



Enabling HTTPS in SapphireIMS using .CRT

Version: v1.0

Last Updated: 23-MAR-2018

Copyright

Copyright © 2017 [Tecknodreams Software Consulting Pvt. Ltd.](#) All Rights Reserved.

Restricted Rights Legend

This documentation is subject to and made available only pursuant to the terms of the Tecknodreams License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the documentation except as specifically allowed in the agreement. This document may not, in whole or in part, be copied photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior consent, in writing, from Tecknodreams.

Information in this document is subject to change without notice and does not represent a commitment on the part of Tecknodreams.

Contents

Introduction	1
Pre-requisites	1

Introduction

This document will represent the how to enable SSL using .crt and .pem files

Pre-requisites

1. Openssl and JDK should be installed
2. gd_bundle-g2-g1.crt - Root Certificate
gdig2.crt.pem - Intermediate Certificate
[randomNumber].crt - Domain Certificate
3. Private Key of the CSR file (key store) : this key has used to generate the CSR file

To enable the SSL follow the below steps :

1. Convert crt to pem. To excute the following commands
 - a. openssl x509 -in gd_bundle-g2-g1.crt -out gd_bundle-g2-g1.pem
 - b. openssl x509 -in [randomNumber].crt -out [randomNumber].pem
2. Join root and intermediate certificate

```
type gdig2.crt.pem gd_bundle-g2-g1.pem >> clientcertchain.pem
```
3. Extract the key from the keystore
 - a. keytool -importkeystore -srckeystore <private key store> -destkeystore keystore.p12 -deststoretype PKCS12 -srcalias <aliasname of the key> -deststorepass <destination key store password> -destkeypass <destination key password >
 - b. openssl pkcs12 -in keystore.p12 -nodes -nocerts -out key.pem
4. Create pkcs12 keystore

```
openssl pkcs12 -export -out final.p12 -inkey key.pem -in [randomNumber].crt -CAfile clientcertchain.pem -name "cacertificates"
```

5. Create JKS key store from pkcs keystore

```
keytool -importkeystore -srckeystore final.p12 -srcstoretype PKCS12 -destkeystore SSL.pfx
```