Re-import LDAP Certificate

Sometimes, after upgrading to RiskVision version 9.4 or above, users are unable to connect to the LDAP source, such as Active Directory, and receive the following error message:

Please check directory server configuration details for domain: qateam.local. javax.naming.CommunicationException: simple bind failed: [hostname]:636 [Root exception is javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]

When this happens, re-importing the LDAP certificate will allow users to access Active Directory.

To re-import the LDAP certificate:

1. Open the command prompt and navigate to where the LDAP certificate was previously imported. By default it should be in the **%AGILIANCE_HOME%\apache2\conf\server.crt** folder.

2. Re-import and store the certificate in the **C:\SecureLDAP\keystore.cer** folder by running the following command all in one line:

    - `keytool -import -alias ldap1 -keystore %AGILIANCE_HOME%\Java\jre\lib\security\cacerts -trustcacerts -file C:\SecureLDAP\keystore.cer`

    > While importing the certificate, the system will prompt for keystore password. The default keystore password for cacerts is **changeit**.

3. Restart the Tomcat server and check your LDAP connection again.