Install an SSL Certificate on the JasperReports Server

JasperReports Server includes a self-signed Secure Sockets Layer (SSL) certificate to ensure a safe, secure, and reliable connection. You can access the JasperReports Server using web services over HTTPS or HTTP.

Note: Since you can set up Jaspersoft reports or dashboards in the RiskVision user interface, you must also be able to access the JasperReports Server repository from the RiskVision application.

To install a third-party SSL certificate:

1. Copy the server.crt file to the `%Agiliance_HOME%\apache2\conf directory.`

2. Navigate to the working directory with the following command:

   ```
   > cd %JAVA_HOME%/ jre /bin
   ```

3. Run the following command to import the SSL certificate:

   ```
   > keytool -import -alias
   server. crt - keystore ../lib/security/ cacerts -file
   %Agiliance_HOME%\apache2\conf\server.crt
   ```

4. When the commands are successfully executed, enter the default password changeit. (Optional) Verify the success of the import by running the following command:

   ```
   > keytool -list - keystore ..\lib\security\cacerts -alias server.crt
   ```

Once the certificate is installed, HTTPS is used for communication between the JasperReports Server and the RiskVision Server. But, if you need to connect the JasperReports Server over HTTP, you must make the following changes to the `agiliance.properties` file, available in the `%AGILIANCE_HOME%\config` directory:

- Enable the property `jasper.use.secure.connection=false`

- Enable the `jasper.admin.port=8480` property

Also, change the property `riskvision` `.host.ipaddress=` to the file `agiliance` `.properties`, available in the directory `%JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF`.

There are times when users run Jaspersoft reports within RiskVision, such as when using the RiskVision Contextual Reporting feature and when running a Jasper report attached to a RiskVision tab. The communication of the available Jasper reports to the RiskVision UI relies on a REST API.

The REST web service fetches the list of reports from the JasperReports Server to RiskVision when the user selects the Analytics report picker. By default, the REST web service uses a secure connection but does not validate the SSL certificate. If you want to force the Jasper REST web services to use an HTTPS connection, then you can set the property and `jasper.api.SSLcertificate.validation=true` install an SSL certificate. The default value of the property is false.

You need to use a fully qualified server name while using the secure connection to display the reports based on user's permissions.