SDN Contribution

HOW TO CONFIGURE XMII 11.5.1 BUILD 63 AND IIS 6.0 FOR HTTPS

Applies to:

Configuring SAP xApp Manufacturing Integration and Intelligence (SAP xMII 11.5.1 build 63) and IIS 6.0 for https.

Summary

This paper outlines the process of configuring SAP xMII and IIS to use https. This document assumes that a certification authority is setup on the network and the logged in user has the necessary rights to perform all steps. 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_07.

Author Bio

Jamie Cawley has worked for Lighthammer Software since September 2004 supporting and doing application development for the Lighthammer CMS product. Since the SAP acquisition of Lighthammer in July 2005 Jamie has become a Sr. Support Consultant for SAP xMII. He is also involved in the testing and development of several of the composite applications being developed with the xMII product

Table of Contents

Requesting A Certificate In IIS

Open IIS (start – run – type: inetmgr – click ok)

Expand the tree under the computer name and expand the Web Sites folder.

Right click on the Web Site designated for xMII and choose properties.

Choose the Directory Security tab and choose Server Certificate.

Click Next and choose “Create a new certificate” and then click Next.

Choose “Send the request immediately…” and click Next.

Fill in a name, leave the bit length to 1024 and Click Next.

Fill in requested information, Organization and Organization Unit, and click Next.

The Common name will need to match the name entered in for the Security Server of xMII. See section “Changing the Security Server” for more information.

If the entry is

https://computername.test.com/LHSecurity

the Common name should be

computername.test.com

Click Next and fill in the Geographical Information and then click Next again.

Leave port 443 as the port for SSL to use and click Next.

Choose the appropriate Certification authority and click Next.

Verify the information entered and click Next.

Click Finish.

Click OK to close the Web Site Properties dialog.

Changing The Security Server

On the server open the menu using http://localhost/Lighthammer/Menu.jsp

Choose Security Services then choose Security Server

Verify that the entry for Security Server includes the ‘s’ in ‘https’

https://computername.test.com/LHSecurity

Click Save if any changes were made.

Exporting The SSL Certificate From IIS

Open IIS (start – run – type: inetmgr – click ok)

Expand the tree under the computer name and expand the Web Sites folder.

Right click on the Web Site designated for xMII and choose properties.

Choose the Directory Security tab and choose View Certificate.

Choose the Details tab.

Click the “Copy to file...” button.

Click Next.

Choose “No, do not export the private key” and click Next.

Choose “DER encoded binary X.509 (.CER)” and click Next.

Click Browse and choose a directory and file name and click Save and then click Next.

Click Finish and then OK. Close the remaining dialog windows.

Configuring The XMII Security Manager 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 Security Manager 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_07 and is installed on the c 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 C:\j2sdk1.4.2_07\bin

Run the following command to do this: *cd C:\j2sdk1.4.2_07\bin*

Run the following command:

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

where

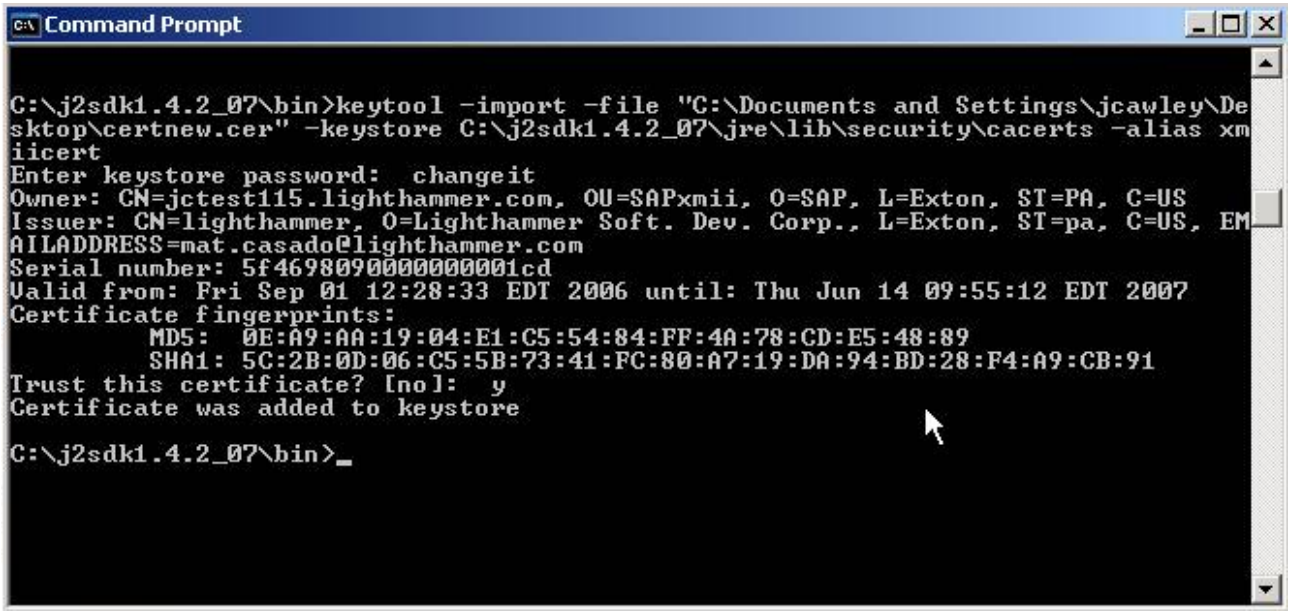
file is the path to the SSL certificate

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:\j2sdk1.4.2_07\jre\lib\security\cacerts -alias certServerName



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 xMII Security Manager.

Start – Run type: services.msc click OK.

Choose ServletExec-xMII and click restart.

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 sdk is 1.4.2_07 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_07\bin

Run the following command to do this: *cd C:\Program Files\Java\j2re1.4.2_07\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)

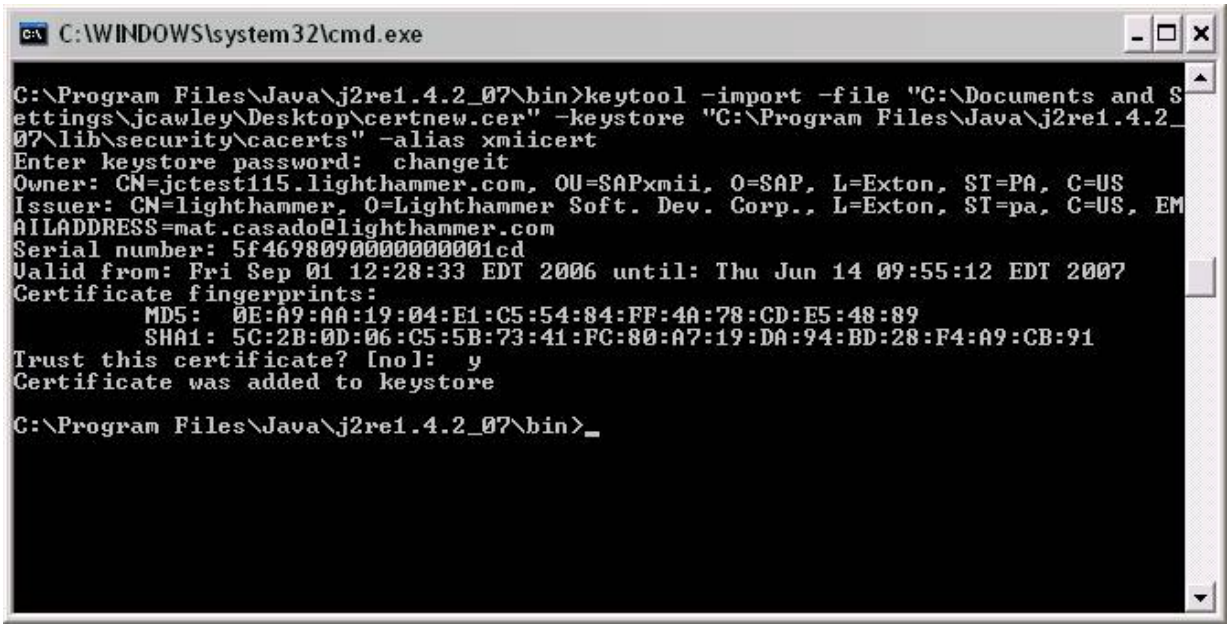
alias is the name you want to use to store the certificate

Example:

keytool -import -file "C:\certnew.cer" -keystore "C:\Program Files\Java\j2re1.4.2_07\lib\security\cacerts" -alias certServerName

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.



Troubleshooting

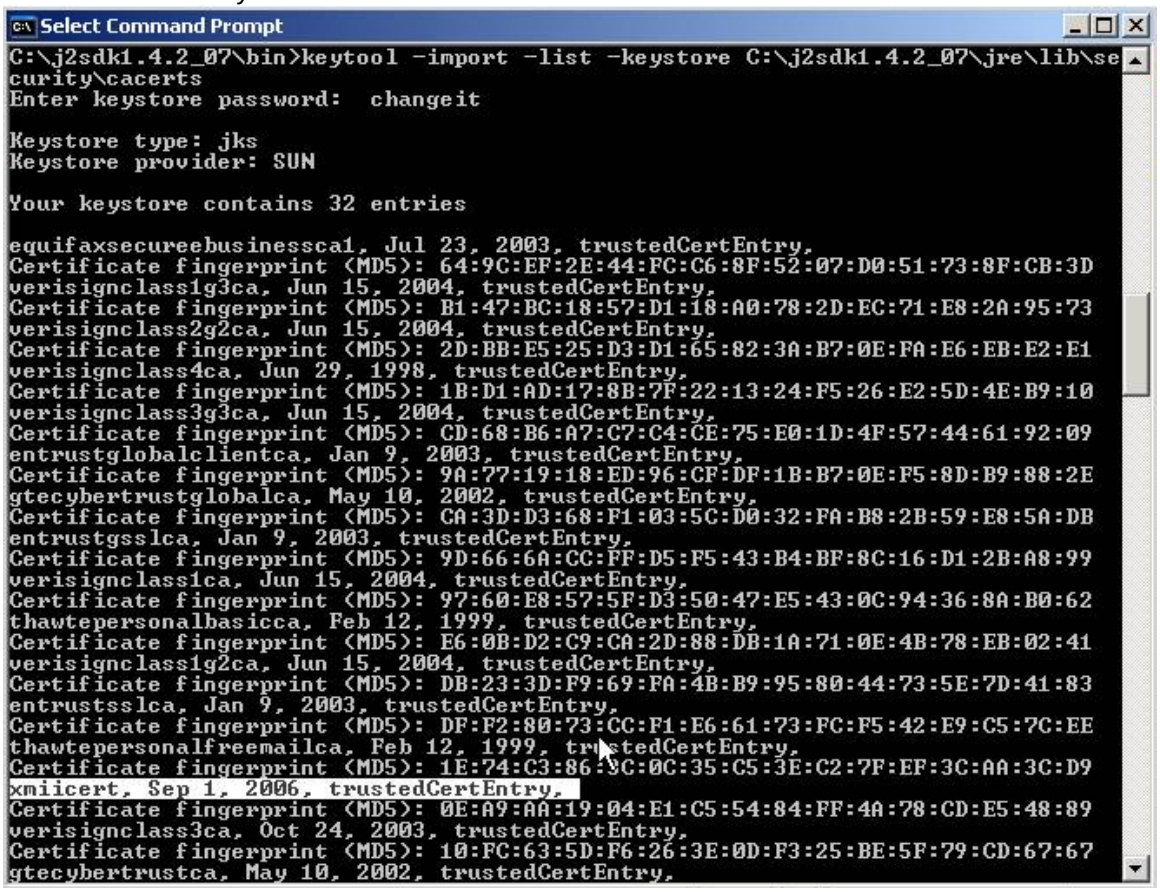
Two common errors that may be received:

1. Receiving the error "No host available, all connections are down"

This can be caused from an incorrect security server or the certificate was not correctly imported into the JVM Truststore. If https://servername.domain.com/LHSecurity will not resolve then verify that the path of the security server is correct. Otherwise verify that the certificate was imported into the JVM Truststore and is correct. The command

keytool –list –keystore <path to the JRE cacerts file>

can be used to verify that the certificate exists



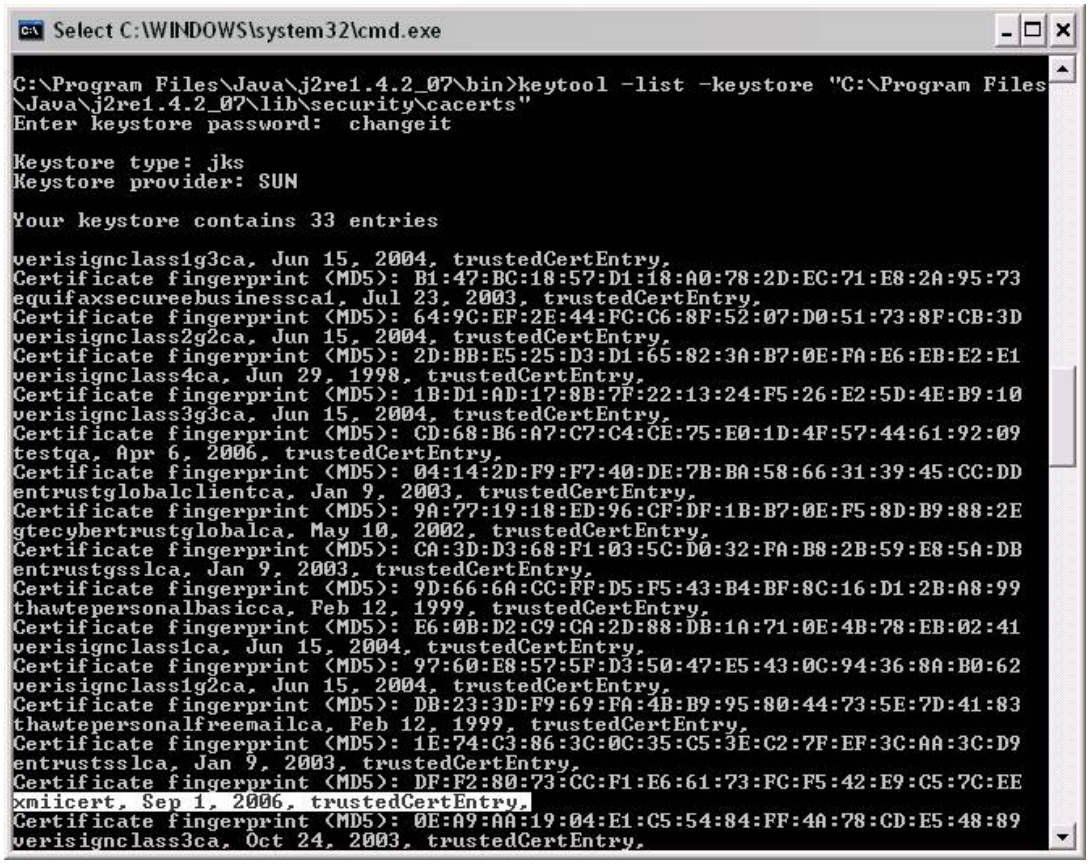
2. Receiving the error "bad session" and "no trusted certificate found" when attempting to access business logic services

Verify that you are running xMII version 11.5.1 build 63 or greater. This can be found on the xMII main menu under Support - About

Otherwise verify that the certificate was imported into the JRE Truststore and is correct. The command

keytool –list –keystore <path to the JRE cacerts file>

can be used to verify that the certificate exists



Copyright