How to update Expired SSL Certificate

USER GUIDE

Security Level:	**Confidential**
Author:	**Nirmal Misra**
Last Edit Date:	**June 6, 2022**
Status	**FINAL**
Created Data:	**January 21st 2020**

Contents

1 Document Version Control

Version	Description	Date	Who
1.0	Initial Document Creation	21 January 2020	Nirmal Misra

Item 1 – Document Version Control

2 Glossary of Terms

Term	Description
.crt	The CRT extension is used for certificates. The certificates may be encoded as binary DER or as ASCII PEM. The CER and CRT extensions are nearly synonymous.
.key	The KEY extension is used both for public and private PKCS#8 keys. The keys may be encoded as binary DER or as ASCII PEM.
.p12	A digital **certificate** that uses PKCS#12 (Public Key Cryptography Standard #12) encryption
.pem	.pem extension is used in different types of X.509 v3 files which contain ASCII (Base64) armoured data prefixed with a "—– BEGIN …" line
SSL file	SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.

Item 2 – Glossary of Terms

3 Pre-Requisites

The following items will be required during the course of the set up:

- The new / renewed PKCS12 certificate
- The Export Password

A file management utility such as WinSCP to transfer certificate to KeyScaler VM.

4 Introduction

This documents how to renew the SSL certificate that has expired or expiring for the SSL for ***.companyname.com** on the Production KeyScaler System.

5 Examine the Expired Certificate Location

Login to Production System and check *.p12 file in /var/www/tomcat/conf/server.xml

```
keystoreType="pkcs12"
keystoreFile="/var/dfactor/conf/.ca4dc6ec4f1257ee.p12"
keystorePass="41rFaC02oJiM" />
```

Item 3 – server.xml file

For example, the old p12 file, ***.ca4dc6ec4f1257ee.p12*** *is located at* /var/dfactor/conf/. The associated export password is **41rFaC02oJiM.**

Note: The above two items need to be updated with the new p12 and associated new password along with the correct location.

Note: The file, *.ca4dc6ec4f1257ee.p12* for security reasons is a hidden file, so you my need to change your file viewing options to be able to see it. Use the Password from the server.xml file to open it

6 Implementing the new SSL Cert

Copy the new p12 Certificate using WinSCP to the Production VM at the right location. Also set the certificate file permissions as shown below:

```
[Tue Jan 21 10:40:23 root@ip-10-253-10-55:/var/www/tomcat/conf]$ chown dfactor_user:tomcat .b96a5e67fb1ef1ed.p12
```

Item 4 – Set File Permissions

As an example the new renewed p12 SSL certificate is .b96a5e67fb1ef1ed.p12 with new export password, DF483NotYoIRd!, with the same location as before, which is /var/dfactor/conf/

Next, Stop the dfactor service on the Production System:

```
[Tue Jan 21 10:40:23 root@ip-10-253-10-55:/var/www/tomcat/conf]$ service dfactor stop
Stopping DeviceAuthority D-Factor
Using DFACTOR_HOME: /var/dfactor
Using CATALINA_BASE:   /var/www/tomcat
Using CATALINA_HOME:   /var/www/tomcat
Using CATALINA_TMPDIR: /var/www/tomcat/temp
Using JRE_HOME:        /usr/java/latest
Using CLASSPATH:       /var/www/tomcat/bin/bootstrap.jar:/var/www/tomcat/bin/tomcat-juli.jar
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option MaxPermSize=256m; support was removed in 8.0
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option UseSplitVerifier; support was removed in 8.0
DeviceAuthority D-Factor stopped successfully
```

Item 5 – Stop the Dfactor service on production System

Edit the ***server.xml*** file to reference the new SSL certificate file and associated password and location:

```
…
      disableUploadTimeout="true"
      acceptCount="100"
      useBodyEncodingForURI="true"
      keystoreType="pkcs12"
      keystoreFile="/var/dfactor/conf/.b96a5e67fb1ef1ed.p12"
      keystorePass="DF483NotYoIRd!" />
   <!-- Define an AJP 1.3 Connector on port 8009
      <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
   -->
…
```

Item 6 – edit server.xml file

Save the server.xml file.

Start the dfactor services:

```
[Tue Jan 21 10:55:58 root@ip-10-253-10-55:/var/dfactor/conf]$ service dfactor start
Starting DeviceAuthority D-Factor
Using DFACTOR_HOME: /var/dfactor
Using CATALINA_BASE:   /var/www/tomcat
Using CATALINA_HOME:   /var/www/tomcat
Using CATALINA_TMPDIR: /var/www/tomcat/temp
Using JRE_HOME:        /usr/java/latest
Using CLASSPATH:       /var/www/tomcat/bin/bootstrap.jar:/var/www/tomcat/bin/tomcat-juli.jar
```

Item 7 – Start the dfactor service

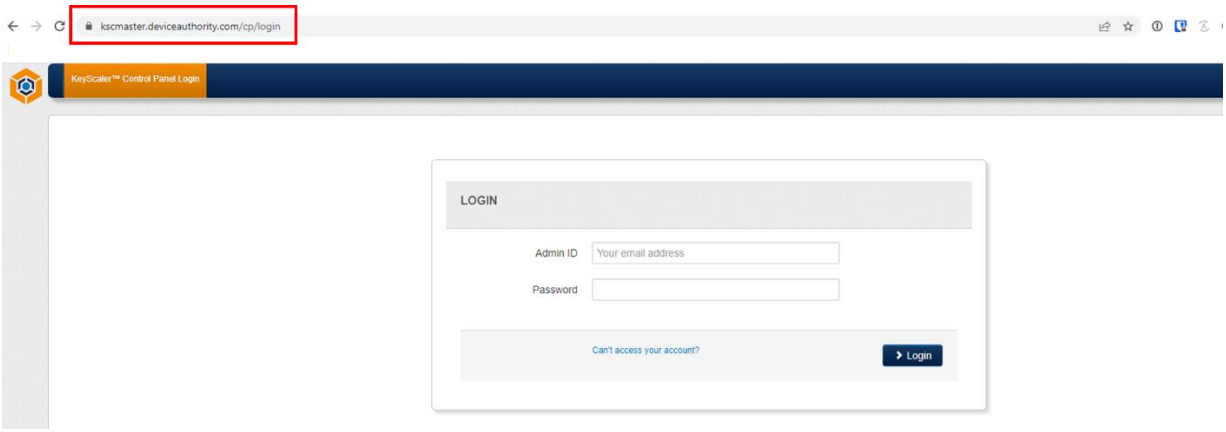
The new SSL certificate is now implemented.

7 Testing

To ensure the new SSL certificate has been implemented correctly, login to Control Panel Host and check the certificate status on the top left corner, usually shown by a closed 'Lock' icon.

If the license information is displayed correctly, then the SSL cert has been successfully implemented.

For example, shown below:



Item 8 – Example CP showing new SSL certificate deployed

---------- End of Document ----------