

How to Configure SAP MII 12.0.3 Build 107 for HTTPS



Applies to:

Configuring SAP Manufacturing Integration and Intelligence (SAP MII 12.0.3 build 107) for HTTPS. For more information, visit the [Manufacturing homepage](#).

Summary

This paper outlines the process of configuring SAP MII to use https. The SAP J2EE Engine must possess a key pair, which consists of a public key, which is distributed using an X.509 public-key certificate, and a corresponding private key. Use the procedure below to create the key pair and public-key certificate on the server. This example that may not apply to all circumstances, certain steps may differ depending on security configurations specific to a network. All paths are relative to the Java SDK Version 1.4.2_17.

Author: Pedro Iglesias

Company: CIBER

Created on: 5 May 2008

Author Bio

Pedro Iglesias was founder of Vitegris GmbH and Head of Vertical Integration Services. Vitegris GmbH used to be Lighthammer's Preferred Enterprise Solution Partner in EMEA since 2002. Since December 2006 he is working in CIBER as Sr. Solution Architect. Since 2008 he is Head of SAP MII Competence Center at CIBER.

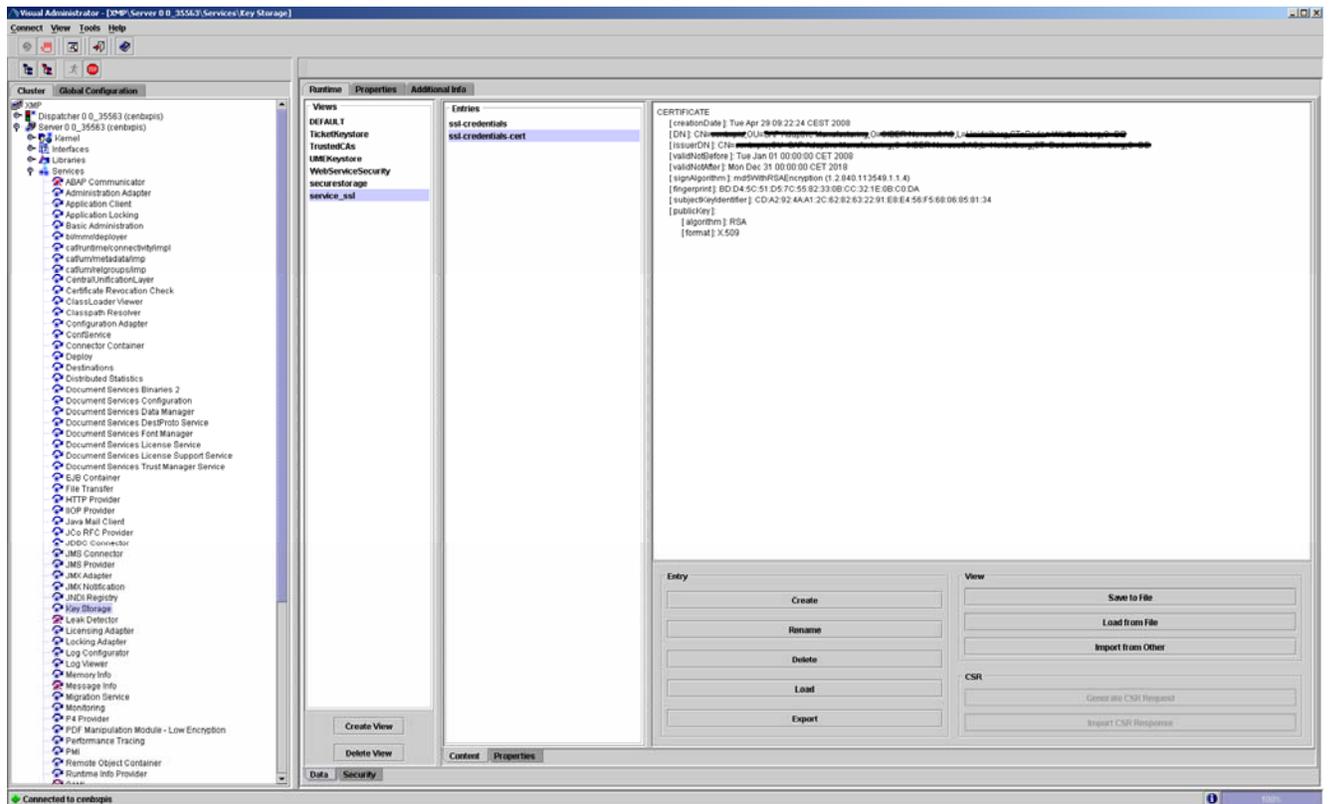
Table of Contents

Generating a Certification in NetWeaver	3
Exporting Certification from NetWeaver.....	4
Configuring the SAP MII for SSL	5
Configuring the SAP MII for SSL on NetWeaver	6
Configuring the Java Web Start for SSL.....	7
Related Content.....	8
Disclaimer and Liability Notice.....	9

Generating a Certification in NetWeaver

These steps are only necessary if you do not have a valid certification for the NetWeaver. The certificate can be created in Visual Admin (describe below) or with your company process for generating certificates. If you are using the company process, then you need to load your certification into the NetWeaver.

- Open Visual Admin (“D:\usr\sap\- Expand the tree under “Server” and also expand the “Services” folder.
- Select the node “Key Storage”.
- Select on right hand Views the entry “service_ssl”.
- Select on “Entries” the “ssl-credentials” and choose Delete Button.
- Select on “Entries” the “ssl-credentials-cert” and choose Delete Button.



- Select on “Entry” the Button “Create” to create a new key pair.
- Specify the Entry Name “ssl-credentials” to use to identify the private key entry in the Key Store.
- Specify the Valid From and the Valid To of the Certification.
- Select “Store Certificate”.
- Choose “Key Length” 1024 to use.
- Choose “Algorithm” RSA to use.

- Specify the server's fully-qualified host name as the "Common Name". Otherwise, certain Web browsers can produce a warning if the host name that users use to access the server does not match the host name found in the server's public-key certificate
- Select the Button "Generate".

Key	Value
Country Name (2 letter code)	US
State/Province (full name)	Pennsylvania
Locality Name (eg. city)	Exton
Organization Name	SAP
Organization Unit Name	SAP MII
Common Name	<FULLQUALIFIEDNAME>

Entry Name
Store Certificate
Valid From
Key Length
Valid To
Algorithm

- Now you will see two entries in "Entries".
- "ssl-credentials"
- "ssl-credentials-cert"
- Choose the "ssl-credentials-cert" and click on the Button "Export" to save the new Certification.

Exporting Certification from NetWeaver

- Open Visual Admin ("D:\usr\sap\<InstanceName>\JC00\j2ee\admin\go.bat").
- Expand the tree under "Server" and also expand the "Services" folder.
- Select the node "Key Storage".
- Select on right hand Views the entry "service_ssl".
- Select on "Entries" the "ssl-credentials-cert" and choose Export Button.
- Choose a directory and file name and click Save.

Configuring the SAP MII for SSL

In order for Secure Sockets Layer (SSL) communications to take place, you must import your server's certificate into the Java Virtual Machine (JVM) on which the NetWeaver is running. This step establishes a trust between the client and the server application. These steps will assume that the version of the Java SDK is 1.4.2_17 and is installed on the D drive.

To import the SSL certificate into the JVM Truststore, complete the following steps:

- Open a command prompt: start – run type: cmd click OK.
- Change the directory to D:\j2sdk1.4.2_17\bin
- Run the following command to do this: cd D:\j2sdk1.4.2_17\bin
- Run the following command:

```
keytool -import -file <path to cert> -keystore <path to the JRE cacerts file> -
alias <name to store cert>
```

Where:

file is the path to the SSL certificate

keystore is the location of the JVM's CACERT file (the list of trusted certificates for the JVM)

alias is the name you want to use to store the certificate

Example

```
keytool -import -file "E:\cenbxpis.crt" -keystore
D:\j2sdk1.4.2_17\jre\lib\security\cacerts -alias certServerName
```

```
C:\WINDOWS\system32\cmd.exe
D:\j2sdk1.4.2_17\jre\bin>keytool -import -file "e:\cenbxpis.crt" -keystore D:\j2
sdk1.4.2_17\jre\lib\security\cacerts -alias cenbxpis
Geben Sie das Keystore-Passwort ein: changeit
Eigent"mer: CN=cenbxpis, OU=SAP Adaptive Manufacturing, O=CIBER Novasoft AG, L=H
eidelberg, ST=Baden-W"rttemberg, C=DE
Aussteller: CN=cenbxpis, OU=SAP Adaptive Manufacturing, O=CIBER Novasoft AG, L=H
eidelberg, ST=Baden-W"rttemberg, C=DE
Seriennummer a9106d
G"ltig ab: Tue Jan 01 00:00:00 CET 2008 bis: Mon Dec 31 00:00:00 CET 2018
Zertifikatfingerabdr"cke:
    MD5: BD:D4:5C:51:D5:7C:55:82:33:0B:CC:32:1E:0B:C0:DA
    SHA1: 1E:45:A3:09:30:30:78:CF:84:09:1F:FC:22:83:D1:AE:A2:65:83:85
Diesem Zertifikat vertrauen? [Nein]: j
Zertifikat wurde zu Keystore hinzugef"gt.

D:\j2sdk1.4.2_17\jre\bin>
```

- You will then be prompted for a password, the password should be "changeit" without the quotes.
- You will then be prompted to "Trust this certificate?" type "y" without the quotes.
- Restart the application server that is hosting the SAP MII (NetWeaver).

Configuring the SAP MII for SSL on NetWeaver

To import the SSL certificate into the JVM Truststore of NetWeaver, complete the following steps:

- Open a command prompt: start – run type: cmd click OK.
- Change the directory to D:\usr\sap\- Run the following command to do this: cd D:\usr\sap\- Run the following command:

```
keytool -import -file <path to cert> -keystore <path to the JRE cacerts file> -
alias <name to store cert>
```

Where:

file is the path to the SSL certificate

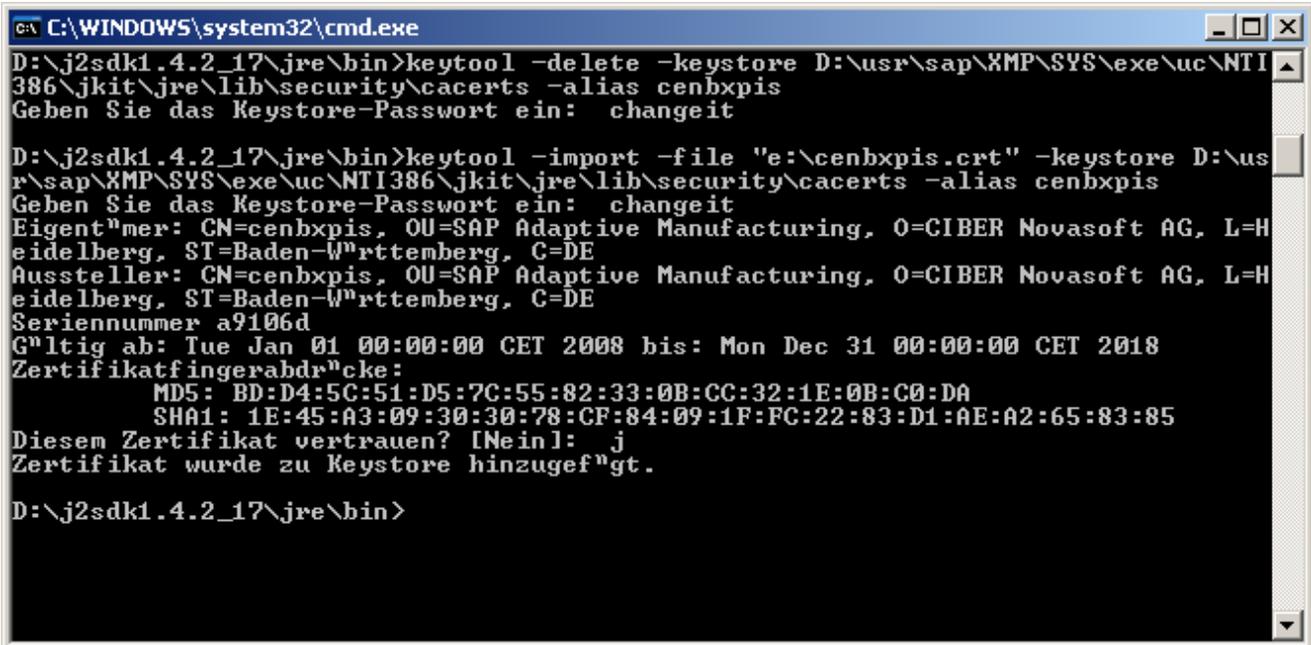
keystore is the location of the JVM's CACERT file (the list of trusted certificates for the JVM)

alias is the name you want to use to store the certificate

Example

```
keytool -import -file "E:\cenbxpis.crt" -keystore
D:\usr\sap\

```



```
C:\WINDOWS\system32\cmd.exe
D:\j2sdk1.4.2_17\jre\bin>keytool -delete -keystore D:\usr\sap\XMP\SYS\exe\uc\NTI
386\jkit\jre\lib\security\cacerts -alias cenbxpis
Geben Sie das Keystore-Passwort ein: changeit

D:\j2sdk1.4.2_17\jre\bin>keytool -import -file "e:\cenbxpis.crt" -keystore D:\us
r\sap\XMP\SYS\exe\uc\NTI386\jkit\jre\lib\security\cacerts -alias cenbxpis
Geben Sie das Keystore-Passwort ein: changeit
Eigent"mer: CN=cenbxpis, OU=SAP Adaptive Manufacturing, O=CIBER Novasoft AG, L=H
eidelberg, ST=Baden-W"rttemberg, C=DE
Aussteller: CN=cenbxpis, OU=SAP Adaptive Manufacturing, O=CIBER Novasoft AG, L=H
eidelberg, ST=Baden-W"rttemberg, C=DE
Seriennummer a9106d
G"ltig ab: Tue Jan 01 00:00:00 CET 2008 bis: Mon Dec 31 00:00:00 CET 2018
Zertifikatfingerabdr"cke:
    MD5: BD:D4:5C:51:D5:7C:55:82:33:0B:CC:32:1E:0B:C0:DA
    SHA1: 1E:45:A3:09:30:30:78:CF:84:09:1F:FC:22:83:D1:AE:A2:65:83:85
Diesem Zertifikat vertrauen? [Nein]: j
Zertifikat wurde zu Keystore hinzugef"gt.

D:\j2sdk1.4.2_17\jre\bin>
```

- You will then be prompted for a password, the password should be "changeit" without the quotes.
- You will then be prompted to "Trust this certificate?" type "y" without the quotes.
- Restart the application server that is hosting the SAP MII (NetWeaver).

Configuring the Java Web Start for SSL

In order for Secure Sockets Layer (SSL) communications to take place between Java Web Start, which runs Business Logic Services, and the server the certificate will need to be imported into the JRE Truststore on the client machine. This is only necessary for machines used for building transactions in Business Logic Services. This will be similar to the previous step but the directory paths will differ. These steps will also assume that the version of the java JRE is 1.4.2_17 and is installed on the C drive.

- Open a command prompt on the machine that will be used to develop transactions: start – run type: cmd click OK.
- Change the directory to C:\Program Files\Java\j2re1.4.2_17\bin
- Run the following command to do this: cd C:\Program Files\Java\j2re1.4.2_17\bin
- Run the following command:

```
keytool -import -file <path to cert> -keystore <path to the JRE cacerts file> -alias <name to store cert>
```

Where:

file is the path to the SSL certificate

keystore is the location of the JVM's CACERT file (the list of trusted certificates for the JVM)

alias is the name you want to use to store the certificate

Example

```
keytool -import -file "C:\certnew.cer" -keystore C:\Program Files\Java\j2re1.4.2_17\jre\lib\security\cacerts -alias certServerName
```

```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Java\j2re1.4.2_17\bin>keytool -import -file "E:\cenbxpis.crt" -keystore "C:\Program Files\Java\j2re1.4.2_17\jre\lib\security\cacerts" -alias cenbxpis
Geben Sie das Keystore-Passwort ein: changeit
Eigent"mer: CN=cenbxpis, OU=SAP Adaptive Manufacturing, O=CIBER Novasoft AG, L=Heidelberg, ST=Baden-W"rttemberg, C=DE
Aussteller: CN=cenbxpis, OU=SAP Adaptive Manufacturing, O=CIBER Novasoft AG, L=Heidelberg, ST=Baden-W"rttemberg, C=DE
Seriennummer a9106d
G"ltig ab: Tue Jan 01 00:00:00 CET 2008 bis: Mon Dec 31 00:00:00 CET 2018
Zertifikatfingerabdr"cke:
    MD5: BD:D4:5C:51:D5:7C:55:82:33:0B:CC:32:1E:0B:C0:DA
    SHA1: 1E:45:A3:09:30:30:78:CF:84:09:1F:FC:22:83:D1:AE:A2:65:83:85
Diesem Zertifikat vertrauen? [Nein]: j
Zertifikat wurde zu Keystore hinzugef"gt.
Keytool-Fehler: java.io.FileNotFoundException: C:\Program Files\Java\j2re1.4.2_17\jre\lib\security\cacerts (The system cannot find the path specified)
C:\Program Files\Java\j2re1.4.2_17\bin>_
```

Example Java Web Start for SSL.

- You will then be prompted for a password, the password should be "changeit" without the quotes.
- You will then be prompted to "Trust this certificate?" type "y" without the quotes.

Related Content

For more information, visit the [Manufacturing homepage](#).

Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.