ADEPTIA

Configure signed SSL Certificate in Adeptia Suite V 5.2

Adeptia Inc.
443 North Clark Ave,
Suite 350
Chicago, IL 60654, USA

Objectives:

This document describes the steps to create a new Keystore within Adeptia and configure the SSL signed certificate in Adeptia Suite V 5.2.

Prerequisites:

1. Access to Adeptia Suite installation directory.
2. Permissions to modify files of Adeptia Suite.
3. Original .jks and .csr files created through Keytool (or any tool for generating jks file).
4. Password of the jks file that was used at the time of creation.
5. Signed certificate (.cer) received from third party against the .csr (certificate signing request) file generated above in step 3.
6. Permission to restart Adeptia Suite when required.

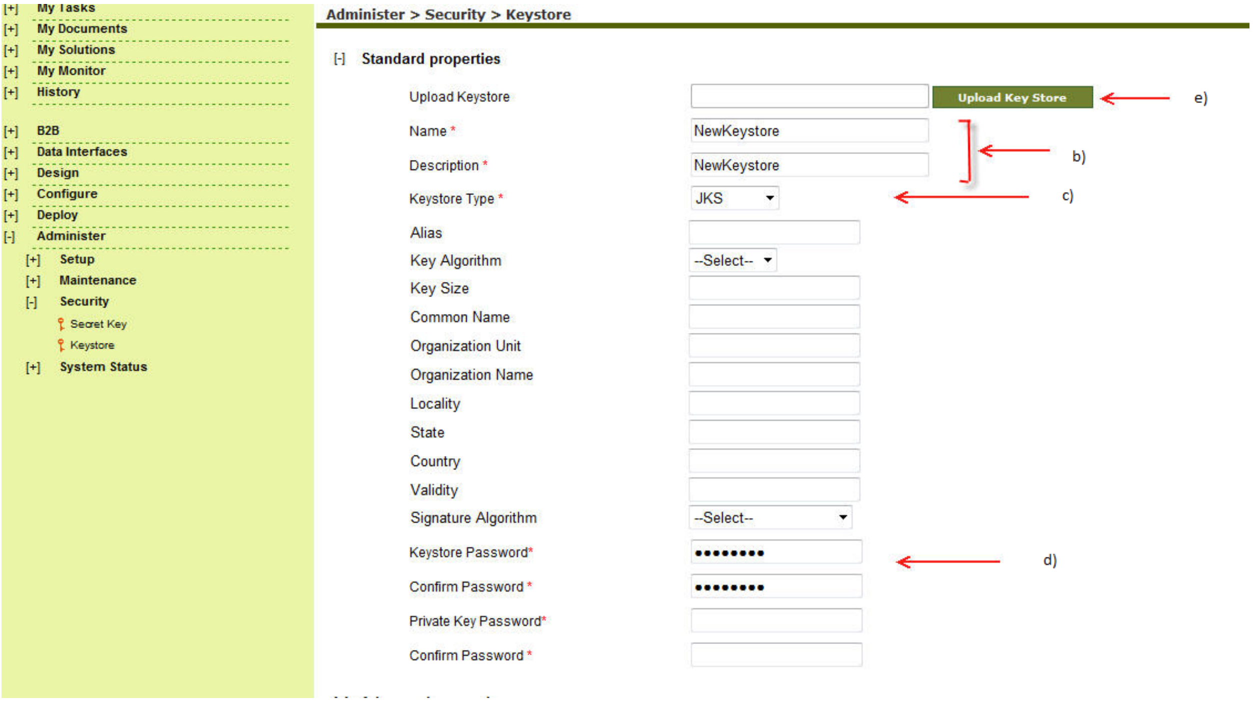
Solution:

Configure Third Party Signed SSL Certificate in Adeptia Suite:

1. Create a new keystore in Adeptia suite using the Original .jks file (refer the screen below):
    a) Goto Administer > Security > Keystore.
    b) Click on 'New' to create a new keystore.
    c) Provide a suitable Name and Description of the keystore.
    d) Select the "keystoretype" from the dropdown list.
    ***Note**: This should match with the keystoretype of the original .jks file*

    e) Provide "keystorePassword" of the keystore that you want to upload.
    ***Note**: Make sure that this password should be same as provided at the time of keystore creation (.jks).*

    f) Click on "UploadKeystore" and upload the original .jks file.
    g) Enter the Private Key Password.
    h) Save this Keystore.



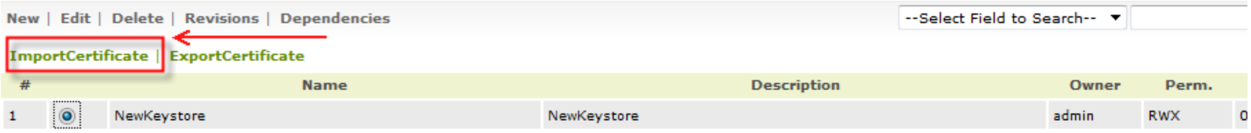
Administer > Security > Keystore

[-] Standard properties

Upload Keystore	
Name *	NewKeystore
Description *	NewKeystore
Keystore Type *	JKS
Alias	
Key Algorithm	--Select--
Key Size	
Common Name	
Organization Unit	
Organization Name	
Locality	
State	
Country	
Validity	
Signature Algorithm	--Select--
Keystore Password*	••••••••
Confirm Password *	••••••••
Private Key Password*	
Confirm Password *	

2. Copy the Alias name (to be used while importing signed certificate)
    a. Goto Administer > Security > Keystore.
    b. Select the keystore created above and click on edit.
    c. Copy the Alias name.
3. Upload signed certificate:-
    a. Goto Administer > Security > Keystore.
    b. Select the keystore created above click on 'ImportCertificate' .
    c. Locate the signed .cer certificate file received from Third Party Vendor.
    d. Provide the Alias name that was copied in step 2-c

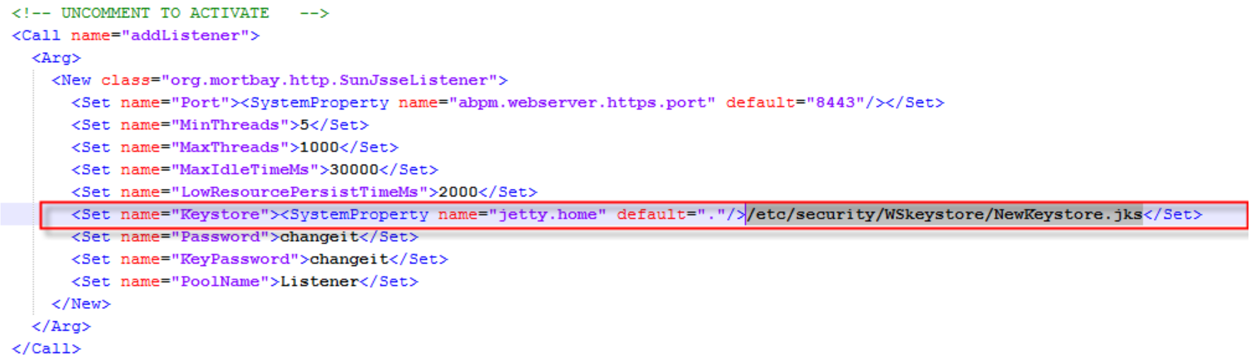
    ***Note**: It is mandatory to provide the same Alias name which appeared while creating the keystore.*



New | Edit | Delete | Revisions | Dependencies
--Select Field to Search--
ImportCertificate | ExportCertificate

#		Name	Description	Owner	Perm.	
1	●	NewKeystore	NewKeystore	admin	RWX	0

4. Register the keystore entry in config.xml file of Adeptia Suite that is located in \..\AdeptiaServer-5.2\ServerKernel\etc\jetty.
    a. Open config.xml in text editor text as shown below:.
    b. Provide the path of the keystore created above.



```
<!-- UNCOMMENT TO ACTIVATE   -->
<Call name="addListener">
  <Arg>
    <New class="org.mortbay.http.SunJsseListener">
      <Set name="Port"><SystemProperty name="abpm.webserver.https.port" default="8443"/></Set>
      <Set name="MinThreads">5</Set>
      <Set name="MaxThreads">1000</Set>
      <Set name="MaxIdleTimeMs">30000</Set>
      <Set name="LowResourcePersistTimeMs">2000</Set>
      <Set name="Keystore"><SystemProperty name="jetty.home" default="."/>/etc/security/WSkeystore/NewKeystore.jks</Set>
      <Set name="Password">changeit</Set>
      <Set name="KeyPassword">changeit</Set>
      <Set name="PoolName">Listener</Set>
    </New>
  </Arg>
</Call>
```

    c. Save config.xml file

5. Restart Adeptia Webrunner.