Setting up and configuring Host On-Demand (HOD) for TLS-secured tn3270 connections -Troubleshooting

Chelsea Jean-Mary Isaac

# Background

Before you begin: **If you have not already attempted to create a secure connection with HOD**, follow the instructions to do so <u>here</u>.

COMM662 is a common error associated with TLS-secured connections on Host On-Demand for Macbook users. This error typically occurs when the server being connected to is using a self-signed certificate. If you are experiencing this issue when you start a session, you will see this error:

Server "XXX" presented a certificate that was not trusted.

This presentation will walk through the process to import the self-signed certificate into your emulator keychain and marking it as trusted.

1. Download the CustomizedCAs.jks file from this <u>link</u>.

On macOS, copy to /Applications/HostOnDemand/lib

2. Create a secure tn3270 session. In the first window, put in details marked by red arrows.

Enter the destination address, destination port, and protocol **Telnet-TLS**.

In this example: hostname is "stfmvs1.pok.ibm.com" and port is "992".



3. Click on the "TLS/SSL" tab in the lefthand navigator. Put in details as shown.

Exit this window and start the session.

| • | 00  | 3270 Displ                                       | ау                                      |    |
|---|---|--|---|----|
| • | Connection<br>Advanced  | TLS/SSL  |   |    |
|   | Associated Printer<br>Backup Servers<br>Proxy Server<br>TLS/SSL<br>SLP<br>Express Logon<br>Terminal Properties<br>Host Graphics<br>File Transfer<br>Data Transfer | Use JSSE   | Yes ONO                                 |    |
|   |   | TLS Version                                      | TLS v1.2                                | \$ |
|   |   | Telnet-negotiated                                | 🔿 Yes 💿 No                              |    |
|   |   | FIPS Mode  | • Yes 🔘 No                              |    |
|   |   | Server Authentication                            | Yes O No                                |    |
| ▼ | Screen  | Add MSIE browser's keyring                       | 🔵 Yes 💿 No                              |    |
|   | Font<br>Print Screen  | If Server Requests Client Certificate (defaults) |   |    |
| • | Preferences   | Send a Certificate                               | 🕨 🔿 Yes 💿 No                            |    |
|   | Start Options   | Certificate Source                               | URL or local file                       | ٥  |
|   |   | URL or Path and Filename                         |   |    |
|   |   |  | Select File                             |    |
|   |   |  | Setup                                   |    |
|   |   | Enable Key Usage                                 | 🔿 Yes 💿 No                              |    |
|   |   |  | Key Usage                               |    |
|   |   | Certificate Name                                 | -any certificate trusted by the server- | ٥  |
|   |   | How often to prompt                              | First time after HOD is started         | 0  |
|   |   | Retrieve certificate before connect              | ⊖ Yes ● No                              |    |

4. Click on the Communication tab and select "Security".

Click on Extract.

|                       | Security Information   |  |  |
|-----------------------|--|--|--|
| Connection Status: Co | nection is secure with TLS_RSA_WITH_AES_256_CBC_SHA and Security Protocol TLS v1 |  |  |
| Server-Certificate In | ormation   |  |  |
|                       | The server sent this certificate in order to identify itself.                    |  |  |
| Field                 | Value  |  |  |
| Name                  | tec2.ztec.dmz.wsclab.washington.ibm.com  |  |  |
|                       | Extract  |  |  |
| Show Client C         | ertificate Show CAs Trusted by Client Show Issuer Certificate                    |  |  |
|                       | OK Help  |  |  |

5. You will need to give the certificate a name and import as binary. Fill in the details as shown and click ok.

In this example, the certificate is named "Servername\_SelfSigned\_ServerCA.der"

This will extract the server's public key and store it in the Applications/HostOnDemand/lib directory on macOS.

| • • •                    | Extract a Certificate           |        |
|--------------------------|---------------------------------|--------|
| URL or Path and Filename | TEC2MVS_SelfSigned_ServerCA.der | Browse |
| Format                   | 🗌 E-mail Address 🛛 Binary       |        |
|                          | OK Cancel Help                  |        |

6. Open the "Terminal" application on macOS and type in

#### cd /Applications/HostOnDemand/lib

7. To import the key, you will need to use the keytool utility. First, change the directory to where the tool is located. Type in the following line:

cd /Library/Internet\ Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin

8. To import the key, type in the following (all one line)

./keytool -import -file /Applications/HostOnDemand/lib/Servername\_SelfSigned\_ServerCA.der -alias "Servername" -keystore /Applications/HostOnDemand/lib/CustomizedCAs.jks storepass hodpwd

In this example, the certificate is named "Servername\_SelfSigned\_ServerCA.der"

If you receive a prompt "Trust this certificate?", type y and press Enter.

9. Close down HOD and restart. You should now be able to connect.