Accessing DoD Enterprise Email, AKO, and other DoD websites with Internet Explorer & Edge on your Windows computer

Presented by: Michael J. Danberry

Last Revision / review: 24 October 2016

Performing these fixes "should" fix most access problems.

Personnel utilizing this guide without CACs should **only** skip the pages marked: "This page is CAC Specific." CAC holders need to follow **ALL** slides.

The most up to date version of this presentation can be found at:
http://milcac.us/tweaks

To successfully access DoD websites, you MUST install the Department of Defense (DoD) certificates

Download links and installation instructions for the InstallRoot file can be found on:

https://militarycac.com/dodcerts.htm

It will not harm your computer to run this file more than once

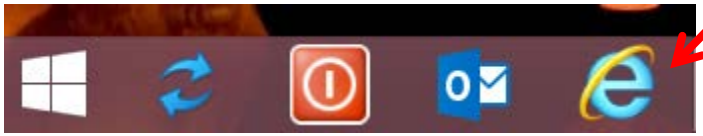
If after installation of DoD certs you see "*There is a problem with this website's security certificate*" or see red certificate errors, follow this guide: https://militarycac.com/files/dodrootca2.pdf

Open Internet Explorer (IE)
Make sure the page you are having problems accessing is **NOT** open in any tabs or another IE browser, Select *Tools,* or the gear

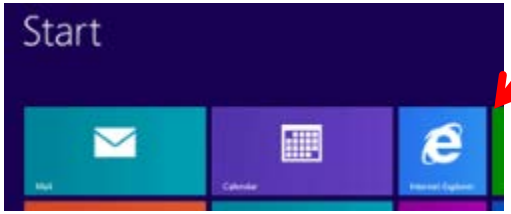
You may also click the "**Alt** & **T**" keys on your computer keyboard

Image from Internet Explorer 9, 10, & 11

Windows 8 / 8.1 users need to use the Internet Explorer from the Desktop taskbar (bottom of screen)



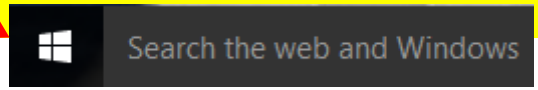
<u>NOT</u> the one from the Start tiles



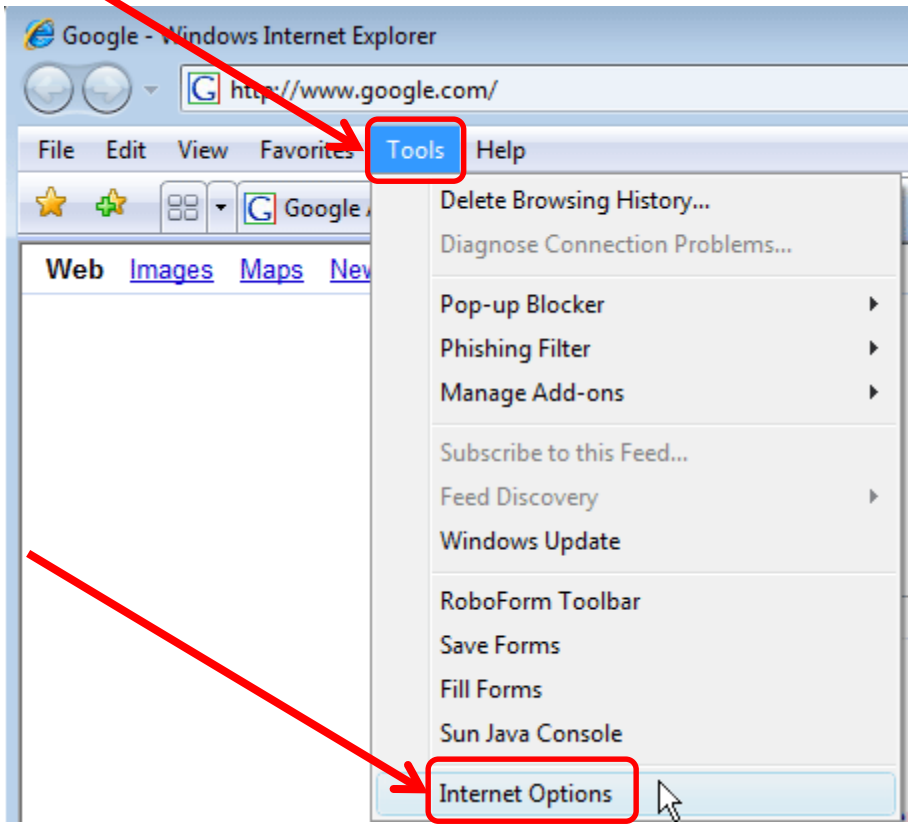
Windows 10 users go to slide <u>5</u>

Select *Internet Options* after clicking the ‘gear’

Windows 10 users [using Edge instead of IE] need to “Right click” the Windows logo in the lower left corner of screen, click *Control Panel* and select *Internet Options* (or *Network and Internet, Internet Options*). Now go to slide 7 to continue

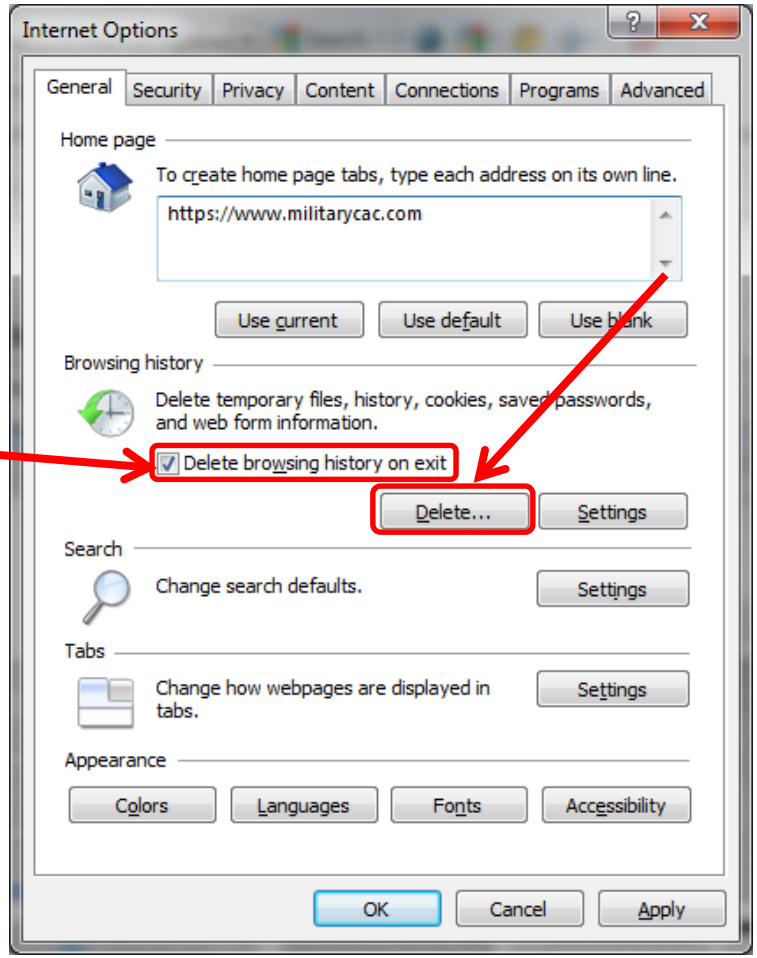


You can also select *Tools*, *Internet Options*

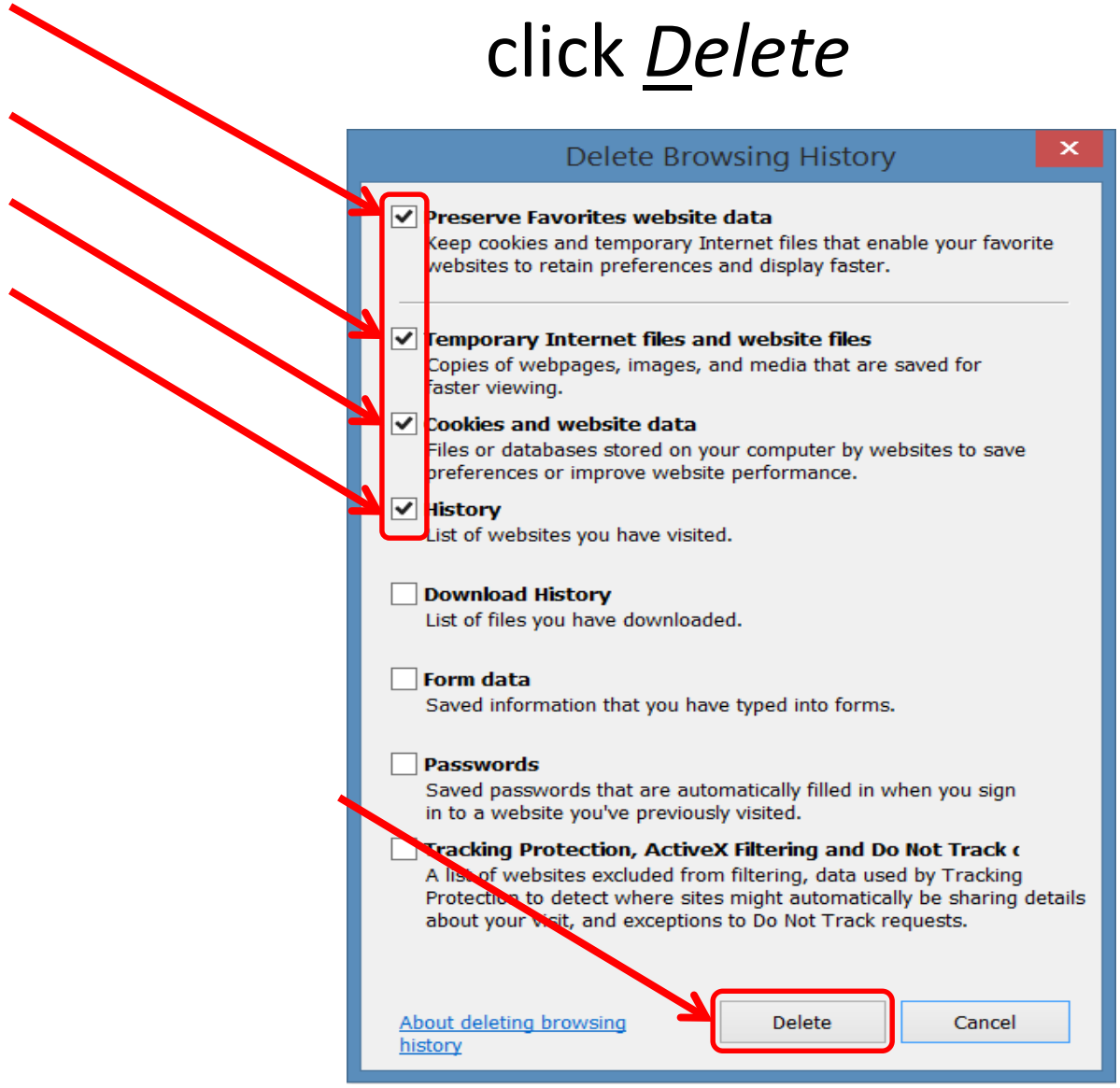


Check the *Delete browsing history on exit* (box) (IE 11 users, See note below) and then click the *Delete…* (button)

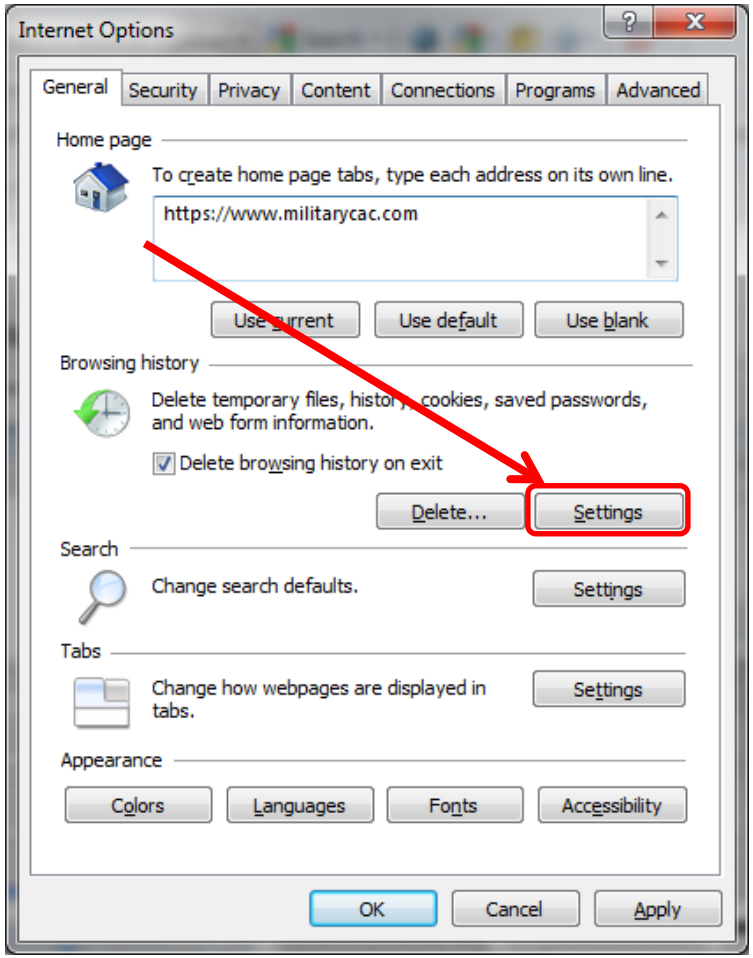
NOTE: IE 11 users may have problems if you check this box.



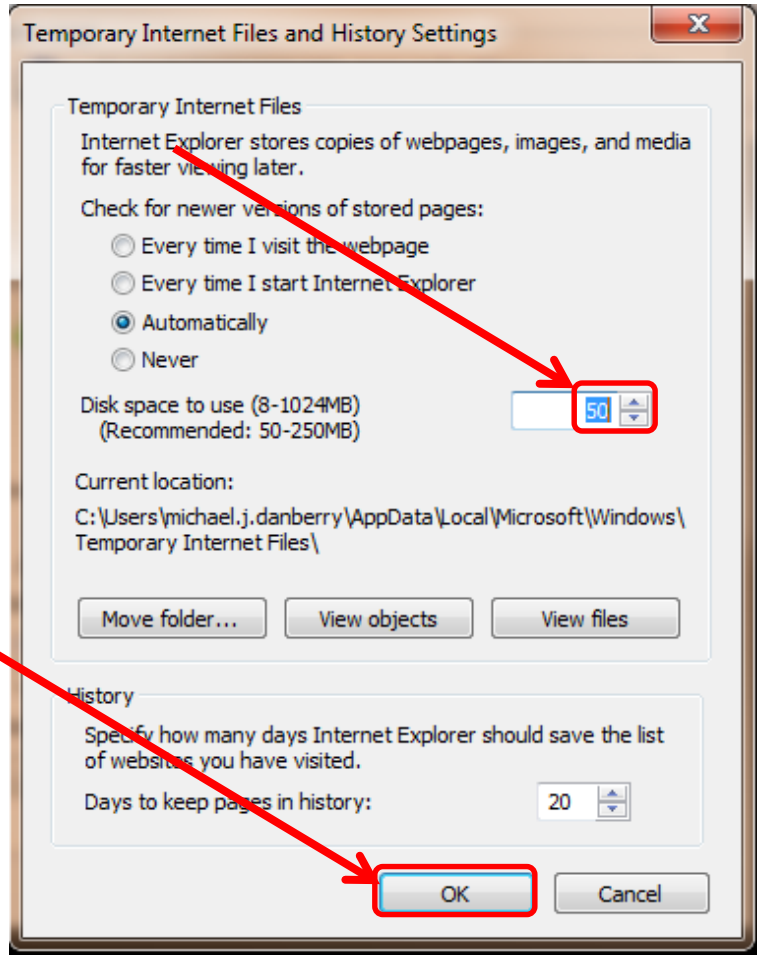
Check the top 4 boxes, leave the rest unchecked, click *Delete*



Click *Settings*

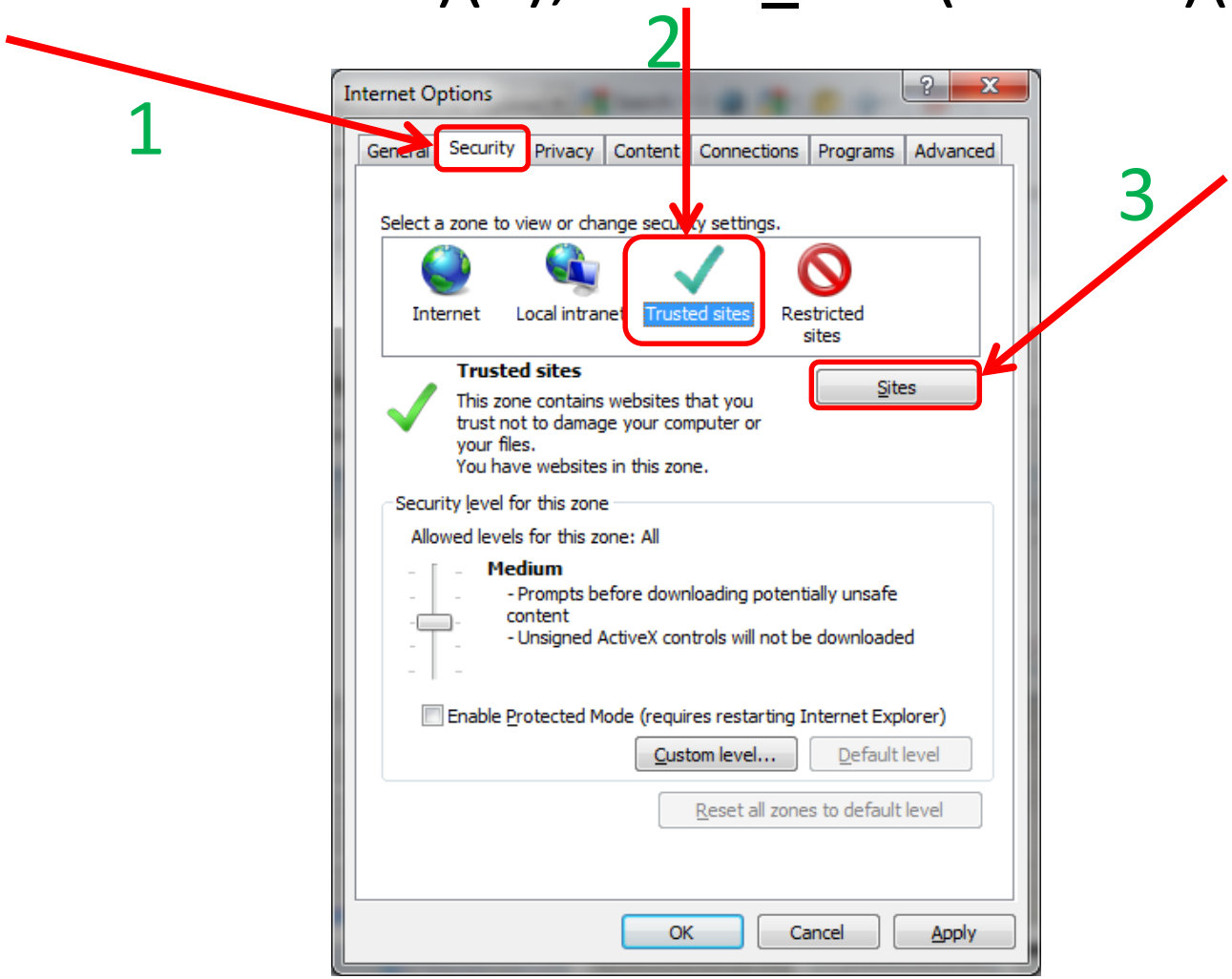


Change this number to ***50***, click *OK*



NOTE: This is my personal recommended size. Making it smaller will make your browser look for an updated page more often. The larger it is, the more web sites are being stored on your computer.

Click the *Security* (tab)(1), *Trusted sites* (green checkmark)(2), then *Sites* (button)(3)



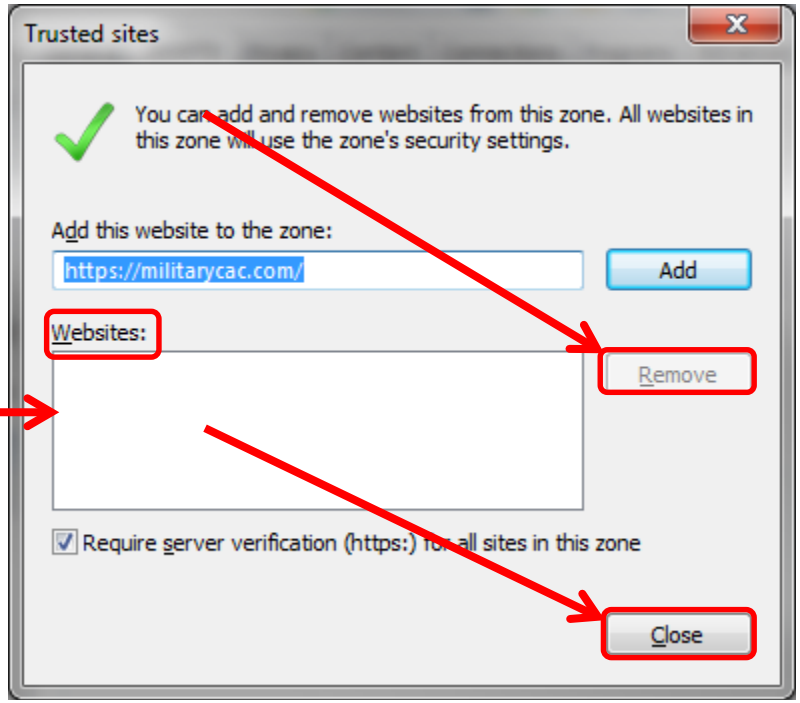
Remove all websites that end in *.mil* from the *Websites:* box by clicking the listed website, selecting *Remove*, then clicking *Close*

Exception: If you have an Oberthur 5.5 (or G&D FIPS 201) CAC on Windows 8.1 / 8 (NOT Windows 10 or 7), you may need to add websites to the zone (see Examples below - left).

Examples for Oberthur 5.5 & G&D FIPS 201 CAC holders, type in, then click Add:
https://*.mail.mil (Mail.mil)
https://*.osd.mil (DTS)
https://*.apps.mil (DCS)
https://*.navy.mil (Navy sites)

This is the *Websites:* box

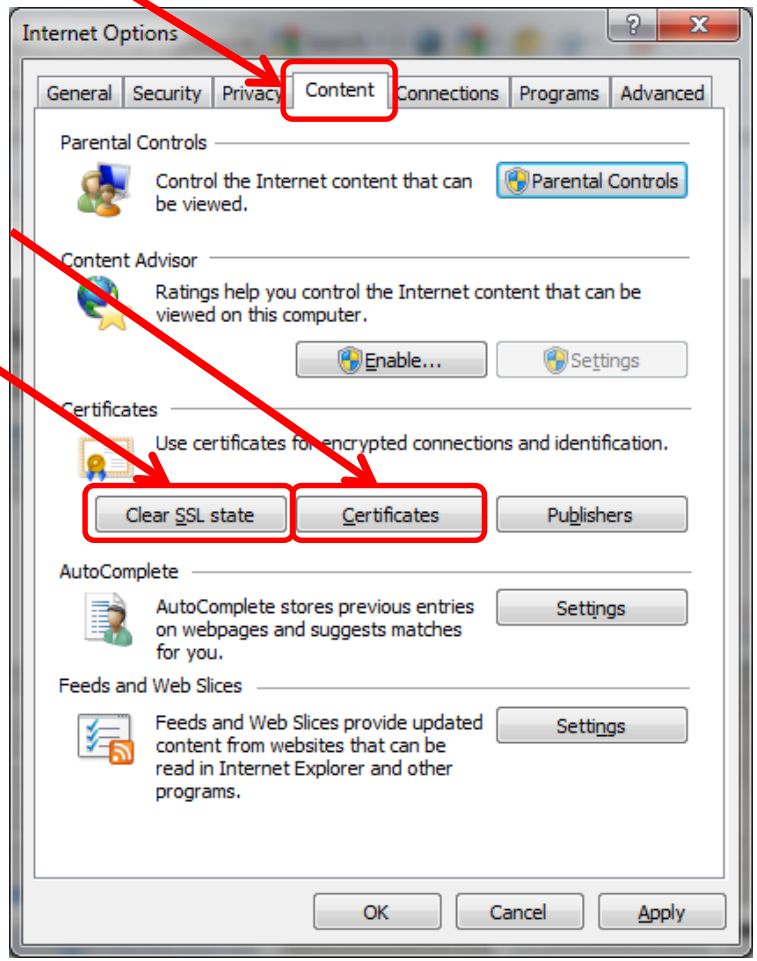
NOTE: Most Government owned computers will not let you access this area to make changes.



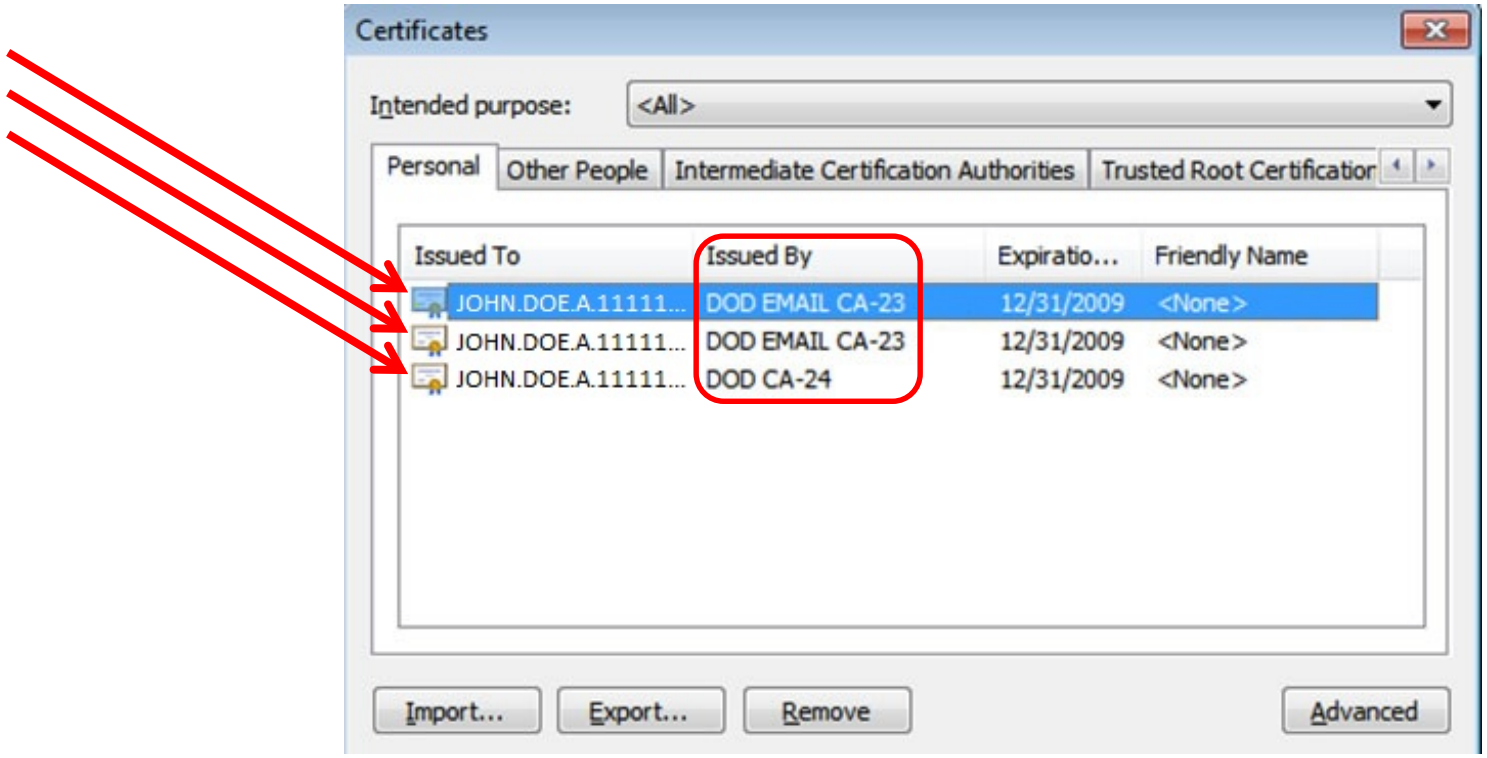
NOTE2: Some people will argue that AKO "should be" in the trusted sites. Here's what I've been able to deduce: it **WAS** needed with **IE 6 & 7**, however, if using: **IE 8, 9, 10, or 11** you will be "recycled" to the AKO home page. So, **IE 8, 9, 10, and 11** users REMOVE it. EXCEPT for Exception above.

Click the *Content* (tab), *Certificates* (button)

Click:
Clear SSL state

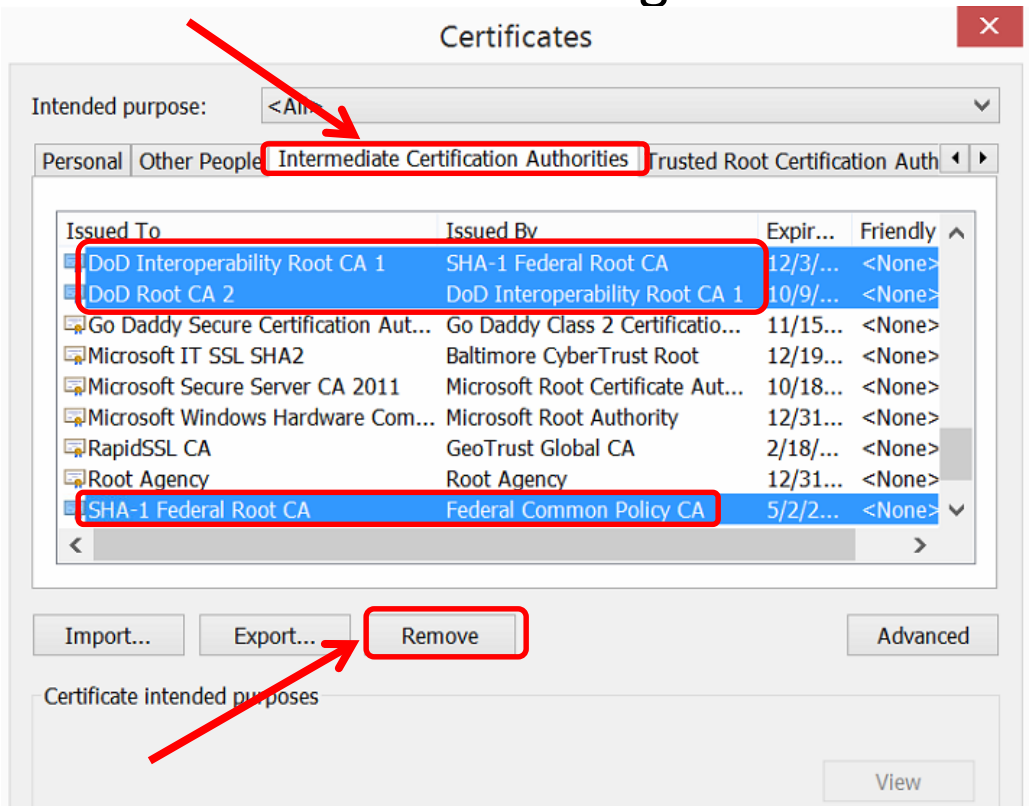


Most people will only see 3 DOD certificates (2 with EMAIL and 1 without) under the *Personal* (tab) *Issued By* (column). If you see more than 3, look at slide 23 for further instructions. Dual CAC holders will see a 4th certificate once their PIV is activated.



This page is CAC Specific

Click the *Intermediate Certification Authorities* (tab). First, verify you have DOD CA-27 through DOD ID SW CA-48 under the *Issued To* (column) (if you don't, go back to slide #2 and install the DoD Root Certificates again). Second, scroll down to below the DOD ID SW CA-48 and look for any of the certificates in the Certificates image below and any shown in the blue box. IF you see any of these certificates, select it, and click *Remove*. If you don't see it, select *Close* on this window and continue with this guide



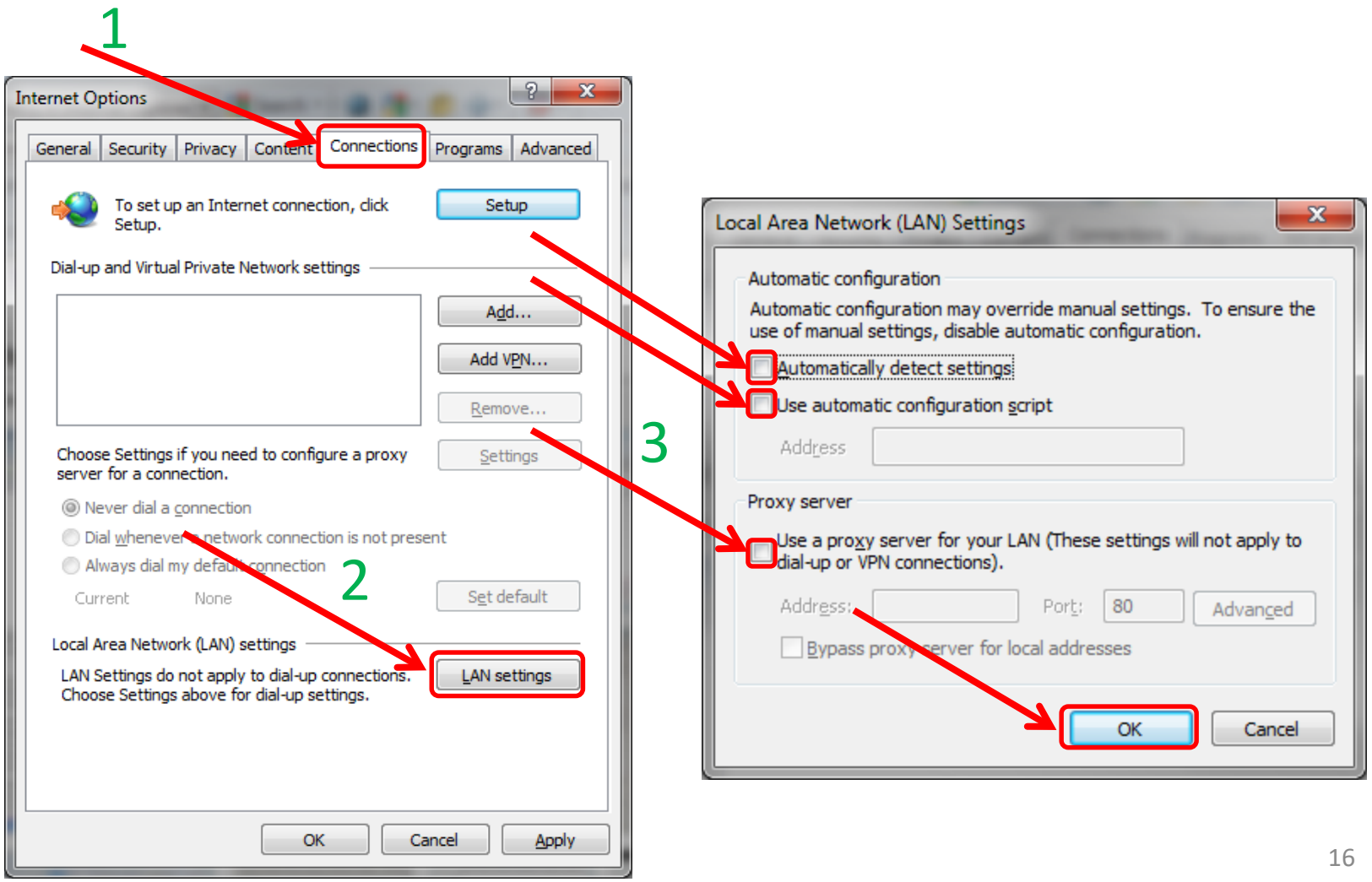
Issued To	Issued By	Expiration
Common Policy	Common Policy	
Entrust Entrust	Common Policy Entrust	
VeriSign Digital ID Certificate		Date is Expired

- Cross Cert remover Automated file (you may need to run as administrator) to remove certificates Listed above (same as slide 2):
Download from MilitaryCAC (3 MAR 16 version)
Download from DISA (3 MAR 16 version)

Another way to remove the certificates utilizing certmgr.msc This guide can be used if the method above doesn't work for you.

Information about the Cross Cert Remover

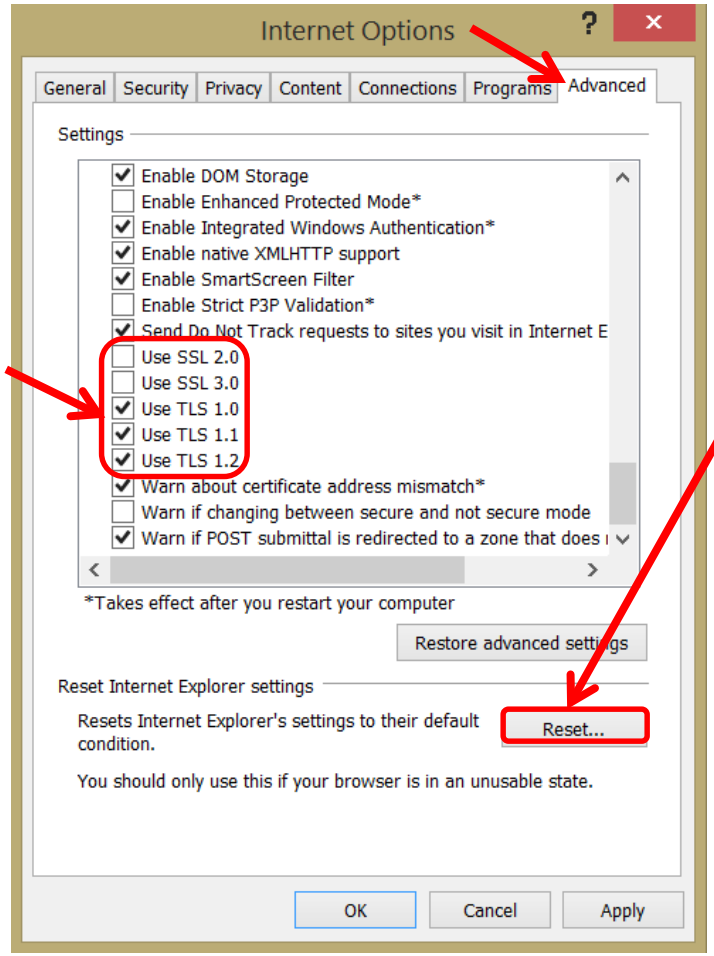
Click the *Connections* (tab)(1), *LAN settings* (button)(2), make sure ***none*** of the boxes are checked(3) (**Personal Computers only**), click *OK*



Click the *Advanced* (tab), scroll to the bottom of the list, make sure that **only** *TLS 1.0, 1.1, & 1.2* (see NOTE2 below) are checked. *SSL 2.0 & 3.0* are **NOT** checked

NOTE: If you are receiving the error: "Error 107 (net::ERR SSL PROTOCOL ERROR): SSL protocol error" or Unknown error you might need to leave SSL 2 checked. Very rare now

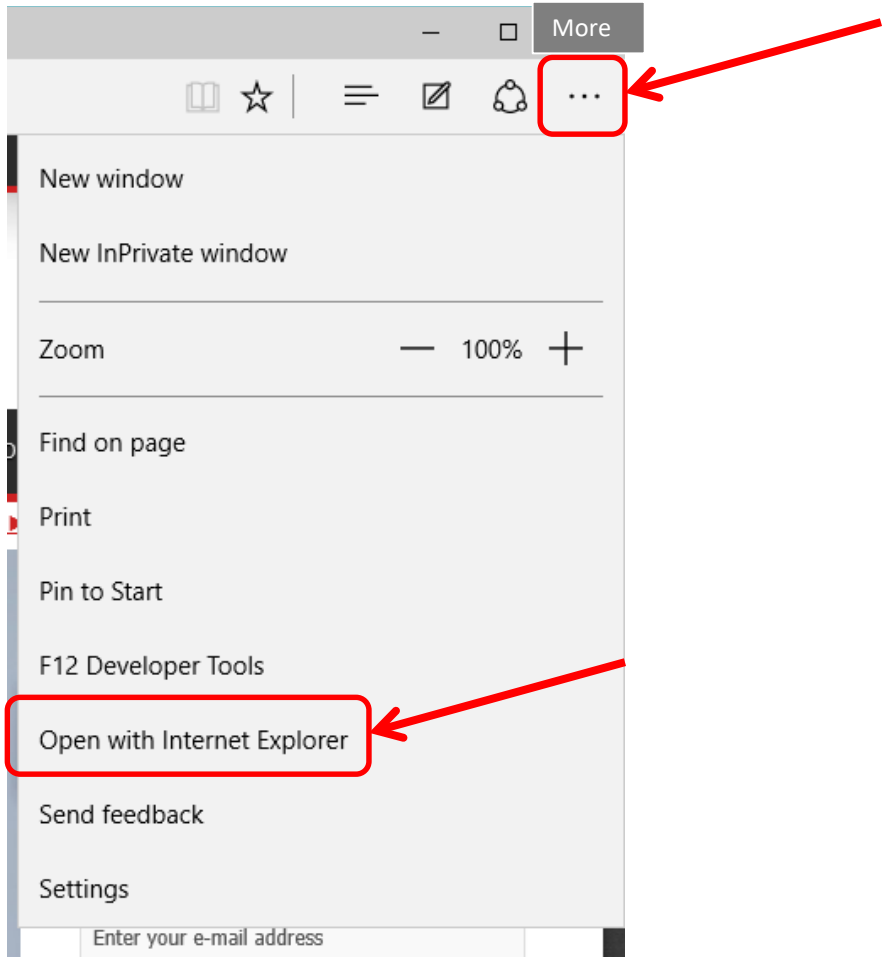
NOTE: Windows XP and Vista users will **not** see TLS 1.1 & 1.2, they are only seen on Windows 7 and above



NOTE: "Some" computers refuse to leave TLS 1.0 checked and SSL 2.0 unchecked. If this happens, click the Reset… (button).

NOTE2: The Air Force AROWS, Navy NROWS, Army's MilSuite & ALMS Websites may need TLS 1.1 & 1.2 **un**checked to be accessed. So, if you are having problems with some sites, uncheck these and try again.

When using Edge in Windows 10, select … (*More*), then select *Open with Internet Explorer*

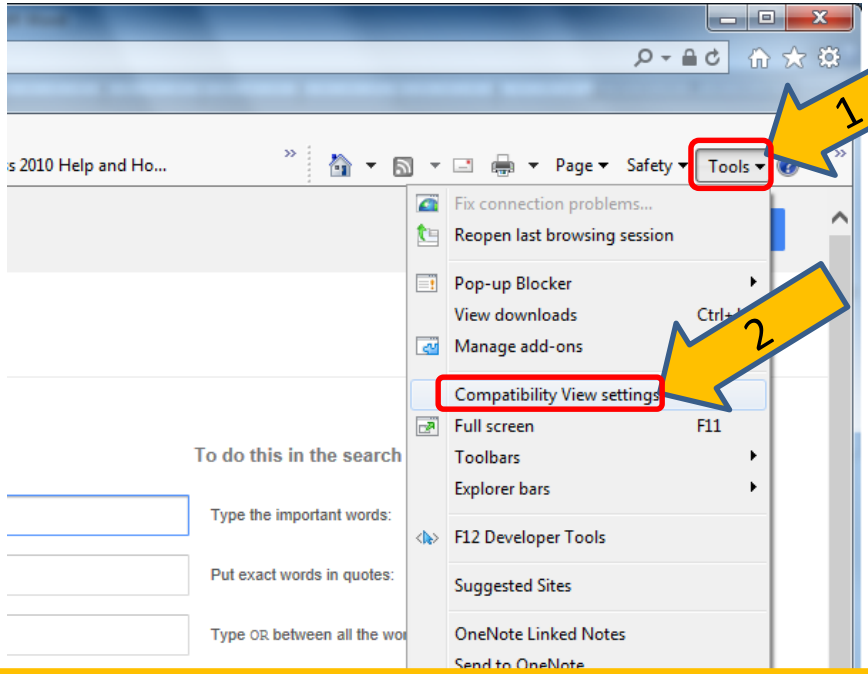


Compatibility View is necessary when using IE 10 - 11 to access some government websites like: OWA / Webmail, NKO, DTS, Army Reserve Citrix / RAP, ALMS, and others

Look for the “torn paper” icon and click it (IE 10 only)

Internet Explorer 11 users will **not** see the “torn paper.” You need to Click *Tools* (or “Alt” & “T” keys on your keyboard), *Compatibility View Settings*, and enter: “*army.mil*”, “*osd.mil*”, “*navy.mil*”, and “apps.mil” in the “*Add this website:*” box. Click *Add*, then *Close* **The next slide shows images how to do this**

Further information regarding this issue can be read on Microsoft.com
http://support.microsoft.com/kb/2866064

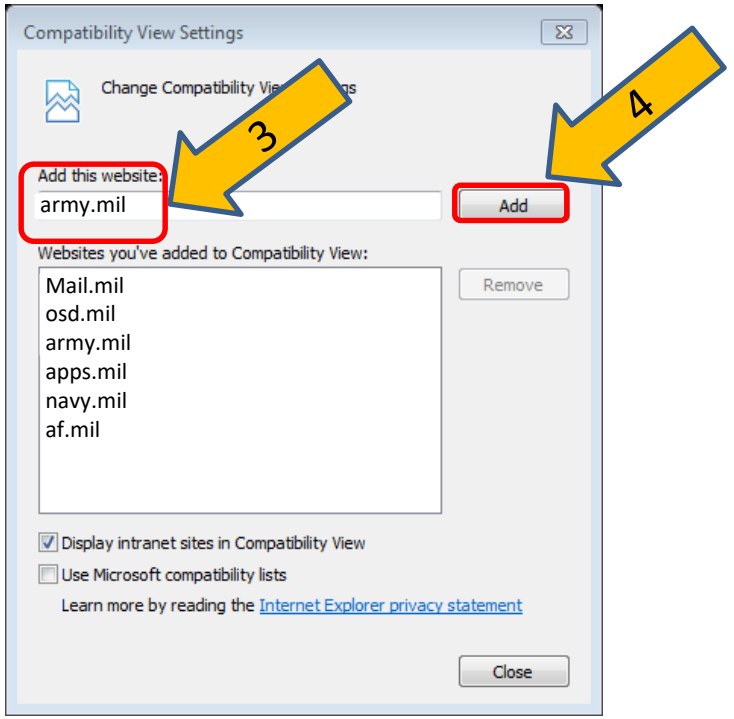


Reasons to do this:

The website worked before, but not now

Internet Explorer 11 is your browser

Add website to compatibility view



An easy way to add the site is to go to the website then click *Compatibility View settings*. The correct website should be automatically inserted into the *Add this website* (box).

DoD Enterprise Email may need **mail.mil** added

-DTS may need **osd.mil** added

-Army Reserve Remote Access Portal (Citrix), ALMS, and some other Army websites need **army.mil** added

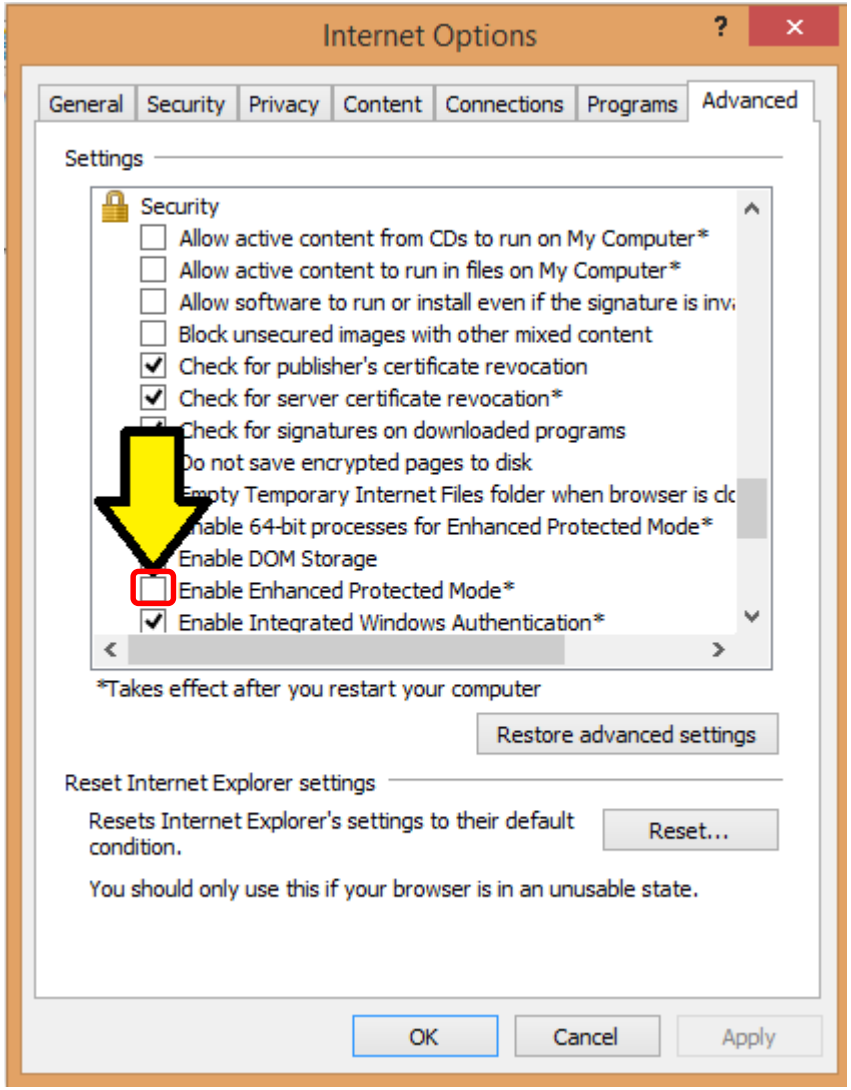
-DCS (DCO replacement) needs **apps.mil** added

-Navy personnel need **navy.mil** added

-Air Force AROWS need **af.mil** added

If you are still having issues, **uncheck** "*Enable Enhanced Protected Mode**" This is sometimes needed to sign evaluations on EES (Army's OER / NCOER system). https://evaluations.hrc.army.mil

More information available at https://MilitaryCAC.com/ees.htm

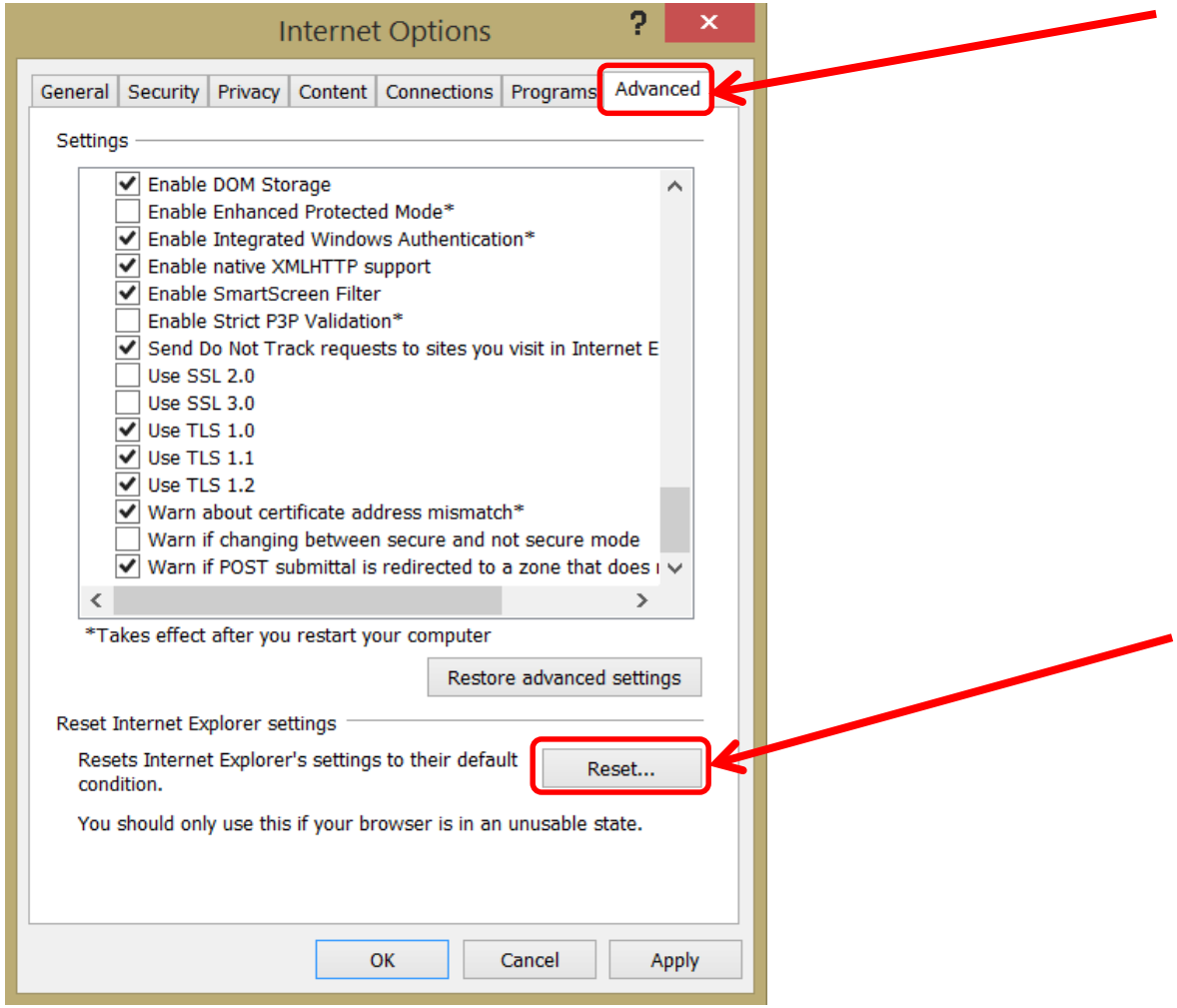


To try this option, Click *Tools*, *Internet Options*, *Advanced* (tab)

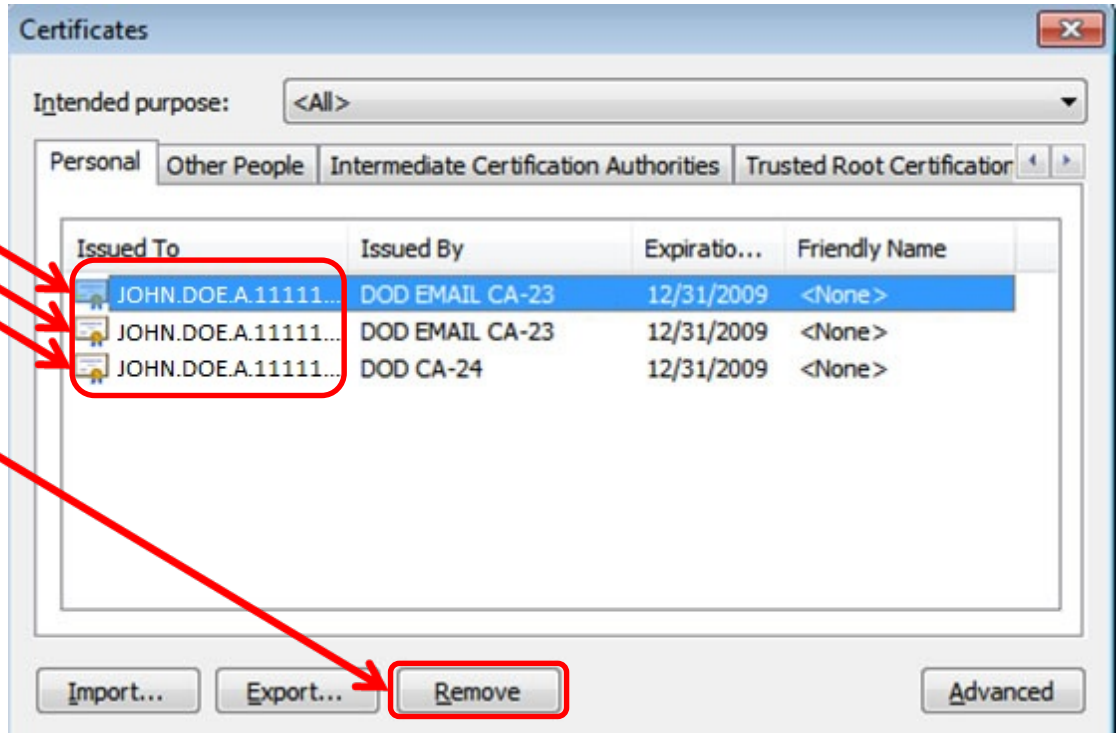
INFORMATION: Running *Enhanced Protected Mode** helps prevent attackers from installing software or modifying system settings if they manage to run exploit code. It is an extra layer of protection that locks down parts of your system that your browser ordinarily doesn't need to use.

- Unfortunately it blocks access and functionality to / on some DoD websites like HRC's EES.

If the previous adjustments did not work, select *Reset…* at the bottom of the *Advanced* (tab), AND what you see on the next page



You may need to *Remove* your certificates (see slide 14 for instructions on how to get to this location). Dual persona personnel will have 4 certs after they have activated their PIV certificate.



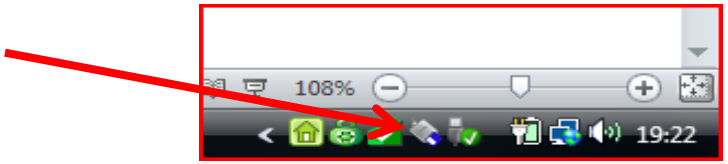
NOTE2: You will receive a message stating: *You cannot decrypt data encrypted using the certificates.* Select: ***Yes***

NOTE: Removing certs and your CAC, then reinserting CAC is a way to test if your reader and middleware are working properly.

This page is CAC Specific

Your certificates “should” automatically be available to Windows when you remove and reinsert your CAC into the reader, however…

- If you have ActivClient 6.2.0.x installed.. You can double click the ActivClient icon (by your clock in the lower right corner of your screen) now *go to slide 26*



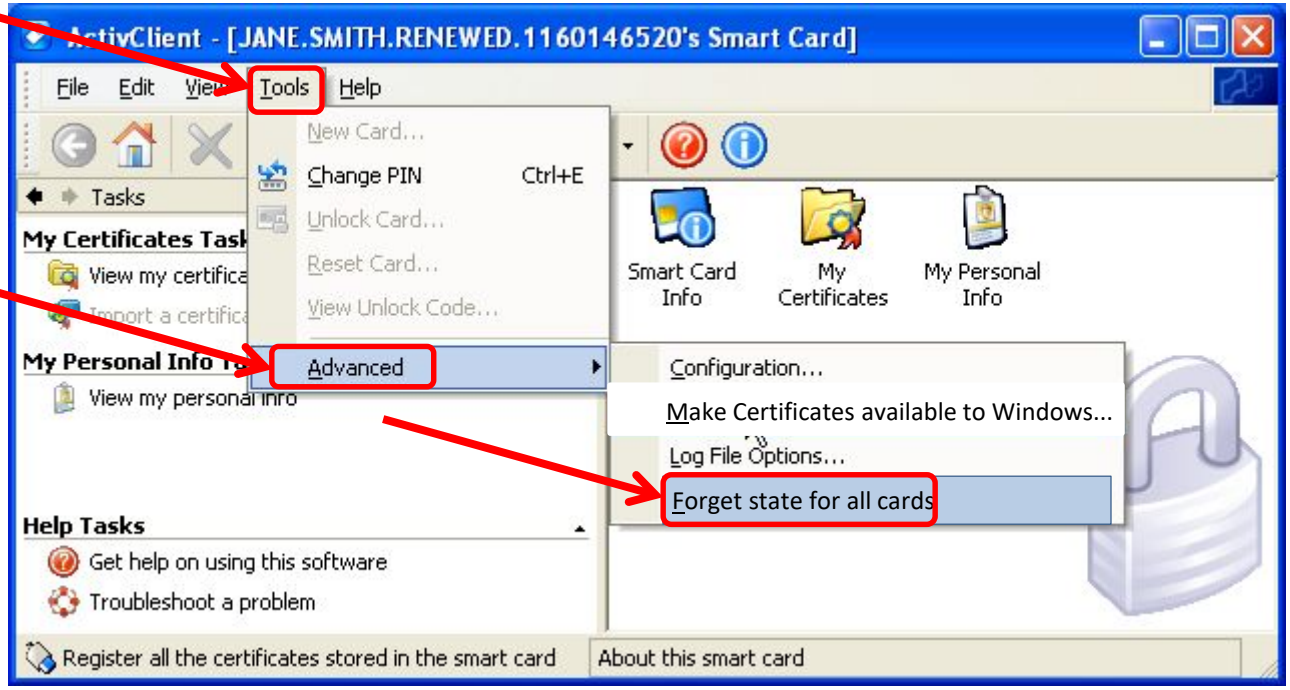
- If you don’t see it there: Windows Vista & 7 users can Click Start / Windows logo, All Programs, ActivIdentity, ActivClient, User Console. *Now go to next slide*

- Windows 7, 8 / 8.1, & 10 native users will not see an ActivClient icon, since you are not using it.

This page is CAC Specific

Forget state for all cards in ActivClient 6.2.0.x, this helps Dual CAC holders immediately after a PIV activation

- Click *Tools*, *Advanced*, *Forget state for all cards (twice)*

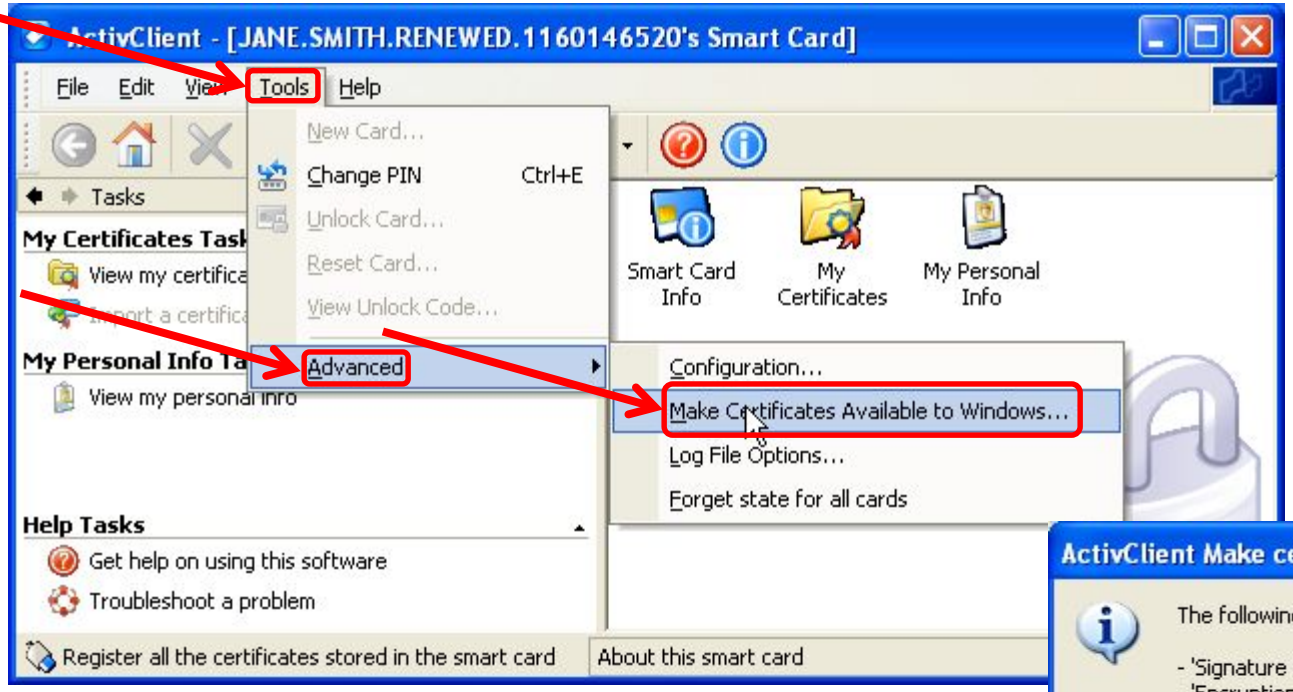


Go to next page to Make Certificates available to Windows

This page is CAC Specific

How to make your certificates available to Windows when using ActivClient 6.2.0.x

- Click *Tools*, *Advanced*, *Make Certificates available to Windows*



You should see this message

This page is CAC Specific

Try these additional items if you are still having issues:

Try using the 32 bit version of Internet Explorer (if you have 64 bit Windows) Please know that IE runs in 32 bit mode by default if you are using IE 10 or IE 11 in Windows 7, 8 / 8.1, & 10

NOTE: In some occasions, your time on your computer may be off by more than the server's 5 minute limit. Please check your clock and time zone.

Try logging into a CAC enabled DoD website with your CAC, it "should" now work

If all of the previous ideas did not work, please visit: https://militarycac.com/cacdrivers.htm to start troubleshooting your CAC reader

Presentation created and maintained by:

Michael J. Danberry

https://MilitaryCAC.com

If you still have questions, visit:

https://militarycac.com/questions.htm