DISA ID51
ENTERPRISE BREAK & INSPECT (EBI) PROGRAM

EBI TROUBLESHOOTING GUIDE
V3.1

September 2019

Table of Contents

1.0 SECTION 1: INTRODUCTION

1.1 Objectives and Scope

This document outlines DoD Enterprise Break & Inspect (EBI) troubleshooting steps. Target audience includes system administrators and operators investigating potential network and workstation problems encountered during the deployment of the EBI. This guide is available in the DoD Cyber Exchange PKI/PKE Document Library under 'WCF':

https://cyber.mil/pki-pke/pkipke-document-library/?_dl_facet_pkipke_topics=wcf

The troubleshooting steps in this document are applicable to Secure Socket Layer/Transport Layer Security (SSL/TLS) traffic flowing through the IAPs and should not be used as a reference for other break and inspect initiatives or non-SSL issues.

This guide assists with the troubleshooting of DoD EBI and Internet access and "source/destination" ticket issues.

1.2 Assumptions

- Operator/Administrator has needed permissions to access and check endpoint status
- Operator/Administrator has needed permissions to make changes to system or ability to escalate to authority that can make changes
- Organization has loaded DoD WCF Root Certificate. DoD PKE/PKI reference site on Cyber Mil includes guidance on certificate installation.

2.0 SECTION 2: ENDPOINT / CLIENT SYSTEM VERIFICATION

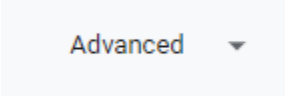
The first step in troubleshooting a suspected problem should be Certificate Verification. In order for SSL/TLS websites to function correctly for users, each user needs to have a specific SSL/TLS Certificate installed on their computer for the appropriate browser. *Internet Explorer* (IE) and *Google Chrome* (Chrome) use the same Certificate Store, so if one of these browsers has the certificate the other browser also has access to the certificate. *Mozilla Firefox* (Firefox) has its own independent Certificate Store and will need to be validated separately from IE or Chrome.

2.1 Certificate Verification / Determining SSL/TLS Certificate Status

2.1.1 Google Chrome

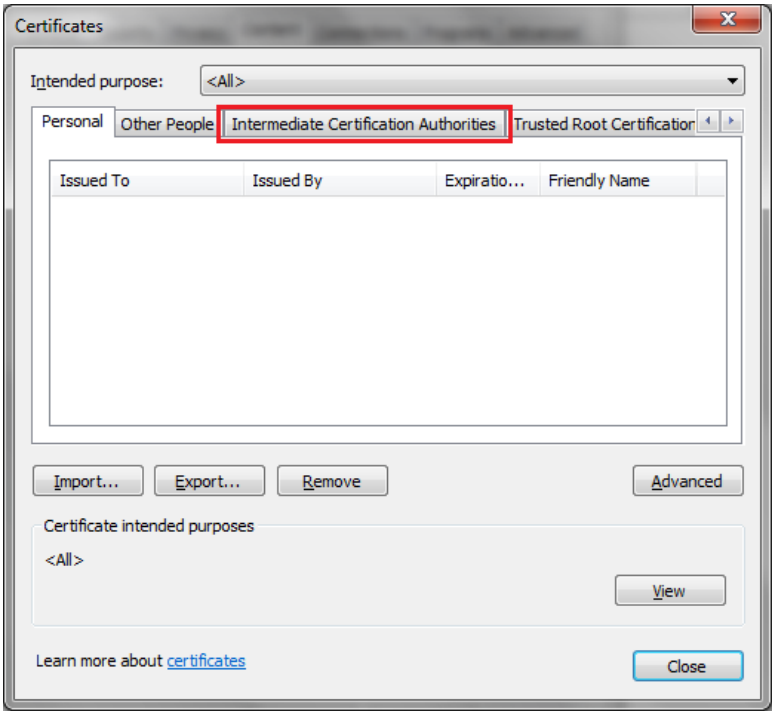
1. Open **Google Chrome** (Version 76 used)
2. Select the URL bar and type the following: chrome://settings/search#HTTPS

3. From the resulting page, select “Advanced”

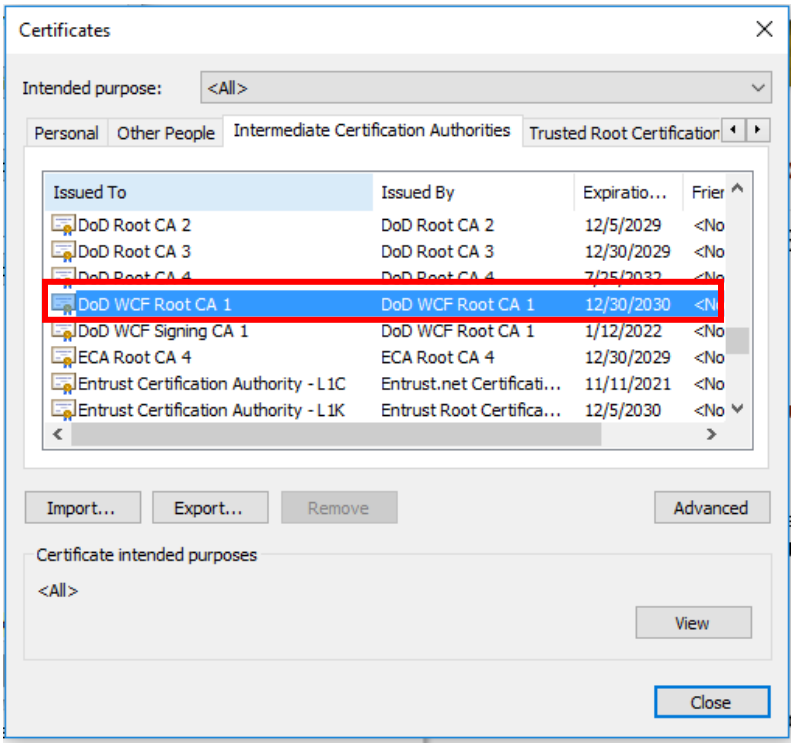


4. Under Privacy and Security select **“Manage Certificates”**

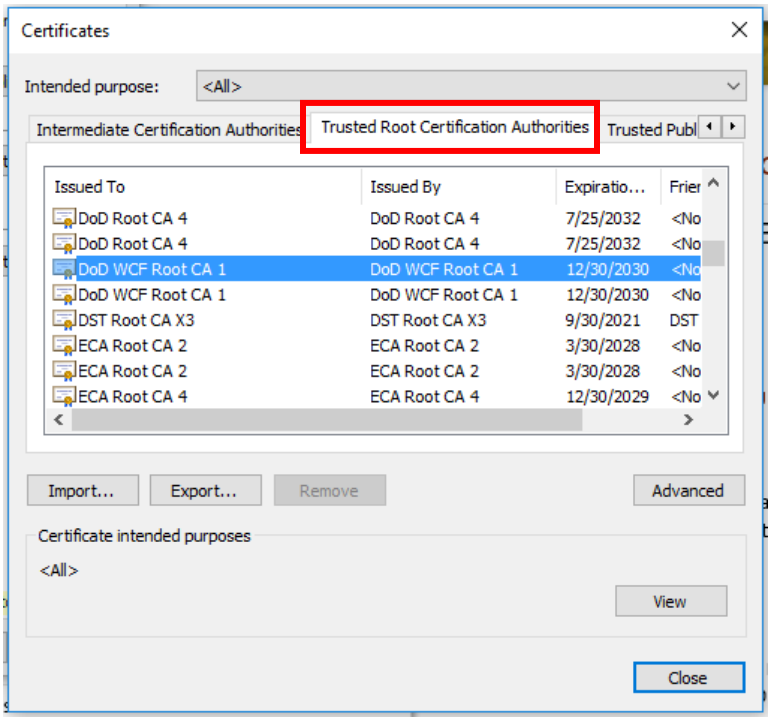
5. Select the **Intermediate Certification Authorities** tab



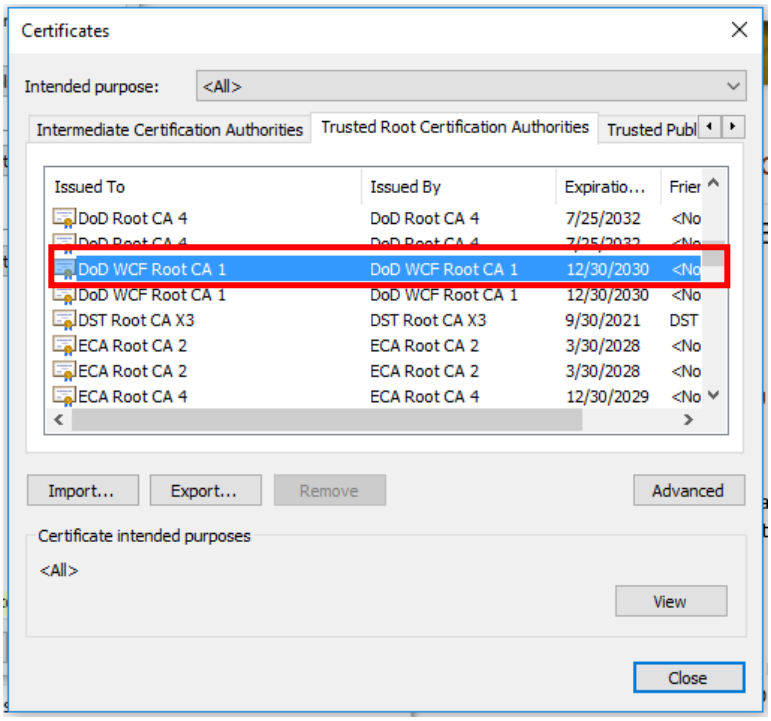
6. Ensure DoD **WCF Root CA-1** certificate is listed



7. Select **Trusted Root Certification Authorities** tab



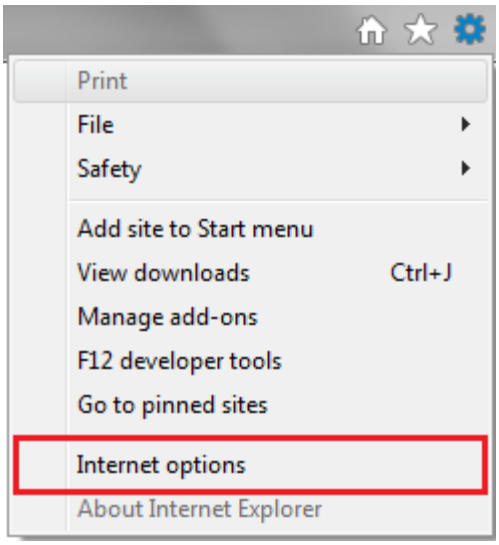
8. Ensure **DoD WCF Root WCF CA-1** certificate is listed



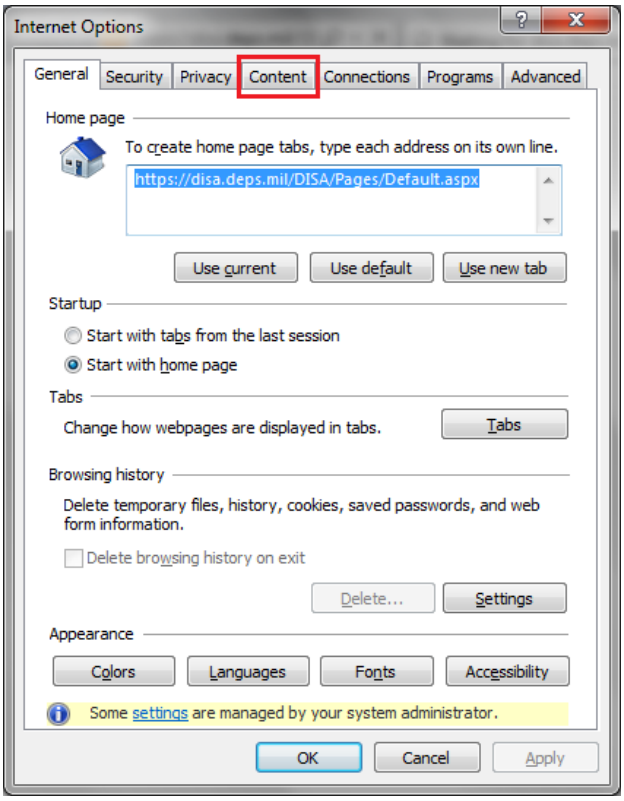
2.1.2 Internet Explorer

1. Open **Internet Explorer**
2. Click the Settings button

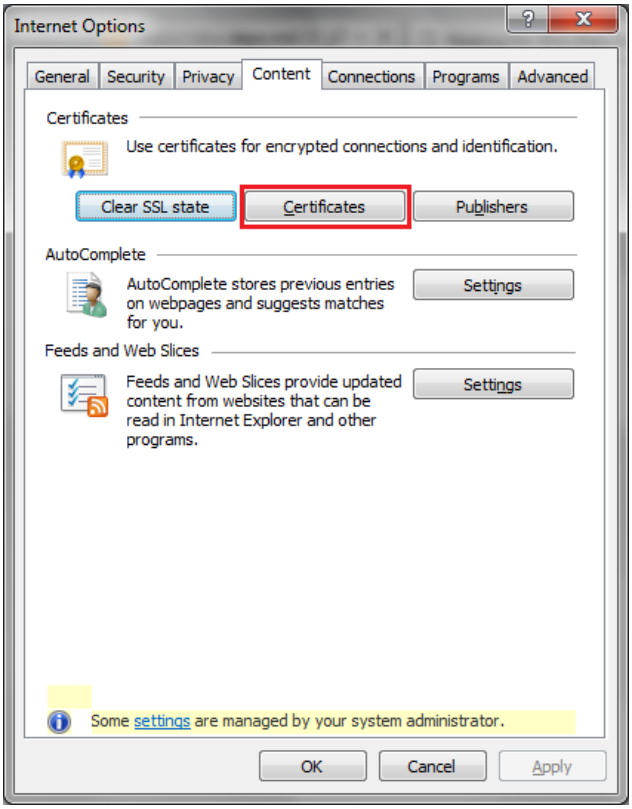
3. From the drop-down menu, select **Internet Options**



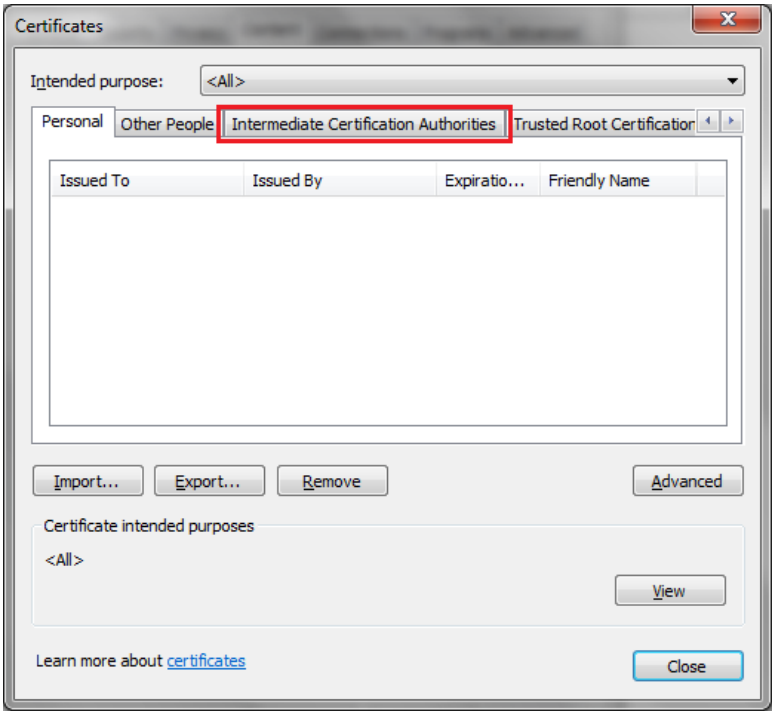
4. A new settings window will open, select the tab **Content**



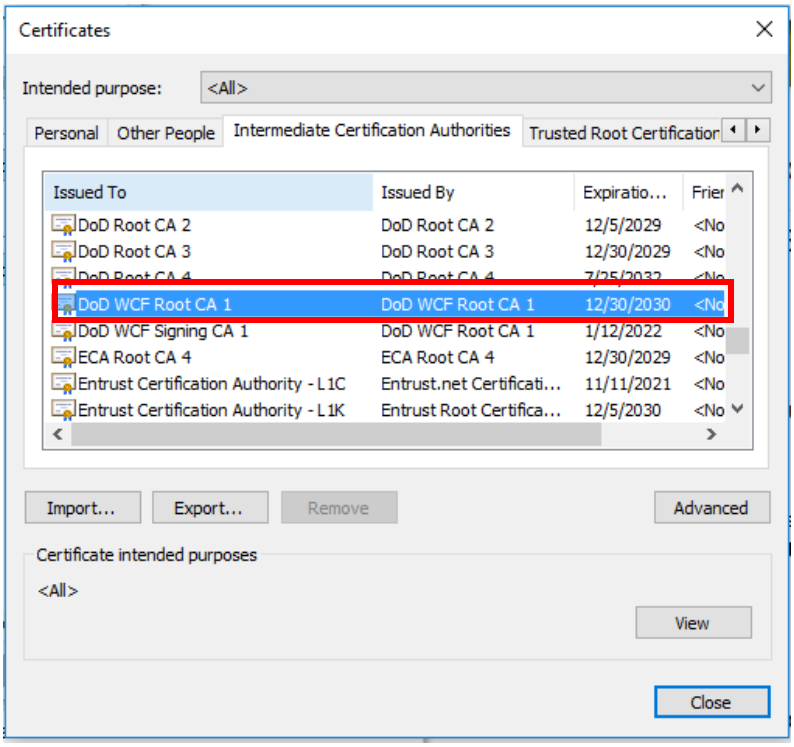
5. From the **Content** tab, click the **Certificates** button



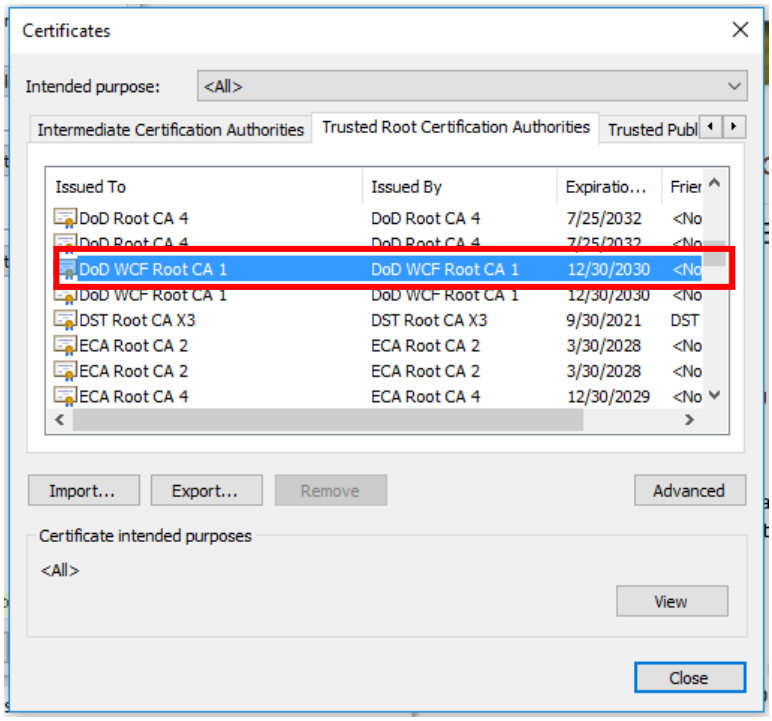
6. Select the **Intermediate Certification Authorities** tab



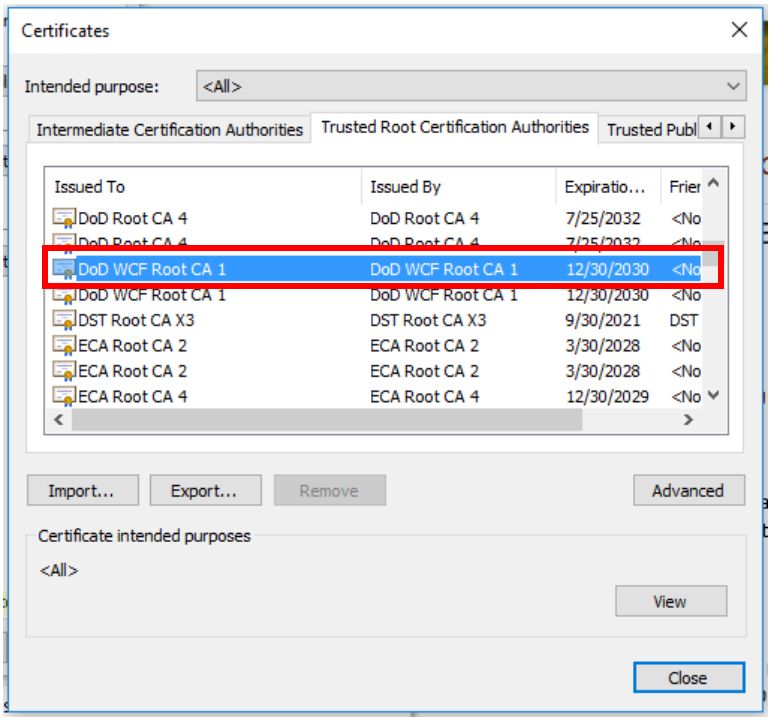
7. Ensure **DoD WCF Root CA-1** certificate is listed



8. Select **Trusted Root Certification Authorities** tab

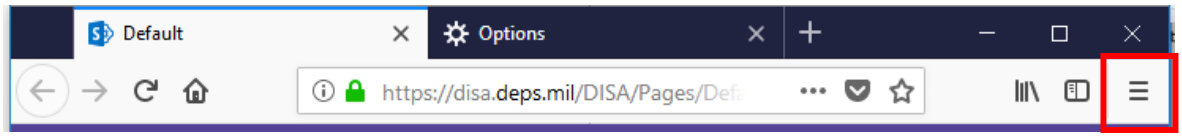


9. Ensure **DoD WCF Root WCF CA-1** certificate is listed

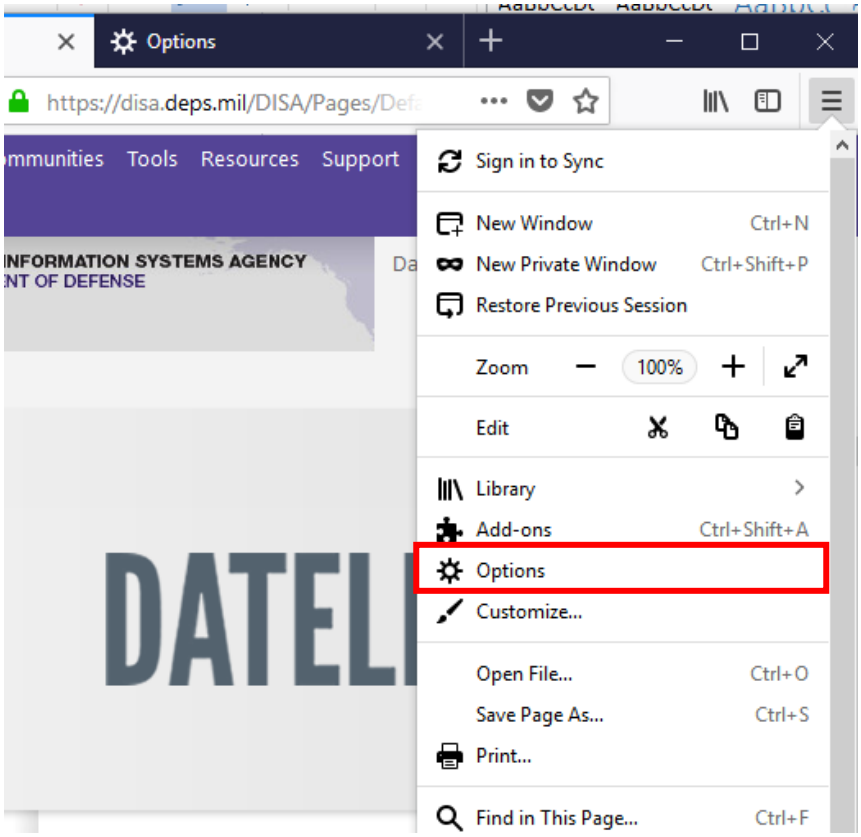


2.1.3 Mozilla Firefox

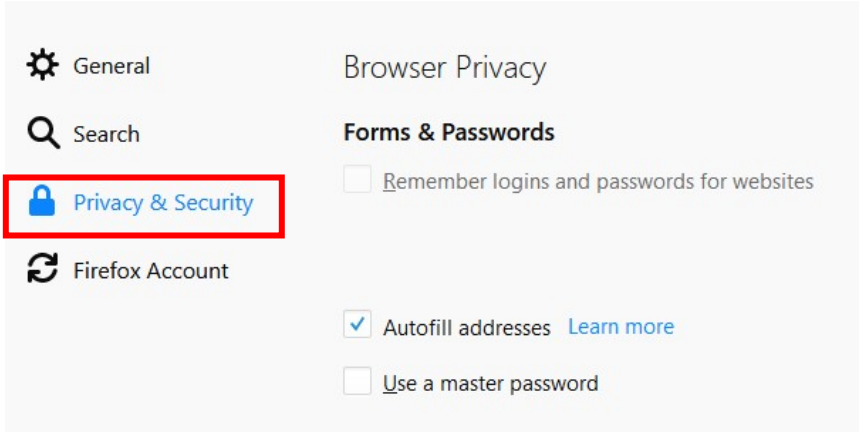
1. Open **Firefox**
2. Select the hamburger menu



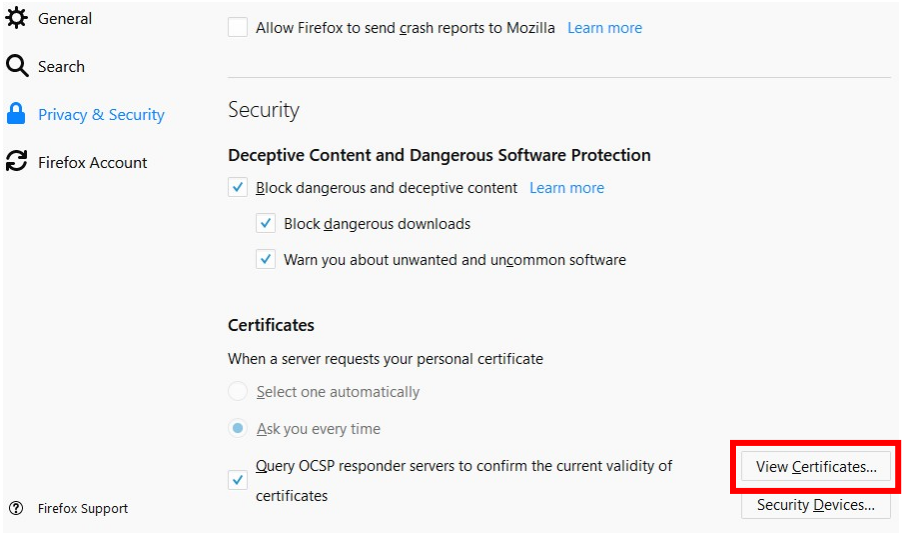
3. Click the Options button



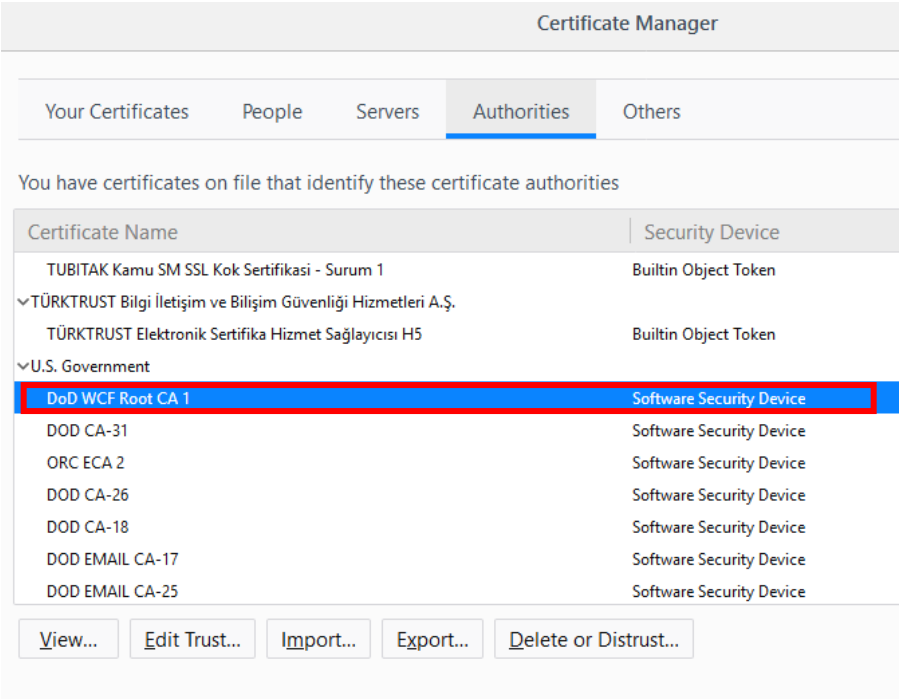
4. Select the **Privacy & Security** tab in the left hand column



5. Scroll to the bottom of the page and click the **View Certificates** button



6. From Firefox's Certificate Manager, **"Authorities"** section, ensure that the certificate **DoD WCF Root CA-1** is listed.



3.0 SECTION 3: SCENARIOS

Prior to handling any of the scenarios listed below the Certificate Stores of the user should be checked to determine whether or not the correct certificates are present. That information will be valuable in determining where the issue lies and how to fix the problem.

3.1 User Is Receiving SSL Certificate Warnings

3.1.1 Symptoms

1. User is receiving a splash page from their browser warning about insecure HTTPS connections or that their connection is not private.
    - Example Error code: SSL_ERROR_BAD_CERT_DOMAIN.
2. User's browser URL bar shows SSL lock icon has an X through it or has 'https://' crossed out.

3.1.2 Resolution

It is most likely the case that the user has not received the "DoD WCF Root CA-1" certificate for their particular browser. Manually install the certificate into the user's Certificate Store. See the Appendix I and/or Appendix III for information on how to do this.

3.2 User's PC Is Missing DoD WCF Root CA-1

3.2.1 Symptoms

1. User's IE/Chrome Certificate Store does not have "DoD WCF Root CA-1"
    - Certificate are not in both Intermediate Certification Authorities and Trusted Root Certification Authorities stores.
2. User's Firefox Certification Store does not have the "DoD WCF Root CA-1" Certificate in the Authorities store.

3.2.2 Resolution

Manually install the certificate into the user's Certificate Store. See Appendix I for information on how to do this.

3.3 Specific URL or Application Is Not Working

3.3.1 Symptoms

1. User is able to access some content over an HTTPS connection; however, a specific website/application is not functioning.
2. Multiple users/customers at different sites are having issues accessing the same specific website over HTTPS.

3.3.2 Resolution

Complete internal/enterprise level trouble shooting efforts. If an application or URL continues to exhibit blocked characteristics, contact the DISA Global Service Desk (GSD). Instructions are in the "APPENDIX III – CONTACTS AND REFERENCES" at the end of this document.

3.4 CAC-Enabled Site Is Not Working

By default sites that have client authentication should bypass SSL Intercept. However, in the event that for some reason the bypass does not occur, sites with CAC Authentication may fail to log users in.

3.4.1 Symptoms

1. User is able to access other websites or applications over SSL
2. User is unable to log into a particular site that requires CAC Authentication
3. User has a valid CAC

3.4.2 Resolution

Complete internal/enterprise level trouble shooting efforts. If an application or URL continues to exhibit blocked characteristics, contact the DISA Global Service Desk (GSD). Instructions are in the "APPENDIX III – CONTACTS AND REFERENCES" at the end of this document.

3.5 Remote Application/URL Uses a Weak Signature Hash Algorithm

If an application or URL is using a weak Signature Hash Algorithm, most likely MD5, then the B&I devices will reject the certificate. This is unlikely to occur in newer certificates, but may be found in older certificates.

3.5.1 Symptoms

1. User is able to access other websites or applications over SSL
2. User receives an error similar to "This webpage is not available"

3.5.2 Resolution

Complete internal/enterprise level trouble shooting efforts. If an application or URL continues to exhibit blocked characteristics, contact the DISA Global Service Desk (GSD). Instructions are in the "APPENDIX III – CONTACTS AND REFERENCES" at the end of this document.

3.6 User Is Having Their Connection Reset on HTTPS or SSL Applications

3.6.1 Symptoms

1. User is receiving Connection Reset errors during long lived connections

3.6.2 Resolution

Complete internal/enterprise level trouble shooting efforts. If an application or URL continues to exhibit blocked characteristics, contact the DISA Global Service Desk (GSD). Instructions are in the "APPENDIX III – CONTACTS AND REFERENCES" at the end of this document.

4.0 TESTING

Upon migration to EBI, testing is conducted IAW with organizational tactics techniques and procedures (TTPs), Standard Operating Procedures (SOPs), and guidance. To assist in troubleshooting a list of webs sites that can be used in troubleshooting is provided.

4.1 TLS/port 443 CAC-Authenticated Sites

TLS Site URL - https://ietf.org/

TLS Site URL - https://defensesystems.com/Home.aspx

CAC –AUTH TLS Site URL - https://portal.cyberforce.site/home

4.2 Dot Mil and Dot Gov Sites

https://cyber.mil/

https://www.noaa.gov/

4.3 Mission Sites

During troubleshooting mission-critical sites may be included on the test list

5.0 APPENDIX I - MANUALLY INSTALL CERTIFICATES INTO CERTIFICATE STORE

Manual Installation of certificates within Internet Explorer and Google Chrome (the instructions for both are the same) and Mozilla Firefox.

5.1 Chrome/IE

1. Open Certificate Manager by clicking the **Start** button, typing **certmgr.msc** into the search box, and then pressing enter. You should be presented with an administrative login prompt.
2. Login with an administrator account.
3. Click the folder **Intermediate Certification Authorities**
4. Click **Action** from the top menu bar, hover item **All Tasks** and click **Import** from the fly out menu
5. Browse to find the appropriate .cer or .crt file that was provided and select it (you will likely have to transfer this to the user's PC)
6. Click **Next**
7. Select option **Place all certificates in the following store** and ensure the listed store is **Intermediate Certification Authorities** and click **Next**
8. Click **Finish**
9. Click the folder **Trusted Root Certification Authorities**
10. Click **Action** from the top menu bar, hover item **All Tasks** and click **Import** from the fly out menu
11. Browse to find the appropriate .cer or .crt file that was provided and select it (you will likely have to transfer this to the user's PC)
12. Click **Next**
13. Select option **Place all certificates in the following store** and ensure the listed store is **Trusted Root Certification Authorities** and click **Next**
14. Click **Finish**

5.2 Alternative Method for Chrome/IE

Most PCs should not require administrator access to import certificates in the manner described above. However, if a user is prompted for administrative credentials and they do not have this access the following instructions can be used as an alternative import method.

1. Open **Internet Explorer**
2. Click the **Settings** button (looks like a cogwheel)
3. Select **Internet Options** from the menu

4. Select the **Content** tab
5. Click the **Certificates** button
6. Select the **Intermediate Certification Authorities** tab
7. Click the **Import…** button
8. In the Certificate Import Wizard click **Next >**
9. Click the **Browse…** button to locate the certificate and click **Open**
10. Click **Next >** to continue
11. Ensure **Place all certificates in the following store** is selected and the **Certification store:** field says **Intermediate Certification Authorities**. If for some reason it does not, select **Browse…** and select it from the list.
12. Click **Next >** to continue
13. Click **Finish**
14. You should receive a prompt informing you the import was successful, click **OK**
15. You should now be back in the **Certificates** window
16. Select the **Trusted Root Certification Authorities** tab
17. Click the **Import…** button
18. In the Certificate Import Wizard click **Next >**
19. Click the **Browse…** button to locate the certificate and click **Open**
20. Click **Next >** to continue
21. Ensure **Place all certificates in the following store** is selected and the **Certification store:** field says **Trusted Root Certification Authorities**. If for some reason it does not, select **Browse…** and select it from the list.
22. Click **Next >** to continue
23. Click **Finish**
24. You should receive a prompt informing you the import was successful, click **OK**

The certificate should now be installed for both IE and Chrome.

5.3 Mozilla Firefox

1. Open Firefox (Steps were tested on version 39)
2. Type "***about:preferences***" in URL bar
3. Click **Privacy & Security** in the Left Column Menu.
4. Find **Certificates** section within the Security area (scrolled down to the bottom of the page).
5. Click **View Certificates** button.
6. Click **Import** and send the certificate file (DoD WCF Root CA 1.pem) on your computer to import.
7. Close browser after successful import of certificate.
8. Re-open Firefox browser.

6.0 APPENDIX II – POTENTIAL ADDITIONAL ERROS

6.1 Remote Web Server

Remote Web Server/Application Has Conflicting SSL Security

A possible problem could be encountered is that a remote web server or application only accepts SSL protocols/cipher combination not supported by the WCF SSL Pilot devices.

6.2 Application Errors

Application Does Not Use Windows Certificate Store

If an application does not use Windows Certificate Store and cannot have a Certificate Authority added there is a possibility that the application will not function as expected. Determining if this is an issue will vary on a case by case issue depending on how applications implement their use of certificates.

7.0 APPENDIX III – CONTACTS AND REFERENCES

7.1 DISA Global Service Desk (GSD)

- Phone
  - Toll Free: (844) 347-2457 | CML: (614)692-0032 | DSN: (312) 850-0032
- Options
  - Select Opt 2 (Infrastructure), then Opt 1 (Network). The GSD should create the ticket as a "Source Destination" ticket and will assign the ticket to the IP NOC.
- Information Required to open a ticket:
  - Public' Source IP address – The IP address being advertised to DISA.
  - Original host source IP address - May be the same as 'public' source IP address
  - Destination IP Address and URL that user cannot access
- Please reference the following keywords:
  - Cannot reach an Internet website / Internet Access issue / NIPRnet outage

7.2 References

Primary Reference: Cyber Mil (https://cyber.mil/)

WCF EBI website:

https://cyber.mil/pki-pke/pkipke-document-library/?_dl_facet_pkipke_topics=wcf