How to setup EEM UI to use a custom signed certificate (R8.4 SP4+ and R12.x)

-This instruction is **not** for setting SSL connectivity to an LDAP source. It is for setting a custom certificate that a customer would use to add the default EEM UI spin page to the local machines' trusted certificate authority. The finished certificate file is made up of only the EEM server certificate. The root, intermediate, and all other associated parts of the chain need not be included and is the responsibility of the customer to deploy to the local machines' trusted certification authorities.
The server certificate should be added in defaultport section in igateway.conf file. Sample for pem certificate is given below.

```
<Connector name="defaultport">
            <port>5250</port>
            <mustlisten>true</mustlisten>
            <conntype/>
            <conntimeout>120</conntimeout>
            <peektimeout>30</peektimeout>
            <maxconnections>1000</maxconnections>
            <maxrequestbytes>10000000</maxrequestbytes>
            <maxpiperequests>10</maxpiperequests>
            <maxAcceptRate/>
            <certType>pem</certType>
            <certURI>Server_cer.cer</certURI>
            <certPW/>
            <keyURI>Server_key.key</keyURI>
            <keyPW/>
            <secureProtocol/>
```

Supported Certificate types are p11, p12 and pem. If the certificate type is p12, you will fill in the certURI and certPW fields. If it is pem, you will fill in the certURI, and keyURI fields. If a password is used to encrypt the key file, you will fill in the keyPW field as well. The top of the .key file will say "Start Encrypted RSA string".
You can remove a passphrase from a private key by running: (Requires openssl libraries)

- openssl rsa -in privateKey.pem -out newPrivateKey.pem

This is the only change required in igateway.conf file.
iGateway always uses munged passwords for certificates. This is true for both pem and p12 certificates. Pem certificates are unencrypted and are not password protected. Hence, igateway does not check the certificate password of pem format certificates.

Although we can directly edit iGateway.conf files, it's not the recommended way to update the certificates and other information in iGateway.conf file. Igateway comes with a tool named "ConfigTool" which can be used to update any iGateway.conf file values.

For example, to munge the certPW password in above sample igateway.conf file, you can use the command below:

```
C:\Program Files (x86)\CA\SC\iTechnology>ConfigTool -munge -version 4.6.0.0 -comp igateway -tag "TransportReceiver=HTTP;Connector=defaultport;certPW;" -passwd testpassword
```

Note: The version number should match the version listed near the top of igateway.conf

Here is another set of steps that can be shared with any customer:
By default EEM/iGateway uses default igateway certificates(igatewayCert) for communication. If you want to change this to a custom p12 certificate, you basically need to make following changes in igateway.conf file.

1. Copy the p12 certificate to iTechnology folder.
2. Stop iTechnology service.
3. Edit igateway.conf and update the <Connector name="defaultport"> section
4. Set certType to p12
5. Set certURI to your .p12 certificate filename
6. Set certPW to munged p12 certificate file password using the ConfigTool.
7. Save and exit the file
8. Start the iTechnology service