



Distributed Tactical Communications System (DTCS) Net Manager Web Portal - Before you Begin

CAC Certificate and Browser Configuration Verification Steps

Contents

Background.....	1
System Requirements.....	2
Verify CAC Reader and Middleware	3
ActivClient Configuration.....	3
Install DoD Root Certificate and CRL	4
For Microsoft Internet Explorer Users.....	7
Microsoft Internet Explorer – Verify your DoD Certificates	7
Fine Tuning Internet Explorer.....	10
Accessing the DTCS Net Manager Web Portal with Internet Explorer	12
For Mozilla Firefox Users	13
Firefox Configuration.....	13
Accessing the DTCS Net Manager Web Portal with Firefox.....	17
Additional Resources	18

Background

The DTCS Net Manager Web Portal requires a DoD-signed “signature” certificate before a user is granted access to the login page for the Web Portal. Certificates are typically stored on a user’s Common Access Card (CAC), but a “soft certificate” stored on the user’s computer can also be used. For a user to be granted access to the Web Portal login page, the certificate must exist, not be expired, and not be revoked. The DOD-signed “signature” certificate is sometimes also called an “email” certificate.

Not all DoD websites use CAC authentication in the same manner. The steps in this document are to assist the DTCS Net Manager Web Portal user in verifying the necessary certificate and browser settings to access the DTCS Net Manager Web Portal. Computers vary and settings may need to be modified according to each computer. This document does not attempt to detail every possible configuration. If you are unable to access the Web Portal

after following the steps in the document, contact your System or Network Administrator. The websites found at <http://militarycac.com/> and http://iase.disa.mil/pki-pke/getting_started/index.html can also be very helpful.

There are 3 primary types of certificates on a CAC:

- ID certificate – needed to access a computer (physical presence)
- Signature certificate – needed to sign documents, email and web-site access
- Encryption certificate – needed for encryption

The DTCS Web Portal server relies on an external U.S. Government certificate validation server to validate that a certificate is DoD-signed, is a “signature” certificate, and is not expired or revoked. If the government’s certificate validation server is unavailable, the Web Portal may not be accessible. If there is a problem with the CAC certificate the user has selected, it might be one of these causes:

- If the certificate is not DoD-signed or is expired, the user may not see anything... Internet Explorer may appear as if the site doesn’t exist; Chrome will state an SSL error, etc.
- If the certificate is DoD-signed, not expired, but is not a “signature” certificate or is revoked, the user will receive a DTCS Web Portal generated message about an invalid certificate.
- If all validations pass, the user will be presented with the DTCS Web Portal login page.

System Requirements

The Web Portal currently supports the following hardware and software configurations for the user’s computer:

- Hardware: Windows-based desktop or laptop computer
- Operating System: Windows XP or Windows 7 Operating System
- Browser: Internet Explorer v8 (IE8); or Firefox v18 (FF18)
Note: While other versions of Internet Explorer and Firefox, as well as the Chrome and Safari browsers, may function properly, they are not currently tested and verified with the Web Portal releases and are therefore not officially supported.
- CAC Handling:
 - A CAC reader should be installed on the user’s computer. ActivClient may or may not be needed. If it is, use:
 - ActivClient hotfix 6.2.0.133 for Windows 7
 - ActivClient hotfix 6.1.3.132 for Windows XP
 - ActivClient hotfix is available on <http://militarycac.com/activclient62update.htm>
 - DoD-signed, “signature” certificate is installed and is not expired or revoked
 - Certificate Revocation List (CRL) files are installed
 - If your CAC certificates, DoD Root certificate or the Certificate Revocation List files are not already installed on the computer, they will need to be installed. You will need rights to install these files on your computer or have your System Administrator do it for you.

NOTE: The below site can be used to download the CA certificates.

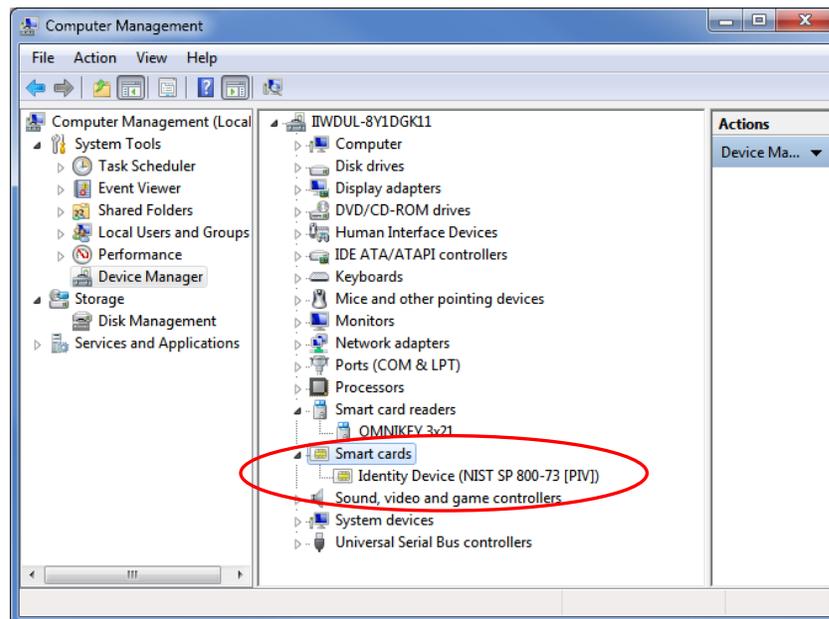
<http://dodpki.c3pki.chamb.disa.mil/rootca.html>

Verify CAC Reader and Middleware

ActivClient Configuration

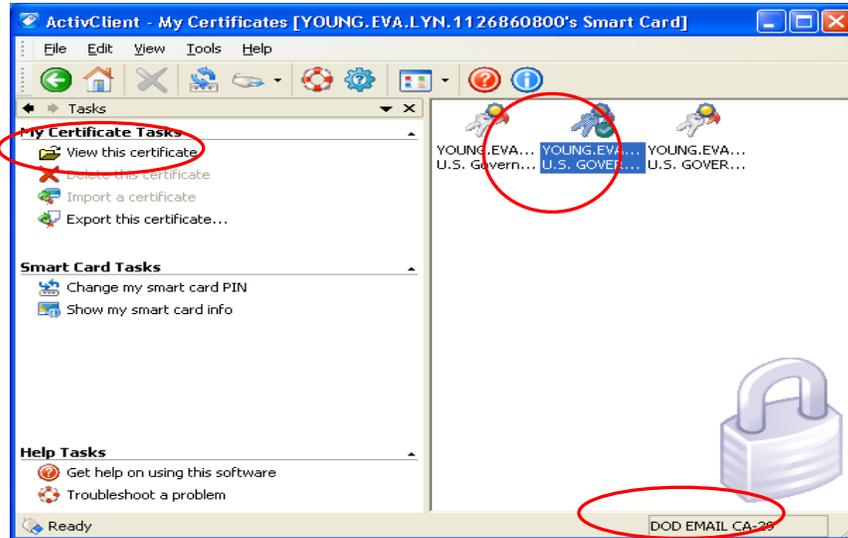
For Windows 7, DTCS Support has found that installing ActivClient hotfix 6.2.0.133 resulted in successfully accessing the DTCS Web Portal with IE8 and IE9. For Windows XP, ActivClient 6.1.3.132 was found to work with IE8. ActivClient hotfix is available from this site <http://militarycac.com/activclient62update.htm>. If you do not have Administrative rights to your computer to install an ActivClient hotfix, you will need to contact your System Administrator.

- For Windows 7 without ActivClient middleware:
 - a. Verify the card reader is properly installed by checking that a reader is listed in the Device Manager under **Smart card readers**.
 - b. Insert your CAC into the reader.
 - c. Verify the card reader is successfully recognizing the CAC by checking that an **Identity Device** is listed in the **Device Manager** under **Smart cards** as shown below.

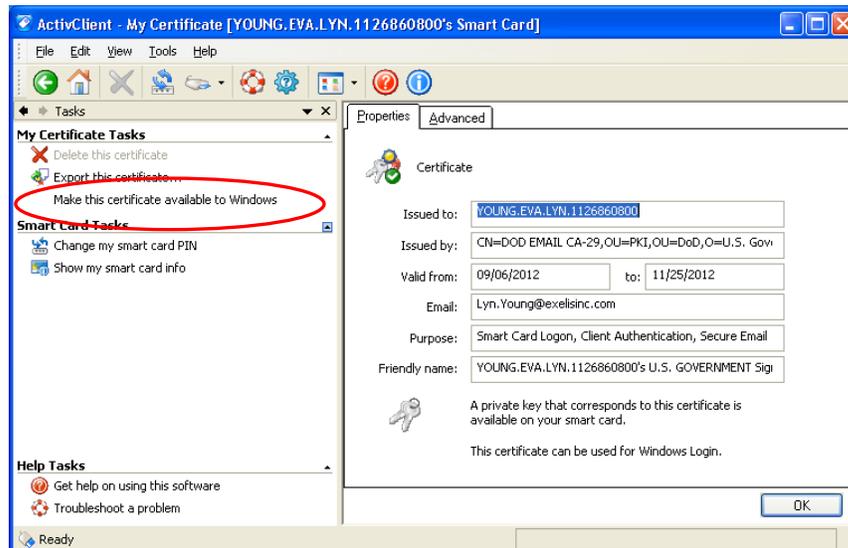


- For Windows 7 with ActivClient middleware:
 - a. Open ActivClient CAC version 6.1 or later.

- b. Select the DOD EMAIL or Signature certificate and View this Certificate.



- c. Select Make this certificate available to Windows.

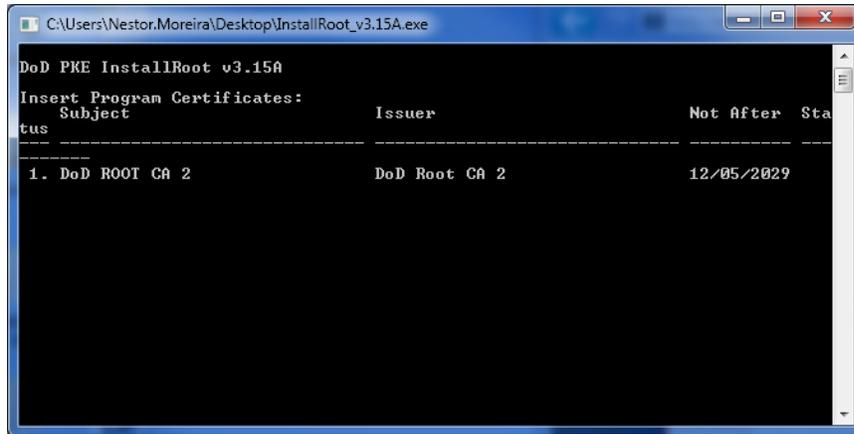


- d. Select **OK** to close.

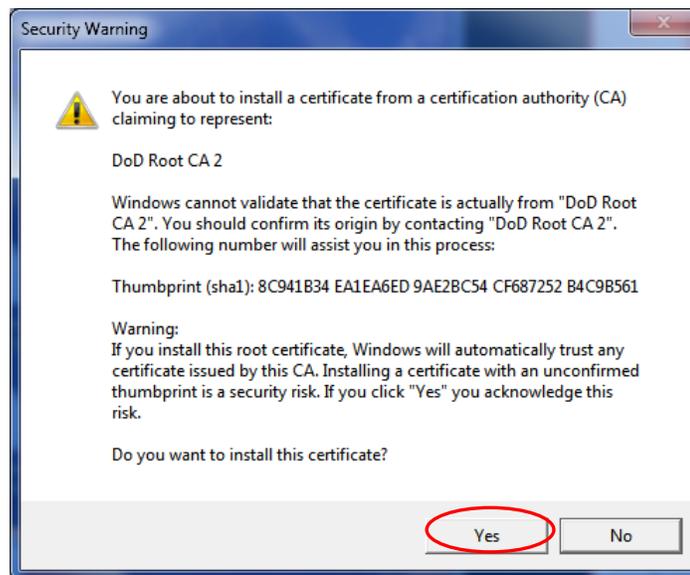
Install DoD Root Certificate and CRL

To Install the DoD Root Certificate:

1. Go to <http://militarycac.com/dodcerts.htm> and follow the instructions for downloading and installing InstallRoot **3.15A.exe** (or latest version as specified by the site). The executable will launch a Windows OS command window.



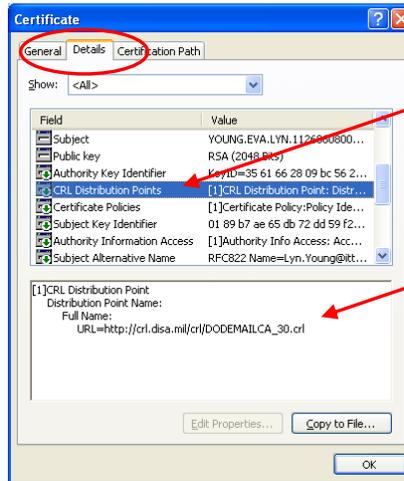
2. Click **Yes**



3. Install the **Certificate Revocation List** file. Certificate Revocation List (CRL) is a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. When a potential user attempts to access a server or application, it allows or denies access based on the CRL entry for that particular user.

Note that Windows caches CRLs when they are fetched from the network, and uses those cached versions until they expire, at which point a newer version of the CRL is fetched and cached. If the cached CRL has expired, or doesn't exist, and a valid version cannot be fetched via the network, then certificate validation will fail and access to the Web Portal will fail.

- View your Signature (aka DOD EMAIL) certificate **Details**. (Refer to the first section for how to view a certificate using ActivClient). Scroll down the details until you find the **CRL Distribution Point**. Copy the URL into your browser and go to the site.



- The site will present a file download dialogue window. Select **Save**.

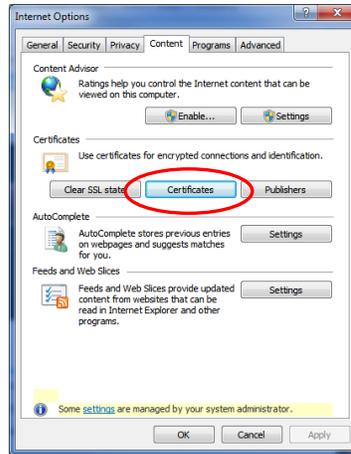


- Right-mouse click on the Certificate Revocation List file that you saved in the step above and select **Install**. Install the file to the default location.
- Close all browser windows.

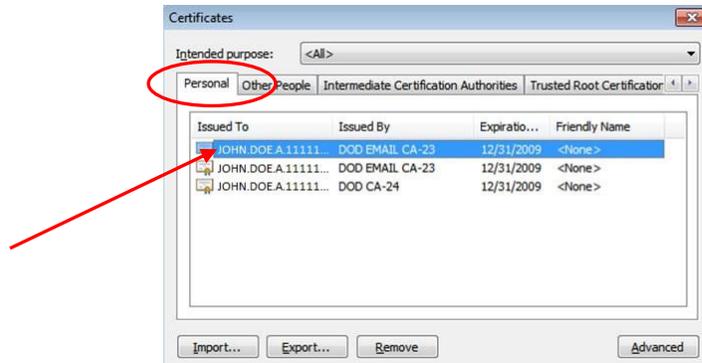
For Microsoft Internet Explorer Users

Microsoft Internet Explorer – Verify your DoD Certificates

1. Open Internet Explorer (IE) and select **Tools > Internet Options > Content (tab)** and select **Certificate**.

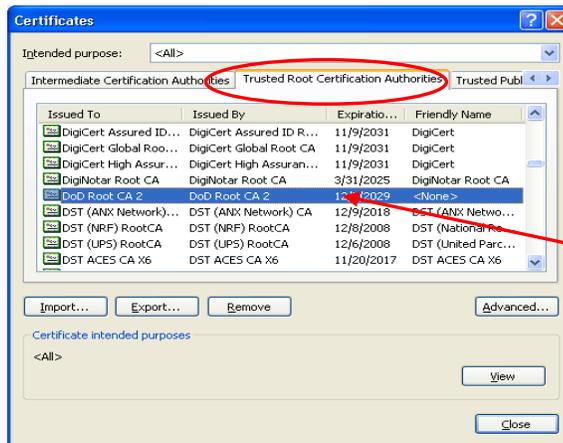


2. The Personal tab should open by default. You should see 3 certificates issued to you by DoD as shown below:

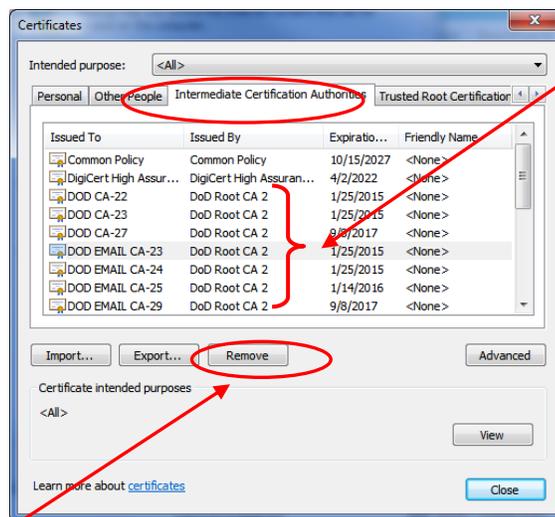


3. The DOD EMAIL (aka signature) certificate is the one you need to use to access the DTCS Web Portal. **Remove** any certificates that are expired, revoked or not yours (unless you share this computer). If your signature certificate is not in the list, stop and contact your Help Desk to get your CAC certificates installed correctly and available to Windows.

- Click the **Trusted Root Certificate Authorities** tab and look for the DoD Root Certificate Authority certificate. DoD Root CA 2 should be in the list. Remove any duplicates, selecting to keep the root certificate with the expiration date that is furthest away.



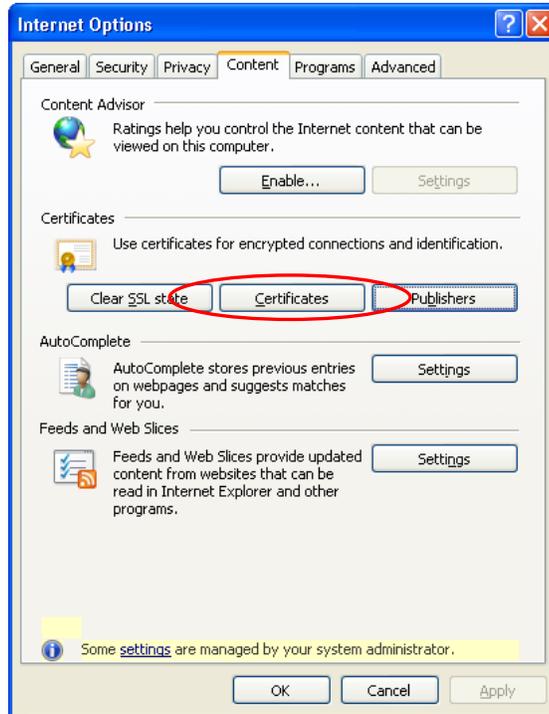
- Click the **Intermediate Certification Authorities** (tab) and look for the DoD certificates. Remove the DOD CA-xx and DOD EMAIL CA-xx intermediary certificates.



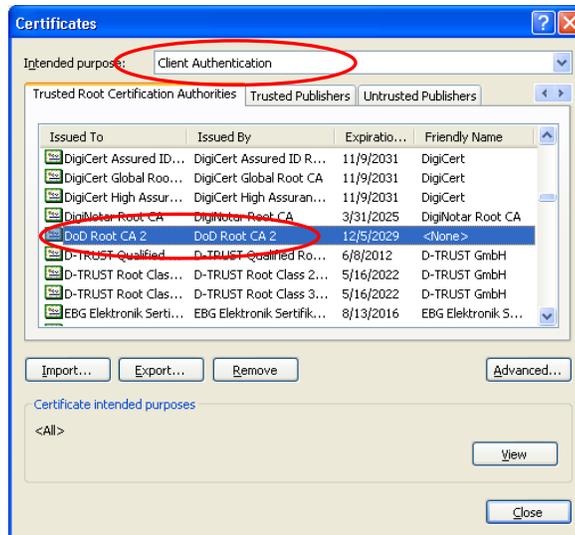
Note: If the Remove (button) is disabled, you may need to close and reopen IE. Right click on the IE executable and select Run as Administrator. If this option is not available to you, contact your System Administrator for support.

- Click **Close**.

7. Select the **Publishers** certificate button from the **Content** tab.



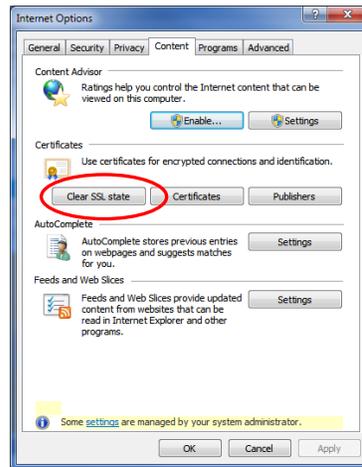
8. Select **Client Authentication** in the **Intended Purpose** dropdown list and look for the DoD Root certificate as shown.



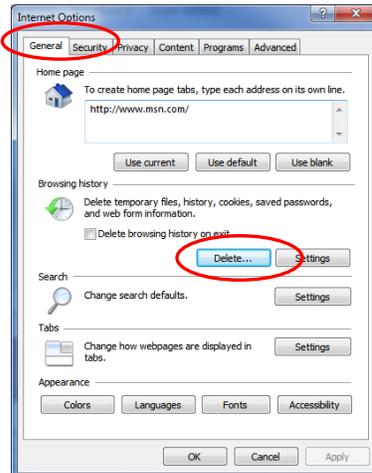
If you did not find the DoD Root certificate listed in step 3 or 6, go back to the previous section and install the DoD Root Certificate. Close Internet Explorer completely after installing the Root Certificate and repeat verification from the beginning of this section.

Fine Tuning Internet Explorer

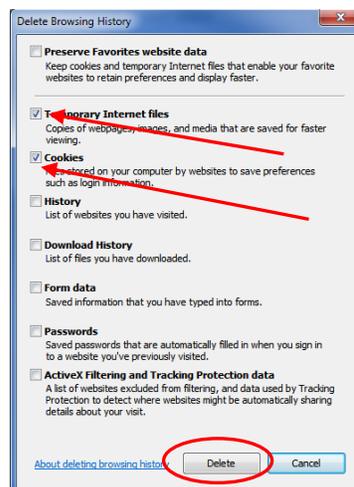
1. Open Internet Explorer (IE) and select **Tools > Internet Options > Content** (tab) and select **Clear SSL state**.



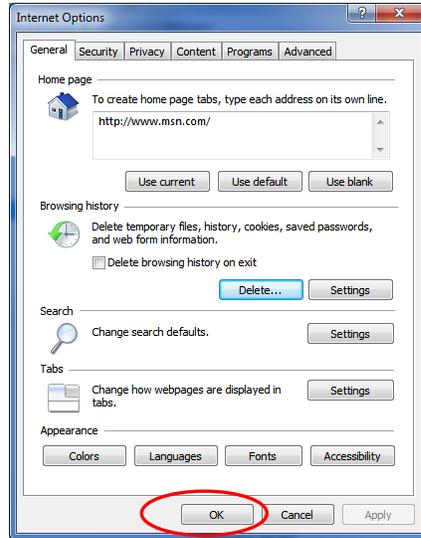
2. Go to the **General** tab and select **Delete**.



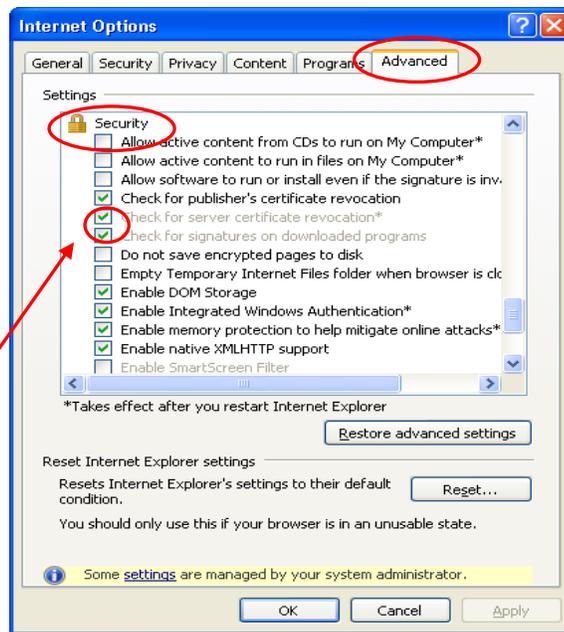
3. Select the 2 check boxes and click **Delete** Temporary Internet Files and Cookies.



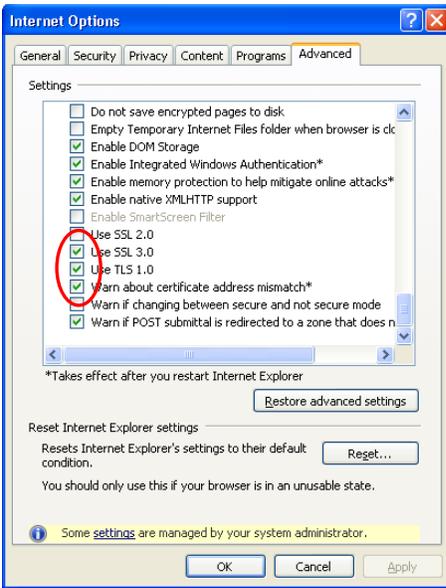
4. Select **OK** to exit.



5. Select the **Advanced** tab and scroll down to the Security section. (NOTE: some settings may be restricted by your System Administrator.)



6. Enable *Check for publisher's certificate revocation*.
7. Also enable *Use SSL 3.0*, *Use TLS 1.0* and *Warn about certificate address mismatch*.



8. Close all browser windows.

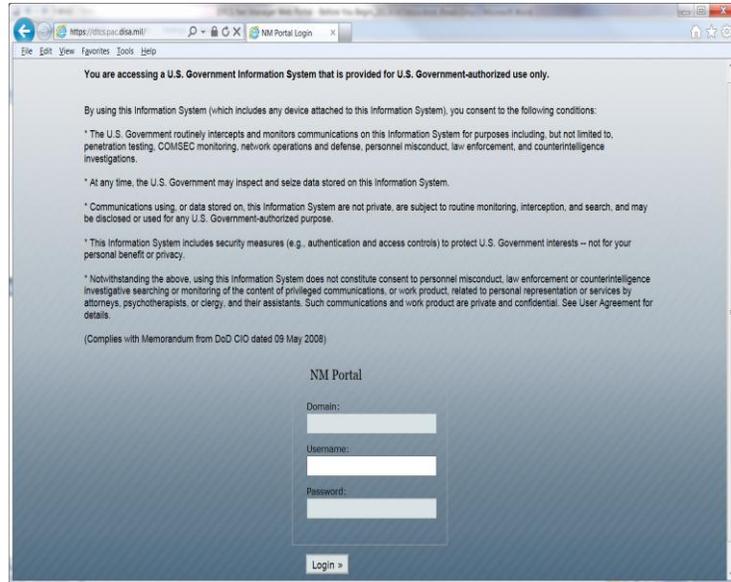
Accessing the DTCS Net Manager Web Portal with Internet Explorer

Open Internet Explorer and go to <https://dtcs.pac.disa.mil>

You will be prompted to select a certificate and enter your Personal Identification Number (PIN) as shown in the screenshots below. Be sure to select your DOD EMAIL certificate.



If successful, you will see the DTCS Net Manager Website as shown below:

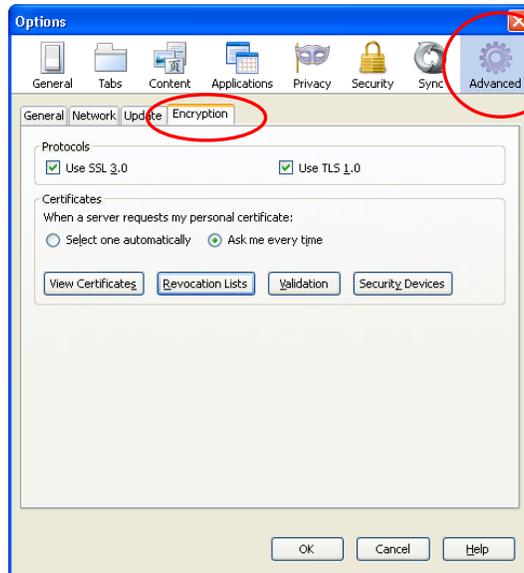


For Mozilla Firefox Users

Firefox Configuration

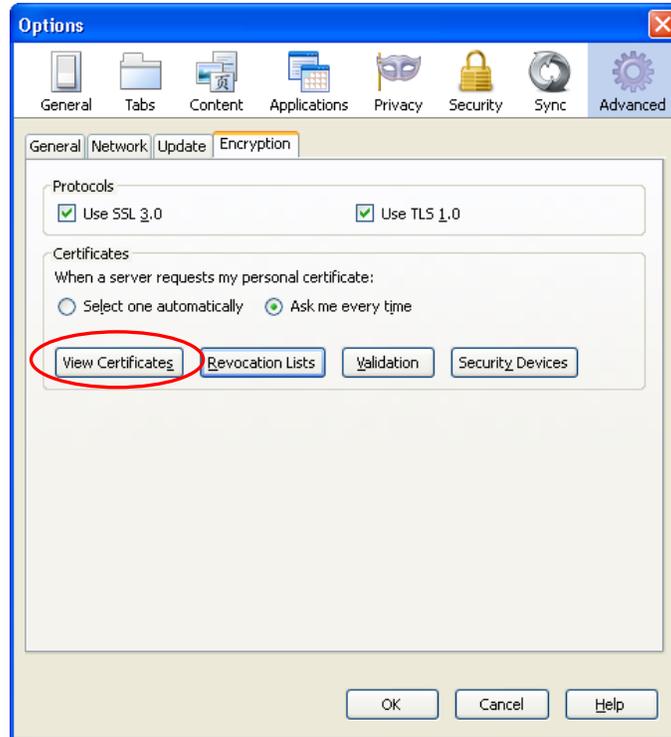
The following steps have not been fully tested or detailed and are offered only as reference in this initial release of this document. Screen shots do not display actual certificate names as of this writing, only where they should be located for verification.

1. Verify Advanced settings. Open Firefox and select **Tools > Options > Advanced > Encryption**

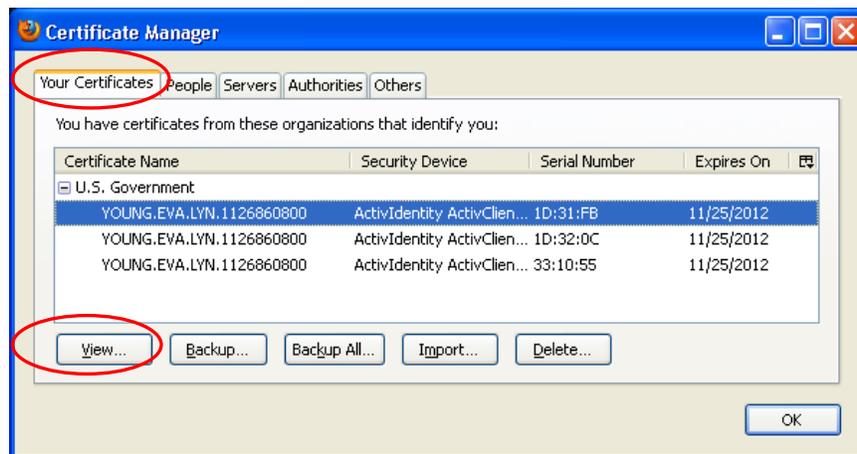


Use SSL 3.0 and Use TLS 1.0 should be enabled (checked).

2. Select **View Certificates**.

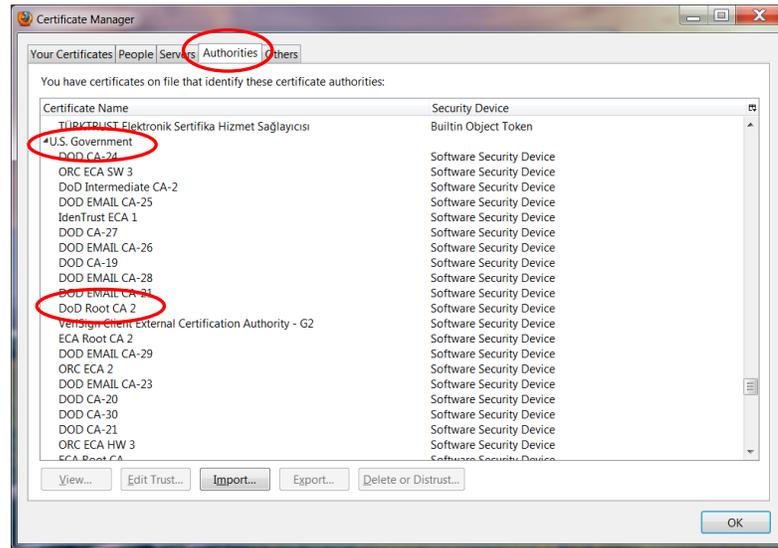


3. **Your Certificates** tab should appear by default. Your personal DOD signature (EMAIL) certificate should show up here:

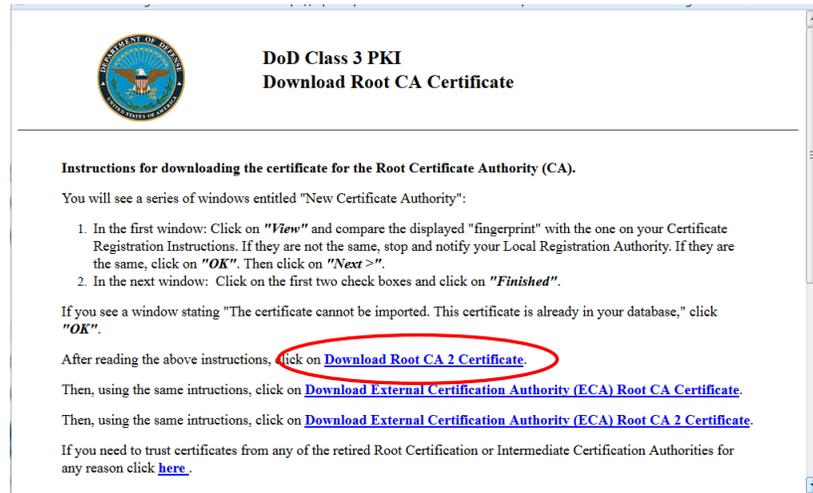


4. Select one from the list and View to find out which one is the Signature (aka DOD EMAIL) certificate. This is the one you need to use to access the DTCS Web Portal. Delete any old or expired certificates. There should only be three (3) (per person, if more than one user shares this computer).

- Select the **Authorities** tab and scroll down the list to see if you have U.S. Government *DoD Root CA 2* certificate.

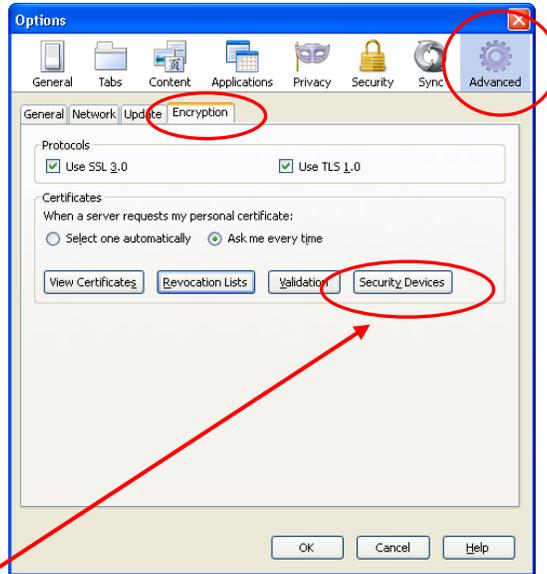


- If the *DoD Root CA 2* is not in the list, use your Firefox browser to go to this website <http://dodpki.c3pki.chamb.disa.mil/rootca.html> and follow the instructions on the page to install only the *DoD Root CA 2* certificate.

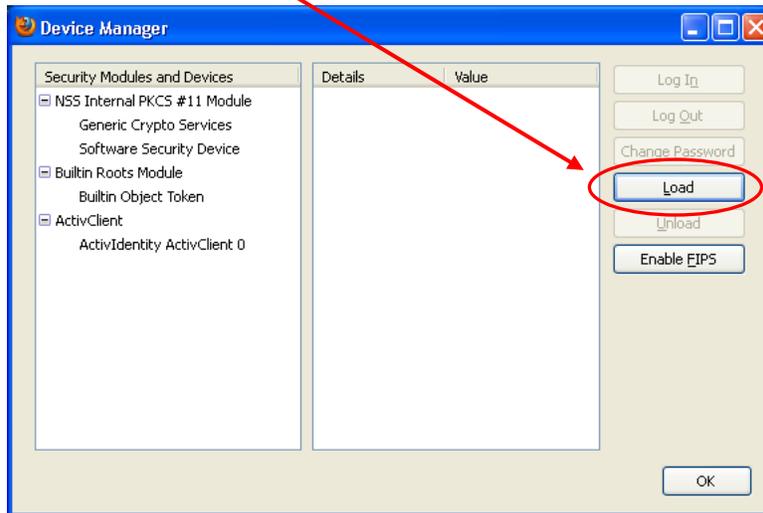


- Close Firefox completely. Repeat Steps 1 & 2 above. If the *DoD Root CA 2* is still not in the list, contact your System Administrator for support. Continue to verify Advanced settings.

8. Go back to **Tools > Options > Advanced > Encryption**

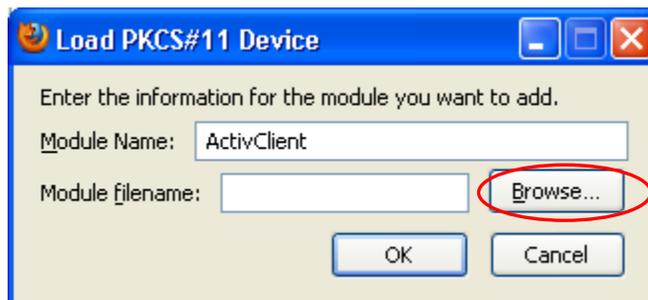


9. Select **Security Devices** and then **Load** (button)



10. Enter the Module Name of your choice (e.g. CAC Reader or ActivClient)

11. Browse to one of the following DLLs, according to your version of ActivClient and operating system.



- ActivClient 6.2 on 32 bit computers: <C:\ProgramFiles\ActivIdentity\ActivClient\acpkcs211.dll> or [acpkcs201-en6.dll](C:\ProgramFiles\ActivIdentity\ActivClient\acpkcs201-en6.dll)

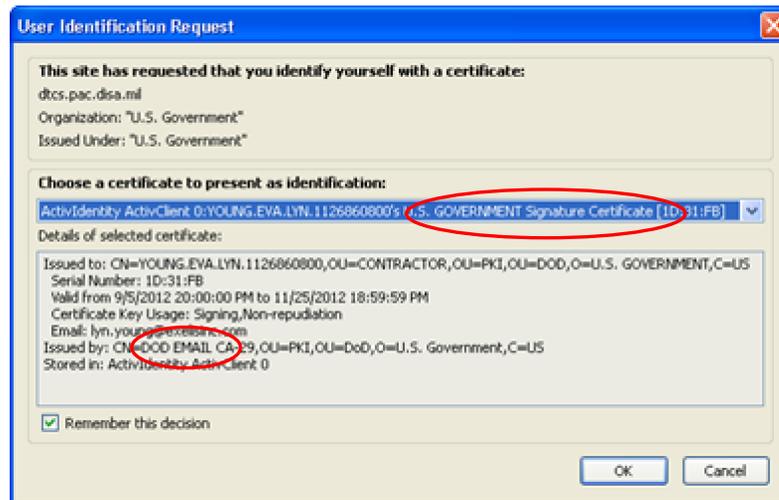
- ActivClient 6.2 on 64 bit computers: [C:\ProgramFiles\(x86\)\ActivIdentity\ActivClient\acpkcs211.dll](C:\ProgramFiles(x86)\ActivIdentity\ActivClient\acpkcs211.dll) or <C:\ProgramFiles\ActivIdentity\ActivClient\acpkcs211.dll>
- ActivClient 6.1 computers: <C:\Windows\System32\acpkcs211.dll> or <acpkcs201-en6.dll>

12. Click **OK** to close.

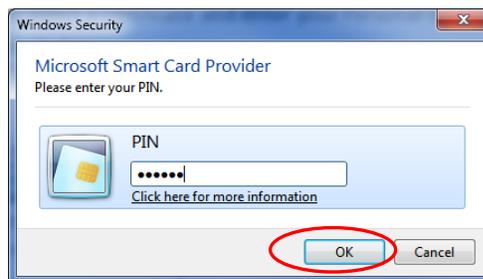
Accessing the DTCS Net Manager Web Portal with Firefox

Open Mozilla Firefox and go to <https://dtcs.pac.disa.mil>

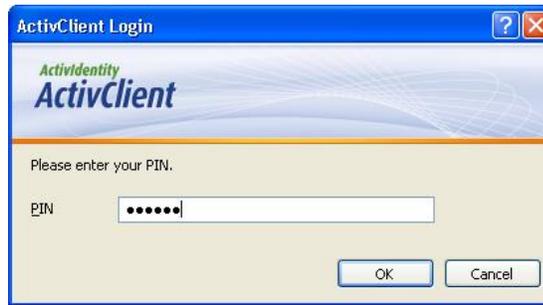
You will be prompted to select a certificate and enter your Personal Identification Number (PIN) as shown in the screenshots below. Be sure to select your DOD EMAIL (aka Signature) certificate.



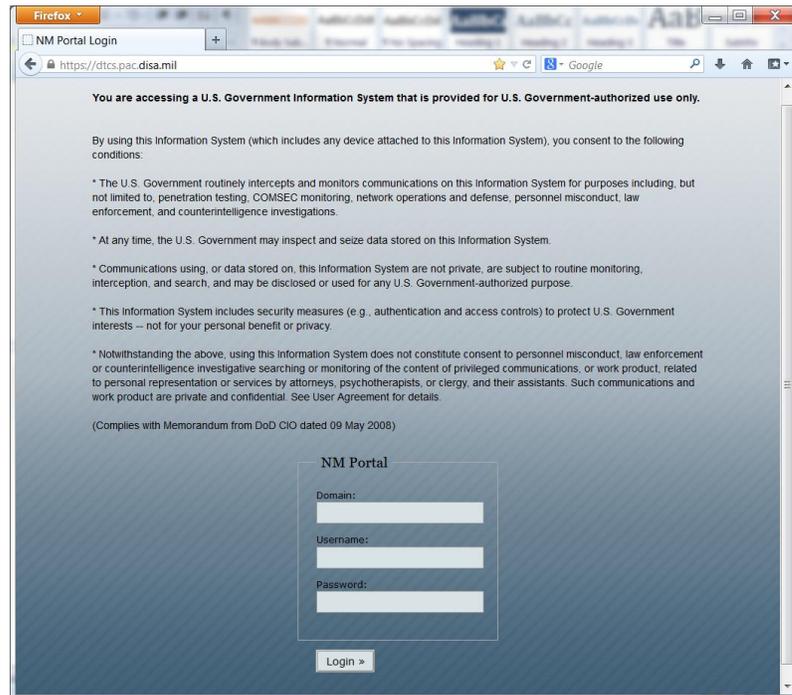
(Windows 7 without ActivClient)



With ActivClient, your view may look like this:



DTCS Net Manager Web Portal login screen



Additional Resources

Firefox SSL errors codes <http://www.mozilla.org/projects/security/pki/nss/ref/ssl/sslerr.html>

Military CAC Firefox resource site <http://militarycac.com/firefox.htm>

Other configuration and troubleshooting steps may be found at

<http://militarycac.com>

http://iase.disa.mil/pki-pke/getting_started/index.html

DTCS Net Manager Support

Monday – Friday 8:30AM – 4:30PM, (US Eastern Time)

(703) 996-2900, option 3

DTCS-Provisioning@exelisinc.com