Replacing default self-signed PM certificate with trusted CA created certificate

Background

Policy Manager uses self-signed certificate used for establishing HTTPS connection between Server with Console and Web Reporting. As certificate is self-signed and thus cannot be validated, web browsers will complain with warning messages about it. For customers having their own company trusted certificates it is possible to replace the default one coming with Policy Manager with there own.

On Windows PMS keystore is located inside "C:\Program Files (x86)\F-Secure\Management Server 5\config\fspms.jks" since version 12.10 (for PMS 12.00 file name is fspms.keystore). For versions before 12 keystore is located inside "C:\Program Files (x86)\F-Secure\Management Server 5\jetty\fspms.keystore".

On Linux PMS 12.10 keystore is located inside "/opt/f-secure/fspms/config/fspms.jks".

Use the following command to query details about certificates stored inside:

```
"C:\Program Files (x86)\F-Secure\Management Server 5\jre\bin\keytool"
-list -v -keystore fspms.jks -storepass superPASSWORD

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: fspms
Creation date: 20.09.2010
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=f-secure.com, OU=f-secure.com, O=f-secure.com, C=EN
Issuer: CN=f-secure.com, OU=f-secure.com, O=f-secure.com, C=EN
Serial number: 4c977fcc
Valid from: Mon Sep 20 18:37:48 EEST 2010 until: Wed Aug 27 18:37:48 EEST 2110
Certificate fingerprints:
MD5: 00:2D:4E:23:3A:9C:68:22:CD:CE:72:43:2B:CC:98:00
SHA1: 7C:F7:E1:2D:2E:6C:0A:86:66:53:E2:C7:59:2C:F2:9E:89:B6:4F:BD
SHA256: 02:87:BD:AF:BB:2B:F2:BB:13:A5:96:A8:F1:5D:DC:5C:67:AB:77:68:AF:36:85:1F:F2:F7:DE:29:88:AD:DF:D1
Signature algorithm name: SHA1withDSA
Version: 3
```

Replacing default certificate

Assume that you have your signed (may be self-signed) certificate and private key for it inside PKCS12 keystore. It is protected with password "srcpassword" and your certificate and private key is referenced by name (alias) "server". Keystore file is "server.p12" and it is located in the same directory as "fspms.jks".

To replace default Policy Manager certificate execute following command from directory where "fspms.jks" is located:

```
"C:\Program Files (x86)\F-Secure\Management Server 5\jre\bin\keytool" -importkeystore
-destkeystore fspms.jks -deststorepass superPASSWORD -destalias fspms -destkeypass superPASSWORD
-srckeystore server.p12 -srcstoretype PKCS12 -srcstorepass srcpassword -srcalias server
```

You are replacing certificate in "fspms.jks" so following message will appear:

```
Existing entry alias server exists, overwrite? [no]:
```

Type "yes" and hit enter. Restart Policy Manager server to start using new certificate.

ATTENTION: when you execute importkeystore command pay attention on "-destkeypass", it should be same as "-deststorepass". If you forget to insert proper "-destkeypass" command can complete successfully but problems on Policy Manager server startup may occur.