FIT LDAP Active Directory SSL Connection Configuration Instructions

Alcea Technologies Inc.

November 19, 2010

If you have any questions or problems during the configuration of the LDAP Module, please contact the team at: fit@alceatech.com.

Installing the FIT LDAP Module

Make sure that you have installed and configured the LDAP module by following the steps in our LDAP Module Installation instructions at the following location: http://www.fittrackingsolutions.com/support/LDAPModuleInstructions-130807.pdf

Configuring Active Directory for SSL access

If the Certificate Authority (CA) is not installed, you can install it on your Active Directory server as follows:

1. Click **Start** -> **Control Panel** -> **Add or Remove Programs**.
2. Click **Add/Remove Windows Components** and select **Certificate Services**.
3. Follow the procedure provided to install the **Certificate Services CA**.

Verifying that SSL is enabled on the Active Directory server

To verify that SSL has been enabled on the Active Directory server, do the following:

1. Ensure that Windows Support Tools is installed on the Active Directory machine. The **suptools.msi** setup program is located in the \Support\Tools directory on your Windows installation CD.
2. Select **Start -> All Programs -> Windows Support Tools -> Command Prompt**. Start the **ldp** tool by typing `ldp` at the command prompt.
3. From the ldp window, select **Connection -> Connect** and supply the host name and port number (**636**). Also select the SSL check box.

   Note: Ensure that you type the Active Directory domain server name correctly.

If successful, a window is displayed listing information related to the Active Directory SSL connection. If the connection is unsuccessful, restart your system, and repeat this procedure.

Exporting the certificate from the Active Directory server

To export the CA certificate from the Active Directory server, follow these steps:

1. Log on as a Domain Administrator to the Active Directory domain.
2. Export the certificate from the Active Directory server to a file. To do so, follow these steps:
   a. Click **Start** -> **Control Panel** -> **Administrative Tools** -> **Certificate Authority** to open the CA Microsoft Management Console (MMC) GUI.
   b. Highlight the CA machine and right-click to select **Properties** for the CA.

c. From General menu, click **View Certificate**.

d. Select the **Details** view, and click the **Copy to File** button on the lower-right corner of the window.

e. Use the Certificate Export Wizard to save the CA certificate in a file.

   Note: You can save the CA certificate in either DER Encoded Binary X-509 format or Based-64 Encoded X-509 format.

Adding the certificate to a Java keystore

Because FIT is built in Java, the CA certificate must be added to a Java keystore using keytool.exe. This can be found in the \bin subdirectory of your Java installation. If you do not know where Java is installed, you can go to Admin Menu->Advanced->System Info->System Properties tab in FIT, and check the sun.boot.library.path property.

1. Select **Start -> Run…** and type `cmd` to open up a command prompt.
2. Enter the following command (modify paths as needed and replace "ActiveDirectory.cer" with the name of the certificate that was exported from Active Directory above):

```
C:/Program Files/FIT/jre/bin/keytool -importcert –trustcacerts -
keystore C:/Program Files/FIT/FIT.ks -file C:/Program
Files/FIT/ActiveDirectory.cer
```

Updating the ldap.cfg file

Open the ldap.cfg file found in the FIT installation directory and add the following lines:

```
### ActiveDirectory SSL
java.naming.security.protocol,ssl
java.naming.referral,follow
javax.net.ssl.trustStore,fit.ks
```

Next, find the line that looks like the following (should be at the top, line 2):

```
java.naming.provider.url,LDAP://192.168.0.201:389/DC=server2003,DC=alce
atech,DC=com
```

To connect via SSL, change "`LDAP:`" to "`LDAPS:`" and the port number () to 636, as shown below:

```
java.naming.provider.url,LDAPS://192.168.0.201:636/DC=server2003,DC=alc
eatech,DC=com
```

After saving these changes, FIT can be restarted and should be able to connect to Active Directory via SSL.