

Accessing Army365 / O365 webmail, DoD Enterprise Email, and other DoD websites with Edge on your Windows computer

Presented by: Michael J. Danberry

Last Revision / review: 08 February 2022

Performing these fixes "should" fix most access problems.

Personnel utilizing this guide without a CAC should <u>only</u> skip the pages marked: "This page is CAC Specific." CAC holders need to follow <u>ALL</u> slides.

The most up to date version of this presentation can be found at: <u>https://milcac.us/tweaks</u>

To successfully access Department of Defense (DoD) websites, you <u>MUST install</u> 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"

There is a problem with this website's security certificate.

or you see red certificate errors,

😂 https://web-mont05.mail.mil/my.r 🔎 👻 Certificate er... 🖒

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

Type "Internet Options" in the "Type here to search" box (or magnifying glass) and select *Internet Options Control Panel.*







Check the *Delete browsing history on exit* (box), click <u>*Delete...*</u>



Check the top 4 boxes, leave the rest unchecked, click <u>Delete</u>



Click <u>Settings</u>

| Internet Options | |
|--|--|
| General Security Privacy Content Connections Programs Advanced | |
| Home page | |
| To create home page tabs, type each address on its own line. | |
| The state of the s | |
| Use gyrrent Use de <u>f</u> ault Use <u>b</u> lank | |
| Browsing history | |
| and web form information. | |
| Delete browsing history on exit | |
| Delete | |
| Search | |
| Change search deradits. | |
| Tabs | |
| tabs. | |
| Appearance | |
| Colors Languages Fonts Accessibility | |
| | |
| OK Cancel Apply | |

Change this number to 50, click OK

| Temporary Internet Files and History Settings |
|---|
| Temporary Internet Files |
| Internet Explorer stores copies of webpages, images, and media for faster viewing later. |
| Check for newer versions of stored pages: |
| Every time I visit the webpage |
| Every time I start Internet Explorer |
| Automatically |
| 🔘 Never |
| Disk space to use (8-1024MB) (Recommended: 50-250MB) |
| Current location: |
| C:\Users\michael.j.danberry\AppData\Local\Microsoft\Windows\ Temporary Internet Files\ |
| Move folder View objects View files |
| History Specify how many days Internet Explorer should save the list |
| of websitus you have visited. |
| Days to keep pages in history: 20 🚔 |
| OK Cancel |

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 <u>Sites</u> (button)(3)



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

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



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

Click: Clear <u>S</u>SL 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.

| Personal | Other People | Intermediate Certification | Authorities | Trusted Root Certificati |
|----------|----------------|----------------------------|-------------|--------------------------|
| Issued | То | Issued By | Expiratio | Friendly Name |
| | HN.DOE.A.11111 | L DOD EMAIL CA-23 | 12/31/20 | 009 <none></none> |
| IOL 🔄 🗌 | HN.DOE.A.11111 | L DOD EMAIL CA-23 | 12/31/20 | 009 <none></none> |
| 101 | IN.DUE.A.IIIII | | 12/51/20 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

This page is CAC Specific

Click the Intermediate Certification Authorities (tab). First, verify you have DOD DERILITY CA-1 through DOD SW CA-69 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 <u>MilitaryCAC</u> (24 OCT 19 version) Download from <u>Cyber.mil</u> (24 OCT 19 version)



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

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

Issued By

SHA-1 Federal Root CA G2
Federal Bridge CA 2013
Federal Bridge CA 2016
Federal Bridge CA G4
DoD Interoperability Root CA 1
DoD Interoperability
Federal Common Policy CA
Federal Common Policy
Federal Common Policy

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. <u>The SSL(s) should NOT be checked</u>

| | Internet Options ? × |
|--|--|
| | General Security Privacy Content Connections Programs Advanced |
| | Settings |
| NOTE: Windows 10 & 11 users will not see <i>Use</i> | Enable DOM Storage Enable Enhanced Protected Mode* Enable Integrated Windows Authentication* Enable Integrated Windows Authentication* Enable SmartScreen Filter Enable Strict P3P Validation* Send Do Not Track requests to sites you visit in Internet E Use SSL 2.0 Use SSL 3.0 |
| SSL 2.0 or 3.0 | ✓ Use TLS 1.0 ✓ Use TLS 1.1 ✓ Use TLS 1.2 ✓ Warn about certificate address mismatch* ✓ Warn if changing between secure and not secure mode ✓ Warn if POST submittal is redirected to a zone that does i ∨ |
| | < >> |
| | *Takes effect after you restart your computer |
| | Restore advanced settings |
| | Reset Internet Explorer settings |
| | Resets Internet Explorer's settings to their default Reset |
| | You should only use this if your browser is in an unusable state. OK Cancel |

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). <u>https://evaluations.hrc.army.mil</u> More information available at <u>https://MilitaryCAC.com/ees.htm</u>

| | | l. I | nternet | Options | | ? | × |
|--------------------|--|--|---|--|---|--------------|-------|
| General | Security | Privacy | Content | Connections | Programs | Adv | anced |
| General Setting | Security Security Security Allow Allow Block Check Check Check Check Do no Empty Check Do no Empty Check | active con active con software for unsecured for publis for serve for signat t save ence Tempora | Content tent from (tent to run to run or in images wi her's certificate tures on do rypted pag ry Internet ocesses fo | Connections CDs to run on l in files on My stall even if th th other mixed icate revocation* ownloaded pro- ges to disk : Files folder wi r Enhanced Pro- | Programs My Compute Computer* e signature i content on grams hen browser | r* s inv; | ^ |
| | Enable Enable | DOM Sto Enhance Integrat | rage d Protecte ed Window | d Mode* s Authenticati | on* | - | ~ |
| < *Ta | kes effect a | after vou | restart vou | ir computer | | > | |
| Reset I | nternet Ex | plorer set | tings | Restore | advanced s | etting | gs |
| Rese | ts Internet | t Explorer' | s settings (| to their default | Res | et | |
| You | should only | use this i | f your brov | vser is in an un | usable state | 2. | |

OK

Cancel

Apply

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

| Internet Options ? × |
|--|
| eneral Security Privacy Content Connections Programs Advanced |
| Settings |
| Enable DOM Storage Enable Enhanced Protected Mode* Enable Integrated Windows Authentication* Enable Integrated Windows Authentication* Enable SmartScreen Filter Enable Strict P3P Validation* Send Do Not Track requests to sites you visit in Internet E Use SSL 2.0 Use SSL 3.0 Use TLS 1.0 Use TLS 1.1 Use TLS 1.2 Warn about certificate address mismatch* Warn if changing between secure and not secure mode Warn if POST submittal is redirected to a zone that does |
| * Takes effect after you restart your computer |
| Restore advanced settings |
| Reset Internet Explorer settings Resets Internet Explorer's settings to their default condition. You should only use this if your browser is in an unusable state. |
| OK Cancel Apply |

You may need to <u>*Remove*</u> 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).

| | Certificates | | | | |
|---------------|--------------------|--------------------------------|-----------------------------|---------------------------|--|
| | Intended purpose: | <all></all> | | | |
| | Personal Other Per | ople Intermediate Certificatio | n Authorities T | rusted Root Certification | |
| | Issued To | Issued By | Expiratio | . Friendly Name | |
| | JOHN.DOE.A.1 | 1111 DOD EMAIL CA-23 | 12/31/2009 | 9 <none></none> | |
| | JOHN.DOE.A.1 | 1111 DOD EMAIL CA-23 | 12/31/2009 | 9 <none></none> | |
| | JOHN.DOE.A.1 | 1111 DOD CA-24 | 12/31/2009 | 9 <none></none> | |
| 2: You will | | | | | |
| e a message 🔪 | | | | | |
| . Vou cannot | | | | | |
| | | | | | |
| τ αατα | | | | | |
| ted using the | | | | | |
| ates. Select: | Import | xport | | Advanced | |
| | | | C C · · · · C | | |

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: <u>https://militarycac.com/cacdrivers.htm</u> to start troubleshooting your CAC reader When checking your email on Windows 10 & 11, make sure you are selecting the correct certificate. Select *More choices* to see additional certificate(s)



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

| | DANBERRY.MICHAEL.J DOD EMAIL CA-50 8/11/2019 | | |
|-------------|--|----|------|
| | DANBERRY.MICHAEL.J DOD ID CA-51 8/11/2019 | | |
| | | | |
| | | | |
| Certificate | information | ОК | Canc |

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.

Quad 9 - 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 <u>https://MilitaryCAC.com</u> <u>https://MilitaryCAC.org</u> (DoD Computers)

If you still have questions, visit: <u>https://militarycac.com/questions.htm</u>

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