



Customer Outreach
ITEMS - User Facing Services

Remote Access User Guide

Windows 10 & Macintosh

This guide covers how to utilize Remote Access for the Telework employee for both Windows 10 and Macintosh. Supported browsers include Microsoft Internet Explorer and Google Chrome.

Overall Classification of this document is:

UNCLASSIFIED

Table of Contents

(U) ITEMS User Facing Services – Customer Outreach.....	1
(U) About Us	1
(U) Overview – Remote Access for Telework Employee’s	2
(U) Chapter One – Pre-Checks	2
(U) Chapter Two – Windows Required Applications Installation.....	3
(U) InstallRoot 5.5	3
(U) Citrix Workspace.....	11
(U) Microsoft Internet Explorer – Verification of DoD Certificate installation	14
(U) Google Chrome – Verification of DoD Certificate installation.....	16
(U) Chapter Three – Windows Remote Access	18
(U) Recently updated Common Access Card (CAC) Users (16 Digit PIV Users)	18
(U) Windows - Microsoft Internet Explorer.....	18
(U) Windows - Google Chrome	22
(U) Existing NGA Common Access Card (CAC) Users	25
(U) Windows - Microsoft Internet Explorer.....	25
(U) Windows - Google Chrome	29
(U) Remote Access – Unlocking the Screen.....	32
(U) Remote Access – Sign out procedure.....	32
(U) Chapter Four – Remote Access Troubleshooting.....	33
(U) Clear Browser Cache – Microsoft Internet Explorer.....	33
(U) Clear Browser Cache – Google Chrome	36
(U) Clear Browser SSL State – Microsoft Internet Explorer.....	38
(U) Chapter Five – Macintosh Required Applications	40
(U) Mac Middleware Software	40
(U) DoD Intermediate Certificates.....	41
(U) Citrix Workspace.....	43
(U) Chapter Six – Macintosh Remote Access	44
(U) Macintosh – Google Chrome	44
(U) Remote Access – Unlocking the Screen.....	46
(U) Remote Access – Sign out procedure.....	47
(U)Appendix.....	48
(U) Appendix A – Agency Service Desk.....	48
(U) Appendix B – Contact Us.....	49

(U) ITEMS User Facing Services – Customer Outreach

(U) About Us

(U) We specialize in the ITEMS User Facing Services, Customer Outreach which incorporates training, knowledge management, and end user communications. From developing skillsets, increasing productivity and ensuring the end user is well informed, we ultimately strengthen the government workforce.

(U) **Our Philosophy**, it's simple: We start by assessing the need presented by the customer based on Service+ feedback, requests, and metrics.

(U) **Our Instructors, Technical Writers, and Communications members.** We observe the different IUFS subject matter experts and together design curriculums, guides, and communications. Prior to any of our products being published or taught, we learn the material inside and out to communicate a clear and precise message to the End User.



(U) Overview – Remote Access for Telework Employee’s

U) This guide covers Microsoft Internet Explorer and Google Chrome for Windows 10 and Google Chrome for Macintosh. Other browsers may not be compatible with the built-in smart card software. To utilize one of the non-supported browsers a secondary middleware application would be required such as ActivClient.

For Macintosh systems, CACKey is the suggested middleware that works with Safari and Google Chrome that requires no additional configuration.

(U) Chapter One – Pre-Checks

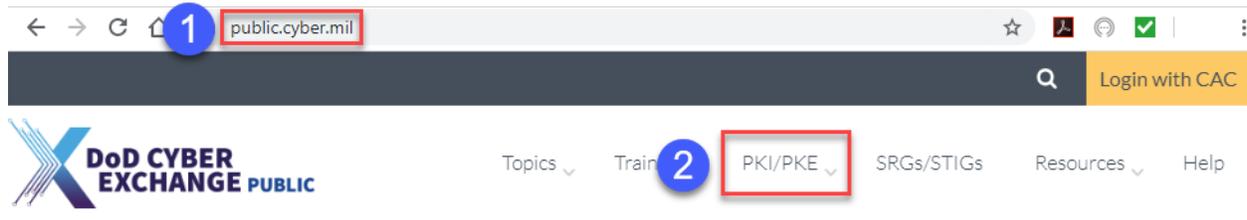
- (U) Ensure the CAC reader is plugged into an available USB port.
 - (U) Additional drivers that may be required will automatically download and install. Administrative rights will be required on your home computer to complete this action.
- (U) Verify that the “**Smartcard Reader**” is available in the Device Manager.
- (U) From the device manager locate the “**Smartcard Reader**” and verify within the properties that drivers are listed for the application. If you are not able to locate the device, unplug and plug the device back into the computer.
- (U) Windows Required Applications for remote access, Citrix Workspace and InstallRoot 5.5.
- (U) Macintosh Required Applications for remote access, Citrix Workspace, CACKey, and Root DoD Certificates

(U) If previous versions currently installed, they will need to be uninstalled prior to installing the latest versions.

(U) Chapter Two – Windows Required Applications Installation

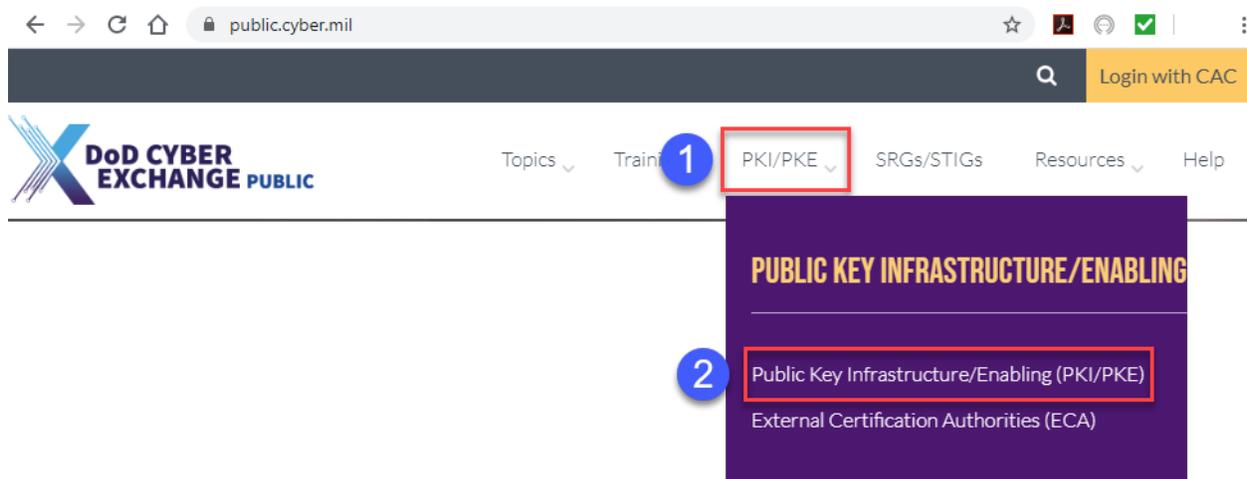
(U) InstallRoot 5.5

(U) Navigate to the DoD Cyber Exchange Public site (<https://public.cyber.mil/>), and select “PKI/PKE” from the top menu bar.



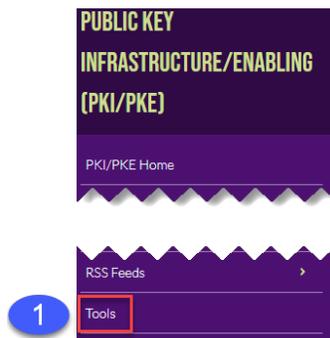
(U) Figure 1 DoD Cyber Exchange Public site

(U) From the drop-down menu select “Public Key Infrastructure/Enabling (PKI/PKE)”



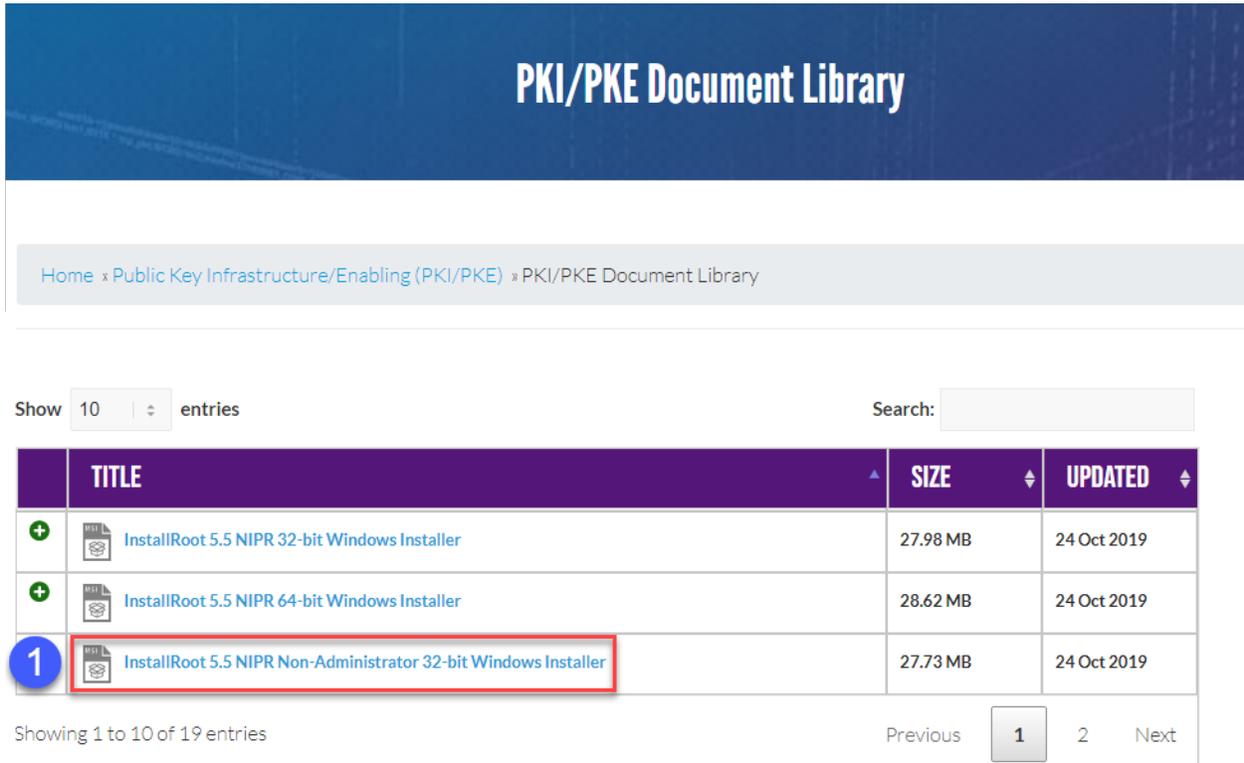
(U) Figure 2 Public Key Infrastructure Exchange (PKI/PKE)

(U) From the Menu on the left on the Public Key Infrastructure/Enabling (PKI/PKE) locate and select “Tools”.



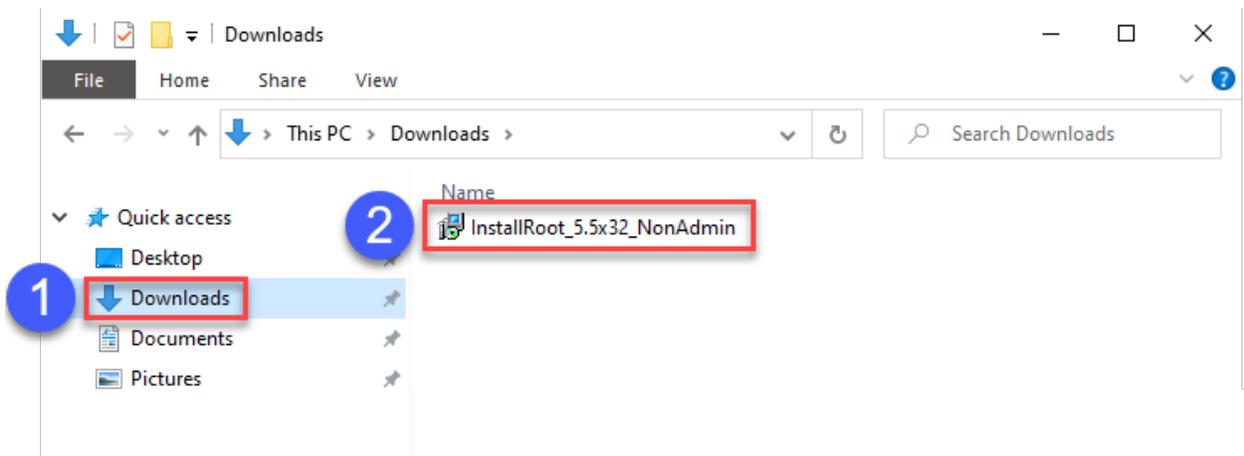
(U) Figure 3 Tools

(U) Within the *PKI/PKE Document Library* select “**InstallRoot 5.5 NIPR Non-Administrator 32-bit Windows Installer**”.



(U) Figure 4 InstallRoot NIPR Non-Administrator 32-bit Windows Installer

(U) Once downloaded, navigate to your “**Downloads**” folder and double-click on the “**InstallRoot_5.5x32_NonAdmin**” application.



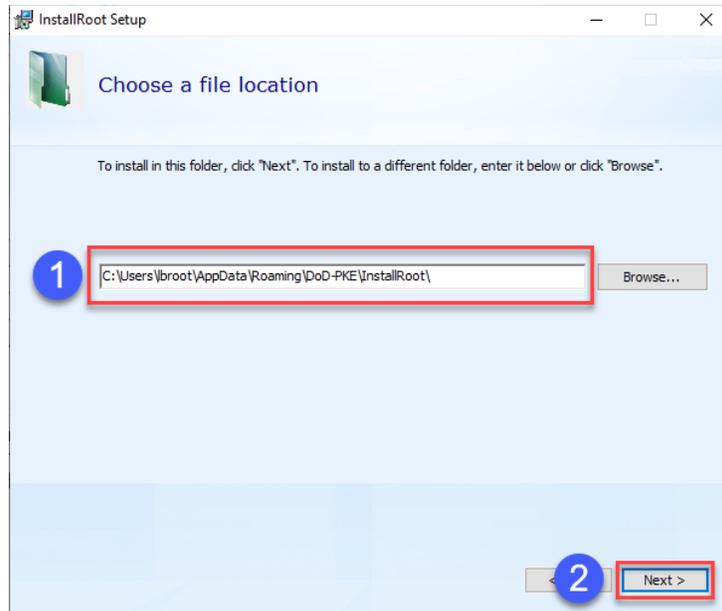
(U) Figure 5 InstallRoot 5.5 Application

(U) Once the installation begins, follow the on-screen prompts.



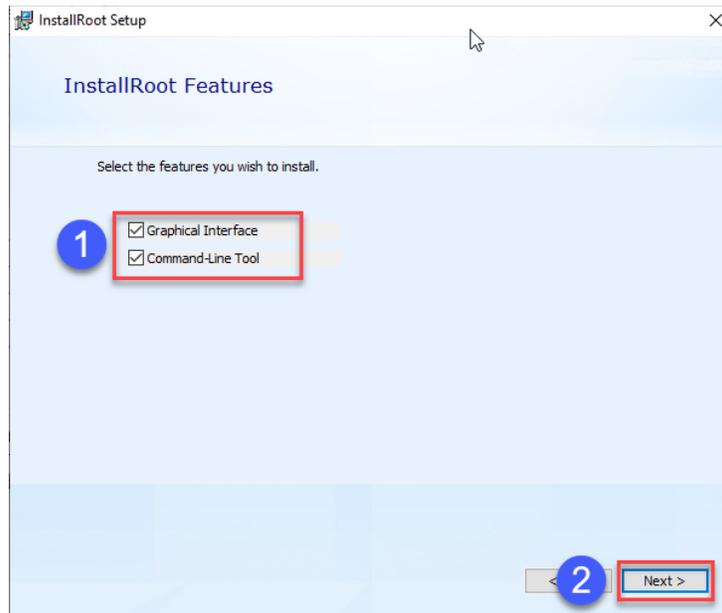
(U) Figure 6 InstallRoot Setup Wizard

(U) It is recommended that the default installation file location is used.



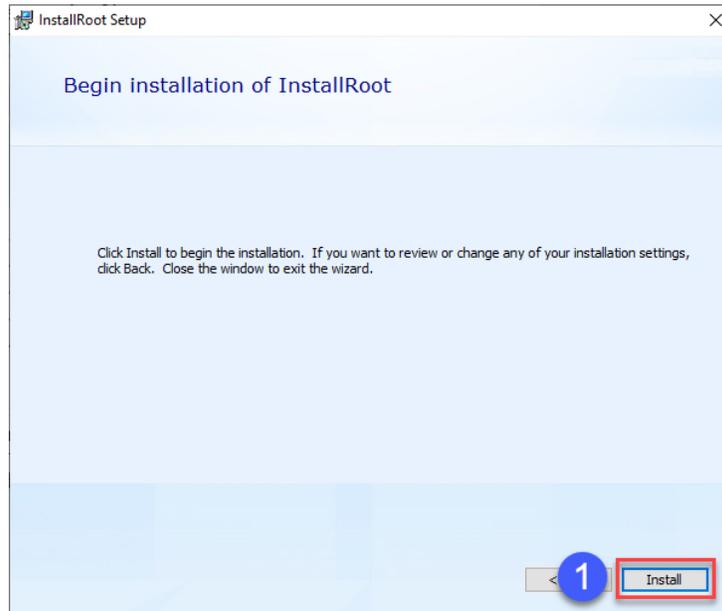
(U) Figure 7 Select Installation folder

(U) Use the default selection of both the “*Graphical Interface*” and “*Command-Line Tool*”.



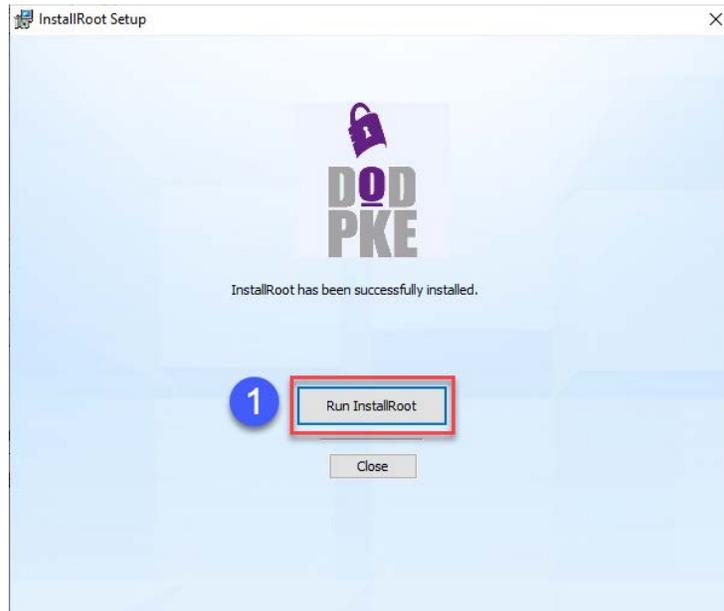
(U) Figure 8 InstallRoot Features

(U) Select “**Install**” to begin the installation.



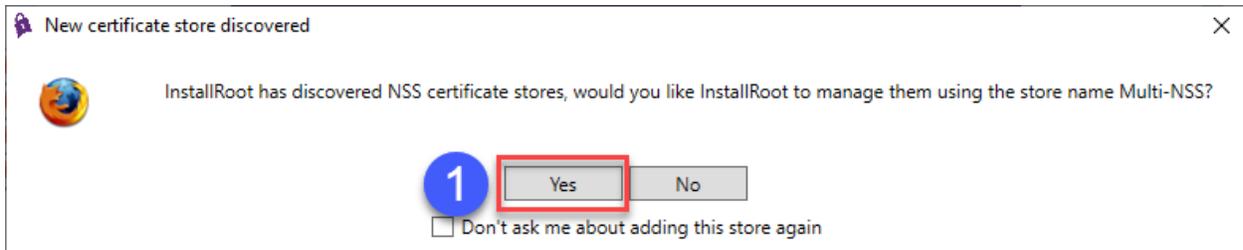
(U) Figure 9 Begin installation

(U) Once the installation has successfully completed, select **“Run InstallRoot”**.



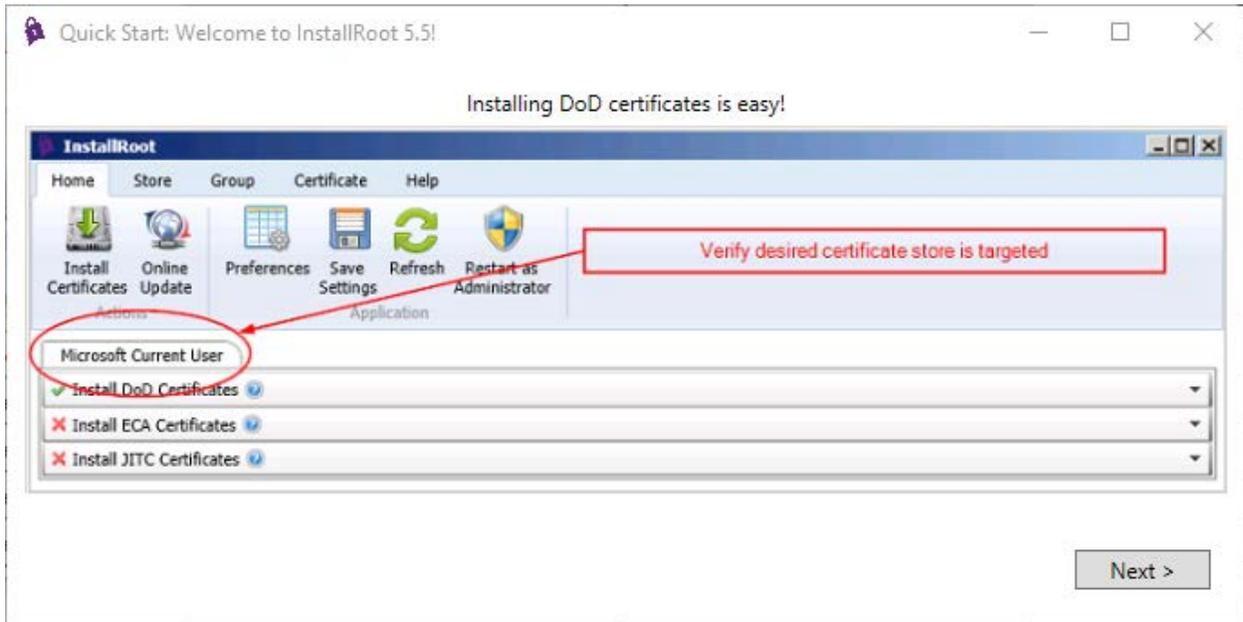
(U) Figure 10 Run InstallRoot

(U) Once the InstallRoot begins to install, the tool may discover a new certificate store. If the pop-up appears select **“Yes”**.



(U) Figure 11 New Certificate store discovered

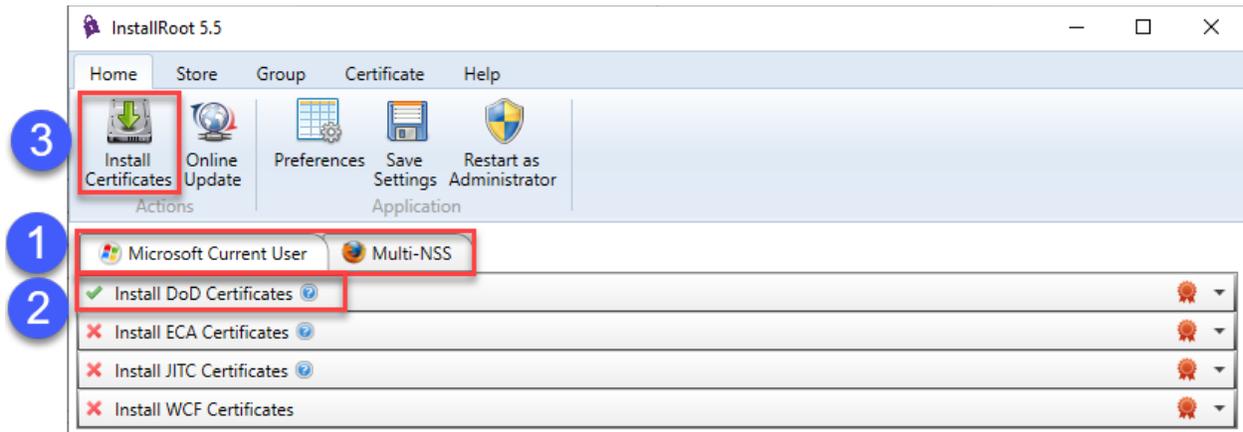
(U) Once the InstallRoot application opens, a “Quick Start” Welcome to InstallRoot 5.5 pop-up will appear and provide directions on how to install the certificates.



(U) Figure 12 Quick Start Guide

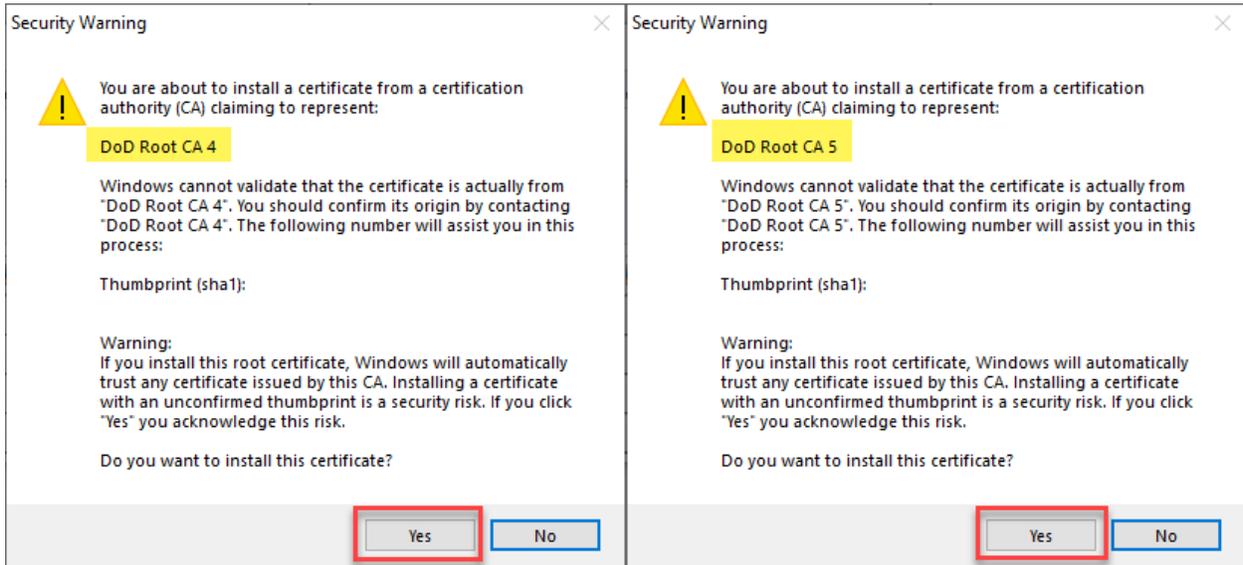
(U) From the InstallRoot 5.5 application perform the following steps:

- Verify for each tab that the “**Install DoD Certificates**” have a **GREEN** check mark.
- After verifying each tab, select “**Install Certificates**”.



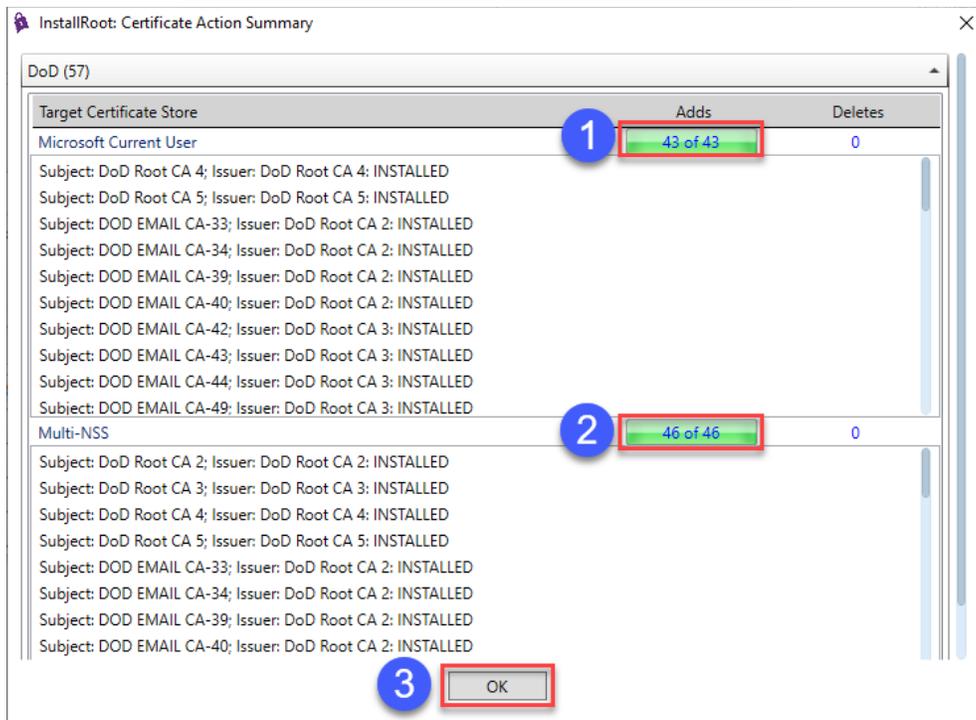
(U) Figure 13 Install Certificates

(U) During the installation, Security Warning pop-up(s) may appear prompting for approval to install the different DoD Root CA's.



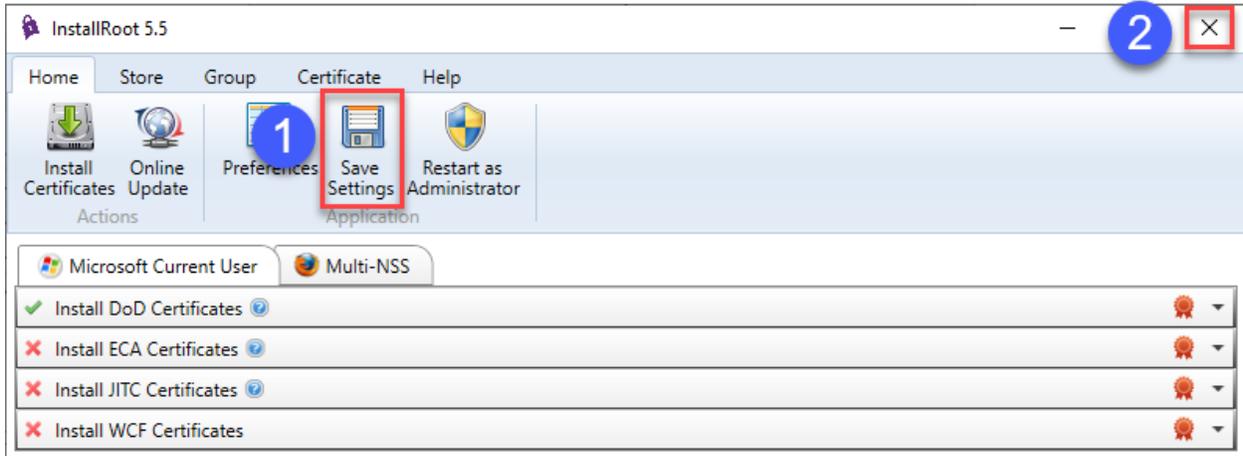
(U) Figure 14 DoD Root CA

(U) From the InstallRoot Certificate Action Summary screen, verify the installation was successful. If any errors appear or the installation was not successful attempt to reinstall prior to calling the Enterprise Service Desk.



(U) Figure 15 InstallRoot Certificate Action Summary

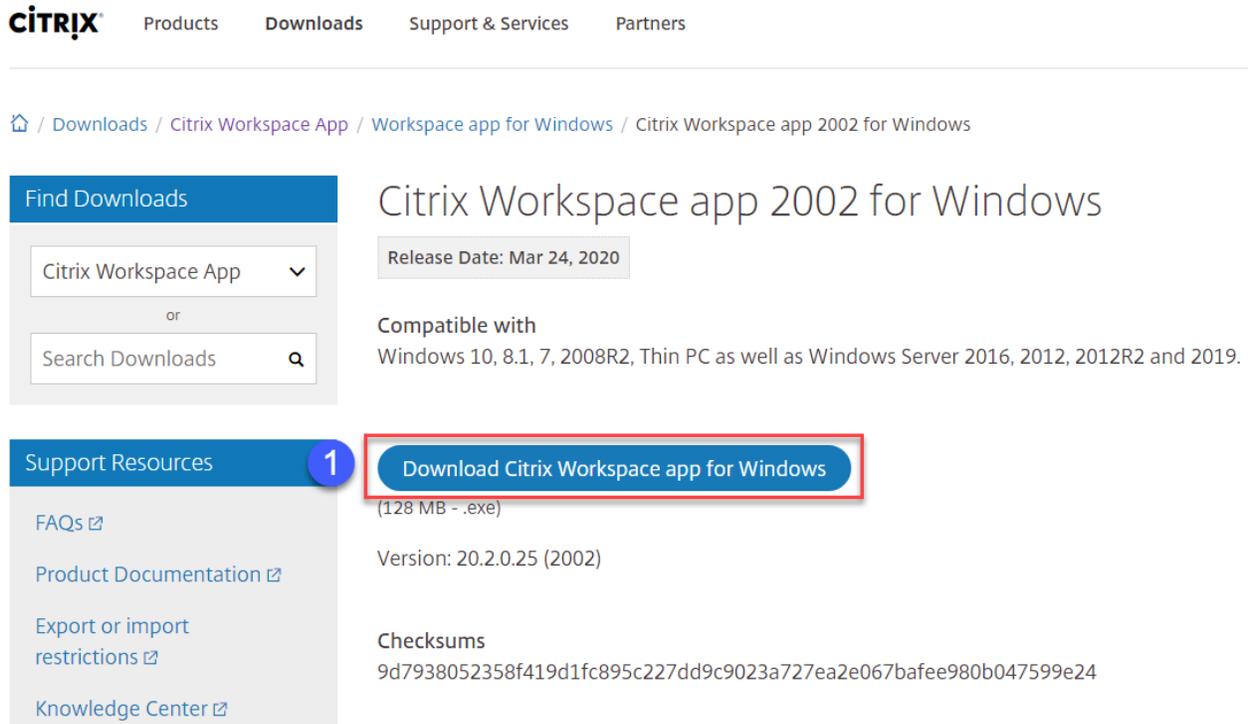
(U) From the InstallRoot 5.5 application screen select “**Save Settings**” and then select the “**X**” in the upper right corner of the application.



(U) Figure 16 save Settings

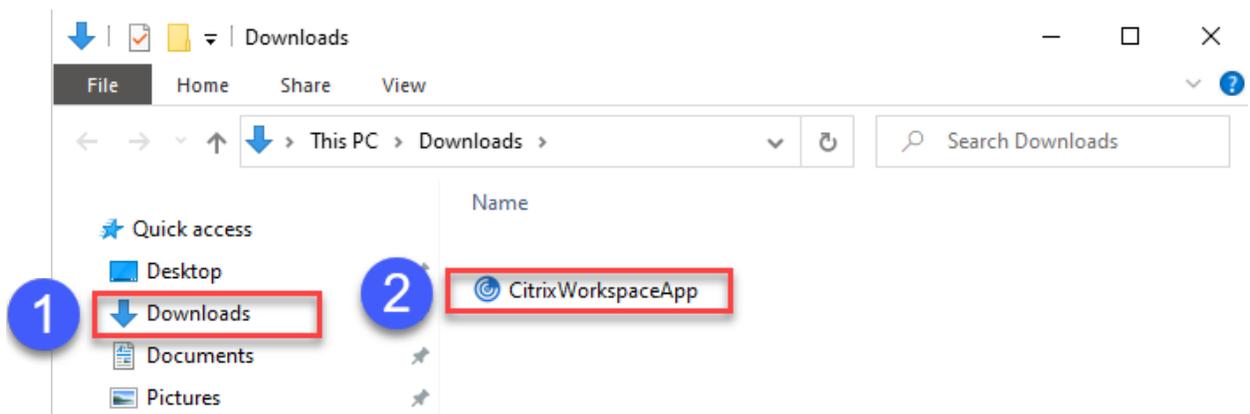
(U) Citrix Workspace

(U) From the Citrix website (<https://www.citrix.com/downloads/workspace-app/windows/workspace-app-for-windows-latest.html>), select **“Download Citrix Workspace app for Windows”**.



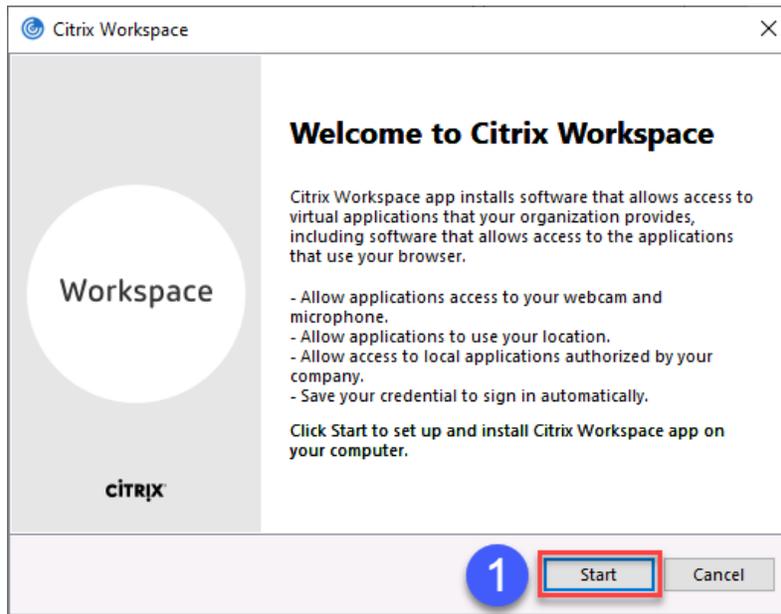
(U) Figure 17 Citrix Workspace download page

(U) Once downloaded, navigate to your **“Downloads”** folder and double-click on the **“CitrixWorkspaceApp”** application.



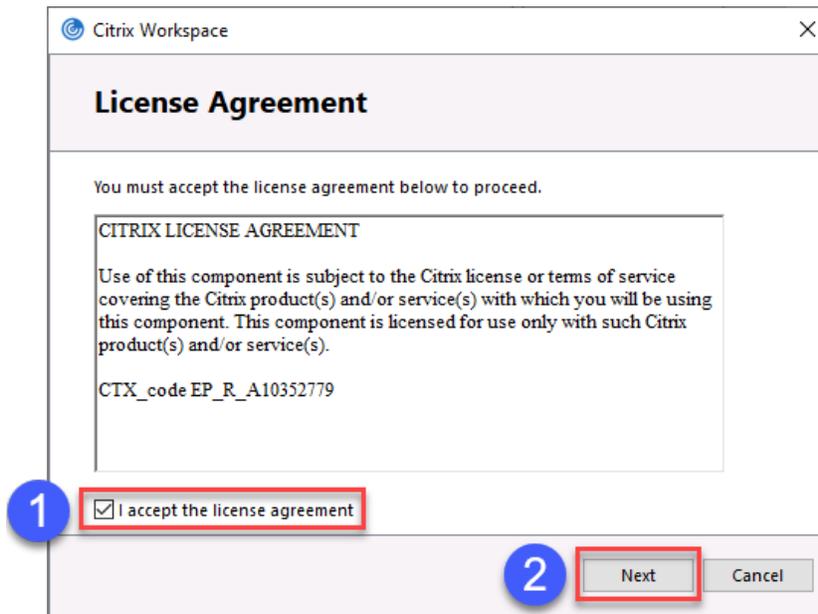
(U) Figure 18 Download Folder

(U) From the Citrix Workspace Setup Wizard, select **“Start”**.



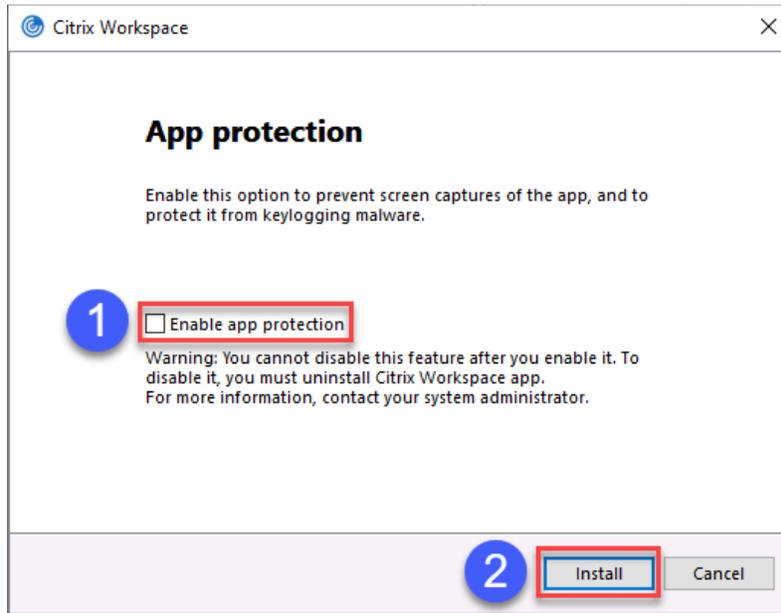
(U) Figure 19 Citrix Workspace Setup Wizard

(U) Select to accept the license agreement and select **“Next”**.



(U) Figure 20 License Agreement

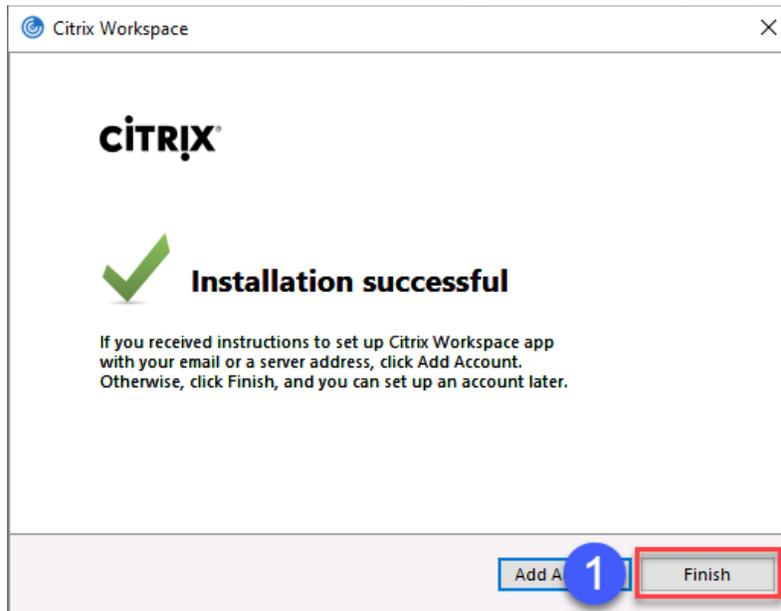
(U) Select to accept the “*Enable app protection*” and select “**Install**”.



(U) Figure 21 App Protection

(U) Once the Installation has completed successfully, select “**Finish**”.

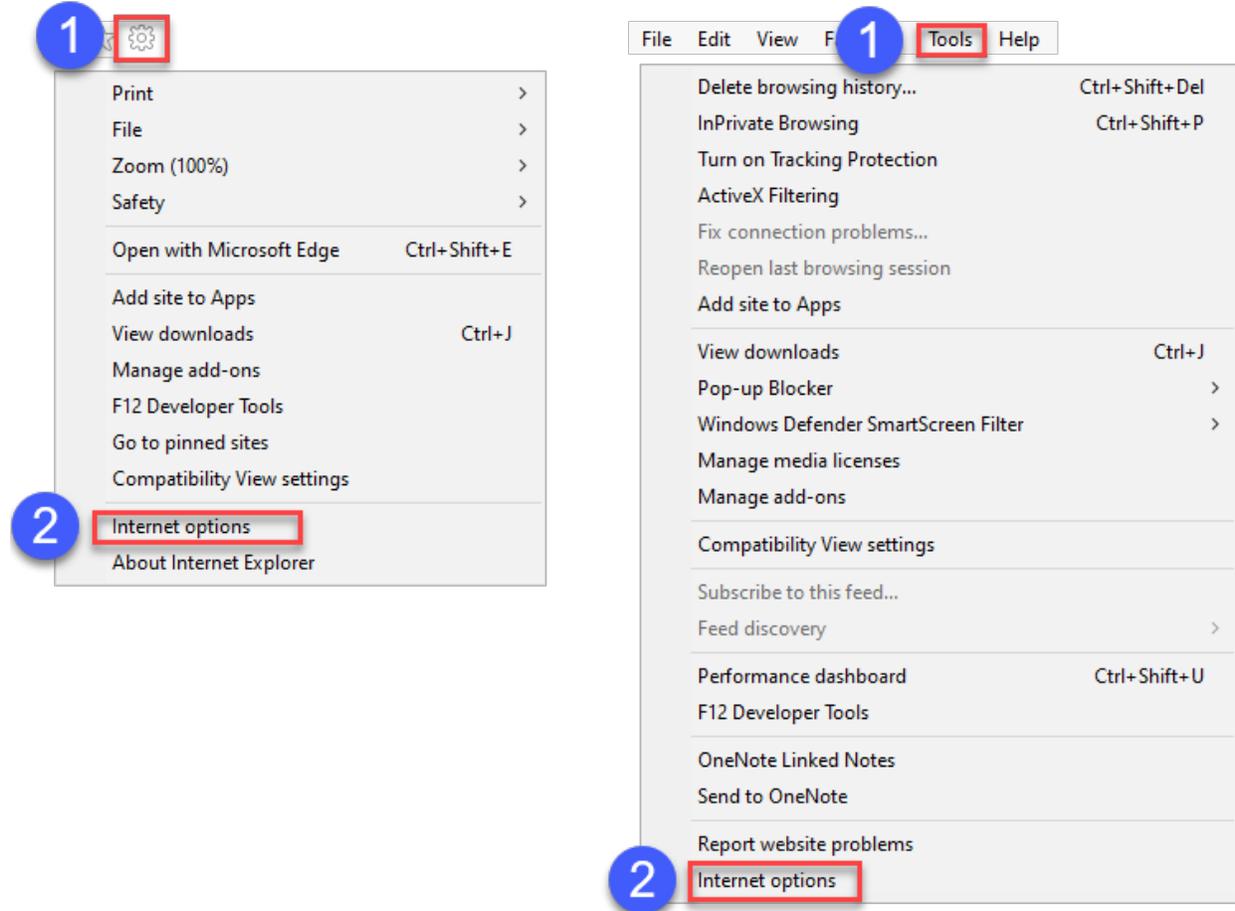
(U) NOTE: No Account needs to be added for Remote Access.



(U) Figure 22 Installation Successful

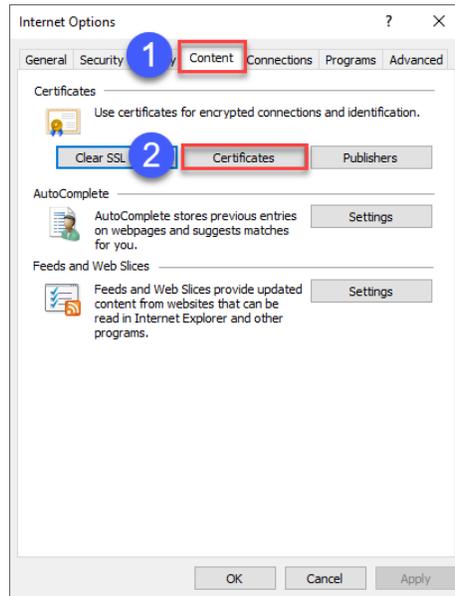
(U) Microsoft Internet Explorer – Verification of DoD Certificate installation

(U) From the Internet Explorer, navigate to “**Internet Options**” by either selecting the “**Gear**” in the upper right corner or from the “**Tools**” menu.



(U) Figure 23 Internet Options

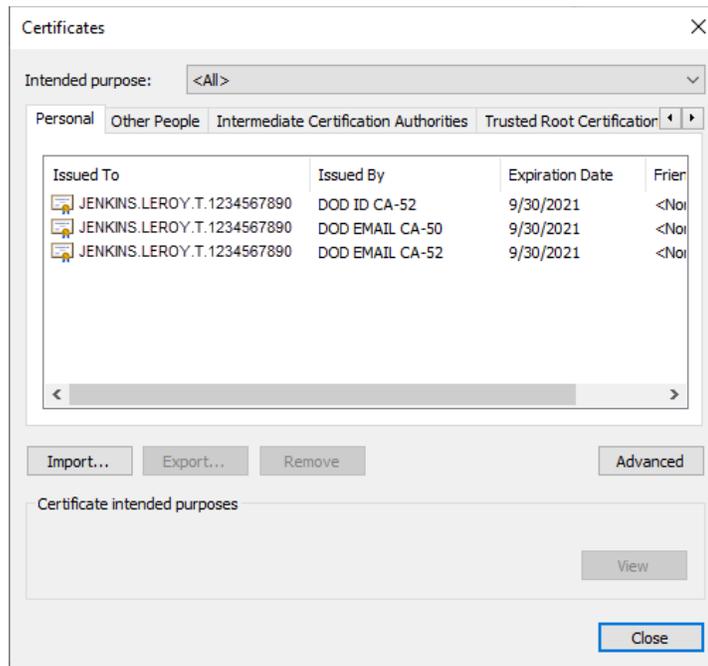
(U) Within the Internet Options menu, select the “**Content**” tab and then select the “**Certificates**” button.



(U) Figure 24 Certificates Button

(U) From the Certificates screen, verify the following:

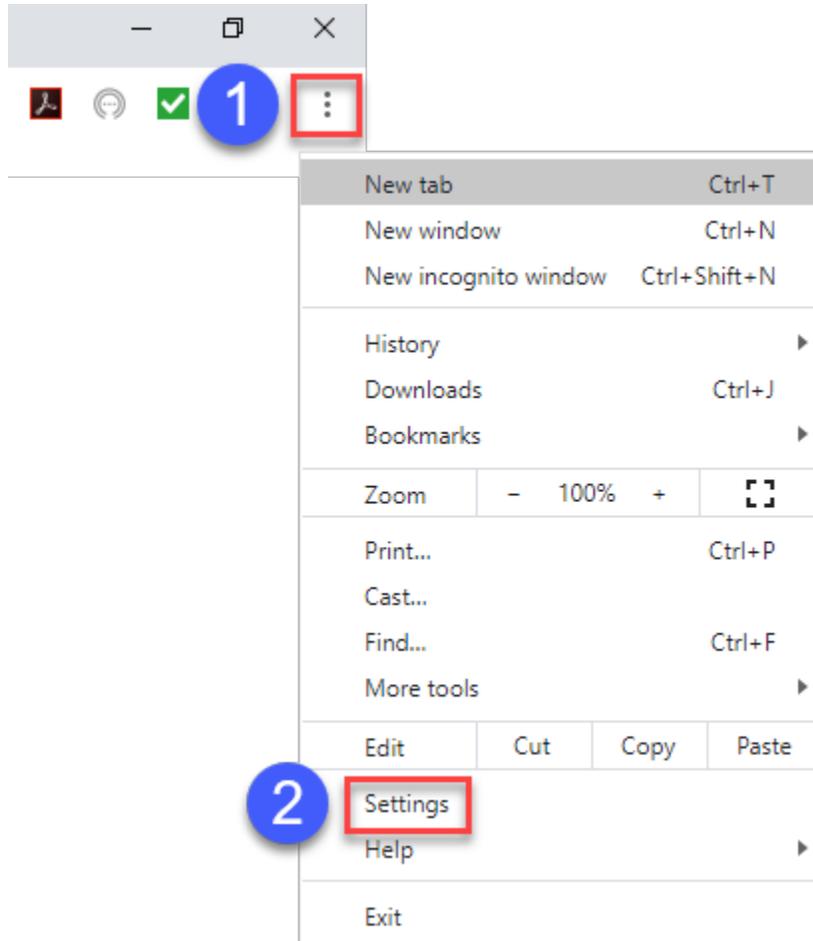
- (U) No **Red “X”** in front of any lines.
- (U) At least one DoD E-mail and ID certificate.
- (U) No certificate is expired.



(U) Figure 25 Certificates

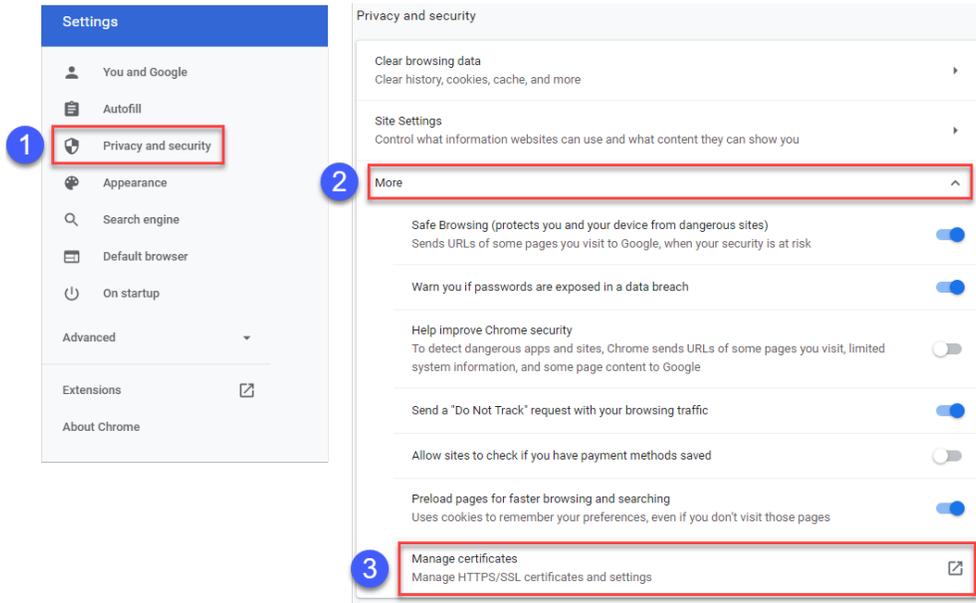
(U) Google Chrome – Verification of DoD Certificate installation

(U) From the Chrome browser, navigate to “**Privacy and Security**” by selecting the three dots in the upper right corner of the browser and then select “**Settings**”.



(U) Figure 26 Settings

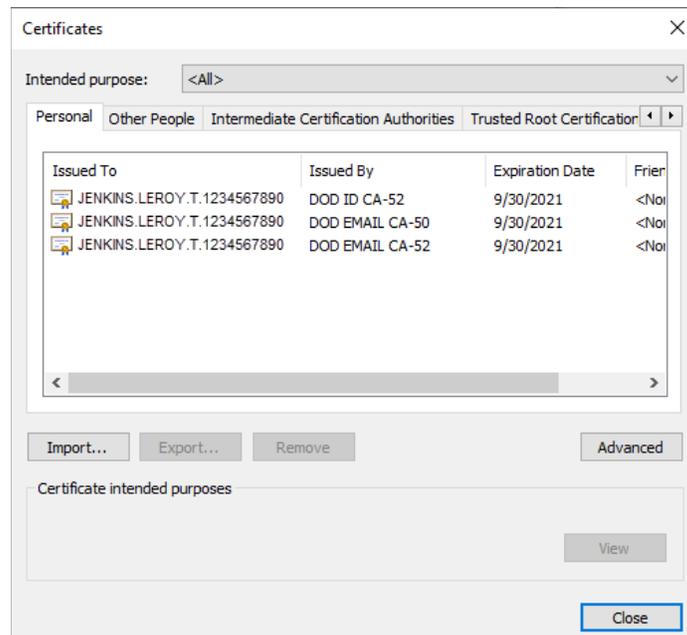
(U) Within the **Settings** menu, select **“Privacy and security”** on the left side. **Privacy and security** menu select **“More”** and then select **“Manage certificates”**.



(U) Figure 27 Manage Certificates

(U) From the Certificates screen, verify the following:

- (U) No **Red “X”** in front of any lines.
- (U) At least one DoD E-mail and ID certificate.
- (U) No certificate is expired.



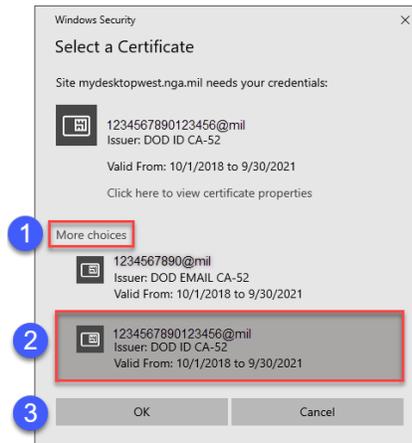
(U) Figure 28 Certificates

(U) Chapter Three – Windows Remote Access

(U) Recently updated Common Access Card (CAC) Users (16 Digit PIV Users)

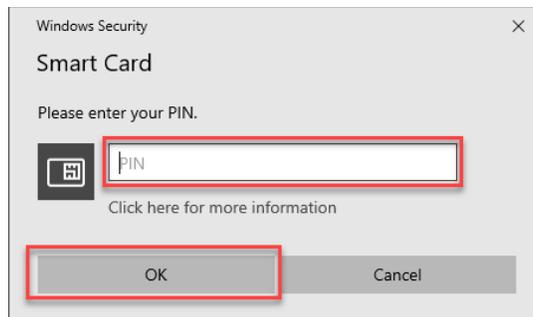
(U) Windows - Microsoft Internet Explorer

- (U) Insert your Common Access Card (CAC) into the reader and navigate to:
 - (U) West Users: <https://mydesktopwest.nga.mil>
 - (U) East Users: <https://mydesktop.nga.mil>
- (U) Select the **“More Choices”**, then click on the 16-digit PIV Auth Certificate before clicking **“OK”** to login.



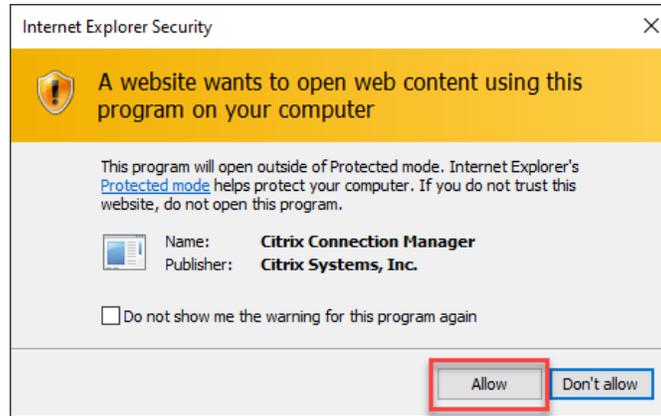
(U) Figure 29 Select a Certificate

- (U) Enter your PIN and click **“OK”**.



(U) Figure 30 Enter PIN

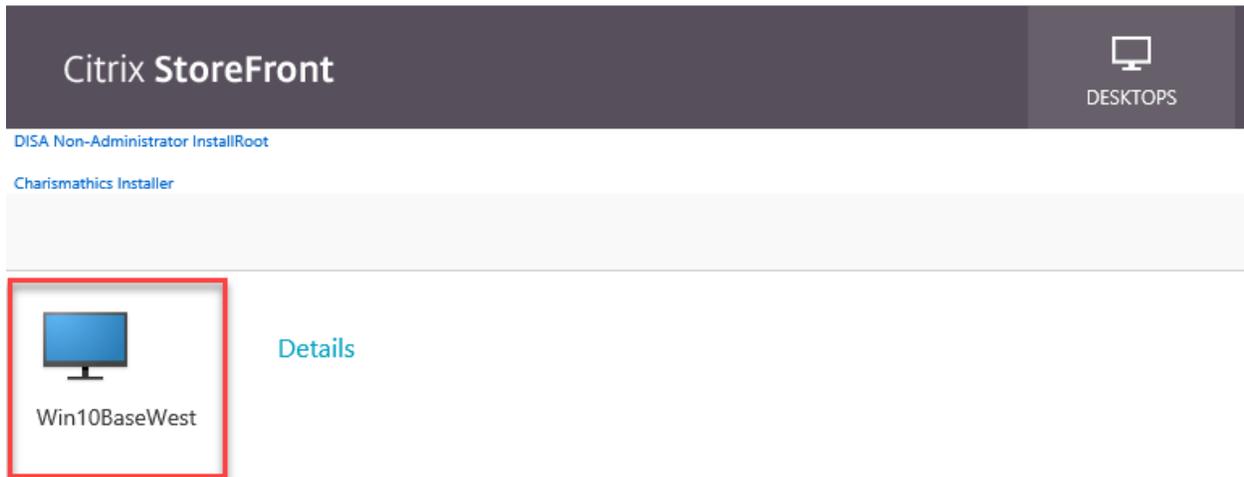
(U) NOTE: You may be prompted to enter your PIN multiple times. After the fifth prompt, select cancel on the prompt before entering it in again.



(U) Figure 31 Internet Explorer Security Warning

(U) NOTE: Internet Explorer Security may pop-up with warnings that “A website wants to open web content using this program on your computer”. If this message appears select “Allow”

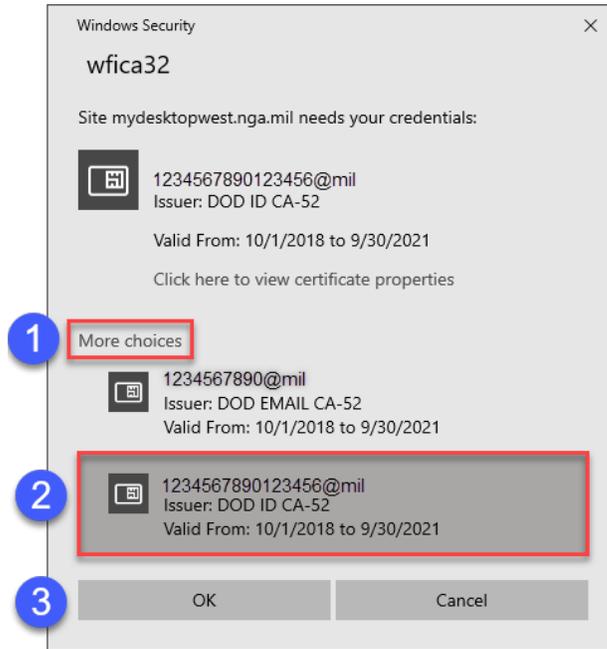
- (U) Next, select the Desktop icon to launch the Citrix session.



(U) Figure 32 Win10 Base

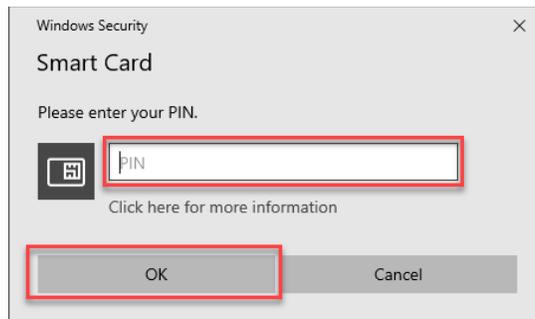
(U) NOTE: After clicking on the Icon, a file may appear at the bottom of your browser that will need to be selected to open the Remote Access session.

- (U) Another Windows Security prompt will appear, select the “**More Choices**”, then click on the 16-digit PIV Auth Certificate before clicking “**OK**” to login



(U) Figure 33 Select 16-Digit PIV Auth Cert

- (U) Enter your PIN and click “**OK**”.



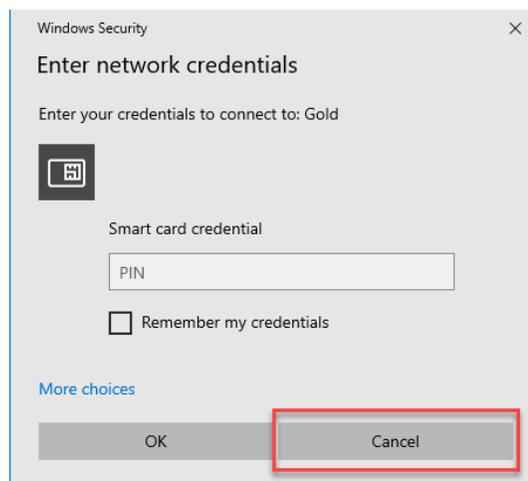
(U) Figure 34 Enter PIN

- (U) From the Remote Access session SBU login screen, select “*Sign-in options*” and choose the CAC icon that displays the 16-digit PIV Auth Certificate prior to entering your CAC pin.



(U) Figure 35 SBU Desktop Login

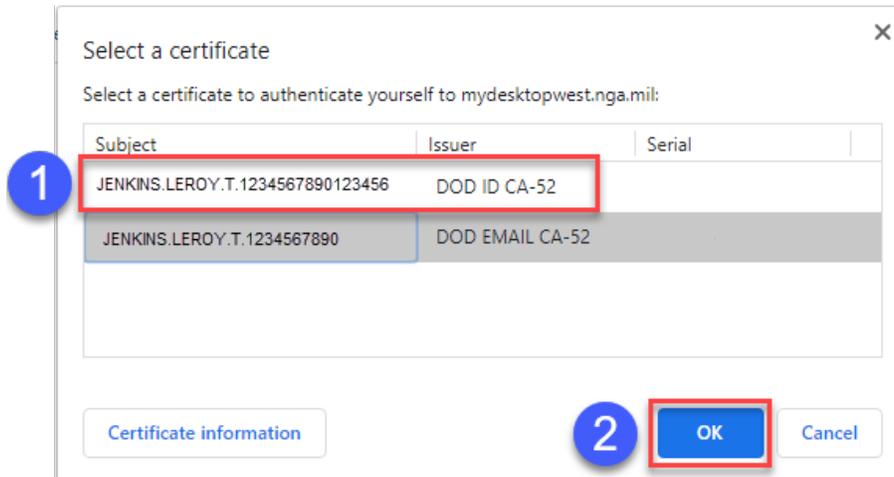
- (U) Once logged in you may be prompted to “**Enter network credentials**”, this prompt can be **Canceled**.



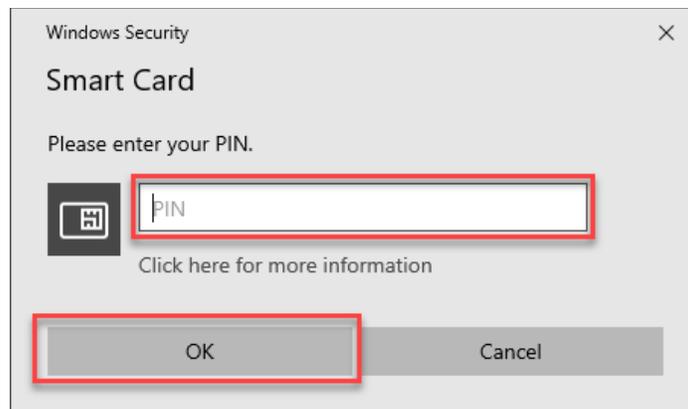
(U) Figure 36 Enter Network Credentials

(U) Windows - Google Chrome

- (U) Insert your Common Access Card (CAC) into the reader and navigate to:
 - (U) West Users: <https://mydesktopwest.nga.mil>
 - (U) East Users: <https://mydesktop.nga.mil>
- (U) Select the **“DOD ID 16-digit PIV Auth Certificate”** to login.

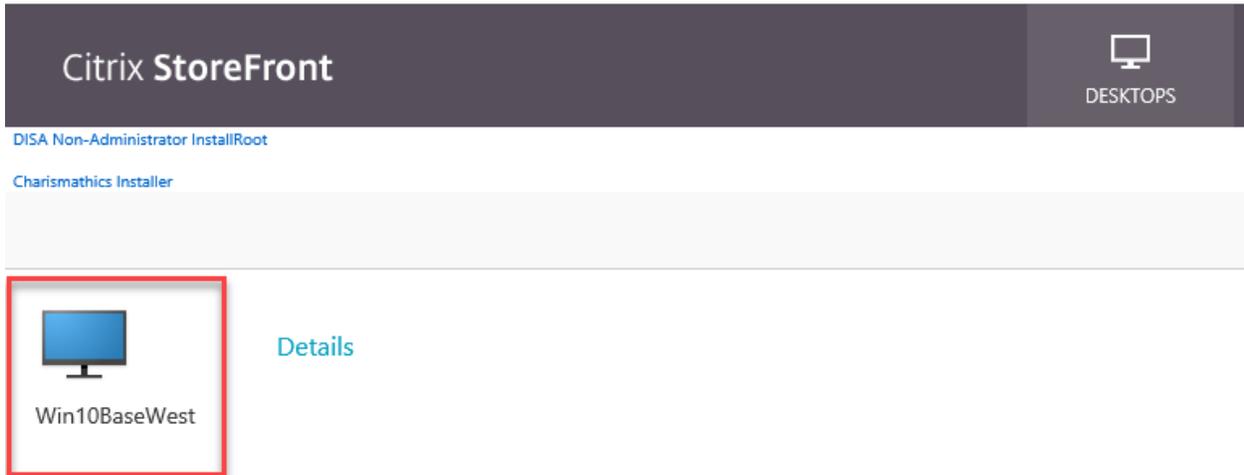
*(U) Figure 37 DOD ID 16-digit PIV Auth Certificate*

- (U) Enter your PIN and click **“OK”**.

*(U) Figure 38 Enter PIN*

(U) NOTE: You may be prompted to enter your PIN multiple times. After the fifth prompt, select cancel on the prompt before entering it in again.

- (U) Next, select the Desktop icon to launch the Citrix session.



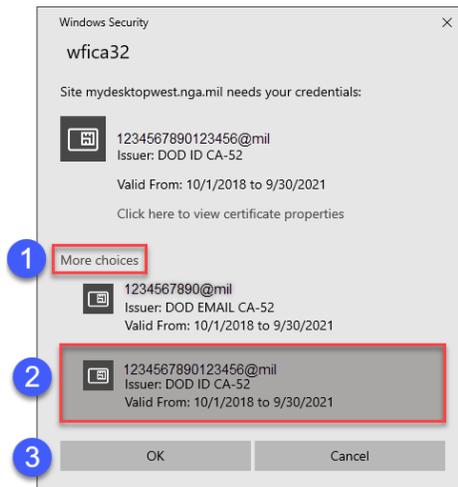
(U) Figure 39 Win10 Base

(U) NOTE: After clicking on the Icon, a file may appear at the bottom of your browser that will need to be selected to open the Remote Access session.



(U) Figure 40 Citrix Session file

- (U) Another Windows Security prompt will appear, select the **“More Choices”**, then click on the 16-digit PIV Auth Certificate before clicking **“OK”** to login



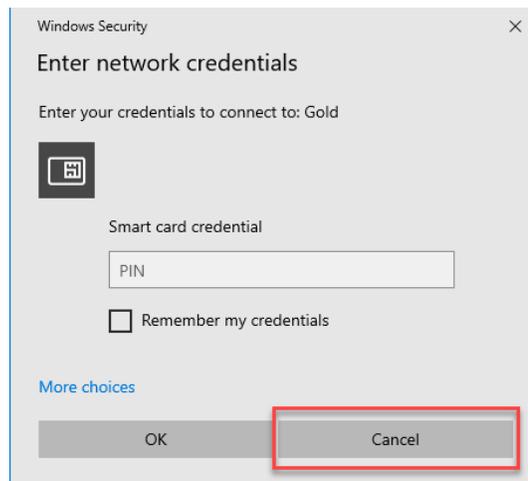
(U) Figure 41 Wfica prompt

- (U) From the Remote Access session SBU login screen, select “*Sign-in options*” and choose the CAC icon that displays the 16-digit PIV Auth Certificate prior to entering your CAC pin.



(U) Figure 42 SBU Desktop Login

- (U) Once logged in you may be prompted to “**Enter network credentials**”, this prompt can be **Canceled**.

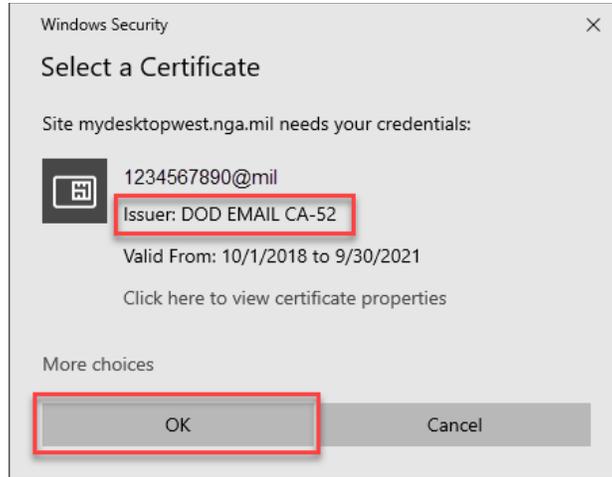


(U) Figure 43 Enter Network Credentials

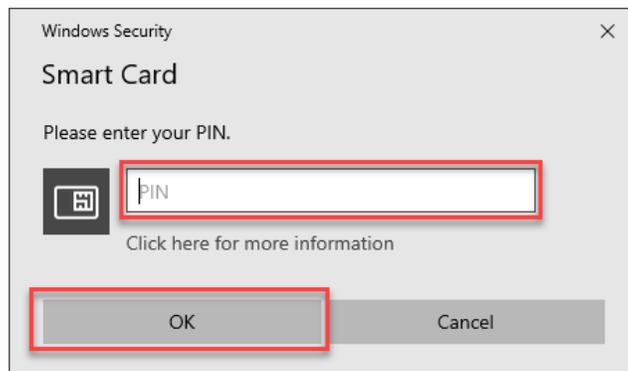
(U) Existing NGA Common Access Card (CAC) Users

(U) Windows - Microsoft Internet Explorer

- (U) Insert your Common Access Card (CAC) into the reader and navigate to:
 - (U) West Users: <https://mydesktopwest.nga.mil>
 - (U) East Users: <https://mydesktop.nga.mil>
- (U) Select the “**Email**” Certificate to login.



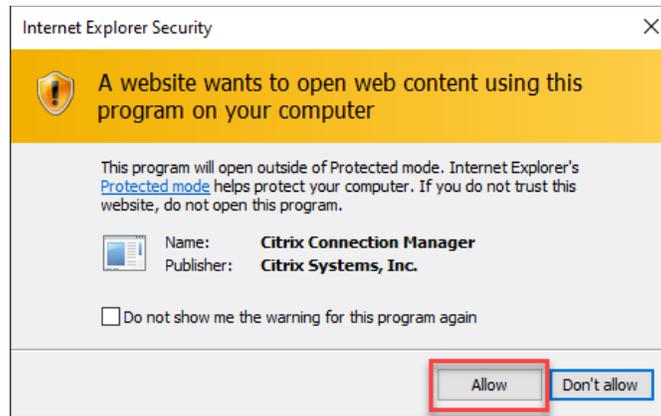
(U) Figure 45 DoD Email Certificate



(U) Figure 44 Pin Number prompt

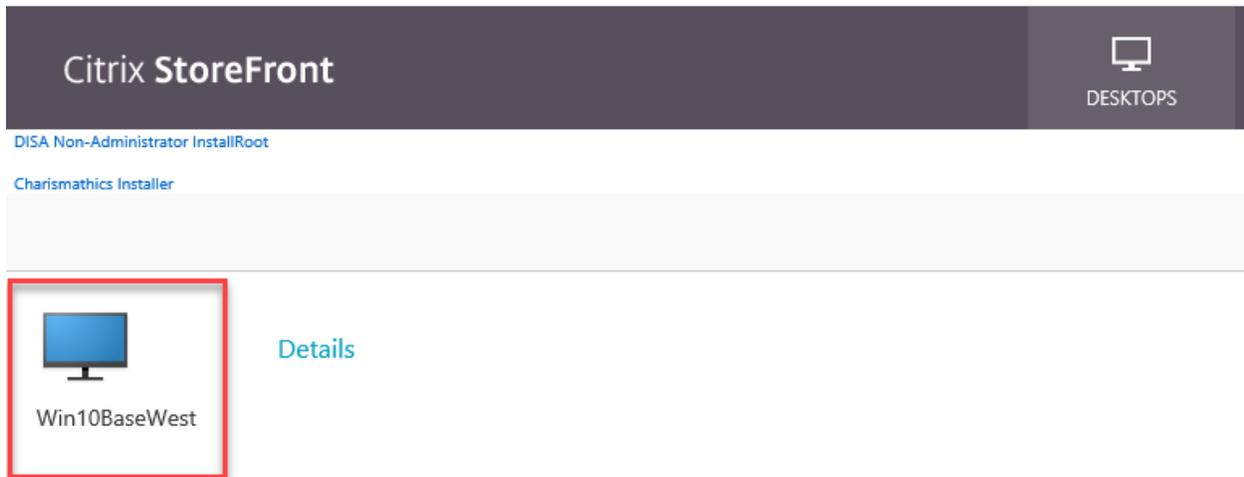
(U) NOTE: You may be prompted to enter your PIN multiple times. After the fifth prompt, select cancel on the prompt before entering it in again.

(U) NOTE: Internet Explorer Security may pop-up with warnings that “A website wants to open web content using this program on your computer”. If this message appears select “Allow”



(U) Figure 46 Internet Explorer Security Warning

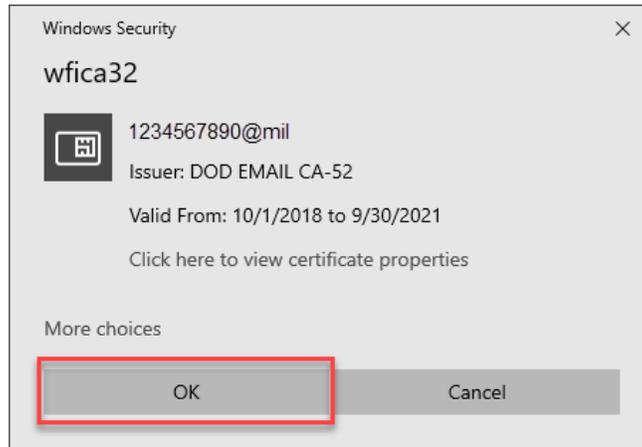
(U) Next, select the Desktop icon to launch the Citrix session.



(U) Figure 47 Win10Base

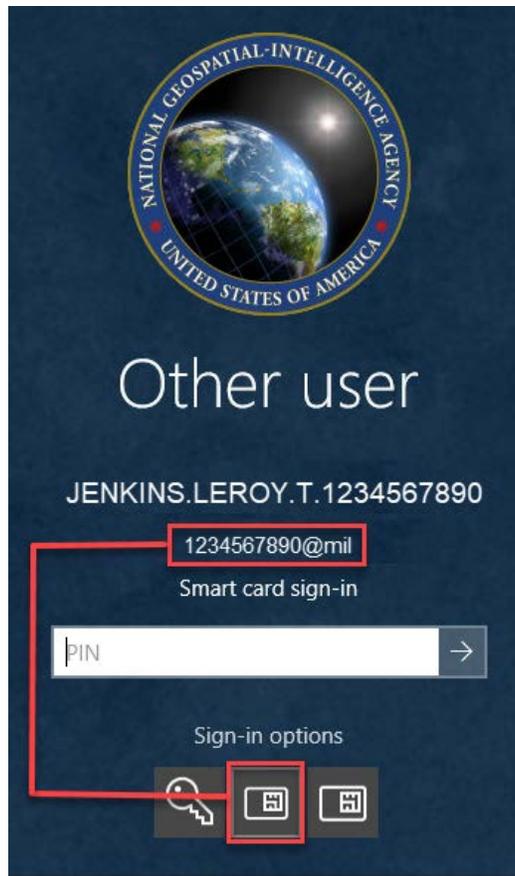
(U) NOTE: After clicking on the Icon, a file may appear at the bottom of your browser that will need to be selected to open the Remote Access session.

(U) Another Windows Security prompt will appear, select the DoD Email certificate to continue.



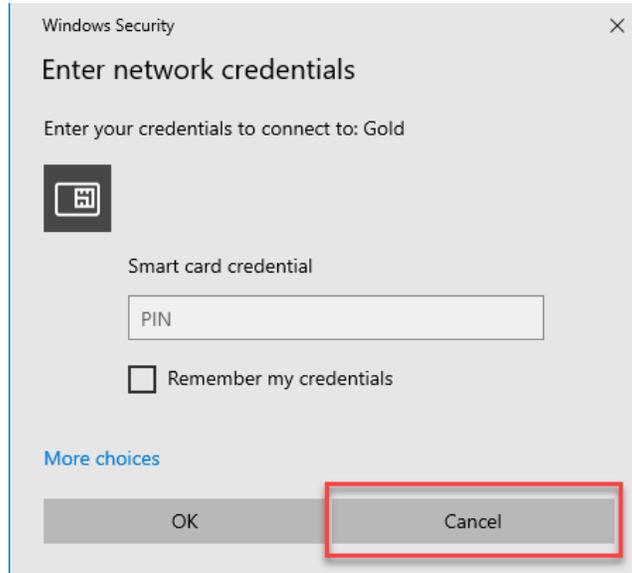
(U) Figure 48 wfica32 prompt

(U) From the Remote Access session SBU login screen, select “*Sign-in options*” and choose the CAC icon that displays the 10-digit PIV certificate prior to entering your CAC pin.



(U) Figure 49 SBU Login Screen

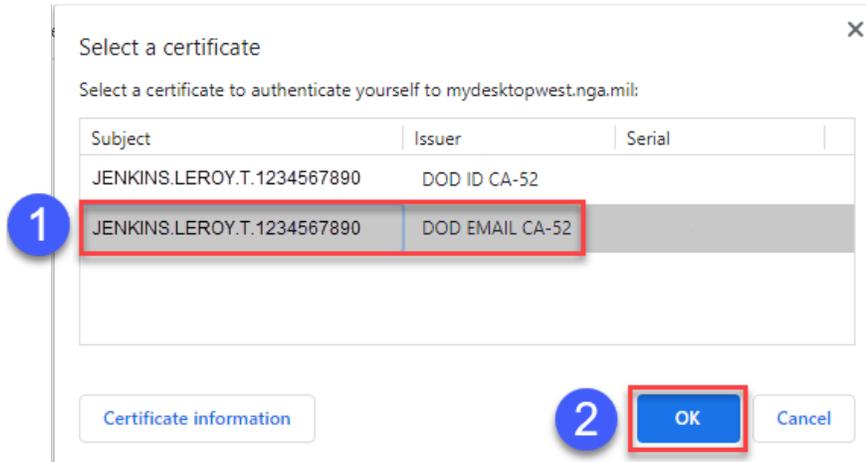
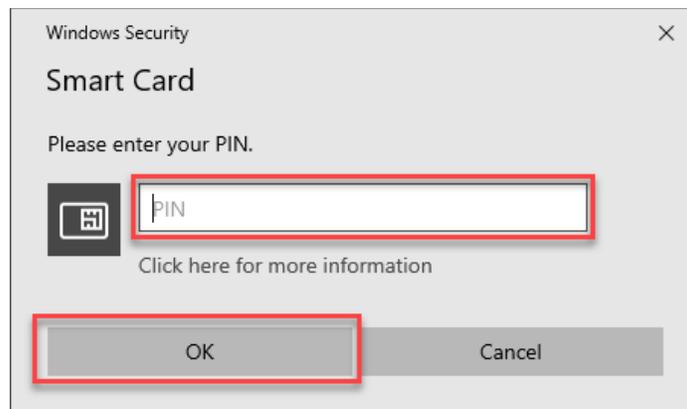
(U) Once logged in you may be prompted to “Enter network credentials”, this prompt can be canceled.



(U) Figure 50 Enter Network Credentials

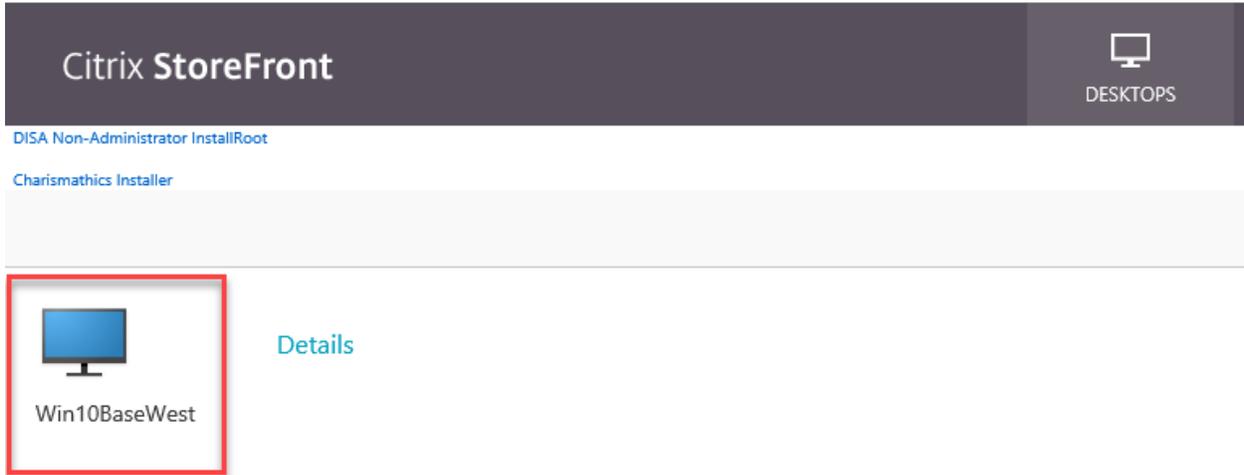
(U) Windows - Google Chrome

- (U) Insert your Common Access Card (CAC) into the reader and navigate to:
 - (U) West Users: <https://mydesktopwest.nga.mil>
 - (U) East Users: <https://mydesktop.nga.mil>
- (U) Select the **“Email”** Certificate to login.

*(U) Figure 52 Email Certificate**(U) Figure 51 PIN Prompt*

(U) NOTE: You may be prompted to enter your PIN multiple times. After the fifth prompt, select cancel on the prompt before entering it in again.

(U) Next, select the Desktop icon to launch the Citrix session.



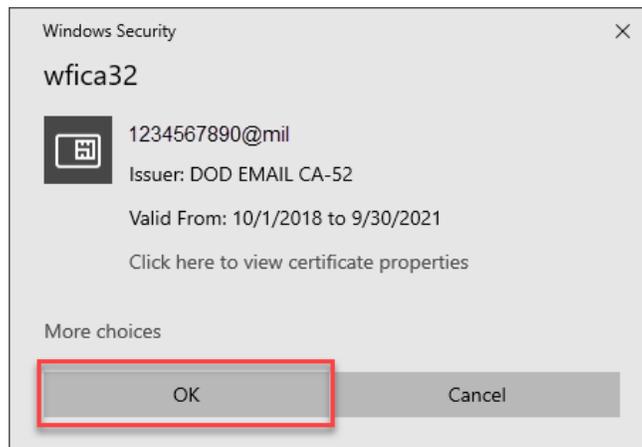
(U) Figure 53 Win10Base

(U) NOTE: After clicking on the Icon, a file may appear at the bottom of your browser that will need to be selected to open the Remote Access session.



(U) Figure 54 Remote Session File download

(U) Another Windows Security prompt will appear, select the DoD Email certificate to continue.



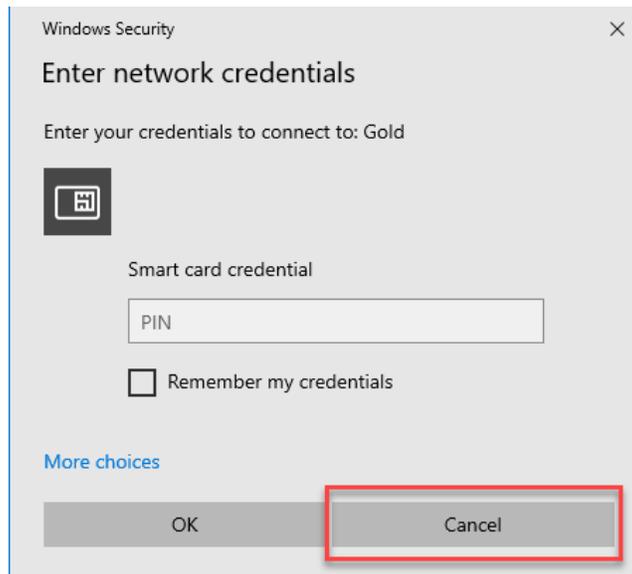
(U) Figure 55 wfica32 prompt

(U) From the Remote Access session SBU login screen, select “*Sign-in options*” and choose the CAC icon that displays the 10-digit PIV certificate prior to entering your CAC pin.



(U) Figure 56 SBU Login Screen

(U) Once logged in you may be prompted to “Enter network credentials”, this prompt can be canceled.



(U) Figure 57 Enter Network Credentials

(U) Remote Access – Unlocking the Screen

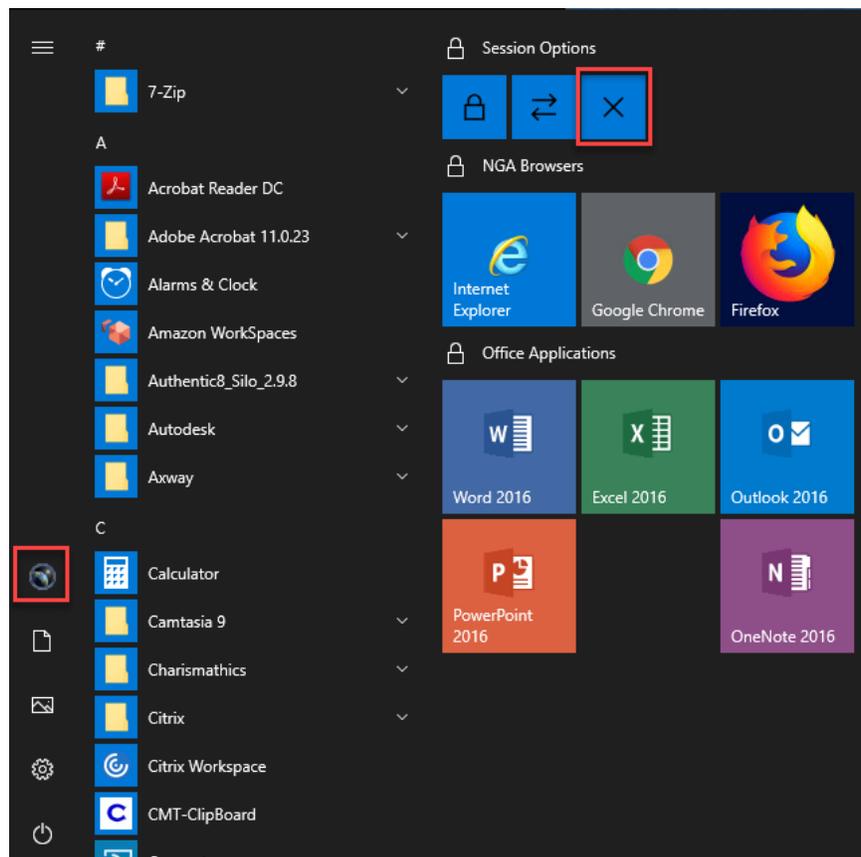
(U) To unlock your Remote Access session, select the menu at the top of the Citrix screen and select the “Ctrl+Alt+Del” icon. Now enter your CAC pin.



(U) Figure 58 Citrix Menu bar

(U) Remote Access – Sign out procedure

(U) To ensure that you have fewer issues signing in the next time select one of the two options from the Start menu to “Sign out” when finished with the Remote Session.

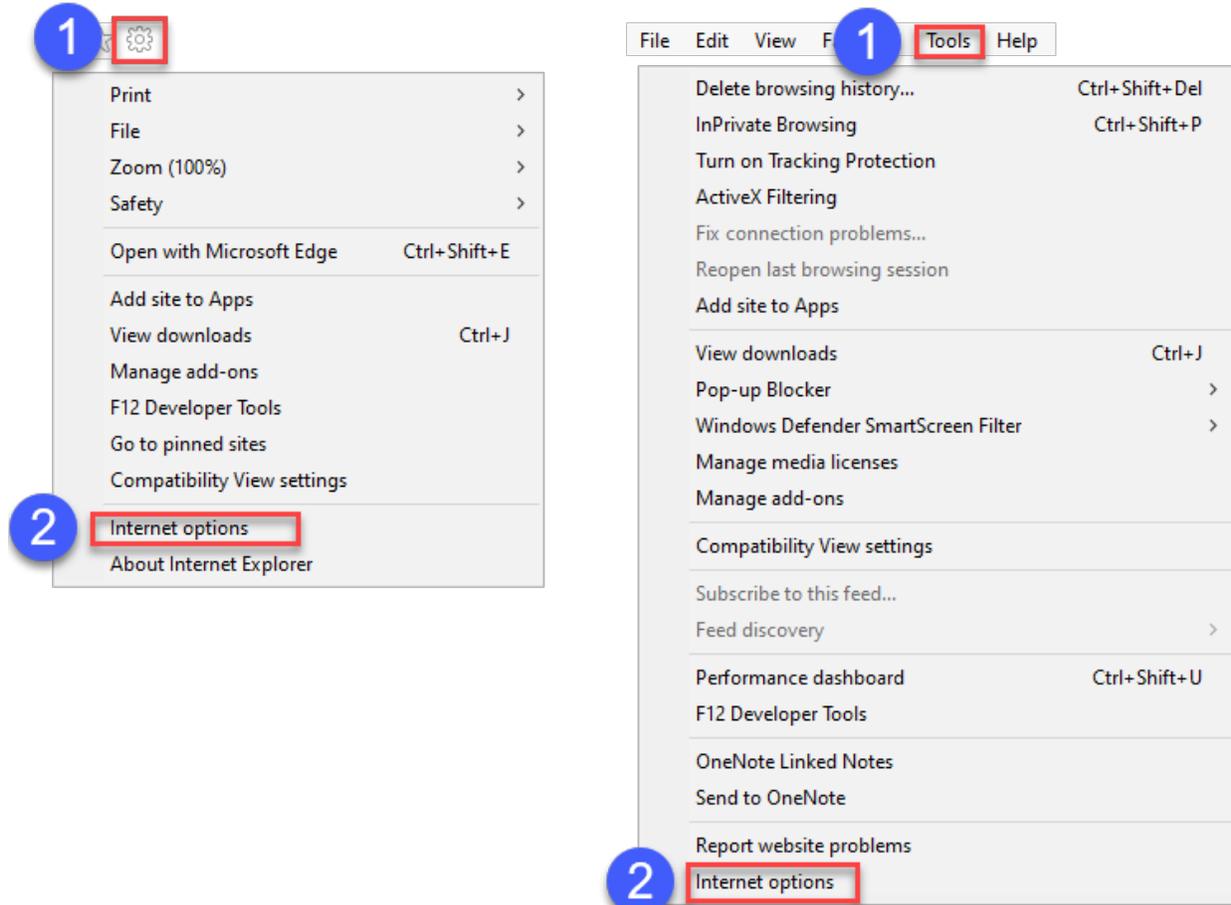


(U) Figure 59 Sign out of the session

(U) Chapter Four – Remote Access Troubleshooting

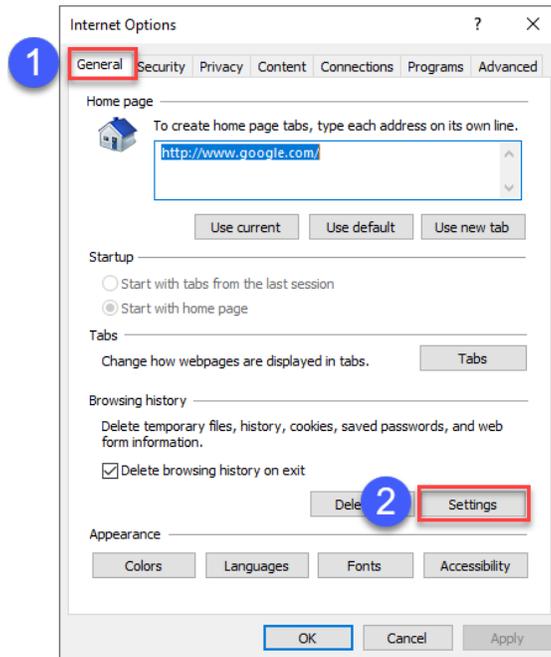
(U) Clear Browser Cache – Microsoft Internet Explorer

(U) From the Internet Explorer, navigate to “**Internet Options**” by either selecting the “**Gear**” in the upper right corner or from the “**Tools**” menu.



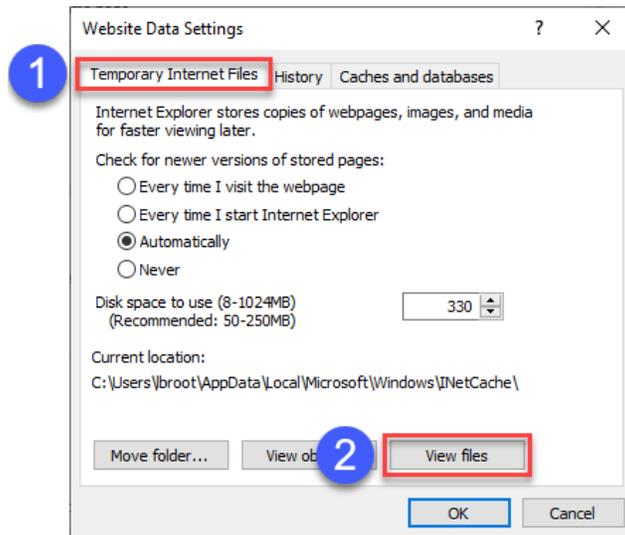
(U) Figure 60 Internet Options

(U) Within the Internet Options menu, select the “**General**” tab and then select the “**Settings**” button.



(U) Figure 61 General Tab

(U) From the *Website Data Settings* screen, select “**View files**” on the *Temporary Internet Files* tab.



(U) Figure 62 View Files

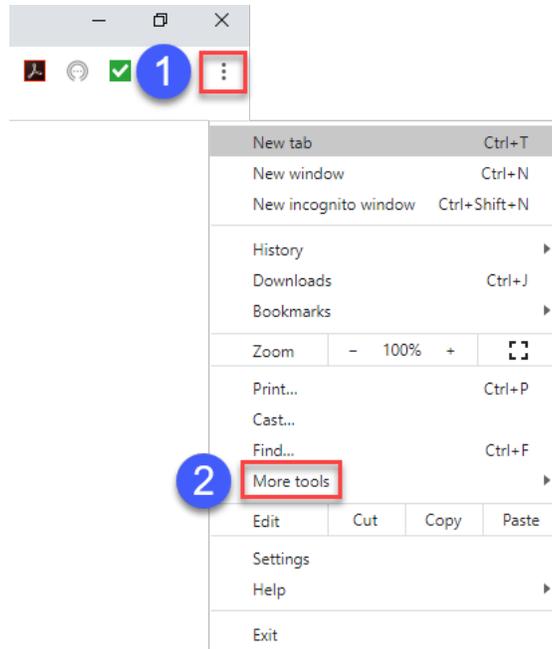
(U) Now from the folder, ***select all files and press delete.*** Now complete close the browser and reopen.



(U) Figure 63 Temporary Files

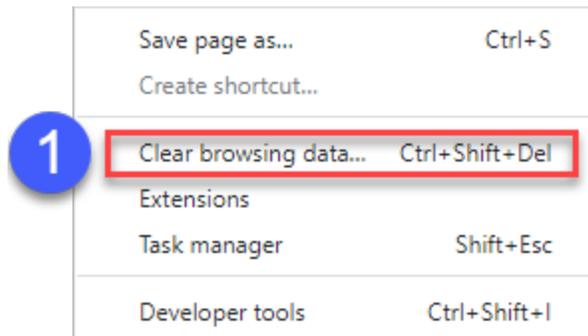
(U) Clear Browser Cache – Google Chrome

(U) From the Chrome browser, navigate to “**More tools**” by selecting the three dots in the upper right corner of the browser.



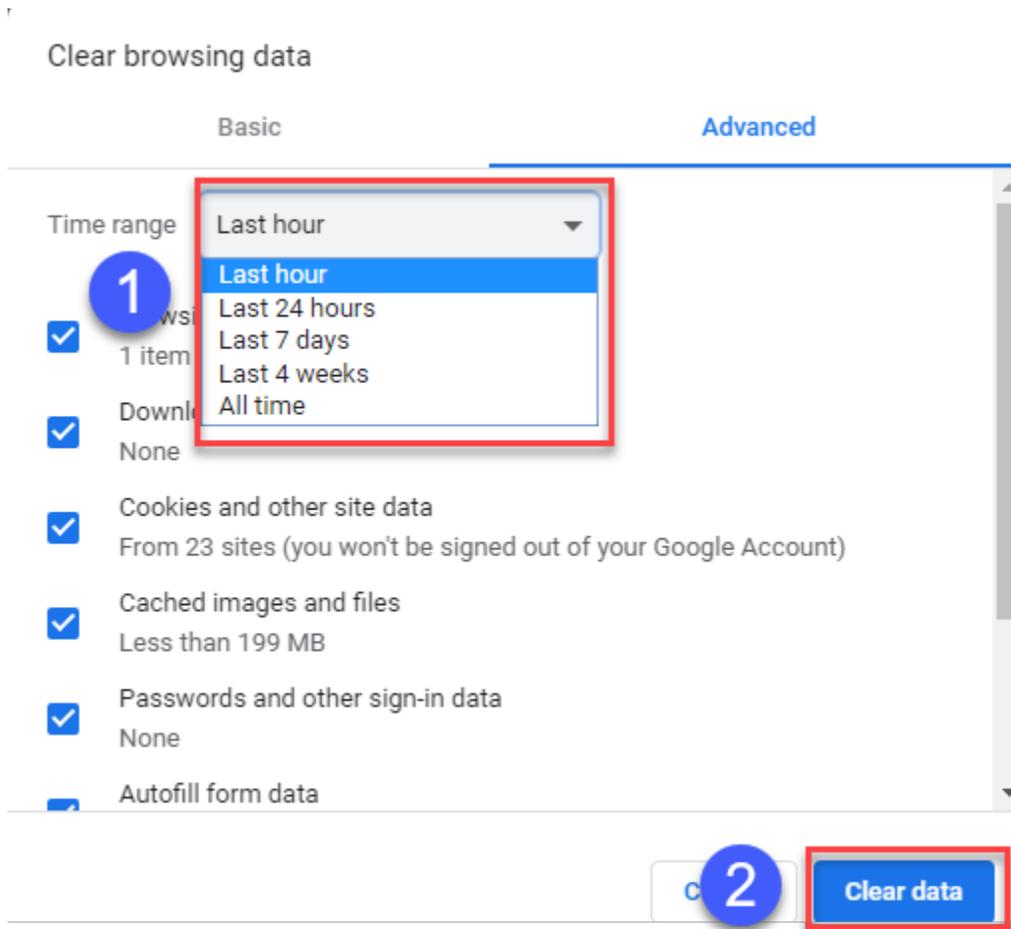
(U) Figure 64 More tools

(U) From the *More tools* sub-menu select “**Clear browsing data...**”



(U) Figure 65 Clear browsing data...

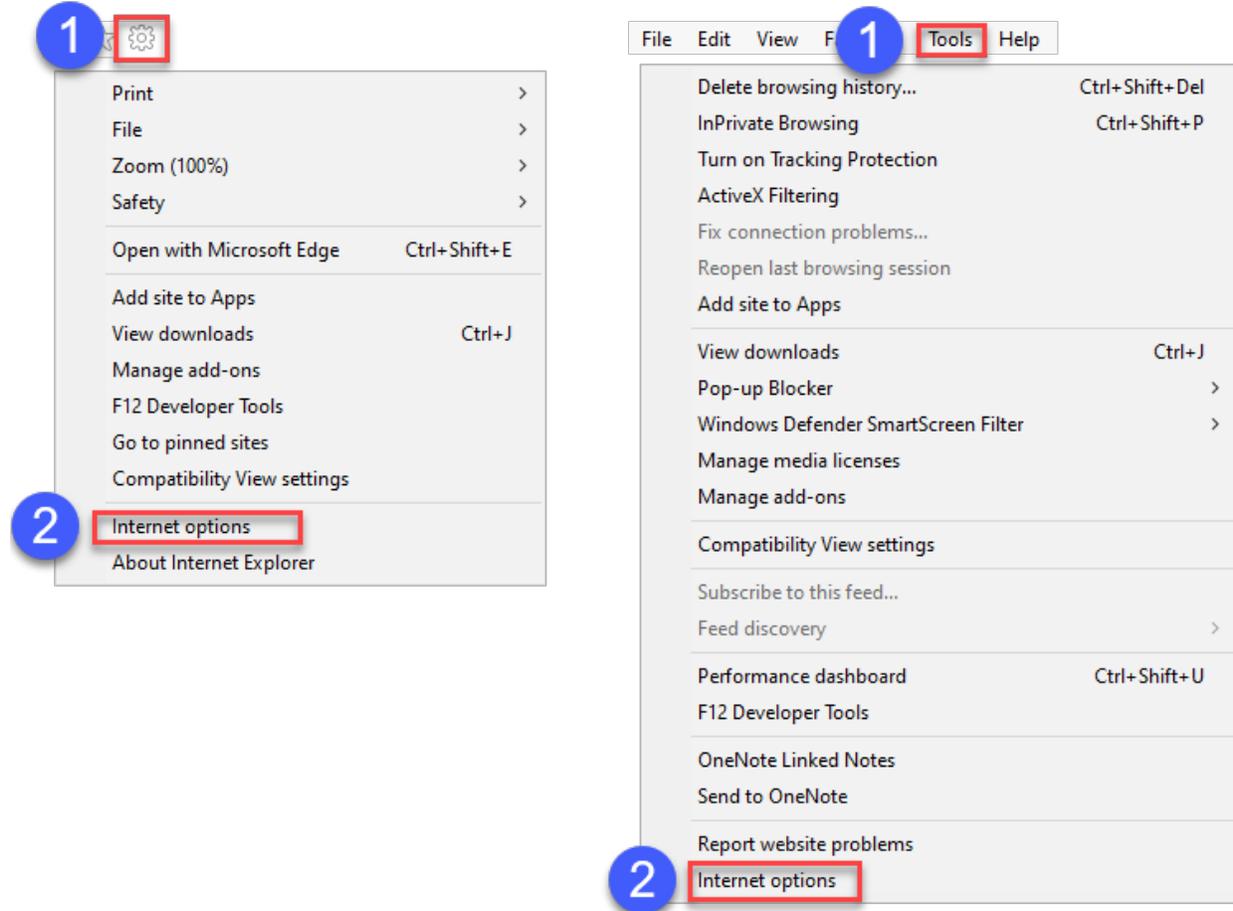
(U) We recommend that the *Time Range* is set to “**Last Hour**” prior to using any other selection to avoid losing personal user information.



(U) Figure 66 Selection of Last Hour

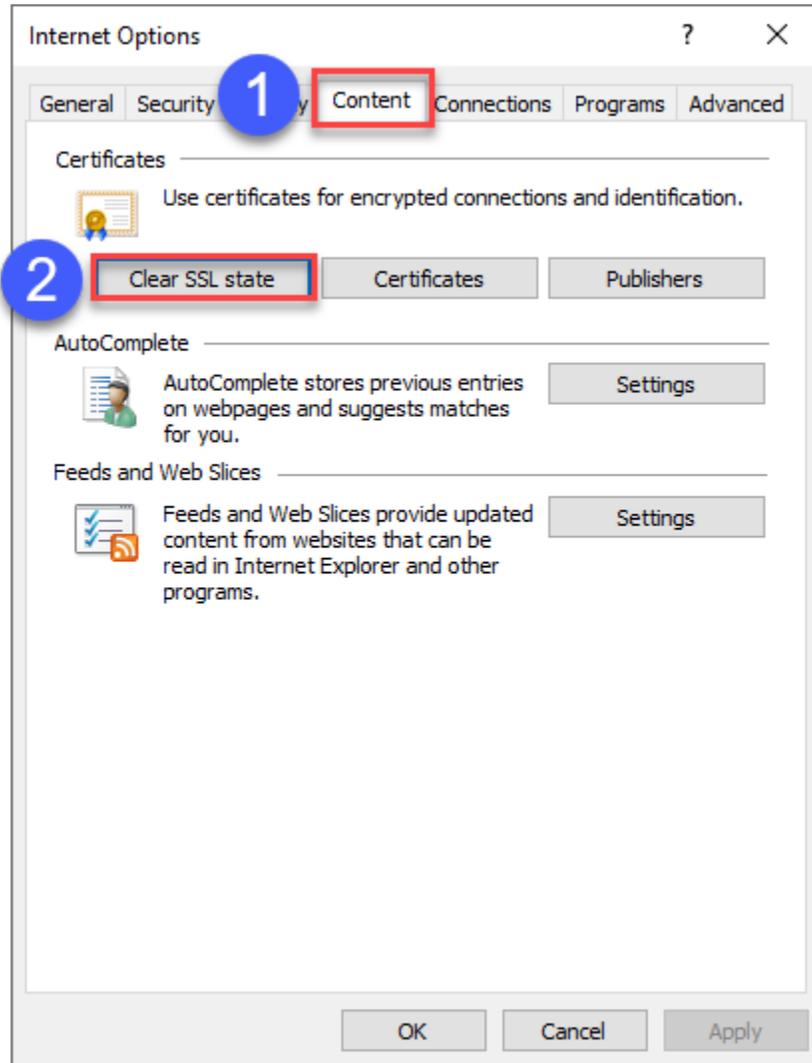
(U) Clear Browser SSL State – Microsoft Internet Explorer

(U) From the Internet Explorer, navigate to “**Internet Options**” by either selecting the “**Gear**” in the upper right corner or from the “**Tools**” menu.



(U) Figure 67 Internet Options

(U) Within the Internet Options menu, select the “**Content**” tab and then select the “**Clear SSL state**” button. Now select **OK**.



(U) Figure 68 Clear SSL state

(U) Chapter Five – Macintosh Required Applications

(U) Mac Middleware Software

(U) The Macintosh middleware software for your appropriate Operating System can be located at (<http://militarycac.com/cacenablers.htm>).

(U) NOTE: It is not necessary to install a third-party CAC enabler if you have upgraded to the Catalina (10.15x) OS. Instructions detailing how to utilize the built-in CAC enabler can be found here (<https://militarycac.com/macuninstall.htm>).

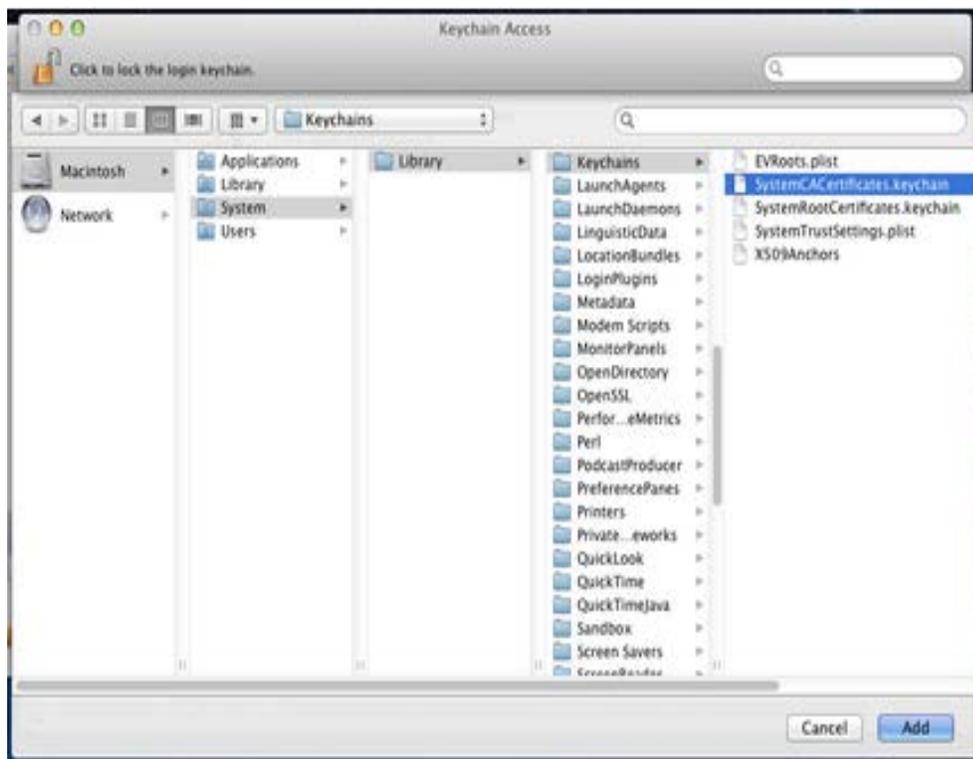
(U) If an error message “*.pkg can’t be opened because it is from an unidentified developer*”. Hold the control {CTRL} key when clicking the .pkg file. Then, select the option to “**Open**”.

- (U) Open OS X System Preferences > *Security & Privacy*.
- (U) On the "**General**" tab click the lock in the lower left corner to unlock the general preference pane.
- (U) Under "**Allow applications downloaded from:**" select the "**Anywhere**" radio button.

(U) DoD Intermediate Certificates

(U) The DoD intermediate certificates are not visible in the keychain by default. However, the certificates are preinstalled on the Macintosh OS X.

- (U) To load the intermediate certificates and make available follow these steps:
- (U) Open Applications, then open the Utilities folder and double-click Keychain Access.
- (U) Select File > Add Keychain.
- (U) Click the Keychains drop down and select the hard drive icon to go to the top level of the disk.
- (U) Navigate to System > Library > Keychains.
- (U) Select “**SystemCACertificate.keychain**”, then click Add.

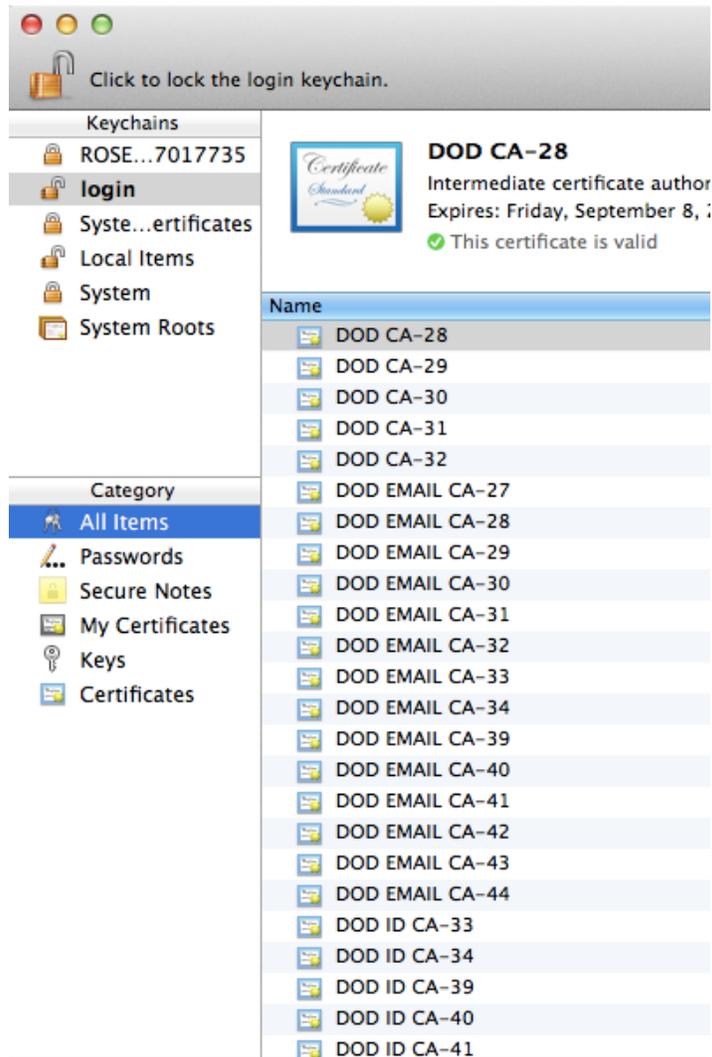


(U) Figure 54 Keychain Access

(U) Download and install the Root DoD Certificates onto your Macintosh. Ensure that each individual certificate is installed separately.

- (U) <https://militarycac.com/maccerts/AllCerts.p7b>
- (U) <https://militarycac.com/maccerts/RootCert2.cer>
- (U) <https://militarycac.com/maccerts/RootCert3.cer>
- (U) <https://militarycac.com/maccerts/RootCert4.cer>
- (U) <https://militarycac.com/maccerts/RootCert5.cer>

(U) Double click the individual certificates you need in the folder to have them installed into the login section of keychain, as seen below:



(U) Figure 55 Keychain

(U) Citrix Workspace

(U) From the Citrix website (<https://www.citrix.com/downloads/workspace-app/mac/workspace-app-for-mac-latest.html>), select **“Download Citrix Workspace app for Mac”**.

(U) Once the Application has downloaded, install the application by following the on screen prompts. No Account is needed for NGA Remote Access.

(U) Chapter Six – Macintosh Remote Access

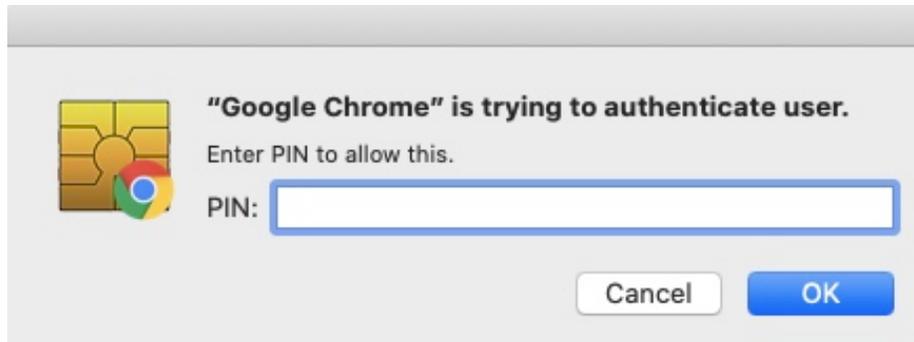
(U) Macintosh – Google Chrome

- (U) Insert your Common Access Card (CAC) into the reader and navigate to:
 - (U) West Users: <https://mydesktopwest.nga.mil>
 - (U) East Users: <https://mydesktop.nga.mil>

(U) Select the **“Email”** Certificate to login.



(U) Figure 56 select a certificate

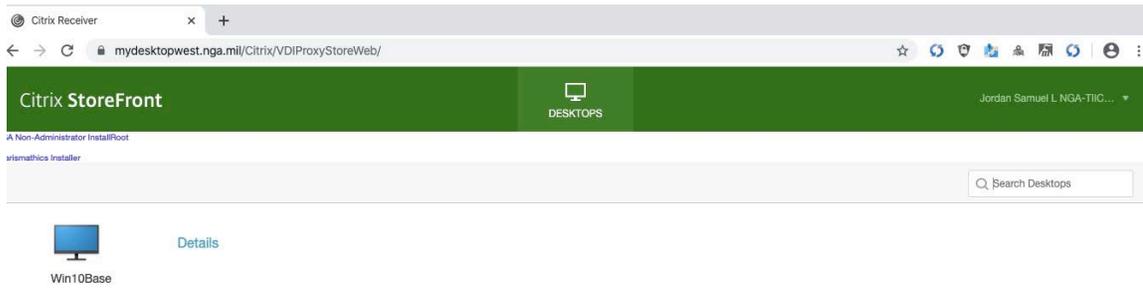


(U) Figure 57 Enter PIN

(U) *NOTE: You may be prompted to enter your PIN multiple times. After the fifth prompt, select cancel on the prompt before entering it in again.*

(U) *NOTE: If you obtain any error messages in the browser, refresh the page in the browser until the error message is gone and you are logged into the website. In some cases, it may be necessary to **“Clear Browsing Data”**.*

(U) Next, select the Desktop icon to launch the Citrix session.



(U) Figure 58 Citrix StoreFront

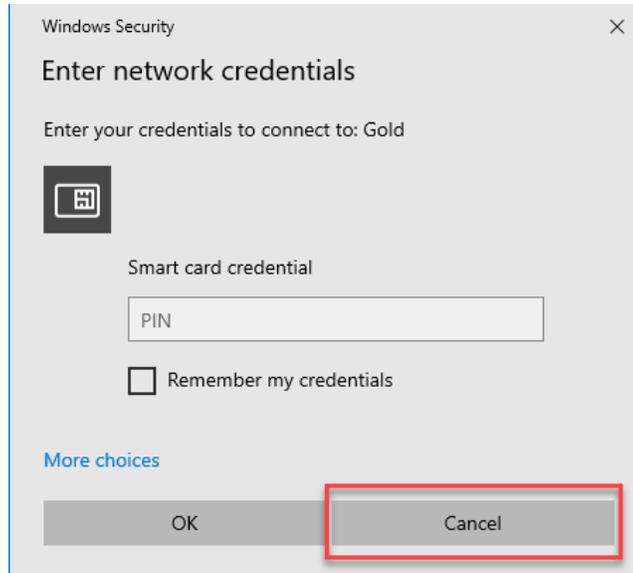
(U) NOTE: After clicking on the Icon, a file may appear at the bottom of your browser that will need to be selected to open the Remote Access session.

(U) From the Remote Access session SBU login screen, select “**Sign-in options**” and choose the CAC icon that displays the 10-digit PIV certificate prior to entering your CAC pin.



(U) Figure 59 Sign-in options

(U) Once logged in you may be prompted to **“Enter network credentials”**, this prompt can be canceled.



(U) Figure 60 Enter Network credentials

(U) Remote Access – Unlocking the Screen

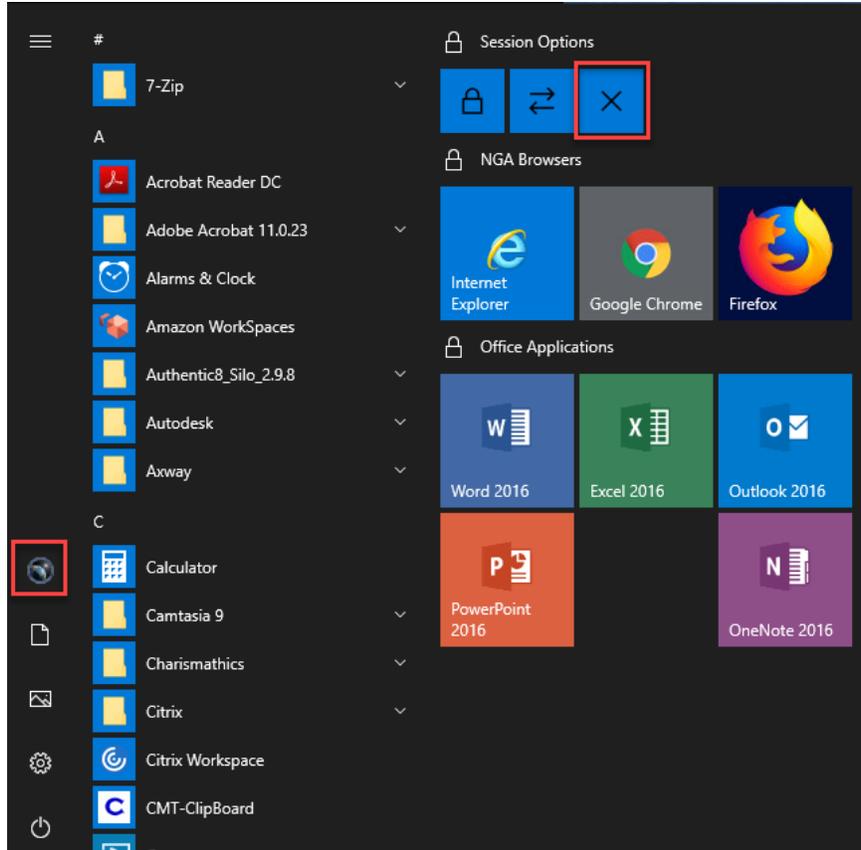
(U) To unlock your Remote Access session, select the menu at the top of the Citrix screen and select the **“Ctrl+Alt+Del”** icon. Now enter your CAC pin.



(U) Figure 61 Citrix Menu bar

(U) Remote Access – Sign out procedure

(U) To ensure that you have fewer issues signing in the next time select one of the two options from the Start menu to “Sign out” when finished with the Remote Session.



(U) Figure 62 Sign out of the session

(U)Appendix

(U) Appendix A – Agency Service Desk

Enterprise Service Center - ESC

NGA Users – (800) 455-0899

(U) Appendix B – Contact Us



Customer Outreach

ITEMS - User Facing Services

Visit us online

<https://www.intranet.nga.mil/sites/training>

Email us

NGAITEMSUFSCustomerOutreachTeam@nga.mil