How to install a signed certificate in Singlewire Applications

Each Singlewire application (InformaCast, LPI, CallAware) has a separate place to store certificates, called a keystore. Each keystore should be handled individually. So, perform these steps for each application keystore.

* InformaCast web certificate keystore location: /usr/local/singlewire/InformaCast/certs
* LPI web certificate keystore location: /usr/local/singlewire/LPI/certs
* CallAware web certificate keystore location: /usr/local/singlewire/CallAware/certs
* Inbound CAP plugin certificate store location: /usr/local/singlewire/InformaCast/web/WEB-INF/plugins/com.singlewire.plugin.icap/plugin/classes

There are other keystores within Singlewire applications used for other purposes. Do not manipulate these.

1. Stop the service in question through webmin (https://x.x.x.x:10000). Do not modify the keystore with the application running.

2. InformaCast generates a self signed certificate that is incompatible with signing authorities. You must first rename the file with the original certificate in it. ssh to the EX/VA server as admin. Substitute one of the above paths for KEYSTORELOCATION.

```
$ cd KEYSTORELOCATION ; mv .keystore .keystore-original
```

3. Generate a new root certificate on the InformaCast host. Make sure to use actual values appropriate for your organization. Consult your SSL provider's website on optimal values here.

The password to use should be "changeMe" (case significant, no quotes). The keystore password must match what is configured in server.xml, and changeMe is the default configuration in server.xml. If the password does not match, the application will not start. All applications use the same default keystore password. Substitute InformaCast, LPI or CallAware for APP below.

```
$ cd /usr/local/singlewire/APP
$ `find ../.. -name keytool | head -1` -genkey -alias tomcat -keyalg RSA -keystore
```

KEYSTORELOCATION/.keystore
 Enter keystore password:
 Re-enter new password:
 What is your first and last name?
   [Unknown]: informacast.singlewire.com
 What is the name of your organizational unit?
  [Unknown]: IT
 What is the name of your organization?
  [Unknown]: Singlewire Software, LLC
 What is the name of your City or Locality?
  [Unknown]: Madison
 What is the name of your State or Province?
  [Unknown]: WI
 What is the two-letter country code for this unit?
  [Unknown]: US
 Is CN=informacast.singlewire.com, OU=IT, O="Singlewire Software, LLC", L=Madison
 , ST=WI, C=US correct?
   [no]: yes

 Enter key password for <tomcat>
        (RETURN if same as keystore password):

Make sure to press return when prompted to use the same as the keystore password, or InformaCast will not start.

4. Generate the CSR (certificate sign request) to send to your SSL provider. Use the changeMe keystore password.

 $ `find ../.. -name keytool | head -1` -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore /usr/local/singlewire/InformaCast/certs/.keystore
 Enter keystore password:

5. PROCESS certreq.csr WITH YOUR SSL PROVIDER. Your SSL provider will need to return the certificate in PEM format (Base64 text).

6. Install new root certificate (may not be necessary). If your root CA is not trusted, you must install its certificate in the trust store. Download the root certificate in a form compatible with tomcat. Example:

-----BEGIN CERTIFICATE-----
MIIEVzCCAz+gAwIBAgIQFoFkpCjKEt+rEvGfsbk1VDANBgkqhkiG9w0BAQUFADCB
jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL

EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xMjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgUm9vdCBDQSAtIEcyMB4X
DTA5MDQwMTAwMDAwMFoXDTI5MDMzMTIzNTk1OVowgYwxCzAJBgNVBAYTAlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3QgUHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMTIwMAYDVQQDEylWZXJpU2lnbiBUcmlh
bCBTZWN1cmUgU2VydmVyIFJvb3QgQ0EgLSBHMjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMCJggWnSVAcIomnvCFhXlCdgafCKCDxVSNQY2jhYGZXcZsq
ToJmDQ7b9JO39VCPnXELOENP2+4FNCUQnzarLfghsJ8kQ9pxjRTfcMp0bsH+Gk/1
qLDgvf9WuiBa5SM/jXNvroEQZwPuMZg4r2E2k0412VTq9CoIODYNDZw3ziiYdSjV
fY3VfbsLSXJIh2jaJC5kVRsUsx72s4/wgGXbb+P/XKr15nMIB0yH9A5tiCCXQ5nO
EV7/ddZqmL3zdeAtyGmijOxjwiy+GS6xr7KACfbPEJYZYaS/P0wctIOyQy6CkNKL
o5vDDkOZks0zjf6RAzNXZndvsXEJpQe5WO1avm8CAwEAAaOBsjCBrzAPBgNVHRMB
Af8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjBtBggrBgEFBQcBDARhMF+hXaBbMFkw
VzBVFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBSP5dMahqyNjmvDz4Bq1EgYLHsZ
LjAlFiNodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvLmdpZjAdBgNVHQ4E
FgQUSBnnkm+SnTRjmcDwmcjWpYyMf2UwDQYJKoZIhvcNAQEFBQADggEBADuswa8C
0hunHp17KJQ0WwNRQCp8f/u4L8Hz/TiGfybnaMXgn0sKI8Xe79iGE91M7vrzh0Gt
ap0GLShkiqHGsHkIxBcVMFbEQ1VS63XhTeg36cWQ1EjOHmu+8tQe0oZuwFsYYdfs
n4EZcpspiep9LFc/hu4FE8SsY6MiasHR2Ay97UsC9A3S7ZaoHfdwyhtcINXCu2IX
W0Gpi3vzWRvwqgua6dm2WVKJfvPfmS1mAP0YmTcIwjdiNXiU6sSsJEoNITR9zCoo
4oKQ8wVoWZpbuPZb5geszhS7YsABUPIAAfF1YQCiMULtpa6HFzzm7sdf72N3HfwE
aQNg95KnKGrrDUI=
-----END CERTIFICATE-----

Here is one way of importing the new root certificate:

```
$ `find .. -name keytool | head -1` -keystore .keystore -import -alias cacert -file root.crt
Enter keystore password:
Owner: CN=VeriSign Trial Secure Server Root CA - G2, OU="For Test Purposes Only.
  No assurances.", O="VeriSign, Inc.", C=US
Issuer: CN=VeriSign Trial Secure Server Root CA - G2, OU="For Test Purposes Only
.  No assurances.", O="VeriSign, Inc.", C=US
Serial number: 168164a428ca12dfab12f19fb1b93554
Valid from: Tue Mar 31 19:00:00 CDT 2009 until: Sat Mar 31 18:59:59 CDT 2029
Certificate fingerprints:
        MD5:  E0:19:F5:FC:C0:9A:13:0E:38:B7:BF:0D:02:40:D3:C2
        SHA1: 51:51:B8:63:8A:4C:1F:15:54:56:ED:37:C9:10:35:CA:D3:01:B9:36
        Signature algorithm name: SHA1withRSA
        Version: 3

Extensions:

#1: ObjectId: 2.5.29.15 Criticality=true
```

```
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 48 19 E7 92 6F 92 9D 34   63 99 C0 F0 99 C8 D6 A5  H...o..4c.......
0010: 8C 8C 7F 65                                        ...e
]
]

#4: ObjectId: 1.3.6.1.5.5.7.1.12 Criticality=false

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

7. If your CA requires an intermediate SSL certificate, you will need to download and install it. Download the certificate in a format compatible with tomcat or apache. Once you have the certificate saved in a file called primary_inter.cer, use this process to install it:

```
$ `find .. -name keytool | head -1` -import - trustcacerts -alias primaryIntermediate -keystore .keystore -file primary_inter.cer
```

8. To install the signed certificate from your provider, you will need to download and install it. Download the certificate in a format compatible with tomcat or apache. Once you have the certificate saved in a file called finalcert.crt, use this process to install it:

```
$ `find .. -name keytool | head -1` -import -keystore .keystore -import -alias tomcat -file finalcert.crt
Enter keystore password:
Certificate reply was installed in keystore
```

9. Restart the app. Browsers should now receive the trusted certificate.

Complete log of a session performing these steps for InformaCast:

```
admin@singlewire:/usr/local/singlewire/InformaCast/certs$ cd
/usr/local/singlewire/InformaCast/certs ; mv .keystore .keystore-original

admin@singlewire:/usr/local/singlewire/InformaCast$ `find .. -name keytool | head -1` -genkey
-alias tomcat -keyalg RSA  -keysize 2048 -keystore
/usr/local/singlewire/InformaCast/certs/.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  jsdev.singlewire.lan
What is the name of your organizational unit?
  [Unknown]:  IT
What is the name of your organization?
  [Unknown]:  Singlewire Software, LLC
What is the name of your City or Locality?
  [Unknown]:  Madison
What is the name of your State or Province?
  [Unknown]:  WI
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=jsdev.singlewire.lan, OU=IT, O="Singlewire Software, LLC", L=Madison, ST=WI, C=US
correct?
  [no]:  yes

Enter key password for <tomcat>
        (RETURN if same as keystore password):

admin@singlewire:/usr/local/singlewire/InformaCast$ `find .. -name keytool | head -1` -certreq
-keyalg RSA -alias tomcat -file certreq.csr -keystore
/usr/local/singlewire/InformaCast/certs/.keystore
Enter keystore password:

admin@singlewire:/usr/local/singlewire/InformaCast$ cat certreq.csr

# Add the root CA certificate

admin@singlewire:/usr/local/singlewire/InformaCast$ `find .. -name keytool | head -1` -keystore
.keystore -import -alias cacert -file ~/SinglewireRootCA.pem
Enter keystore password:
```

```
Re-enter new password:
Owner: CN=SinglewireRootCA, C=US, ST=Wisconsin, L=Madison, O=SinglewireSoftwareLLC
Issuer: CN=SinglewireRootCA, C=US, ST=Wisconsin, L=Madison, O=SinglewireSoftwareLLC
Serial number: 7c77c6fbd5f8dd874f57619353b7909d
Valid from: Wed Oct 03 14:48:16 CDT 2012 until: Mon Oct 03 14:58:12 CDT 2022
Certificate fingerprints:
         MD5:  4B:F4:3E:41:26:E5:BF:33:BA:48:7D:24:38:BB:D1:5E
         SHA1: 04:E3:69:6C:E6:77:9A:CF:39:91:8E:42:8F:7F:46:FF:CC:83:E2:B6
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 2E 3D 0D 5E 81 7C 88 3E   21 E8 AA 4C A7 F2 CC 6F  .=.^...>!..L...o
0010: 5B 78 6F 0F                                        [xo.
]
]

#4: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false

Trust this certificate? [no]:  yes
Certificate was added to keystore

# Add the issuing CA certificate

admin@singlewire:/usr/local/singlewire/InformaCast$ `find .. -name keytool | head -1` -keystore
.keystore -import -alias cacertintermed -file ~/singlewire-issuing-CA.pem
```

Enter keystore password:
Certificate was added to keystore

Signed certificate from certificate authority is certnew.cer

admin@singlewire:/usr/local/singlewire/InformaCast$ `find .. -name keytool | head -1` -import -keystore .keystore -import -alias tomcat -file ~/certnew.cer
Enter keystore password:
Certificate was added to keystore

How to Install a Certificate in InformaCast's Trust Store

InformaCast can access URL's that require SSL. Examples:
* LDAPs
* IMAPs
* Facebook, Twitter

Here, InformaCast is acting as a client.

Typically, these applications are secured with certificates that are already present in InformaCast's native trust store. In the case of connecting with a server that uses a self signed certificate, however, the server's certificate will need to be installed manually.

This describes the process of downloading a certificate from an Exchange server and installing it in InformaCast's trust store.

Export the cert that the server is using. You can do this directly on the OVA. Here are some examples for how to do this using different protocols:

- In this example, we will use Exchange for IMAP. The server here is qa-exchange2010.lab.lan, the port to connect on is 143. We download the cert to imap-cert.txt in support's home directory.

  root@singlewire:~#echo -n | openssl s_client -connect qa-exchange2010.lab.lan:143 -starttls imap | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > imap-cert.txt
- In this example, we will use Exchange for SMTP. The server here is qa-exchange2010.lab.lan, the port to connect on is 25. We download the cert to smtp-cert.txt in support's home directory.

  root@singlewire:~#echo -n | openssl s_client -connect qa-exchange2010.lab.lan:25 -starttls smtp | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > smtp-cert.txt

- In this example, we will use the secure web server on google.com.

  root@singlewire:~#echo -n | openssl s_client -connect www.google.com:443 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > https-cert.txt

Confirm that you've downloaded a cert.

root@singlewire:/usr/local/singlewire/InformaCast# cat /home/support/imap-cert.txt
-----BEGIN CERTIFICATE-----
MIIDKDCCAhCgAwIBAgIQHTOsSwpsfZZPknrTTXEQ8TANBgkqhkiG9w0BAQUFADAa
MRgwFgYDVQQDEw9RQS1FeGNoYW5nZTIwMTAwHhcNMTMwMzE5MTkwMTQ1WhcNMTgw
MzE5MTkwMTQ1WjAaMRgwFgYDVQQDEw9RQS1FeGNoYW5nZTIwMTAwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCyRTeC6v7kQyYH6Ht+kx1YBtdKQs5SnHiT
zNypTECi3vIwb57s51iFJPlHbXix1F5cslZ4ht98gy6N12LLX6NhJ7l/aCgsea2S
pu97cLw05USjXrtD7ztx31pke6A6Rju/SxybHBqM5d0wt8IDRFItc1X/Xa2Vduv+
98qmt+gBf7ddCdZMMqcvaGdKMP6wNn1FkXBg0iNNHkRnjumZO5lVF4XHbf+VghWj
+6qWXc7Ea0XFHClvsIl6kc79VOiq9SL3ahDhaQ8frDBZ8POnqvzPshtaFNaF18F0
q36mJsoS3tJ2vWMOFS1QhfCUw1Nzih/PyviUATu+e2BwjP2Niw/XAgMBAAGjajBo
MA4GA1UdDwEB/wQEAwIFoDAzBgNVHREELDAqgg9RQS1FeGNoYW5nZTIwMTCCF1FB
LUV4Y2hhbmdlMjAxMC5sYWIubGFuMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAwGA1Ud
EwEB/wQCMAAwDQYJKoZIhvcNAQEFBQADggEBAJimkuUrH1tOpfptgfuiuOE1xEfC
lLcv/JZaVhkFUziK/H6OV8BMAZTtlOcus2gNl4fNXkQ9h/pyeZcqFwngcr32loRB
EflJOKGOCG6d1ly8u8AvVDksvjEpWP+s7qf7ztXqJqE1GZ+kD2JhWClbpNCHc5tc
N+Wy6O7SPbL/qusrzUNBxIJWGdVIjJwKazYl24LSOA/ZgPMTYgVbTytpEQ5UXIHH
0mKIoucit8LETm3QXHc7KhE365oyLl12X2N6naTl+fkaaZwR7buqC3TLKFSrAwaC
mM4fBboh/GSTWvxRLqVTIi9r8Ze6KdXeYgw/tOCbusAWoGj6e246Bwaf8X4=
-----END CERTIFICATE-----

Import it to java's default cert store:

root@singlewire:/usr/local/singlewire/InformaCast# `find /usr/local/singlewire -name keytool | head -1` -keystore /usr/local/singlewire//java/jdk1.6.0_23/jre/lib/security/cacerts -import -file ~/imap-cert.txt -alias imapex -trustcacerts
Enter keystore password:
Owner: CN=QA-Exchange2010
Issuer: CN=QA-Exchange2010
Serial number: 1d33ac4b0a6c7d964f927ad34d7110f1
Valid from: Tue Mar 19 14:01:45 CDT 2013 until: Mon Mar 19 14:01:45 CDT 2018
Certificate fingerprints:
	MD5: 5A:CF:1E:BE:63:E0:F8:B9:2C:BA:4E:82:09:A2:57:39
	SHA1: 60:25:9F:D7:A7:0E:15:61:DC:D9:5B:2F:59:7C:CF:D5:51:2D:4E:25
	Signature algorithm name: SHA1withRSA
	Version: 3

Extensions:

#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#3: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
]

#4: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: QA-Exchange2010
  DNSName: QA-Exchange2010.lab.lan
]

Trust this certificate? [no]: yes
Certificate was added to keystore

Restart InformaCast:

root@singlewire:/usr/local/singlewire/InformaCast# /etc/init.d/singlewireInformaCast restart
Restarting InformaCast: singlewireInformaCast.

Your certificate is now trusted.