Disable SSL Encryption for your MySQL Database

This section is applicable only for the MySQL database if you have enabled SSL encryption for the MySQL database in version 6.5 SP1 and above. Unless you disable SSL encryption settings, the RiskVision Upgrade Setup will not upgrade to a newer version of RiskVision.

To disable SSL encryption:

1. Check to see if the my.ini file in the %AGILIANCE_HOME%\MySQL\config directory is backed up. If not, see Backing up the RiskVision Server Configuration for more details.
2. Go to the %AGILIANCE_HOME%\MySQL\config directory. Open the my.ini file by using a text editor, locate the Client and Server sections in the my.ini file, and comment the lines shown below in the respective sections.
    - Client Section
        - `ssl-ca="~/ca-cert.pem"`
        - `ssl-cert="~/client-cert.pem"`
        - `ssl-key="~/client-key.pem"`
        - `ssl-cipher=DHE-RSA-AES256-SHA`
    - Server Section
        - `ssl-ca="~/ca-cert.pem"`
        - `ssl-cert="~/server-cert.pem"`
        - `ssl-key="~/server-key.pem"`
        - `ssl-cipher=DHE-RSA-AES256-SHA`

    Where, "~" denotes certificate's directory.
3. Go to the directory `%AGILIANCE_HOME%\config`. Open the agiliance.properties file by using a text editor, comment the property `database.mysql.useSSL=true` and specify the database hostname in the file.
4. Connect to the MySQL database and run the following commands to disable the SSL encryption:

    `GRANT USAGE ON` `agiliance` `.* TO '` `agiliance` `'@' REQUIRE NONE;`

    `GRANT USAGE ON` `agiliance` `.* TO '` `reportuser` `'@' REQUIRE NONE;`

    `FLUSH PRIVILEGES;`
5. Restart the RiskVision Tomcat and RiskVision MySQL services to apply the latest changes.