

Configuring Teamcenter for SSL

v1.1

Unrestricted

Table of Contents

Expectations of this guide:	
Details to know about the Certificate being used	
Teamcenter Preference Updates	7
Create a self signed certificate via Java keytool utility	
Export a certificate from the keystore using the Java keytool utility	
Enabling SSL within the Web Application	
JBoss EAP 6.3 (7.1 as well)	
Thin Client validation	
Import Certificate into IE Browser Trust Store	
Create a PEM formatted certificate file from Web Tier SSL config	
4-TIER updates to support Web Tier SSL	
2-TIER updates to support Web Tier SSL	
Teamcenter Active Workspace Client updates for Web Tier SSL	24
Teamcenter Active Workspace FTS Indexer updates for Web Tier SSL	25
Teamcenter Client Communication (TCCS) updates for Web Tier SSL	
Teamcenter Over the Web updates for Web Tier SSL	
Teamcenter Client for Office updates for Web Tier SSL	
Teamcenter MUX (J2EE web tier) Updates	
Teamcenter Visualization Updates	
2-tier	
NX Integration Updates	
2-tier	
4-tier	
Configuring FMS for one way SSL	
Teamcenter Preference:	
FMS Master:	
FSC configuration:	
FCC Configuraton:	
FSCADMIN utility update:	
Teamcenter Active Workspace Client updates for FMS FSC SSL	
Keytool Explorer	
Download	
Generate new keystore with self signed certificate	
Import Key Pair into Java Keystore (cacerts file)	

Expectations of this guide:

- TC 11.2.3 version
- Monolithic installation. All components on the same single machine.
- Not a deep dive into SSL
- General overview and technical transfer based on docs and case work
- Cover one way SSL using a self-signed certificate.

Difference: One way has client trust the server it is connecting to. 2-way has the client trust the server and the server trust the client.

Details to know about the Certificate being used

<u>Is the certificate self-signed?</u> A self-signed certificate is an identity certificate that is signed by the same entity whose identity it certifies. Not one signed by a well-known certificate authority (CA) like Entrust, VeriSign, and Thawte to name a few.

<u>NOTE</u>: Teamcenter documentation does not recommend using self-signed certificates in production environment. However, for testing, a self-signed certificate is used for this document.

Or is it signed by a Trusted CA? What does that mean?

The Browser and JAVA come pre-loaded with a list of trusted CA's. If the certificate is signed by one of those the browser displays the page without prompting the user to trust the server cert.

For example in IE:

Connecting the SSL based URL for Google (https://google.com) the user is presented the web page without any certificate related prompts. The certificate PATH for that ULR is:

	ttps://www. googl e	.com/	5 - Q	G Google
	Cer	tificate		x
General Detail	Certification Path path st Global CA gle Internet Authori www.google.com	ty G2		
			View Certifica	ate
Certificate sta	tus:			
This certificate	is OK.			

Within IE that highlighted CA is Trusted:

Internet Options	? X	- Hotmail, Outlo
General Security Privacy Content Connections Programs	Advanced	
Certificates Use certificates for encrypted connections and identifi Clear SSL state Certificates Publishe	cation.	java Verify Java
Certificates		x
Intended purpose: <a>		~
Intermediate Certification Authorities Trusted Root Certification	n Authorities	Trusted Publ < >
Issued To Issued By	Expiratio	Friendly Nar A
DST Root CA X3 DST Root CA X3	9/30/2021	DST Root C/
Equifax Secure Certificate Equifax Secure Certific	8/22/2018	GeoTrust
GeoTrust Global CA GeoTrust Global CA	5/20/2022	GeoTrust Gl
GlobalSign GlobalSign	3/18/2029	GlobalSign ≡
Go Daddy Class 2 Certificat Go Daddy Class 2 Certi	6/29/2034	Go Daddy C
GTE CyberTrust Global Root GTE CyberTrust Global	8/13/2018	DigiCert Glol
Microsoft Authenticode(tm) Microsoft Authenticode	12/31/1999	Microsoft Au
Microsoft Root Authority Microsoft Root Authority	12/31/2020	Microsoft Rc 🗸
	- /- /	>
Import Export Remove Certificate intended purposes		Advanced
Server Authentication, Client Authentication, Secure Email, Code Stamping	Signing, Time	View
		Close

For example in JAVA the same CA listed as a Signer CA:

🛃 Java C	a Control Panel		
General Java Security Advanced			
Enable Java content in the browser			
Security Level	Cer	tificates ×	
Very High (Most secure setting)	Certificate type: Signer CA	~	
allowed to run.	User System		
● High (Minimum recommended)	Issued To	Issued By	
Java applications identified by a certifi	VeriSign Class 3 Public Primary Certification Aut	VeriSign Class 3 Public Primary Certification Aut 🔨	
	VeriSign Universal Root Certification Authority	VeriSign Universal Root Certification Authority	
 Medium (Least secure setting) 	GeoTrust Global CA	GeoTrust Global CA	
All Java applications will be allowed to	VeriSign, Inc. Class 3 Public Primary Certificatio	VeriSign, Inc. Class 3 Public Primary Certificatio	
	Certum Trusted Network CA	Certum Trusted Network CA	
	SECOM Trust.net Security Communication Root	. SECOM Trust.net Security Communication Root	
	AffirmTrust Premium	AffirmTrust Premium V	
Exception Site List			
Applications launched from the sites lister prompts.	Import Export	Remove Details	
Click Edit Site List to add items to this list.		Close	
Re	store Security Prompts Manage Certificates		
	OK Cancel Apply		

What is the difference between a keystore and truststore?

The keystore is needed when you are setting up server side on SSL, it is used to store server's identity certificate, which the server will present to a client and the client will need to have that servers keystore certificate detail in its truststore in order for the connection to work. If your browser connects to a website over SS, it verifies the certificate presented by server against its truststore.

Teamcenter Preference Updates

Update the 'Web_protocol preference to be 'https':

Search On Keywords)	Interface. Thin Client. Gene
*protocol		Description
Filter by category	r by category Sets the	
Filter by protection scope	-	
Name	Location	Value
	011-	Labora 11
<pre>FC_RA_server_parameters</pre>	Site	ntups://

Create a self signed certificate via Java keytool utility

The following command will generate a self signed certificate within the 'keystore' file specified by the '-keystore' option (C:\keystore).

%JAVA_HOME%\bin\keytool -keystore c:\keystore -alias gtac -genkey -keyalg RSA

The command will prompt for a number of values. In this example the alias for the cert is 'gtac'. The first prompt will be for 'First and Last name'. That value is the CN (common name) and should be the HOSTNAME of the Web app server. <u>NOTE</u>: The 'Common Name (CN)' of the web application hostname <u>MUST</u> match how that hostname will be provided in the URL. For example: If the URL that the end users will use is fully qualified (myserver.us.com) then the CN needs to be 'myserver.us.com'. If the CN name in the certificate does not match the hostname the connection will fail.

The remaining entries for the certificate used for this guide were entered as follows:

```
What is the name of your organizational unit?

[Unknown]: GTAC

What is the name of your organization?

[Unknown]: GTAC

What is the name of your City or Locality?

[Unknown]: Milford

What is the name of your State or Province?

[Unknown]: OH

What is the two-letter country code for this unit?

[Unknown]: US

Is CN=civjmsrv2012r21, OU=GTAC, 0=GTAC, L=Milford, ST=OH, C=US correct?

[no]: y

Enter key password for <gtac>

(RETURN if same as keystore password):

Re-enter new password:
```

The password entered above is 'changeit'.

Export a certificate from the keystore using the Java keytool utility

This is a proactive step as the .crt generated will be required later for import into Teamcenter RAC client Java keystore. The keystore used in the command below is the 'C:\keystore' that was created in the last section.

%JAVA_HOME%\bin\keytool -exportcert -alias gtac -file c:\webappcert.crt -keystore c:\keystore -storepass changeit

The output from the utility run: Certificate stored in file <c:\webappcert.crt>

Enabling SSL within the Web Application

JBoss EAP 6.3 (7.1 as well)

Update the Jboss standalone.xml file to include the location and connection information for the C:\keystore file that was generated in the 'Create a self signed certificate via Java keytool utility' section earlier in this guide. Added the highlighted section below:

```
<subsystem xmlns="urn:jboss:domain:web:1.1" native="false" default-virtual-server="default-host">
    </connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="https" secure="true">
    </connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
    </ssl key-alias="gtac" password="changeit" certificate-key-file="C:/keystore" protocol="ALL" verify-client="false"/>
    </connector>
    </understand secure="default-host" enable-welcome-root="true">

    <alias name="localhost"/>

    <alias name="localhost"/>

    <alias name="localhost"/>
```

</subsystem>

The default HTTPS port is listed at the bottom of the standalone.xml file. The default is '8443'. For example:

Start up Jboss and verify the SSL port.

https://<web_app_servername>:8443

For example: For this guide the Web Application server name is 'gtac1' so the URL would be: <u>https://gtac1:8443</u>

That should result in this page. Select the 'Continue' option:



That should bring up the Jboss splash screen:

RED HAT JBOSS ENTE	RPRISE APPLICATION PLATFORM 6
	Welcome to JBoss EAP 6
	Your Red Hat JBoss Enterprise Application Platform is running.
	Administration Console Documentation Online User Groups
	To replace this page set "enable-welcome-root" to false in your server configuration and deploy your own war with / as its context path.

To review the certificate select the 'Certificate Error' / 'view certificate' to the right of the URL address bar.



Unrestricted Page 10 of 46

Thin Client validation

Launch the thin client URL. Until the certificate is imported into the Browsers truststore, the user will see the following page when launching the thin client:



Select the 'Continue to the website' option. Then the user will be presented the login page.

One may see the following messages as well. These appear to be Java 'untrusted' related.



These are corrected by adding the server URL to exception list within the Java control panel.

4	Java Contro	l Panel	– – ×
General	Java Security Advanced		
Enab	le Java content in the browser		
Securit	y Level		
⊖ Ve	ry High (Most secure setting)		
O al	nly Java applications identified by a non-expired owed to run.	certificate from a trusted aut	hority will be
● Hi	gh (Minimum recommended)		
Ja	va applications identified by a certificate from a	trusted authority will be allow	ed to run.
OM	dium (Least secure setting)		
A	Java applications will be allowed to run after pr	esenting a security prompt.	
Except	on Site List		
App	ications launched from the sites listed below will	be allowed to run after the ap	propriate security
http: http: http: http:	//gtac1:7001 //gtac1 :://gtac1	^ Edit	: Site List
	Restore Se	curity Prompts Manage	Certificates
		OK Cano	el Apply

This one still appeared:

			Security Warning	x
Do yo	u want t	o run this	application?	
		Name:	applauncher	
/	<u>-</u>	Publisher:	Siemens Product Lifecycle Management	
	_	Location:	https://gtac1:8443	
Runnin	g this app	lication ma	y be a security risk	
Risk: T ir ra	his application formation at un this applic	on will run with u t risk. The information unless yo	unrestricted access which may put your computer and personal mation provided is unreliable or unknown so it is recommended no u are familiar with its source	t to
U M	nable to ens lore Informa	ure the certific tion	ate used to identify this application has not been revoked.	
Select t	ne box bek	ow, then click	Run to start the application	
<u> </u>	accept the ri	sk and want to	run this application. Run Cancel	

Disable cert validation in Java control panel kept that warning from appearing. Depending on the certificate this option may not be required. In this test use it is a result of the certificate being self-signed.



And now prompts for this:

Do you want to run this application?			×		
	Nam	e:	DocMgtApplet		
	See Publi	isher:	Siemens Product Lifecycle Manag	gement	
	Loca	tion:	https://gtac1:8443		
This app informat	lication will run with (ion at risk. Run this a	unrestri applicati	cted access which may put your c ion only if you trust the location a	omputer and perso nd publisher above	nal
🗌 Do n	ot show this again fo	or apps f	from the publisher and location ab	ove	
1	More Information			Run	Cancel

Have to select the check box in order to select 'RUN'.

Import Certificate into IE Browser Trust Store

To import the certificate into the IE Browser certificate store select the 'padlock' or Certificate warning located to the right of the URL address. Then select 'View certificates' option.



Select 'Install Certificate' option:

<u>.</u>	Certificate	x
G	eneral Details Certification Path	
	Certificate Information	
	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.	
	Issued to: GTAC1	-
	Issued by: GTAC1	
	Valid from 1/30/2017 to 4/30/2017	
	Issuer Statement	
	ОК	

<u></u>	Certificate Import Wizard	×
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	Store Location Current User Current User	
	To continue, dick Next.	
	<u>N</u> ext Cancel	

Import the certificate into the Trusted Root Certificate Authorities

📀 🍠 Certificate Import Wizard
Certificate Store Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
\bigcirc Automatically select the certificate store based on the type of certificate
 Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities Browse
Next Cancel

	Security Warning	x	
<u>^</u>	You are about to install a certificate from a certification authority (CA) claiming to represent:		
	Windows cannot validate that the certificate is actually from "GTAC1". You should confirm its origin by contacting "GTAC1". The following number will assist you in this process:		
	Thumbprint (sha1): B8DB22F8 FD2C8C83 F87EC394 D5AF5AE2 51A99ED9 Warning:		
	If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.		
	Do you want to install this certificate?	_	
	Yes No		

Once complete the cert will be listed in the Certificates trust store:

Internet Options	X Teamcenter Web - M
General Security Privacy Content Connections Programs Advance Certificates	ed ncat Web Application
Certificates	×
Internediate Certification Authorities Trusted Root Certification Authorities	v
Issued To Issued By Equifax Secure Certificate Authority Equifax Secure Certificate Authority GeoTrust Global CA GeoTrust Global CA GlobalSign GlobalSign Go Daddy Class 2 Certification Aut Go Daddy Class 2 Cert GTAC1 GTAC1 Microsoft Authenticode(tm) Root A Microsoft Authenticod Microsoft Root Authority Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certific	Expiratio Frienc 8/22/2018 GeoTr 5/20/2022 GeoTr 3/18/2029 Globa 6/29/2034 Go Da 4/30/2017 <non< td=""> 12/31/1999 Micros 12/31/2020 Micros 5/9/2021 Micros > ></non<>
Import Export Remove Certificate intended purposes <all></all>	Advanced
9 7	Close

With that import completed, there will no longer be certificate warnings during thin client launch. Security padlock no longer RED



Create a PEM formatted certificate file from Web Tier SSL config

This is a proactive step as some integrations will require this specific format of the certificate.

- A List of integrations that will need this are:
 - o Native implementation of the FSCClientAgent
 - NX Integration
 - TCVis Integration
 - NOTE: The list of integration that use this will be added as confirmed
- 1. One option to create a PEM formatted certificate file is to leverage the certificate already in use by the Web tier. Launch the web tier URL:



Certificate	X
General Details Certification Path	📀 🍠 Certificate Export Wizard
Show: <al> Show: Field Value Version Serial number 2d c1 1d 82 Signature algorithm sha256 Issuer GTAC1, GTAC, GTAC, Milford, Valid from Monday, January 30, 2017 3: Valid to Sunday, April 30, 2017 3:07:5 Subject GTAC1, GTAC, GTAC, Milford, Edit Properties </al>	Export File Format Certificates can be exported in a variety of file formats. Select the format you want to use: DER encoded binary X.509 (.CER) Bage-64 encoded X.509 (.CER) Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) Indude all certificates in the certification path if possible Delete the private key if the export is successful Export gll extended properties Microsoft Serialized Certificate Store (.SST)
ОК	<u>N</u> ext Cancel

Make sure that the created PEM file has a .pem extension. From the above step the cert was saved as C:\cert.pem:

N De Videon	users 🖉	2/0/2014 3:45 PIVI FII	etoider
V 📑 Videos	Windows	1/30/2017 7:08 PM Fil	e folder
4 📥 Local Disk (C:)	.keystore	1/30/2017 3:08 PM KE	YSTORE File 3 KB
4 🎍 apps	cert.pem	1/31/2017 3:05 PM PE	M File 2 KB
CAD	🚳 msdia80.dll	12/1/2006 10:37 PM Ap	plication extens 884 KB
🛛 🖉 🔟 LocalData	735° I .	4/00/0016 6 10 DE4 - W/	1 D.L.E.1 D.V.D.

4-TIER updates to support Web Tier SSL

1. Update the web tier URI to be 'HTTPS' and reflect the correct SSL port:

URI			 Connectio
https://gtac1:8443/t	c TcWe	b1	

2. Import the certificate from the 'C:\keystore' into the Teamcenter 4-tier client based Java cacerts file. The export process was completed earlier in this guide in the 'Export a certificate from the keystore using the Java keytool utility' section. From that export a 'c:\webappcert.crt' file was created. That cert file is the one that will be imported into the java keystore in the command below. %JAVA_HOME% = installation location of the Java that the 4-tier client is using.

%JAVA_HOME%\bin\keytool -importcert -alias gtac -file c:\webappcert.crt -keystore %JAVA_HOME%\lib\security\cacerts - storepass changeit

<u>NOT A PROCESS TESTED IN THIS GUIDE</u> but it may be possible to import directly out of the C:\keystore file. For example: %JAVA_HOME%\bin\keytool -importcert -alias gtac -file c:\keystore -keystore %JAVA_HOME%\lib\security\cacerts -storepass changeit

The output from executing that command:

```
C:\jre780 64\bin>%JAVA HOME%\bin\keytool -importcert -alias gtac -file c:\webappcert.crt -keystore
%JAVA_HOME%\lib\security\cacerts -storepass changeit
Owner: CN=GTAC1, OU=GTAC, O=GTAC, L=Milford, ST=OH, C=US
Issuer: CN=GTAC1, OU=GTAC, O=GTAC, L=Milford, ST=OH, C=US
Serial number: 2dc11d82
Valid from: Mon Jan 30 15:07:55 EST 2017 until: Sun Apr 30 16:07:55 EDT 2017
Certificate fingerprints:
    MD5: 47:DE:B1:FD:62:77:D6:82:40:38:EF:B6:A7:41:5E:BC
    SHA1: B8:DB:22:F8:FD:2C:8C:83:F8:7E:C3:94:D5:AF:5A:E2:51:A9:9E:D9
    SHA256: C8:49:86:5E:91:E1:9B:B8:93:2B:2D:F9:84:97:8C:00:08:A9:21:BF:41:31:69:81:EF:B1:2F:64:5E:08:A9:21
    Signature algorithm name: SHA256withRSA
        Version: 3
        Extensions:
        #1: ObjectId: 2.5.29.14 Criticality=false
        SubjectKeyIdentifier [
        Keyldentifier [
        0000: 84 A6 BF AF 5A 55 FD F8 4E 71 53 11 3E 14 96 91 ....ZU..NqS.>...
        0010: C2 51 CE 9E
                                               .Q..
        ]
        1
        Trust this certificate? [no]: y
        Certificate was added to keystore
```

C:\jre780_64\bin>

3. To confirm if the certificate is in the keystore that it was imported in or to see if it has already been imported previously use the '-list' option of the keytool utility. For example:

%JAVA_HOME%\bin\keytool -list -keystore %JAVA_HOME%\lib\security\cacerts -storepass changeit

Output highlighting the 'gtac' cert that was imported from step 2: Certificate fingerprint (SHA1): C9:3C:34:EA:90:D9:13:0C:0F:03:00:4B:98:BD:8B:35:70:91:56:11 verisignclass2g2ca, Mar 25, 2004, trustedCertEntry, Certificate fingerprint (SHA1): B3:EA:C4:47:76:C9:C8:1C:EA:F2:9D:95:B6:CC:A0:08:1B:67:EC:9D gtac, Jan 31, 2017, trustedCertEntry, Certificate fingerprint (SHA1): B8:DB:22:F8:FD:2C:8C:83:F8:7E:C3:94:D5:AF:5A:E2:51:A9:9E:D9 geotrustprimarycag3, Dec 10, 2009, trustedCertEntry, Certificate fingerprint (SHA1): 03:9E:ED:B8:0B:E7:A0:3C:69:53:89:3B:20:D2:D9:32:3A:4C:2A:FD geotrustprimarycag2, Dec 10, 2009, trustedCertEntry, Certificate fingerprint (SHA1): 8D:17:84:D5:37:F3:03:7D:EC:70:FE:57:8B:51:9A:99:E6:10:D7:B0 swisssigngoldg2ca, Oct 31, 2008, trustedCertEntry,

<u>NOTE</u>: If the certificate is not imported into the Teamcenter 4-tier client Java cacerts file then the following error will appear during login:

	Login	x
8	com.teamcenter.soa.client.SoaRuntimeException: Failed to send the service reques encountered an HTTP I/O error. peer not authenticated	st,

<u>NOTE:</u> If you have other 4-tier clients at the same java version you can copy this cacerts file to all other client java installations to save you from manually running the import command on each.

2-TIER updates to support Web Tier SSL

No updates required as it does not connect to web tier during login process

Teamcenter Active Workspace Client updates for Web Tier SSL

Update the 'Teamcenter 4-tier URL' and FSC settings to reflect correct HTTPS protocol and port:

	TEAMCENTER
Active Workspace Clien Specify Active Workspace clien	nt Settings t installation settings below.
Teamcenter 4-tier URL	https://gtac1: <mark>8443</mark> /tc
JDK Home	C:Uavaljdk7x64
• Use as Bootstrap URLS	
Bootstrap URLs	http://gtac1:4544
Bootstrap Client IP	
Use Assigned FSC URLs	
Assigned FSC URLs	http://gtac1:4544
Enable TcSS Support	
Enable TcSS Support	
TcSS Application ID Te	eamcenter
TcSS Login URL	
and the second s	
Contraction of the owner own	Advanced
2	Back Next Cancel

Teamcenter Active Workspace FTS Indexer updates for Web Tier SSL

4-tier URL entry via TEM:

	TEAMCENTER
Active Workspace Indexer Se Specify Active Workspace Indexer insta Connections specifies the maximum in Teamcenter server and the indexer at of warmed up Teamcenter servers ava . Teamcenter Retry Count specifies the server.	ettings allation settings below. Maximum Teamcenter number of open connections between the a given time. It should be less than the number allable in the server manager. e number of tries to connect to the Teamcenter
Dispatcher-based indexing envi	ronment
Teamcenter 4-tier URL	https://gtac1:8443/tc
Teamcenter Connections	30
Dispatcher Server URL	mi//localhost:2001
Staging Directory	PLMITc11ltc_rootlTcFTSIndexerlworking
	T-A
0	Back Next Cancel

OR 4-tier URL entry in the 'TcFtsIndexer.properties' file:

C:\apps\PLM\Tc11\tc_root\TcFTSIndexer\conf				
dm ^ fsc iiopservers include include_cpp install jtutilities I10n_cots lang lib	Name InguageProfiles Dispatcher.properties Iog4j.properties TcFtsIndexer.properties TcFtsIndexer_objdata.properties TcFtsIndexer_structure.properties TcFtsIndexer_structure.properties TcFtsIndexer_structure.properties TcFtsIndexer_structure.properties TcFtsIndexer_structure.properties TcFtsTikaConfig.xml TimeRanges.properties			

Teamcenter Client Communication (TCCS) updates for Web Tier SSL

Update the middle tier URI to reflect HTTPS and proper port value:

Environment Settings for Client Communication System

Enter the middle-tier web application servers information. To enable applet-free SSO support, append '/tccs' to the end of SSO Login URL in the formation of http://host:port/SSO_LOGIN_SERVICE_NAME/tccs.

Name	URI	Tag	SSO App ID	SSO Login URL	Add
TcEnv1	https://gtac1:8443/tc				

The default SSL setting is to reference the IE trust store for certificate validation. One can select to manually configure an alternate trust store file or key store file. Either of those options could be used to point to a Java cacerts file for example.

TE/	AMCENTER
Secure Socket Layer (SSL) Settings	-
Specify the Client Communication System SSL settings below.	
 Use Internet Explorer Certificate Store (Recommended) 	
Disable SSL	
Configure Certificate Store Manually	States
Configure trust store	
Use trust store (supported type is JKS)	
File	
Accept untrusted certificates	\rightarrow
Configure key store	
Use Key Store	
File	
Type JKS	
1 and the second	
Back Nex	d Cancel

Teamcenter Over the Web updates for Web Tier SSL

SSL Setting Type can be updated to reflect where the 4-tier client will look to validate the certificate. If selecting the 'trust store' option then enter proper values for the 'TrustStoreFile' or 'KeyStoreFile' path and file as located from the clients perspective.

	I cCSAlwaysPromptForUserID	false
	Set FMS_HOME	Set when missing
	SSLSettingType	Use Internet Explorer Certificate Store (Recommended)
	TrustStoreFile	Use Internet Explorer Certificate Store (Recommended)
	KeyStoreFile	Disable SSL
	KeyStoreType	Use trust store (Supported type is JKS)
	TcSS Unix Browser	
V	WebBrowserUnixLocation	Accept unit usieu ceruncates
~	RichClientHelpWebServer	http://host:8080/tc

Update the middle tier URI to reflect HTTPS and proper port value:

Name	ОТW		Mod	ifv Wet	Application I	nformation	
Staging Location	C:\01	TW\otw_instance			the Direk Lange		
Description		Modify Tables		x	ontext Para	meters	
Solution Type: Installed Solutions	Dist	Tables HTTPServerTable TcCSEnvironmentTable TcCSReverseProxyConfigu	Modi	fy	odify Tables))	1 KI
2		Modify	Table			_ □	x
Table: HTTPServe	erTable						
Name		URI	TcSS Applic	ati To	SS Login S		
TcWeb1	https://qtao	:1: <mark>8443</mark> /tc					
						Add Row Remove Row	,

Teamcenter Client for Office updates for Web Tier SSL

Update the middle tier URI to reflect HTTPS and proper port value:

	Teamcenter Client for Office - InstallShield Wizard				
PI	Please enter Teamcenter server connection information:				
TI	The URI is in the form of http:// <host>:<port>/<tc></tc></port></host>				
	Connection Name:	MyData			
	Connection URI				
	Protocol:	HTTPS V			
	Teamcenter Host:	gtac1			
		(e.g myhost or myhost.mycompany.com)			
	Port Number:	8443			
	Application Name:	td			
Install	Shield	Cancel OK			

<u>NOTE</u>: The certificate validation is done through the browser trust store. So if the certificate is not in that trust store the following message during login will appear:

Teamcenter Error Information	x			
A serious error has occurred.				
Failed to exectue the service request Core-2008-06-Session/login at the server addres HTTPS://gtac1:8443/tc/. The underlying connection was closed: Could not establish trust relationship for the SS TLS secure channel. The remote certificate is invalid according to the validation procedure.				
< III >	·			
Details Teamcenter.Schemas.Soa2006_03.Exceptions.ConnectionException: Failed to exe The underlying connection was closed: Could not establish trust relationship for the S The remote certificate is invalid according to the validation procedure. at Teamcenter.Soa.Internal.Client.HttpTransport.ExecuteRequest(String service, St at Teamcenter.Soa.Internal.Client.XmlRestSender.Invoke(String service, String ope <				
Copy details to the Clipboard Retry Stop]			

Teamcenter MUX (J2EE web tier) Updates

- This is updated via TEM within the Java EE based Server Manager.
- Enable SSL in the ADVANCED panel and set the Keystore to reflect the same keystore file created earlier in this guide (c:\keystore). The format of that keystore file is JKS with a password of 'changeit'. KeyManager Password also set to 'changeit'.

	SSL Configuration	siemens X
	SSL Configuration	
Multiplexing Proxy (MUX)	KevStore c	:kevstore
The proxy that routes communications	KeyStore Type	KS
The MUX listens on a single port for inc	KeyStore Password	•••••
request to an appropriate Teamcenter ? Web Tier, The MIX also listens on the	KeyManager Password 🔹	•••••
messages from servers, and forwards t	TrustStore	
be managed within the Teamcenter En	TrustStore Type	
container.	TrustStore Password	
Port 8087		
TECS Admin Port 8084		
	2	OK Cancel
		Advanced ervice
	Back	ext Cancel Fervice

This is the type of pop up the user will see if MUX is not configured correctly with SSL.



<u>NOTE:</u> Stopping the Server Manager may not stop the MUX. To shut it down run the 'tecsstop.bat' inside the Server Manager folder.

Teamcenter Visualization Updates

2-tier

• Open in Standalone Vis or Embedded Vis within a 2-tier client does not require any additional configuration.

4-tier

• Opening in Standalone from within a 4-tier results in this message:

	Warning	x
Â	Failed to encrypt/decrypt the service request. SSL certificate problem, verify that the CA cert is OK. Deta error:14090086:SSL routines:func(144):reason(134)	ils:
	C	ж

Selecting OK on the above form but the same form keeps appearing. Have to kill Vis manually.

• Opening in Embedded Vis from within a 4-tier results in the same message:



SOLUTION:

TCVis has its own 'certs' folder within its installation.



Convert the certificate into a PEM format (performed in the 'Create a PEM formatted certificate file from Web Tier SSL config' section of this guide) and copy it into this folder. For example copy the C:\cert.pem file, created from the previous section of this guide, into the TCVis 'cert' folder:

Copy from:				
Videos	Users Users	2/0/2014 5:45 PIVI	File Tolder	
(Level Dick (C))		1/30/2017 7:08 PN	A File folder	
	.keystore	1/30/2017 3:08 PN	A KEYSTORE File	3
A in apps	Cert.pem	1/31/2017 3:05 PN	A PEM File	2
	🚳 msdia80.dll	12/1/2006 10:37 P	M Application extens	884
De localData	738T1	4/20/2016 C 10 D	A MALE BALLEY	2
Copy to:	^ Name	*		
🌗 etc	CAROOT Firmaprofesional.pem			
acknowledgements	CC_Signet_RootCA.pem			
🍶 certs	cert.pem			
🐌 DFx	CertEurope.pem			
ECADReports	Certigna.pem			
🔒 Images	Certinomis.pem			

NX Integration Updates

<u>2-tier</u>

• Open in NX does not require any additional configuration.

<u>4-tier</u>

• Open in NX failed with the following message:



Solution:

Set the following variable to point to the PEM formatted certificate file. PEM file creation outlined earlier in the 'Create a PEM formatted certificate file from Web Tier SSL config' of this guide. In that section the created pem file was: c:\cert.pem

set TEAMCENTER_SSL_CERT_FILE=c:\cert.pem

This can be set as a system variable on the client host or within the startnxmanager.bat file:

```
91 rem Start NX through the launcher program
92
93 set TEAMCENTER_SSL_CERT_FILE=c:\cert.pem
94 start "Teamcenter Integration for NX" /B "%UGII_ROOT_DIR%\ugs_router" -ugm -enable_cancel -
95 goto :ENDOFFILE
96
97 inv error
```

If setting that variable still shows the error, review the protocol setting in the https connector section of the Jboss standalone.xml. Setting it to 'ALL' was found to help resolve the issue.

```
<subsystem xmlns="urn:jboss:domain:web:1.1" native="false" default-virtual-server="default-host">
<connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="https" secure="true">
<connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
<ssl key-alias="gtac" password="changeit" certificate-key-file="C:/keystore" protocol="ALL" verify-
client="false"/>
</connector>
<virtual-server name="default-host" enable-welcome-root="true">
<a href="https"></a>
```

Setting that protocol to TLSv1 for example did not correct the issue. Others [SSLv2Hello, TLSv1, TLSv1.1, TLSv1.2]

Configuring FMS for one way SSL

Teamcenter Preference:

Add the URL of the local HTTPS host to the list of servers defined in the Fms_BootStrap_Urls preference.

Name	Location
Default_Transient_Server	Site
ETS.TRANSLATORS.SIEMENS	Site
FMS_SAF_Batch_Transfer_Enabled	Site
Fms_BootStrap_Urls	Site
Multisite_Ticket_Expiration_Interval	None
Ticket_Expiration_Interval	None

FMS Master:

Update the FMS master to reflect the correct SSL based URL address

FSC configuration:

Update the fsc.FSC_<host>_<userid>.properties file in the FSC_HOME directory with the keystore information. The information used below is based on the keystore created in the 'Create a self-signed certificate via Java keytool utility' section of this guide.

Copy the 'fsc.properties.template' file to 'fsc.FSC_<host>_<userid>.properties' and open it for edit.

NOTE: Important that the properties filename be in the format listed above. Example for this would be: fsc.FSC_gtac1_yytcadm.properties

Edit the keystore related fields. Notice the direction of the slashes (/). FSC will fail to start and complain about file not found if the slashes are not correct.

```
# These are required for ssl support:
#
com.teamcenter.fms.servercache.keystore.file=c:/keystore
com.teamcenter.fms.servercache.keystore.password=changeit
com.teamcenter.fms.servercache.keystore.ssl.certificate.password=changeit
#
```

Since this process is using a self signed certificate we need to also uncomment this line in the 'fsc.FSC_gtac1_yytcadm.properties' file as well:

```
32 #
33 # Optionally trust self signed server certificates:
34 com.teamcenter.fms.allowuntrustedcertificates=true
35 #
```

FCC Configuraton:

Non-Native:

Update FCC.xml to reflect parent FSC's SSL based URL address.

```
<!-- default parentfsc - this is a marker that will be overwritten
<parentfsc address="https://gtac1:4544/" priority="0" />
</fccconfig>
```

With that in place the 4-tier client login appears to have hung and sits at the login page with the status bar continually scrolling across the page. Review of the tcserver.fscproxlog shows this:

```
Tue Jan 31 14:31:06 2017-com.teamcenter.fmg.gervercache.proxy.FSCNativeClientProxy Thr3196
N:\units\fmg\fmg.11.2.3_wnti32\grc\FSCNativeClientProxy\FSCClientAgent.cpp:96
WARNING: FSCClientAgent.init(): https://gtac1:4544/mapClientIPToFSCs failed: 60 CURLE_SSL_CACERT: Problem with the CA cert(path?)
Tue Jan 31 14:31:36 2017-com teamcenter fmg servercache proxy FSCNativeClientProxy Thr3196
```

Two ways to correct this:

1. For 4-tier, set the following within the %TC_DATA%\tc_profilevars.bat file OR set as a system variable. In either case the Server Manager will need to be restarted after setting it:

SET TC_USE_FSC_CPROXY_VIA_JVM=true

For 2-tier, set the same variable in %TC_DATA%\tc_profilevars.bat or as a system variable as well.

2. Configure native FSC client proxy:

Create the %FSC_HOME%/fsc.clientagent.properties file. Add the 'com.teamcenter.fms.curl.cacerts.file' property to it and set its value to the absolute path and file name to the PEM formatted file. For example based on the PEM file created in an earlier step of this guide ('Create a PEM formatted certificate file from Web Tier SSL config') the line would appear as follows:

com.teamcenter.fms.curl.cacerts.file=C:\cert.pem

In addition to that line, given that this is a untrusted self-signed certificate, add the following line as well:

com.teamcenter.fms.allowuntrustedcertificates = true

File content after edit will look like this:



FSCADMIN utility update:

The fscadmin script most also be configured to allow untrusted certificates. Use the $\FSC_HOME\%\fscadmin.properties.template file to create a \%FSC_HOME\%\fscadmin.properties file. Within that file uncomment the line shown below:$

```
24 # Optionally trust self signed server certificates:
25 com.teamcenter.fms.allowuntrustedcertificates=true
26 #
```

If the self-signed certificate has been imported into the Java cacerts file of the JAVA that the FSCAdmin utility is using, then this file and edit is not required. Otherwise, if the cert is untrusted the following type of message will appear when trying to run the fscadmin utility:

```
C:\apps\PLM\Tc11\tc_root\fsc>fscadmin -s <u>https://gtac1:4544</u> ./cachesummary
OS name is Windows Server 2012 R2
JVM vendor is Oracle Corporation
Data model is 32
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed:
java.security.cert.CertPathValidatorException: signature check failed
at sun.security.ssl.Alerts.getSSLException(Unknown Source)
at sun.security.ssl.SSLSocketImpl.fatal(Unknown Source)
at sun.security.ssl.Handshaker.fatalSE(Unknown Source)
at sun.security.ssl.Handshaker.fatalSE(Unknown Source)
```

Teamcenter Active Workspace Client updates for FMS FSC SSL

		TEAMCENTER
Active Workspace Clier Specify Active Workspace clien	nt Settings It installation settings below.	1
Teamcenter 4-tier URL	http://gtac1:8080/tc	
JDK Home	C:Uavaljdk7x64	
Use as Bootstrap URLS		Participan .
Bootstrap URLs	https://gtac1:4544	
Bootstrap Client IP	200	
Use Assigned FSC URLs		
Assigned FSC URLs	http://gtac1:4544	
Enable TcSS Support		
Enable TcSS Support		
TcSS Application ID Te	eamcenter	
TcSS Login URL		
		Advanced
2		Back Next Cancel

Keytool Explorer

Download

http://keystore-explorer.org/downloads.html

Generate new keystore with self signed certificate





Select the 'Generate Key Pair' icon and accept defaults:



Select 'EDIT NAME' icon and populate the fields. Remember that the 'Common Name (CN)' needs to reflect the host name of the web application server. The CN <u>MUST</u> match how that hostname will be provided in the URL. For example: If the URL that end users will use is fully qualified (myserver.us.com) then the CN needs to be 'myserver.us.com'. If the CN name in the certificate does not match the hostname the connection will fail.

	Generate Key Pair Certificate			
	Version:) Version 1 () Version 3		
	Signature Algorithm:	HA-256 with RSA 🗸 🗸		
	Validity Period:	1 vear(s) v		
	Serial Number:	486065972		
	Name:			
		Name 😽 🗙	ή	
		Common Name (CN): GTAC1		
		Organization Unit (OU): GTAC		
		Organization Name (O): GTAC		
		Locality Name (L): Milford		
		State Name (ST): OH		
		Country (C): US		
		Email (E):		
K	eyStore Type: JKS, Size:	OK Cancel		

Provide an alias name:

New Key Pair Entry Alias	x
Enter Alias: gtac	
OK Cancel	

Provide a password.

New Key Pair Entry Password		
Enter New Password:		
Confirm New Password:		
OK Cancel		
Generate Key Pair		
Key Pair Generation Successful.		
OK		

Save the new keystore to a location of your choice:

File	File Edit View Tools Examine Help					
		× 🖿 🖺 🏗 % 死 🕾 🗊 😶 🕕 🖻 🔯 😡 🕢				
	A-	Save KeyStore As				
	Save in:	📇 Local Disk (C:) 🗸 🤌 📴 🗔 🗸				
	Recent Items	apps Users dwork Windows Java - Copy.keystore_original jboss63 cert.pem ire780.64 explorerkeystore				
	Desktop	KeyStore Explorer 5.1.1 keystore KeyStore Explorer 5.2.2 msdia80.dll MSOCache servers.bat				
	Documents	oracle OTW Program Files				
	This PC	 Program Files (x86) ProgramData Siemens Temp 				
	Network	File name: keystore Save				
	NEWOR	Files of type: All Files Cancel				

Import Key Pair into Java Keystore (cacerts file)

Open the keystore that was created in the last step.

Select the key and from the right mouse button menu, select 'Export Certificate Chain':

I		E	Entry Name	Algorithm			Key Size			Certific
Ħ	ſ	0	gtac	RSA	Q	View Details	0N0C	-		2/2/201
					×	Cut	Ctrl+X			
					ľ	Сору	Ctrl+C			
					1	Export	•	R	Export Key Pair	
						Generate CSR		R	Export Certificate Chain	
					*	Import CA Reply	•	9	Export Private Key	
					9	Edit Certificate Chair	n I	7	Export Public Key	
					2	Sign	•			
					лî.	Unlock				
						Set Password				
					X	Delete				
					Ť	Rename				

Take default options and enter a path and cert name:

Export Certificate Chain from entry 'gtac'								
Export Length:	Head Only	O Entire Chain						
Export Format:	• X.509	O PKCS #7	O PKI Path					
PEM:	✓							
Export File:	C:\gtac.cer				Browse			
				Export	Cancel			

NOTE: The 'PEM' option of this export will not only be a format that can be imported into the Java cacerts file (next step) but will be the PEM file needed for some of the Teamcenter integration configurations to use.

Open the cacerts file from within the Java instance that the Teamcenter RAC client is using:

<u>A</u> -		explore	rkeystore - KeyS	tore Explorer 5.	2.2
File Edit View T	ools Examine	Help			
	≠ × h B	17 % A 17 ···	0 0 0	0	
*		Open	KeyStore		x
Look in	: 鷆 security			v 🤌 📂 🗄	•
Recent Items Desktop Documents	blacklist cacerts java.polic java.secu javafx.pol javafx.pol javaws.po local_poli trusted.lik	Copy y ity icy licy cy.jar oraries cpolicy.jar			
This PC					
	File name:	cacerts			Open
Network	Files of type:	All Files		~	Cancel

The default password for Java cacerts file is 'changeit'.

Select 'Import Trusted Certificate' option and browse to the PEM cert file created in the last step:



Enter the alias for that cert:

Trusted Certificate Entry Al ×						
Enter Alias: gtac						
OK Cancel						

Confirm import:

霓	-	۲	globalsignr3ca	RSA	2048
党	-	۲	godaddyclass2ca	RSA	2048
党	-	۲	gtac	RSA	2048
党	-	۲	gtecybertrustglobalca	RSA	1024
10		-	1		

Be sure to SAVE the cacerts file after the import is completed:

			* * × L B 76 8 9 77	••• 📵 🔯 🔕 🔞			
explorerkeystore * acerts * *							
Ι		E	Entry Name	Algorithm	Key Size		
党	-		globalsignr 2ca	RSA	2048		
党	-	۲	globalsignr3ca	RSA	2048		
2	-	۲	godaddyclass2ca	RSA	2048		
- 🁮	-	۲	gtac	RSA	2048		
党	-	۲	gtecybertrustglobalca	RSA	1024		
	-		kevnectisrootca	RS0	2048		