How to Configure HTTPS for AXIS

Task 1: Configure all Aimetis services to log on with user other than Local System Account

Important: You can bypass all of the steps in Task 1 and configure user on a per service basis for each added camera. See “Configure all Aimetis Services to log on using an account other than “Local System Account”” on page 3.

1. Assign Windows permission to log on as a service.
   a. In Windows 7, from the Start menu, open Control Panel. Select Administrative Tools.
   b. Select Local Security Policy and then Local Policies.
   c. Select User Rights Assignments.
   d. Add a Windows administrator user to the Log on as a service policy group.
   e. Grant the Windows user account access to IIS directories. At command line, type:
      ```
      CD C:\Windows\Microsoft.NET\Framework\v2.0.50727
      aspnet_regiis.exe -ga <computer name>\<username>
      ```
   2. Start Symphony Client and create password that will be required later.
      a. From the Server menu, select User Configuration. The User Configuration dialog box opens.
      b. In the left pane, click New User. The User Information dialog box opens. By default, the new user is a member of Symphony Users and is designated as a Symphony User Type.
      c. In the User Name field, enter “TempUser.”
      d. In the Password field, enter the same password as your Windows user account that will be used for all Aimetis services to log on under. (This is the password used in step 1d.)
      e. Click OK.
      f. In the command line, type:
         ```
         dupdater "select PasswordHash from [user] where LoginID='TempUser'"
         ```
      g. Copy the password hash.
      h. In Symphony Client, delete the TempUser you created: From the Server menu, select User Configuration. The User Configuration dialog box opens. Select the TempUser name and click Remove User. Click OK when prompted to delete user.

3. Start Symphony Client and configure all Aimetis Services to log on with a specific Windows account.
   a. From the Server menu, select Manual Configuration Editor.
b. Click the **Add a new setting...** field. In the blank field under the **Type**, **Section**, **Key**, and **Value** columns, enter **Global**, **Main**, **ServiceUsername**, and `.\<username>`, respectively, where the `<username>` is the Windows User account that had Admin and **Log on as service** permissions, as used in step 1d.

c. Click **Add a new setting...** again. In the blank field under the **Type**, **Section**, **Key**, and **Value** columns, enter **Global**, **Main**, **ServicePassword**, and `<password>`, respectively, where the `<password>` is the password that was generated earlier.

d. Click **OK**.

e. Wait for all Aimetis services to reconfigure and for Symphony Client to reconnect.

---

**Note:** If Aimetis Services do not start and “Error 1069: The service did not start do to a logon Failure” message is displayed, the username and password is wrong.

1. In **Windows Services Manager**, find **AI InfoService** and right click.
2. Select **Properties**, **Log On** tab, and then select (enable) the **Local System account** option.
3. Select the **Allow service to interact with desktop** check box.
4. Click **OK**.
5. Repeat this with **Al Scheduler** service to regain Symphony client’s connection with the server.
6. Redo the steps to ensure you use the right password hash instead of plain text.
7. If the **ServiceUsername** and **ServicePassword** keys are already present in **Manual Configuration Editor**, simply modify the **Values** instead of adding a new setting.

---

**Task 2: Configure AXIS camera for HTTPS**

1. On your AXIS Camera Web interface, click **Setup**, **System Options**, **Security**, and then **HTTPS**. You will see a message similar to the following. Read it carefully and follow instructions.

   **HTTPS Settings**
   - To enable HTTPS, create either a self-signed certificate, or create a request for a certificate from a Certificate Authority (CA.)

   Although a self-signed certificate is useful for initially testing HTTPS, true security will only be implemented after the installation of a signed certificate issued by a certificate authority. The HTTPS Connection Policy must also be set to enable HTTPS on this server.
2. A self-signed certificate is not a trusted certificated. If you create a self-signed certificate on your AXIS camera, then you must:

   **Step 1:** Install the self-signed certificate through IE to be trusted.
   a. Start IE and navigate to https://<camera ip>. If the certificate is self-signed IE will display the following message: “There is a problem with this website’s security certificate”.
   b. Click **Continue to this website (not recommended)**.
   c. Follow instructions and click **Place all certificates in the following store**.
   d. **Browse** to the **Trusted Root Certification Authorities** folder and click **OK**.

   **Step 2:** Disable peer verification in Symphony Client later in this setup process

**Task 3: Add the camera in Symphony Client**

1. If in the AXIS camera HTTPS settings, you had selected to accept only HTTPS connection (and not HTTP & HTTPS), AND you selected self-signed certificate on the AXIS camera setup, you must disable peer verification:
   a. In Symphony Client, from the **Server** menu, select **Manual Configuration Editor**.
   b. Click the **Add a new setting...** field. In the blank field under the **Type**, **Section**, **ID**, **Key**, and **Value** columns, enter **Server**, HTTPS, 5000, and VerifyPeer, and 0, respectively.
   c. Restart **AI InfoService**. This ensures that the setting is loaded.

2. From the **Server** menu, select **Configuration**. The **Configuration** dialog box appears with **Devices** displayed in the right pane.

3. In the right pane, click **New**. The **Network** tab appears.

4. In the **URL** field, enter an IP address of the camera.

5. From the **Manufacturer** list, select **AXIS**.

6. Click **Connect to Camera** and click **OK**.

**Task 4: Configure all Aimetis Services to log on using an account other than “Local System Account”**

---

**Important:** If you have configured all Aimetis services to log on with an account other than “Local System account”, then omit this task.

---

AXIS Media Parser SDK (AMP) does not work with HTTPS when used from a Windows Service process. You must configure Aimetis Services to log on using an account other than “Local System account.”

1. From the **Start** menu, open **Control Panel**. Select **Administrative Tools**.
2. Select **Services**.
3. For each Aimetis service that starts with **AI**, right-click and select **Properties**.
4. Click the **Log On** tab.
5. Select the **This account** option.
6. Enter username and password and click **OK**.
Task 5: Self-signed Certificate

If you selected self-signed certificate on the AXIS camera setup, then you must disable peer verification in Symphony Client.

1. In Symphony Client, from the Server menu, select Manual Configuration Editor.
2. Expand Type: Camera.
3. For all your cameras that are HTTPS, find the camera ID in the list.
4. Under the Key column, find dev_options.
5. In the Value field of that row, append VerifyPeer=0; (at the end of the field).
6. Click OK.

Task 6: Restart AI Tracker Services

Video should be available now over HTTPS.