Cyber Virtual Training Environment

Things You Will Need

- Common Access Card
- Common Access Card Reader
- Internet
- VMware Horizon Client (2212 8.8.1 or higher)
- CVTE User Account

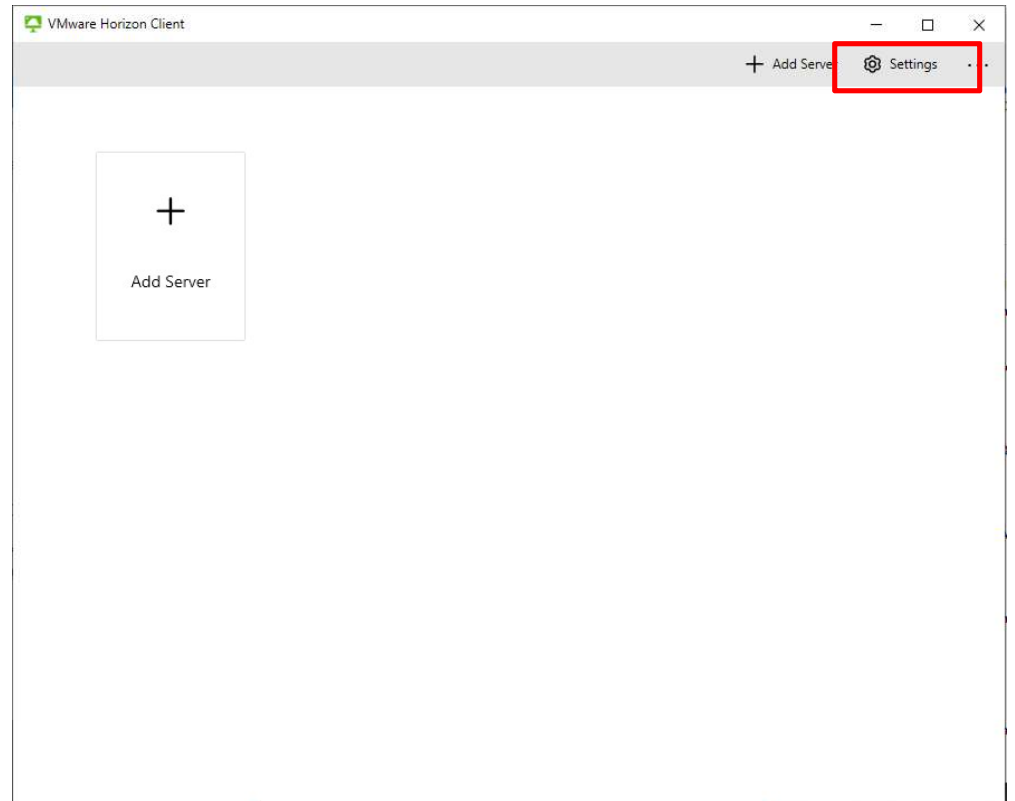https://customerconnect.omnissa.com/downloads/info/slug/desktop_end_user_computing/omnissa_horizon_clients/8

Setting up
VMware Horizon Client

- From your standard desktop double-click the "VMware Horizon Client" shortcut
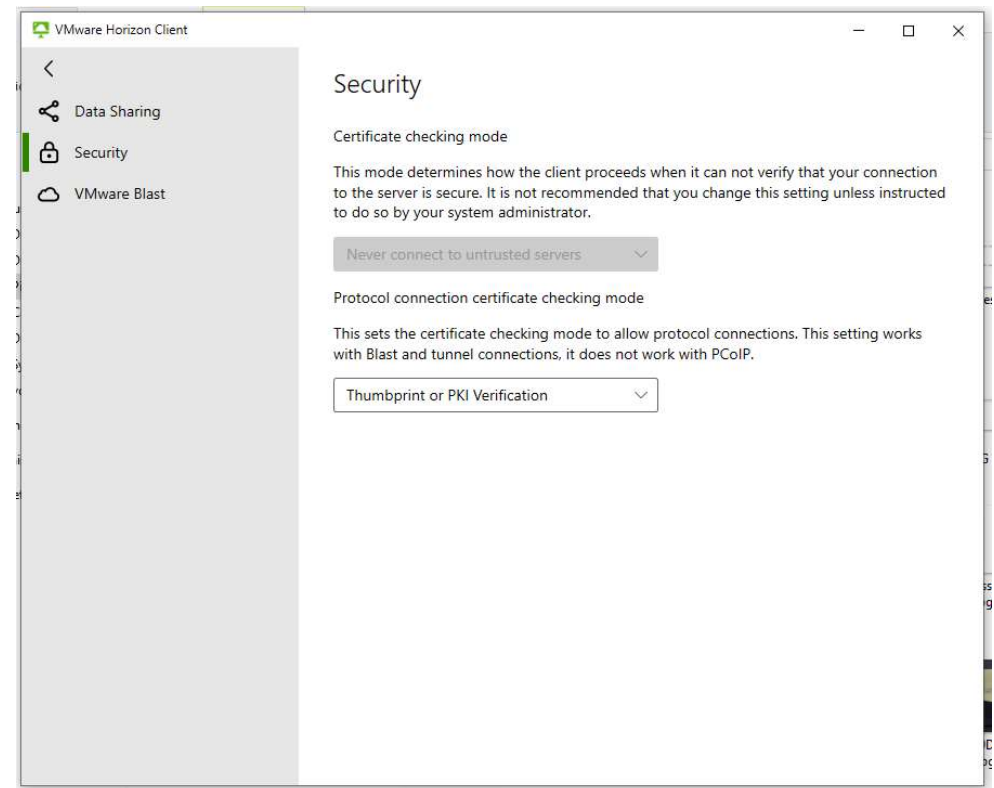
Set Security

On the home screen. Click the "Settings" in the upper right corner.

- On the "Settings" screen, select "Security" from the left side navigation. From the "Security" page. In the second drop down menu, select "Thumbprint or PKI Verification".
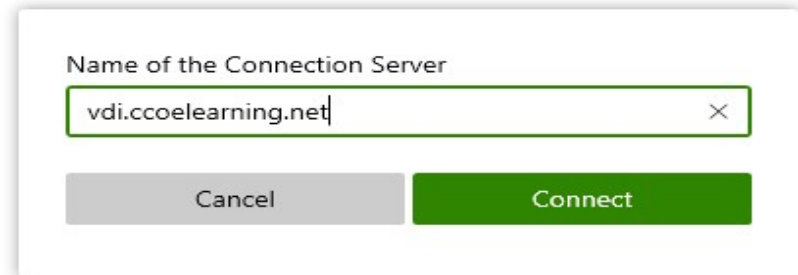
Add the CCOELEARNING server

• Click the back arrow in the upper left corner and return to the home screen. Click on '+Add Server' on the home page in either of the two locations.
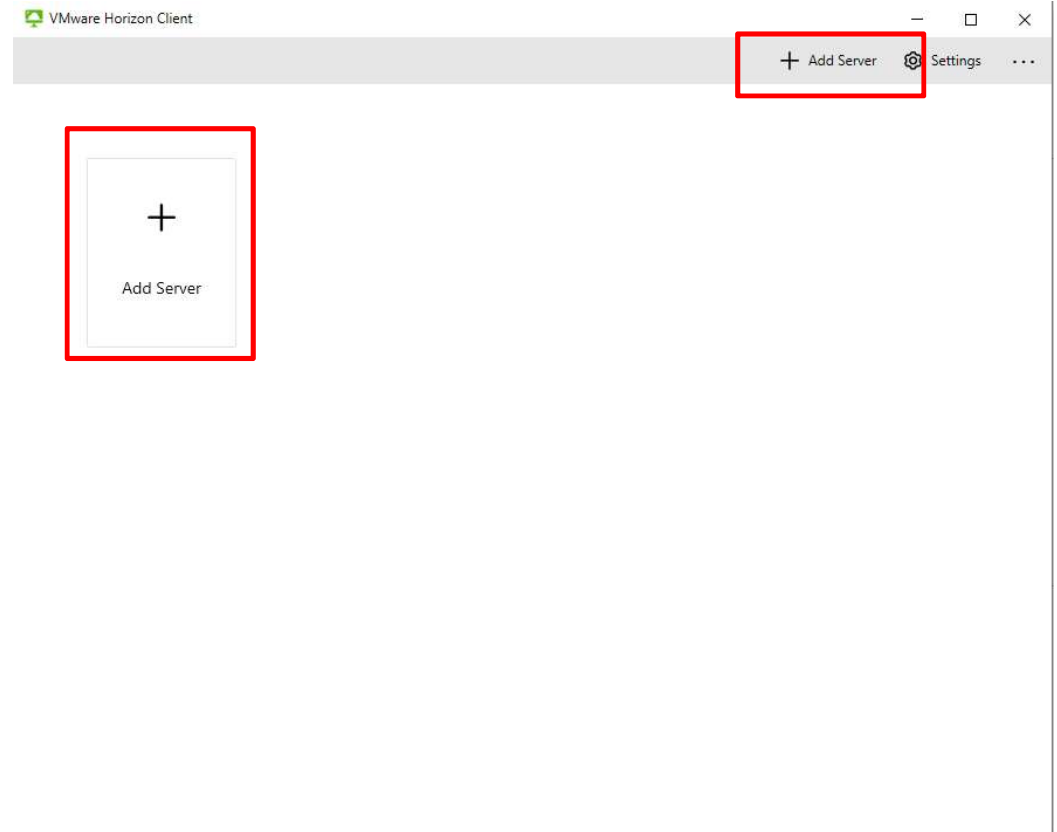
In the pop-up box, type "vdi.ccoelearning.net" and hit connect.

# Add the connection server

Name of the Connection Server

vdi.ccoelearning.net   ×

Cancel   Connect

VMware Horizon Client   —   □

＋ Add Server   ⚙ Settings

vdi.ccoelearning.
net

•••

Authenticating to the server

- Select your correct AUTHENTICATION certificate

- A DoD Notice and Consent Banner will appear. Click Accept. When prompted, select your PIV authentication certificate. Enter your PIN when prompted and click login. You will see a 2nd DoD Notice and Consent Banner. Click Accept.
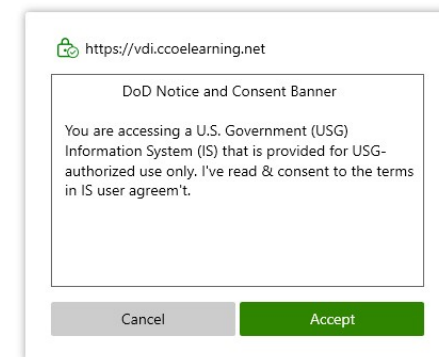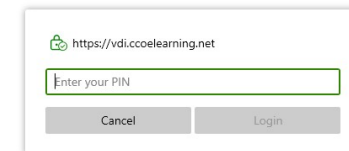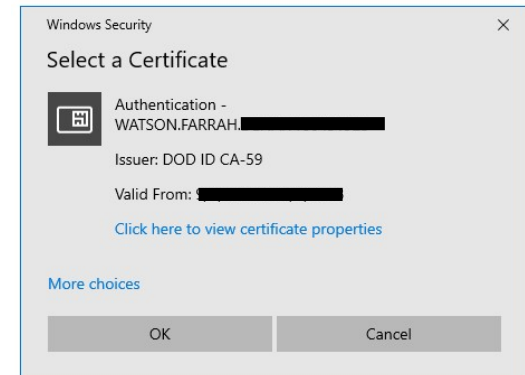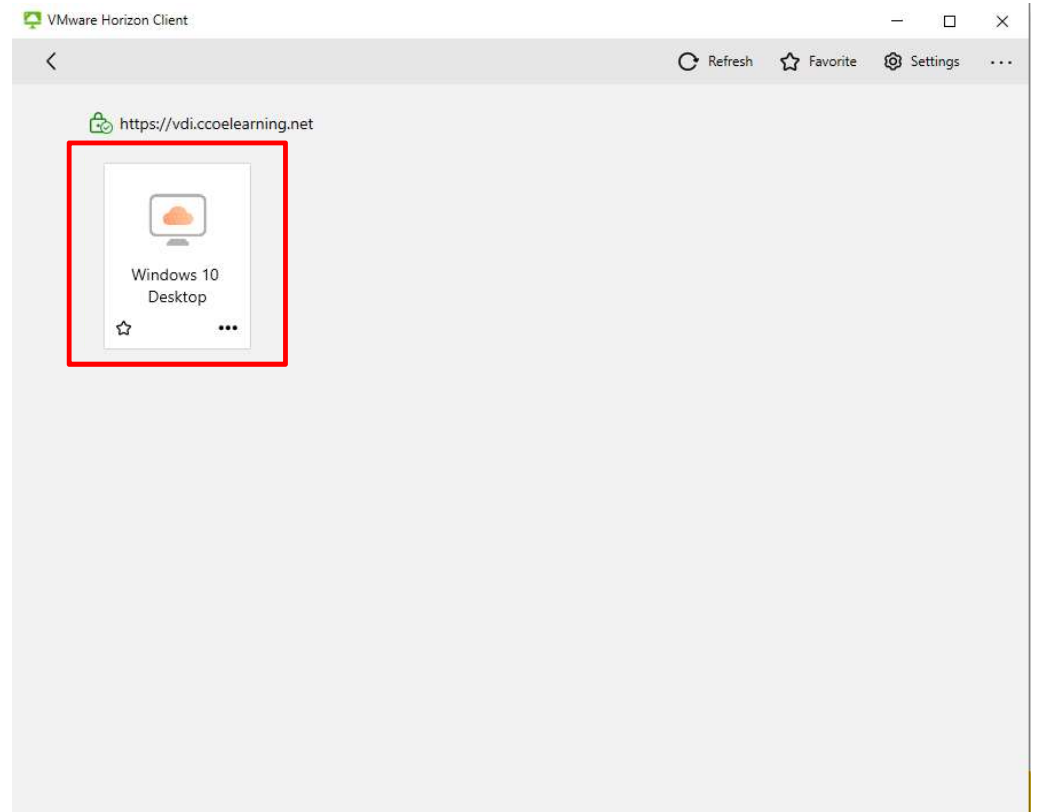
Horizon Client Pools

- VMware Horizon Client will open to the pools that your account has access to.
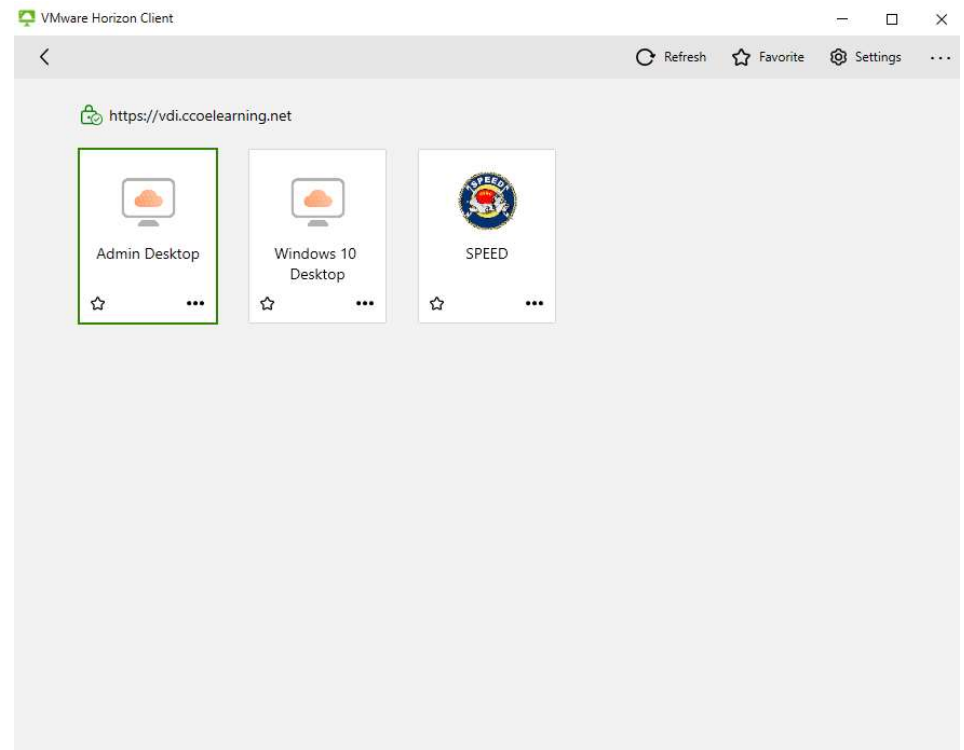
Accessing the VDI desktop

- Double-click the icon "Windows 10 Desktop" . The window will change and show "Loading Desktop".

Logging into your desktop

- Your desktop will open to the lock screen. At the top of the screen, click "Ctrl+Alt+Del" in the menu bar. The desktop will change to the blue Consent Screen and you must click "OK". SSO will automatically sign you into the VDI desktop environment.
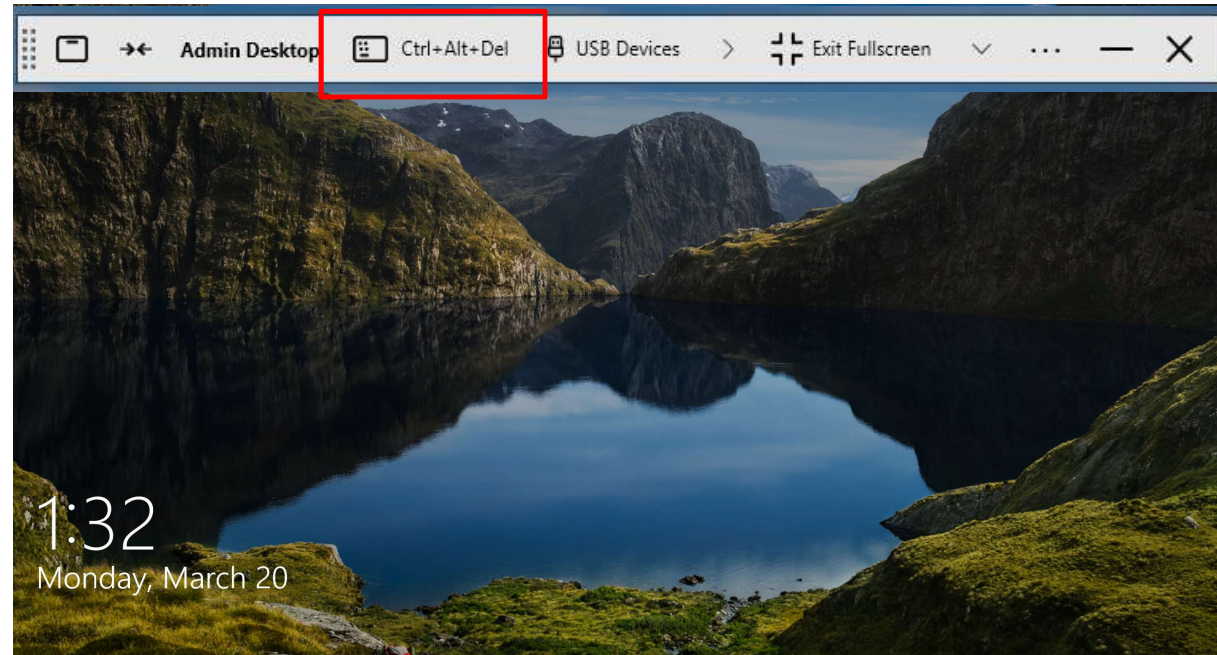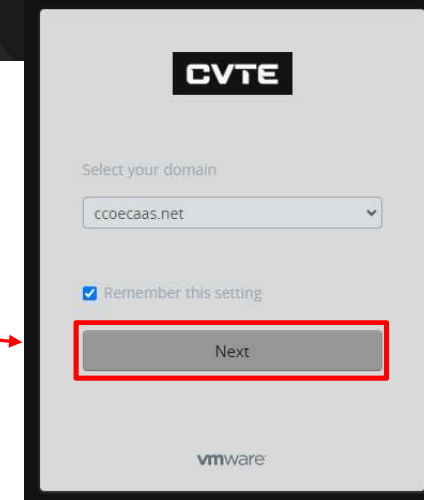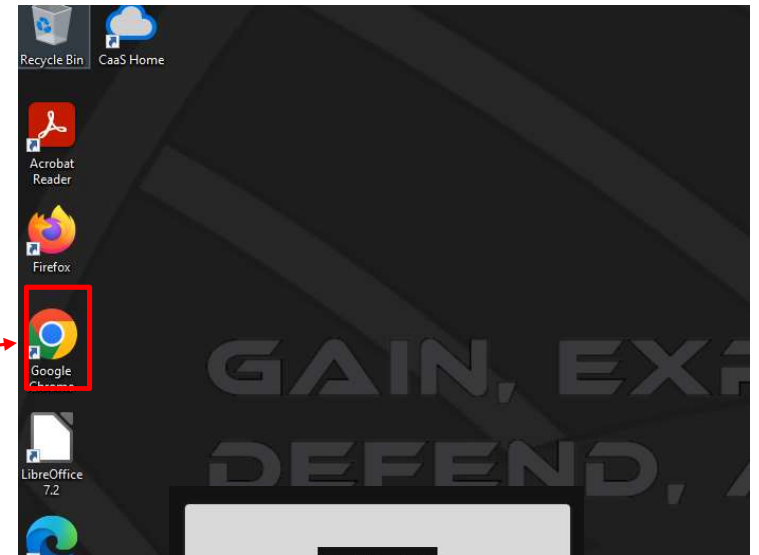
Accessing CVTE

- Navigate to the CAAS intranet by:
  launching Google Chrome from the
  desktop shortcut (CVTE Home is the
  landing page) or
  https://home.ccoecaas.net

- Click "Next"

- Select "Agree" to the Consent Banner to access the platform

CVTE

You are accessing a U.S Government(USG) Information System(IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct(PM), law enforcement(LE), and counterintelligence(CI) investigations.
At any time, the USG may inspect and seize data stored on this IS.
Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
This IS includes security measures(e.g., authorization and access controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.

(ucfgllcpvd073.ccoecaas.net)

Cancel

Agree

vmware

Authenticating to CVTE

- Select your correct AUTHENTICATION certificate. Click OK.

  *****If you are unsure of what certificate to use click on the certificate once and select "Certificate Information" and find the one that has the correct expiration date.*

- When the Windows Security window appears, input your PIN and Click OK.
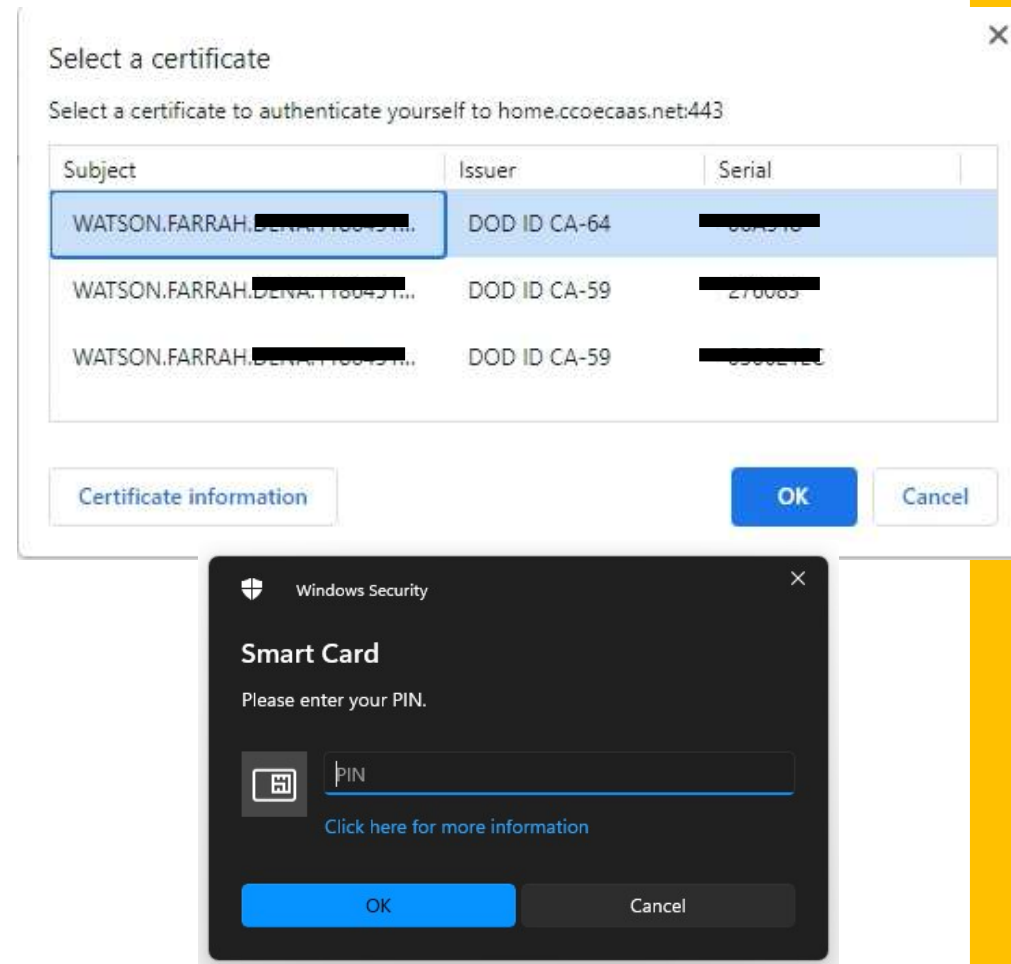
Accessing CSTN

Once you have successfully signed in to the CVTE, click "Open" on the CSTN Production App
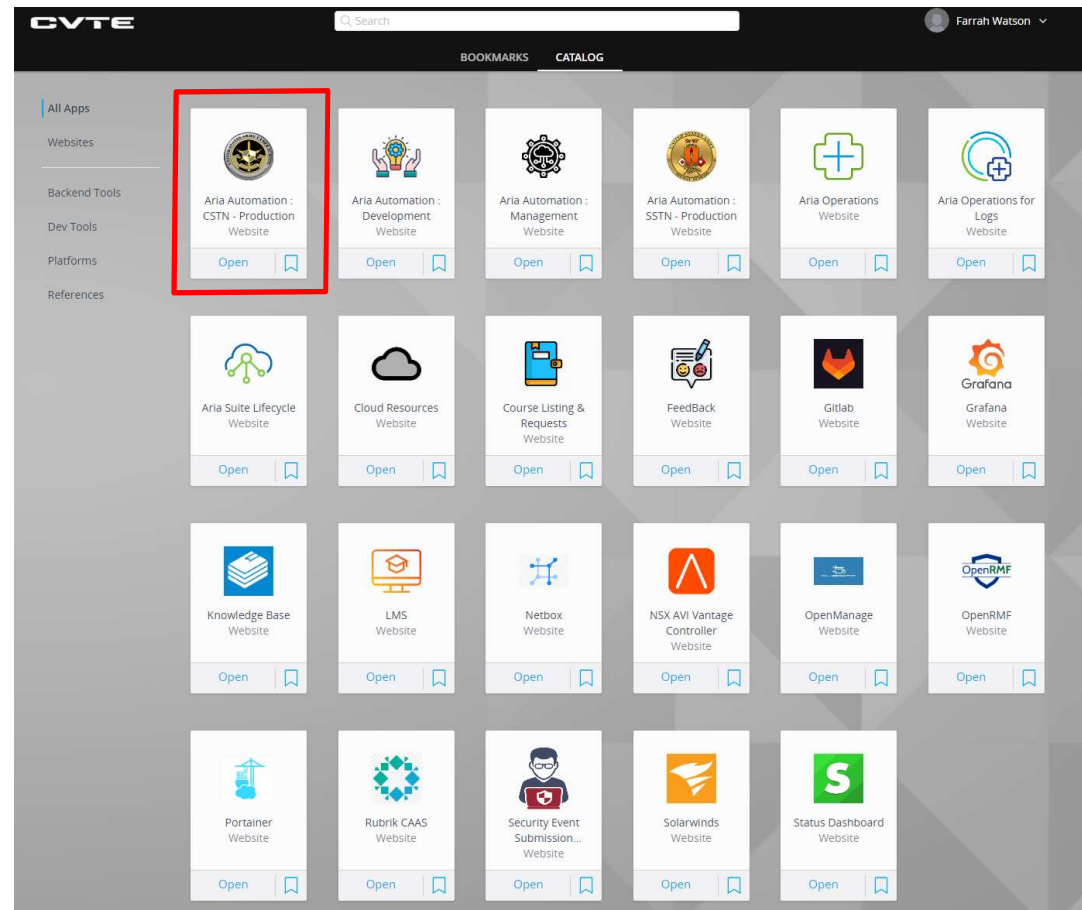
Cyber Virtual Training Environment

- Gaining Privileged Instructor Access in the CVTE