



NAVY RESERVE FORCE HEADQUARTERS

STANDARD OPERATING
PROCEDURES

07 August 2013



1. INTRODUCTION

The purpose of this guide is to provide a comprehensive installation guide to Navy Reserve personnel for installing CAC devices on personal computing equipment.

1.1. Process:

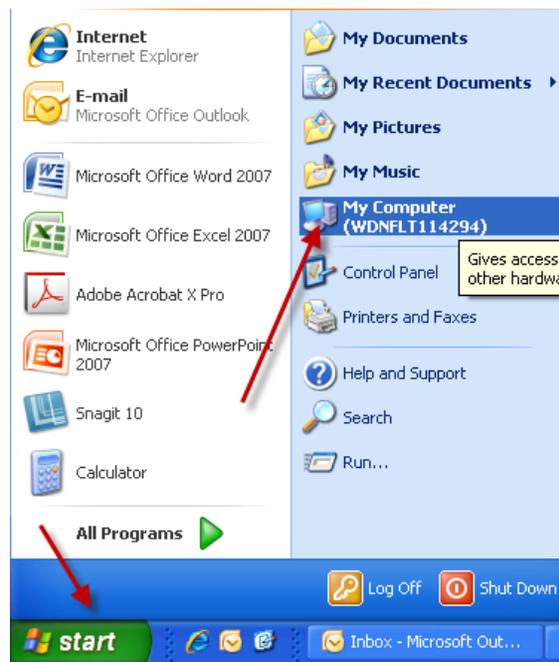
- A. Obtaining required files
- B. Installing Active Identity
- C. Installing Root Certificates
- D. Configuring Internet Explorer
- E. Adding sites to trusted domains
- F. Adding sites to compatibility mode

A. Obtaining required files

- In order for your CAC to properly work on your computer, you will need to obtain a CD that holds the **ActivClient 6.2** and **InstallRoot 3.16A** software on it. You can obtain this CD from the IT department of the command you are attached to.
- If you are a machine with CAC access and wish to burn the software to a CD; the software can be obtained at the Navy Reserve Homeport at <https://private.navyreserve.navy.mil/cnrfc/N-Codes/N6/Information%20Assurance/ActivClient%206.2>.

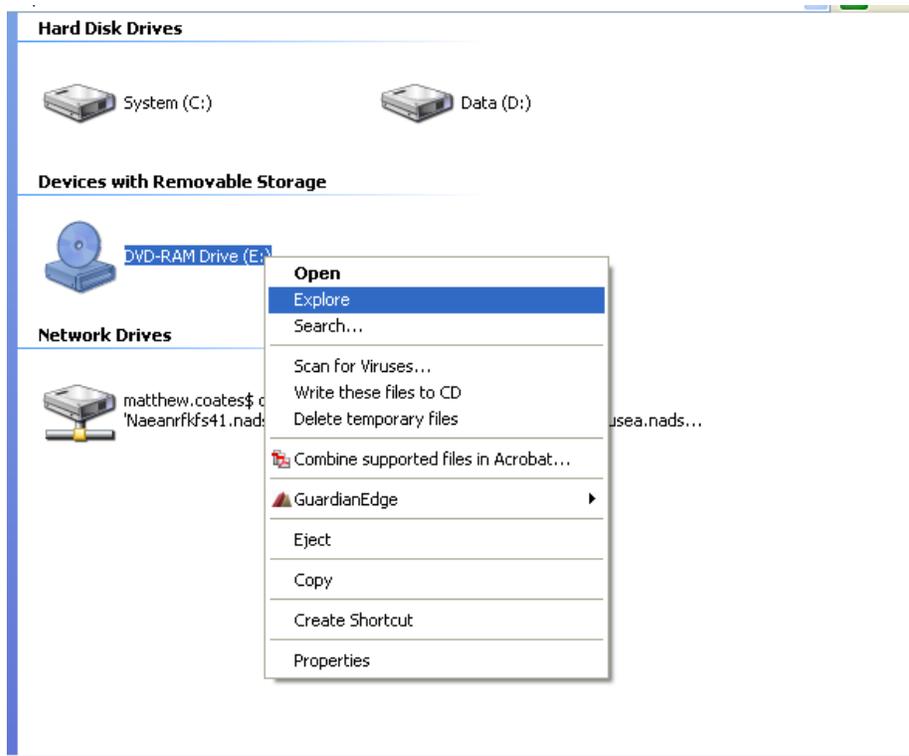
B. Installing Active Identity

1. Ensure you have inserted the above mentioned CD into your computer. Select “Start” and then select “My Computer”.

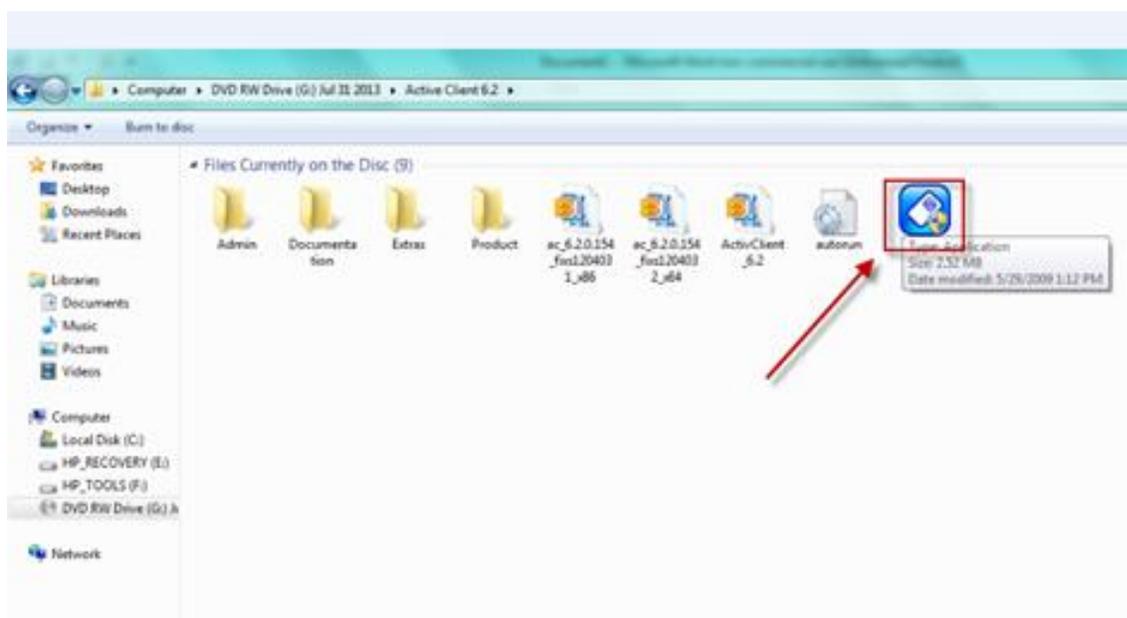




2. Right click on your 'D: Drive' and select "Explore".

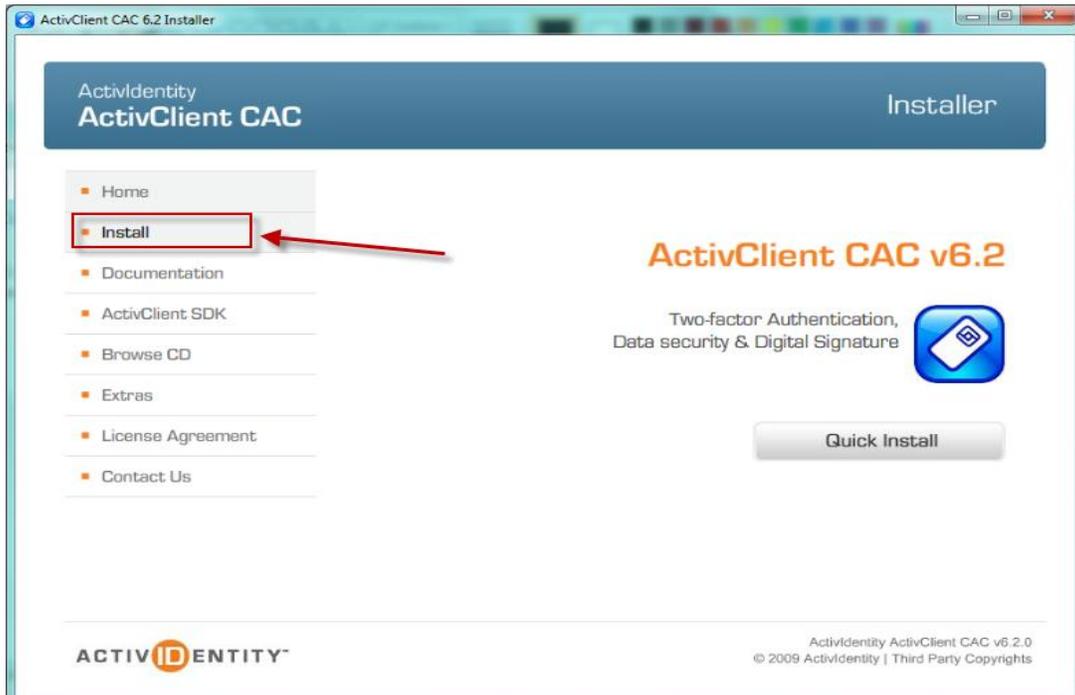


3. Double click "Activ Client 6.2"

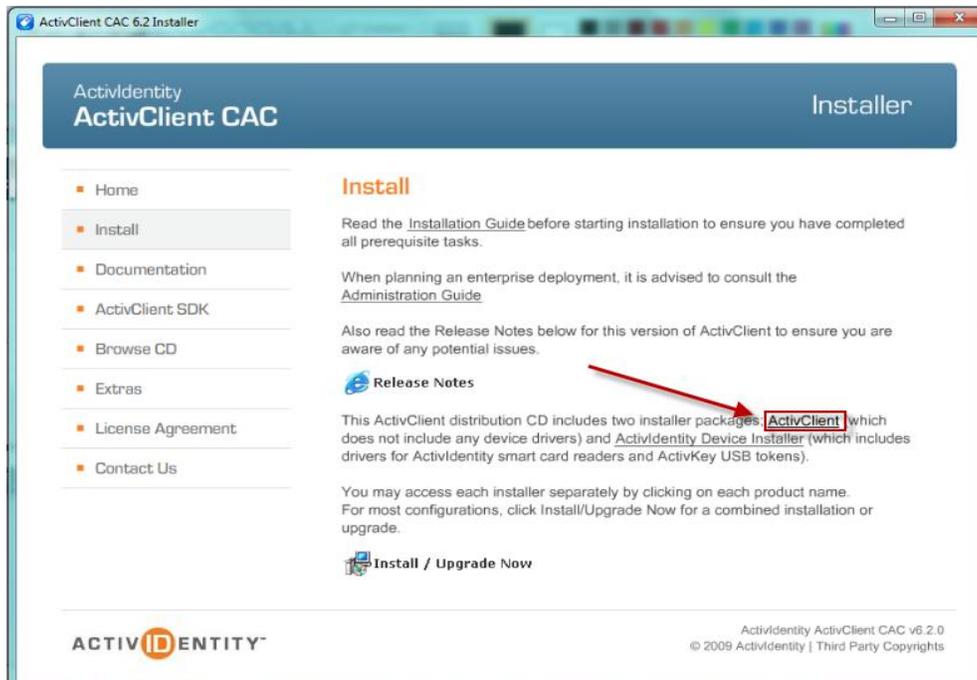




4. Select "Install".

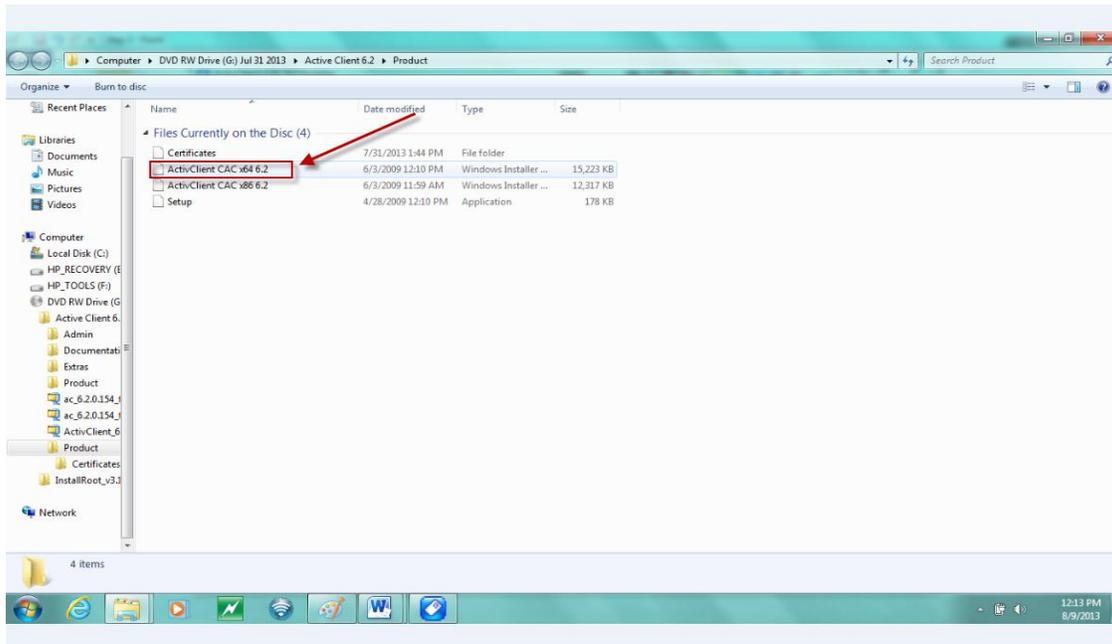


5. Select "ActivClient" as shown below.

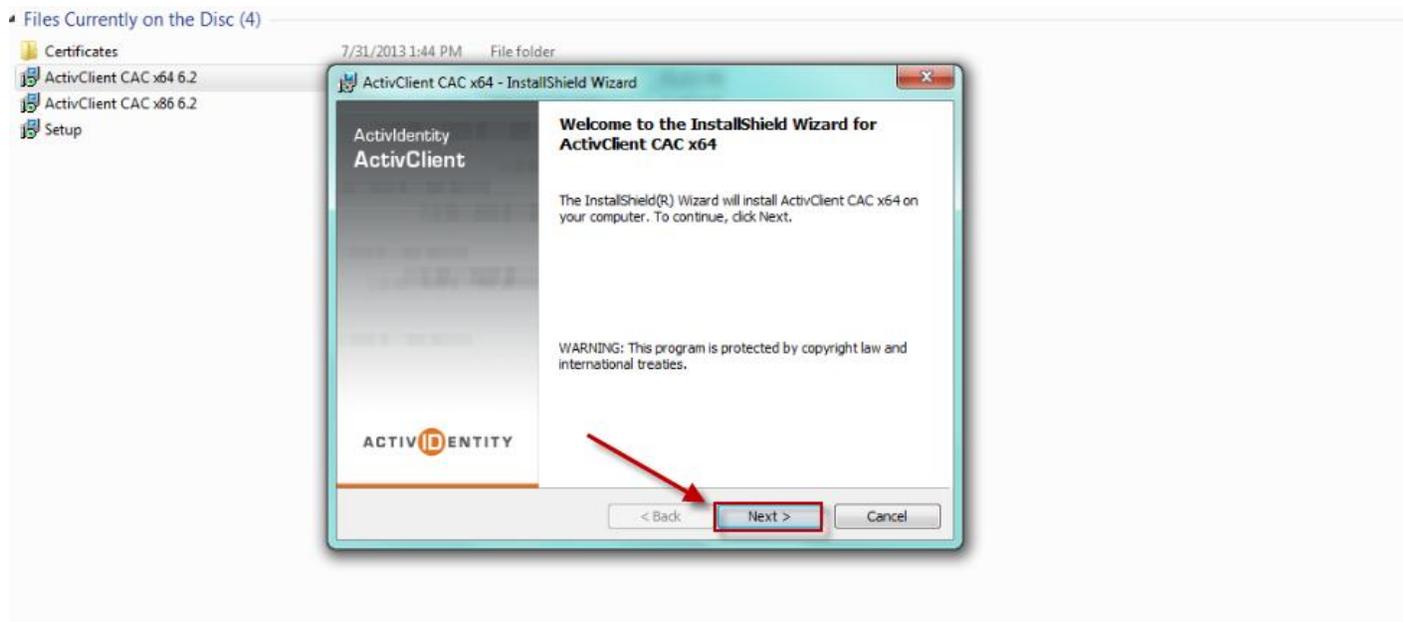




6. Double click “ActivClient CAC x64 6.2”

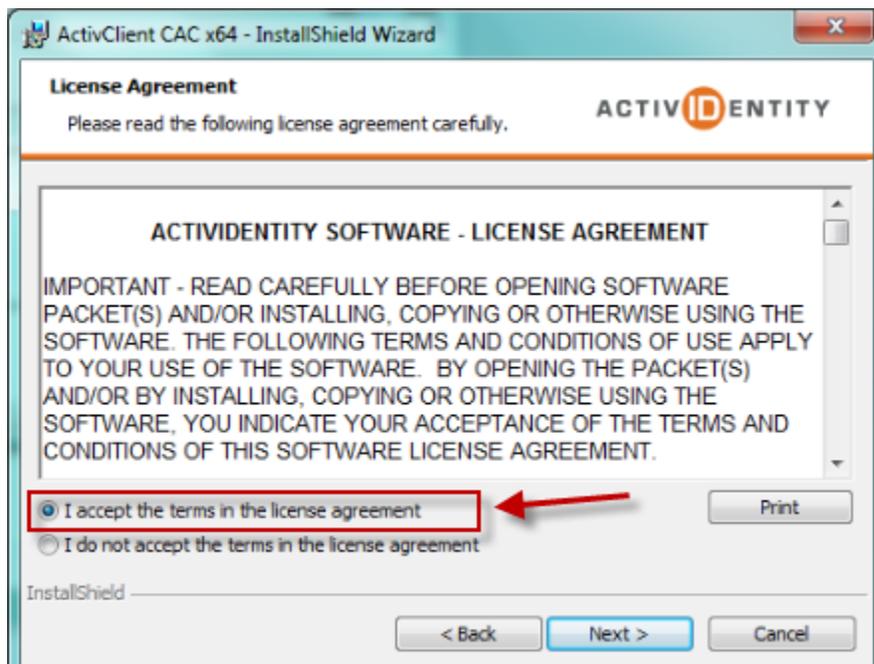


7. Click “Next” on the InstallShield Wizard that pops up.

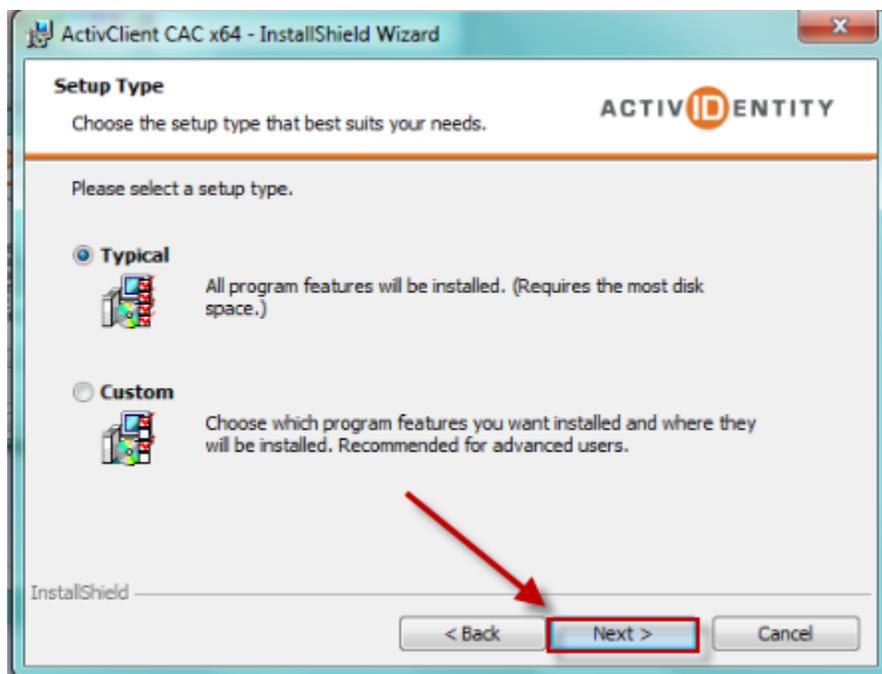




8. Read the License Agreement and then select the radio button for “I accept the terms in the license agreement.”

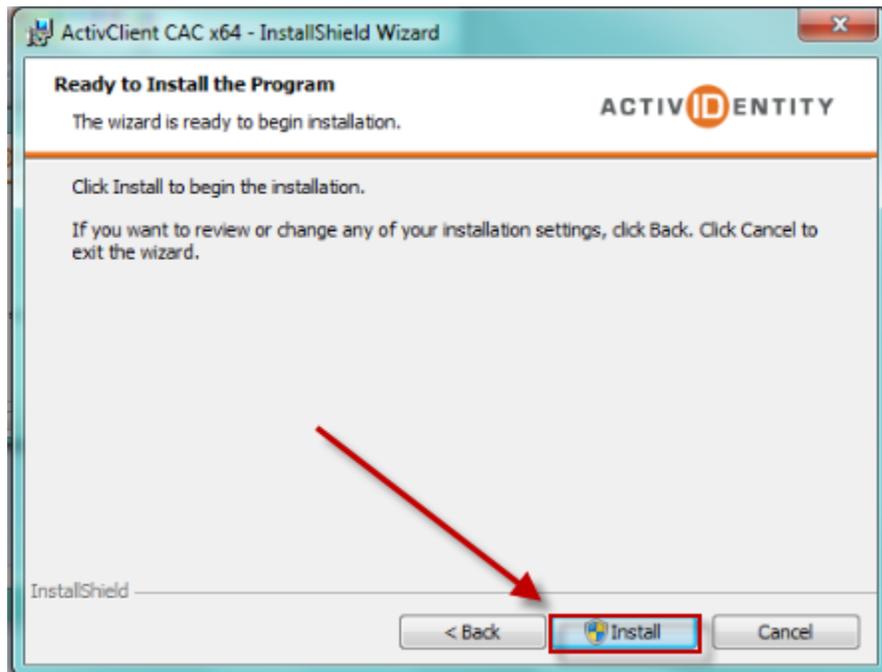


9. Select the “Typical” setup type and select next.

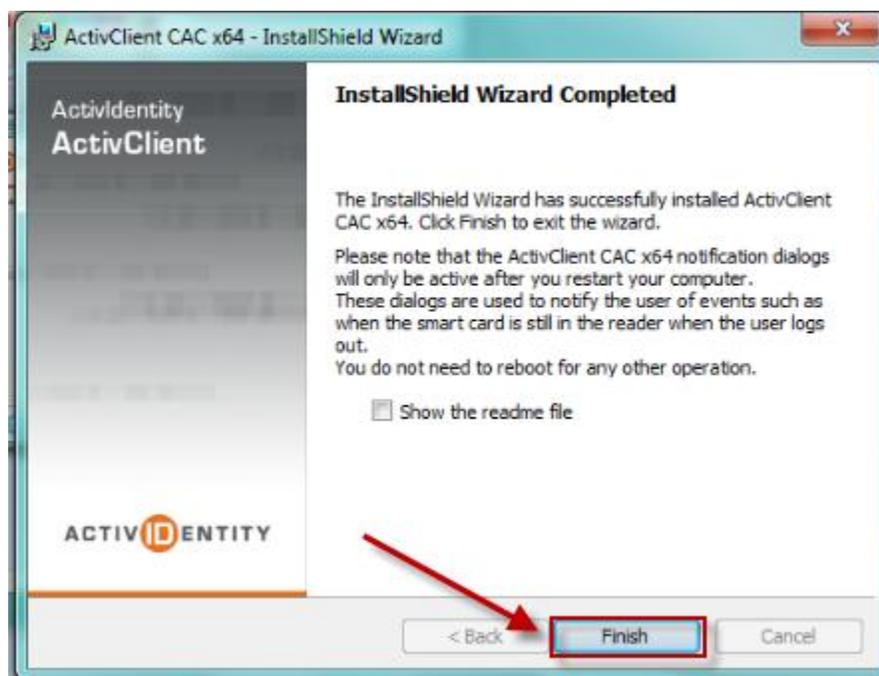




10. Select "Install"

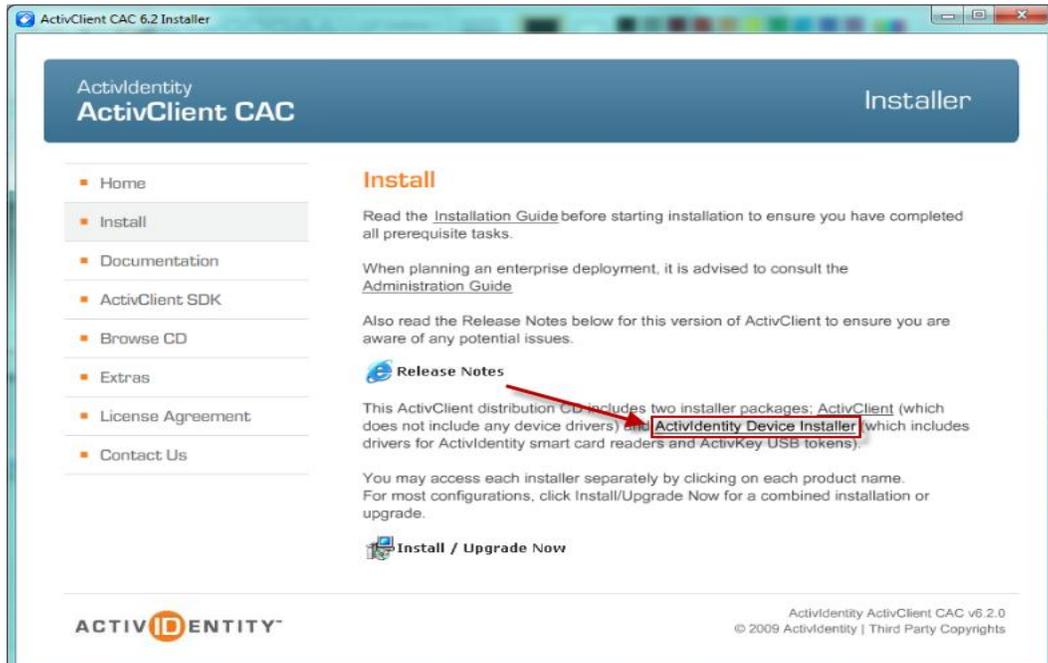


11. Wait for the install to finish and select "Finish"

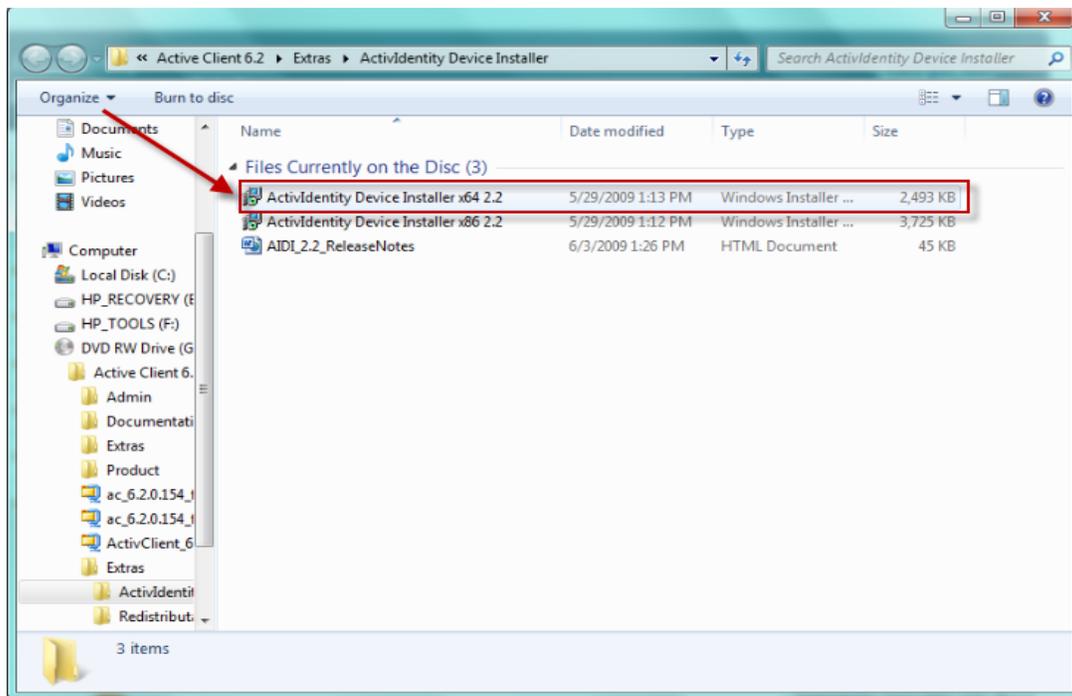




12. On the ActivClient CAC 6.2 Installer page, select “ActivIdentity Device Installer” as shown below.

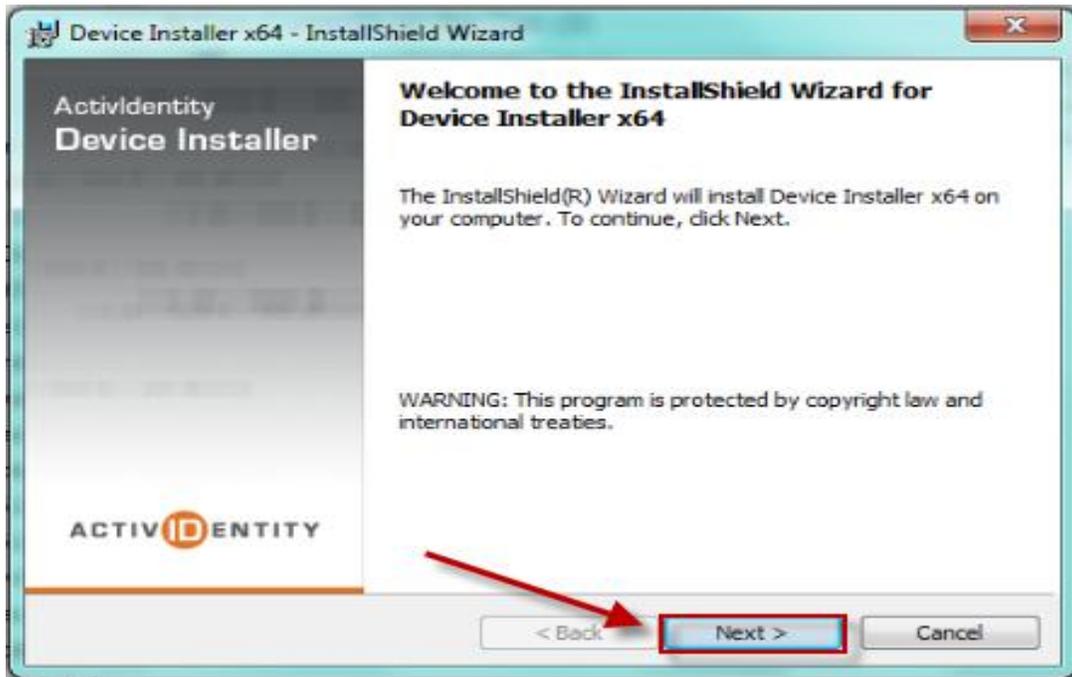


13. Double Click on “ActivIdentity Device Installer x64 2.2”

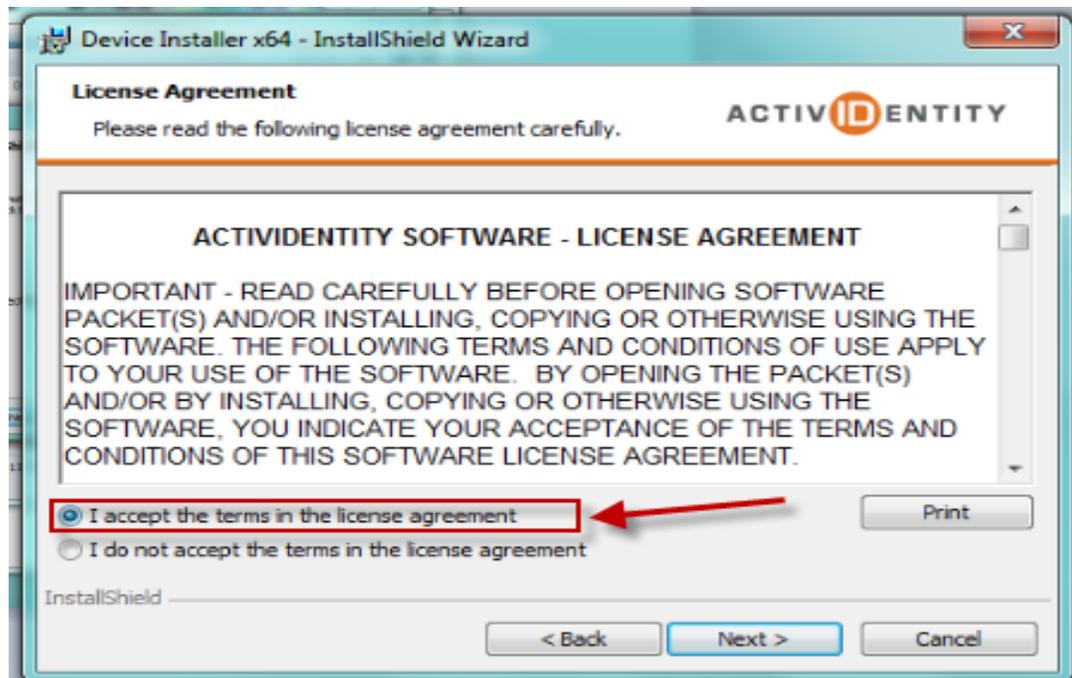




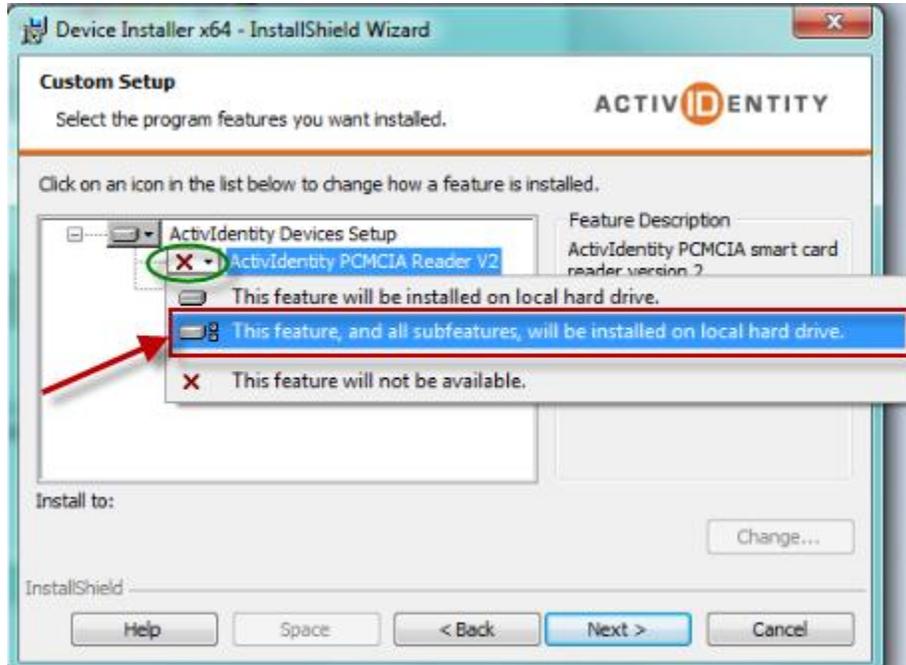
14. Select “Next” on the InstallShield Wizard.



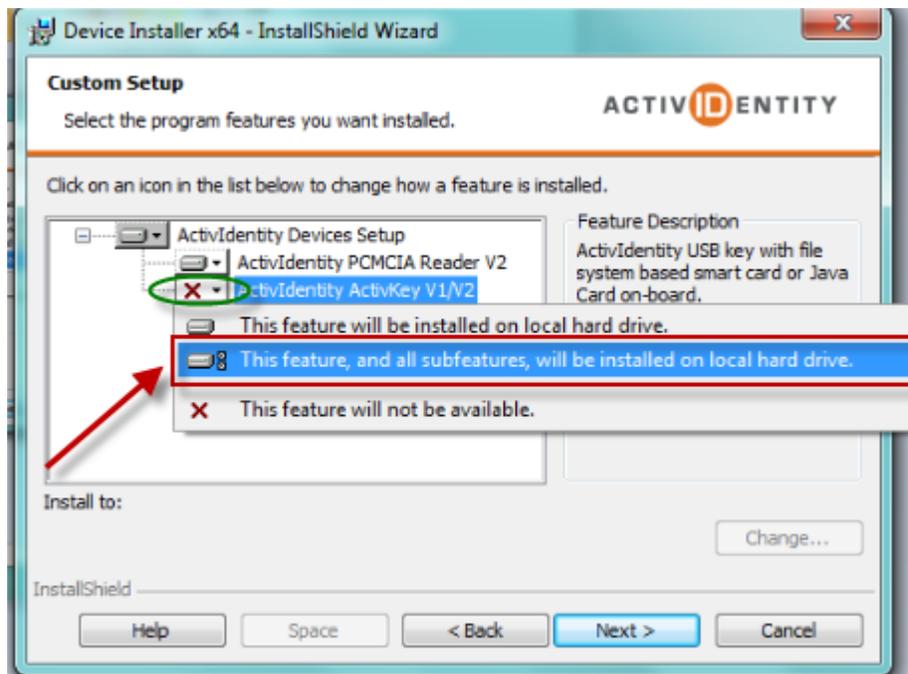
15. Review the License Agreement and select the radio button stating you have done so. Select Next.



16. Click the drop down menu for “ActivIdentity PCMCIA Reader V2” and select “This feature, and all sub features, will be installed on local hard drive.” as shown below.

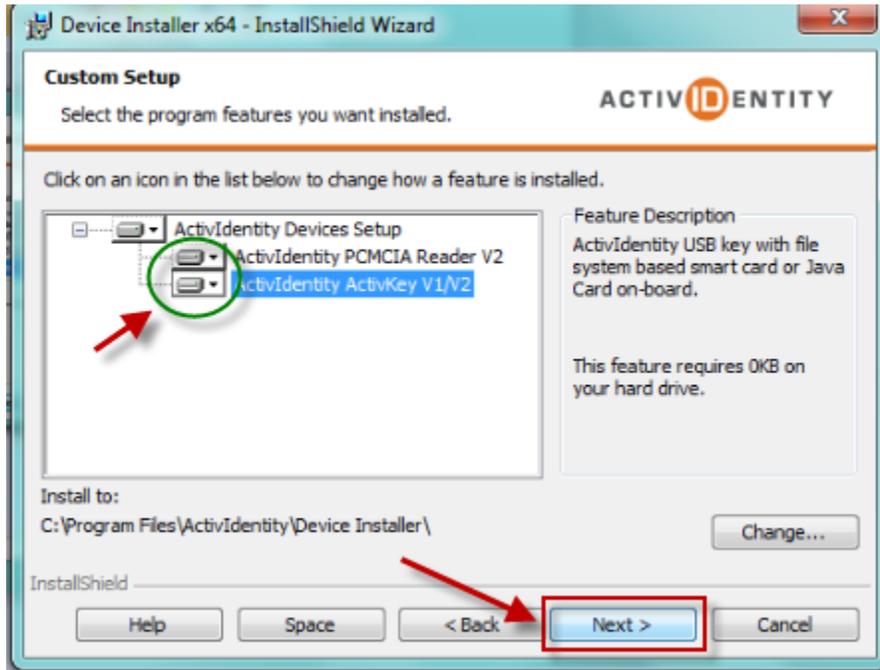


17. Click the drop down menu for “ActivIdentity ActivKey V1/V2” and select “This feature, and all sub features, will be installed on local hard drive.” as shown below.

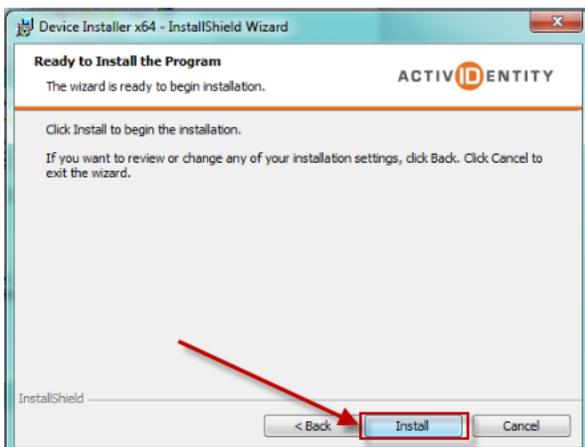




18. Select “Next” on the InstallShield Wizard.



19. Select “Install”. Once the Installation is complete, Select “Finish”.





C. Installing Root Certificates

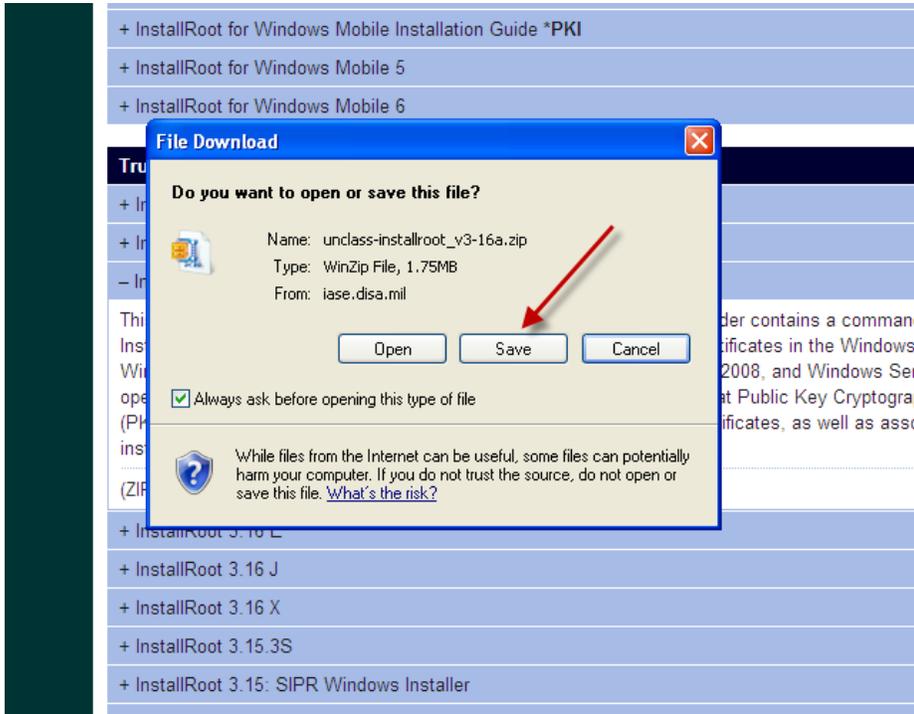
1. Go to http://iase.disa.mil/pki-pke/function_pages/tools.html and scroll down to Trust Store Management to locate “InstallRoot 3.16 A”

Trust Store Management	back to top
+ InstallRoot 3.16: User Guide	
+ InstallRoot 3.16: NIPR Windows Installer	
+ InstallRoot 3.16 A	
+ InstallRoot 3.16 E	
+ InstallRoot 3.16 J	
+ InstallRoot 3.16 X	
+ InstallRoot 3.15.3S	
+ InstallRoot 3.15: SIPR Windows Installer	
+ NSSdb CertLoader for Linux *PKI	
+ NSSdb CertLoader for Linux User Manual *PKI	
+ NSSdb CertLoader for Windows *PKI	
+ NSSdb CertLoader for Windows User Manual *PKI	

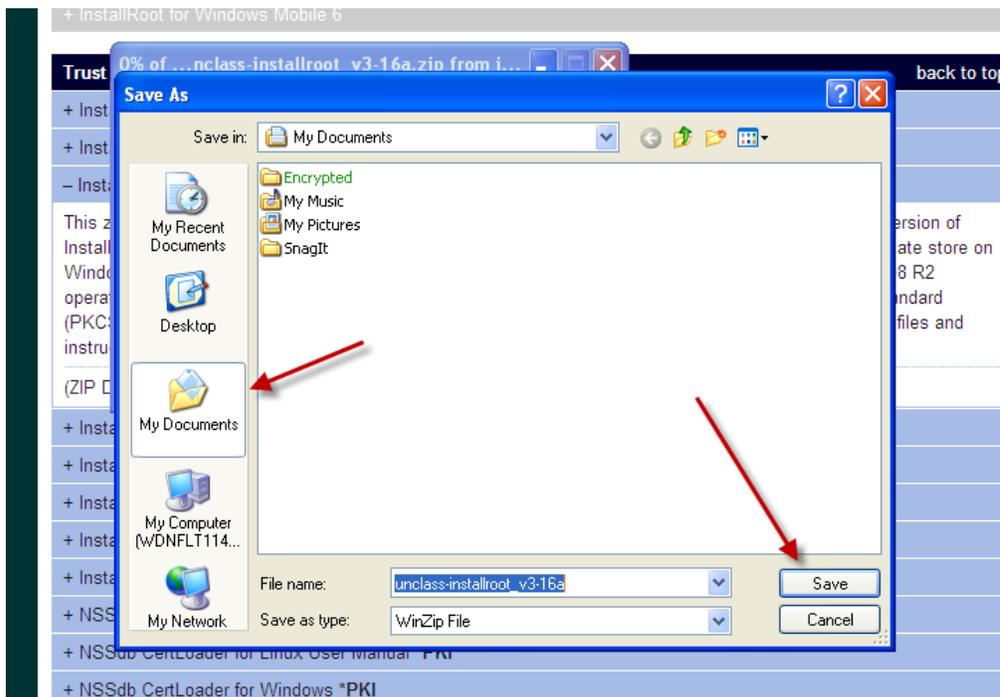
2. Expand “InstallRoot 3.16 A” and click on “(ZIP Download) Size: 1,803 KB”

Trust Store Management	back to top
+ InstallRoot 3.16: User Guide	
+ InstallRoot 3.16: NIPR Windows Installer	
- InstallRoot 3.16 A	
This zip file contains two folders: Windows and PKCS7. The Windows folder contains a command-line version of InstallRoot which installs all of the DoD PKI root and intermediate CA certificates in the Windows certificate store on Windows XP, Vista, Windows 7, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 operating systems. The PKCS7 folder contains both PEM and DER format Public Key Cryptography Standard (PKCS) #7 certificate bundles containing the DoD PKI production CA certificates, as well as associated files and instructions for validating the PKCS#7 bundles.	
(ZIP Download) Size: 1,803 KB	
+ InstallRoot 3.16 E	
+ InstallRoot 3.16 J	
+ InstallRoot 3.16 X	
+ InstallRoot 3.15.3S	
+ InstallRoot 3.15: SIPR Windows Installer	
+ NSSdb CertLoader for Linux *PKI	
+ NSSdb CertLoader for Linux User Manual *PKI	

3. A file download box will pop up asking you whether you want to open or save this file. Click “Save”.

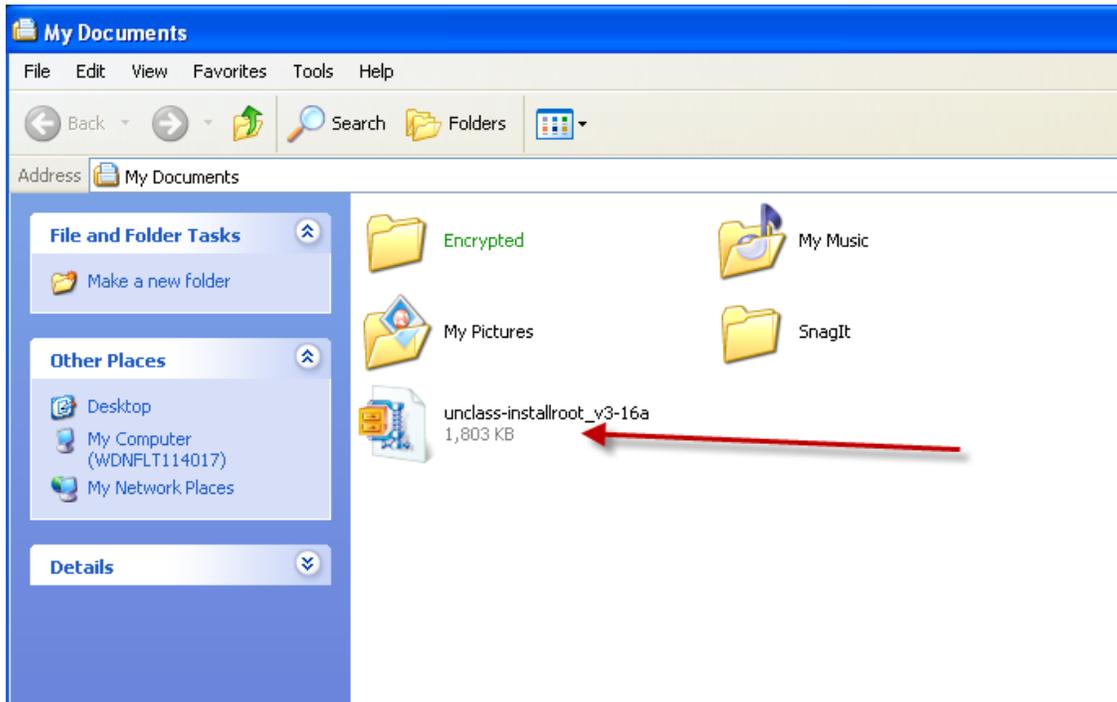


4. Save the file to your “My Documents” folder.

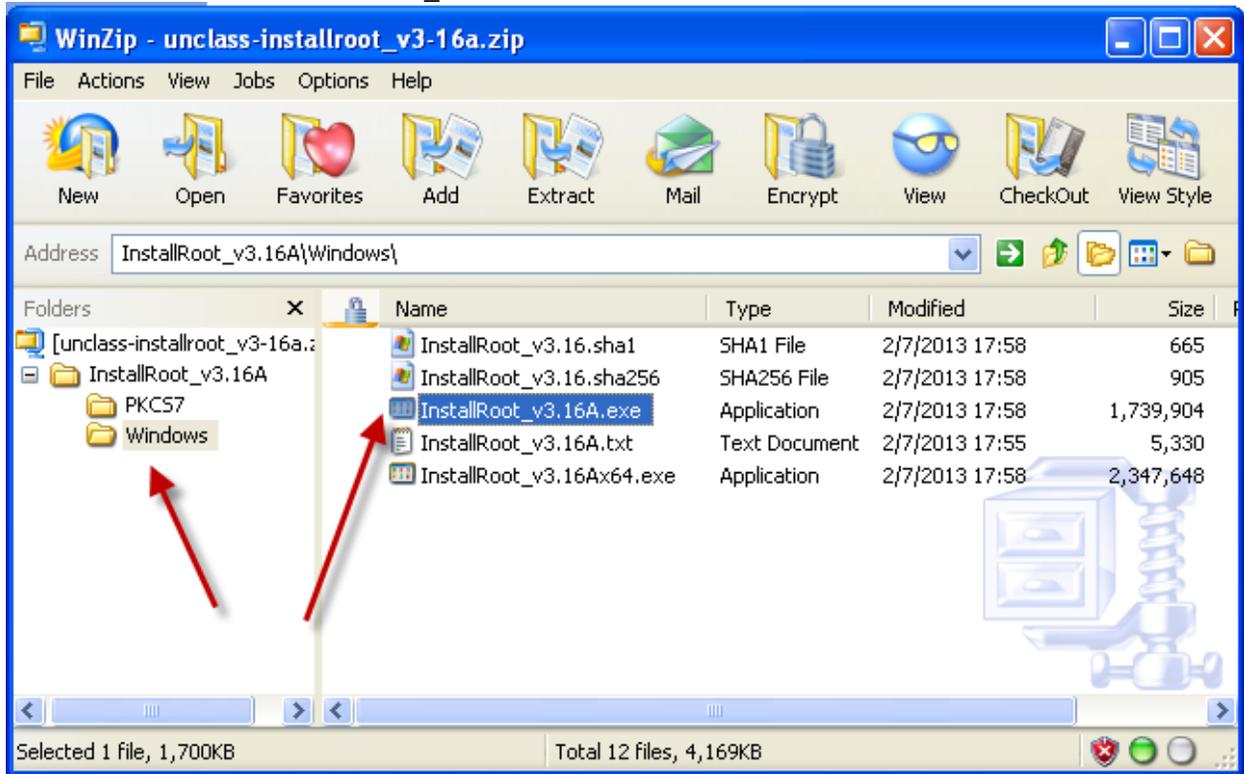




5. Go to your “My Documents” and double click “unclass-installroot_v3-16a”

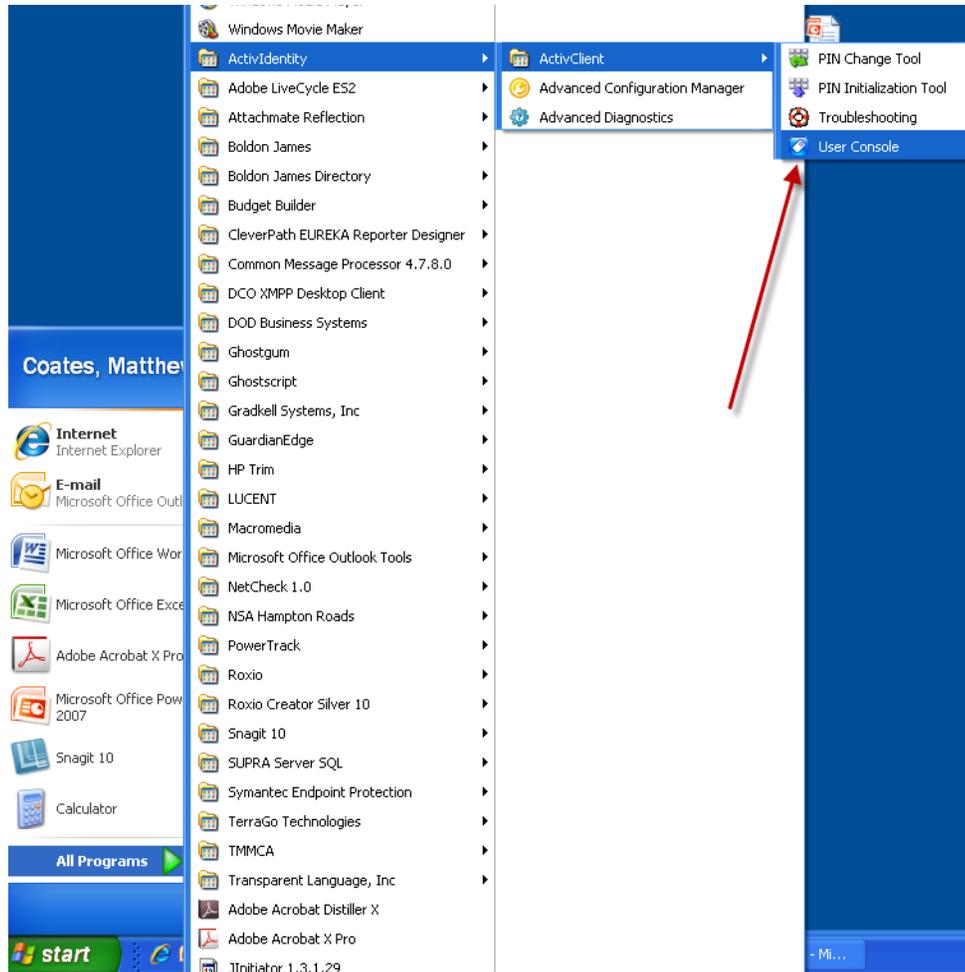


6. On the WinZip screen, navigate to the Windows folder as shown in the below diagram. Double Click on “InstallRoot_v3.16A.exe”.

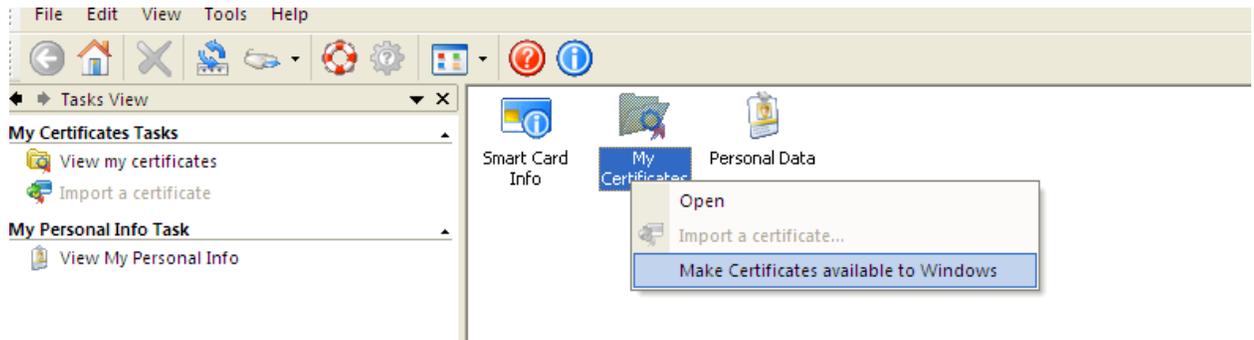




7. You will see a command prompt (black window) pop up and run a script. XP users will be fine after this. However, on WIN7 it may pop up something to the effect that "This software may not have installed correctly". The software did install correctly so there is no need to repeat installation.
8. Pull your CAC out of the CAC reader and re-insert your CAC into the reader.
9. Navigate to **Start – All Programs – Actividentity – ActiveClient – User Console** as displayed in the below image.



10. Right Click the “Certificates” icon and select “Make certificates available to Windows”



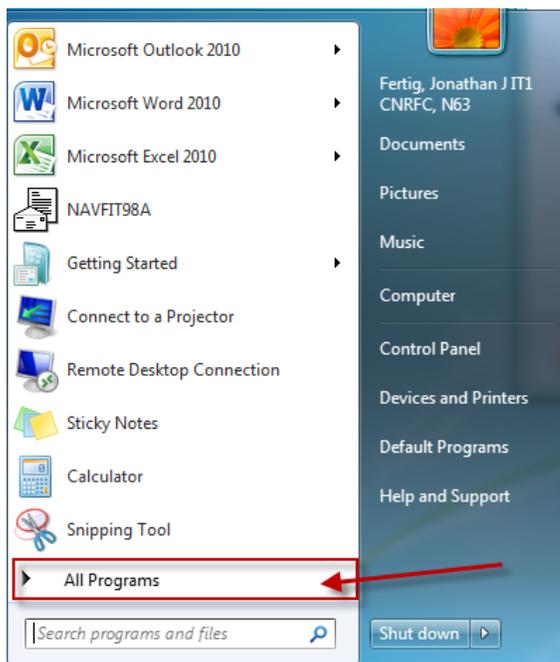
11. Select “Ok” on the popup notifying you that your certificates have been made available.

D. Configuring Internet Explorer

1. Select Start

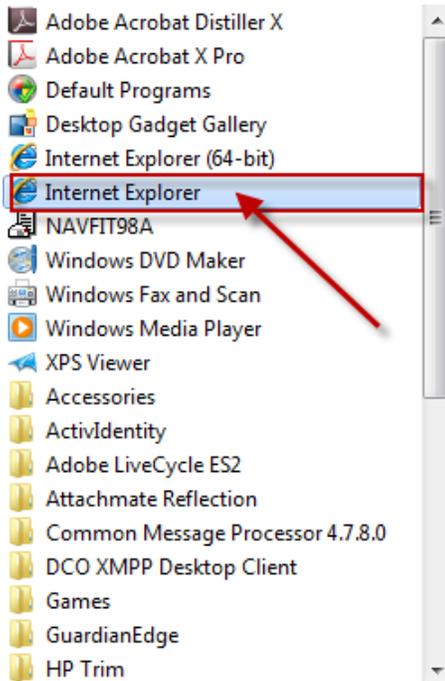


2. Select “All Programs”





3. Select "Internet Explorer"

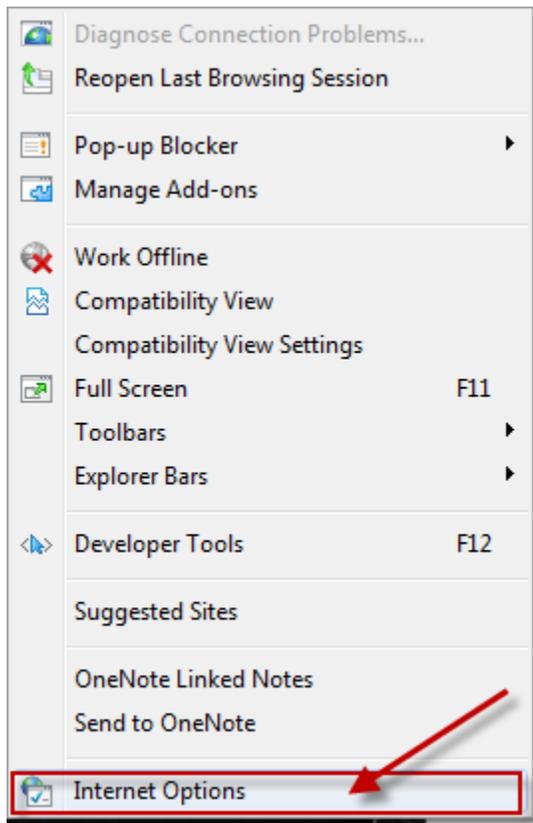


4. Select "Tools"

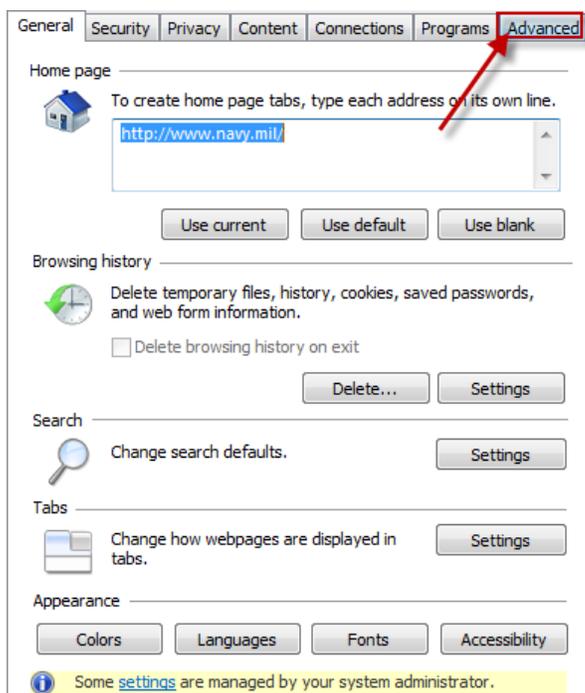




5. Select “Internet Options”

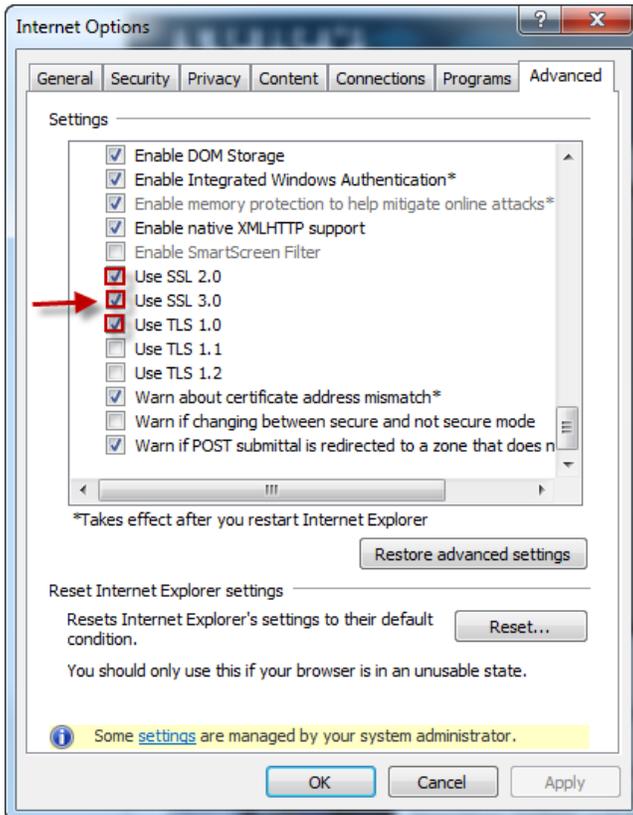


6. Select the “Advanced” tab

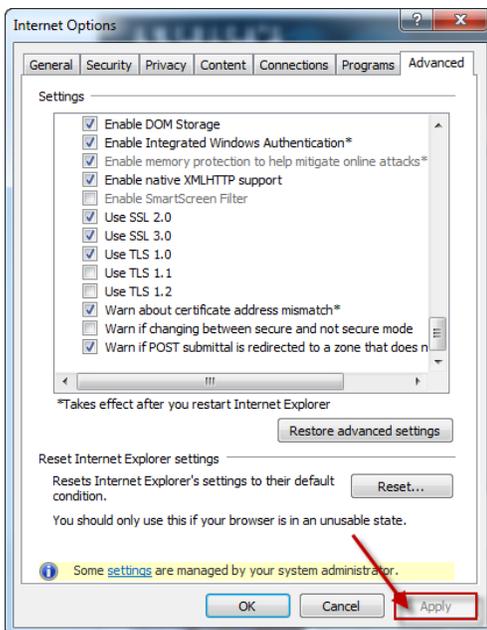




7. Ensure “TLS 1.0” “SSL 2.0” “SSL 3.0” are checked

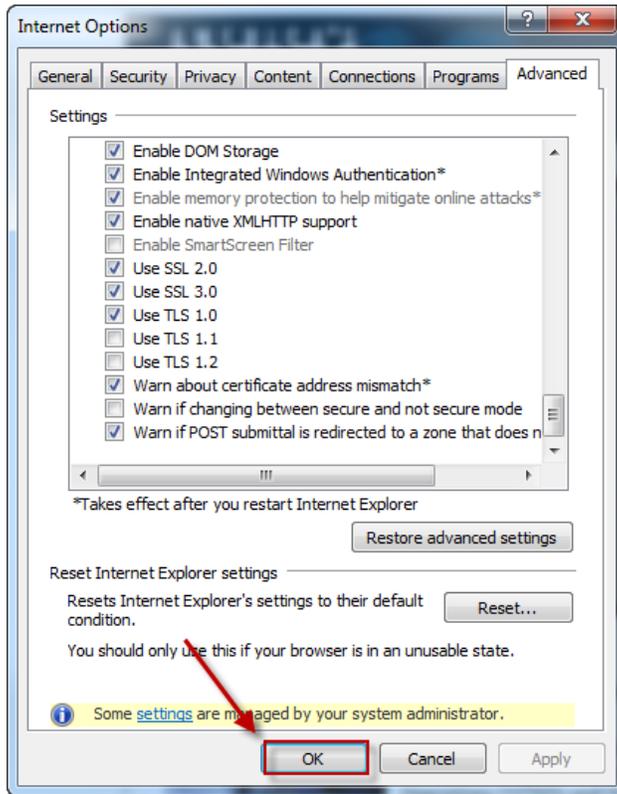


8. Select “Apply”



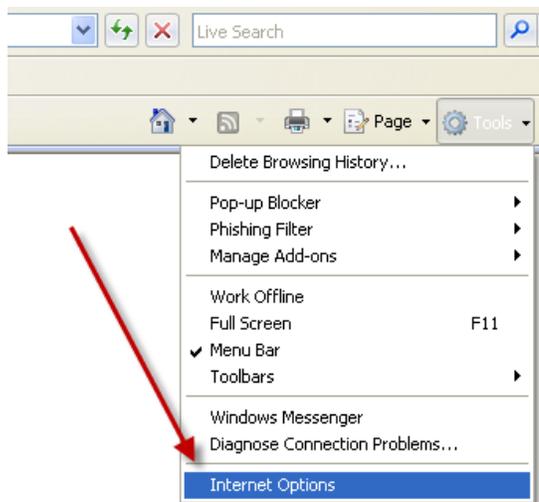


9. Select “OK”



E. Adding Sites to trusted Domains

1. Open Internet Explorer, select “Tools” and click on “Internet Options”

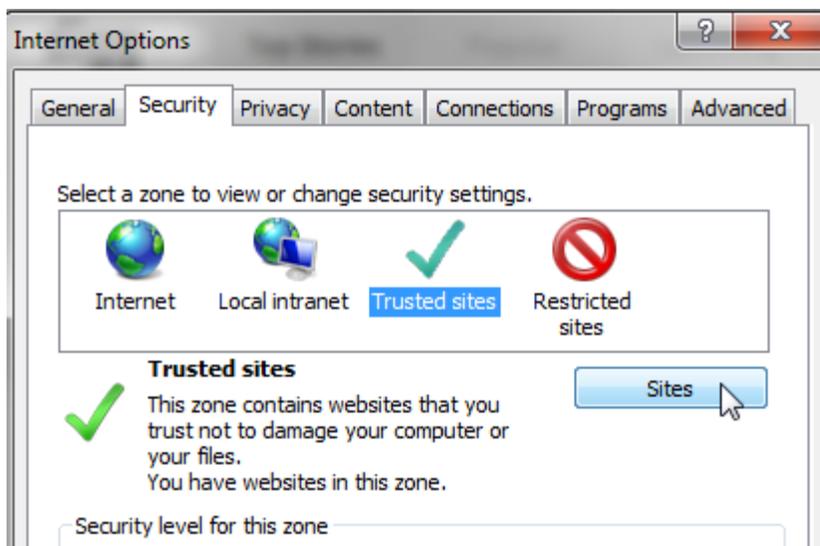




2. Click on the “Security Tab” and select Trusted Sites

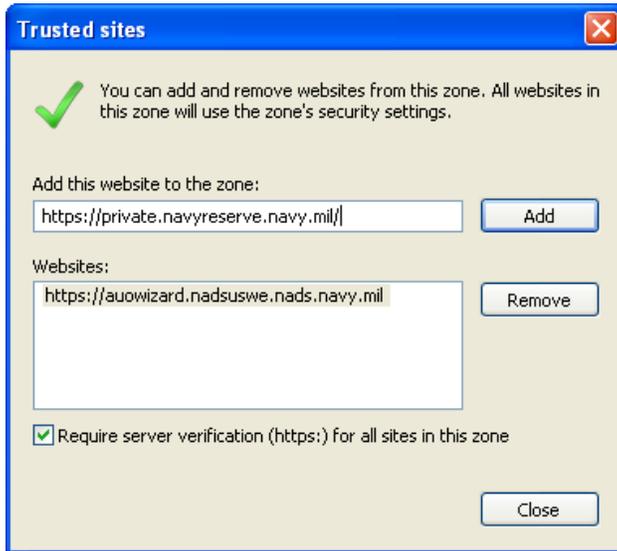


3. Click on the “Sites” button.





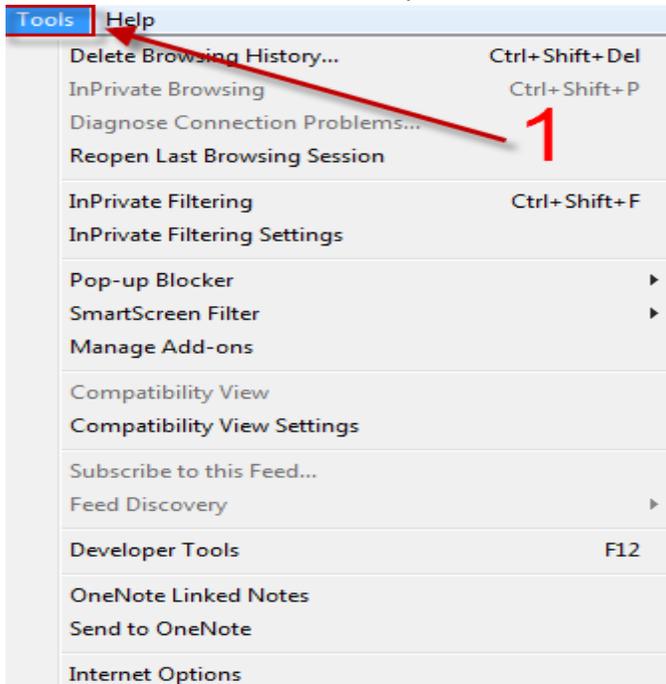
4. In the box that pops up, you can enter any sites that you are attempting to access. Simply copy the URL into the box and select “Add”. An example is below.



5. Select “Close” to save your changes.

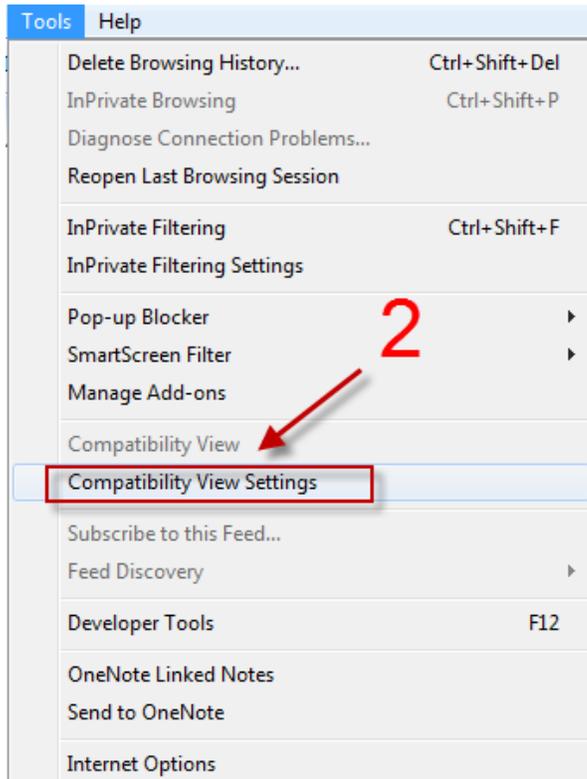
F. Adding Sites to Compatibility Mode

1. Click on the **Tools** menu/icon in your browser.

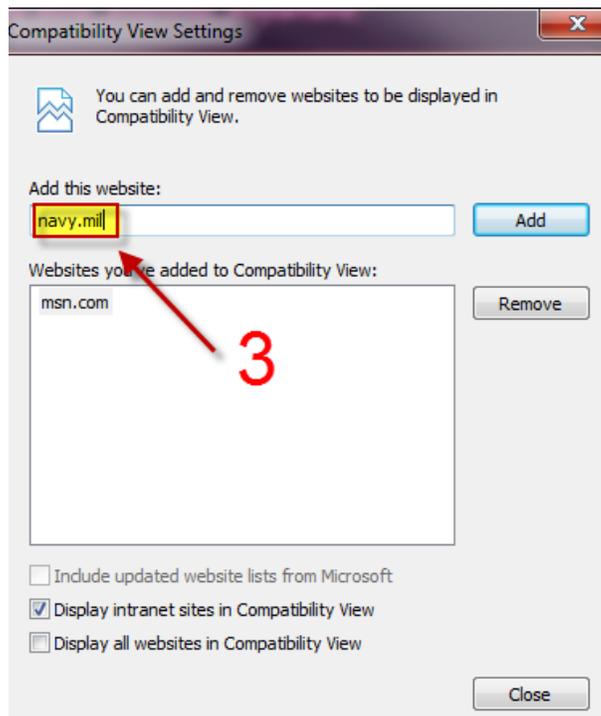




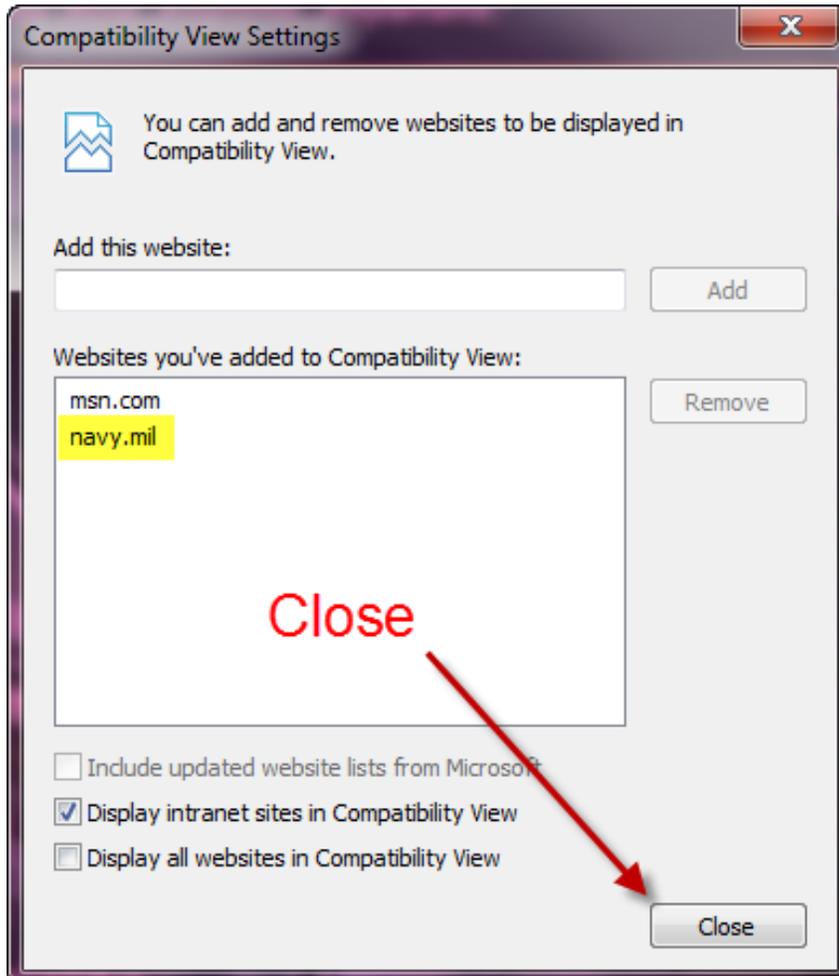
2. Select **Compatibility View Settings** from the Tools menu.



3. In the Compatibility View Settings dialog box, you need to add navy.mil and select add.



4. Click **Close** to close the dialog box.



4.1. Responsibilities:

User:

- Follow the directions outlined by this process to ensure that your CAC will work properly on your PC.
- In the event that this process does not solve your CAC installation issues, please contact COMNAVRESFORCOM N6

4.2. Systems Supported

This standard operating procedure supports the following operating systems and web browsers.

- Operating Systems
 - Windows XP (All versions)
 - Windows 7 (All versions)
 - Windows 8 (Professional edition only.)
- Web Browser
 - Internet Explorer versions 7 through 10



4.3. References

Points of Contact

- COMNAVRESFORCOM Customer Service Center
 - Commercial Number: 1-(866)830-6466
 - Email: navyreservecsc@navy.mil
- Active Client Software
<https://private.navyreserve.navy.mil/cnrfc/N-Codes/N6/Information%20Assurance/ActivClient%206.2>
- Active Client Hotfixes
<https://private.navyreserve.navy.mil/sites/HelpDesk/Software%20Library/Forms/AllItems.aspx>
- Antivirus Software
<https://infosec.navy.mil/main/home?p=5-1>
- Root Certificates
http://iase.disa.mil/pki-pke/function_pages/tools.html