Solution ID : **SO9282**

Last Modified : **12/18/2018**

Share Via Email

WSS

Installation Instructions for IBM Websphere using the command line

Solution

This document provides instructions for installing SSL Certificates for IBM Websphere using **iKeycmd**. If unable to use these instructions for your server, Symantec recommends that you contact IBM.

NOTE: Keep in mind that to successfully use the certificate sent by Symantec, the Intermediate CA certificate and SSL certificate must be imported into same key file from which the certificate request was generated. Ikeyman gives errors when you try to import the Symantec certificate into a key file that does not contain the certificate request.

NOTE: Click here to install the SSL Certificate by using the IKEYMAN GUI (/content/digicertknowledgebase/en/us/generalinformation/INFO230.html).

Step 1: Download the Symantec Intermediate CA Certificate

1. Download the Intermediate CA certificate from this link (/content/digicertknowledgebase/en/us/generalinformation/INFO657.html).
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
   NOTE: To check which certificate type you have purchased, follow the steps from this link

(/content/digicertknowledgebase/en/us/solution/SO13499.html).
2. Copy the Intermediate CA certificate and paste it on a Notepad.
3. Make sure there are 5 dashes to either side of the BEGIN CERTIFICATE and END CERTIFICATE and that no white spaces, extra line breaks or additional characters have been inadvertently added.
4. Save the file as **intermediate.cer.**

Step 2: Install Symantec Intermediate CA Certificate

1. Run following command to add the **intermediate.cer** into the key database:

   For UNIX:

   gsk7cmd -cert -add -db filename -pw password -label label -file filename -format ascii

   For Windows**:**

   runmqckm -cert -add -db filename -pw password -extensionel -file filename -format ascii

   - **-db** filename is the fully qualified file name of a CMS key database, for example: dbkey.kdb.
   - **-pw** password is the password for the CMS key database with an extansion .cms.
   - **-label** is the key label attached to the certificate, for example: "ibmwebspheremqqmname".
   - **-file** filename is the fully qualified file name of the file containing the Intermediate CA certificate, for example intermediate.cer.
   - **-format** ascii is the format of the certificate. The value can be ascii for Base64-encoded ASCII. The default is ascii.

Step 3: Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad
   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

-----END CERTIFICATE-----

3. Make sure there are 5 dashes to either side of the BEGIN CERTIFICATE and END CERTIFICATE and that no white spaces, extra line breaks or additional characters have been inadvertently added.

   NOTE: You can also download the certificate from your Symantec account by following this link (https://www.symantec.com/page.jsp?id=ssl-my-account&inid=vrsn_symc_ssl_MyAccount).
   When downloading the certificate, please select **X.509** as a certificate format and copy only the **End Entity Certificate**.

4. Save the file with extension **.cer**

Step 4: Install the SSL Certificate

1. To install a certificate in iKeycmd (using UNIX command line), run following command:

   For UNIX:

   gsk7cmd -cert -receive -file filename -db filename -pw password -format ascii

   For Windows:

   runmqckm -cert -receive -file filename -db filename -pw password -format ascii

   - **-file** filename is the fully qualified file name of the file containing the personal certificate.
   - **-db** filename is the fully qualified file name of a CMS key database, for example: dbkey.kdb.
   - **-pw** password is the password for the CMS key database with an extansion .cms.
   - **-label** is the key label attached to the certificate, for example: "ibmwebspheremqqmname".
   - **-format** ascii is the format of the certificate. The value can be ascii for Base64-encoded ASCII. The default is ascii.

Step 5: Extract SSL Certificate

1. To extract a certificate in iKeycmd, run following command:

For UNIX:

gsk7cmd -cert -extract -db filename -pw password -label label -target filename -format ascii

For Windows

runmqckm -cert -extract -db filename -pw password -label label -target filename -format ascii

- **-db** filename is the fully qualified pathname of a CMS key database.
- **-pw** password is the password for the CMS key database with an extansion .cms
- **-label** label is the label attached to the certificate.
- **-target** filename is the name of the destination file
- **-format** ascii is the format of the certificate. The value can be ascii for Base64-encoded ASCII. The default is ascii

2. Verify your installation with the Symantec Installation Checker (https://ssltools.digicert.com/checker/views/checkInstallation.jsp).

IBM Support

For more information, refer to IBM documentation (http://www-01.ibm.com/support/docview.wss?uid=swg27023472&aid=1) / IMB Support (http://publib.boulder.ibm.com/infocenter/wmbhelp/v7r0m0/index.jsp?topic=%2Fcom.ibm.etools.mft.doc%2Fbp10610_.htm)