Joint Knowledge Online

CAC Login Troubleshooting Guide

Updated Thursday, September 13, 2012

UNCLASSIFIED

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 <u>DoD Root Certificate Chaining Issue</u> (PDF) for an in depth discussion of this problem and the recommended solution from Defense Information Systems Agency.



Problem behavior

- User can open the JKO login page (<u>https://jkodirect.jten.mil</u>)
- 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"

Ø	Internet Explorer cannot display the webpage
	What you can try: Diagnose Connection Problems More information

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

Internet Options	? X				
General Security Privacy Content Connections Programs	Advanced				
Settings					
 Do not save encrypted pages to disk Empty Temporary Internet Files folder when browse ✓ Enable DOM Storage ✓ Enable Integrated Windows Authentication* ✓ Enable memory protection to help mitigate online at ✓ Enable native XMLHTTP support Enable SmartScreen Filter ✓ Use SSL 2.0 ✓ Use SSL 3.0 ✓ Use TLS 1.1 Use TLS 1.1 Use TLS 1.2 ✓ Warn about certificate address mismatch* Warn if changing between secure and not secure m ✓ Warn if POST submittal is redirected to a zone that 	tacks*				
< III	•				
*Takes effect after you restart Internet Explorer					
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.					
Some settings are managed by your system administrator.					
OK Cancel	Apply				

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"

Certificates					
Intended purpose:	<all></all>			•	
Trusted Root Certification	on Authorities Trusted	Publisher	Untrusted Publishe	ers · ·	
Common Policy	Common Policy GTE CyberTrust Gl	10/15/2 10/6/20 9/20/20	<none> <none> Untrusted</none></none>		
DigiNotar Cyber DigiNotar PKIove DigiNotar PKIove	Staat der Nederla Staat der Nederla	9/27/20 3/23/20 6/23/20	Untrusted Untrusted Untrusted	Ŧ	
Import Expo				Advanced	
				View	
Learn more about <u>certifi</u>	<u>cates</u>			Close	

Clear SSL State

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

Internet Options				
General Security Privacy Content Connections Programs Advanced				
Content Advisor Ratings help you control the Internet content that can be viewed on this computer.				
Certificates Use certificates for encrypted connections and identification.				
Clear SSL state Certificates Publishers AutoComplete				
AutoComplete stores previous entries Settings on webpages and suggests matches for you.				
Feeds and Web Slices				
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.				
Some <u>settings</u> are managed by your system administrator.				
OK Cancel Apply				

Clear Browser Cache

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

Internet Options					
General Security Privacy Content Connections Programs Advanced					
Home page To create home page tabs, type each address on its own line.					
http://go.microsoft.com/fwlink/?LinkId=69157					
Use current Use default Use blank					
Browsing history					
Delete temporary files, history, cookies, saved passwords, and web form information.					
Delete browsing history on evit					
Delete Settings					
Search					
Change search defaults. Settings					
Tabs					
Change how webpages are displayed in Settings tabs.					
Appearance					
Colors Languages Fonts Accessibility					
Some <u>settings</u> are managed by your system administrator.					
OK Cancel Apply					

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 757 203-5654 (Commercial) 668-5654 (DSN)