Walter Reed
National Military
Medical Center

General Internal Medicine Service
Walter Reed National Military Medical Center
8901 Wisconsin Avenue
Bethesda, MD 20889
301-295-0196

27 Mar 2020

TO: GIMS Employees

FROM: Lt Col Brian Neubauer
Chief, General Internal Medicine Service

SUBJECT: Remote Access to IT Systems

Employees may access clinical platforms and Outlook remotely using either a government furnished laptop/VPN connection or a personal device equipped with a USB CAC reader. CAC readers may be supplied by your institution or procured on your own from a commercial source (e.g. Amazon). The attached instruction addresses how to set up a CAC reader on your personal device.

Respectfully,

BRIAN E. NEUBAUER, MD, MHPE, FACP
Lt Col, USAF, MC
Chief, General Internal Medicine Service

Read first!

You will need to maximize your network performance at home in order to keep AVHE stable. Recommendations:

- Disconnect gaming devices (e.g. PS4)
- Limit/eliminate other drains on bandwidth such as streaming music services, Netflix, mobile devices
- IT recommends using a personal PC or laptop only (Windows based). They do not recommend a Mac OS device for accessing AVHE. Some individuals have had success with a Mac device and instructions for how to configure your Mac are available later in this document if you wish to attempt it.

CAC Reader Set-up

1. Plug in CAC reader to USB port. It should automatically install.
2. Open Device Manager (On Control Panel or use Windows Search feature), look for “Smart card readers” to verify that the device is installed.
    a. If it is not there, you will need to download the drivers.
    b. Visit http://militarycac.com/cacdrivers.htm for links to smart card reader drivers.
3. Download the DoD certificates (http://militarycac.com/dodcerts.htm)
    a. There are specific steps for Windows and Mac.
    b. You will need to restart your computer after downloading for this to take effect.
    c. If militarycac.com does not work try https://public.cyber.mil/pki-pke/end-users/getting-started/#toggle-id-1

Configure your Web Browser

Use Internet Explorer 11 ONLY. If your computer does not have this you can download it from this site: https://www.microsoft.com/en-us/download/details.aspx?id=41628

- Do not use MS Edge, Chrome, Firefox or any other browser.
- When first setting this up do NOT access AVHE through Citrix.

1. Properly configure the Internet Explorer 11 settings.
    a. Launch Internet Explorer.
    b. Go to the Menu Bar, click Tools (or the icon that looks like a gear or sprocket).
    c. Click Pop-Up Blocker.
    d. Turn this off or set it to allow pop-ups from this website.
        i. If you turn it on then either click Tools and click Pop-up blocker settings or Internet Options/Privacy tab and click Settings.
        ii. In the “Address of website to allow:” field enter*.health.mil and click Add.
        iii. *.health.mil will now appear under “Allowed Sites” field.
        iv. Click OK.
    e. Click Manage Add-ons. Skip the Manage Add-On section until you have installed Citrix and have logged on to AVHE successfully.
        i. Search for Citric ICA Client and make sure it is enabled.

ii. Click OK.

f. Click Safety. Make sure that there are no check marks to the left of ActiveX Filtering. If you have it then deselect it.

g. Click Internet Options.

i. On the General tab, click Delete… under the Browsing History section. When the screen comes up, verify that at least these options (Temporary Internet Files, Cookies, and History are checked).

ii. Click Delete.

1. If Delete button is grayed out then click Settings. Click View Files. Click Select All under Organize Menu option. Click Delete on your keyboard.

iii. Close the folder and previous screen.

iv. Click Security tab.

1. Click Trusted Sites.
2. Click Sites.
3. Verify you have HTTPS://*.health.MIL <HTTPS://*.health.MIL> listed in the "Website:" field but if not then enter it in "Add this website to the zone:" field and click Add.
4. Click Close.

v. Click Restricted Sites.

1. Click Sites.
2. Make sure that the AVHE web address is NOT listed here. If it is then remove it.

vi. Click Connections Tab.

1. Click LAN settings.

a. Make sure that no options are selected.

b. Click OK if you made any changes.

vii. Click Advanced tab.

1. In the Settings section, under the Security header, make sure that the “Do not save encrypted pages to disk” option should not be checked.
2. Deselect “Use SSL 3.0” and “Use TLS 1.0” options.

viii. Click OK to close Internet Options Screen.

h. Click Comparability View Settings

i. If “health.mil” is not listed in the “Websites you’ve added to Compatibility View” field then do the following:

1. In the “Add this website:” field, enter health.mil if it is not already there.
2. Click Add.
3. Click Close.

Add AVHE

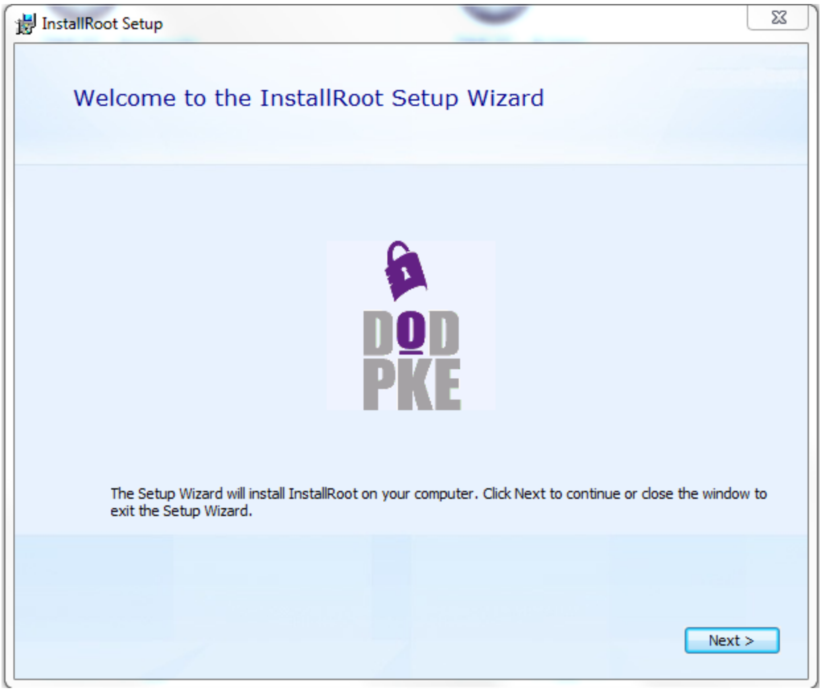
1. Install InstallRoot v5.5 32-Bit for Non-Admin (https://avhe-support.health.mil) on your computer.

a. Any previous versions of InstallRoot should be uninstalled first.

b. Run InstallRoot while logged into your computer as Administrator (for people with multiple Microsoft Accounts on their home device).

c. Under For End-Users header, click DoD Root Cert Installer link.

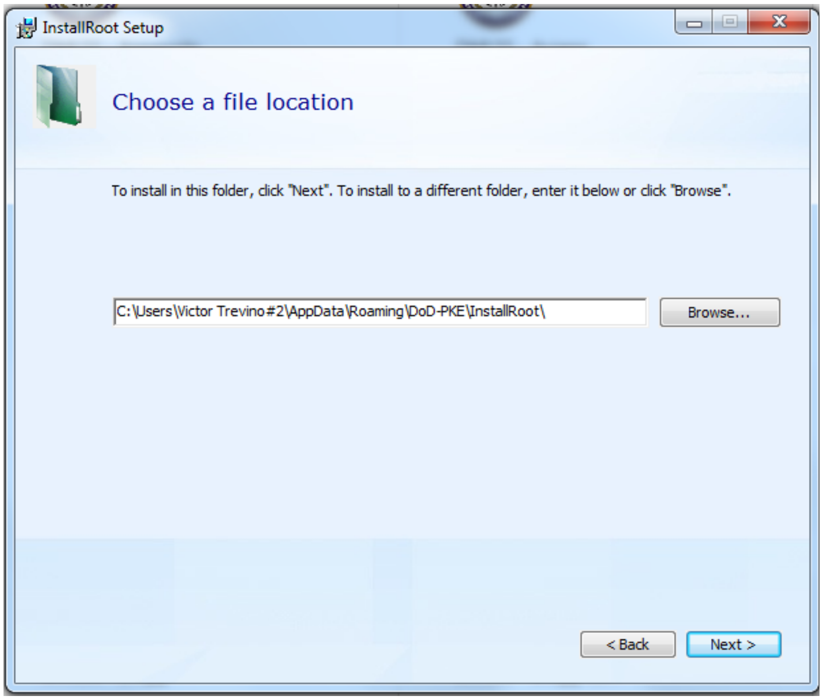
d. Detailed installation instructions



Welcome to the InstallRoot Setup Wizard

The Setup Wizard will install InstallRoot on your computer. Click Next to continue or close the window to exit the Setup Wizard.

Click next.

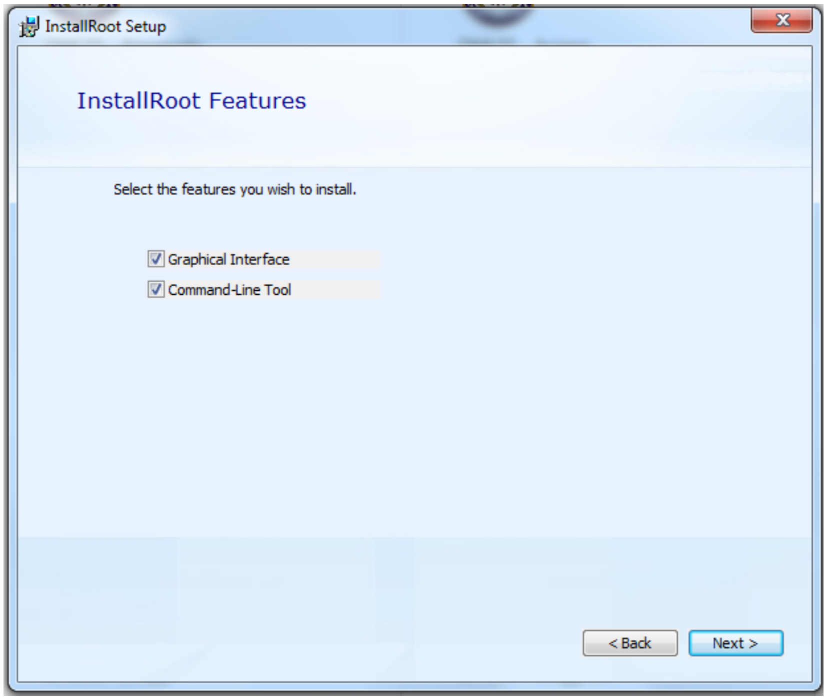


Choose a file location

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

C:\Users\Victor Trevino#2\AppData\Roaming\DoD-PKE\InstallRoot\

Click Next.



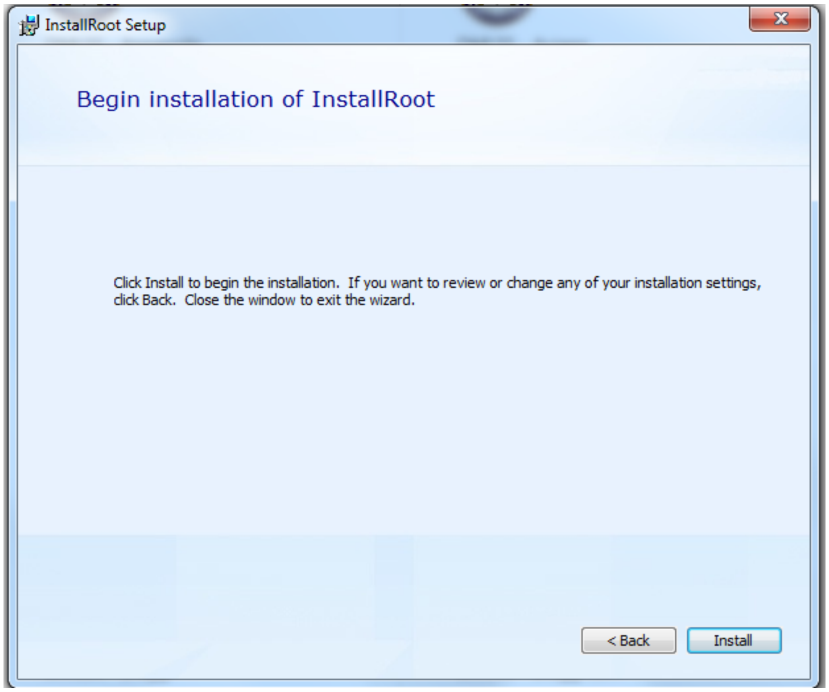
InstallRoot Features

Select the features you wish to install.

☑ Graphical Interface

☑ Command-Line Tool

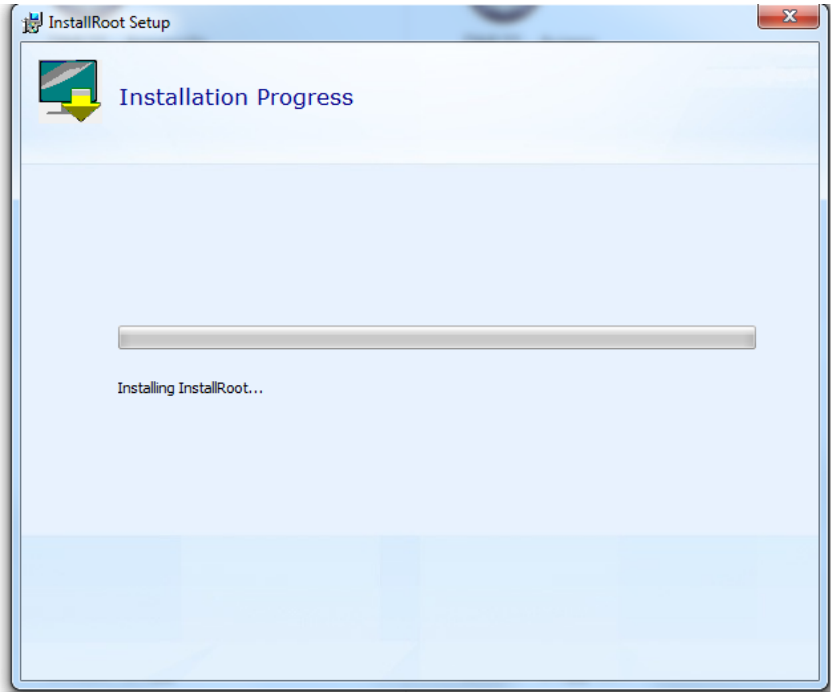
Click Next.



Begin installation of InstallRoot

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Close the window to exit the wizard.

Click Install.

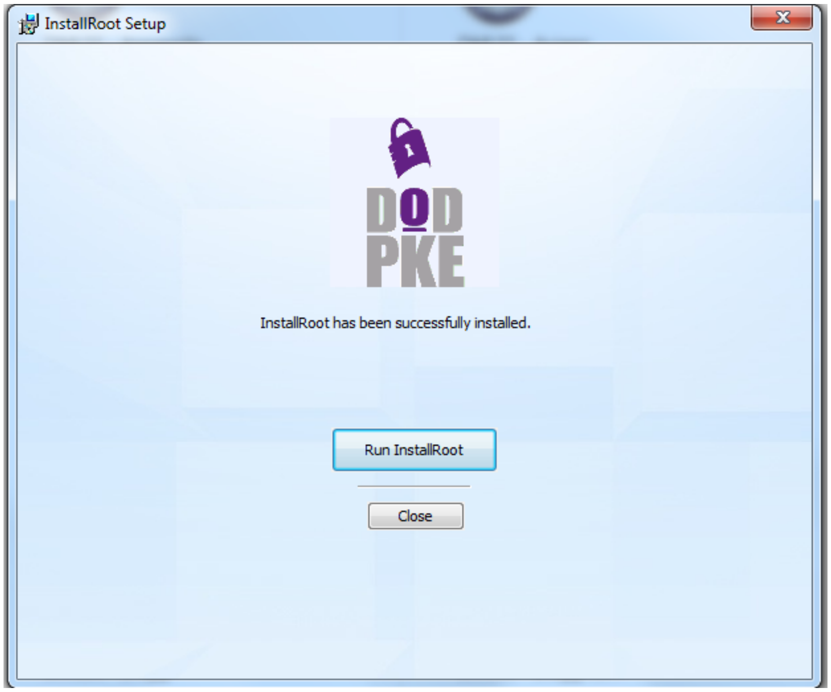


InstallRoot Setup

Installation Progress

Installing InstallRoot...

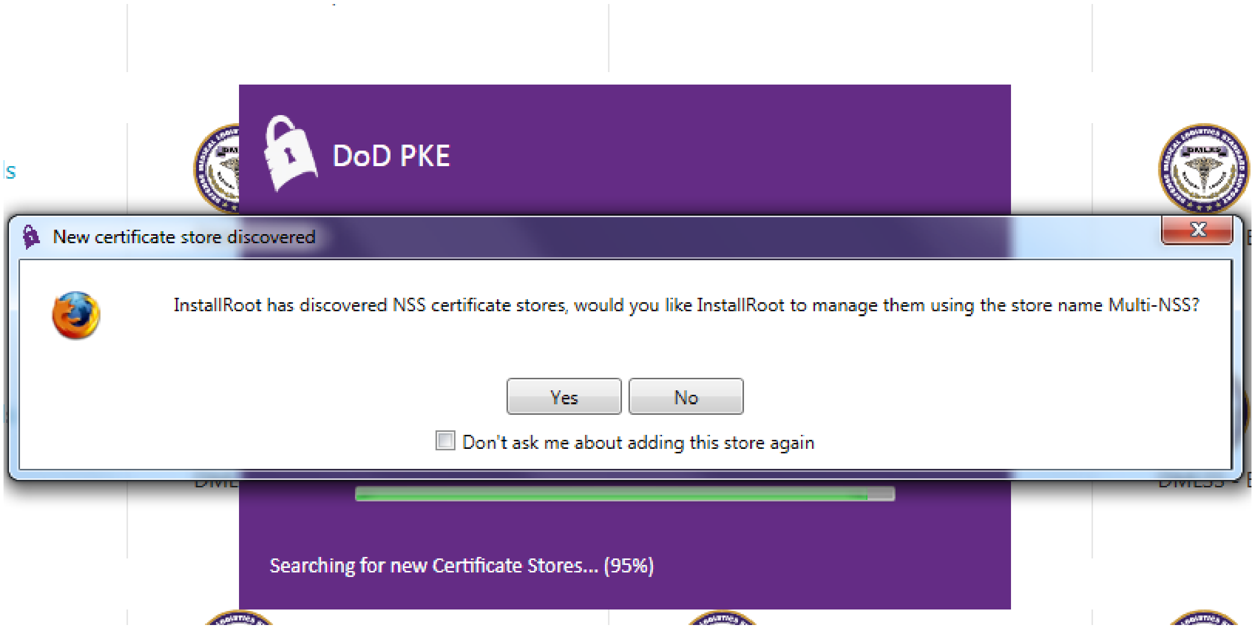
This will take a few minutes.



InstallRoot Setup

InstallRoot has been successfully installed.

Click Run InstallRoot.



DoD PKE

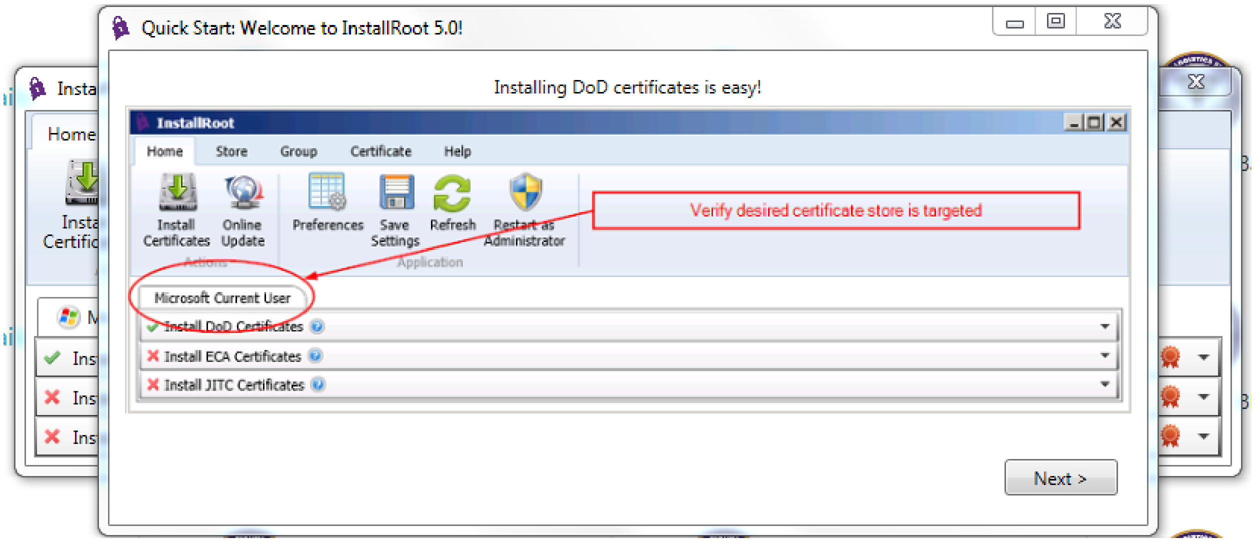
New certificate store discovered

InstallRoot has discovered NSS certificate stores, would you like InstallRoot to manage them using the store name Multi-NSS?

☐ Don't ask me about adding this store again

Searching for new Certificate Stores... (95%)

Click Yes (may need to do > once).



Quick Start: Welcome to InstallRoot 5.0!

Installing DoD certificates is easy!

Verify desired certificate store is targeted

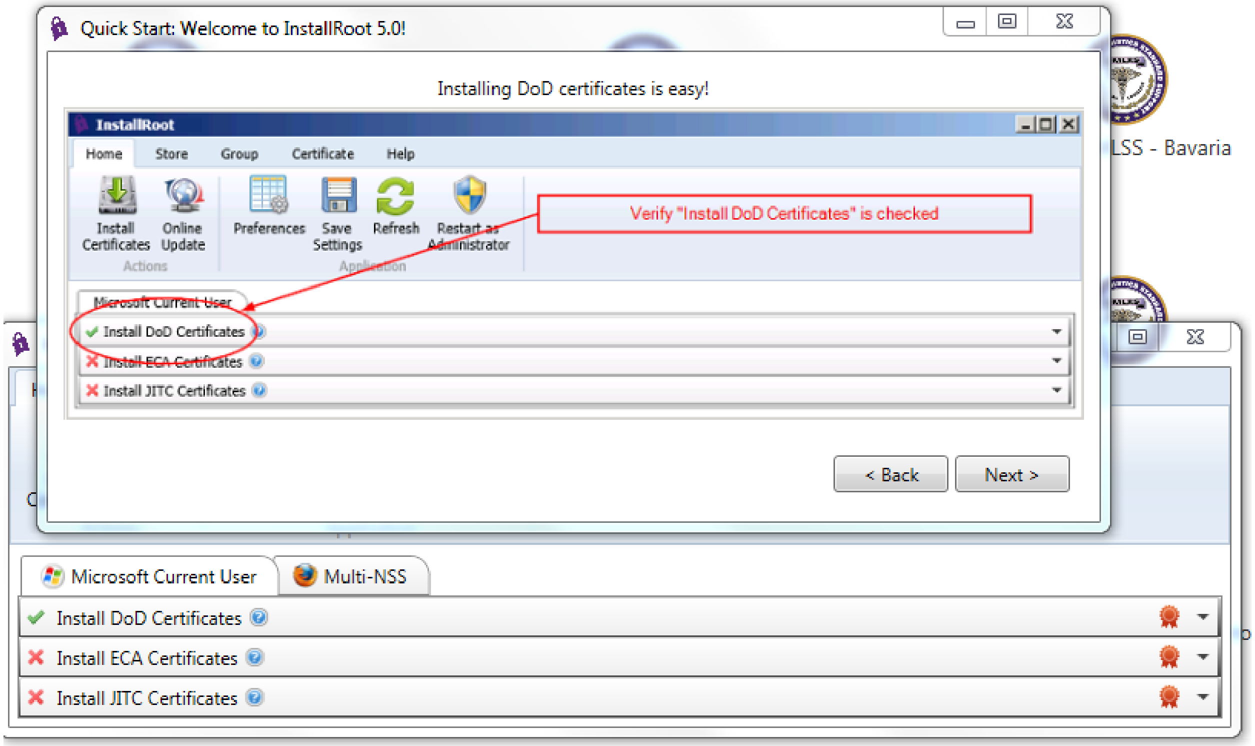
Microsoft Current User

✓ Install DoD Certificates

✗ Install ECA Certificates

✗ Install JITC Certificates

Click Next.



Quick Start: Welcome to InstallRoot 5.0!

Installing DoD certificates is easy!

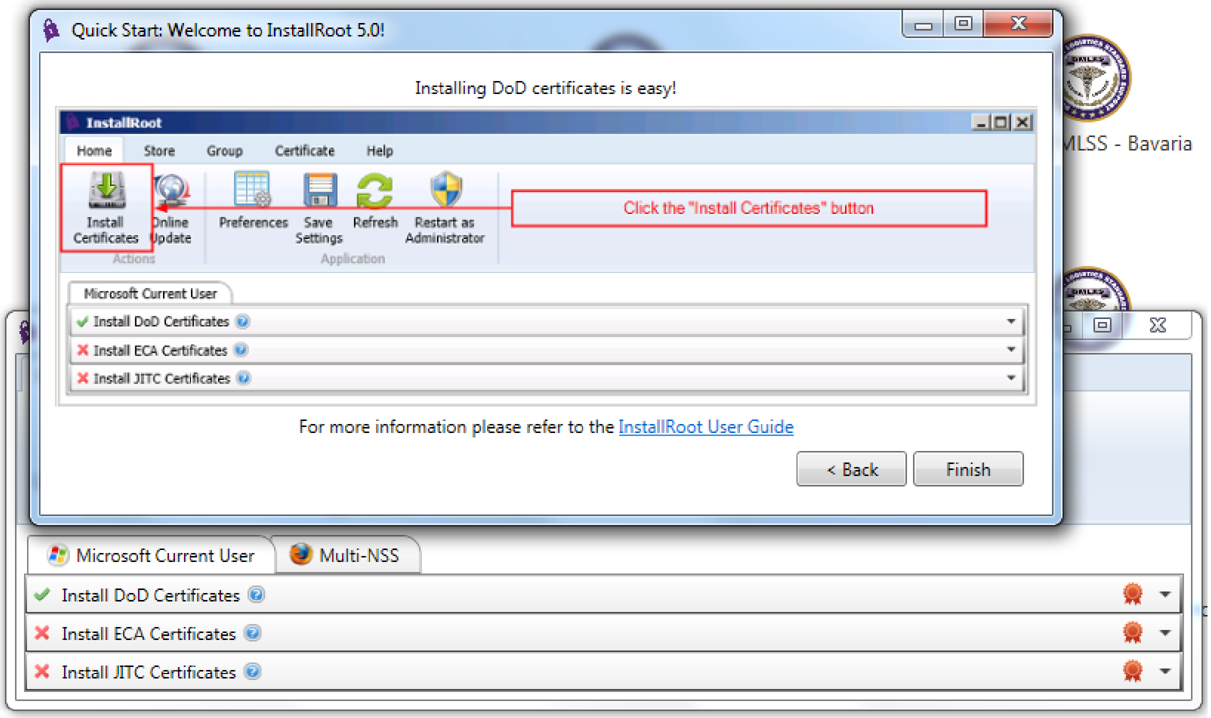
Verify "Install DoD Certificates" is checked

✓ Install DoD Certificates

✗ Install ECA Certificates

✗ Install JITC Certificates

Click Next.



Quick Start: Welcome to InstallRoot 5.0!

Installing DoD certificates is easy!

Click the "Install Certificates" button

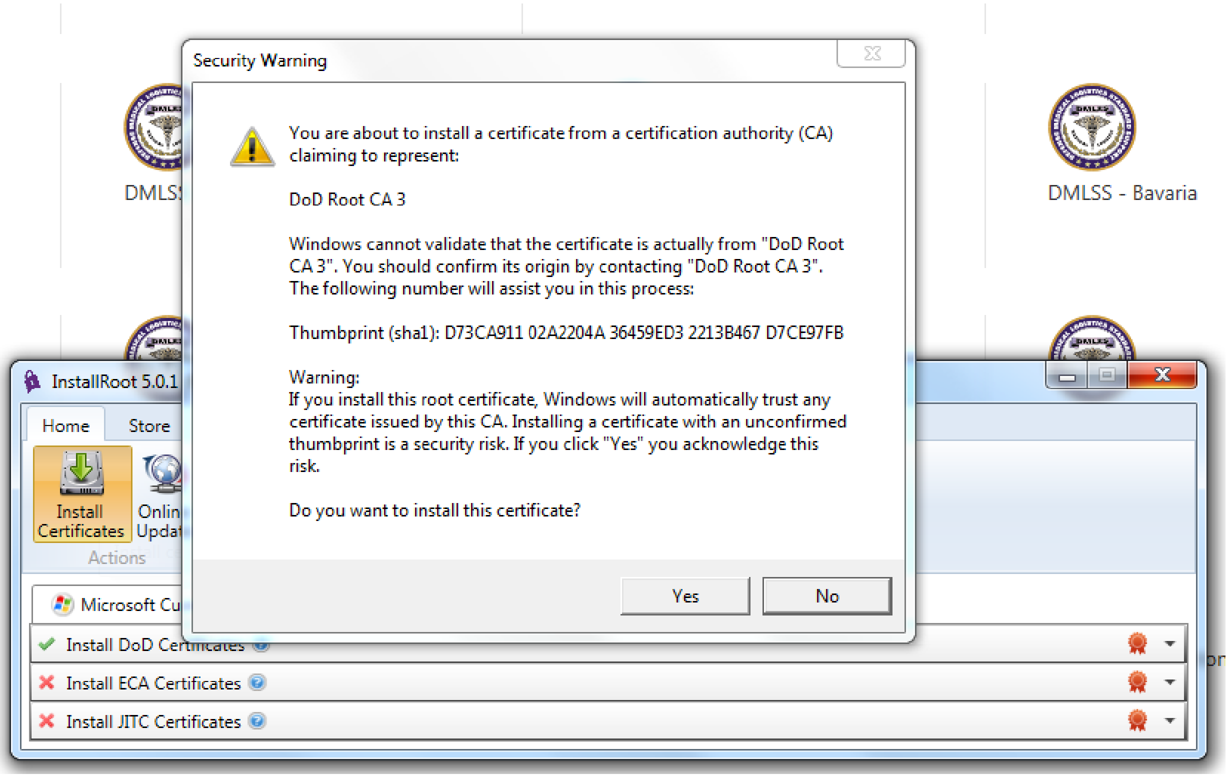
✓ Install DoD Certificates

✗ Install ECA Certificates

✗ Install JITC Certificates

For more information please refer to the InstallRoot User Guide

Click Finish.



You are about to install a certificate from a certification authority (CA) claiming to represent:

DoD Root CA 3

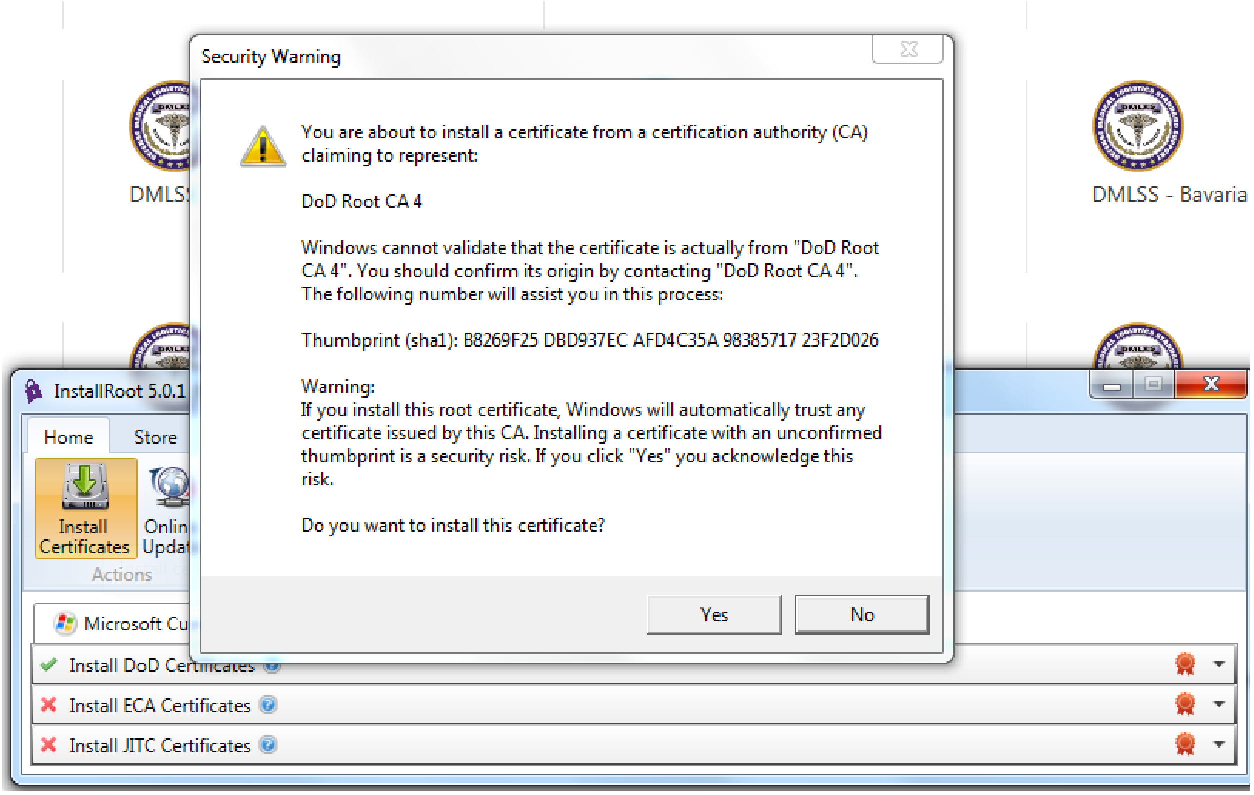
Windows cannot validate that the certificate is actually from "DoD Root CA 3". You should confirm its origin by contacting "DoD Root CA 3". The following number will assist you in this process:

Thumbprint (sha1): D73CA911 02A2204A 36459ED3 2213B467 D7CE97FB

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Click Install Certificates.



You are about to install a certificate from a certification authority (CA) claiming to represent:

DoD Root CA 4

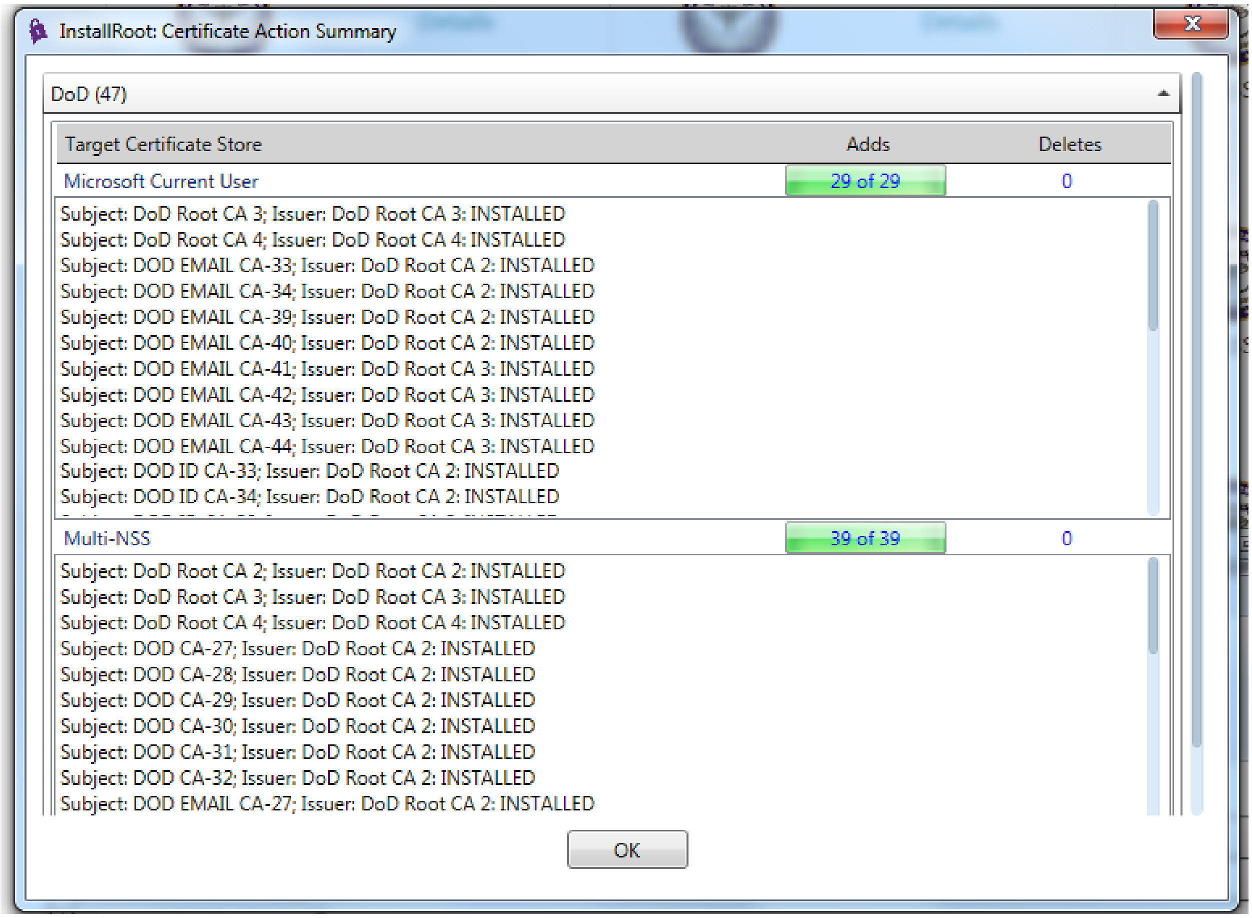
Windows cannot validate that the certificate is actually from "DoD Root CA 4". You should confirm its origin by contacting "DoD Root CA 4". The following number will assist you in this process:

Thumbprint (sha1): B8269F25 DBD937EC AFD4C35A 98385717 23F2D026

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Click Yes to the Security Warning.



InstallRoot: Certificate Action Summary

DoD (47)

Target Certificate Store	Adds	Deletes
Microsoft Current User	29 of 29	0

Subject: DoD Root CA 3; Issuer: DoD Root CA 3: INSTALLED
Subject: DoD Root CA 4; Issuer: DoD Root CA 4: INSTALLED
Subject: DOD EMAIL CA-33; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD EMAIL CA-34; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD EMAIL CA-39; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD EMAIL CA-40; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD EMAIL CA-41; Issuer: DoD Root CA 3: INSTALLED
Subject: DOD EMAIL CA-42; Issuer: DoD Root CA 3: INSTALLED
Subject: DOD EMAIL CA-43; Issuer: DoD Root CA 3: INSTALLED
Subject: DOD EMAIL CA-44; Issuer: DoD Root CA 3: INSTALLED
Subject: DOD ID CA-33; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD ID CA-34; Issuer: DoD Root CA 2: INSTALLED

Target Certificate Store	Adds	Deletes
Multi-NSS	39 of 39	0

Subject: DoD Root CA 2; Issuer: DoD Root CA 2: INSTALLED
Subject: DoD Root CA 3; Issuer: DoD Root CA 3: INSTALLED
Subject: DoD Root CA 4; Issuer: DoD Root CA 4: INSTALLED
Subject: DOD CA-27; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD CA-28; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD CA-29; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD CA-30; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD CA-31; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD CA-32; Issuer: DoD Root CA 2: INSTALLED
Subject: DOD EMAIL CA-27; Issuer: DoD Root CA 2: INSTALLED

Scroll to bottom of screen, click Yes.

2. FBCA Cross Certificate Remover Tool v1.18 (https://cyber.mil).
    a. Click PKI/PKE menu option. Select Public Key Infrastructure/Enabling (PKI\PKE) link. On the left pane, click For Administrators, Integrators, and Developers link. Wait for the page to fully load then scroll down. You will then see a list. At the top, right hand side of the list there is a Search field. Use this field to search for FBCA. Click FBCA Cross-Certificate Remover 1.18 link. Extract the file before installing.
3. Install CITRIX WORKSPACE APP 1812 for Windows (https://avhe-support.health.mil) or Alternate URL for the latest Citrix Workspace version (https://www.citrix.com/downloads/workspace-app/windows/workspace-app-for-windows-latest.html).
    a. Scroll to the bottom of the page, under For End-Users right click on Download Citrix Receiver.
    b. Extract the file before installing. Install Admin or Elevated privileges (Right click file and select Run As Administrator).
4. WINDOWS 10 REGISTRY FIX (Local Admin Rights required) (https://io.dha.health.mil/fls/fls_mdi/Win10RegFix.txt), see additional notes at end of this document or AVHE User Guide for details. Do not make a mistake in the registry for it could render your PC inoperable.

a. All end-user Windows workstations (ESPECIALLY Windows 10 users) connecting with AVHE will benefit greatly from adding the following 2 Windows Registry keys:
b. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Base Smart Card Crypto Provider
    i. TransactionTimeoutMilliseconds
    ii. DWORD Decimal value of 3000
c. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais
    i. TransactionTimeoutDelay
    ii. DWORD Decimal value of 45
d. The settings above have been determined by the AVHE Engineering team, to be the OPTIMAL settings for the AVHE environment. Windows 10 does not have these Registry keys.
e. Even if you do not have ActivClient installed, these additions to the Windows 10 registry will improve timeouts and AVHE end-user session reliability.
f. https://support.citrix.com/article/CTX228009 (but, use the values above. Citrix actually used our AVHE Engineer research for the article)

Using AVHE

1. Go to https://avhe.health.mil
2. Log in with your EMAIL certificate. You may have to enter your pin several times.
3. Along the top, you will see “APPS”
4. Click on Apps.
5. Find “AHLTA – Bethesda” and click “Details”.
6. Click “Add to Favorites”
7. Do this for CHCS and Essentris. You can then double click the icons to log in to the systems.
8. The AVHE user guide is attached to this document.
9. If you are having difficulty logging into the AVHE, contact the DHA GSC. If you have not used AVHE in the past or you cannot access those systems please contact AVHE directly at: 1-800-600-9332.

Using Outlook Email via Web Browser

1. Access Outlook remotely using Web Mail at https://web.mail.mil/my.policy
2. Select your latest email certificate and enter PIN.
3. Requires a CAC reader which is available from IT.
4. You will not be able to open encrypted messages with Web Mail (this is a limitation of this service).

H: Drive Folder

1. There is no other way to access PSD folders (H: drive folders) remotely without a government furnished laptop and VPN connection.

Using a MAC

1. Requirements
    a. Mac (MacOS 10.6.x and later)
    b. Chrome or Safari (Safari requires additional set-up).
2. Install CITRIX (https://www.citrix.com/downloads/workspace-app/mac/workspace-app-for-mac-latest.html)
3. Download and install 5 DoD Certificate files (see www.militarycac.com/macnotes.htm)
    a. With CAC inserted into reader go to your Keychain Access (you can find this with Finder)
    b. Under ‘System Certificates’ locate DoD Root CA 2-5.
    c. If there is a red X you need to manual set your Mac to trust these certificates.
        i. Double click on the red X’d DoD Root Certificate.
        ii. Click on Trust and change the “When using this certificate” to ’Always trust’ then exit out the window and save with admin password.
        iii. Complete this with each DoD Root Certificate that is untrusted.

AVHE Application Delivery

Application Virtualization Hosting Environment

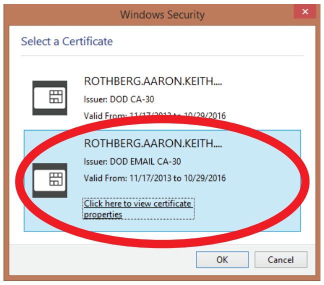
User Guide- Accessing Applications through a Web Browser

1 Open your web browser and enter the URL below into the address bar.

https://avhe.health.mil

NOTE: AVHE no longer uses site specific URLs. All applications are available using the link above.

2 Select the DOD EMAIL Certificate from your CAC, or the correct certificate from your PIV card, and then click "OK."



Windows Security

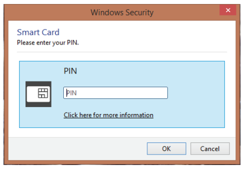
Select a Certificate

ROTHBERG.AARON.KEITH....
Issuer: DOD CA-30
Valid From: 11/17/2013 to 10/29/2016

ROTHBERG.AARON.KEITH....
Issuer: DOD EMAIL CA-30
Valid From: 11/17/2013 to 10/29/2016
Click here to view certificate properties

OK Cancel

3 "ActivClient Login" or "Windows Security Smart Card" box will now be displayed. Enter your pin and click "OK."



Windows Security

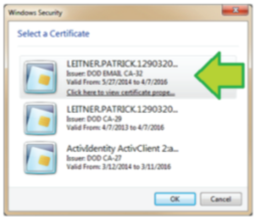
Smart Card
Please enter your PIN.

PIN
Click here for more information

OK Cancel

NOTES: 1) If you receive a screen that says "You are not allowed to login. Please contact your administrator." there is a problem with your Joint Active Directory Account. You will need to contact the DHA Global Service Center via the information below.

Incorrect Certificate Chosen



Windows Security

Select a Certificate

LEITNER.PATRICK.1290320...
Issuer: DOD EMAIL CA-32
Valid From: 5/27/2014 to 4/7/2016
Click here to view certificate prope...

LEITNER.PATRICK.1290320...
Issuer: DOD CA-29
Valid From: 4/7/2013 to 4/7/2016

ActivIdentity ActivClient 2:a...
Issuer: DOD CA-27
Valid From: 3/12/2014 to 3/11/2016

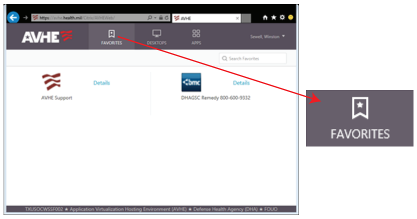
OK Cancel

2) If you receive a screen that says "Incorrect Certificate Chosen" then you have NOT selected your DOD EMAIL cert (or the correct PIV cert) from your DOD CAC or PIV cards. Please close out your browser, reconnect to the AVHE URL, and select your DOD EMAIL cert when prompted.

4 The United States Department of Defense banner will now be displayed. Please read and then click "Accept."

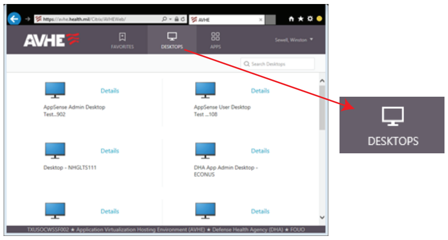
NOTE: If you receive an "Error: Access is Denied. Client SSL Certificate Invalid" error message when connecting through a web browser, then you will need to run the FBCA Cross-Certificate Remover tool from DISA.
•DISA tool link:
http://iase.disa.mil/pki-pke/function_pages/tools.html
•Then select tab "Certificate Validation"
•Then select "FBCA Cross-Certificate Remover" current version

5 On first logon, the "Favorites" tab will display the default system applications in the AVHE browser window.



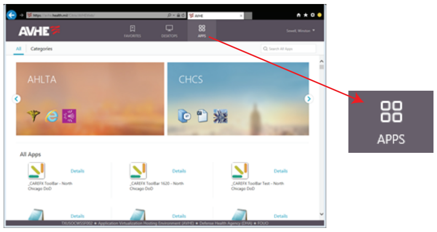
NOTE: The default favorites are the AVHE Support Page link, which contains the full AVHE User Guide, and the DHAGSC Remedy Trouble Ticket submission link.

6 Click the "Desktops" tab to see any published desktops that have been made available to you.

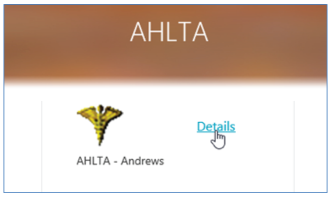


7 The Apps tab is intended to work like the Apple or Google Play app stores you may be familiar with on your mobile devices.

You can use the Categories menu, the featured Groups or the Search box to help you find the app you are looking for.



8 When you find an app that you plan to use frequently click the Details link.

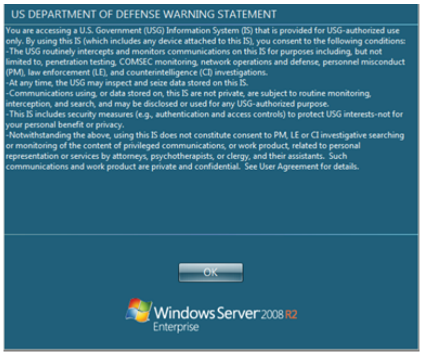


Next, click the Add To Favorites button to move the app to the front page, making it easier to find.

Add To Favorites

9 To launch an app, single click your desired application icon.

When the US DOD Warning Statement appears, please read and click OK.



US DEPARTMENT OF DEFENSE WARNING STATEMENT

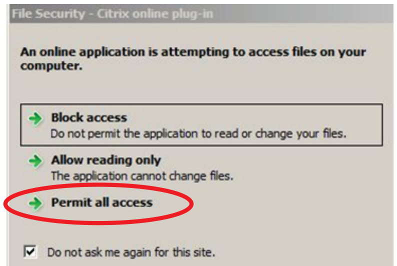
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for purposes 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., authentication 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. See User Agreement for details.

OK

Windows Server 2008 R2 Enterprise

10 You may see this Citrix File Security Screen when you access your application.

-Select "Permit all access."



File Security - Citrix online plug-in

An online application is attempting to access files on your computer.

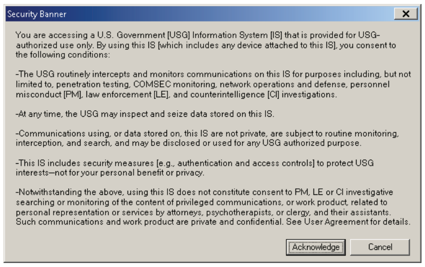
Block access
Do not permit the application to read or change your files.

Allow reading only
The application cannot change files.

Permit all access

☑ Do not ask me again for this site.

11 Your application's Security Banner will display. Click "Acknowledge."



Security Banner

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.

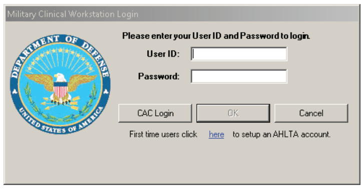
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures [e.g., authentication 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. See User Agreement for details.

Acknowledge Cancel

12 The application login window is now displayed.
•Enter your Username/ID and Password
•Next click "OK."



Military Clinical Workstation Login

Please enter your User ID and Password to login.
User ID:
Password:

CAC Login OK Cancel

First time users click here to setup an AHLTA account.

NOTE: If you experience any issues with accessing applications on AVHE, please contact the DHA Global Service Center (DHAGSC) at (800) 600-9332 (or by using the appropriate country access code for OCONUS) or via email at dhagsc@mail.mil. To submit a support ticket via the web, log on to the DHAGSC Remedy Service Request Management module at https://support-gsc.health.mil and search for "AVHE" (requires an active Remedy account). For more information or to download the Citrix client, please visit https://avhe-support.health.mil.