Hewlett Packard Enterprise

HPE Propel

Software version 2.10

HPE Propel SSL renewal process using customer certificates

Contents

Legal Notices 2

Introduction 3

Preparation work 3

Load the customer Certificate Authority (CA) into the Propel global Java keystore 3

Prepare for a Certificate Signing Request (CSR) 5

Update Propel in case you have a certificate with wildcard 13

HP Operations Orchestration 13

RabbitMQ 15

Restart Propel and Testing 16

Appendix 18

Support 20

Documentation release date: May 2016

Software release date: December 2015

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise (HPE) products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

Documentation Updates

The title page of this document contains the following identifying information:

- *Software Version number, which indicates the software version.*
- *Document Release Date, which changes each time the document is updated.*
- *Software Release Date, which indicates the release date of this version of the software.*

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: https://softwaresupport.hp.com/group/softwaresupport

Use the Search function at the top of the page to find documentation, whitepapers, and other information sources. To learn more about using the customer support site, go to: https://softwaresupport.hp.com/documents/10180/14684/HP_Software_Customer_Support_Handbook/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

Introduction

Most of the instructions defined in this white paper are based on the HPE Propel 2.10 Administration Guide. See chapter Replacing Generated HP Propel SSL Certificates with CA-Signed Certificates (page 10 – 13). This document can be seen as an addendum on the official HPE Propel 2.10 Administration Guide.

Documentation

HP Propel documentation can be found at https://softwaresupport.hp.com/group/softwaresupport.

You need to sign-in or register to use this site. Use the Search *function at the top of the page to find documentation, whitepapers, and other information sources. To learn more about using the customer support site, go to:*
https://softwaresupport.hp.com/documents/10180/14684/HP_Software_Customer_Support_Handbook/

For more information or to track updates for all HP Propel documentation, refer to the HP Propel Documentation List.

To help us improve our documents, please send feedback to Propel_IE@hpe.com.

Preparation work

Import Supplier certificates

Before changing the the Propel certificates, make sure the SSL integrations with the back end systems (like SM, CSA, OO or SAW) work correctly. This will help you to nail down SSL issues after you changed the Propel certificate. See the official Propel documentation how back end supplier certificates should be imported in Propel.

Setup Suppliers

Configure Suppliers f.i. SM, CSA, SAW, start the aggregation, create a catalog and publish your items. Test the ordering and support request part. If all of this works, you know you can perfectly SSL integrate with your back end systems.

Load the customer Certificate Authority (CA) into the Propel global Java keystore

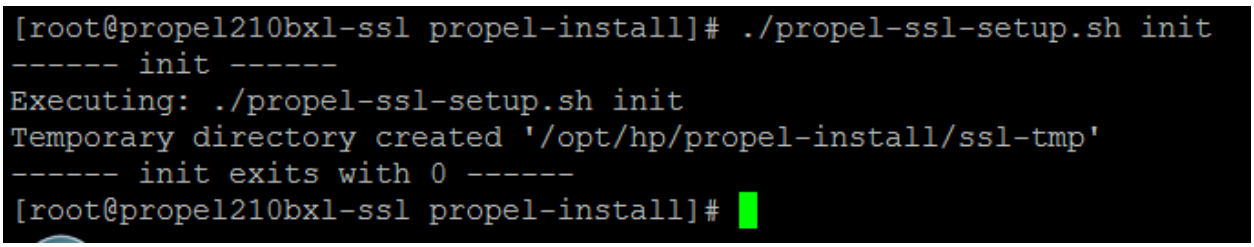
1. *Stop the HPE Propel services:*

   ```
   # propel stop
   ```

2. *Initialize the SSL-tmp working directory*

   ```
   # cp -rp /opt/hp/propel-install/ssl-tmp /opt/hp/propel-install/ssl-tmp.orig
   # cd /opt/hp/propel-install
   # ./propel-ssl-setup.sh init
   ```

   Note: this will recreate `/opt/hp/propel-install/ssl-tmp` *and remove all existing files.*



3. *Load the Certificate Authority (CA) into the global java keystore*

Ask the customer for the public certificate of their CA.

- *It needs to be in PEM format.*
- *PEM certificates usually have extensions such as* `.pem`*,* `.crt`*,* `.cer` *and* `.key`*.*
- *They are Base64 encoded ASCII files and contain:*

`"-----BEGIN CERTIFICATE-----"`
and
`"-----END CERTIFICATE-----"`
statements.

Copy the CA certificate to /opt/hp/propel-install/ssl-tmp

Example:

```
[root@propel210globiconssl ssl-tmp]# more myCompanyCA.pem
-----BEGIN CERTIFICATE-----
MIIFHjCCBAagAwIBAgIJANpvILXWFh+tMA0GCSqGSIb3DQEBBQUAMIG6MQswCQYD
VQQGEwJCRTERMA8GA1UEBxMIQnJ1c3NlbHMxGDAWBgNVBAoTD0hld2xldHQtUGFj
a2FyZDELMAkGA1UEChMCSFAxFDASBgNVBAsTC0hQIFNvZnR3YXJlMScwJQYDVQQL
Ex5FQiBTVyBCVE8gUHJvZmVzc2lvbmFsIFNlcnZpY2UxEzARBgNVBAMTCkhQIEND
Uk0gQ0ExHTAbBgkqhkiG9w0BCQEWDmJydW5vZGdAaHAuY29tMB4XDTEyMDExMDIx
```

Once you have this file, copy it to the new file ***CA.crt*** *in* `/opt/hp/propel-install/ssl-tmp` *(f.i.: cp /opt/hp/propel-install/ssl-tmp/myCompanyCA.pem /opt/hp/propel-install/ssl-tmp/CA.crt):*

```
/opt/hp/propel-install/ssl-tmp/CA.crt
```

It's important to keep the name as CA.crt ! Plenty of Propel configuration files are using this name.

Backup the existing cacerts file:

```
# cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/cacerts /usr/lib/jvm/java-
1.8.0-openjdk/jre/lib/security/cacerts.orig
```

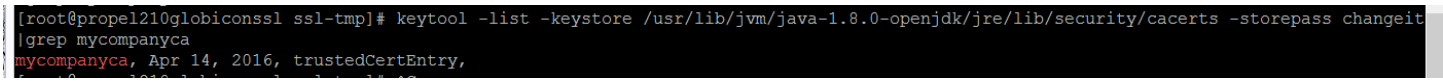
Then import the CA.crt in the cacerts file

```
# keytool -import -file /opt/hp/propel-install/ssl-tmp/CA.crt -alias mycompanyca -
trustcacerts -keystore /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/cacerts
```

cacerts password = changeit

You can check if the Propel truststore contains your CA cert:

```
# keytool -list -keystore /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/cacerts
-storepass changeit |grep mycompanyca
```



4. *Backup the existing SSL configuration used by the Propel microservices (cf. their configuration files), most of the important SSL-related files are here:*

```
# cd /opt/hp/propel
# cp -rp security security.orig
```

These files will be removed or updated in a later step.

5. *Optional – Only if your HPE Propel VM needs multiple hostnames, all of these name must appear in the certificate. This is achieved by using the Subject Alternative Names (SAN) attribute.*

If it is necessary to include multiple hostnames, edit the file:

```
/etc/pki/tls/openssl.cnf
```

Ensure that it has entries like this:

```
# This is required for TSA certificates.
# extendedKeyUsage = critical,timeStamping

[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = server1.example.com
DNS.2 = mail.example.com
DNS.3 = www.example.com
```

Important: the host name returned from the hostname command must also appear as one of the SAN entries in openssl.cnf.

Prepare for a Certificate Signing Request (CSR)

In the following steps we'll generate the Certificate Signing Request (CSR) and Server Private Key pair.

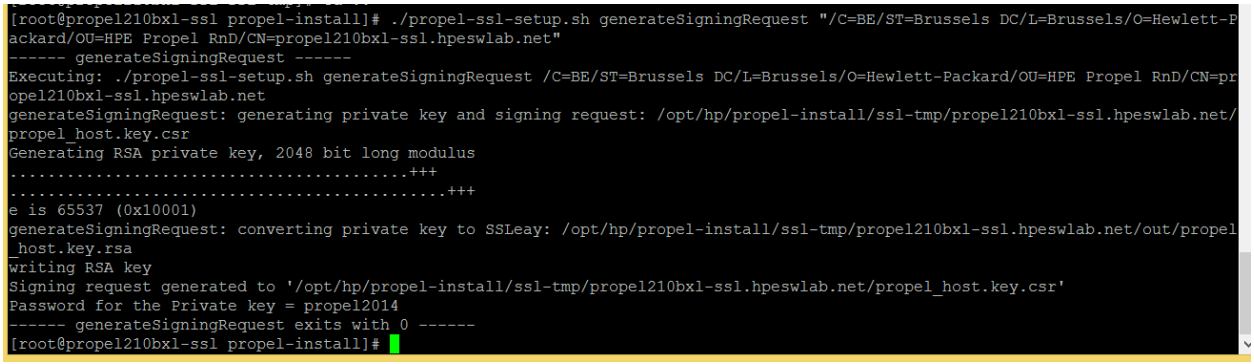
6. *Generate a Certificate Signing Request and Server Private Key pair, where* **<FQDN>** *is the fully-qualified domain name of your Propel host.*

```
# cd /opt/hp/propel-install
# ./propel-ssl-setup.sh generateSigningRequest "/C=BE/ST=Brussels
DC/L=Brussels/O=Hewlett-Packard/OU=HPE Propel RnD/CN=<FQDN>"
```

Note: SUBJECT is the signing request subject in the slash-separated form. "CN" must be the last field in the subject and contain the fully qualified hostname of the HPE Propel VM. Enclose the subject in double quotes, such as: "/C=US/ST=CA/L=San Jose/O=StartUpCompany/OU=Software/CN=mypropelserver.example.com"

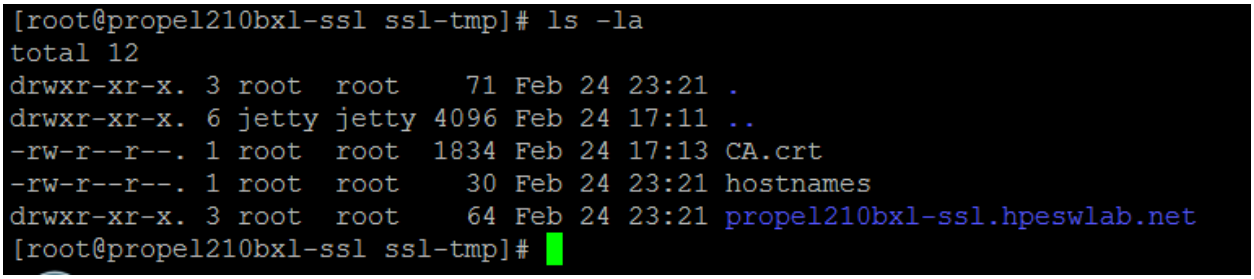
f.i.: `./propel-ssl-setup.sh generateSigningRequest "/C=BE/ST=Brussels DC/L=Brussels/O=Hewlett Packard Enterprise/OU=HPE Propel RnD CPE/CN=propel210bxl-ssl.hpeswlab.net"`

Note: The private key password (= propel2014) is automatically generated by the script. (You could modified the propel-ssl-setup.sh script to display it). On page 11 of the 2.10 Administration guide it's indicated it can be changed but that's not the case. A QCCR is opened for this issue.



The command propel-ssl-setup.sh creates 4 new files and 2 new directories:

```
/opt/hp/propel-install/ssl-tmp/hostnames
/opt/hp/propel-install/ssl-tmp/<FQDN>/
/opt/hp/propel-install/ssl-tmp/<FQDN>/private.key.pem
/opt/hp/propel-install/ssl-tmp/<FQDN>/propel_host.key.csr
/opt/hp/propel-install/ssl-tmp/<FQDN>/out/
/opt/hp/propel-install/ssl-tmp/<FQDN>/out/propel_host.key.rsa
```



```
[root@propel210bxl-ssl propel-install]# ls -l /opt/hp/propel-install/ssl-tmp/propel210bxl-ssl.hpeswlab.net
total 8
drwxr-xr-x. 2 root root   32 Feb  9 11:23 out
-rw-r--r--. 1 root root 1751 Feb  9 11:23 private.key.pem
-rw-r--r--. 1 root root 1078 Feb  9 11:23 propel_host.key.csr
[root@propel210bxl-ssl propel-install]#
```

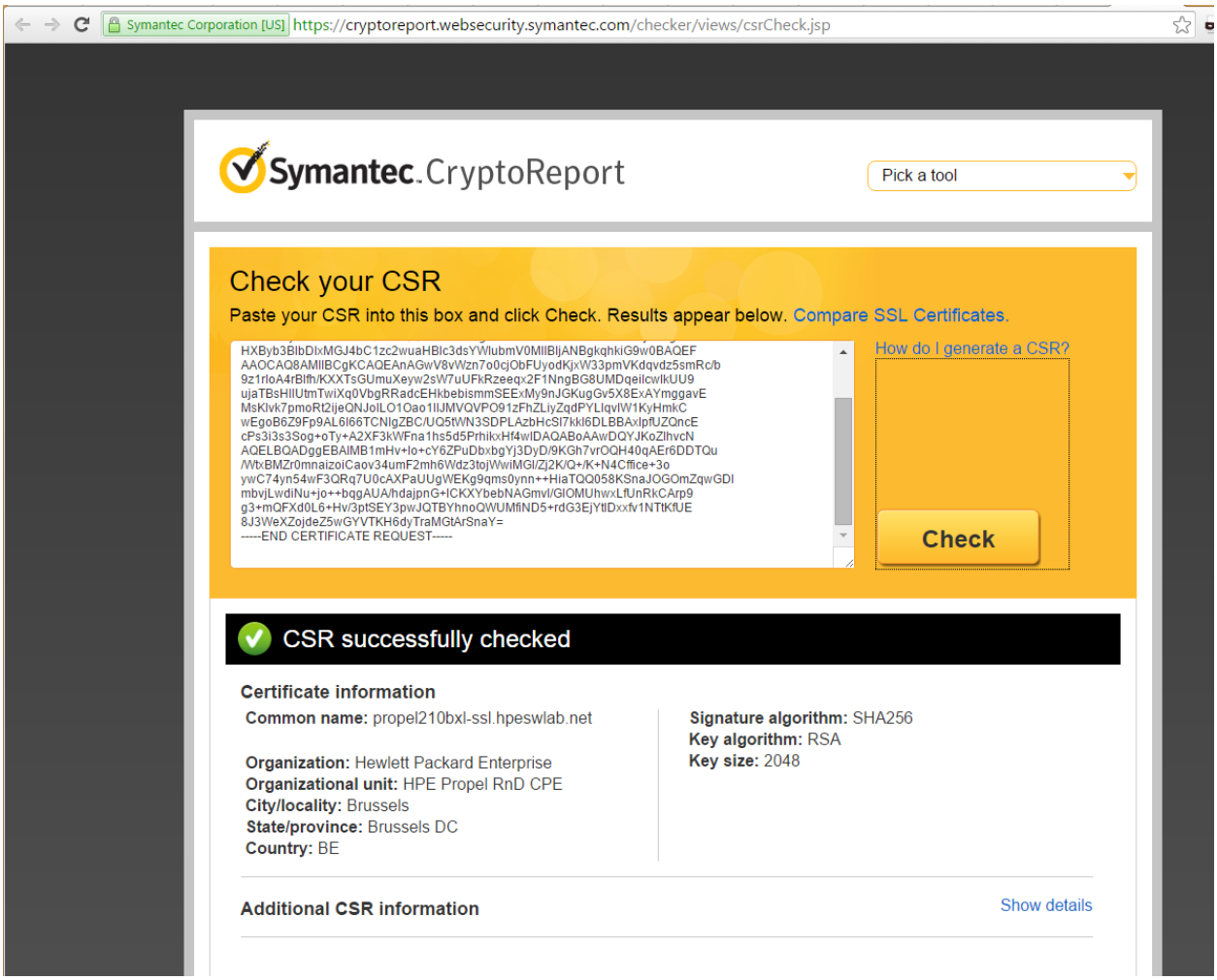
```
[root@propel210bxl-ssl propel-install]# ls -l /opt/hp/propel-install/ssl-tmp/propel210bxl-ssl.hpeswlab.net/out
total 4
-rw-r--r--. 1 root root 1679 Feb  9 11:23 propel_host.key.rsa
[root@propel210bxl-ssl propel-install]#
```

7. *You can verify the content of your CSR by pasting the text in here:*
   https://ssltools.websecurity.symantec.com/checker/views/csrCheck.jsp

   Content of the CSR:

```
drwxr-xr-x. 2 root root   32 Feb  9 11:23 out
-rw-r--r--. 1 root root 1751 Feb  9 11:23 private.key.pem
-rw-r--r--. 1 root root 1078 Feb  9 11:23 propel_host.key.csr
[root@propel210bxl-ssl propel210bxl-ssl.hpeswlab.net]# cat propel_host.key.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC4jCCAcoCAQAwgZwxCzAJBgNVBAYTAkJFMRQwEgYDVQQIDAtCcnVzc2VscyBE
QzERMA8GA1UEBwwIQnJ1c3NlbHMxIzAhBgNVBAoMGkhld2xldHQgUGFja2FyZCBF
bnRlcnByaXNlMRcwFQYDVQQLDA5IUEUgUHJvcGVsIFJuRDEmMCQGA1UEAwwdcHJv
cGVsMjEwYnhsLXNzbC5ocGVzd2xhYi5uZXQwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCccbHODotCkRXV79LnHKZ0IhtCcxmZ/HpZW/Ia8Rhl6NLYwA9j
ik1ym0ecQMyLpIw0mFJFIG/qJE8ZCui74HKWHOkZ0vZmHEe1Bu0T1JHz3dz+dXQS
1rQuRyCckPVfZwo8uhObCD+/q512VtJwogVpI6bzjsqgBa2ByxE2wJjZ14vJDXl8
sHv2hAEzuMY9TwvLgs4JLVrtBb6SkAZ8l8AlQcwVlL6anJkvCElU+hkklQn7X3J4
vXpNm7/6Vfk3EQTmvrEDTVEavOOZdEyufmlqWNsyJXfFKu3Up0ToshACjCOLt9uW
aKZVzTZpSdq75s5raCTh0d67BvOOOf1BYobNAgMBAAGgADANBgkqhkiG9w0BAQsF
AAOCAQEAWV/SxfO8aWrpQVaSJANEOGcoNnsuasy/KhJkpi2lmIWexRbqC3ZqCUS3
ASsR0n+WXitEH0AUiovVuCVRfutyy9h0o9c4ILYwziLQfhWDp+UDpdaVvCnJKc5W
GQ8kjGtdcvrIwtEerbjc2YGfMWxa6YlxfaaAUJp1phq48bFvjclAKG6HDVrolggs
8ZYf+qbX0eXqMFB5XVxchV+n/uigDjbc0npVNiR0i1pCV9pL1gjf70kgho16tIXu
alnDS83cAa1IyGyz3hdN/WwPMpb/66BaJx3j7vOF1lnkG8FsRHu5GwEsPICuvmUv
moGHDVIKi5zSFqgl9IiSgSUh1buLjQ==
-----END CERTIFICATE REQUEST-----
[root@propel210bxl-ssl propel210bxl-ssl.hpeswlab.net]#
```

   Content check:



8. *Send the CSR containing the public key to your CA. This is a process specific to your company, and network administrators should know how to accomplish this. Ask for the certificate to be delivered in PEM format. If it is not, you can convert formats with the openssl command. (see an example on point 8 page 11, Propel 2.10 Admininistration guide)*

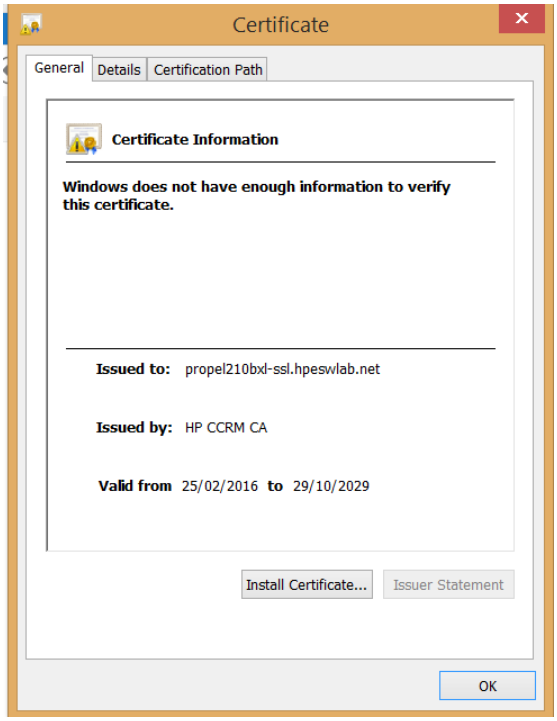
   See Appendix for an example using openssl to sign the Propel server certificate with a self-signed CA.

9. *Once the certificates have been received, copy the new host certificate to* `/opt/hp/propel-install/ssl-tmp/<FQDN>/out/` *and call it* ***propel_host.crt****.*

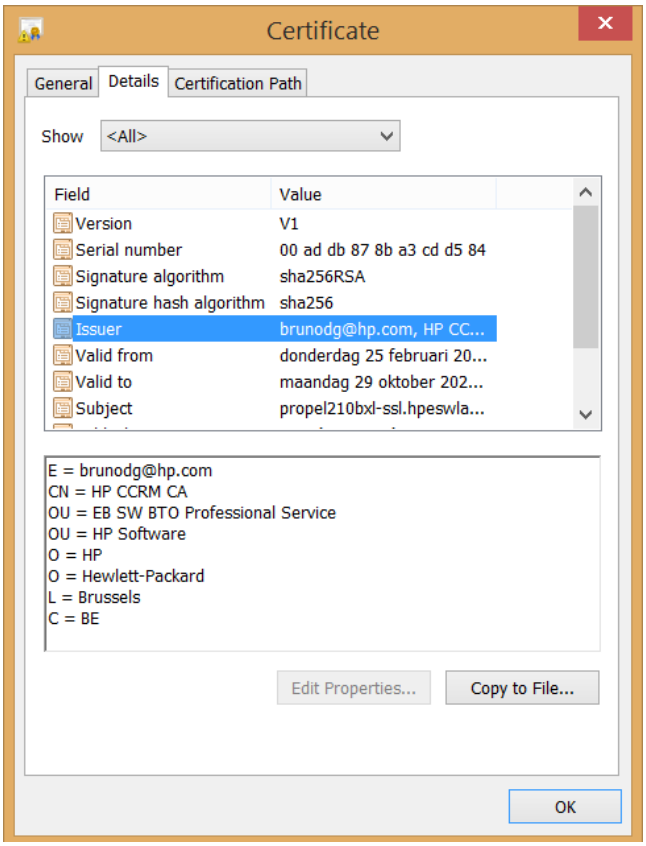
   `/opt/hp/propel-install/ssl-tmp/<FQDN>/out/propel_host.crt`

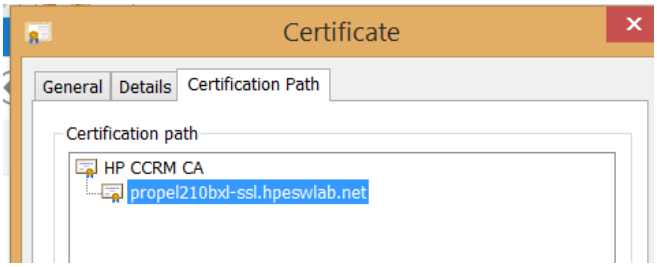
```
[root@propel210bxl-ssl propel210bxl-ssl.hpeswlab.net]# cd out
[root@propel210bxl-ssl out]# ls -l
total 4
-rw-r--r--. 1 root root 1679 Feb  9 11:36 propel_host.key.rsa
[root@propel210bxl-ssl out]# vi propel_host.crt
[root@propel210bxl-ssl out]# ls -la
total 8
drwxr-xr-x. 2 root root   54 Feb  9 11:41 .
drwxr-xr-x. 3 root root   64 Feb  9 11:36 ..
-rw-r--r--. 1 root root 2358 Feb  9 11:41 propel_host.crt
-rw-r--r--. 1 root root 1679 Feb  9 11:36 propel_host.key.rsa
[root@propel210bxl-ssl out]# cat propel_host.crt
-----BEGIN CERTIFICATE-----
MIIGoDCCBYigAwIBAgIQEJHBerqeRy3i7oEBpBbM+TANBgkqhkiG9w0BAQUFADCB
njEPMA0GA1UEChMGaHAuY29tMRowGAYDVQQLExFJVCBJbmZyYXN0cnVjdHVyZTEL
MAkGA1UEBhMCVVMxIDAeBgNVBAoTF0hld2xldHQtUGFja2FyZCBDb21wYW55MUAw
PgYDVQQDEzdIZXdsZXR0LVBhY2thcmQgUHJpdmF0ZSBDbGFzcyAyIENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5MB4XDTE2MDIwOTAwMDAwMFoXDTE3MDIwODIzNTk1OVow
XDEgMB4GA1UEChQXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkxEDAOBgNVBAsUB1Nl
cnZlcnMxJjAkBgNVBAMTHXByb3BlbDIxMGJ4bC1zc2wuaHBlc3dsYWIubmV0MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlt6vy02IEKJepCLI9XztgwZv
wqfncRuRHqTuEj+FTzfq0NzB7i8RhcfEy598L/JQYel0CXWkh6xJm6TPmi4hll/L
r82mlyoaCeNo8Zd0y8BG6k8fouX/xWEsB0MlnyjlBhpCu5IQD/o8DmLV0RDyrCyX
jaHES6vOfPELxZWQMwp90/w355oPotEJcH1cRQ3sxfEGSyV5AJ0IpjTV2rkN9AiK
um2qi++SvmBTYcRPRKMQjywDn+e08SXTT9k/dXu18UEI6RmQzqDlFgE+86C4KscM
Xzu27hU3FRH8b475cmrS3OTHD8O8u9I+7LLG9GqCSQ0RKV3UU5dH2FbXIOtjhwID
AQABo4IDGTCCAxUwDAYDVR0TAQH/BAIwADADBgNVHQ8BAf8EBAMCBLAwHwYDVR0j
BBgwFoAUN+33FXktMKWYmnW2XDfjiOoRatUwHQYDVR0OBBYEFDUjInZLav6d4gB9
```

10. *Display the content of the certificate on a Windows PC*

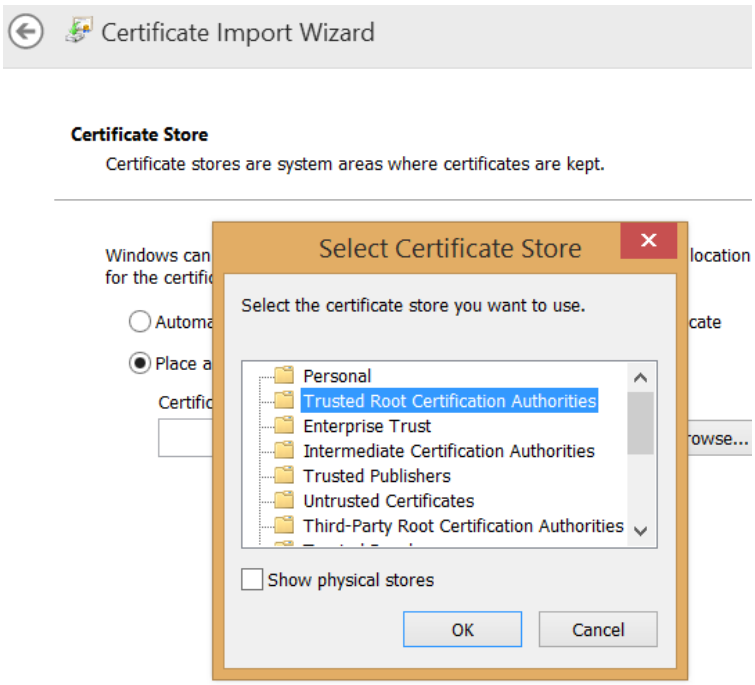


It provides info which CA signed the cert:





Note: don't forget to import your CA cert into the Trusted Root CA:



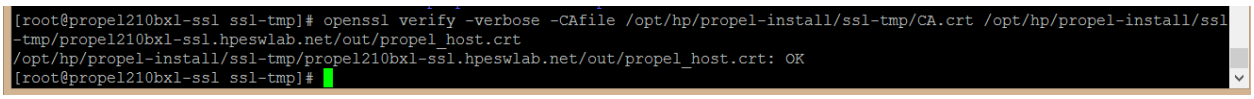
11. *Validate that the certificate and the CA match:*

```
# openssl verify -verbose -CAfile /opt/hp/propel-install/ssl-tmp/CA.crt
/opt/hp/propel-install/ssl-tmp/<FQDN>/out/propel_host.crt
```

You should see the following message:

```
/opt/hp/propel-install/ssl-tmp/<FQDN>/out/propel_host.crt: OK
```

Do not proceed if you see any error messages, you will need to have the CA and certificate matching first. Restart the entire procedure if necessary.



12. *Create the certificate and key stores:*

```
# cd /opt/hp/propel-install
# ./propel-ssl-setup.sh finish
```

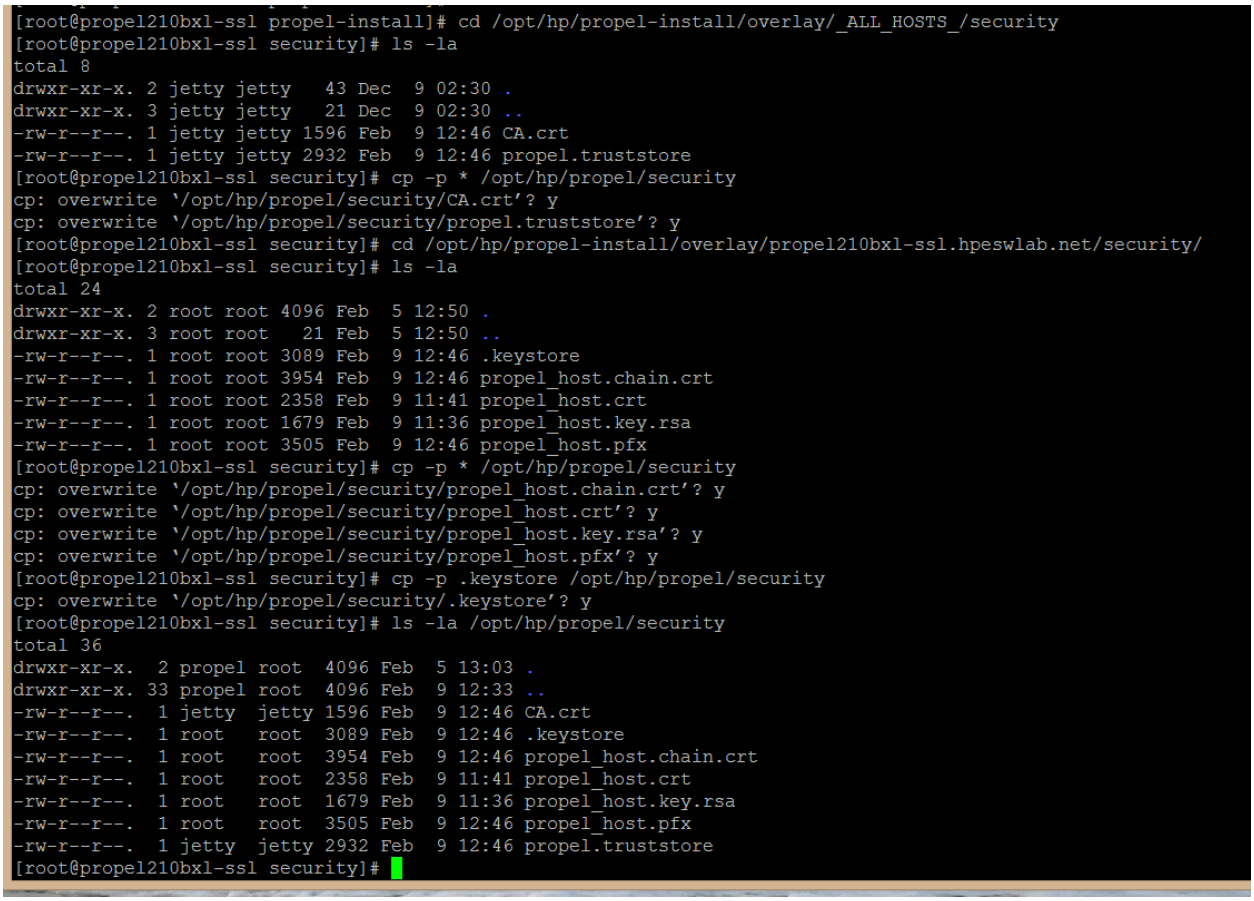
```
[root@propel210bxl-ssl propel-install]# ./propel-ssl-setup.sh finish
------ finish ------
Executing: ./propel-ssl-setup.sh finish
targetDir=overlay
addTrustedKey: Removing alias 'CA' from the truststore
keytool error: java.lang.Exception: Keystore file does not exist: /opt/hp/propel-install/ssl-tmp/propel.truststore
addTrustedKey: Importing '/opt/hp/propel-install/ssl-tmp/CA.crt' into truststore as 'CA'
Certificate was added to keystore
generateKeystore: *** generating keypair in p12 ***
generateKeystore: *** generating keystore ***

Keystore generated to '/opt/hp/propel-install/ssl-tmp/propel210bxl-ssl.hpeswlab.net/out/.keystore'
addTrustedKey: Removing alias 'propel210bxl-ssl.hpeswlab.net' from the truststore
keytool error: java.lang.Exception: Alias <propel210bxl-ssl.hpeswlab.net> does not exist
addTrustedKey: Importing '/opt/hp/propel-install/ssl-tmp/propel210bxl-ssl.hpeswlab.net/out/propel_host.crt' into trust
ropel210bxl-ssl.hpeswlab.net'
Certificate was added to keystore
targetDirAbs=/opt/hp/propel-install/overlay
Security files created in directories '/opt/hp/propel-install/overlay/*/security/'
------ finish exits with 0 ------
[root@propel210bxl-ssl propel-install]#
```

```
[root@propel210bxl-ssl propel-install]# ls -la /opt/hp/propel-install/overlay/*/security/
/opt/hp/propel-install/overlay/_ALL_HOSTS_/security/:
total 8
drwxr-xr-x. 2 jetty jetty   43 Dec  9 02:30 .
drwxr-xr-x. 3 jetty jetty   21 Dec  9 02:30 ..
-rw-r--r--. 1 jetty jetty 1596 Feb  9 12:46 CA.crt
-rw-r--r--. 1 jetty jetty 2932 Feb  9 12:46 propel.truststore

/opt/hp/propel-install/overlay/${hostname}/security/:
total 24
drwxr-xr-x. 2 jetty jetty 4096 Dec  9 02:30 .
drwxr-xr-x. 3 jetty jetty   21 Dec  9 02:30 ..
-rw-r--r--. 1 jetty jetty 2141 Dec  9 02:30 .keystore
-rw-r--r--. 1 jetty jetty 2433 Dec  9 02:30 propel_host.chain.crt
-rw-r--r--. 1 jetty jetty 1099 Dec  9 02:30 propel_host.crt
-rw-r--r--. 1 jetty jetty 1679 Dec  9 02:30 propel_host.key.rsa
-rw-r--r--. 1 jetty jetty 2500 Dec  9 02:30 propel_host.pfx

/opt/hp/propel-install/overlay/propel210bxl-ssl.hpeswlab.net/security/:
total 24
drwxr-xr-x. 2 root root 4096 Feb  5 12:50 .
drwxr-xr-x. 3 root root   21 Feb  5 12:50 ..
-rw-r--r--. 1 root root 3089 Feb  9 12:46 .keystore
-rw-r--r--. 1 root root 3954 Feb  9 12:46 propel_host.chain.crt
-rw-r--r--. 1 root root 2358 Feb  9 11:41 propel_host.crt
-rw-r--r--. 1 root root 1679 Feb  9 11:36 propel_host.key.rsa
-rw-r--r--. 1 root root 3505 Feb  9 12:46 propel_host.pfx
[root@propel210bxl-ssl propel-install]#
```

13. *Move all the created files into their final locations:*

```
# cd /opt/hp/propel-install/overlay/_ALL_HOSTS_/security
# yes|cp -p * /opt/hp/propel/security

# cd /opt/hp/propel-install/overlay/<FQDN>/security
# yes|cp -p * /opt/hp/propel/security
# yes|cp -p .keystore /opt/hp/propel/security
```

example:



*Note: the **yes|** in front of the cp commands allow to automatically sent a y when asked if you want to overwrite the existing files*

Update Propel in case you have a certificate with wildcard

To get a wildcard certificate to work (f.i. CN=.hpe.com) the below action has to be done:.*

Switch off strictSSL in all the app.json config files:

```
# cd /opt/hp/propel
# sed -i -e 's!"strictSSL": true!"strictSSL": false!' $(find . -print |grep app.json)
```

Note: HPE doesn't recommend to switch off StrictSSL and encourages to request certificates with valid Common Names.

HP Operations Orchestration

HP Operations Orchestration (HP OO) needs to be updated. (Page 12 propel 2.10 Admin guide, point 13).

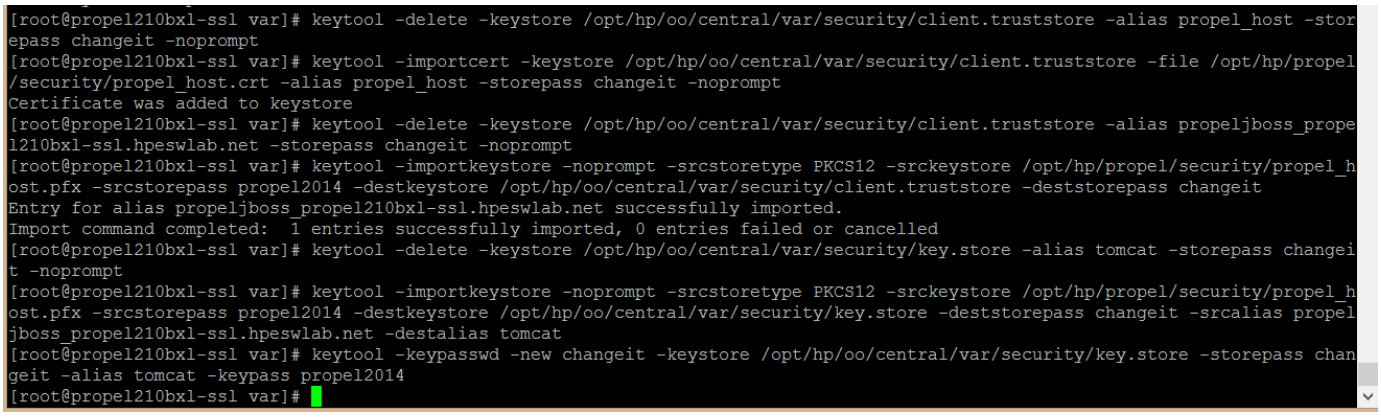
14. *Backup the existing configuration:*

```
# cd /opt/hp/oo/central/var/
# cp -rp security security.backup
```

15. *Manually delete the old certificates from the OO stores and install the new certificates:*

```
# keytool -delete -keystore /opt/hp/oo/central/var/security/client.truststore -
alias propel_host -storepass changeit -noprompt

# keytool -importcert -keystore /opt/hp/oo/central/var/security/client.truststore -
file /opt/hp/propel/security/propel_host.crt -alias propel_host -storepass changeit
-noprompt

# keytool -delete -keystore /opt/hp/oo/central/var/security/client.truststore -
alias propeljboss_<FQDN> -storepass changeit -noprompt

# keytool -importkeystore -noprompt -srcstoretype PKCS12 -srckeystore
/opt/hp/propel/security/propel_host.pfx -srcstorepass propel2014 -destkeystore
/opt/hp/oo/central/var/security/client.truststore -deststorepass changeit

# keytool -delete -keystore /opt/hp/oo/central/var/security/key.store -alias tomcat
-storepass changeit -noprompt

# keytool -importkeystore -noprompt -srcstoretype PKCS12 -srckeystore
/opt/hp/propel/security/propel_host.pfx -srcstorepass propel2014 -destkeystore
/opt/hp/oo/central/var/security/key.store -deststorepass changeit -srcalias
propeljboss_<FQDN> -destalias tomcat

# keytool -keypasswd -new changeit -keystore
/opt/hp/oo/central/var/security/key.store -storepass changeit -alias tomcat -
keypass propel2014
```

Example:



16. *Restart OO*

```
# systemctl restart central
```

Propel (2.10)

RabbitMQ

Error

Rabbit MQ logs in /var/log/rabbitmq might show:

```
=ERROR REPORT==== 9-Feb-2016::14:52:07 ===
Error on AMQP connection <0.20931.1>:
{ssl_upgrade_error,{tls_alert,"certificate unknown"}}

=ERROR REPORT==== 9-Feb-2016::14:57:01 ===
SSL: certify: tls_connection.erl:375:Fatal error: certificate unknown
```

Solution

Update /etc/rabbitmq/rabbitmq.config. The cacertfile should point to CA.crt instead of propel_host.crt.

```
# vi /etc/rabbitmq/rabbitmq.config
```

After the modifications are done, restart RabbitMQ:

```
# systemctl stop rabbitmq-server

# rm -rf /var/log/rabbitmq/*

# systemctl start rabbitmq-server
```

Check if there're any errors in /var/log/rabbitmq/rabbit@<your Propel short hostname>.log

Exchange again SSL certs between Propel and fulfillment systems

Re-Import the Propel CA and host certificate in the backend systems. Import the backend systems certificates again in the Propel truststore.

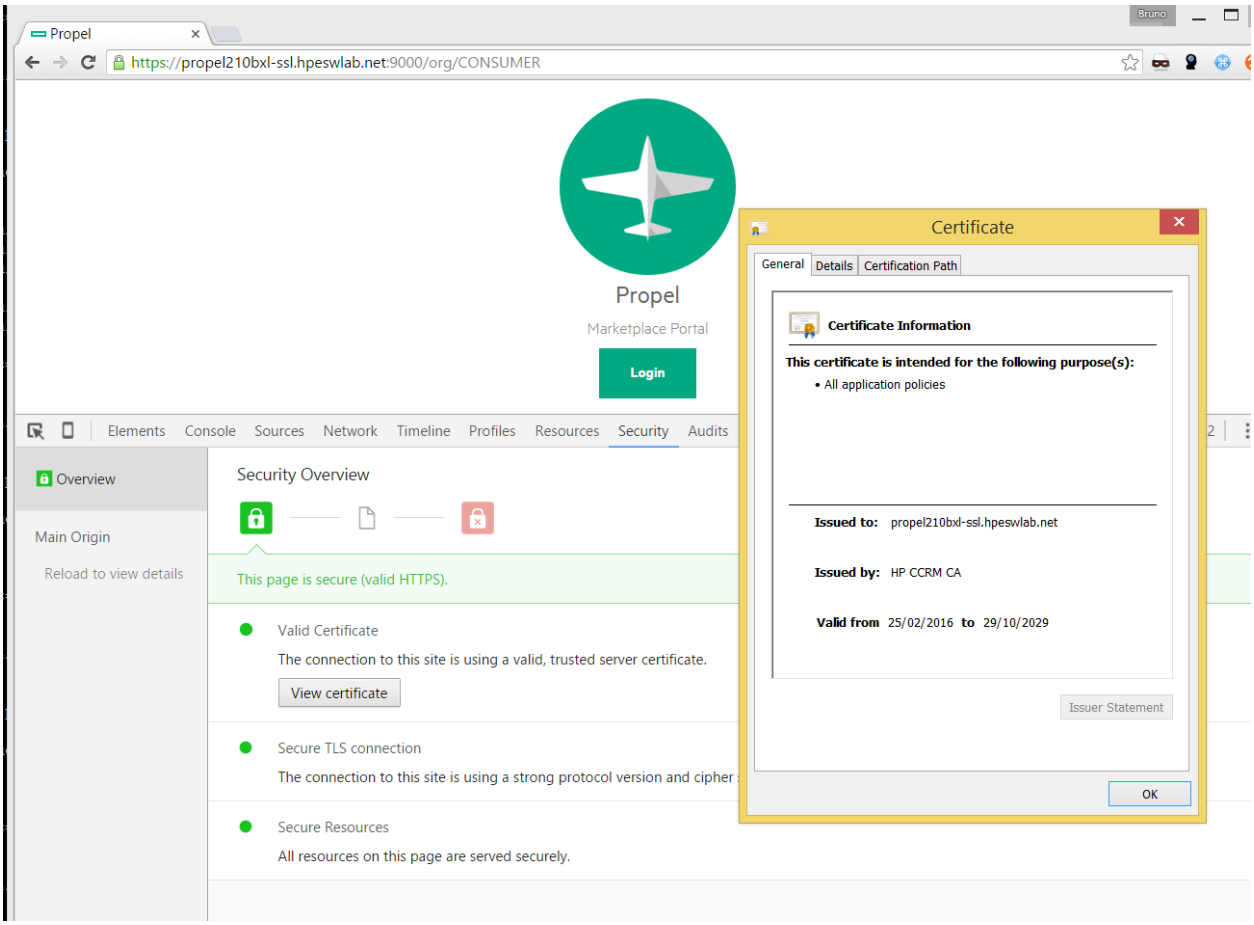
Restart Propel and Testing

Restart Propel (+ cleanup PID and log files):

```
# propel stop

# yes | rm -f /var/run/propel/*.pid

# yes | rm -rf /var/log/propel/*/*.*

# propel start
```

Ensure that you can login to the Propel Market Place Portal and use all functionalit in the UI as well interact with the fulfillment systems.

Check the new certificate:


Propel
https://propel210bxl-ssl.hpeswlab.net:9000/org/CONSUMER
Propel
Marketplace Portal
Login
Elements
Console
Sources
Network
Timeline
Profiles
Resources
Security
Audits
Overview
Main Origin
Reload to view details
Security Overview
This page is secure (valid HTTPS).
Valid Certificate
The connection to this site is using a valid, trusted server certificate.
View certificate
Secure TLS connection
Secure Resources
All resources on this page are served securely.
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All application policies
Issued to: propel210bxl-ssl.hpeswlab.net
Issued by: HP CCRM CA
Valid from 25/02/2016 to 29/10/2029
Issuer Statement
OK

Appendix

CA creation example

Windows command to create a self signed CA, used in this example setup. Download the latest OpenSSL binaries to run these commands and modify openssl.conf to your wishes.

Commands example:

```
openssl genrsa -des3 -out cakey.pem 2048
openssl req -new -x509 -days 5000 -key cakey.pem -out cacert.pem -config .\openssl.conf
openssl x509 -in cacert.pem -text -noout
copy cacert.pem cacert.crt
```

Sign Propel CSR with CA example

CMD-file:

```
rem
echo off

set JAVA_HOME=C:\PROGRA~2\HP\SERVIC~1.40\Server\RUN\jre
rem set JAVA_HOME=C:\PROGRA~2\Java\jre1.8.0_60

if not "%JAVA_HOME%" == "" goto gotJAVAHome
echo JAVA_HOME environment variable is not set!
exit /b 1

:gotJAVAHome


if not exist "%JAVA_HOME%\bin\keytool.exe" goto noKeyTool


rem prompt the user for the hostname of the server

echo .

set /p propelserverhost=Please enter the FQDN (Fully Qualified Domain Name) of the Propel server
host:
rem Assuming the CSR is called: propel_host-<Propel FQDN>.key.csr

echo .

echo "Now have the private CA issue a signed Propel certificate"

echo .
echo "The Propel server certificate will be written to propel_host-%propelserverhost%.cert.pem and
signed by the CA"
echo "When asked for a CA password: HPitsm_9"
echo .
set /p foobar=Press enter to continue
rem example: propel_host-propel210bxl-ssl.hpeswlab.net.key.csr
bin\openssl x509 -days 4995 -req -in propel_host-%propelserverhost%.key.csr -CA cacert.pem -CAkey
cakey.pem -CAcreateserial -out propel_host-%propelserverhost%.cert.pem
copy propel_host-%propelserverhost%.cert.pem propel_host-%propelserverhost%.crt

if not exist "%CD%\propel_host-%propelserverhost%.cert.pem" goto noCert
```

```
goto end

:noKeyTool

echo Can't find %JAVA_HOME%\bin\keytool.exe!
exit /b 1

:noCert

echo Something went wrong with certificate creation!
exit /b 1

:end
```

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hp.com/

This web site provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- *Search for knowledge documents of interest*
- *Submit and track support cases and enhancement requests*
- *Download software patches*
- *Manage support contracts*
- *Look up HPE support contacts*
- *Review information about available services*
- *Enter into discussions with other software customers*
- *Research and register for software training*

To learn more about using the customer support site, go to:
https://softwaresupport.hp.com/documents/10180/14684/HP_Software_Customer_Support_Handbook/

Most support areas require that you register and sign in as an HP Passport user. Many also require an active support contract. To find more information about support access levels, go to the following URL:
http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to the following URL:
http://h20229.www2.hp.com/passport-registration.html

Learn more at

hpe.com/software/propel

Sign up for updates

December 2015

Hewlett Packard Enterprise