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

Presented by: Michael J. Danberry

Last Revision / review: 31 August 2021

Performing these fixes "should" fix most access problems.

Personnel utilizing this guide without a CAC 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:
https://milcac.us/tweaks

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

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

https://militarycac.com/dodcerts.htm

If after installation of the DoD certs you [still] see "*There is a problem with this website's security certificate*"

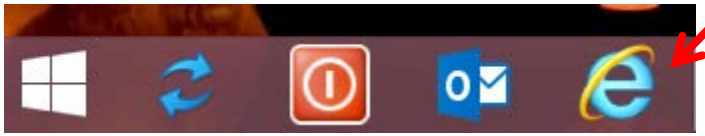
or you see red certificate errors,

follow this guide: https://militarycac.com/files/dodrootca2.pdf

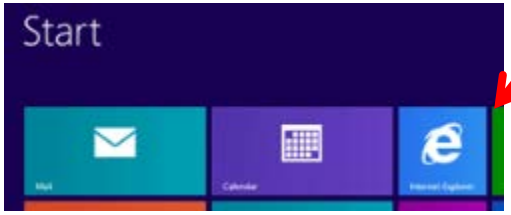
Open Internet Explorer (IE) [Make sure the page you are having problems accessing is **NOT** open in any tabs or another IE browser], Select the gear

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

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



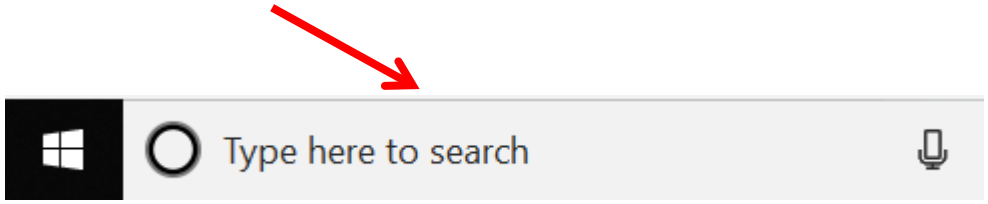
NOT the one from the Start tiles



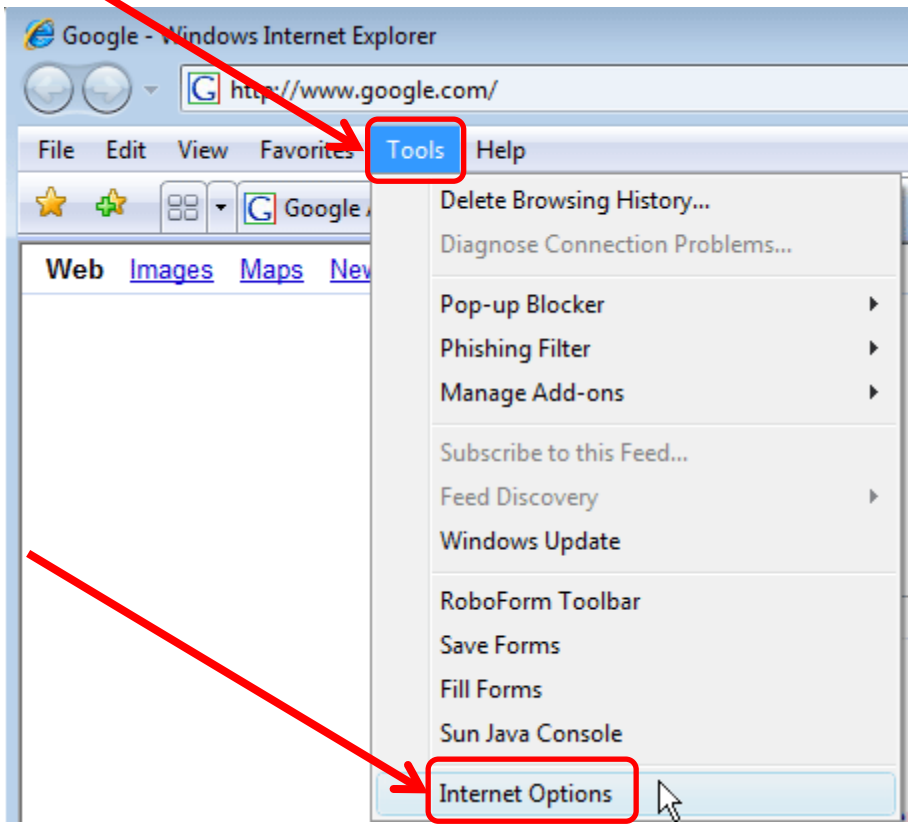
Windows 10 & 11 users go to slide 5

Select *Internet Options* after clicking the 'gear'

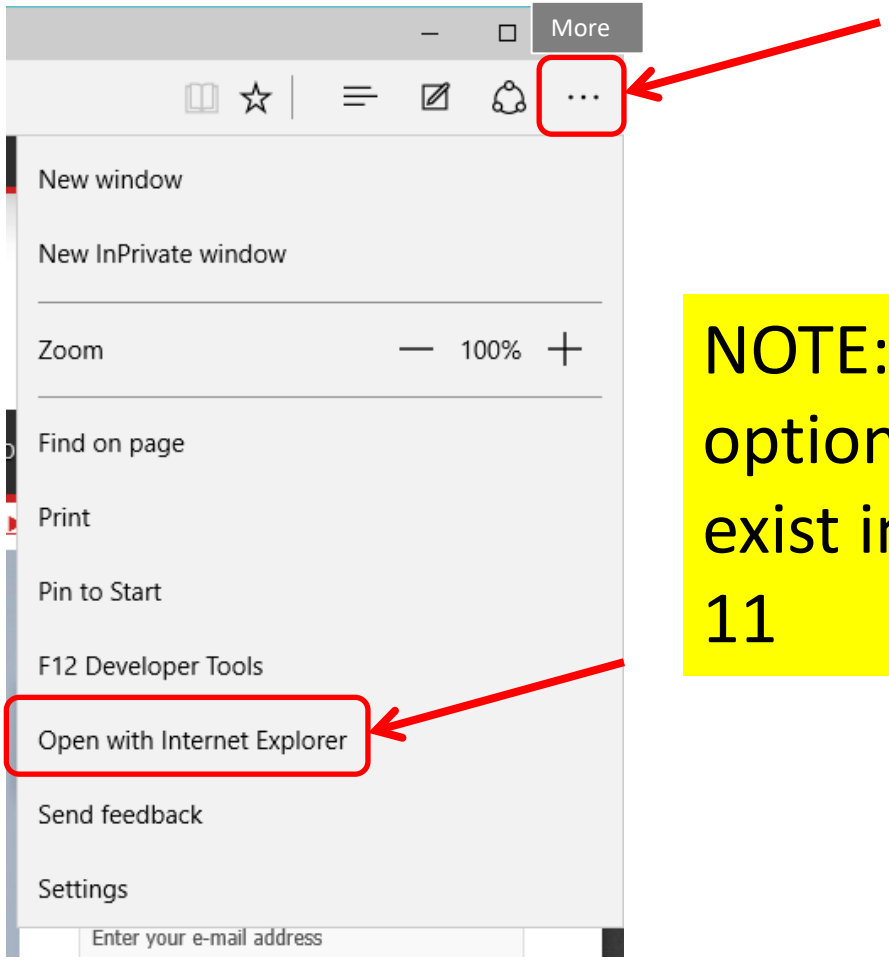
Windows 10 & 11 users need to type "Internet Options" in the "Type here to search" box and select *Internet Options Control Panel.* You may now skip to slide 7 to continue



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



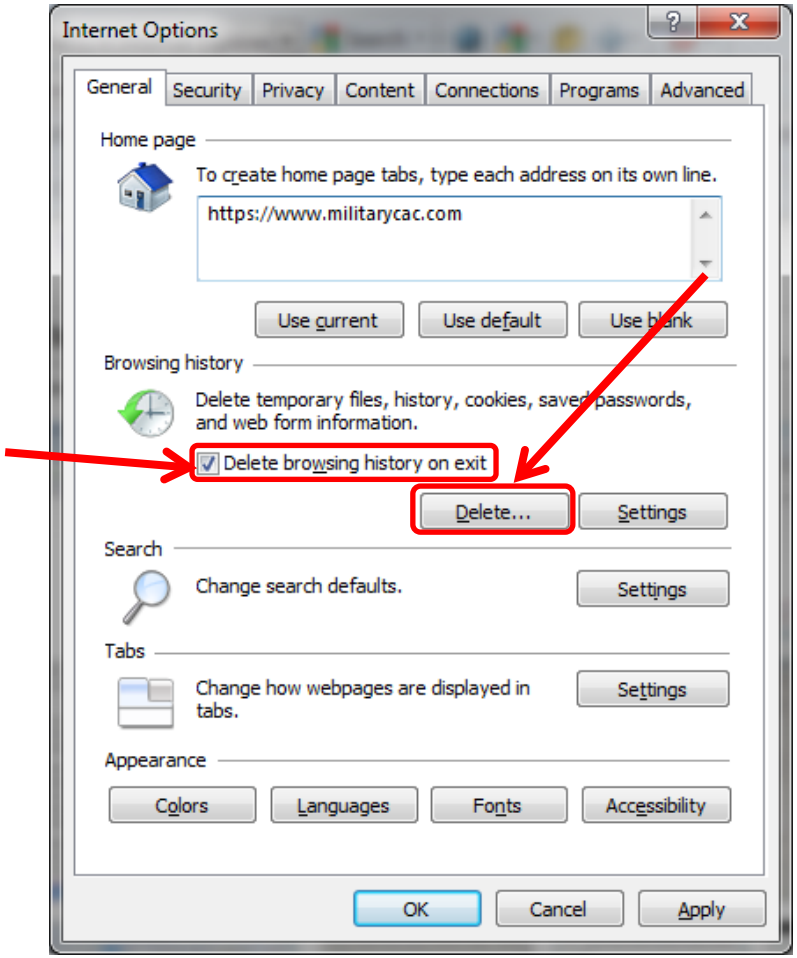
When using Edge in Windows 10, you may select … (*Settings and More*), then *Open with Internet Explorer*



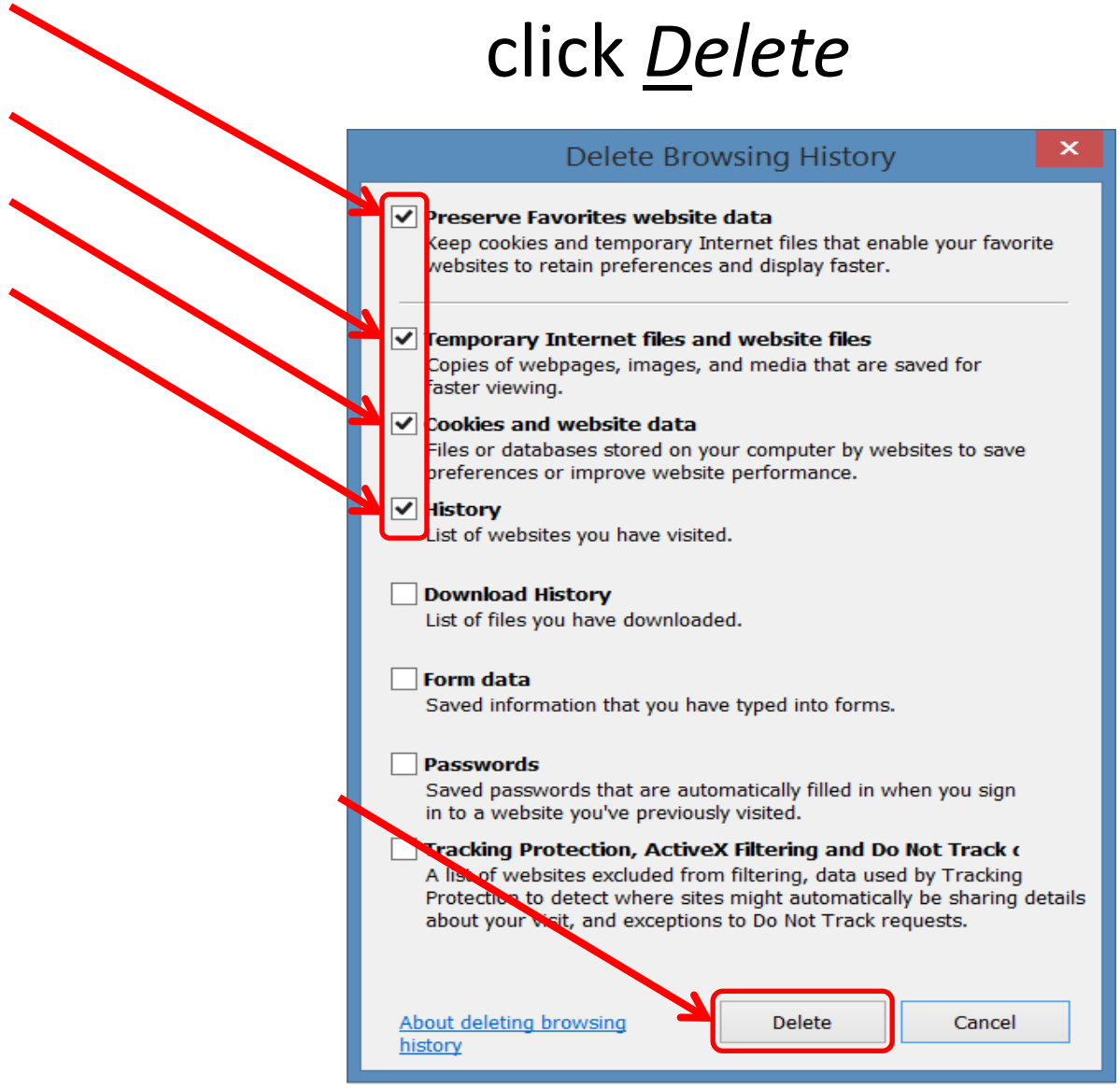
NOTE: This option does NOT exist in Windows 11

Check the *Delete browsing history on exit* (box), click *Delete…*

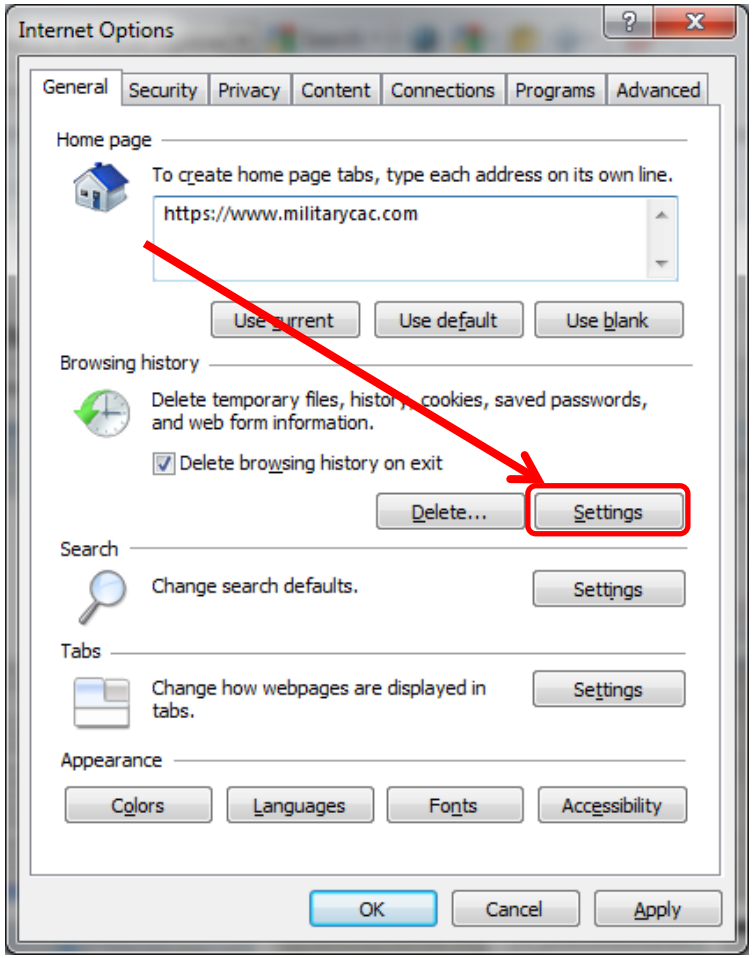
NOTE: "A few" IE 11 users have experienced problems when checking this box.



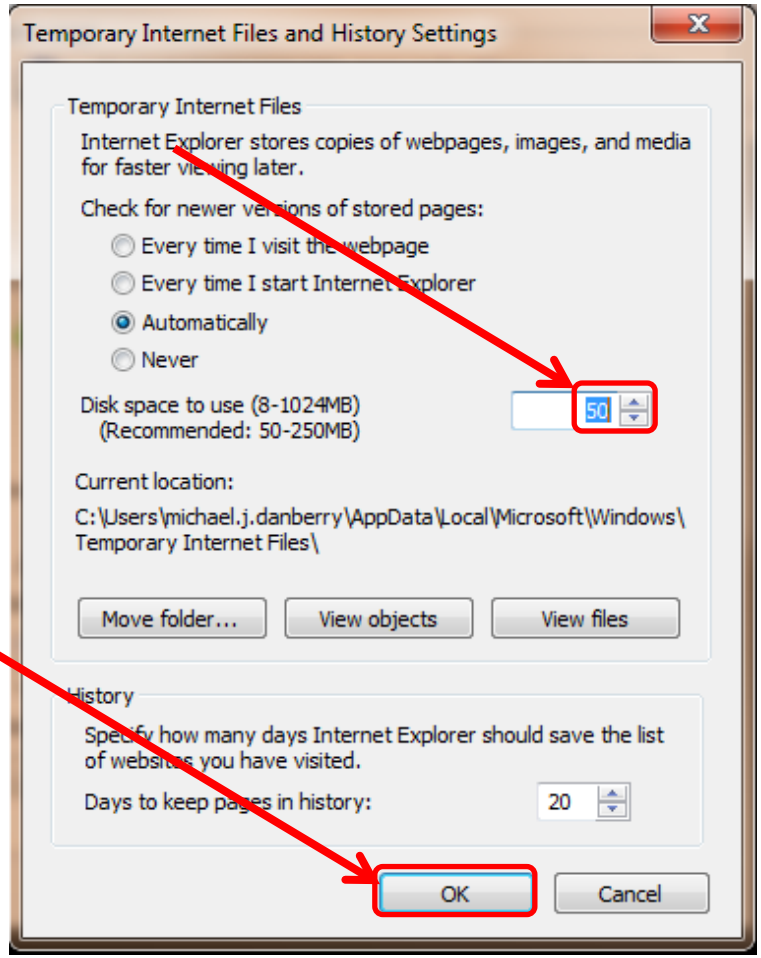
Check the top 4 boxes, leave the rest unchecked, click *Delete*



Click *Settings*

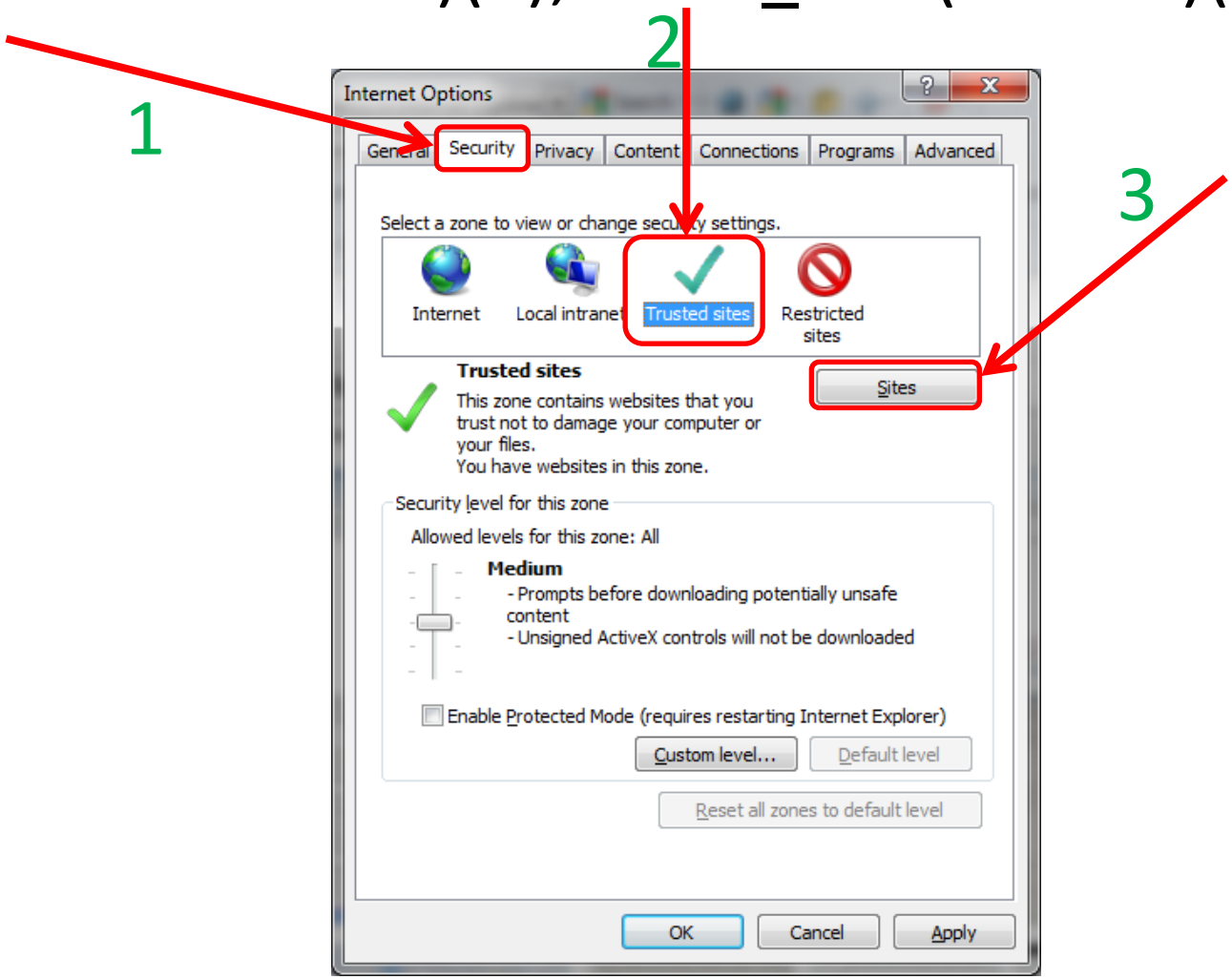


Change this number to ***50***, click *OK*



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.

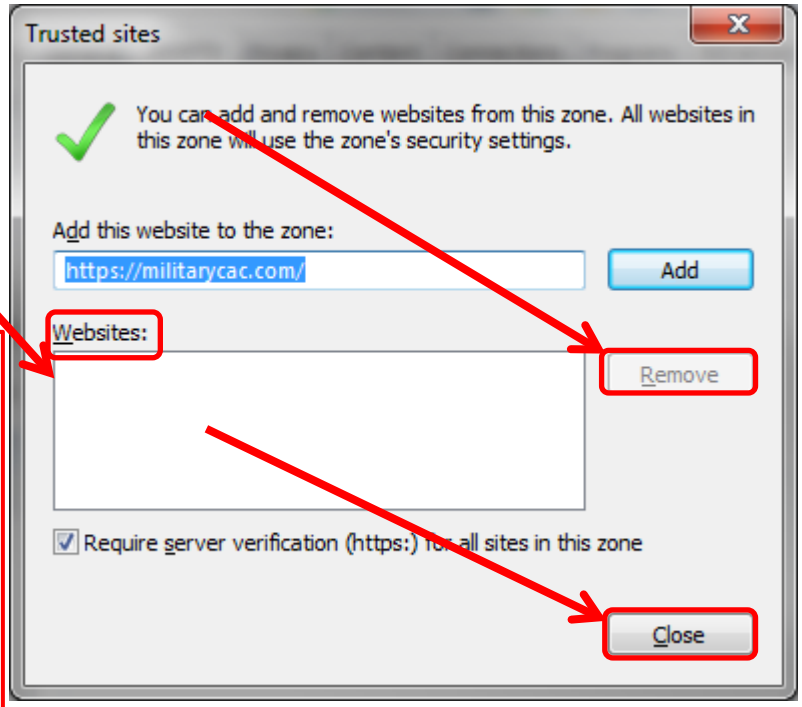
Click the *Security* (tab)(1), *Trusted sites* (green checkmark)(2), then *Sites* (button)(3)



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

NOTE: Most Government owned computers will not let you make changes to this area. Your only option is to skip this step.

This is the *Websites:* box



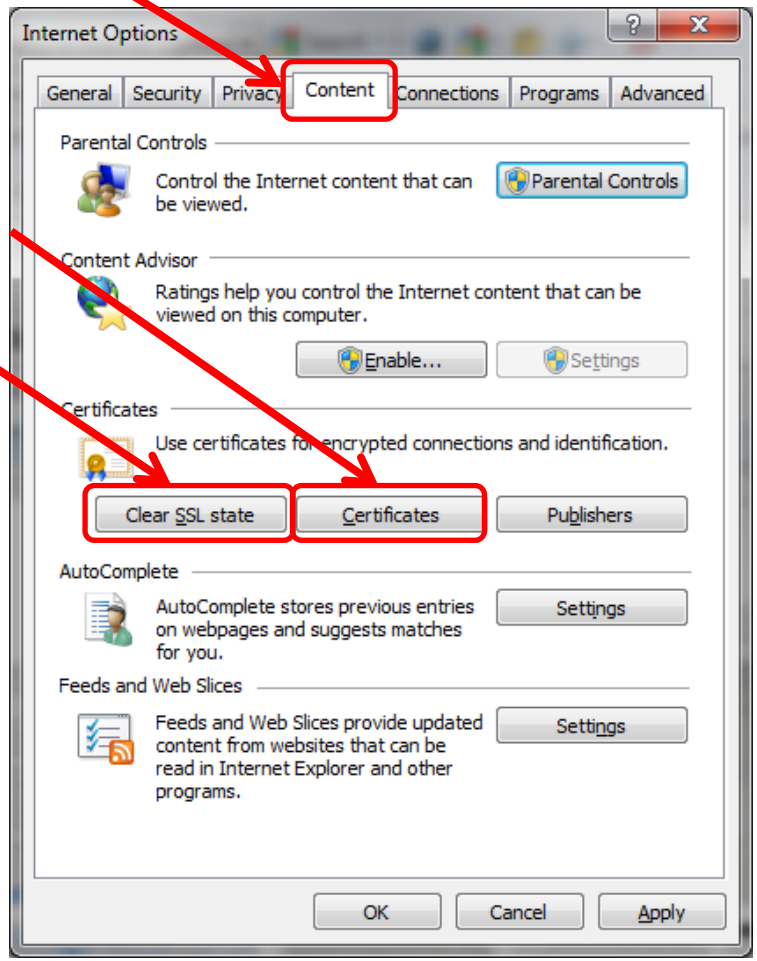
NOTE2: Some people will argue that AKO "should be" in the trusted sites. Here's what I've been able to deduce: it **WAS** needed with **IE 6 & 7**, however, if using **IE 11,** AKO users will be "recycled" to the AKO home page. So, **IE 11** users REMOVE it.

-NOTE3: As of 13 APR 17, if you need the ability to send and receive encrypted email in OWA, you'll need to add https://.mail.mil , more information can be read in the URL here ---------->

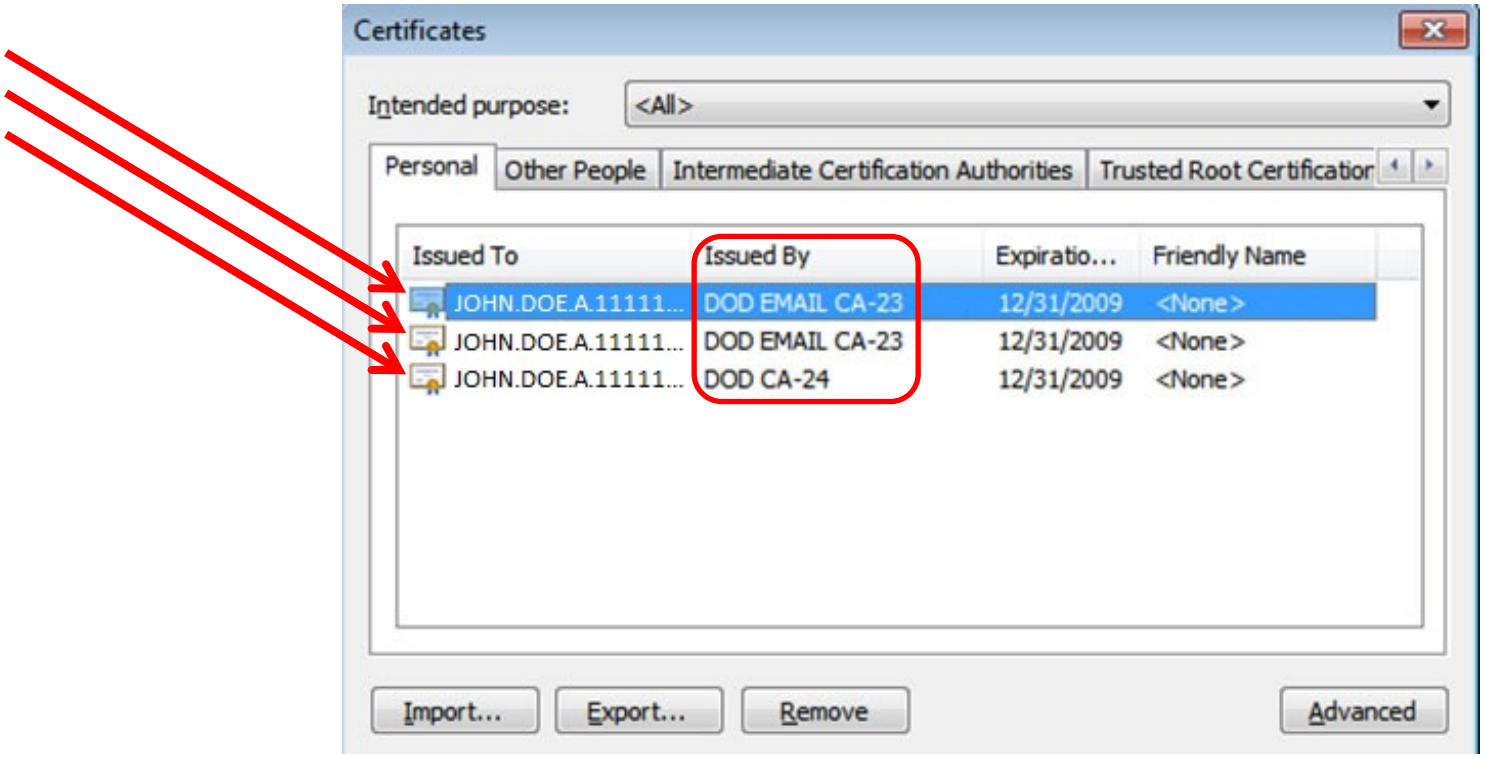
https://milcac.us/files/win10smime.pdf then come back to this guide

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

Click:
Clear SSL state



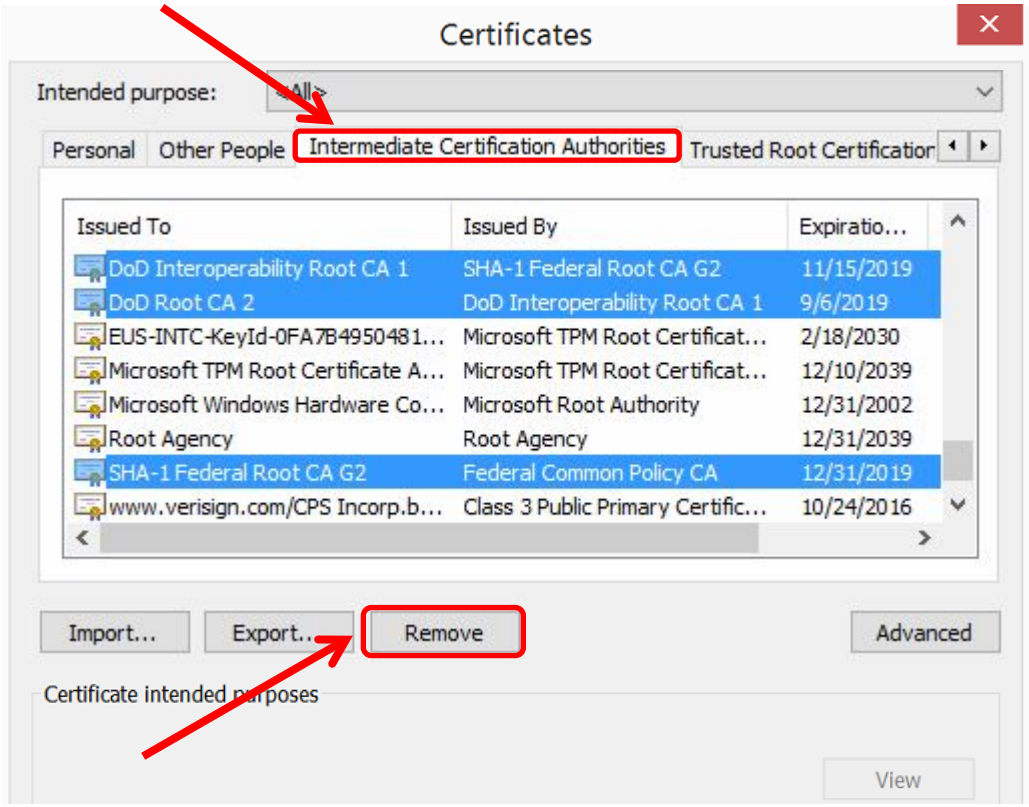
Most people will see 3-4 DOD certificates (2 with EMAIL and 1-2 without) under the *Personal* (tab) *Issued By* (column). CACs issued between 25 FEB 2018 and 28 FEB 2021 may see 4 certificates on their card. Cards issued after 1 MAR 2021 will see 3 in this view, 1 on websites.



This page is CAC Specific

Click the *Intermediate Certification Authorities* (tab). First, verify you have DOD EMAIL CA-33 through DOD SW CA-67 under the *Issued To* (column) (if you don't, go back to slide #2 and install or rerun the DoD Root Certificates again). Second, scroll down to below the DOD ID SW CA-48 and look for all of the listed certificates on the next page.

IF you see any of the certificates shown on the next slide, select it, and click *Remove.*



- Cross Cert remover Automated file (you may need to run as administrator) to remove certificates Listed above (Does not always work)
Download from MilitaryCAC (24 OCT 19 version)
Download from Cyber.mil (24 OCT 19 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

These are the known "bad certs" that need to be removed from *Intermediate Certification Authorities* (tab) [if found]:

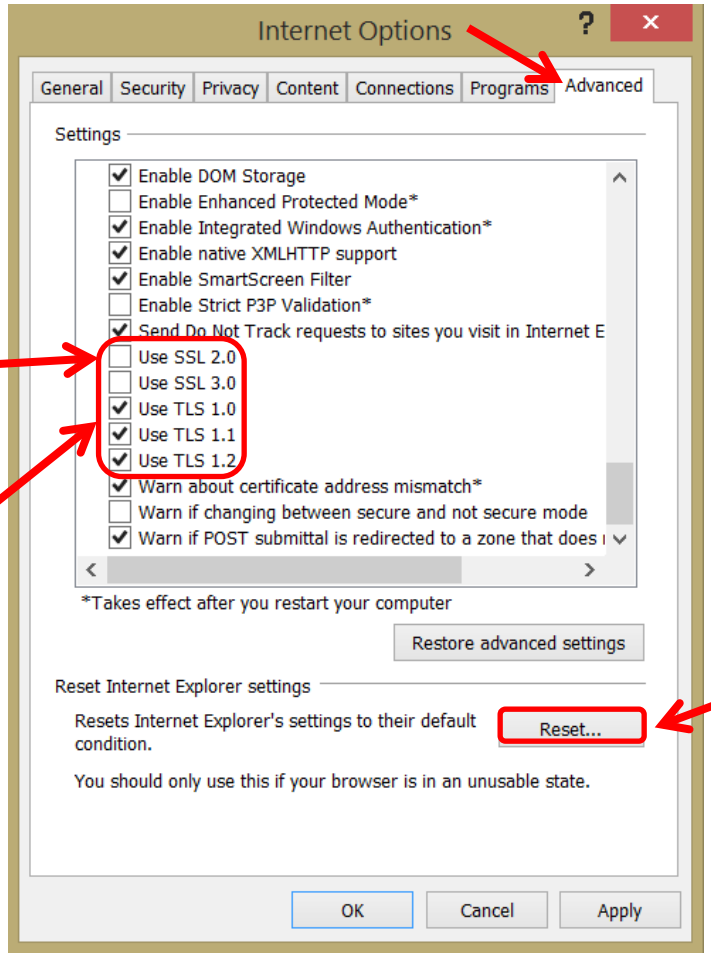
Issued To	Issued By
DoD Interoperability Root CA1	SHA-1 Federal Root CA G2
DoD Interoperability Root CA2	Federal Bridge CA 2013
DoD Interoperability Root CA2	Federal Bridge CA 2016
DoD Interoperability Root CA2	Federal Bridge CA G4
DoD Root CA 2	DoD Interoperability Root CA 1
DoD Root CA 3	DoD Interoperability
Federal Bridge CA 2016 or 2013	Federal Common Policy CA
Federal Bridge CA G4 or G6	Federal Common Policy
SHA-1 Federal Root CA G2	Federal Common Policy
US DoD CCEB Interoperability Root CA 1	

NOTE: If you don't see any of these, select *Close* on this window and continue with this guide

Click the *Advanced* (tab), scroll to the bottom of the list, make sure that **only** *TLS 1.0, 1.1, & 1.2* are checked. *The SSL(s)* should **NOT** be checked

NOTE: Windows 10 users will not see *Use SSL 2.0*

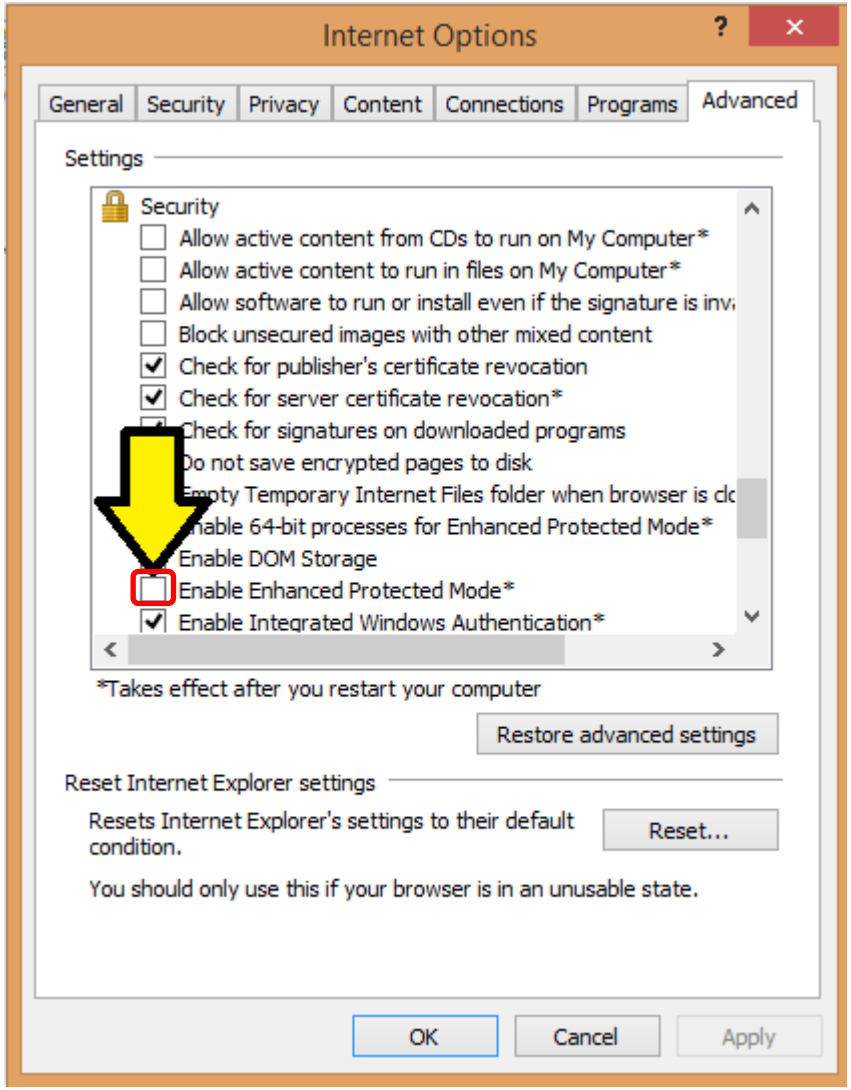
Another NOTE: If you are getting an error message regarding "Cannot connect securely to this page" try **UNChecking** *Use TLS 1.0*



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

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

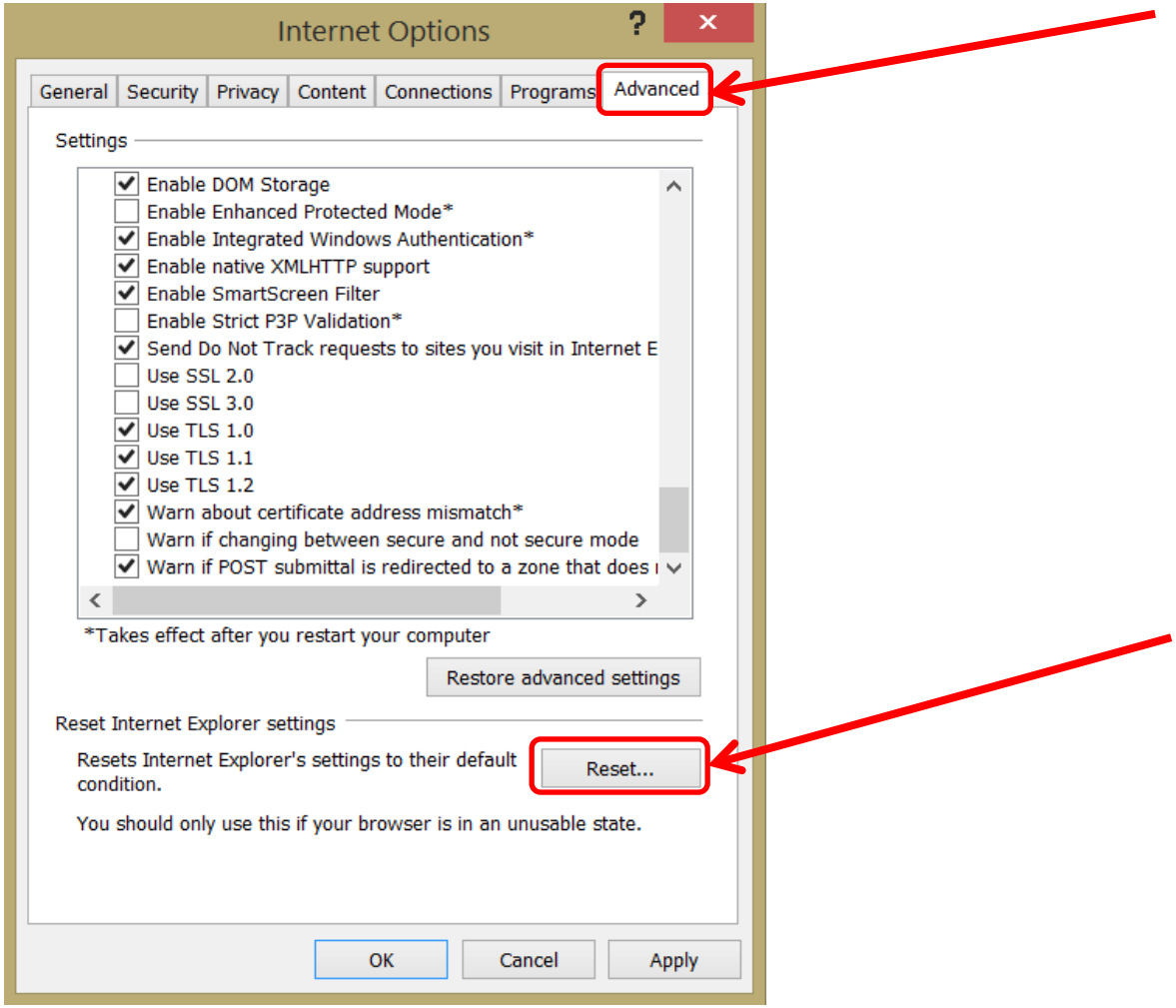


To try this option, Click *Tools*, *Internet Options*, *Advanced* (tab)

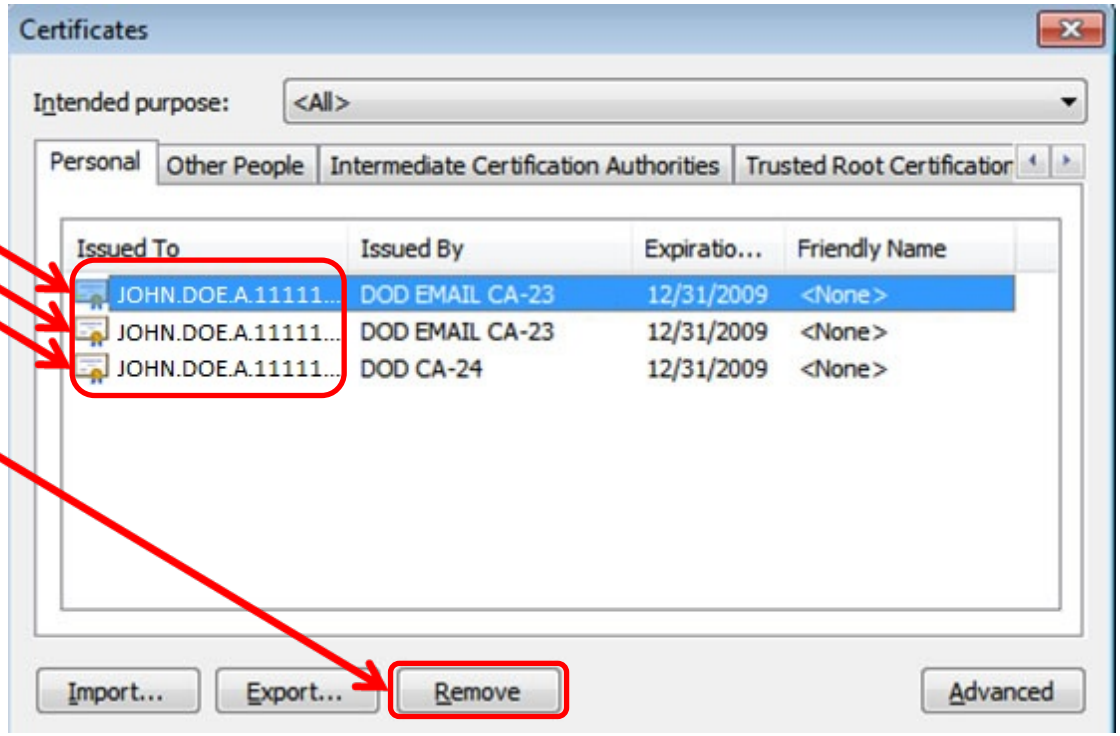
INFORMATION: Running *Enhanced Protected Mode** helps prevent attackers from installing software or modifying system settings if they manage to run exploit code. It is an extra layer of protection that locks down parts of your system that your browser ordinarily doesn't need to use.

- 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* certificates (see slides 5 & 13 for instructions on how to get to this location). People with 2 CACs may see up to 8 certs after they have activated their PIV certificates (4 certs per card).



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

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

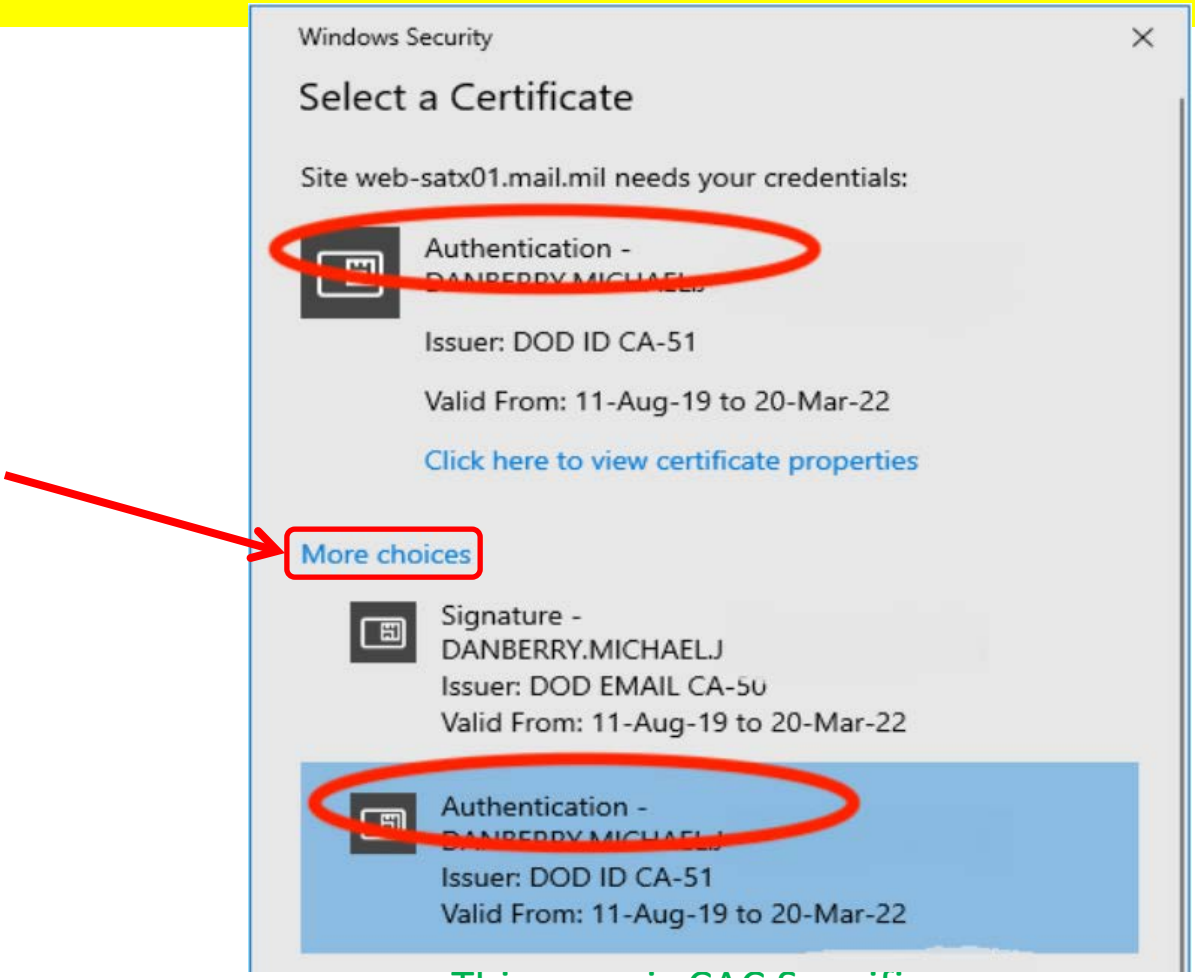
This page is CAC Specific

Try these additional items if you are still having issues:

Your time on your computer may be off by more than the server's 5 minute allowed limit. Check your clock and time zone.

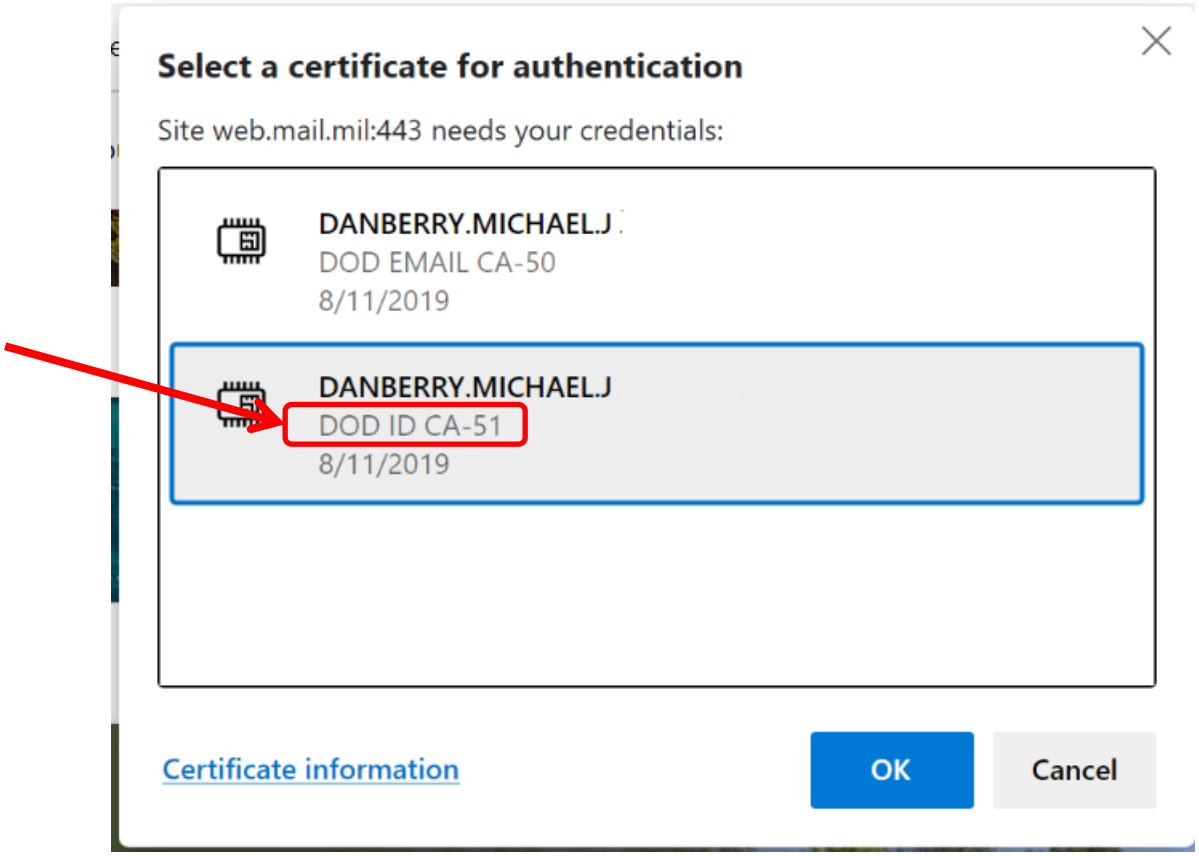
If all of the previous ideas did not work, please visit: https://militarycac.com/cacdrivers.htm to start troubleshooting your CAC reader

When checking your email on Windows 10, make sure you are selecting the correct certificate. Select *More choices* to see additional certificate(s)



This page is CAC Specific

When checking your email on Windows 11, make sure you are selecting the correct certificate (WITHOUT EMAIL)



This page is CAC Specific

There have been DNS issues for some people, please try the ideas below if still having problems

Here's how in <u>Windows</u> to manually configure the DNS settings.

1. Right click on your Wireless / Ethernet connection (down by your clock)
2. Select *Open Network and Sharing Center*
3. Click *Change Adapter Settings*
4. Right Click on your active internet connection, select *Properties*
5. Under *This connection uses the following items:* scroll down and click on *Internet Protocol Version 4 (TCP/IPv4)*, then click *Properties*
6. Select the option *Use the following DNS server addresses:*. This is where you manually configure your DNS servers:

NOTE: It is up to you if you want to use Open DNS, Quad 9, or Cloudflare. You might try each of them separately.

<u>Quad 9</u> - enter **9.9.9.9** for Preferred DNS server, and leave alternate DNS server blank. Click OK, then click Close

or

<u>Cloudflare</u> – enter **1.1.1.1** for Preferred DNS server, and **1.0.0.1** for Alternate DNS, Click OK, then click Close

Presentation created and maintained by:

Michael J. Danberry

https://MilitaryCAC.com

https://MilitaryCAC.org (DoD Computers)

If you still have questions, visit:

https://militarycac.com/questions.htm

https://militarycac.org/questions.htm (DoD Computers)