

**Joint Knowledge Online**  
**CAC Login Troubleshooting Guide**

Updated Thursday, September 13, 2012

## Overview

Some users experience problems accessing JKO using CAC. This problem is often the result of a well known and documented problem with incorrectly configured Internet Explorer settings. This problem is known as the “DoD Root Certificate Chaining Problem” per Defense Information Systems Agency (DISA). DISA has documented the problem and the recommended solution in detail. Please note DISA’s recommended solution requires elevated privileges.

From DISA guidance on the DoD Root Certificate Chaining Problem:

“Department of Defense (DoD) Public Key Enabling (PKE) and the DoD Public Key Infrastructure (PKI) Program Management Office (PMO) have received several reports from DoD services about DoD certificates chaining improperly to cross-certificates or the Common Policy Root Certificate Authority (CA). When this occurs on DoD systems, PKI validation does not work properly.”

“Administrators should run the Federal Bridge Certification Authority (FBCA) Cross-Certificate Removal Tool v1.06 once as an administrator and once as the current user.”

See [DoD Root Certificate Chaining Issue](#) (PDF) for an in depth discussion of this problem and the recommended solution from Defense Information Systems Agency.



The banner features the DoD PKE logo on the left, which includes a padlock icon and the text 'DOD PKE'. The main content is on a purple background with white text. It reads: 'DoD Public Key Enablement (PKE) Frequently Asked Questions', 'DoD Root Certificate Chaining Problem', 'Contact: PKE\_Support@disa.mil', 'URL: http://iase.disa.mil/pki-pke', and 'Enabling PKI Technology for DoD users'.

**DOD PKE**

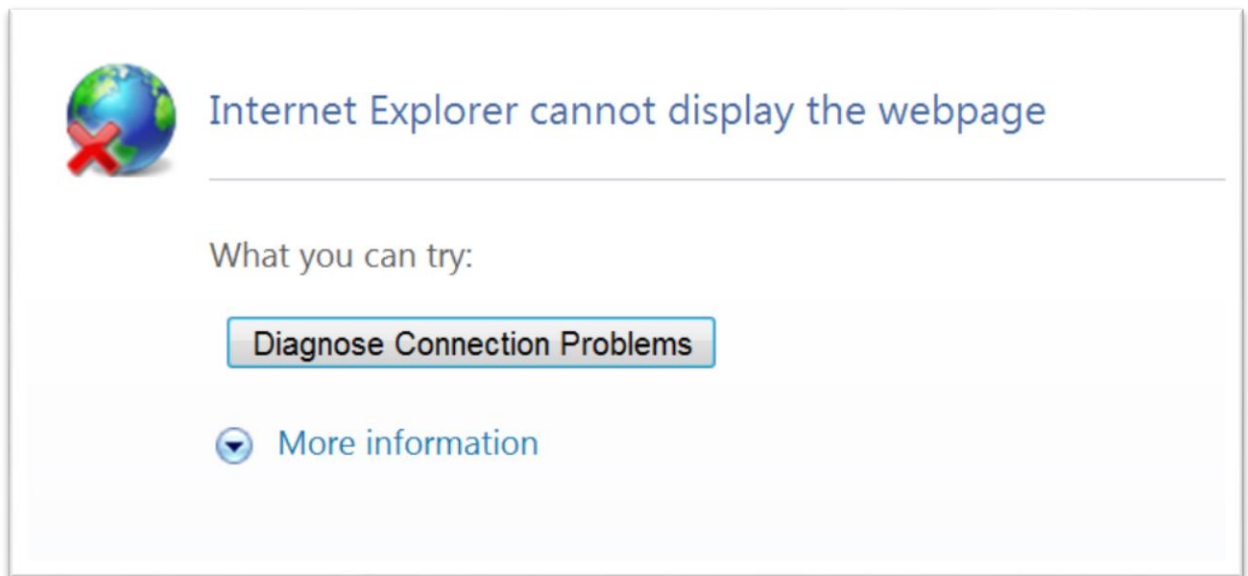
**DoD Public Key Enablement (PKE) Frequently Asked Questions**  
**DoD Root Certificate Chaining Problem**

Contact: PKE\_Support@disa.mil  
URL: <http://iase.disa.mil/pki-pke>

Enabling PKI Technology  
for DoD users

**Problem behavior**

- User can open the JKO login page (<https://jkodirect.jten.mil>)
- User selects “Login using my CAC” link on page
- User is prompted for their CAC certificate
- User selects a certificate and may be prompted for PIN
  - User enters PIN if prompted
- Internet Explorer displays “Cannot display the page”



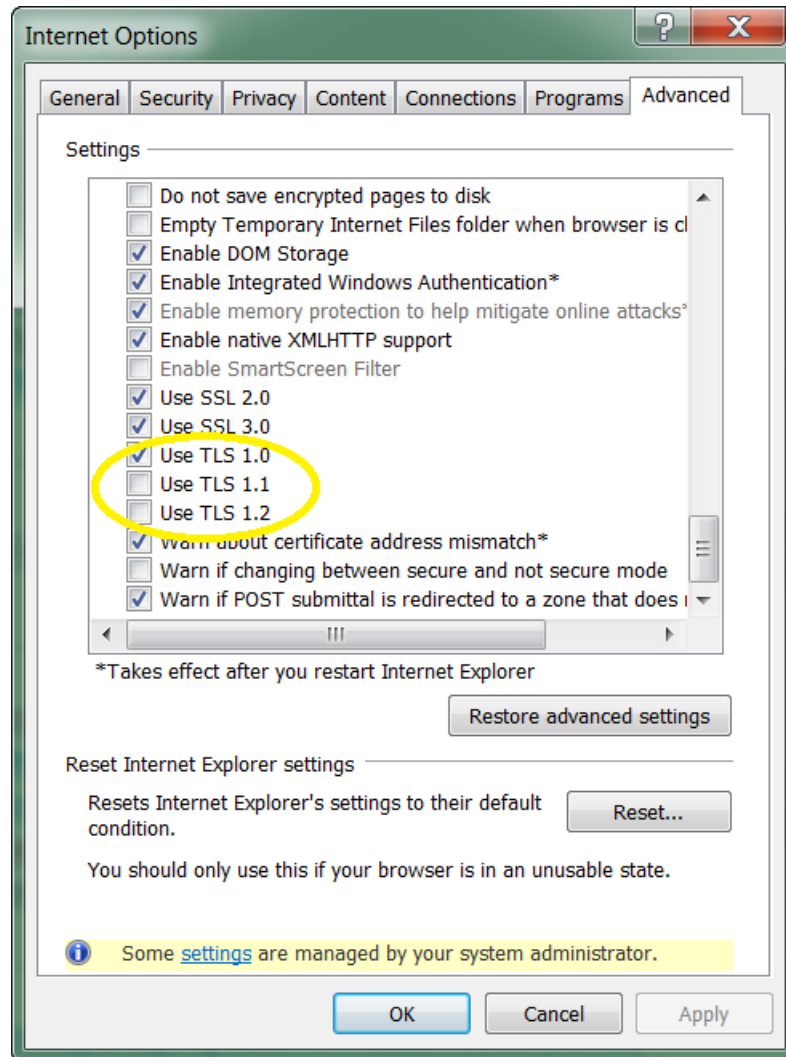
This behavior is often the result of incorrectly configured browser settings. This document shows how to correct the most common causes of the CAC login problem.

**NOTE: Administrative rights are required to complete some or all of the steps outlined below, depending on your local workstation policy. Please request assistance from your local help desk in completing the steps below.**

## TLS options

Ensure only TLS v 1.0 is checked

Open the “Tools – Internet Options” menu item in Internet Explorer and then click the *Advanced* tab



**NOTE:** If you are unable to open “Tools- Internet Options” menu item, please contact your local help desk.

## Internet Explorer Certificates (requires administrative privileges)

There are some certificates that are often included in Internet Explorer that cause problems accessing DoD systems via CAC. Use the DISA tool for correcting this problem.

### Run DISA Federal Bridge Certificate Authority Cross Certificate Remover Tool

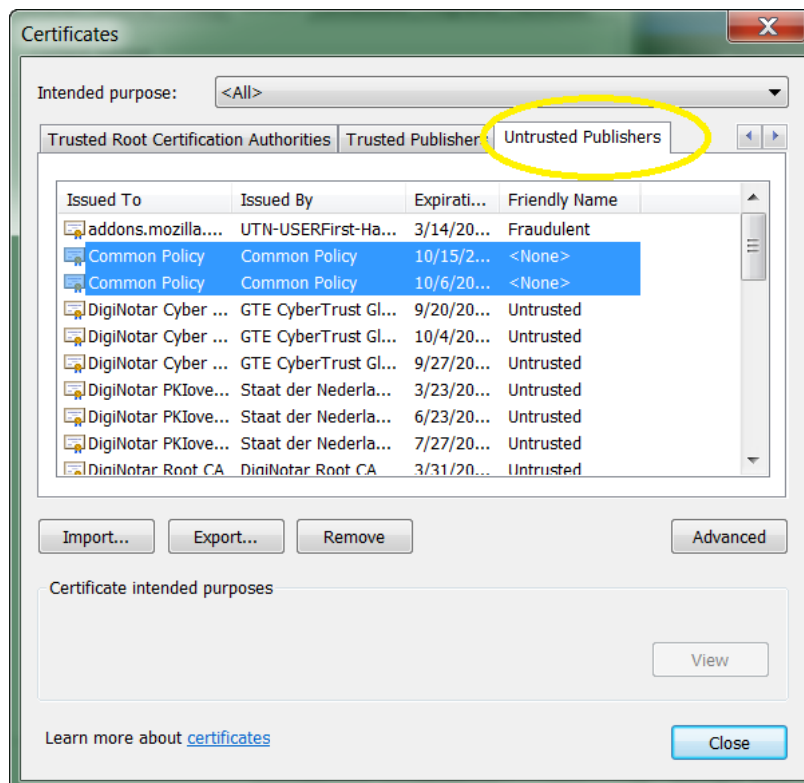
Have an administrator run DISA's Federal Bridge Certification Authority (FBCA) Cross-Certificate Remover Tool on the user's workstation. **The user should then run the FBCA tool again.**

- [DISA FCBA Cross-Certificate Remover Tool](#) (ZIP file containing EXE provided by DISA)
- [FBCA Remover Tool User Guide](#) (PDF user guide provided by DISA)

### Verify Cross Certificate Remove Tool Run

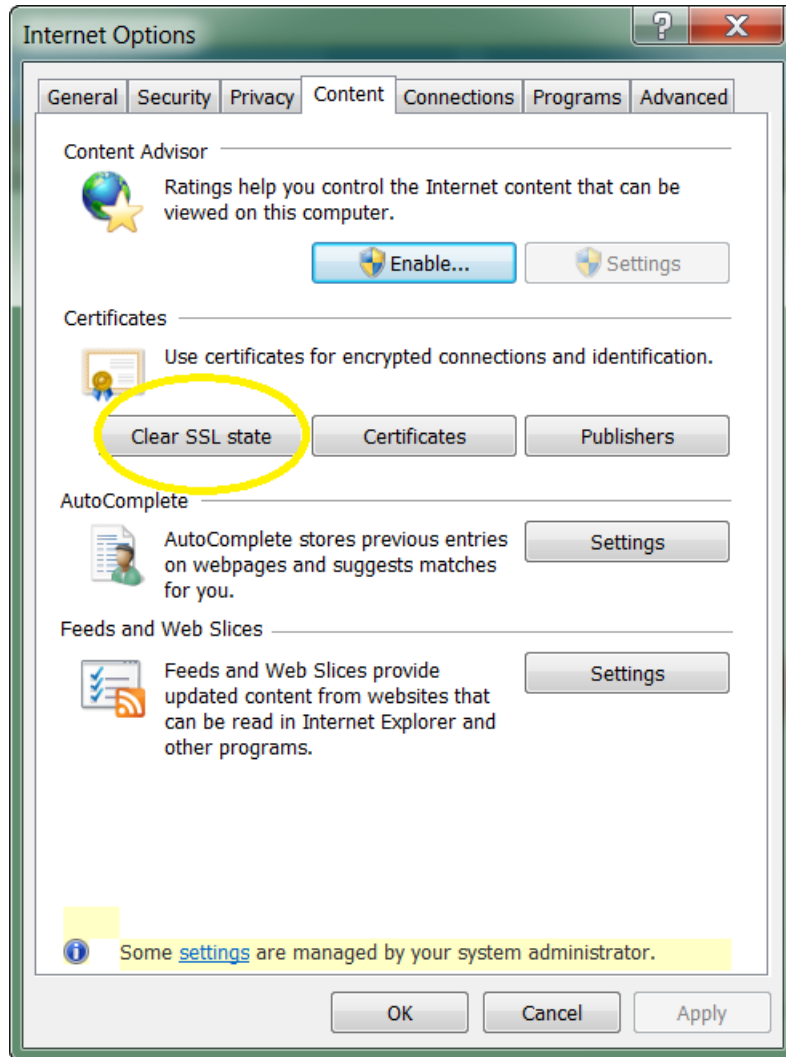
Verify the FBCA Cross-certificate Remover tool placed two Common Policy certificates into the Internet Explorer "Untrusted Publishers" list.

- Open Tools – Internet Options / "Content" tab
- Click the "Certificates" button
- Click the "Untrusted Publishers" tab (you will have to arrow to the right to see it)
- Verify 2 entries Issued to "Common Policy"



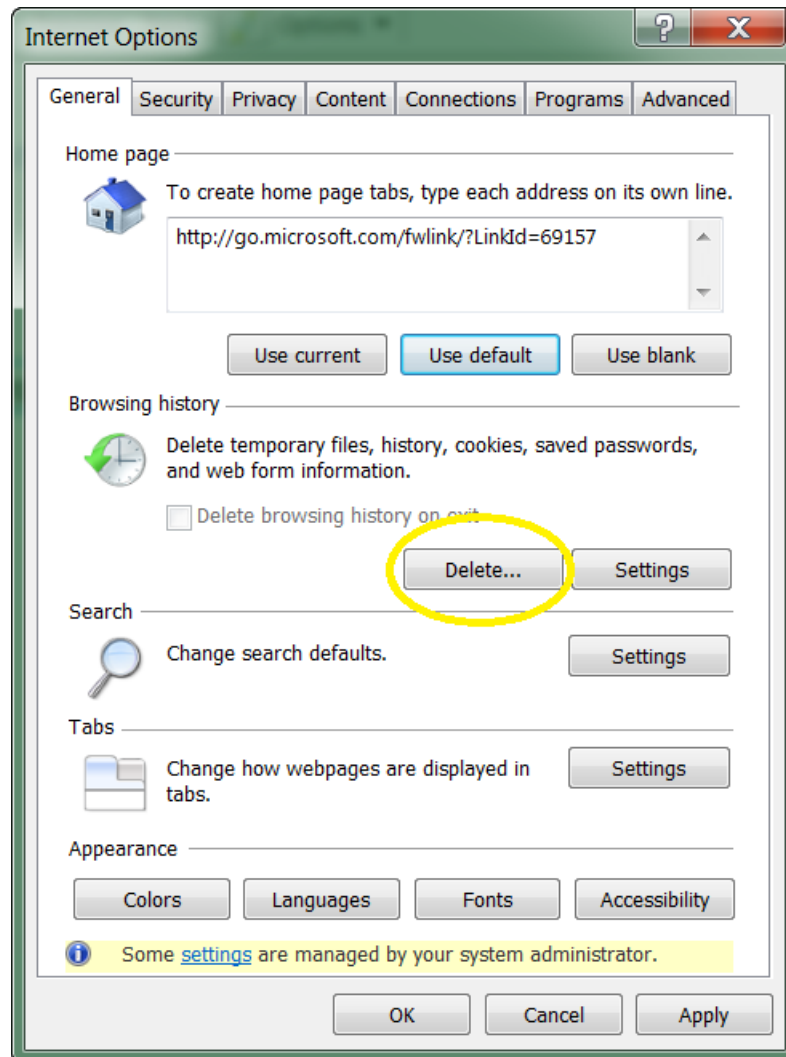
### Clear SSL State

Open the Internet Options – Content tab and click “Clear SSL state” button.



## Clear Browser Cache

Open the Internet Options – Content tab and click “Clear SSL state” button.



## Close all IE windows

Have user close all IE windows

Reopen IE and attempt login to JKO <https://jkodirect.jten.mil> via CAC

For further assistance, please contact the JKO Help Desk

JKO Help Desk  
[JKOHelpdesk@jten.mil](mailto:JKOHelpdesk@jten.mil)  
757 203-5654 (Commercial)  
668-5654 (DSN)