Bond V6 - Https configuration

- Over view
- Enable Https for ECC in Tomcat
 - Open cmd as Administrator
 - Move to the Tomcat config directory by using: cd YOUR_TOMCAT_DIRECTORY/conf
 - Generating Keystore
 - Uncomment Connector to port 8443 in YOUR_TOMCAT_DIRECTORY/conf/server.xml
 - Access your application
- Enable Https for BOND in IIS (Internet Information Services)
 - Open Internet Information Services (IIS) Manager
 - In the explorer, select YOUR_SERVER
 - In the IIS tab in the middle, double-clicked to select Server Certification
 - In Server Certificates, chose "Create Self-Signed Certificate...", uses localhost as your friend name for the certificate
 - Change the Binding of the Default Web Site:
 - Access your application
- Add Certification to Java TrustStore
 - Export IIS certification:
 - Add IIS certification to Java Trust Store
- Add IIS certificate to Browsers
 - Chrome, IE (Internet Exploxer)
 - In IE 11Firefox

Over view

This documentation is about guide user to config system to run both ECC and BOND through Https.

To make ECC and BOND run through Httpss user needs:

- Enable Https for ECC in Tomcat.
- Enable Https for BOND in IIS (Internet Information Services).
- Add BOND's certificate to Trust Store of Tomcat's JVM (Tomcat which run ECC).
- Add BOND's certificate to Browsers (Chrome, Firefox, IE) run ECC.

Enable Https for ECC in Tomcat

Open cmd as Administrator



Move to the Tomcat config directory by using: cd YOUR_TOMCAT_DIRECTORY/conf



Generating Keystore

C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf>"%JAVA_HOME%\bin\keytool" -genkey -alias nb080010 -keyalg RSA -keystore myKeystore.jks -storepass administrator2011@ What is your first and last name? [Unknown]: localhost What is the name of your organizational unit? [Unknown]: YOUR_UNIT What is the name of your organization? [Unknown]: YOUR_ORGANIZATION What is the name of your City or Locality? [Unknown]: YOUR_CITY What is the name of your State or Province? [Unknown]: YOUR_STATE What is the two-letter country code for this unit? [Unknown]: VN IS CN=localhost, OU=YOUR_UNIT, O=YOUR_ORGANIZATION, L=YOUR_CITY, ST=YOUR_STATE, C=VN correct? [no]: YES Enter key password for <nb080010> (RETURN if same as keystore password): Re-enter new password:

Note:

In the question "What is your first and last name?", uses "localhost".

Uncomment Connector to port 8443 in YOUR_TOMCAT_DIRECTORY/conf/server.xml

	C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml - Notepad++	×
<u>File Edit Se</u>	arch <u>V</u> iew Encoding Language Se <u>t</u> tings Macro Run Plugins <u>W</u> indow <u>?</u>	Х
🕞 🖨 🗄 I	≌ В 6 🕼 🕼 🕼 🗊 🗢 ⊄ # 🧏 🔍 🤫 🖳 🖾 11 🧱 🥃 🖉 / ● 🗉 12 🔤 🤹 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉	
📄 server xml 🗵		
79	redirectPort="8443" />	^
80 -	>	
81 🛱	Define a SSL HTTP/1.1 Connector on port 8443</td <td></td>	
82	This connector uses the JSSE configuration, when using APR, the	
83	connector should be using the OpenSSL style configuration	
84 -	described in the APR documentation>	_
85	<connector <="" maxthreads="200" port="8443" td=""><td></td></connector>	
86	scheme=" <u>https</u> " secure="true" SSLEnabled="true"	
87	keystoreFile='\${ <u>catalina.home}/conf</u> /tomcatKeyStore.jkg' keystorePass="ventum20110" truststoreFile='C:/Program Files/Java/jre7/lib/security/ <u>cacerts</u>	
88	truststorePass=' <u>changeit</u> '	
89	clientAuth="false" sslProtocol="TLS"/>	
90		
91 🛱	</td <td></td>	
92	<connector <="" port="8443" protocol="HTTP/1.1" sslenabled="true" td=""><td></td></connector>	
93	maxThreads="150" scheme="https" secure="true"	
94	clientAuth="false" sslProtocol="TLS" />	
95 -	>	
96		~
<		>
eXtensible Mark	up Language file length : 6903 lines : 150 Ln : 1 Col : 1 Sel : 0 0 Dos\Windows UTF-8 w/o BOM	INS

Note: keystorePass is the password you've enter when Generating Keystore above

Please see this for example.

Reset tomcat to apply the changes

Access your application

Enable Https for BOND in IIS (Internet Information Services)

Open Internet Information Services (IIS) Manager

In the explorer, select YOUR_SERVER

In the IIS tab in the middle, double-clicked to select Server Certification



In Server Certificates, chose "Create Self-Signed Certificate...", uses *localhost* as your friend name for the certificate

Conver Contificate		Actions		
				Import
Use this feature to request and man		Create Certificate Request		
Name	Issued To	Issued By	Expiration	Complete Certificate Request
localhost	VVNCOREWIN01.sbb01.spoc.global	AutomicSoftwareGmbHIssuingCA	6/18/201	Create Domain Certificate
automic.com	VVNCOREWIN01.sbb01.spoc.global	VVNCOREWIN01.sbb01.spoc.gl	3/24/201	Create Self-Signed Certificate
	VVNCOREWIN01.sbb01.spoc.global	AutomicSoftwareGmbHRootCA	4/4/2016	Create Deir-Digned Certificate
Create Self-Signed Certificate		<u> </u>	4/6/2016	😢 Help
Cupatifu Fuland	Name		5/6/2019	Online Help
specity menu	y Name			
Specify a file name for the certi	ificate request. This information can be sent to a	certificate authority		
ror signing:				
Specify a friendly name for the	certificate:			
localbost				
liccanteset				
		OK Cancel		

Change the Binding of the Default Web Site:

Step 1: Select "Default Web Site"

Step 2: Under Edit Site, select Bindings ...

Step 3: Select row *https*, then chose *Edit*

Step 4:

Type: https

IP address: All Unassigned

Port: the port, example: 2222

SSL certificate: Link to your "Self-Signed Certificate" created in above step.



Access your application

By using: https://YOUR_DOMAIN:2222/YOUR_APPLICATION/ Example: https://localhost:2222/BOND/

Add Certification to Java TrustStore

Export IIS certification:

- Step 1: Select "Default Web Site"
- Step 2: Under Edit Site, select Bindings ...
- Step 3: Select row https, then chose Edit
- Step 4: Seleect View
- Step 5: Select Details tab then click "Copy to File..."
- Step 6: Click Next



Chose No, do not export the private key

xport Private Key	
You can choose to export the private key	v with the certificate.
Private keys are password protected. If y certificate, you must type a password on	you want to export the private key with the a later page.
Do you want to export the private key wi	ith the certificate?
C Yes, export the private key	
No, do not export the private key	¥
are more shout experting private keys	
sammore about <u>exporting private keys</u>	
	<back next=""> Ca</back>

Chose DER encoded binary X.509

Sel	ect the format you want to use:
00	DER encoded binary X.509 (.CER)
	© Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	C Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	C Microsoft Serialized Certificate Store (.SST)

Select destination to export Certificate file

Certificate Export Wizard		×
File to Export Specify the name of the file you want to exp	ort	
File name:		
C:\Users\Administrator\Desktop\BondCert\	localhostCertificate.cer	Browse
	< Back Next	> Cancel

Click Next then Finish.

Add IIS certification to Java Trust Store

Copy certificate file generated above step to folder Security of Tomcat JVM (can be found in the Tomcat file config: server.xml, property: truststoreFile)



<connector p<mark="">ort="8443" protocol=' maxThreads="150" schem</connector>	Computer + Local	Disk (C:) 🔹 Pro	gram Files 👻 Java 👻 jdk1.7.0	_51 🔹 jre 🔹 lib 🔹 secu	ity	👻 🔽 S	earch security	2
clientAuth="false" ssl >	Organize 👻 Include in library 👻	Share with \bullet	New folder					💷 🝷 🚺 😧
	🔆 Favorites	_	Name ^		Date modified	Туре	Size	
<pre><!-- Define an AJP 1.3 Connector<br--><connector catalina"="" defaultho<="" port="8009" protocol="</pre></td><td>🧮 Desktop</td><td></td><td>📄 blacklist</td><td>Truct store file</td><td>5/27/2014 8:03 AM</td><td>File</td><td>3 KB</td><td></td></tr><tr><td></td><td>Downloads</td><td></td><td>Cacerts</td><td>Trust store me</td><td>4/6/2015 9:30 AM</td><td>File</td><td>83 KB</td><td></td></tr><tr><td>d by Remine concerned the sur-</td><td>Recent Places</td><td></td><td>🔄 certification.cer</td><td></td><td>4/2/2015 5:23 PM</td><td>Security Certificate</td><td>1 KB</td><td></td></tr><tr><td>every request. The Engine i</td><td>benerat 2021</td><td>_</td><td>java.policy</td><td></td><td>5/27/2014 8:03 AM</td><td>POLICY File</td><td>3 KB</td><td></td></tr><tr><td>analyzes the HTTP headers ir</td><td>Tomcat 7</td><td></td><td>java.security</td><td></td><td>5/27/2014 8:03 AM</td><td>SECURITY File</td><td>18 KB</td><td></td></tr><tr><td>on to the appropriate Host</td><td>automic</td><td></td><td>javaf×.policy</td><td></td><td>5/27/2014 8:03 AM</td><td>POLICY File</td><td>1 KB</td><td></td></tr><tr><td>Documentation at /docs/confi</td><td>BondCert</td><td></td><td>javaws.policy</td><td>Self ce</td><td>rtificate file</td><td>POLICY File</td><td>1 KB</td><td></td></tr><tr><td><! You should set jvmRoute to s</td><td>openssl-0.9.8k_X64</td><td></td><td>🛋 local_policy.jar</td><td>ex</td><td>ported M</td><td>Executable Jar File</td><td>3 KB</td><td></td></tr><tr><td><Engine name=" td=""><td>퉬 security</td><td></td><td>localhostCertificate.cer</td><td></td><td>AM</td><td>Security Certificate</td><td>1 KB</td><td></td></connector></pre>	퉬 security		localhostCertificate.cer		AM	Security Certificate	1 KB	
<pre>> <engine defaulthc<="" name="Catalina" pre=""></engine></pre>	📔 Installations		trusted.libraries		5/27/2014 8:03 AM	LIBRARIES File	0 KB	
			🔳 US_export_policy.jar		3/26/2015 3:10 PM	Executable Jar File	3 KB	
For clustering, please take</td <td>Calibraries</td> <td></td> <td>vvncorewin01Cert.cer</td> <td></td> <td>4/6/2015 9:13 AM</td> <td>Security Certificate</td> <td>1 KB</td> <td></td>	Calibraries		vvncorewin01Cert.cer		4/6/2015 9:13 AM	Security Certificate	1 KB	
/docs/cluster-howto.html (/docs/config/cluster.html)	Documents							
</td <td>Pictures</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Pictures							

Open cmd and move it to folder Security of Tomcat JVM:

Add certificate to cacerts Trust Store by using: keytool -import -alias ca -file <your_self_certificate.cer> -keystore cacerts -storepass changeit

Example: keytool -import -alias ca -file localhostCertificate.cer -keystore cacerts -storepass changeit

	i ini consection consectiat. 200	C:\WINDOWS\system32\cmd.exe		×
	C:\Program Files\Java\jre7\lib\security>keytool -impo	rt -alias ca -file localhostCertificate.cer -keystore cacerts -storepass	changeit	^
3				

Select Trust this certificate

C:\Program Files\Java\jre7\lib\security>keytool -import -alias ca -file vvncorewin01Cert.cer -keystore cacerts -storepass changeit Owner: CN=UUNCOREWIN01.sbb01.spoc.global Issuer: CN=UUNCOREWIN01.sbb01.spoc.global Serial number: 4c44cc93a1af2cb44be3410c7e152d7f Ualid from: Mon Apr 06 09:08:12 ICT 2015 until: Wed Apr 06 07:00:00 ICT 2016 Certificate fingerprints: Certificate fingerprints: MD5: 92:03:6C:4C:02:EA:BC:DA:9B:9D:58:EB:CB:F4:CA:3F SHA1: 2A:84:D7:28:11:F5:CB:B8:46:3B:F1:4A:2A:20:CA:7E:64:9D:75:6A SHA256: 00:DA:E2:EA:9B:41:99:60:5E:77:E7:3D:39:17:B0:8F:32:03:9C:3D:5E:76:A1:AC:77:A0:4A:1D:A4:5E:AB:9C Signature algorithm name: SHA1withRSA Version: 3
Extensions:
#1: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth]
#2: ObjectId: 2.5.29.15 Criticality=false KeyUsage [Key_Encipherment Data_Encipherment]
Trust this certificate? [no]: yes Certificate was added to keystore
C:\Program Files\Java\jre7\lib\security>_

Add IIS certificate to Browsers

Chrome, IE (Internet Exploxer)

Copy IIS certification (the same file IIS certification in step "Add IIS certification to Java Trust Store" above) to you local PC (PC which run Browsers). Assume IIS is copied to C:/Cerfitication

Start Mircrosoft Management Console by open run (Select Start, then Run).

In the Run, type mmc.exe then press Enter

Programs(1)	
🙀 🚟 mmc.exe	
A	
>> See more results	
mmc 🔀 Log off 🕨	

Select File -> Add/Remove Snap-in (Ctrl+M).

Under "Available snap-ins", select Certificates then click Add.

A Certificates snap-in window will show up, select Computer account, then Next

sole1 - [Console Root]					
Action View Favorites Window Help					
- I 🖬 I 🗟 🔳					
nsole Root	Name				Actions
	I	*1 *	p to show in this view.		Console Root
dd or Remove Snap-in s		×			More Actio
You can select snap-ins for this console from those av extensible snap-ins, you can configure which extensi	vailable on your computer and configure th ons are enabled.	e selected set of snap-ins. For	Certificates snap-in		
Available snap-ins:	Selected snap-ins:		This snap-in will always manage certificates for:		
Snap-in Vendor 🔺	Console Root	Edit Extensions	C. Muluser account		
ActiveX Control Microsoft Cor			C Service account		
Authorization Mar Microsoft Cor		Remove			
Certificates Microsoft Cor			Computer account		
Component Services Microsoft Cor		Move Up	<u> </u>		
Computer Managem Microsoft Cor					
Device Manager Microsoft Cor	Add >	Move Down			
Brucesh Viewer Microsoft and	Hdd 2				
Eolder Microsoft Cor					
Group Policy Object Microsoft Cor					
LP Security Monitor Microsoft Cor					
R IP Security Policy Ma Microsoft Cor					
Link to Web Address Microsoft Cor					
💻 Local Users and Gro Microsoft Cor 🔳 👘		Advanced			
Description:					
The Certificates spap-in allows you to browse the co	ontents of the certificate stores for yourse	If. a service, or a computer.		C Rook News	Canaal
		,,,, pater (< Daux Next>	Cancel
		OK Cancel			
	1		1		

Select Local Computer, click Finish then OK

Add or Remove Snap-ins	×
Yot ext Select Computer	snap-ins. For
Ava Select the computer you want this snap-in to manage. Si This snap-in will always manage: Image: Image: Image: Image:	Edit Extensions
Another computer: Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	Move <u>U</u> p Move <u>D</u> own
	Ad <u>v</u> anced
Des	computer.
ОК	Cancel

Expand Certificates (Local Computer), expand Trusted Root Certification Authorities.

Under Trusted Root Certification Authorities, right click into Certificates, select All Tasks, Import then click Next

🚟 Console1 - [Console Root\Certificates (Local Com	puter)\Trusted Root Certification Au	ithorities\Certificates]				
🚟 File Action View Favorites Window Help						
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status Certil
📃 👼 Certificates (Local Computer)	a-sign projects	a-sign projects	18/09/2032	<a >	<none></none>	
🕀 🚞 Personal	🔄 a-sign uni	a-sign uni	14/09/2032	<all></all>	<none></none>	
Trusted Root Certification Authorities	A-Trust-nQual-01	A-Trust-nQual-01	01/12/2014	<all></all>	<none></none>	
	Trust-Qual-01	A-Trust-Qual-01	01/12/2014	<all></all>	<none></none>	
Enterp All Tasks Interp	Trust-Qual-02	A-Trust-Qual-02	03/12/2014	<all></all>	<none></none>	
	automic.com	automic.com	18/06/2043	<all></all>	<none></none>	CA
Invite New Window from Here	AutomicSoftwareGmbHRootCA	AutomicSoftwareGmbHRootCA	18/06/2043	<all></all>	<none></none>	CA
Third-E May Taskand View	AutomicSoftwareGmbHRootCA	AutomicSoftwareGmbHRootCA	18/06/2043	<all></all>	<none></none>	CA
	Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Server Authenticatio	Baltimore CyberTrust	
E C Remoty Refresh	Class 3 Public Primary Certification	Class 3 Public Primary Certification A	02/08/2028	Secure Email, Client	VeriSign Class 3 Publi	
Certific Export List	🔄 🔄 Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Time Stamping	Microsoft Timestamp	
🕀 🧰 Smart (👘 👘	🔄 🖾 DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	Server Authenticatio	DigiCert	
	DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	10/11/2031	Server Authenticatio	DigiCert	
	Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	22/08/2018	Secure Email, Server	GeoTrust	
	🔄 🔄 f.decrypt01	f.decrypt01	15/02/2105	File Recovery	<none></none>	

Browser to copied IIS certificate, then Next

	1 months and a second se	
Certificate Import Wizard	G open	×
File to Import	ν 🌀 🕞 🗸 Komputer 🔸 Local Disk (C:) 🔹 Certification 👘 🔹 🛃	Search Certification 🛛 😰
Specify the file you want to import.		
	E Organize ▼ New rolder	
Ele somo	c 🔆 Favorites 📥 Name A	Date modified Type
Prie name:	i 📃 Desktop 🗔 localhostCertificate.cer	06/04/2015 9:13 SA Security Cerl
	i 🚯 Downloads	
Note: More than one certificate can be stored in a single file in the following formats:	🖞 🖳 Recent Places 🛛 🦉	
Personal Information Exchange- PKCS #12 (.PEXP12)	automic	
Cryptographic Message Syncax Scandard- PKCS #7 Certificates (.P7B)	1 sonarqube-5.0.1	
Microsoft Serialized Certificate Store (.SST)	li 🦰 Libravies	
	Documents	
	li 🔛 Pictures	
	🗧 🔣 Videos	
Learn more about <u>certificate file formats</u>		
	c File name: localhostCertificate.cer 🗾 🗙	.509 Certificate (*.cer;*.crt)
< Back Next > Cancel		Open Cancel
	· · · · · · · · · · · · · · · · · · ·	

Select "Place all certificates in the following store", click Next, then Finish

tificate 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 loca the certificate.	ation for
\odot Automatically select the certificate store based on the type of certifica	te
Place all certificates in the following store	
Certificate store:	
Trusted Root Certification Authorities Brow	vse
earn more about <u>certificate stores</u>	
	Canad

Success window will be shown



In IE 11

If got below warning



Click Add, a Trusted sites window will show up. Click Add, then Close



Firefox

Select Open Menu, chose Option



Select Advanced, tab Certificates, click View Certificates, Certificate Manage window will open.

Under Certificate Manager, select tab Servers, click Add Exception, an Add Security Exception window will open.

Under Add Security Exception, past BOND's full address to Location, then click Get Certificate. Keep check-box at Permanently store this exception, then click Confirm Security Exception.

Options		×	
General Tabs Search Content App	lications Privacy Security	Sync Advanced	
General Data Choices Network Update Cer When a server requests my personal certificate: © Select one automatically © Ask me every © Query OCSP responder servers to confirm th View Certificates Security Devices © Certificate Manager	tificates / time		You are about to override how Firefox identifies this site. Legitimate banks, stores, and other public sites will not ask you to do this. Server Location: https://vvncorewin01.sbb01.spoc.global:2222/BOND/ Certificate Status This site attempts to identify itself with invalid information. Unknown Identity The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
Your Certificates People Servers Authoritie You have certificates on file that identify these Certificate Name Server DigiNotar DigiNotar Cyber CA * DigiNotar Cyber CA * DigiNotar Root CA DigiNotar Services 10 * DigiNotar Services 10 * DigiNotar PKIoverheid * DigiNotar Services 10 * Digisign Server ID - (E * Yjew	s Others servers: Lifetime Expires On Permanent 04/10/2011 Permanent 20/09/2013 Permanent 01/04/2025 Permanent 26/08/2013 Permanent 23/03/2020 Permanent 27/07/2015 Permanent 17/07/2015 Permanent 17/07/2015		Permanently store this exception <u>Confirm Security Exception</u> Cancel