# **How to setup LDAP/Active directory to use SSL**

EBX Integration is using JNDI integration to access LDAP/Active Directory

To enable SSL with LDAP there are 2 options:

1. Import the server (LDAP/Active directory) certificate into the Java Runtime Engine libraries
2. Use a System variable that points to the certificate file
3. Setup EBX to use SSL

Note: The server (LDAP/Active Directory) needs to support LDAPS and be configured accordingly. As part of this it needs to have a valid certificate for Clients to access it.

## **Import a certificate into certificate into the Java Runtime Engine libraries**

To implement this step, you will need a valid certificate for the server you plan to use SSL with.

Java has a built-in tool named keytool located in the Bin folder of the JRE/JDK.

Navigate to the JRE security library that runs the EBX server:

e.g. [Java Runtime Home directory] \lib\security

This folder contains all certificates known to this JRE.

By executing the following command, you can import the new certificate into the default java security libraries:

**keytool -import -alias [an alias name] -file [Server certificate] -keystore [**default Java keystore**: cacerts]**

## **Use a System variable that points to the certificate file**

Create a certificate store file using the keytool command

Import server certificate into the certificate store file.

Use of system variables to specify the Java trusted store for certificates:

Javax.net.ssl.trustStore = “path to a certificate store file”

Javax.net.ssl.trustStorePassword = “password for the certificate store file”

You can add those system variables to the startup script that starts EBX server.

## **Setup EBX to use SSL**

In ebx.properties, modify the property ebx.directory.ldap.path to ldaps://[host name]:[port number]/

Restart EBX.