Configuring SSL on an exacqVision Server for Active Directory/LDAP (Linux)

exacqVision 7.2 and higher:

Check the box labeled "Use SSL" on the "ActiveDirectory/LDAP" configuration page, then press "Apply".

exacqVision prior to 7.2:

This article contains procedures for configuring SSL on exacqVision servers so that you can make Active Directory operations more secure.

There are many ways to generate, install, and manage certificates in order to use SSL, but this document explains one simple option: exporting the trusted root certificate that already exists in your Active Directory domain and installing it on each exacqVision server.

Export Trusted Root Certificate for Your Domain

1. Log in to any Windows workstation that has already been added to your domain. The login account must have at least local admin permissions.
2. Start the **Microsoft Management Console** (mmc.exe).
3. If you haven't already, add the **Certificates** snap-in:

   a) On the File menu, click **Add/Remove Snap-In**.
   b) Select **Certificates** and click **Add**.
   c) When prompted, select the option to manage certificates for your user account (instead of the service or computer account).
   d) Click **Finish**.
   e) Click **OK** to complete this step.
4. Expand **Certificates - Current User** in the left pane.
5. Expand **Trusted Root Certification Authorities**.
6. Select the **Certficates** folder to display your workstation's currently installed CA certificates. The **Issued To** field should contain something similar to *mydomain-ROOT-CA*, where *mydomain* is your domain name.
7. Select that **Issued To** entry, right-click **All Tasks**, and select **Export**.
8. In the **Certificate Export Wizard**, select the format choice of **Base-64 encoded binary X.509 (.CER)**. Save it to a local .cer file that you can relocate later. You will

then install this same certificate file on every exacqVision Server for which you intend to use SSL.

Certificate Database Location on exacqVision Server

Whenever exacqVision Server attempts to connect to an Active Directory server, it creates the following files in the installation directory, if necessary:

cert8.db
key3.db
secmod.db

Import Trusted Root Certificate into Each exacqVision Server

1. On the exacqVision server, copy your trusted root certificate to the server's installation directory at **/usr/local/exacq/server**.
2. If you have not already verified your exacqVision Server's LDAP configuration with SSL disabled, do this now. This will create your certificate database files if they do not exist already.
3. Open a Terminal window and type the following:

   sudo openssl s_client -connect **FQDN**:636 -ssl3 | sed -ne "/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p" > ad.pem && sudo mv ad.pem /usr/local/exacq/server

   where **FQDN** is the fully qualified domain name of your Domain Controller.
4. Press **Enter** twice to create the .pem file and move it to the **Servers** directory.
5. Change to the exacqVision server's directory with

   cd /usr/local/exacq/server
6. Run the following two commands:

   sudo certutil -d . -A -t "C,C,C" -i **MY_CERT_FILE** -n adca

   where **MY_CERT_FILE** represents your trusted root certificate file; and

   sudo certutil -d . -A -t "u,u,u" -i ad.pem -n ad
7. In a Terminal window, restart your exacqVision server with the following command:

   sudo service edvrserver restart
8. On your exacqVision server, run exacqVision Client and open the **Active Directory/LDAP** tab. Select the **SSL** checkbox (the port should automatically change to 636), and then click **Apply**. Your exacqVision Server should then reconnect to your Active Directory domain controller.