Ellucian: 000046191 - 000046191 - Applications Manager 9.3 - Steps to create a self signed ssl certificate (Click here to view Article in the Support Center)

000046191 - Applications Manager 9.3 - Steps to create a self signed ssl certificate

In Applications Manager 9.3, a custom ssl certificate must be used when using java versions 1.8.0_201 (and higher) as well as with OpenJDK 11.0.2 (and higher)

This snippet comes from the 9.3 Release Notes:
================================

Custom SSL Certificates for Connection Authentication Now Required
You must use a custom SSL certificate for connection authentication by creating user_keystore and user_keystore_config files on the Automation Engine and client machines. For more information, see Using Custom SSL Certificates for Connection Authentication in the *Installation Guide.*
================================

SPECIAL NOTE REGARDING SIGNED CERTIFICATES. In versions 9.3.0 - 9.3.2, you can use a signed certificate from a certificate authority, which can be imported into the user_keystore. Using a signed certificate eliminates the need to copy the user_keystore files to end user pc's and remote agents. However, : in 9.3.3 and 9.3.3+hf1, only self signed certificates work. We will publish more information here once it is available from Broadcom.

==================================
Example Steps to create a self signed user_keystore.
Change values in this example as desired.
NOTE: When creating the keystore using OpenJDK 11 (this test was with 11.0.5), you must include the -keyalg RSA parameter.   Be sure to use the applicable keytool line noted below.

==========
UNIX/LINUX
==========

1. Create user_keystore
    (the validity represents the # of days until expiration. For example -validity 1095 for 3 years or -validity 3650 for 10 years.)
cd $AW_HOME/data
keytool -keystore user_keystore -genkey -alias automic -validity 1095   <------ use this keytool line if Java 8, specifically 1.8.0_201 or higher
keytool -keyalg RSA -keystore user_keystore -genkey -alias automic -validity 1095 <-------   use this keytool line if OpenJDK 11.0.2 or higher
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]: Ellucian
What is the name of your organizational unit?
  [Unknown]: Support
What is the name of your organization?
  [Unknown]: Ellucian
What is the name of your City or Locality?
  [Unknown]: Malvern
What is the name of your State or Province?
  [Unknown]: PA
What is the two-letter country code for this unit?
  [Unknown]: US
Is CN=Ellucian, OU=Support, O=Ellucian, L=Malvern, ST=PA, C=US correct?
  [no]: yes

Enter key password for <automic>
      (RETURN if same as keystore password):

2. confirm that file is created
ls -l user_keystore

-rw-r--r-- 1 appmgr dba 2577 Nov 4 16:13 user_keystore

3. Create the file user_keystore_config and add the password in plain text
echo 'u_pick_it' >user_keystore_config

4. Confirm that the password is correct
cat user_keystore_config
u_pick_it

5. Encrypt the user_keystore_config file:
cd $AW_HOME/web/classes
java -DAW_HOME=${AW_HOME} -cp AppWorx.jar:uc4-ra.jar com.appworx.util.EncryptKeystoreFile u_pick_it

6. You should see a new timestamp on the file:
ls -l user_keystore_config
-rw-r--r-- 1 ban9js dba   28 Nov 4 16:33 user_keystore_config

7. Confirm that the password is encrypted
more user_keystore_config
ENC:TzgHOCKB6SmISxPahgkJpQ==

8. *Stop and restart the Applications Manager processes* (stopso awcomm, followed by startso) and confirm the processes are running with this command:
awexe node

9. *If you have remote agents,* the user_keystore and user_keystore_config files must also be copied to the remote agent(s) data directory ($AW_HOME/data or %AW_HOME%\data)

10. *The self signed user_keystore and user_keystore_config files must be copied to all end user pc's*
Version 9.3 did not allow for multiple keystore files. One keystore had to be used for all masters. Starting with version 9.3.1, you can have multiple keystore files.

If you have one set of user_keystore and user_keystore_config files, copy them to C:\users\<username>\.Appworx directory

If you have multiple sets of keystore files (and are on minimum version 9.3.1)
- create a C:\Users\<user name>\AppWorx\<master name> folder for each master, like this example for AMTEST and AMPROD masters:
      C:\Users\<user name>\AppWorx\AMTEST
      C:\Users\<user name>\AppWorx\AMPROD
      (** This is NOT under the .AppWorx directory)
- Copy the respective user_keystore and user_keystore_config files to the sub-directory for each master.

NOTE: If you make a mistake and need to start over, delete the $AW_HOME/data/user_keystore* files and re-do the steps.

=========
WINDOWS
=========

1. Create user_keystore
cd %AW_HOME%\data
keytool -keystore user_keystore -genkey -alias automic   <------- use this keytool line if Java 8, specifically 1.8.0_201 or higher
keytool -keyalg RSA -keystore user_keystore -genkey -alias automic   <-------   use this keytool line if OpenJDK

11.0.2 or higher
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]: Ellucian
What is the name of your organizational unit?
  [Unknown]: Support
What is the name of your organization?
  [Unknown]: Ellucian
What is the name of your City or Locality?
  [Unknown]: Malvern
What is the name of your State or Province?
  [Unknown]: PA
What is the two-letter country code for this unit?
  [Unknown]: US
Is CN=Ellucian, OU=Support, O=Ellucian, L=Malvern, ST=PA, C=US correct?
  [no]: yes

Enter key password for <automic>
      (RETURN if same as keystore password):

2. confirm that file is created
dir user_keystore

10/25/2019 12:45 PM   2,577 user_keystore

3. Create the file user_keystore_config and put in the password in plain text
echo 'u_pick_it' >user_keystore_config

4. Confirm that the password is correct
cat user_keystore_config
u_pick_it

5. Encrypt the user_keystore_config file:
cd %AW_HOME%\web\classes
java -DAW_HOME=${AW_HOME} -cp AppWorx.jar;uc4-ra.jar com.appworx.util.EncryptKeystoreFile u_pick_it

6. You should see a new timestamp on the file:
dir user_keystore_config
10/25/2019 12:50 PM   28 user_keystore_config

7. Confirm that the password is encrypted
more user_keystore_config
ENC:TzgHOCKB6SmISxPahgkJpQ==

8. Stop and restart the Applications Manager processes (stopso awcomm, followed by startso) and confirm the processes are running with this command:
awexe node

9. The user_keystore and user_keystore_config files must also be copied to the remote agent(s) data directory ($AW_HOME/data or %AW_HOME%\data)

10. The self signed user_keystore and user_keystore_config files must be copied to all end user pc's
Version 9.3 did not allow for multiple keystore files. One keystore had to be used for all masters. Starting with version 9.3.1, you can have multiple keystore files.

If you have one set of user_keystore and user_keystore_config files, copy them to C:\users\<username>\.Appworx directory

If you have multiple sets of keystore files (and are on 9.3.1)
- create a C:\Users\<user name>\AppWorx\<master name> folder for each master, like this example for AMTEST and AMPROD masters:

C:\Users\
C:\Users\
(** This is NOT under the .AppWorx directory)
- Copy the respective user_keystore and user_keystore_config files to the sub-directory for each master.

NOTE: If you make a mistake and need to start over, delete the %AW_HOME%\data\user_keystore* files and re-do the steps.

Related Articles:
[000046205 - Applications Manager not starting after creating user_keystore files - RmiServer.log java.security.NoSuchAlgorithmException: Error constructing implementation](#)

===============
lstevens 11/6/2019
updated 2/9/2021

Type : Solution

===

 First Published : 2019-11-06 19:53:45
 Last Modified : 2021-02-09 19:02:59
 Last Published : 2021-02-09 19:02:59
 Article Number : 000046191
 Product Line: Automic
 Product: Automic Enterprise Scheduler Package

Please Click on File Name to Download.

===