# DISS JVS JVS Troubleshooting Guide

Version 1.0 DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY July 23, 2021



# **REVISION HISTORY**

DATE	VERSION	CHANGE DESCRIPTION	AUTHOR
07/23/2021	1.0	Published Version	DCSA

# **Table of Contents**

OVERVIEW	3
TROUBLESHOOTING STEPS	4
<ul> <li>2.1 Refresh the Page</li> <li>2.2 Remove CAC/Smart Card</li> <li>2.3 Update Browser Settings</li> <li>2.3.1 Internet Explorer</li> </ul>	4 4
<ul> <li>2.3.1.1 Clear the SSL state</li></ul>	6 7
<b>2.3.3 Chrome</b>	1
2.3.3.1 Clear SSL State	3
2.4 Install Required Certificates	
<b>2.5.1 Internet Explorer</b>	





# **1.0 Overview**

In order to maintain the highest security standards and optimal performance, the JVS application is currently supported by certain browsers, operating systems, and security requirements. To access JVS, users first go to the JVS website (<u>https://dissportal.nbis.mil/diss-jvs-ui/faces/consent.jsp</u>). When logging into JVS, you may experience access barriers like the ones shown below. This document provides recommended troubleshooting steps for mitigating JVS access issues. Please note that depending on your organization's security restrictions, you may need to consult your IT department for additional support.

Can't connect security to t × S Can't connect security to t × S Rie Edit. View Favorites 'Bools Help	
Can't connect securely to this page	
This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website's owner.	
Your TLS security settings aren't set to the defaults, which could also be causing this error.	
Try this:	
Go back to the last page	
Charge settings	

Image 1 Can't connect securely error page in Internet Explorer

#### Image 2 404 Error Page

	X 📓 Status Dashboard	X Error 404Not Found	🗙 🧕 DES-CATS - Reports Re-desig - X – 📲 NS, Reports als	× +	
- → C @	🖲 🔏 🛱 jesappöžhą.	workscorp.com/8002/disa-jvs-ui/8	aces/consent.jsp	90% ··· 🖾 🗘	¥ W @ @ @ :
rror 404Not F	ound				
From RFC 2068 Hyp	pertext Transfer Protocol H	TTP/1.1:			
10.4.5 404 Not Found			ation is given of whether the condition is temp	porary or permanent.	
10.4.5 404 Not Found The server has not	found anything matching th	he Request-URI. No indic			

The 404 error appears when the application is not running on the managed servers. Effective August 2, 2021 users should contact the DCSA DISS Customer Engagements Team (CET), 727-794-7765 or email <u>dcsa.ncr.nbis.mbx.contact-center@mail.mil</u> for assistance with this error message.



# 2.0 Troubleshooting Steps

JVS is currently supported by Internet Explorer version 11, Firefox version 11 and Chrome. Using these browsers minimizes access issues as they are more compatible with the JVS application. Note that certain browser settings need to be updated with the correct security protocols required to access JVS. Follow steps below to troubleshoot access barriers.

**Note for Windows Users:** Windows 8.1 and 10 are most compatible with the JVS application. Several users have experienced access issues when using Windows 7 or older versions. To check for operating system information, reference the Microsoft Support guidance.

Note for Mac Users: There are currently no recommended Mac operating systems.

*Note:* The following instructions apply to computers with a Windows-based operating system.

# 2.1 Refresh the Page

Try refreshing the <u>https://dissportal.nbis.mil/diss-jvs-ui/faces/consent.jsp</u> page when any of the error messages above display:

- Press the F5 key on your keyboard or click the refresh symbol in your browser.
- Refresh multiple times. If the page continues to not load correctly, follow the steps below.

### 2.2 Remove CAC/Smart Card

Try removing your CAC or Smart Card from your device:

- Close any open browsers.
- Remove your CAC, ECA token, PKI token, or Smart Card.
- Insert your card again then re-open the browser.
- Try logging into JVS again. If you continue to encounter the error page, try the steps in the "Update Browser Settings" section of this guide for either <u>Internet Explorer</u>, <u>Firefox</u> or <u>Chrome</u> browsers

## 2.3 Update Browser Settings

Users may have to update certain settings in their browser in order to resolve their access issue. Some examples including clearing the cache, deleting browsing history, updating "Trusted Sites", and reconfiguring the SSL/TSL setting. This section is divided by instructions specific to Internet Explorer, Firefox, and Chrome.





#### 2.3.1 Internet Explorer

#### 2.3.1.1 Clear the SSL state.

• Open the browser. Click "Tools", or the **gear icon**, in the top right corner of the browser then select **Internet Options**.



- From the "Internet Options" window, click the Content tab.
- Click the Clear SSL state button.

nternet Options		?
General Security Privacy Con	tent Connections Progr	ams Advanced
Certificates Use certificates for	encrypted connections a	and identification.
Clear SSL state	Certificates	Publishers
AutoComplete		
	res previous entries suggests matches for	Settings
Feeds and Web Slices		
	ces provide updated ites that can be read er and other	Settings

• Click the **OK** button on the confirmation message.



- Exit out of the Internet Options window then exit the browser. Re-open the browser.
- Try accessing JVS again.



#### 2.3.1.2 Delete browsing history:

- Open the browser. Click "Tools", or the **gear icon**, in the top right corner of the browser then select **Internet Options**.
- From the "General" tab, click the **Delete...**button.

Internet Opt	ions	?	×
General Sec	urity Privacy Content Connections Programs	Advanced	
Home page	9		-
	To create home page tabs, type each address of	on its own line.	
	http://dssinside.dss.mil/default.aspx	1	
			/
	Use current Use default	Use new tab	
Startup —			- 1
Start	with tabs from the last session		
<ul> <li>Start</li> </ul>	with home page		
Tabs —			- 1
Change	how webpages are displayed in tabs.	Tabs	
Browsing h	istory		_
	emporary files, history, cookies, saved password privation.	ls, and web	
Delet	e browsing history on exit		
	Delete	Settings	

• From the "Delete Browsing History" window, **select the first three checkboxes** as shown below.Click the **Delete** button.



• Exit out of the Internet Options window then exit the browser. Re-open the browser.



• Try accessing JVS again.

#### 2.3.1.3 Update Trusted Sites:

- Open the browser. Click "Tools", or the **gear icon**, in the top right corner of the browser then select **Internet Options**.
- From the "Internet Options" window, click the **Security** tab then click the **Sites** button.



• Verify or add <u>https://dissportal.nbis.mil/diss-jvs-ui/faces/consent.jsp</u> to the list of trusted sites. Click the **Add** button to add the site. Click the **Close** button when done.

Trusted sites	×
You can add and remove websites from this zone. All website this zone will use the zone's security settings.	s in
Add	
Websites:	
*.29palmsbomi-nsn.gov *.absenteeshawneetribe-nsn.gov *.access-board.gov *.acom.mil	
*.adInet.gov	
Require server verification (https:) for all sites in this zone	

**Note:** Some users might not have permissions needed to complete this step as demonstrated by the greyed-out buttons in the screenshot above. If these permissions are disabled, contact your IT Administrator for additional support.

- Exit out of the Internet Options window then exit the browser. Re-open the browser.
- Try accessing JVS again.

#### 2.3.1.4 Update SSL and TLS criteria:

Click "Tools", or the **gear icon**, in the top right corner of the browser then select **Internet Options**.



• From the "Internet Options" window, click the Advanced tab.

Enable Enhanced Protected Mode*	Enable Integrated Windows Authentication*	<ul> <li>Enable Enhanced Protected Mode*</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable SmartScreen Filter</li> <li>Enable SmartScreen Filter</li> <li>Use SSL 2.0</li> <li>Use SSL 3.0</li> <li>Use TLS 1.0</li> <li>Use TLS 1.1</li> <li>Use TLS 1.2</li> <li>Warn about certificate address mismatch*</li> <li>Warn if changing between secure and not secure mode</li> </ul>	Enable Enhanced Protected Mode* Enable Integrated Windows Authentication* Enable SmartScreen Filter Enable SmartScreen Filter Enable Strict P3P Validation* 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 n * Takes effect after you restart your computer	Enable Enhanced Protected Mode* Enable Integrated Windows Authentication* Enable SmartScreen Filter Enable Strict P.P Validation* 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 n * Takes effect after you restart your computer Restore advanced settings		rity Privacy	Content	Connections	Programs	Advanced
Enable Integrated Windows Authentication*     Enable native XMLHTTP support	✓       Enable Integrated Windows Authentication*         ✓       Enable smartScreen Filter         Enable SmartScreen Filter       Enable Strict P3P Validation*         Use SSL 2.0       Use SSL 3.0         Use SL 3.10       ✓         ✓       Jse TLS 1.1         ✓       Use TLS 1.2         ✓       Warn about certificate address mismatch*         ✓       Warn if changing between secure and not secure mode	<ul> <li>Enable Integrated Windows Authentication*</li> <li>Enable states XMLHTTP support</li> <li>Enable Strict P3P Validation*</li> <li>Use SSL 2.0</li> <li>Use SSL 2.0</li> <li>Use TLS 1.0</li> <li>Use TLS 1.1</li> <li>Use TLS 1.1</li> <li>Use TLS 1.2</li> <li>Warn about certificate address mismatch*</li> <li>Warn if changing between secure and not secure mode</li> <li>Warn if POST submittal is redirected to a zone that does n</li> </ul>	<ul> <li>Enable Integrated Windows Authentication*</li> <li>Enable shartScreen Filter</li> <li>Enable SmartScreen Filter</li> <li>Enable Strict P3P Validation*</li> <li>Use SSL 2.0</li> <li>Use SSL 3.0</li> <li>Use TLS 1.0</li> <li>Use TLS 1.1</li> <li>Use TLS 1.2</li> <li>Warn about certificate address mismatch*</li> <li>Warn if changing between secure and not secure mode</li> <li>Warn if POST submittal is redirected to a zone that does n</li> <li>*Takes effect after you restart your computer</li> </ul>	<ul> <li>Enable Integrated Windows Authentication*</li> <li>Enable shartScreen Filter</li> <li>Enable Shirt P.PP Validation*</li> <li>Use SSL 2.0</li> <li>Use SSL 3.0</li> <li>Use TLS 1.0</li> <li>Use TLS 1.1</li> <li>Use TLS 1.2</li> <li>Warn about certificate address mismatch*</li> <li>Warn if changing between secure and not secure mode</li> <li>Warn if POST submittal is redirected to a zone that does n</li> <li>Takes effect after you restart your computer</li> <li>Restore advanced settings</li> </ul>	Settings				0 10	
Enable Strict P3P Validation* Use SSL 2.0 Use SSL 3.0 Use TLS 1.0 Use TLS 1.1 Warn about certificate address mismatch* Warn if changing between secure and not secure mode	· · · · · · · · · · · · · · · · · · ·	۰ III ۲	*Takes effect after you restart your computer	*Takes effect after you restart your computer Restore advanced settings	V En V En En Us Us V Us V Us V Wi	hable Integrate hable native XP hable SmartScr hable Strict P38 se SSL 2.0 se SSL 3.0 se TLS 1.0 se TLS 1.1 se TLS 1.2 /arn about cert /arn if changing	ed Window «LHTTP su een Filter Validation tificate add	s Authenticatio opport * Iress mismatch secure and no	* t secure mod	
*Takes effect after you restart your computer Restore advanced settings Reset Internet Explorer settings to their default condition.	Reset Internet Explorer settings           Resets Internet Explorer's settings to their default         Reset	Reset Internet Explorer's settings to their default Reset	Resets Internet Explorer's settings to their default Reset		You should	only use this it	f your brov	vser is in an un	usable state	•1

- Scroll to the Security section and uncheck SSL 2.0, SSL 3.0, TLS 1.0, and check TLS 1.1 and TLS 1.2.
- Click the **OK** button.

**Note:** Some users might not have the permissions needed to complete this step. If these permissions are disabled, contact your IT Administrator for additional support.

- Exit out of the Internet Options window then exit the browser. Re-open the browser.
- Try accessing JVS again. If you continue to encounter access issues, proceed to <u>Install</u> <u>Required Certificates</u> section of this guide.
- 2.3.2 Firefox

#### 2.3.2.1 Clear Cookies and Site Data:

• Open Firefox - click the **Menu** button (3 horizontal line icon) then select **Options**.





• Select Privacy and Security then click the Clear Data button.

🛱 General	Choose what to block.	
Home	Send websites a "Do Not Track" signal that you don't want to be tracked I	eam more
Privacy & Security	Only when Firefox is set to block known trackers	
C Sync	Cookies and Site Data	
	Your stored cookies, site data, and cache are currently using 193 MB of	Clear Data
	disk space. Learn more	Manage Data
	Delete cookies and site data when Firefox is closed	Manage Permissions

• Click the Clear button.



- Exit the browser then re-open the browser.
- Try accessing JVS again.

#### 2.3.2.2 Change browser TLS configuration:

• Open Firefox - in the address bar, type **about:config** and press **Enter**.

out:config	× +		
-) -> C @	Sirefox	about:config	



Note: If you receive the message below, click the I accept the risk button to proceed.

abo	utconfig	× +		1.0		0	×
+) → 9 Welco	C <sup>e</sup> ගි me∣DSS Portal	C Firefox aboutconfig	\$	μι\		۲	-
	Th	is might void your warranty	I				
		s might tota jour namany					
		jing these advanced settings can be harmful to the stabili d only continue if you are sure of what you are doing.	ity, security, and performance of	this application	n. You	l.	
	🗸 S	how this warning next time					
	- La	ccept the riskl					
	6						

- In the Search field, enter "security.tls.version.max".
- Find and double-click the listed entry.
- Under the Value column, set the integer to 4.

about:config	× +			
$\leftarrow \rightarrow C^{*}$	Sion.max	fig		
Preference Name		▲ Status	Туре	Valu

**Note**: If the issue persists or if you run into a different access issue, proceed to the next section.

#### 2.3.3 Chrome

#### 2.3.3.1 Clear SSL State

- Select the 3 vertical dots in the upper right and select the **Settings** icon, and then click **Settings**.
- Click Show Advanced Settings.
- Select **System**, then Open your computer's proxy settings



← →	C O Chrome   chrome://settin		★      ★
Setti	ings	Q. Search settings	
÷	You and Google	System	
Ê	Autofill	Continue running background apps when Google Chrome is closed	-
0	Safety check		
0	Privacy and security	Use hardware acceleration when available	
۲	Appearance	Open your computer's proxy settings	
Q	Search engine		
	Default browser	Reset and clean up	
U	On startup	Restore settings to their original defaults	
Advar	nced *	Clean up computer	$\mathbf{x}$
۲	Languages		
<u>+</u>	Downloads		
ŧ	Accessibility		
٩	System		
Ð	Reset and clean up		
Exten	sions 🖸		

- Click Change Proxy Settings. The Internet Properties dialog box appears.
- Click the **Content** tab.
- Click Clear SSL state, and then click OK.





#### 2.3.3.2 Clear Cookies and Browsing Data

 On your computer, open Chrome. Select the 3 vertical dots in the upper right and select the Settings icon, and then click Settings.

Click More Tools. Click Clear Browsing Data.

• At the top, choose a time range. To delete everything, select **All time**.

• Check the boxes next to "Cookies and other site data" and "Cached images and files."

• Click Clear data.

Cle	ar browsir	ng data			
	1	Basic		Advance	d
Tim	e range l	.ast hour	Ŧ		Â
	Browsing 5 items	history			
	Downloa None	d history			
	Cookies From 11	and other site data sites			
	Cached in Less thar	mages and files n 640 MB			
	Passwore None	ds and other sign-in dat	a		
	Autofill fo	orm data			•
				Cancel	Clear data

#### 2.3.3.3 Change Browser TLS Configuration

- On your computer, open Chrome. Select the 3 vertical dots in the upper right and select the Settings icon, and then click Settings.
  - Scroll down and select Show advanced settings
  - Select System and click Open your computer's proxy settings
  - Select the Advanced tab.
  - Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2.



• Click OK.



## 2.4 Install Required Certificates

While most computers automatically recognize public Certification Authorities (CAs) that are trusted to validate the identity of secure (HTTPS) websites, many .MIL sites are verified through private DoD CAs whose certificates require manual installation by a local system administrator. IT departments within the DoD typically install and update these certificates for their employees automatically, but there are occasions that updates do not reach all user workstations and a manual installation becomes necessary. Non-DoD agencies, private sector organizations and home users do not typically have DoD CA certificates installed on their computers requiring manual installation.

Follow the instructions below to install the required PKI certificates for DoD websites by accessing the following link: <u>https://militarycac.com/dodcerts.htm</u>

## 2.5 Remove Revoked Certificates

#### 2.5.1 Internet Explorer

Now that the new certificates have been installed, you will need to ensure that certain revoked certificates are not reflected in your system. To do so, please click on your Windows **Start** menu and type "**Internet Options**" in the search bar; press **ENTER**. Windows 10 users may type the same text in their Cortana ("Ask me anything") search field on the Windows Taskbar.

命	Best match
	Control panel
	Settings
	Block or allow pop-ups
\$	
	$\mathcal{P}$ internet options

**Note**: Alternatively, open Internet Explorer  $\rightarrow$  click the **gear icon** ("Tools")  $\rightarrow$  select **Internet Options**.



• Click on the **Content** tab at the top of the Internet Options window and select **Certificates**.



• Select the tab for Intermediate Certification Authorities.

Personal Other Pe	ople Intermediate	Certificatio	on Authorities	Trusted Root Certification	ו Auth
Issued To	Issued By	Expir	Friendly N		^
DOD CA-27	DoD Root CA 2		· · · ·		
DOD CA-28	DoD Root CA 2				
DOD CA-29	DoD Root CA 2				
DOD CA-30	DoD Root CA 2	9/8/2	<none></none>		
DOD CA-31					
DOD CA-31	DoD Root CA 2	1/16/	<none></none>		
DOD CA-32	DoD Root CA 2	2/4/2	<none></none>		
DOD CA-32	DoD Root CA 2	2/4/2	<none></none>		
DOD EMAIL	. DoD Root CA 2	1/14/	<none></none>		
DOD EMAIL	. DoD Root CA 2	1/14/	<none></none>		~
Import	Export	Remove	1	4	Advanced
Certificate intende	d purposes				
Smart Card Logon,	, Client Authentica	tion			
					/iew
					ien.

 Scroll through the list of certificates, looking under the Issued To column, and ensure that there are *nocertificates that reference* "DoD Interoperability". If you find any certificates with this text, select the certificate and choose the Remove button. Select Yes on the confirmation window to finalize this action.

**Note**: If your Remove button is disabled, please contact your local IT department; a systemadministrator will need to complete this action.



😭 Certificates				×
Intended purpose	e: <all></all>			~
Personal Other	People Intermediate	Certification Authori	ties Trusted Root Certificati	on Auth 🔹 🕨
	<ul> <li>B DoD Root CA 2</li> <li>D DoD Root CA 2</li> </ul>	9/8/2 <none> 9/8/2 <none> 9/8/2 <none> 1/16/ <none> 1/16/ <none> 2/4/2 <none></none></none></none></none></none></none>	N	^
	L DoD Root CA 2 L DoD Root CA 2			~
Import Certificate inter		Remove		Advanced
Smart Card Log	on, client Addientica			View
			C	Close

• Scroll through the same list of certificates, this time looking under the **Issued By** column, and ensure that there are NO certificates that reference "**DoD Interoperability**." If you find any certificates with this text, please select the certificate and choose the **Remove** button. Select **Yes** on the confirmation window to finalize this action.

**Note**: If your Remove button is disabled, please contact your local IT department; a systemadministrator will need to complete this action.

ntended purpose:	<all></all>			
Personal Other Pe	ople Intermediate	Certificati	on Authorities	Trusted Root Certification Auth
Issued To	Issued By	Expir	Friendly N	1
DOD CA-27	DoD Root CA 2	9/8/2	<none></none>	
DOD CA-28	DoD Root CA 2	9/8/2	<none></none>	
DOD CA-29	DoD Root CA 2	9/8/2	<none></none>	
DOD CA-30	DoD Root CA 2	9/8/2	<none></none>	
DOD CA-31	DoD Root CA 2	1/16/	<none></none>	
DOD CA-31	DoD Root CA 2	1/16/	<none></none>	
DOD CA-32	DoD Root CA 2	2/4/2	<none></none>	
DOD CA-32	DoD Root CA 2	2/4/2	<none></none>	
GDOD EMAIL	. DoD Root CA 2	1/14/	<none></none>	
DOD EMAIL	. DoD Root CA 2	1/14/	<none></none>	×
Import	Export	Remove		Advance
Certificate intende	d purposes			
Smart Card Logon	Client Authentica	tion		
Sindi Colla Logon,				View
				-



• Click the **Close** button to exit the Certificates window.

tended purpose:	<all></all>				
ersonal Other F	People Intermediate	e Certificati	on Authorities	Trusted Root Certification Auth	10
Issued To	Issued By	Expir	Friendly N		,
DOD CA-27	DoD Root CA 2	9/8/2	<none></none>		
DOD CA-28	DoD Root CA 2	9/8/2	<none></none>		f
DOD CA-29	DoD Root CA 2	9/8/2	<none></none>		
DOD CA-30	DoD Root CA 2	9/8/2	<none></none>		
DOD CA-31	DoD Root CA 2	1/16/	<none></none>		
DOD CA-31	DoD Root CA 2	1/16/	<none></none>		
DOD CA-32	DoD Root CA 2	2/4/2	<none></none>		
DOD CA-32	DoD Root CA 2	2/4/2	<none></none>		
DOD EMAIL	DoD Root CA 2	1/14/	<none></none>		
DOD EMAIL	DoD Root CA 2	1/14/	<none></none>		•
Import	Export	Remove		Advan	ce
Certificate intend	ded purposes				
Smart Card Logo	n, Client Authentica	ation			
				View	
				Close	5

• Return to the "Content" tab then click **Clear SSL State.** Select **OK** on the confirmation window. Formore information, see the <u>Clear the SSL State</u> section of this guide.

#### 2.5.2 Firefox

• Open Firefox - click the Menu button then select Options.





• Select **Privacy and Security** then click **View Certificates**.

🔆 General	Security	
Home Home	Deceptive Content and Dangerous Software Protection	
<b>Q</b> Search	✓ Block dangerous and deceptive content Learn more	
Privacy & Security	✓ Block dangerous downloads	
Privacy & Security	Warn you about unwanted and uncommon software	
C Sync		
	Certificates	
	When a server requests your personal certificate	
	Select one automatically	
	Ask you every time	-
	Query OCSP responder servers to confirm the current validity of	View Certificates
Extensions & Themes	certificates	Security <u>D</u> evices
⑦ Firefox Support		

- From the "Certificate Manager" window, click the Authorities tab.
- Scroll through the list of certificates and ensure that there are *no certificates that reference* "*DoDInteroperability*". If you find any certificates with this text, select the certificate then choose the **Delete or Distrust** button.

Vaux Cartificates	Decele	Coming	A ush a visi a	a	
Your Certificates	People	Servers	Authoritie	25	
You have certificates c	n file that id	entify these c	ertificate auth	norities	
Certificate Name		Se	curity Device		1
► AC Camerfirma S A					1
		08 Built	tin Object Tol	(en	
		Built	tin Object Tok	en	1
► AC					
		Built	tin Object Tok	(en	
		ot Built	tin Object Tol	ken	
₩ AC				_	
		Built	tin Object Tol	(en	,
View Edit	Trust	Import	Export	Delete or Distrust	





Click **OK** on the confirmation window.

Delete or Distrust CA Certificates	$\times$
You have requested to delete these CA certificates. For built-in certificates all trust will be removed, which has the same effect. Are you sure you want to delete or distrust?	
Chamb	
If you delete or distrust a certificate authority (CA) certificate, this application who longer trust any certificates issued by that CA.	,

- From the Options page, under Privacy & Security, click the **Clear Data** button. For more information, see the <u>Clear Cookies and Site Data</u> section of this guide.
- 2.5.3 Chrome



Select the 3 vertical dots in the upper right and select

- Settings. Select Privacy • and Security and go to **Privacy and Security** section.
- Scroll down and click on Manage certificates.
- On the **Personal** tab, your expired electronic certificate should appear.
- Select the one you want to delete and click Remove.

settings		C. Search settings	
You an	d Google	Privacy and security	
Autofil     Safety		Clear browsing data Clear history, cookies, cache, and more	,
-	y and security	Cookies and other site data Third-party cookies are blocked in Incognito mode	,
Appear Q Search	engine	Security Safe Browsing (protection from dangerous aites) and other security settings	×
Default	t browser rtup	Site Settings Controls what information sites can use and show (location, camera, pop-ups, and more)	+
Advanced	•	Privacy Sandbox Trial features are on	
Extensions About Chrome		Appearance	
About Gillome		Theme Open Chrome Web Store	Ø
		Show home button Disabled	
		Show bookmarks bar	-

ntended p	urpose:	<all></all>					×
Personal	Other Peo	ple Interm	ediate Certifi	cation Author	rities Trusted	Root Certi	fication
Issued	То	Issued	Ву	Expirati	Friendly Nam	e	
C	ertificate	es will be	displayed	here			
Import.		xport	Remove				ådvanced
Certificat	E e intended p thentication	purposes	Remove				<u>A</u> dvanced

For assistance contact the DCSA DISS Customer Engagements Team, 8 a.m. – 8 p.m. EST, Monday – Friday Toll Free Telephone: 724-794-7765 Email: dcsa.ncr.nbis.mbx.contact-center@mail.mil