Configuring Password Manager Pro to Run in FIPS 140-2 Compliant Mode

(Procedure applicable only for builds 7002 and later)

Overview

Password Manager Pro can be configured to run in Federal Information Processing Standard (FIPS) 140-2 compliant mode. This document provides the step-by-step procedure to configure FIPS 140-2 compliant mode.

By, 'FIPS 140-2-compliant mode', we mean that all encryption in Password Manager Pro (PMP) is done through FIPS 140-2 certified systems and libraries.

Step-by-Step Procedure

The following steps are for configuring PMP Windows build (with a self-signed certificate and MS SQL Server as backend database) in FIPS mode.

Pre-requisite

Before configuring PMP to run in FIPS mode, the machine where MS SQL server is running should be configured to run in FIPS mode. Follow the procedure explained in this knowledge base article on Microsoft site:

http://support.microsoft.com/kb/920995

Step 1

- Navigate to **<PMP-Installation-Folder>\fips** directory and copy the nss-3.12.4 folder files and put it under a specific folder, say for example C:\fips\windows

- Create two new folders named **lib** and **cert** in **C:\fips\windows**

Step 2

- Copy the files present in **<PMP-Installation-Folder>\fips \nss-3.12.4\lib** folder and paste them in **C:\fips\windows\lib folder**

- Now, from **<PMP-Installation-Folder>\fips \nss-3.12.4\lib folder**, copy the following **.dll** and **.chk** files and paste them in **C:\windows\system32** or **C:\Windows\SysWow64**

  freebl3.chk,freebl3.dll,libnspr4.dll,libplc4.dll,libplds4.dll,nss3.dll,nssckbi.dll,nssdbm3 .chk,nssdbm3.dll,nssutil3.dll,smime3.dll,softokn3.chk,softokn3.dll,sqlite3.dll,ssl3.dll

Step 3

- Open a command-line interface and navigate to **C:\fips\windows\nss-3.12.4\bin** and execute the command:

  certutil -N -d C:\fips\windows\cert

  (This command will create a database in the cert directory. The password used here should be entered in the **<PMP-Installation-Folder>\conf\server.xml)**

- Execute the command:

  modutil -fips true -dbdir C:\fips\windows\cert
  (This command will enable FIPS mode to certificate database)

Step 4 - To create self-signed certificate

- Create a new text file inside c:\fips\windows and name it as pwd.txt and add a password in it which is used by the certificate.

- Create self-signed certificate by executing the command:

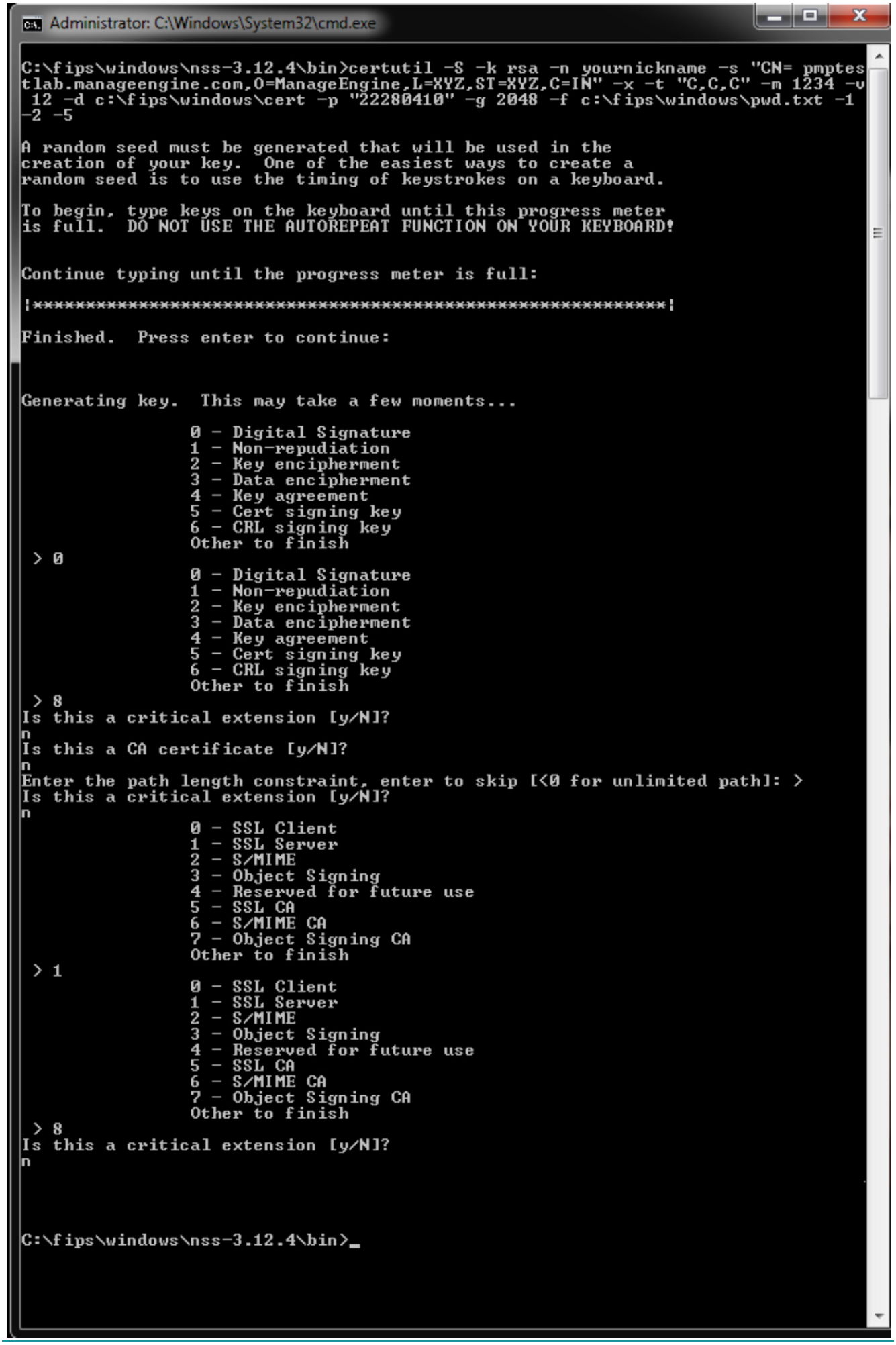
certutil -S -k rsa -n yournickname -s "CN= pmptestlab.manageengine.com,O=ManageEngine,L=XYZ,ST= XYZ,C=IN" -x -t "C,C,C" -m 1234 -v 12 -d C:\fips\windows\cert -p "22280410" –g 2048 -f C:\fips\windows\pwd.txt -1 -2 -5

Replace the values for the parameters shown in green as described below. That means, you will have to replace the example entries shown in red with the required information related to your organization.

-n	Enter host name of the server
CN	Enter the FQDN of the host replacing the example entry
O	Enter organization name
L	Enter location or city
ST	Enter state name
C	Enter country name
-p	Enter organization phone number

For more details, refer to the certutil knowledge base article: https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/tools/NSS_Tools_certutil

You need to change the CN name based on the host name and also create a pwd.txt file, where your cert database password should be present. Refer to the screenshot below:


Administrator: C:\Windows\System32\cmd.exe
C:\fips\windows\nss-3.12.4\bin>certutil -S -k rsa -n yournickname -s "CN= pmptestlab.manageengine.com,O=ManageEngine,L=XYZ,ST=XYZ,C=IN" -x -t "C,C,C" -m 1234 -v 12 -d c:\fips\windows\cert -p "22280410" -g 2048 -f c:\fips\windows\pwd.txt -1 -2 -5
A random seed must be generated that will be used in the creation of your key. One of the easiest ways to create a random seed is to use the timing of keystrokes on a keyboard.
To begin, type keys on the keyboard until this progress meter is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!
Continue typing until the progress meter is full:
Finished. Press enter to continue:
Generating key. This may take a few moments...
0 - Digital Signature
1 - Non-repudiation
2 - Key encipherment
3 - Data encipherment
4 - Key agreement
5 - Cert signing key
6 - CRL signing key
Other to finish
> 0
0 - Digital Signature
1 - Non-repudiation
2 - Key encipherment
3 - Data encipherment
4 - Key agreement
5 - Cert signing key
6 - CRL signing key
Other to finish
> 8
Is this a critical extension [y/N]?
n
Is this a CA certificate [y/N]?
n
Enter the path length constraint, enter to skip [<0 for unlimited path]: >
Is this a critical extension [y/N]?
n
0 - SSL Client
1 - SSL Server
2 - S/MIME
3 - Object Signing
4 - Reserved for future use
5 - SSL CA
6 - S/MIME CA
7 - Object Signing CA
Other to finish
> 1
0 - SSL Client
1 - SSL Server
2 - S/MIME
3 - Object Signing
4 - Reserved for future use
5 - SSL CA
6 - S/MIME CA
7 - Object Signing CA
Other to finish
> 8
Is this a critical extension [y/N]?
n
C:\fips\windows\nss-3.12.4\bin>

- To list the certificate of alias/nickname, execute the command:

  certutil -L -n yournickname -d C:\fips\windows\cert
  (This will list the certificate of alias/nickname)

Step 4.1 - To import signed certificate into FIPS DB

- To import signed certificate into FIPS DB, execute the command:

  certutil.exe -A -n "pmpca1" -t ",," -i C:\fips\windows\pmp-2k8-latest-with-key.cer -d c:\fips\windows\cert

- To list the certificate of alias/nickname, execute the command:

  certutil.exe -L -n pmpca1 -d C:\fips\windows\cert
  (This will list the certificate of alias/nickname)

Step 5

- Create a new file named **nss.cfg** file under **C:\fips\windows\cert** and add the below contents
  - nssLibraryDirectory=C:\fips\windows\lib
  - nssSecmodDirectory=C:\fips\windows\cert
  - nssDbMode=readWrite
  - nssModule=fips

Step 6

Carry out of the following steps for SQL Server Setup

- Create a certificate for SQL Server using certutil command as explained in Step 4 above and add the certificate in the NSS CertDB. **CN name should be FQDN of the server where SQL Server is running**

- Export the SQL Server certificate from the NSS Cert DB using the command below

  pk12util.exe -d c:\fips\windows\cert -n PMPSQLSERVER -o c:\fips\windows\name.fqdn.p12

- Import the .p12 file in 'Personal and trusted stores' by selecting Windows Local Computer & Local User Store. (Use MMC->Certificate)

- Export the certificate alone from the personal store (**name**.fqdn.cer -DER Format)

Step 7

Configure Service Broker Endpoint in SQL server:

- CREATE ENDPOINT BrokerEndpoint
  STATE=STARTED
  AS TCP (LISTENER_PORT=9999)
  FOR SERVICE_BROKER
  (AUTHENTICATION=WINDOWS, ENCRYPTION=REQUIRED ALGORITHM AES)

  Note: TCP LISTENER_PORT 9999 is configurable.

- To enable the service broker query:
  ALTER DATABASE [msdb] SET ENABLE_BROKER;

- Service Broker transport will now be running in FIPS compliance mode.

- Open SQL Server configuration manager, select the imported certificate and restart the SQL Server. In the SQL logs, you will find this trace: **"Service Broker transport is running in FIPS compliance mode."**

For more details, refer to the SQL Server knowledge base article:
http://www.sqlservercentral.com/Forums/Topic446704-359- 1.aspx#bm483639

Step 8

- Navigate to **<PMP-Installation-Folder>\fips\jre\lib\security folder** and copy the **java.security** file and paste it under **<PMPInstallation-Folder>\jre\lib\security** folder. This will overwrite the java.security file.

- Now, open the **<PMP-Installation-Folder>\jre\lib\security\java.security** folder. Look for the following line:
  security.provider.1=sun.security.pkcs11.SunPKCS11 C:\\fips1\\windows\\cert\\nss.cfg

- Replace the above line with the following:
  security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSSFIPS

Step 9

- Import the name.fqdn.cer into the cacerts of the PMP build using the command **importCert.bat name.fqdn.cer**

- Now, go to **<PMP-Installation-Folder>/bin/ChangeDB.bat.**
  Open the file and look for the entry
  -Dswing.aatext=true

- Replace the above line with the following entries:
  -Dswing.aatext=true -Djavax.net.ssl.keyStoreType=”PKCS11” -Djavax.net.ssl.keyStoreProvider=SunPKCS11-NSSFIPS -Djavax.net.ssl.keyStore=NONE -Djavax.net.ssl.keyStorePassword=passtrix Djavax.net.ssl.keyStoreProvider=SunPKCS11-NSSFIPS

Step 10

- Add the below system properties in the **<PMP-Installation-Folder>/conf/wrapper.conf**

  wrapper.java.additional.21=-Djavax.net.ssl.keyStoreType=PKCS11
  wrapper.java.additional.22=-
  Djavax.net.ssl.keyStoreProvider=SunPKCS11-NSSFIPS
  wrapper.java.additional.23=-Djavax.net.ssl.keyStore=NONE
  wrapper.java.additional.24=-Djavax.net.ssl.keyStorePassword=passtrix
  wrapper.java.additional.25=-Dnet.phonefactor.pfsdk.debug=false
  wrapper.java.additional.26=-Duser.home=../logs/

Step 11

- Navigate to **<PMP-Installation-Folder>/conf/server.xml directory** and carry out the following changes:

  - Search for 7272 connector and remove the line keystoreFile=**"conf/server.keystore"**
  - Instead, add the line **keystoreType="pkcs11"**
  - Remove the line **truststoreFile="jre/lib/security/cacerts" truststorePass="changeit" truststoreType="JKS"**
  - If your certificate database password is different from passtrix, edit the attribute and enter the new password **keystorePass="passtrix"**

Now repeat the above steps searching for 7070 as explained below:

- Search for 7070 connector and remove the line **keystoreFile="conf/server.keystore"**
- Instead, add the line **keystoreType="pkcs11"**
- Remove the line **truststoreFile="jre/lib/security/cacerts" truststorePass="changeit" truststoreType="JKS"**
- If your certificate database password is different from passtrix, edit the attribute and enter the new password **keystorePass="passtrix"**

Step 12

- Now use **<PMP-Installation-Folder> /ChangeDB.bat** to create a new database in SQL Server
- Start PMP Server, launch web interface and check the certificate.

Troubleshooting: FIPS-compliant mode configuration issues

If you encounter problems while configuring Password Manager Pro (PMP) to run in FIPS-compliant mode, verify the files mentioned below during PMP server startup:

- **wrapper.conf**
- **java.security** file, <PMP_home>/fips folder.