File Encryption

There are two types of files that RiskVision encrypts:

- Files that have been uploaded to RiskVision (e.g. questionnaire evidence, files added to the document repository, and attachments to entities, tickets, etc.); and
- Any reports archived using the R6 Reporting engine.

If the RiskVision Server is running any version that is 8.5 GA or higher, the above files will be automatically encrypted using AES 256 bit encryption. However, it is possible that some installations have disabled automatic encryption or chose to opt out during the upgrade. If this has happened, the server's encryption can be re-enabled.

Re-enabling automatic encryption will encrypt all files in the following folders:

- **%RISKVISION_HOME%\data\attachments**
- **%RISKVISION_HOME%\data\reports**
- **%RISKVISION_HOME%\data\dashboards**

Once automatic encryption has been re-enabled, all future files in the above folders will be encrypted. However, in order to encrypt existing files, the encryption utility to encrypt existing files must be run again. The below steps will show both how to re-enable automatic encryption and how to run the utility. If automatic encryption were to be disabled for any reason, all files in the above folders would lose their encryption.

These steps will only work for RiskVision version 9.5 or higher.

To re-enable automatic file encryption:

1. Navigate to **C:\Server\config**.
2. Open the **agiliance.properties** file.
3. Change the following properties as shown:
    - `Attachment.EncryptionEnabled=true`
    - `Attachment.newVersion=true`
4. Copy the **esapi** folder from **C:\AGILIANCE_HOME\Tomcat\webapps\spc\WEB-INF\classes** and paste it into **C:\AGILIANCE_HOME\install\toolbox\bin**.

To encrypt existing files:

1. Navigate to the **AGILIANCE_HOME\install\toolbox\bin** folder.
2. Run the following commands:
    - `encrypt_attachment_directory.cmd > attachment.log`
    - `encrypt_data_directory.cmd > data.log`