Configure RiskVision Server to Use Kerberos AES 256 Bit Encryption

Configure the following files specific to the RiskVision Tomcat Application Server:

- applicationContext-kerberos.xml
- agiliance.default.application.properties

applicationContext-kerberos.xml

Go to the `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF` directory and open the `applicationContext-` `kerberos` `.` `xml` file by using a text editor and perform the following changes:

1. Uncomment all the lines in-between start Kerberos configuration and end Kerberos configuration.
2. By default, the Kerberos debugging is enabled. To disable the debugging, set the following property to false:

   `class="org.springframework.security.extensions.kerberos.GlobalSunJaasKerberosConfig">`

agiliance.default. application.properties

Go to the `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes` directory, open the **agilaince.default.application.properties** file by using a text editor and then perform the following changes:

`kerberos.host=`

Make sure that `RiskVisionWebServer_Hostname` is in lowercase.

Using the property above helps LDAP users to access the RiskVision application using Kerberos SSO.

`password.disableAfterNFailedLogin=`

By default, the value is '0', which signifies that the policy is not enforced.

1. **serviceprincipal**

   Specify the Service Principal Name that was configured on the Active Directory for the RiskVision hostname. Only one SPN is allowed per domain and only one SPN is required for a hostname.

   `serviceprincipal=@`

2. **keytab.file**

   Specify the location of .keytab file in RiskVision Server which was generated in the active directory.

   `keytab.file=file:`

   Any changes to SPN or .keytab file requires restarting the RiskVision Tomcat service.

3. Specify the RiskVision Web Server hostname, provided during the .generation of .keytab file in the following property:

4. Set the following property to true. Add the property if it does not exist.

```
authentication.allow.kerberos=true
```

5. Specify another hostname of RiskVision Web Server, to allow vendors and internal users to access RiskVision application using credentials.

   ```
   virtual.host=
   ```

6. Use the following property to specify the number of attempts a user can make while logging into RiskVision. A user is disabled after all the attempts are exhausted.

After you finish configuring the settings, restart the RiskVision Tomcat to show the latest changes.

RiskVision strongly recommends copying the properties above to the `%AGILIANCE_HOME%\config\agiliance.properties` file to ensure that Kerberos configuration is intact even after upgrading the RiskVision Server.