

How to manually add a certificate to the Mobility Java keystore

Problem

The Secure Proxy's NGINX /usr/local/nginx/logs/controller.log file has "Failed to create SSL Connection" on the javax.net.ssl.SSLHandshakeException. This SSL handshake error is preventing the Secure Proxy server from registering to the Symantec Mobility Front End.

This same error may also prevent email sync and push functionality while communicating between the EAS/EWS front ends. See the note below regarding how to use these same steps to resolve other SSL Java related connectivity issues.

Error Message

javax.net.ssl.SSLHandshakeException

Cause

The SSL certificate installed on the network resource is not trusted by Java.

Solution

Note: Several things can cause an Secure Proxy server to not be able to register to a Mobility Suite Front End (FE) server or lose its connectivity thereto. First verify that the server has direct outbound access over TCP 443 to the fully qualified domain name (FQDN) of the FE. Also confirm that a local administrative account is being used to register the Secure Proxy to the FE. Steps 5 and 6 may be repeated substituting the internal CAS/EAS/EWS server FQDN for the Mobility FQDN in the **keytool** command if having this connectivity issue while attempting to send/receive email or register the impersonation account.

1. Verify that Oracle JRE 1.8 or later is installed by entering the following, as root:
java -version
2. If the output of the above command contains OpenJDK or an earlier JRE version, remove the OpenJRE package by entering the following, as root:
sudo yum -y remove java
3. Download **find** for **Linux x64** by navigating to <http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html>
Tip: For step by step guide on how to transfer files between a Linux and Windows see [HOWTO110248](#).
4. Once the RPM, from step 3, has been transferred to the Secure Proxy server, run the following command, as root from the location of the **jre-8u45-linux-x64.rpm** file, to install Oracle JRE:
rpm -ivh jre-8u45-linux-x64.rpm

```
[root@= ~]# rpm -ivh jre-8u45-linux-x64.rpm
Preparing...                               #####
 1:jre1.8.0_45                             #####
Unpacking JAR files...
   rt.jar...
   jsse.jar...
   charsets.jar...
   localedata.jar...
   jfxrt.jar...
   plugin.jar...
   javaws.jar...
   deploy.jar...
[root@= ~]#
```

5. Once JRE is successfully installed transfer the SSL certificate, installed on the Mobility Suite FE to the Secure Proxy by entering a command like:
openssl s_client -showcerts -connect <FQDNofMobilityFE>:443 </dev/null 2>/dev/null | openssl x509 -outform PEM >mycertfile.pem
Note: The SSL certificate of the Mobility Suite FE has been stored into a file named **mycertfile.pem**. If troubleshooting Email Proxy to EAS or CAS connectivity substitute their locations in place of the FQDN of the

Mobility Suite FE.

```
[root@= ~]# openssl s_client -showcerts -connect multife3:443 </dev/null  
null|openssl x509 -outform PEM >mycertfile.pem
```

6. Add the certificate file to the Java trust by entering the following, as root:

```
keytool -import -noprompt -trustcacerts -file mycertfile.pem -  
keystore /usr/java/jre1.8.0_45/lib/security/cacerts
```

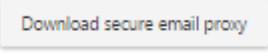
Note: The default Java password is: changeit

```
[root@= ~]# keytool -import -noprompt -trustcacerts -file mycertfile.pem  
re /usr/java/jre1.8.0_45/lib/security/cacerts  
Enter keystore password:  
Certificate was added to keystore
```

Note: If adding additional certificates for the EAS and CAS servers use the `-alias` tag to give the certificate a specific name. For example:

```
keytool -import -noprompt -trustcacerts -file cascert.pem -alias cascert -  
keystore /usr/java/jre1.8.0_45/lib/security/cacert
```

7. Ensure that the latest Secure Email ISO has been downloaded from the Mobility Suite FE by navigating to the

Mobility **Admin console > Downloads** and click  (**Download secure email proxy**).

Tip: To get to the Mobility admin console navigate to **https://<FQDNofMobility>/admin/login**

8. Transfer the ISO to the Secure Proxy server.

Tip: For step by step guide on how to transfer files between a Linux and Windows see [HOWTO110248](https://www.ibm.com/docs/en/secure-email/11.0.248).

9. Create a new mount point for the ISO by entering the following, as root:

```
mkdir /mnt/iso
```

Tip: If the `/mnt/iso` directory already has an ISO mounted, close any sessions accessing this location and type, **sudo umount /mnt/iso**

10. Mount the transferred ISO to the `/mnt/iso` directory by entering the following, as `root`:

```
sudo mount -o loop <PathToSecureProxyISO> /mnt/iso
```

11. Change the terminal's directory to `/mnt/iso`:

```
cd /mnt/iso
```

12. Remove any previous installation by entering the following, as `root`:

```
sudo ./setup.sh --uninstall
```

13. After the un-installation completes, re-install by entering the following, as root:

```
sudo ./setup.sh --install
```

14. Complete the installation by following the Mobility Suite Administration Guide