CA Identity Manager 12.6.x and below
Steps to Resolve OOTB Provisioning Certificates that expired on 6th Oct,2017

Contents

Prerequisites

- **ootb_certs.zip (**Click here to download and extract the new certificates.**)**
- **Java Connector Server Password**
- **Backup following folders**
  - <DXHOME>\config\ssld
  - <Provisioning Server>\data\tls\

How to check if certs are expired

- Make sure JAVA_HOME is set

This method can be done in **3 ways**:

1) **Using the Openssl tool**
   - Run command: C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls>..\..\bin\openssl x509 -enddate -noout -in et2_cacert.pem

```
C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls>..\..\bi
n\openssl x509 -enddate -noout -in et2_cacert.pem
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
notAfter=Sep 24 04:55:38 2026 GMT
```

The above example shows that the current cert is not expired. An expired one will show:

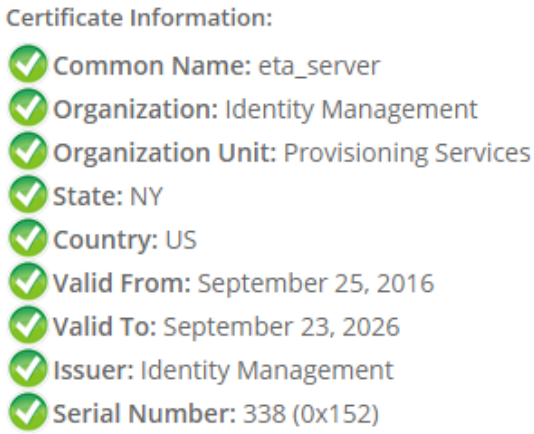
notAfter=Oct 6 08:25:50 2017 GMT -> in this example, this means certificate expired on Oct 6

2) **SSLSHOPPER Website**

This website will help verify your pem files for you:
https://www.sslshopper.com/certificate-decoder.html

An example of the .pem locations are:
/opt/CA/Directory/dxserver/config/ssld/personalities

Copy and paste the contents in there and an image like below will show you if it's verified.



3) **Using the keytool command** (Only works with Java JDK 1.7 and higher)

```
C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls>"C:\Prog
ram Files\Java\jdk1.8.0_144\bin\keytool" -printcert -file et2_cacert.pem
Owner: OU=Provisioning Services, O=Identity Management, L=Islandia, ST=NY, C=US
Issuer: OU=Provisioning Services, O=Identity Management, L=Islandia, ST=NY, C=US

Serial number: b284b8faf7e667ca
Valid from: Mon Sep 26 10:25:38 IST 2016 until: Thu Sep 24 10:25:38 IST 2026
Certificate fingerprints:
         MD5:  31:0E:E8:30:E8:59:83:78:03:D7:CE:02:83:F9:42:5B
         SHA1: 60:DA:71:80:88:1E:F8:7C:CC:5E:88:08:EA:D8:3A:79:04:30:A1:62
         SHA256: BC:A4:07:1E:EE:F6:3E:63:9C:57:B7:3C:1D:AF:D7:B5:84:CA:D4:2C:24:
10:FE:E7:B0:12:11:F6:18:7C:7D:80
         Signature algorithm name: SHA256withRSA
         Version: 3
```

Command ran:

keytool -printcert -file et2_cacert.pem

This command can be used to check all pem files.

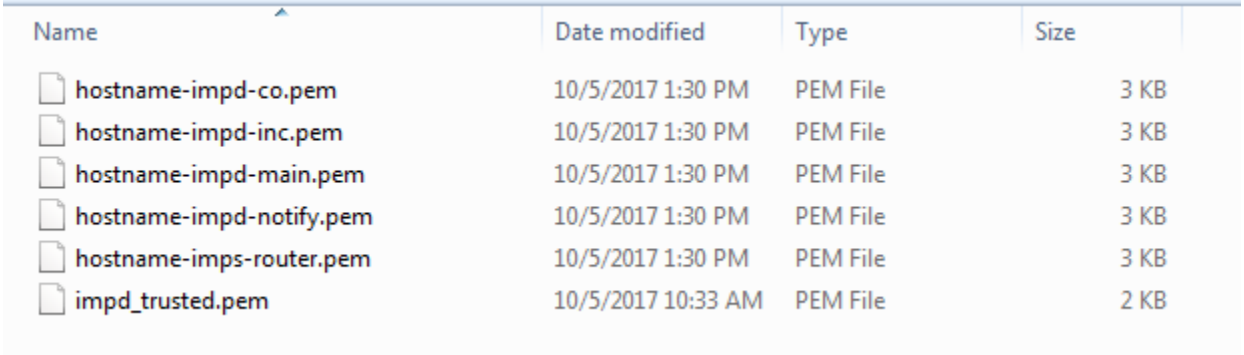
ootb_certs.zip and ootb_certs_SHA1 .zip contents

Name	Date modified	Type
conxp	7/24/2017 2:40 PM	File folder
jcs	7/24/2017 2:40 PM	File folder
jiam	7/24/2017 2:40 PM	File folder
pd	7/24/2017 2:40 PM	File folder
prov	7/24/2017 2:40 PM	File folder

Replace Provisioning Server Router DSA certs

On each Provisioning Server (where **imps-router** DSA running):

Navigate to the pd folder on ootb_certs.zip



Name	Date modified	Type	Size
hostname-impd-co.pem	10/5/2017 1:30 PM	PEM File	3 KB
hostname-impd-inc.pem	10/5/2017 1:30 PM	PEM File	3 KB
hostname-impd-main.pem	10/5/2017 1:30 PM	PEM File	3 KB
hostname-impd-notify.pem	10/5/2017 1:30 PM	PEM File	3 KB
hostname-imps-router.pem	10/5/2017 1:30 PM	PEM File	3 KB
impd_trusted.pem	10/5/2017 10:33 AM	PEM File	2 KB

Copy the impd_trusted.pem file to DXHOME\config\ssld location, and overwrite the existing one. From the same pd folder, rename the provided imps-router.pem

hostname-imps-router.pem	9/26/2016 10:52 AM	PEM File	4 KB

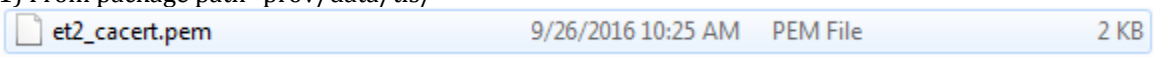
Note: Make sure the hostname is named *correctly*!
to the actual local hostname, and copy that into your DXHOME\config\ssld\personalities location and overwrite the existing one.

Delete any other ".pem" files related to 'imps' and 'impd' you have in there.
Restart your DSA performing 'dxserver stop all' followed by 'dxserver start all' command.

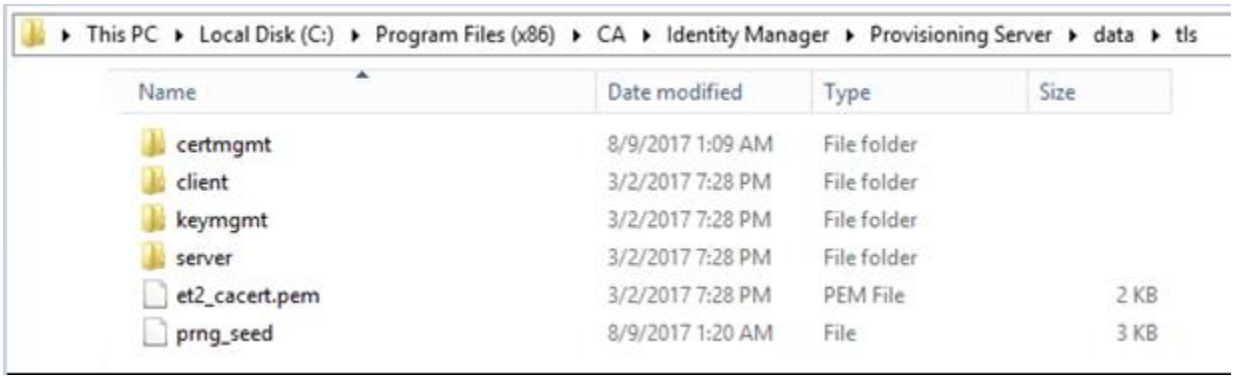
```
dxserver stop all
Running the following command: su - dsa -c "dxserver stop all"
============================================================
Stopping all dxservers
ca-prov-srv-01-impd-notify stopped
..
ca-prov-srv-01-imps-router stopped
dxserver start all
Running the following command: su - dsa -c "dxserver start all"
============================================================
Starting all dxservers

ca-prov-srv-01-imps-router starting
..
ca-prov-srv-01-imps-router started
```

Replace Provisioning Server Certs

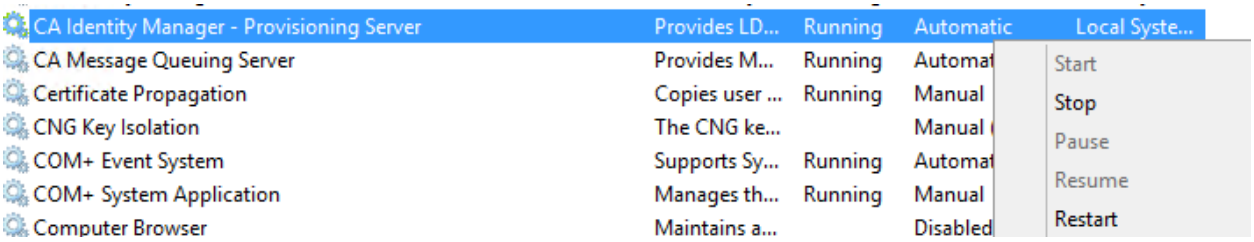
- For Prov Server you replace in just one place.
  1) From package path "prov/data/tls/"



Insert the file from ootb_certs.zip into <Provisioning Server>/data/tls/ as seem in screenshot below.



2) Restart Provisioning Server. This can be found in the Services window,



Replace Provisioning Directory DSA certs

On each Provisioning Directory Server (where you typically have impd-main, impd-inc, impd-co and impd-notify DSAs running):

CA Directory -	hostname-impd-co	Provides LD...	Running	Automatic (D...	Local Service
CA Directory -	hostname-impd-inc	Provides LD...	Running	Automatic (D...	Local Service
CA Directory -	hostname-impd-main	Provides LD...	Running	Automatic (D...	Local Service
CA Directory -	hostname-impd-notify	Provides LD...	Running	Automatic (D...	Local Service

Shut these DSA's down

- Take the same impd_trusted.pem used above in the pd folder on ootb_certs.zip and copy it to your DXHOME\config\ssld location and overwrite the existing one.
- From that same ootb_certs.zip/ootb_certs_SHA1.zip extraction and pd folder, rename the provided impd files (ex. hostname-impd-co.pem) to reflect your local data DSA names, and then copy the files into your DXHOME\config\ssld\personalities location and overwrite the existing ones.

Name	Date modified	Type	Size
hostname-impd-co.pem	10/5/2017 1:30 PM	PEM File	3 KB
hostname-impd-inc.pem	10/5/2017 1:30 PM	PEM File	3 KB
hostname-impd-main.pem	10/5/2017 1:30 PM	PEM File	3 KB
hostname-impd-notify.pem	10/5/2017 1:30 PM	PEM File	3 KB
hostname-imps-router.pem	10/5/2017 1:30 PM	PEM File	3 KB
impd_trusted.pem	10/5/2017 10:33 AM	PEM File	2 KB

Note: Make sure the hostname is named *correctly*!

- Delete any other .pem files related to 'imps' and 'impd' you have in there.
- Restart your DSAs by performing 'dxserver stop all' followed by 'dxserver start all' command.

Replace Provisioning Manager Certs

For Provisioning Manager you replace in two places.
1) from package path "prov/data/tls/" -> on the host under <Provisioning Manager>/data/tls/
2) from package path "prov/data/tls/client/ -> on the host under <Provisioning Manager>/data/tls/client
3) Restart Provisioning Manager.

Replace Provisioning Server Certs

For Provisioning Server you replace in just one place.
1) from package path "prov/data/tls/" -> on the host under <Provisioning Server>/data/tls/
2) Restart Provisioning Server.

Replace jiam.jar file

Now you can follow information in https://docops.ca.com/ca-identity-manager/12-6-8/EN/upgrading/upgrade-provisioning-components/update-your-provisioning-certificates starting at:

- Java Connector Server
- Connector Xpress

  NOTE: For both of the above, if you are running Java/JRE 1.5, the provided keytool command in the documentation will not work as that version doesn't support '-importkeystore' option. Your workaround would be to upgrade Java/JRE to at least 1.7 and the command should work.
- Connector Server SDK
- Update jiam.jar File (Ensure you follow the right Use Case 1 or 2 depending on your IDM release)

  NOTE: 'Use Case 2' also applies to IDM 12.5X release (or you can use this TEC1561732 for the same)

In **Jboss 6.x** go to this location:

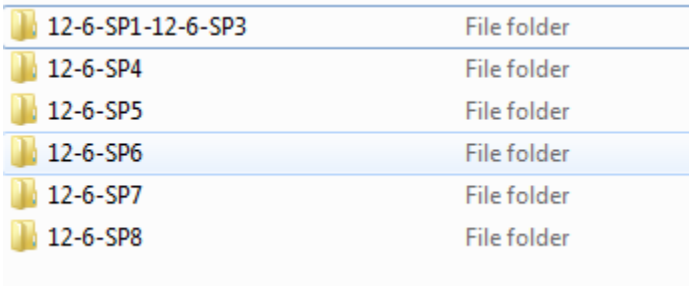
<Jboss_Home>\standalone\deployments\iam_im.ear\library

In **JBoss 5.x** go to this location:

jboss-5.1.0.GA\server\default\deploy\iam_im.ear\library

Replace the jiam.jar file here with the one located in ootb_certs\jiam Pick the correct IDM version you are currently using in your environment.

Contents of ootb_certs\jiam:



References

Docops:
https://docops.ca.com/ca-identity-manager/12-6-8/EN/upgrading/upgrade-provisioning-components/update-your-provisioning-certificates#UpdateYourProvisioningCertificates-ProvisioningDirectoryandProvisioningServeronDifferentSystems

CA Communities:
https://communities.ca.com/message/242012911-steps-to-address-expired-6-oct-2017-provisioning-certificates-in-identityminder

Proactive Notification:
https://support.ca.com/us/product-content/status/announcement-documents/2017/ca---proactive-notification---idmgr---advisory---aidmgr-100477.html