ESET Tech Center

Kennisbank > ESET PROTECT > ESET PROTECT Webconsole (Apache Tomcat) - SSL Certificate from windows keystore

ESET PROTECT Webconsole (Apache Tomcat) - SSL Certificate from windows keystore

Mitchell | ESET Nederland - 2022-10-26 - Reacties (0) - ESET PROTECT

Pre-requisites:

1. Certificate in p12 or pfx format (with private key)

Configuring Apache Tomcat:

- open powershell as the service account used by Apache Tomcat: runas /user:domain\sa-eset powershell.exe
- Open certmgr.msc in the powershell session running as the service account. certmgr.msc
- 3. In certmgr.msc import the certificate into the Personal store:

🥁 certmgr - [Certificates - Current User\Personal]						\times	
File Action View							
🔶 🚈 📰 🖻 🗟 📑 🖉 📷							
Certificates - Current User Object		t Type					
> Trusted F	Find Certificates		There are no items to show in this	view.			
Enterpris	All Tasks	>	Find Certificates				
> 📫 Active Di	View	>	Request New Certificate				
> 📔 Trusted F	Refresh		Import				
> Contruster	Export List		Advanced Operations >				
> 📫 Trusted F > 📫 Client Au	Trusted F Help						
Smart Card Trus	ted Roots						

4. Note that the "friendly name" should contain a value in order for Apache Tomcat to use the certificate, if the friendly name value is empty, right click the certificate after importing and select properties: 🜇 certmgr - [Certificates - Current User\Personal\Certificates]

File Action View Help = 🔿 📅 4 🖏 💥 🗒 🗟 ? 🗊 Certificates - Current User Issued To Issued I ✓ [™] Personal protect.lab.local protect 📔 Certificates Open Trusted Root Certification Au > > 📔 Enterprise Trust All Tasks > > 📔 Intermediate Certification Au Cut Active Directory User Object > Сору Trusted Publishers 5 Untrusted Certificates Delete 5 Third-Party Root Certification > Properties Trusted People > Client Authentication Issuers 5 Help > i Smart Card Trusted Roots

Fill in the friendly name field:

protect.la	?	\times	
General	Cross-Certificates OCSP Extended Validation		
Friendly Descrip Oertif Dis Dis En	tion: icate purposes able all purposes for this certificate sable all purposes for this certificate able only the following purposes Note: You may only edit certificate purposes that are a the certification path.	llowed by	
	 Server Authentication Client Authentication Code Signing Secure Email Time Stamping Microsoft Trust List Signing Microsoft Time Stamping Add F 	Purpose	*
	OK Cancel	Арр	oly

 Go back to the powershell session and verify the certificate exists: dir Cert:\CurrentUser\My



 Open the Apache Tomcat server.xml, by default located at: "C:\Program Files\Apache Software Foundation\apache-tomcat-9.0.64\conf\server.xml" (path may vary, based on installed version of Apache Tomcat)

```
A. Find the following line:
<Connector server="OtherWebServer" port="443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true" maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Program
Files\Apache Software Foundation\apache-tomcat-9.0.64\.keystore"
keystorePass="******" keyAlias="tomcat"
sslEnabledProtocols="TLSv1.2,TLSv1.3" honorCipherOrder="true"
ciphers="TLS AES 256 GCM SHA384, TLS CHACHA20 POLY1305 SHA256,
TLS AES 128 GCM SHA256, TLS ECDHE RSA WITH AES 256 GCM SHA384,
TLS DHE RSA WITH AES 256 GCM SHA384,
TLS ECDHE ECDSA WITH AES 256 GCM SHA384,
TLS ECDHE ECDSA WITH AES 128 GCM SHA256,
TLS ECDHE RSA WITH AES 128 GCM SHA256,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256" />
```

B. Change it to: (note that the keyAlias value should match the friendly name set in step 4.

```
<Connector server="OtherWebServer" port="443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true" maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreType="Windows-My"
keystoreFile="" keystorePass="" keyAlias="tomcat"
sslEnabledProtocols="TLSv1.2,TLSv1.3" honorCipherOrder="true"
ciphers="TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256,
TLS_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384,
```

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"
- sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImple
 mentation" />
- 7. Restart the Apache Tomcat Service, It should now use the certificate from the certificate store.