Configure the Tomcat for Kerberos Single Sign-On

The following provides instructions for configuring the following files for the RiskVision Tomcat Application Server:

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

applicationContext-kerberos.xml

To configure the applicationContext-kerberos.xml file:

1. Go to %AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF directory and open the applicationContext-kerberos.xml file using a text editor.
2. Uncomment all lines in-between start Kerberos configuration and end Kerberos configuration.
3. By default, Kerberos debugging is enabled. To disable debugging, set the following property to false:

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

agiliance.default. application.properties

To configure the agiliance.default.application.properties file:

1. Go to %AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes directory and open the agilaince.default.application.properties file using a text editor.
2. 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=@`

3. 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.

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

   `kerberos.host=`

   Note: Make sure that `RiskVisionWebServer_Hostname` is in lowercase

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

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

   `authentication.allow.kerberos=true`

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

   `virtual.host=`

7. 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.
   `password.disableAfterNFailedLogin=`
   By default, the value is '0', which signifies that the policy is not enforced.

8. 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 RiskVisionServer.