Removing the Federal Bridge cross certification certificates.

These instructions are intended to help you remove the Federal Bridge certificates from the Microsoft Certificate store on your computer. The objective of the Federal Bridge is to 'cross certify' the different certificate policies of all the federal agencies. The Federal Bridge has succeeded in getting Microsoft to include the Federal Bridge certificates in the Microsoft Certificate Store through initial operating system installation (it comes from the factory that way) and/or software updates.

Unfortunately, cross certification does not always work well in implementation. If you are trying to connect to a server (for instance, JPAS) and the server is not configured to account for the efforts of the Federal Bridge (perhaps because it is an old server), then it could cause an SSL Transaction (certificate log-on) to fail.

Before you remove the FBCA Certificates, please trust the DoD and ECA PKIs (<u>http://eca.orc.com/wp-content/uploads/ECA_Docs/Trusting_DoD_PKIs.pdf</u>). This will ensure that the Trust path created by the DoD is installed into the Microsoft certificate store. Microsoft might try to 'hold onto' the FBCA certificates if they form the only possible Trust Path that Microsoft has available. By installing the DoD's trust path, we ensure that Microsoft has an alternative to the FBCA certificates that we are trying to delete.

The DoD has created a tool to automatically remove these certificates. You can find instructions on using that tool, here:

http://eca.orc.com/wp-content/uploads/ECA_Docs/Removing_Federal_Bridge_certificates_Tool.pdf

In order to remove these certificates from the Microsoft Certificate Store in Windows 7, you will need to use the Microsoft Management Console.

Click on the Start button and then click Run.



Enter "mmc" in the text field and click OK

📼 Run	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	mmc
	OK Cancel <u>B</u> rowse

Alternatively, you can enter "mmc" in the search test field, and then double click the mmc.exe entry

Programs (1)		
₽ Seemore results		
mmc	×	Shut down 🕨

Console1 - [Console Root]		1 Mar.	
File Action View Favorites	Window	Help	_ 8 ×
New	Ctrl+N		
Open	Ctrl+0		Actions
Jave	Ctrl+S	There are no items to show in this view.	Console Root
St.V. As			More Actions
Add/Remove Snap-in	Ctrl+M		
Options			
1 eventvwr.msc			
2 devmgmt.msc			
3 certmgr.msc			
Exit			
Enables you to add snap-ins to or rem	ove them fro	m the snap-in console.	

When the Management Console opens, select File, then Add/Remove Snap-in...

Select Certificates and click the Add button

Add or Kemove Snap-ins You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.						
Available <u>s</u> nap-ins:		_	S <u>e</u> lected snap-ins:			
Snap-in	Vendor	*	Console Root	Edit Extensions		
ActiveX Control	Microsoft Cor Microsoft Cor			<u>R</u> emove		
Componente Services	Microsoft Cor	E		Move Up		
Computer Managem	Microson, Cor			Move Down		
Disk Management	Microsoft Cor Microsoft and		<u>Add</u> >			
🛃 Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
Group Policy Object	Microsoft Cor					
lP Security Monitor	Microsoft Cor					
😓 IP Security Policy M	Microsoft Cor					
Link to Web Address	Microsoft Cor	÷		Ad <u>v</u> anced		
Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.						
				OK Cancel		

Select Computer account and click Next

Certificates snap-in	x
This snap-in will always manage certificates for:	
Service account	
Computer account	
< Back Next > Can	cel

Select Local computer account and click Finish

Select Computer
Select the computer you want this snap-in to manage.
This snap-in will always manage:
Local computer: (the computer this console is running on)
<u>Another computer:</u> Browse
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
< <u>B</u> ack Finish Cancel

Select Certificates and click the Add button, again

Snap-in ActiveX Control Certificates Certificates Component Services Computer Managem Device Manager Disk Management Event Viewer Folder Group Policy Object	Vendor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	Add >	Console Root	er) Edit E <u>x</u> tensions Remove Move Up Move Down
IP Security Monitor IP Security Policy M Link to Web Address escription: The Certificates snap-in allo	Microsoft Cor Microsoft Cor Microsoft Cor	+ the contents of the	certificate stores for yourself, a se	Ad <u>v</u> anced rvice, or a computer. OK Cancel

This time, select My user account and click Finish



Click the OK button

Add or Remove Snap-ins You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled. Available gnap-ins: Selected snap-ins:							
Snap-in ActiveX Control ActiveX Control Authorization Manager Certificates Component Services Computer Managem Device Manager Disk Management Event Viewer Folder Group Policy Object Folder IP Security Monitor IP Security Policy M Link to Web Address	Vendor Microsoft Cor Microsoft Cor	E	<u>Add</u> >	Console Root	Edit Extensions Remove Move Up Move Down		
Link to Web Address Microsoft Cor Adwanced Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer. OK Cancel							

Click on the arrow by <u>Certificates (Local Computer)</u>, then click the arrow by <u>Trusted Root Certification</u> <u>Authorities</u>, then select the <u>Certificates</u> folder under <u>Trusted Root Certification</u> <u>Authorities</u>. Then, scroll through the listings and select all certificates the have the phrases," Common Policy", "Federal Bridge", "Federal Common Policy", "SHA-1 Federal Root CA" in either the <u>Issued To</u> or <u>Issued By</u> columns. Then, click the red X delete button. You may need to do this several times, to get them all. [Note: Not every certificate that needs to be removed is shown in the screen capture below. Be thorough and remove the certificates described above.]



The computer will produce the following warning message. Click the Yes button.



Then, click the arrow by <u>Intermediate Certification Authorities</u>, then select the <u>Certificates</u> folder under <u>Intermediate Certification Authorities</u>. Then, scroll through the listings and select all certificates the have the phrases," Common Policy", "Federal Bridge", "Federal Common Policy", "SHA-1 Federal Root CA" in either the <u>Issued To</u> or <u>Issued By</u> columns. Then, click the red X delete button. You may need to do this several times, to get them all. [Note: Not every certificate that needs to be removed is shown in the screen capture below. Be thorough and remove the certificates described above.]



The computer will produce the following warning message. Click the Yes button



Click on the arrow by <u>Certificates - Current User</u>, then click the arrow by <u>Trusted Root Certification</u> <u>Authorities</u>, then select the <u>Certificates</u> folder under <u>Trusted Root Certification</u> <u>Authorities</u>. Then, scroll through the listings and select all certificates the have the phrases," Common Policy", "Federal Bridge", "Federal Common Policy", "SHA-1 Federal Root CA"in either the <u>Issued To</u> or <u>Issued By</u> columns. Then, click the red X delete button. You may need to do this several times, to get them all. [Note: Not every certificate that needs to be removed is shown in the screen capture below. Be thorough and remove the certificates described above.]

🚡 Console1 - [Console Root\Certifica	tes (Local Computer)\Trusted Root Cer	tification Authorities\Certificates]							
🚡 File Action View Favorites Window Help									
Trusted Publishers	Issued To	Issued By	Expiration Date	*	Actions				
Dirtusted Certificates Dirtusted Certificates	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	1/7/2004		Certificates 🔺				
Trusted People	Common Policy	Common Policy	10/15/2027		More 🕨				
D Other People	Common Policy	Common Policy Copyright (c) 1997 Microsoft Corp.	12/30/1999		Colored Ik				
Certificate Enrollmen R Smart Card Trusted Ruc	Dev ORC Government Root	Dev ORC Government Root	3/31/2037		These				
Certificates (Local Comput)	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root	11/9/2031		Cortificatos				
👂 🚞 Personal	🔄 DoD Root CA 2	DoD Root CA 2	12/5/2029		Certificates				
Trusted Root Certificat	🔄 DST Root CA X3	DST Root CA X3	9/30/2021		are				
Certificates	ECA Root CA	ECA Root CA	6/14/2040		necessary				
Enterprise Trust	ECA Root CA 2	SHA-1 Federal Root CA	1/1/2014						
Intermediate Certification	ECA Root CA 2	ECA Root CA 2	3/30/2028		leave them				
Trusted Publishers	Entrust.net Certification Author	Entrust.net Certification Authority	7/24/2029						
D Intrusted Certificates	🔄 🔄 Entrust.net Secure Server Certifi	Entrust.net Secure Server Certifica	5/25/2019						
D Third-Party Root Certifi	Equifax Secure Certificate Auth	Equifax Secure Certificate Authority	8/22/2018						
Trusted People	🖏 Federal Bridge CA	Federal Bridge CA	10/11/2016						
Other People	🐺 Federal Common Policy CA	Federal Common Policy CA	12/1/2030						
Remote Desktop	🔄 GeoTrust Global CA	GeoTrust Global CA	5/21/2022						
Certificate Enrollment F	🔄 GlobalSign Root CA	GlobalSign Root CA	1/28/2028						
Smart Card Trusted Roc	Go Daddy Class 2 Certification	Go Daddy Class 2 Certification Au	6/29/2034						
Trusted Devices	GTE CvberTrust Global Root	GTE CvberTrust Global Root	8/13/2018	-					
Trusted Root Certification Authorities s	tore contains 42 certificates.								
				_					

The computer will produce the following warning message. Click the Yes button



Then, click the arrow by <u>Intermediate Certification Authorities</u>, then select the <u>Certificates</u> folder under <u>Intermediate Certification Authorities</u>. Then, scroll through the listings and select all certificates the have the phrases," Common Policy", "Federal Bridge", "Federal Common Policy", "SHA-1 Federal Root CA"in either the <u>Issued To</u> or <u>Issued By</u> columns. Then, click the red X delete button. You may need to do this several times, to get them all. [Note: Not every certificate that needs to be removed is shown in the screen capture below. Be thorough and remove the certificates described above.]

🚡 Console1 - [Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates]								
🚟 Eile Action View Favorites Window Help								
Trusted Publishers	Issued To	Issued By	Expiration Date	*	Actions			
Untrusted Certificates	🔄 DOD EMAIL CA-30	DoD Root CA 2	9/8/2017		Certificates 🔺			
Ihird-Party Root Certin	🔄 DoD Intermediate CA-1	DoD Root CA 2	2/4/2018		More 🕨			
Trusted People Other Records	🔄 DoD Intermediate CA-2	DoD Root CA 2	5/7/2018					
Certificate Enrollment	🔄 IdenTrust ECA 2	ECA Root CA 2	5/6/2014	N	Selected It 🔺			
Smart Card Trusted Rog	🔄 IdenTrust ECA 3	ECA Root CA 2	3/28/2017					
A 🔄 Certificates (Local Comput	Microsoft Windows Hardware	Microsoft Root Authority	12/31/2002		These			
Personal	GRC ACES Dev Government CA	Dev ORC Government Root	4/4/2011		Certificates			
a 📔 Trusted Root Certificati	🔄 ORC ECA HW 3	ECA Root CA 2	6/10/2014					
📔 Certificates	🔄 ORC ECA HW 4	ECA Root CA 2	5/30/2017		are			
📐 🚞 Enterprise Trust	🔄 ORC ECA SW 3	ECA Root CA 2	6/10/2014		necessary,			
Intermediate Certificati	GORC ECA SW 4	ECA Root CA 2	5/30/2017		loovo thom			
Certificate Revocati	🔄 ORC SSP USA	ORC ACES Dev Government CA	5/31/2010		leave them			
Certificates	Root Agency	Root Agency	12/31/2039					
Trusted Publishers	🛱 SHA-1 Federal Root CA	Federal Common Policy CA	1/1/2014					
Untrusted Certificates	🛱 SHA-1 Federal Root CA	VeriSign Class 2 SSP Intermediate	12/31/2013					
Dirid-Party Root Certifi	🛛 🔄 VeriSign Class 2 SSP Intermedia	VeriSign Class 2 Public Primary Ce	2/4/2019	I 🗐				
Irusted People	🔄 VeriSign Client External Certific	ECA Root CA 2	7/1/2014	7				
Other People	🔄 VeriSign Client External Certific	ECA Root CA 2	7/4/2017					
 Remote Desktop Certificate Enrollment F - 	www.verisign.com/CPS Incorp	Class 3 Public Primary Certificatio	10/24/2016	-				
			Þ					
Intermediate Certification Authorities s	tore contains 59 certificates.							

The computer will produce the following warning message. Click the Yes button



Then close the Management Console

Console1 - [Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates]										
File Action View Favorites	<u>W</u> indow <u>H</u> elp				_ 8 ×					
Trusted Publishers Image: A contrast of the second secon	Issued To	Issued By	Expiration Date	^	Actions					
 Third-Party Root Certifi Trusted People 	DOD EMAIL CA-28	DoD Root CA 2 DoD Root CA 2	9/8/2017 9/8/2017		More					
 Other People Certificate Enrollment F 	DOD EMAIL CA-30	DoD Root CA 2 DoD Root CA 2	9/8/2017 2/4/2018							
 Smart Card Trusted Roc Certificates (Local Comput 	DoD Intermediate CA-2	DoD Root CA 2 ECA Root CA 2	5/7/2018 5/6/2014							
 Personal Trusted Root Certificati 	Galden Trust ECA 3	ECA Root CA 2 Microsoft Root Authority	3/28/2017 12/31/2002							
Certificates Enterprise Trust		ECA Root CA 2	6/10/2011 5/20/2017							
Certificate Revocati		ECA Root CA 2 ECA Root CA 2 ECA Root CA 2	6/10/2014 5/20/2017							
Trusted Publishers Untrusted Certificates		ORC ACES Dev Government CA	5/31/2010							
 Third-Party Root Certifi Trusted People 	VeriSign Class 2 SSP Intermedia	VeriSign Class 2 Public Primary Ce ECA Root CA 2	2/4/2019	Ш						
 Other People Remote Desktop 	VeriSign Client External Certific	ECA Root CA 2 Class 3 Public Primary Certificatio	7/4/2017 10/24/2016							
Certificate Enrollment F +	•		F	*						
Intermediate Certification Authorities s	tore contains 59 certificates.									

When your computer asks you if you want to save the Console settings click No.



You should now be ready to put back (only) the certificates required to trust the DoD and ECA PKIs by running the **Trust DoD PKIs** instruction. Then try to access your web site (JPAS) again.