Keystore Password Encryption for Jasper Report Server

RiskVision provides a default encryption key. You can change it into a unique encryption key by following the below steps.

To enable keystore password encryption for the JasperReports Server and Connector Manager:

Copy the agiliance.keystore file from RiskVision server side to the following locations:

1. %JASPER_HOME%\Agiliance
2. %JASPER_HOME%\Agiliance\config
3. %ConnectorManager_Home%\ConnectorManager\config

Encryption

To encrypt using a keystore based password, you will have to set the `PBEPassword.disableKeyStoreBasedPwd=false` in the agiliance.properties file. **encrypt.cmd** is a command line utility for encrypting strings such as those in properties files.

To use a keystore based password:

Set the following property as false `PBEPassword.disableKeyStoreBasedPwd=false` in the agiliance.properties file in the following locations:

1. %AGILAINCE_HOME%\config if run from RiskVision side.
2. %JASPER_HOME%\apache-tomcat\webapps\jasperserver-pro\WEB-INF and copy this agiliance.properties file in %JASPER_HOME%\Agiliance\config.
3. %ConnectorManager_Home%\ConnectorManager\config, if run from connector side.

> ℹ The PBEPassword.disableKeyStoreBasedPwd is only needed for encryption. However it's good practice to have all the properties files in synchronization for PBEPassword.disableKeyStoreBasedPwd, even if you don't encrypt from that location.

Decryption

The code automatically detects what type of password was used in encryption, either hardcoded or keystore based. You do not need to set `PBEPassword.disableKeyStoreBasedPwd` for decryption. Nonetheless, you should keep the property the same across all locations to avoid confusion and accidental errors, such as accidentally runing encrypt.cmd with the wrong setting.