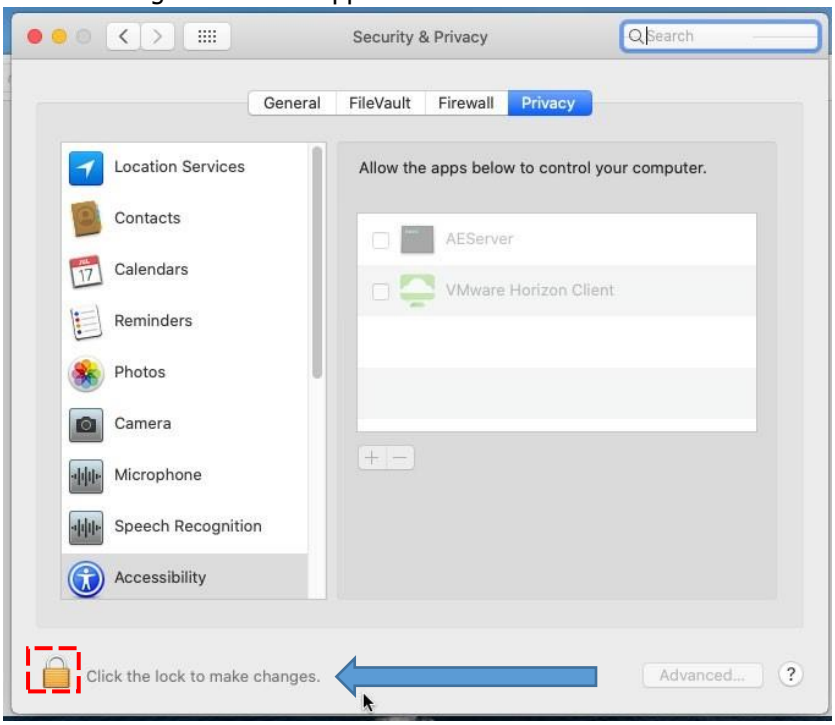
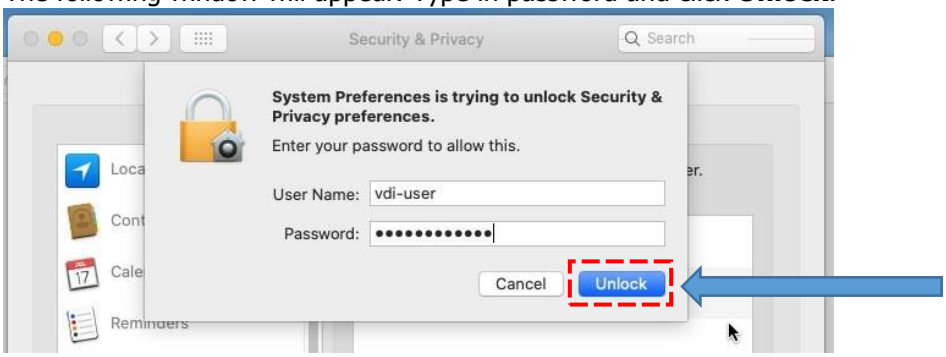
3.	Start VMWare Horizon by clicking the **Launchpad** icon. 

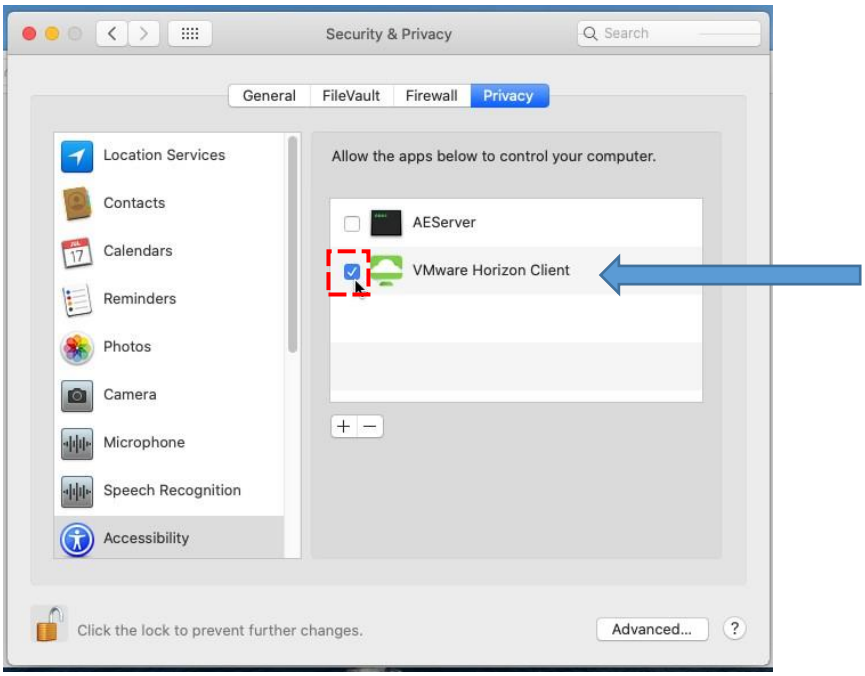
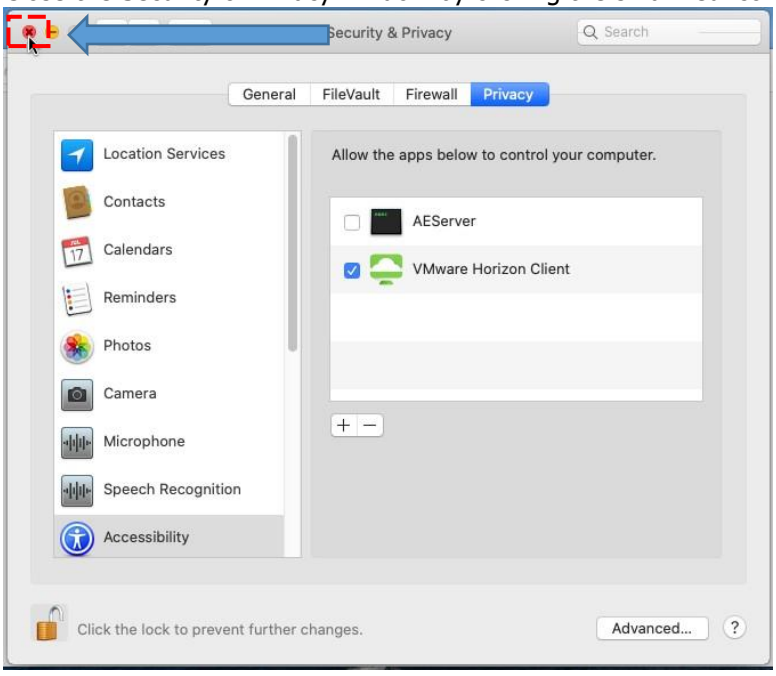
Step	**Connecting to VDI**

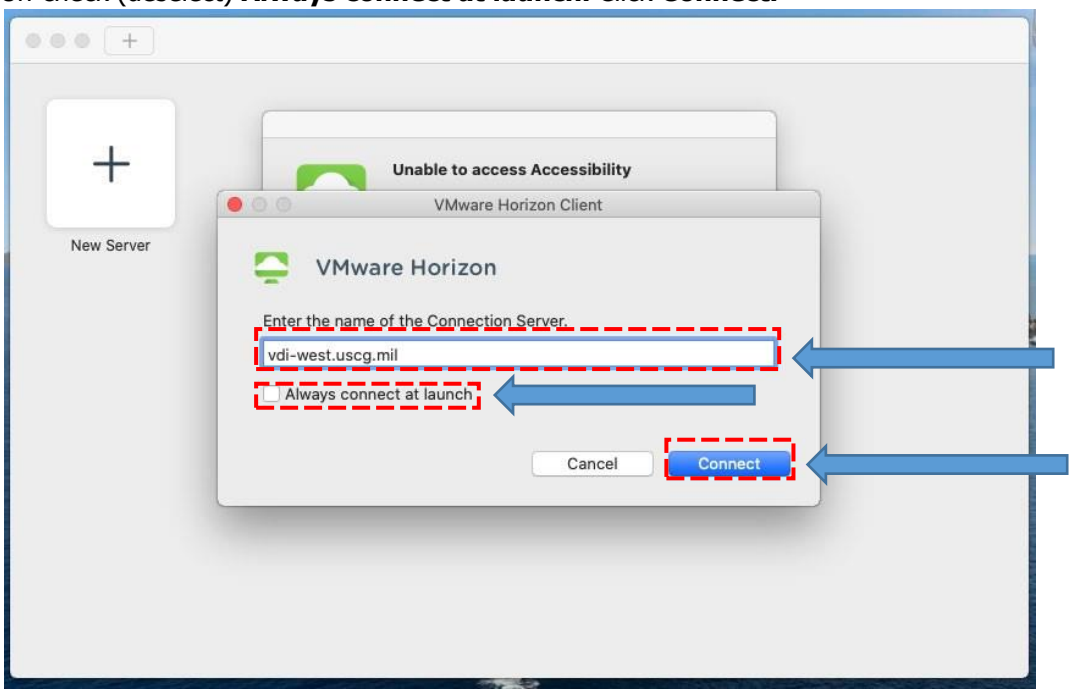
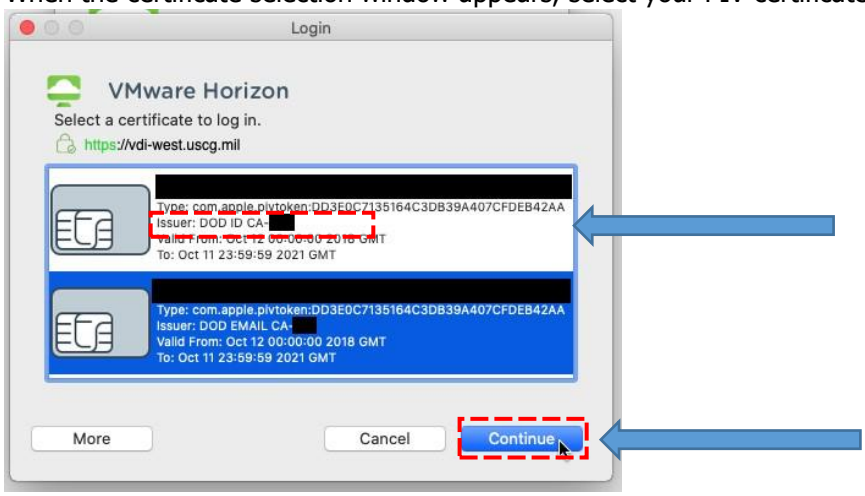
4.	If needed to locate the client, select the search bar at the top, and type in "VMware". Click the **VMWare Horizon Client** icon. 
5.	The following window will appear. Click **Open.** 
6.	The following window will appear. Most users do not need USB redirection, and should click **Cancel.** This setting can be changed later, if necessary. 

Step	Connecting to VDI

7.	When the PIN dialog appears, enter it and click **Continue**. 
8.	The following window will appear. Click **OK.** 
9.	The following window will appear. Click **Open System Preferences.** 

10.	The following window will appear. Click the **small lock** in the lower left corner. 
11.	The following window will appear. Type in password and click **Unlock**. 

12.	Enable the requested accessibility permissions by checking the box next to **VMware Horizon Client**. 
13.	Close the Security & Privacy window by clicking the small red icon in the upper left corner. 
14.	In VMware Horizon click **New Server**

15.	The following window will appear. Enter the appropriate Connection Server in the field, using the designated primary listed below: • For HQ, D01, D05, D07, D08, and D09, the primary server is **VDI-OSC.uscg.mil** or **VDIEast.uscg.mil**. • For D11, D13, D14, and D17, the primary server is **VDI-West.uscg.mil**. Un-check (deselect) **Always connect at launch.** Click **Connect.** 
16.	When the certificate selection window appears, select your PIV certificate, and click **Continue.** 

Step	Connecting to VDI
17.	When the certificate selection window appears, select your PIV certificate.
18.	A list of VDI desktop pools will appear. Double-click the **Remote Access** pool to launch your Windows VDI session. These pools may have a Windows 10.X naming convention attached. 
End	The procedure to Connect to VDI is complete.

Appendix A: Troubleshooting

Here are a few common errors and the most likely resolution.

User not recognized

This is most likely due to selecting the wrong certificate. When you choose the certificate to sign in with, select the "PIV" certificate.

User not entitled to resources

This means your user account is not set up to access VDI. Contact CSD support to request access.

Desktop resource not available (after selecting the pool to launch)

Either there are no desktops available to log in to, or your specific desktop is rebooting or is not responding. Wait 2 to 3 minutes and try again. If available, try a different desktop pool. If this issue persists for more than 10 minutes, please contact support.

VMware Horizon does not detect smart card (requests "Insert a smart card to log in.")

Occasionally, the CryptoTokenKit driver within macOS detects the smart card removal, but not the re-insertion. Close VMware Horizon, and unplug smart card reader. Then insert smart card into reader, then re-connect smart card reader to computer. Wait 30 seconds for macOS to detect both items, and restart VMware Horizon.

Appendix B: Update SCR-3500 Driver

Use the following simplified procedures to update the drivers used by macOS for the SCR3100A card reader.

Step	Enable Browser CAC Access - Firefox
1.	Using Safari, open the following link: http://files.identiv.com/products/smart-cardreaders/common-drivers/uTrust_MAC_Driver.zip

2.	The download warning screen likely appears (unless you have already granted download permissions). Click **Allow.**
3.	Open the extracted directory by clicking the Download icon on the Dock. The uncompressed folder should be visible. Click on the folder icon.
4.	Double click the file **scmccid_5_0_38_release_signed.pkg**.
5.	A warning message regarding the inability of Apple checking it for malicious software. Click **OK.**
6.	Grant permission for the file to be opened by clicking **Open.**
7.	The installer window appears. Click **Continue**.
8.	The ReadMe is displayed. Review, if desired, then Click **Continue.**
9.	The Software License Agreement is displayed. Review, then click **Continue.**
10.	Another software license window appears. Click **Agree.**
11.	The Installation confirmation window appears. Click **Install.**
12.	You will be prompted for authorization. Type in your password and click **Install Software.**
13.	The Installation Summary window is displayed. Click **Close.**
14.	The Installer will attempt to clean-up (delete) the downloaded files. Click **OK.**
15.	Another confirmation window will appear. Click **Move to Trash.**
End	The procedure Update SCR-3500 Driver is complete.

End of Document