IBM

WebSphere Application Server

9.0.5

Integration Guide

CryptoServer HSM

SecurityServer v4.51.0.1

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-03-16
Status	PUBLISHED
Document No.	IG-2026-0014

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle.

All Utimaco SecurityServer product documentation is available from Utimaco's website at https://utimaco.com/.

1.1 About This Guide

This guide describes how to integrate an Utimaco CryptoServer Hardware Security Module (HSM) with IBM WebSphere Application Server. Utimaco HSM securely generates and stores the private key and certificate used by IBM WebSphere Application Server for SSL.

1.1.1 Target Audience for This Guide

This guide is intended for IBM WebSphere Application Server and Utimaco HSM administrators.

1.1.2 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

Table 1: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

1.1.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
CA	Certificate Authority
CSADM	CryptoServer Command-line Administration Tool
CSR	Certificate Signing Request
EC	Elliptic Curve
GUI	Graphical User Interface
HSM	Hardware Security Module
IBM	International Business Machines

Abbreviation	Meaning
IP	Internet Protocol
JCA	Java Cryptography Architecture
JCE	Java™ Cryptography Extension
JDK	Java Development Kit
LAN	Local Area Network
MBK	Master Backup Key
PCIe	PCI Express Interface
PIN	Personal Identification number
PKCS#11	Public-Key Cryptography Standard #11
RSA	Rivest-Shamir-Adleman
SSL	Secure Sockets Layer
SO	Security Officer
URL	Uniform Resource Locator
VM	Virtual Machine

Table 2: List of abbreviations

2 Overview

2.1 IBM WebSphere Application Server

IBM WebSphere Application Server is a flexible, secure Java server runtime environment for enterprise applications. Deploy and manage applications and services regardless of time, location, or device type. Integrated management and administrative tools provide enhanced security and control, and support for multi-cloud environments lets you choose your deployment method. IBM WebSphere Application Server has continuous delivery capabilities and services that helps you to respond at the speed of your business needs.

2.2 Utimaco SecurityServer HSM

SecurityServer is a hardware security module developed by Utimaco IS GmbH. SecurityServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Integration Requirements and Prerequisites

Ensure the system environment you will be using meets the following hardware and software requirements.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with IBM WebSphere Application Server.

Operating System	IBM WebSphere Application Server	Utimaco Security Server Version	Utimaco HSM
RHEL 8	9.0.5	SecurityServer V4.51.0.1	CryptoServer CSe-Series/Se-Series
Windows Server 2019	9.0.5	SecurityServer V4.51.0.1	CryptoServer CSe-Series/Se-Series

Table 3: List of tested versions

3.2 Software Requirements

Software	Software Requirements
IBM WebSphere Application Server	9.0.5
IBM JDK 8	1.8.0_361
HSM Interfaces	SecurityServer PKCS#11

Software	Software Requirements
Host VM	RHEL 8 and Windows 2019 server
HSM Software	Utimaco SecurityServer Software 4.51.0.1
P11tool2	p11tool2 (3.1.1) from product package Utimaco SecurityServer 4.51.0.1

Table 4: List of software requirements

Here you find additional notes or supplementary information. To download IBM java: https://developer.ibm.com/languages/java/semeru-runtimes/downloads/.

3.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.51.0.1 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.51.0.1 or higher

Table 5: List of hardware requirements

Setup an account on the Utimaco support portal and request download access at the following URL: https://support.hsm.utimaco.com/.

3.4 Prerequisites

Before you begin, please ensure that you have:

- SecurityServer setup and configured. Refer to the SecurityServer documentation to set up the HSM.
- Replaced the SecurityServer Default Admin with a new admin user.
- Created and stored the MBK onto each HSM. Refer to the SecurityServer documentation to set up the MBK.
- The operating system listed in Tested Versions.
- The SecurityServer version listed in Tested Versions.
- Familiarized yourself with the IBM WebSphere Application Server documents and setup process.
- The admin user for installing software on IBM WebSphere Application Server set up.
- Allowed port 9043 through the firewall.

4 Installing and Configuring Utimaco SecurityServer Software

4.1 On Linux

4.1.1 Download and Install Utimaco Software

If you have not already done so, please create and request an Utimaco Support Portal Account. This will allow you to download the software components needed for this installation.

1. Copy the downloaded software at the appropriate location on the IBM WebSphere Application Server.
2. Create utimaco folder under /opt directory and further create 2 directories: /opt/utimaco/bin and /opt/utimaco/lib.

›_ Console

```
# mkdir -p /opt/utimaco/bin

# mkdir /opt/utimaco/lib
```

3. Copy pkcs11 library file libcs_pkcs11_R3.so from Utimaco SecurityServer software to the /opt/utimaco/lib directory.

›_ Console

```
# cp ~/path_to_application_folder/lib/libcs_pkcs11_R3.so /opt/utimaco/lib
```

4. Copy the csadm and p11tool2 files from Utimaco SecurityServer software to /opt/utimaco/bin directory and make both the files executable.

›_ Console

```
# cd ~/path_to_application_folder

# cp csadm p11tool2 /opt/utimaco/bin

# chmod +x /opt/utimaco/bin/csadm /opt/utimaco/bin/p11tool2
```

4.1.2 SecurityServer PKCS#11 Configuration

1. Create the directory /etc/utimaco. Locate the Utimaco PKCS#11 configuration file in your SecurityServer directory, Linux/x86-64/Crypto_APIS/PKCS11_R3/sample. Copy the Utimaco PKCS#11 configuration file cs_pkcs11_R3.cfg into /etc/utimaco directory.

›_ Console

```
# mkdir /etc/utimaco
# cd <install directory>/Software/Linux/x86-64/Crypto_APIs/PKCS11_R3/sample
# cp cs_pkcs11_R3.cfg /etc/utimaco
# cd /etc/utimaco
```

2. Edit the cs_pkcs11_R3.cfg file and make the appropriate changes to the file.

cs_pkcs11_R3.cfg

```
[Global]
# For unix:
Logpath = /tmp
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1
Keepalive = true
# Set the Device to connect with
[CryptoServer]
# Device specifier
Device = <HSM_IP>
```

For more information regarding the commands and command parameters please check the Utimaco CryptoServer documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor: **Device = 288@<HSM IP address>** Hardware (LAN) HSM

OR

Device = /dev/cs2.0 Hardware (PCIe) HSM

To make your testing easier, it would be good to enable the PKCS#11 log file. That can be enabled by editing the **Logging** Loglevel. Set the **LogPath** and Logging **Loglevel** to **1**. For testing you may want to increase it to **4**.

The added **LogPath** points to a writable directory, not to a file.

If you encounter problems, check the log file named **cs_pkcs11_R3.log** in the **LogPath** defined directory. When you are done testing, you should change **Logging** to **1** or **2**. This will limit the logging to only critical and important messages.

4.1.3 Create SO User and Initialize a Slot

You must initialize a slot with a custom label using p11tool2.

First using p11tool2 create, the SO or Security Officer and then using p11tool2 command initialize the Slot that you want to use, and the slot user as shown below.

›_ Console

```
# ./p11tool2 slot=<slot_no> Label=<token_label> Login=ADMIN,ADMIN.key
InitToken=<ask>

# ./p11tool2 slot=<slot_no> LoginSO=<ask> InitPin=<ask>
```

```
[root@hj-ibmibm16959 bin]# ./p11tool2 slot=0 Label=IBM Login=ADMIN,ADMIN.key InitToken=ask
Enter SO PIN:
Repeat SO PIN:
```

Figure 1 : Slot initialization output

```
[root@hj-ibmibm16959 bin]# ./p11tool2 slot=0 LoginSO=ask InitPin=ask
Enter SO PIN:
Enter normal user PIN:
Repeat normal user PIN:
```

4.1.4 Create pkcs11.cfg at /etc/utimaco/

Create a file /etc/utimaco/pkcs11.cfg and add below contents to it.

pkcs11.cfg

```
name=CryptoServer
library= C:\\Program Files\\Utimaco\\SecurityServer\\Lib\\cs_pkcs11_R3.dll
slotListIndex=0
publickeyimportonly = true
attributes(*, CKO_SECRET_KEY, *) = {
   CKA_ENCRYPT=true
   CKA_DECRYPT=true}
attributes(GENERATE, CKO_PRIVATE_KEY,
   CKK_RSA) = { CKA_TOKEN=true
   CKA_DECRYPT=true
   CKA_UNWRAP=true}
attributes(GENERATE, CKO_PUBLIC_KEY, *) = {
   CKA_TOKEN=true CKA_VERIFY=true} attributes(*,
   CKO_PUBLIC_KEY, CKK_RSA) = {
   CKA_ENCRYPT=true
   CKA_WRAP=true
   CKA_VERIFY=true}
attributes(IMPORT, CKO_PRIVATE_KEY, CKK_RSA) = {
   CKA_DECRYPT=true CKA_UNWRAP=true CKA_DERIVE=true}
attributes(*,CKO_PRIVATE_KEY,CKK_EC) = {
   CKA_SIGN=true
   CKA_DERIVE=true
   CKA_TOKEN=true}
```

This file will be used by IBMPKCS11 provider to get library and slot information and perform cryptographic operation on Utimaco HSM.

Specify correct library path and slot index.

4.2 On Windows

On windows, as part of CryptoServer software installation, `cs_pkcs11_R3.cfg` will get automatically created and will be available under the "`C:\ProgramData\Utimaco\PKCS11_R3`" folder.

4.2.1 Update cs_pkcs11_R3.cfg

Example Values:

cs_pkcs11_R3.cfg

```
[Global]
# For windows:
Logpath = C:/ProgramData/Utimaco/PKCS11_R3
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1

# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true

# Set the Device to connect with
[CryptoServer]
# Device specifier
Device = <HSM_IP>
```

For more information regarding the commands and command parameters please check the Utimaco CryptoServer documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

Device = 288@<HSM IP address> Hardware (LAN) HSM

OR

Device = /dev/cs2.0 Hardware (PCIe) HSM

To make your testing easier, it would be good to enable the PKCS#11 log file. That can be enabled by editing the **Logging** Loglevel. Set the **LogPath** and Logging **Loglevel** to **1**. For testing you may want to increase it to **4**.

The added **LogPath** points to a writable directory, not to a file.

If you encounter problems, check the log file named **cs_pkcs11_R3.log** in the **LogPath** defined directory. When you are done testing, you should change Logging to **1** or **2**. This will limit the logging to only critical and important messages.

4.2.2 Create pkcs11.cfg at C:\Program Files\Utimaco\

Create a file C:\Program Files\Utimaco\pkcs11.cfg and add below contents to it.

pkcs11.cfg

```
name=CryptoServer
library= C:\\Program Files\\Utimaco\\SecurityServer\\Lib\\cs_pkcs11_R3.dll
slotListIndex=0
publickeyimportonly = true
attributes(*, CKO_SECRET_KEY, *) = {
   CKA_ENCRYPT=true
   CKA_DECRYPT=true}
attributes(GENERATE, CKO_PRIVATE_KEY, CKK_RSA) = {
   CKA_TOKEN=true
   CKA_DECRYPT=true
   CKA_UNWRAP=true}
attributes(GENERATE, CKO_PUBLIC_KEY, *) = {
   CKA_TOKEN=true
   CKA_VERIFY=true}
attributes(*, CKO_PUBLIC_KEY, CKK_RSA) = {
   CKA_ENCRYPT=true
   CKA_WRAP=true CKA_VERIFY=true}
attributes(IMPORT, CKO_PRIVATE_KEY, CKK_RSA) = {
   CKA_DECRYPT=true CKA_UNWRAP=true
   CKA_DERIVE=true}
attributes(*,CKO_PRIVATE_KEY,CKK_EC) = {
   CKA_SIGN=true
   CKA_DERIVE=true
   CKA_TOKEN=true}
```

This file will be used by IBMPKCS11 provider to get library and slot information and perform cryptographic operation on Utimaco HSM.

Specify correct library path and slot index.

5 IBM JAVA Configuration to Use Utimaco HSM

5.1 Update java.security file to use Utimaco HSM on Linux

1. Go to the <JDK_Installation_directory>/jre/lib/security directory.

›_ Console

```
# cd /opt/IBM/WebSphere/AppServer_1/java/8.0/jre/lib/security/java.security
```

2. Edit the java.security configuration file to add IBMPKCS11Impl provider as highlighted below.

›_ Console

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.plus.provider.IBMJCEPlus
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL
security.provider.7=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.8=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.10=sun.security.provider.Sun
security.provider.11=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /etc/
utimaco/pkcs11.cfg
```

Specify correct provider number and path for pkcs11.cfg file.

5.2 Update java.security file to use Utimaco HSM on Windows

1. Go to the <JDK_Installation_directory>\jre\lib\security directory.

›_ Console

```
# cd C:\Program
Files\IBM\WebSphere\AppServer\java\8.0\jre\lib\security\java.security
```

2. Edit the java.security configuration file to add IBMPKCS11Impl provider as highlighted below.

›_ Console

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.plus.provider.IBMJCEPlus
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL
security.provider.7=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.8=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.10=sun.security.provider.Sun
security.provider.11=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl C:\
\Program Files\\Utimaco\\pkcs11.cfg
```

Specify correct provider number and path for pkcs11.cfg file.

6 Integrating IBM WebSphere Application Server with Utimaco HSM

6.1 Generating SSL Key and Certificate on Linux

6.1.1 For RSA Key and Certificate Generation

1. Generate a keypair on Utimaco HSM with the help of keytool command.

›_ Console

```
# keytool -genkey -alias ibmrsa -keyalg RSA -keysize 2048 -keystore NONE
storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
```

Provide information when prompted.

Here:

- RSA is the key algorithm
- 2048 is the key size
- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider name
- ibmrsa is the key name that will be generated on Utimaco HSM

Provide the keystore password when prompted.

```
[root@hj-ibmibm16959 bin]# ./keytool -genkey -alias ibmrsa -keyalg RSA -keysize 2048 -keystore NONE -storetype PKCS11IMPLKS -pro
vidername IBMPKCS11Impl-CryptoServer
Enter keystore password:
What is your first and last name?
  [Unknown]:  test demo
What is the name of your organizational unit?
  [Unknown]:  security
What is the name of your organization?
  [Unknown]:  utimaco
What is the name of your City or Locality?
  [Unknown]:  pune
What is the name of your State or Province?
  [Unknown]:  mh
What is the two-letter country code for this unit?
  [Unknown]:  in
Is CN=test demo, OU=security, O=utimaco, L=pune, ST=mh, C=in correct? (type "yes" or "no")
  [no]:  yes

Enter key password for <ibmrsa>:
        (RETURN if same as keystore password):
[root@hj-ibmibm16959 bin]#
```

Figure 2 : Key generation using Keytool command

2. Verify the entry with same alias name using keytool command.

›_ Console

```
# keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername
IBMPKCS11Impl-CryptoServer
```

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider's name

Provide the keystore password when prompted.

```
[root@hj-ibmibm16959 bin]# ./keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
Enter keystore password:

Keystore type: PKCS11IMPLKS
Keystore provider: IBMPKCS11Impl-CryptoServer

Your keystore contains 2 entries

ibmrsacert0, null, trustedCertEntry,
Certificate fingerprint (SHA1): 41:AF:6B:B1:D6:CC:B2:B9:55:DA:DC:A5:DC:09:7C:C8:21:8F:15:63
ibmrsa, null, keyEntry,
Certificate fingerprint (SHA1): 41:AF:6B:B1:D6:CC:B2:B9:55:DA:DC:A5:DC:09:7C:C8:21:8F:15:63
[root@hj-ibmibm16959 bin]#
```

Figure 3 : Keytool list output

3. List the objects using p11tool2.

›_ Console

```
# p11tool2 Slot=0 LoginUser=ask ListObjects
```

Enter user PIN when prompted.

```
[root@hj-ibmibm16959 bin]# ./p11tool2 slot=0 loginuser=ask ListObjects
Enter normal user PIN:


CKO_CERTIFICATE:

+ 1.1
  CKA_CERTIFICATE_TYPE          = CKC_X_509
  CKA_UNIQUE_ID                 = 51A90CC7-8F61-4D28-B7FF-972E36B279E7
  CKA_LABEL                     = ibmrsa
  CKA_ID                        =

  CKA_SUBJECT                   =
               0x3062310B 30090603 55040613 02696E31 |0b1 0   U    in1|
                 0B300906 03550408 13026D68 310D300B | 0   U    mh1 0 |
                 06035504 07130470 756E6531 10300E06 |  U    pune1 0  |
                 0355040A 13077574 696D6163 6F311130 | U    utimaco1 0|
                 0F060355 040B1308 73656375 72697479 |   U    security|
                 31123010 06035504 03130974 65737420 |1 0   U    test |
                 64656D6F                            |demo            |



CKO_PUBLIC_KEY:

+ 2.1
  CKA_KEY_TYPE                  = CKK_RSA
  CKA_UNIQUE_ID                 = 24E38F51-06CC-47D0-B53B-B5EBB25CD629
  CKA_LABEL                     =
  CKA_ID                        =
```

Figure 4 : ListObjects output using p11tool2

```
CKO_PRIVATE_KEY:

+ 3.1
  CKA_KEY_TYPE                    = CKK_RSA
  CKA_UNIQUE_ID                   = 9D3101AB-DEC6-4203-B851-D466F7FD3256
  CKA_SENSITIVE                   = CK_TRUE
  CKA_EXTRACTABLE                 = CK_FALSE
  CKA_LABEL                       =
  CKA_ID                          =


+ 3.2
  CKA_KEY_TYPE                    = CKK_RSA
  CKA_UNIQUE_ID                   = E6EF65D0-C6AD-4B0E-814D-430C4A6CF056
  CKA_SENSITIVE                   = CK_TRUE
  CKA_EXTRACTABLE                 = CK_FALSE
  CKA_LABEL                       = ibmrsa
  CKA_ID                          =

[root@hj-ibmibm16959 bin]#
```

4. Generate a CSR using Keytool command.

›_ Console

```
# keytool -certreq -alias ibmrsa -keystore NONE -storetype PKCS11IMPLKS
providername IBMPKCS11Impl-CryptoServer -file ibm.csr
```

```
[root@hj-ibmibm16959 bin]# ./keytool -certreq -alias ibmrsa -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-C
ryptoServer -file ibm.csr
Enter keystore password:
[root@hj-ibmibm16959 bin]#
```

Figure 5 : Generate CSR command output

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider name
- ibmrsa is the key name
- ibm.csr is the CSR file name that will be generated

Provide keystore password when prompted.

5. Get this CSR signed by CA.
6. Copy the signed certificate and root CA certificate on the IBM WebSphere Application Server.
7. Import Root CA certificate into HSM keystore.

```
[root@hj-ibmibm16959 bin]# ./keytool -importcert -alias rootca -file /home/LAbCA-Root.crt -storetype PKCS11IMPLKS -keystore NONE
 -providername IBMPKCS11Impl-CryptoServer
Enter keystore password:
Owner: CN=LabCA-Root, OU=IT, O=security, L=Campbell, ST=Austin, C=US
Issuer: CN=LabCA-Root, OU=IT, O=security, L=Campbell, ST=Austin, C=US
Serial number: 40f8f17a48d0bcc3
Valid from: 11/29/22 11:06 AM until: 11/29/32 11:06 AM
Certificate fingerprints:
         MD5:  80:E7:CE:91:84:D6:E9:D9:03:53:DB:F3:11:84:F3:34
         SHA1: D9:BE:FA:00:CB:52:0E:7F:7B:82:CE:D3:54:02:BB:1F:43:21:B8:A1
         SHA256: 58:E9:C6:A3:12:0D:A9:3A:97:E8:0D:03:06:9B:89:0F:05:E6:EB:1F:46:1C:E8:B1:B6:DF:DE:3E:4D:0B:EC:64
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL CA
   S/MIME CA
   Object Signing CA]

#2: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 0e 49 6e 66 6f 73 65  63 20 4c 61 62 20 43 41  ..Infosec.Lab.CA
```

Figure 6 : Importing root CA certificate into keystore

```
#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 85 42 28 42 84 18 55 2c  73 aa 74 dc 23 ee 74 7a  .B.B..U.s.t.#.tz
0010: 00 fe 2e dc                                       ....
]
]

#5: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[root@hj-ibmibm16959 bin]#
```

Provide keystore password when prompted.

8. Import the signed certificate reply using the command below.

›_ Console

```
#  keytool -importcert -alias ibmrsa -file /home/test_demo.p7b -storetype
PKCS11IMPLKS -keystore NONE -providername IBMPKCS11Impl-CryptoServer
```

```
[root@hj-ibmibm16959 bin]# ./keytool -importcert -alias ibmrsa -file /home/test_demo.p7b -storetype PKCS11IMPLKS -keystore NONE
-providername IBMPKCS11Impl-CryptoServer
Enter keystore password:
```

Figure 7 : Importing user certificate into keystore

9. Verify that the keytool command shows the signed certificate as well as root CA certificate

›_ Console

```
# keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername
IBMPKCS11Impl-CryptoServer
```

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider's name

Provide the keystore password when prompted.

```
[root@hj-ibmibm16959 bin]# ./keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
Enter keystore password:

Keystore type: PKCS11IMPLKS
Keystore provider: IBMPKCS11Impl-CryptoServer

Your keystore contains 3 entries

rootca, null, trustedCertEntry,
Certificate fingerprint (SHA1): D9:BE:FA:00:CB:52:0E:7F:7B:82:CE:D3:54:02:BB:1F:43:21:B8:A1
ibmrsacert0, null, trustedCertEntry,
Certificate fingerprint (SHA1): 39:08:9E:28:36:38:1B:25:75:CA:16:41:29:C1:EC:D6:50:05:30:92
ibmrsa, null, keyEntry,
Certificate fingerprint (SHA1): 39:08:9E:28:36:38:1B:25:75:CA:16:41:29:C1:EC:D6:50:05:30:92
[root@hj-ibmibm16959 bin]#
```

Figure 8 : Keytool list output showing signed certificate as well as root CA certificate

6.1.2 For ECC Key and Certificate Generation

1. Generate an EC keypair on Utimaco HSM.

›_ Console

```
# keytool -genkey -alias ibmec -keyalg EC -keystore NONE -storetype
PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
```

Provide information when prompted.

Here:

- EC is the key algorithm
- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider name
- ibmec is the key name that will be generated on Utimaco HSM

Provide the keystore password when prompted.

```
[root@hj-ibmibm16959 bin]# ./keytool -genkey -alias ibmec -keyalg EC -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKC
S11Impl-CryptoServer
Enter keystore password:
What is your first and last name?
  [Unknown]:  ec demo
What is the name of your organizational unit?
  [Unknown]:  security
What is the name of your organization?
  [Unknown]:  utimaco
What is the name of your City or Locality?
  [Unknown]:  pune
What is the name of your State or Province?
  [Unknown]:  MH
What is the two-letter country code for this unit?
  [Unknown]:  IN
Is CN=ec demo, OU=security, O=utimaco, L=pune, ST=MH, C=IN correct? (type "yes" or "no")
  [no]:  yes

Enter key password for <ibmec>:
        (RETURN if same as keystore password):
[root@hj-ibmibm16959 bin]#
```

Figure 9 : Key generation using keytool command

2. Verify the entry with same alias name is generated using keytool command.

›_ Console

```
# keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername
IBMPKCS11Impl-CryptoServer
```

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider name

Provide the keystore password when prompted.

```
[root@hj-ibmibm16959 bin]# ./keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
Enter keystore password:

Keystore type: PKCS11IMPLKS
Keystore provider: IBMPKCS11Impl-CryptoServer

Your keystore contains 5 entries

rootca, null, trustedCertEntry,
Certificate fingerprint (SHA1): D9:BE:FA:00:CB:52:0E:7F:7B:82:CE:D3:54:02:BB:1F:43:21:B8:A1
ibmec, null, keyEntry,
Certificate fingerprint (SHA1): B0:14:78:65:1D:E9:4D:BB:B1:D5:31:50:E6:A8:2D:AC:81:FE:6B:71
ibmeccert0, null, trustedCertEntry,
Certificate fingerprint (SHA1): B0:14:78:65:1D:E9:4D:BB:B1:D5:31:50:E6:A8:2D:AC:81:FE:6B:71
ibmrsacert0, null, trustedCertEntry,
Certificate fingerprint (SHA1): 39:08:9E:28:36:38:1B:25:75:CA:16:41:29:C1:EC:D6:50:05:30:92
ibmrsa, null, keyEntry,
Certificate fingerprint (SHA1): 39:08:9E:28:36:38:1B:25:75:CA:16:41:29:C1:EC:D6:50:05:30:92
[root@hj-ibmibm16959 bin]#
```

Figure 10 : Keytool list command output

3. List the objects using p11tool2.

›_ Console

```
# p11tool2 Slot=0 LoginUser=ask ListObjects
```

Enter user PIN when prompted.

```
[root@hj-ibmibm16959 bin]# ./p11tool2 Slot=0 LoginUser=ask ListObjects
Enter normal user PIN:

+ 1.3
  CKA_CERTIFICATE_TYPE          = CKC_X_509
  CKA_UNIQUE_ID                 = 8789CEDE-4F52-4B38-AD43-87C78B5E495C
  CKA_LABEL                     = ibmec
  CKA_ID                        =

  CKA_SUBJECT                   =
                0x3060310B 30090603 55040613 02494E31 |0`1 0   U    IN1|
                  0B300906 03550408 13024D48 310D300B | 0   U    MH1 0 |
                  06035504 07130470 756E6531 10300E06 |  U    pune1 0  |
                  0355040A 13077574 696D6163 6F311130 | U    utimaco1 0|
                  0F060355 040B1308 73656375 72697479 |   U    security|
                  3110300E 06035504 03130765 63206465 |1 0   U    ec de|
                  6D6F                                |mo             |

CKO_PUBLIC_KEY:

+ 2.1
  CKA_KEY_TYPE                  = CKK_ECDSA
  CKA_UNIQUE_ID                 = 818D24A0-8FE7-4079-B73D-620BE7FA32B5
  CKA_LABEL                     =
  CKA_ID                        =
```

Figure 11 : ListObjects output using p11tool2

```
CKO_PRIVATE_KEY:

+ 3.1
  CKA_KEY_TYPE                  = CKK_ECDSA
  CKA_UNIQUE_ID                 = BDB281FF-DA70-45B8-BB83-D09F04C42168
  CKA_SENSITIVE                 = CK_TRUE
  CKA_EXTRACTABLE               = CK_FALSE
  CKA_LABEL                     =
  CKA_ID                        =


+ 3.2
  CKA_KEY_TYPE                  = CKK_ECDSA
  CKA_UNIQUE_ID                 = 92E942BB-F8D1-40BC-BEFE-4842345F4216
  CKA_SENSITIVE                 = CK_TRUE
  CKA_EXTRACTABLE               = CK_FALSE
  CKA_LABEL                     = ibmec
  CKA_ID                        =
```

4. Generate a CSR using Keytool command.

›_ Console

```
# keytool -certreq -alias ibmec -keystore NONE -storetype PKCS11IMPLKS
providername IBMPKCS11Impl-CryptoServer -file ec.csr
```

```
[root@hj-ibmibm16959 bin]# ./keytool -certreq -alias ibmec -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-Cr
yptoServer -file ec.csr
Enter keystore password:
[root@hj-ibmibm16959 bin]#
```

Figure 12 : Generate CSR command output

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- Provide the keystore password when prompted
- IBMPKCS11Impl-CryptoServer is the provider name
- ibmec is the key name
- ec.csr is the CSR file name that will be generated

Provide the keystore password when prompted

5. Get this CSR signed by CA.
6. Copy the signed certificate and root CA certificate on the IBM WebSphere application server.
7. Import Root CA certificate into HSM keystore.

›_ Console

```
#  keytool -importcert -alias rootca -file /home/LAbCA-Root.crt -storetype
PKCS11IMPLKS -keystore NONE -providername IBMPKCS11Impl-CryptoServer
```

```
[root@hj-ibmibm16959 bin]# ./keytool -importcert -alias rootca -file /home/LAbCA-Root.crt -storetype PKCS11IMPLKS -keystore NONE
 -providername IBMPKCS11Impl-CryptoServer
Enter keystore password:
Owner: CN=LabCA-Root, OU=IT, O=security, L=Campbell, ST=Austin, C=US
Issuer: CN=LabCA-Root, OU=IT, O=security, L=Campbell, ST=Austin, C=US
Serial number: 40f8f17a48d0bcc3
Valid from: 11/29/22 11:06 AM until: 11/29/32 11:06 AM
Certificate fingerprints:
         MD5:  80:E7:CE:91:84:D6:E9:D9:03:53:DB:F3:11:84:F3:34
         SHA1: D9:BE:FA:00:CB:52:0E:7F:7B:82:CE:D3:54:02:BB:1F:43:21:B8:A1
         SHA256: 58:E9:C6:A3:12:0D:A9:3A:97:E8:0D:03:06:9B:89:0F:05:E6:EB:1F:46:1C:E8:B1:B6:DF:DE:3E:4D:0B:EC:64
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL CA
   S/MIME CA
   Object Signing CA]

#2: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 0e 49 6e 66 6f 73 65  63 20 4c 61 62 20 43 41   ..Infosec.Lab.CA
```

Figure 13 : Importing root CA certificate into keystore

```
#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 85 42 28 42 84 18 55 2c  73 aa 74 dc 23 ee 74 7a  .B.B..U.s.t.#.tz
0010: 00 fe 2e dc                                       ....
]
]

#5: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[root@hj-ibmibm16959 bin]#
```

8. Import the signed certificate reply using the command below.

›_ Console

```
#  keytool -importcert -alias ibmec -file /home/ec_demo.p7b -storetype
PKCS11IMPLKS -keystore NONE -providername IBMPKCS11Impl-CryptoServer
```

```
[root@hj-ibmibm16959 bin]# ./keytool -importcert -alias ibmec -file /mnt/ec_demo.p7b -storetype PKCS11IMPLKS -keystore NONE -pro
vidername IBMPKCS11Impl-CryptoServer
Enter keystore password:
Certificate reply was installed in keystore
[root@hj-ibmibm16959 bin]#
```

Figure 14 : Importing user certificate into keystore

9. Verify that the keytool command shows the signed certificate as well as root CA certificate.

›_ Console

```
# keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername
IBMPKCS11Impl-CryptoServer
```

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider's name

Provide the keystore password when prompted.

```
[root@hj-ibmibm16959 bin]# ./keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
Enter keystore password:

Keystore type: PKCS11IMPLKS
Keystore provider: IBMPKCS11Impl-CryptoServer

Your keystore contains 5 entries

rootca, null, trustedCertEntry,
Certificate fingerprint (SHA1): D9:BE:FA:00:CB:52:0E:7F:7B:82:CE:D3:54:02:BB:1F:43:21:B8:A1
ibmec, null, keyEntry,
Certificate fingerprint (SHA1): 79:55:79:B9:B5:C8:FF:62:82:6A:EF:83:72:C8:88:89:0C:BC:DE:43
ibmeccert0, null, trustedCertEntry,
Certificate fingerprint (SHA1): 79:55:79:B9:B5:C8:FF:62:82:6A:EF:83:72:C8:88:89:0C:BC:DE:43
ibmrsacert0, null, trustedCertEntry,
Certificate fingerprint (SHA1): 39:08:9E:28:36:38:1B:25:75:CA:16:41:29:C1:EC:D6:50:05:30:92
ibmrsa, null, keyEntry,
Certificate fingerprint (SHA1): 39:08:9E:28:36:38:1B:25:75:CA:16:41:29:C1:EC:D6:50:05:30:92
[root@hj-ibmibm16959 bin]#
```

Figure 15 : Keytool list output showing signed certificate as well as root CA certificate

6.2 Generating SSL Key and Certificate on Windows

6.2.1 Generating SSL Key and Certificate on Windows for RSA Key and Certificate Generation

1. Generate a keypair on Utimaco HSM with the help of keytool command.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool.exe -genkey
-alias ibmrsa -keyalg RSA -keysize 2048 -keystore NONE -storetype PKCS11IMPLKS
-providername IBMPKCS11Impl-CryptoServer
```

Provide information when prompted.

Here:

- RSA is the key algorithm
- 2048 is the key size
- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider name
- ibmrsa is the key name that will be generated on Utimaco HSM

Provide the keystore password when prompted.

Figure 16 : Key generation using keytool command

2. Verify the entry with same alias name is generated using keytool command.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool -list keystore
NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
```

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider's name

Provide the keystore password when prompted.

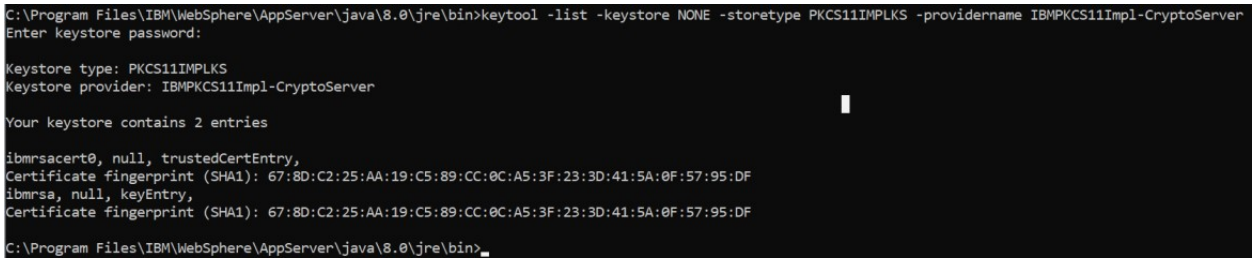


Figure 17 : Keytool list output

3. List the objects using p11tool2.

›_ Console

```
C:\Program Files\Utimaco\SecurityServer\Administration>p11tool2.exe slot=0
 Loginuser=ask ListObjects
```

Enter user PIN when prompted.

```
C:\Program Files\Utimaco\SecurityServer\Administration>p11tool2 Slot=0 LoginUser=ask ListObjects
Enter normal user PIN:


CKO_CERTIFICATE:

+ 1.1
  CKA_CERTIFICATE_TYPE          = CKC_X_509
  CKA_UNIQUE_ID                 = 3BBBA1D8-849A-45F9-8D60-22E17CA4A403
  CKA_LABEL                     = ibmrsa
  CKA_ID                        =

  CKA_SUBJECT                   =
               0x3061310B 30090603 55040613 02494E31 |0a1 0   U    IN1|
                 0B300906 03550408 13024D48 310D300B | 0   U    MH1 0 |
                 06035504 07130470 756E6531 10300E06 |  U    pune1 0  |
                 0355040A 13077574 696D6163 6F311130 | U    utimaco1 0|
                 0F060355 040B1308 73656375 72697479 |   U    security|
                 3111300F 06035504 03130872 73612064 |1 0   U    rsa d|
                 656D6F                              |emo             |



CKO_PUBLIC_KEY:

+ 2.1
  CKA_KEY_TYPE                  = CKK_RSA
  CKA_UNIQUE_ID                 = 5B8D54CF-96C8-43BF-A27B-E1427AE09E97
  CKA_LABEL                     =
  CKA_ID                        =
```

Figure 18 : ListObjects output using p11tool2

```
CKO_PRIVATE_KEY:

+ 3.1
  CKA_KEY_TYPE                  = CKK_RSA
  CKA_UNIQUE_ID                 = 2A8ABC9E-DE86-431A-8607-E5B96B2285CF
  CKA_SENSITIVE                 = CK_TRUE
  CKA_EXTRACTABLE               = CK_FALSE
  CKA_LABEL                     =
  CKA_ID                        =


+ 3.2
  CKA_KEY_TYPE                  = CKK_RSA
  CKA_UNIQUE_ID                 = FD359C05-CEEA-4362-9B44-284CDC6E8C22
  CKA_SENSITIVE                 = CK_TRUE
  CKA_EXTRACTABLE               = CK_FALSE
  CKA_LABEL                     = ibmrsa
  CKA_ID                        =


C:\Program Files\Utimaco\SecurityServer\Administration>_
```

4. Generate a CSR using Keytool command.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool.exe -certreq
-alias ibmrsa -keystore NONE -storetype PKCS11IMPLKS -providername
IBMPKCS11Impl-CryptoServer -file ibm.csr
```

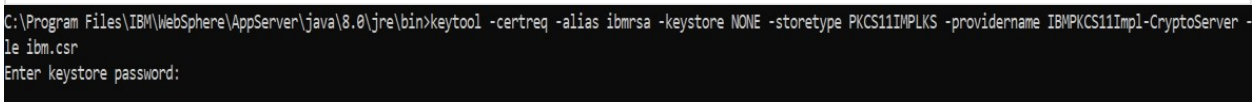


Figure 19 : Generate CSR command output

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider name
- ibmrsa is the key name
- ibm.csr is the CSR file name that will be generated

Provide keystore password when prompted.

5. Get this CSR signed by CA.
6. Copy the signed certificate and root CA certificate on the IBM WebSphere application server.
7. Import Root CA certificate into HSM keystore.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool.exe importcert
-alias rootca -file C:\Users\Downloads\RootCA.crt -storetype PKCS11IMPLKS
-keystore NONE -providername IBMPKCS11Impl-CryptoServer
```

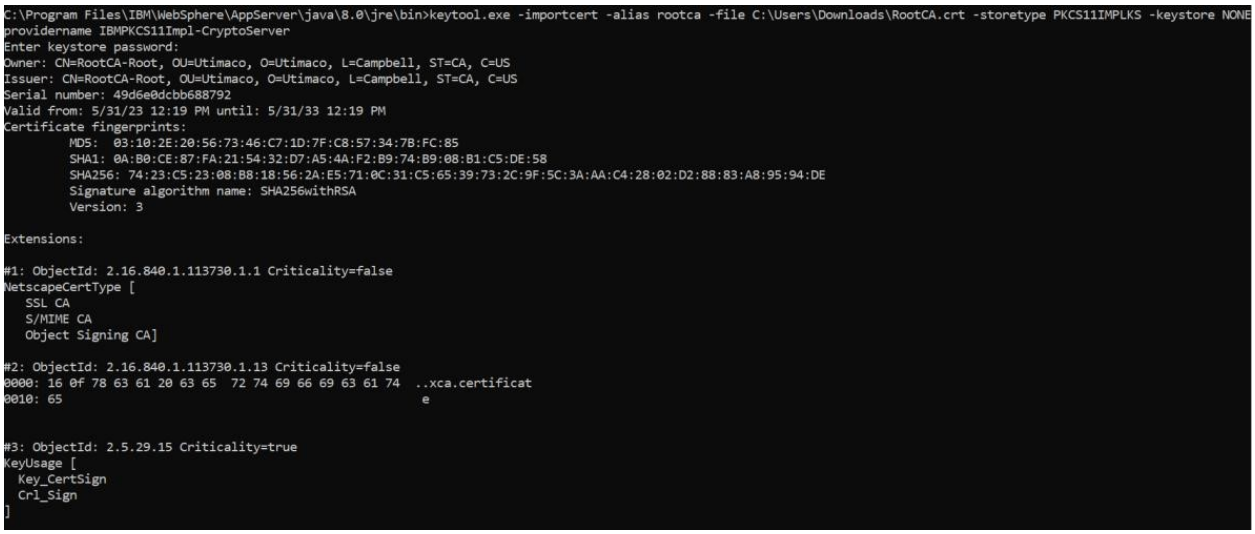
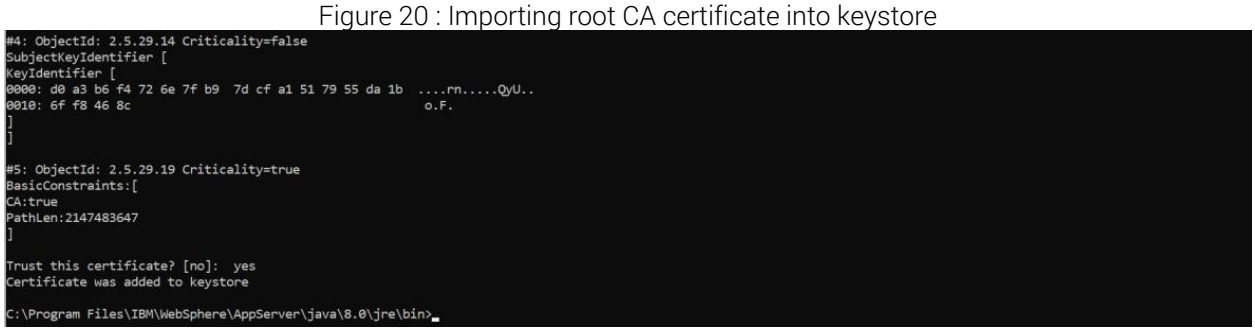


Figure 20 : Importing root CA certificate into keystore



8. Import the signed certificate reply using the command below.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool.exe importcert
-alias ibmrsa -file C:\Users\Downloads\rsa_demo.p7b -storetype PKCS11IMPLKS
-keystore NONE -providername IBMPKCS11Impl-CryptoServer
```

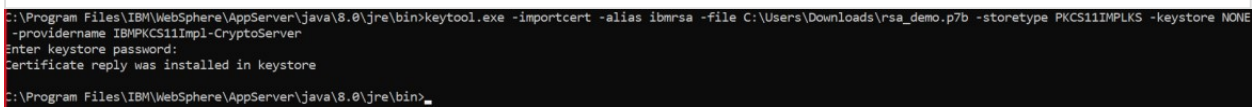


Figure 21 : Importing user certificate into keystore

9. Verify that the keytool command shows the signed certificate as well as root CA certificate.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool -list keystore
NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
```

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider's name

Provide the keystore password when prompted.

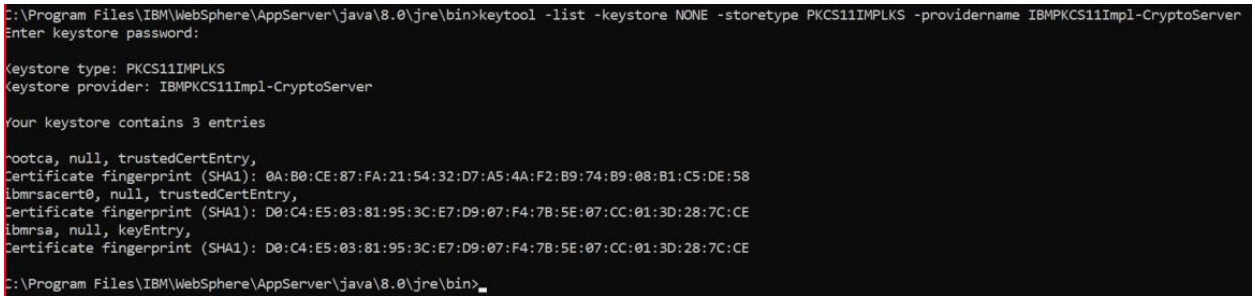


Figure 22 : Keytool list output showing signed certificate as well as root CA certificate

6.2.2 Generating SSL Key and Certificate on Windows for ECC Key and Certificate Generation

1. Generate an EC keypair on Utimaco HSM.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool -genkey alias
ibmec -keyalg EC -keystore NONE -storetype PKCS11IMPLKS -providername
IBMPKCS11Impl-CryptoServer # keytool -genkey -alias ibmec -keyalg EC -keystore
NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
```

Provide information when prompted.

Here:

- EC is the key algorithm
- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider name
- ibmec is the key name that will be generated on Utimaco HSM

Provide the keystore password when prompted.

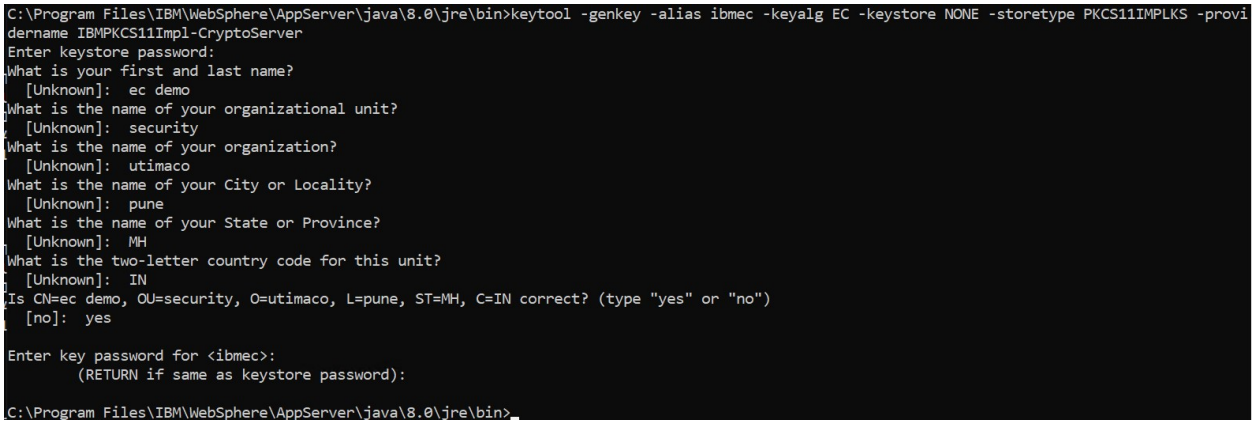


Figure 23 : Key generation using keytool command

2. Verify the entry with same alias name is generated using keytool command.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool -list keystore
NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
```

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider name

Provide the keystore password when prompted.

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool -list -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
Enter keystore password:

Keystore type: PKCS11IMPLKS
Keystore provider: IBMPKCS11Impl-CryptoServer

Your keystore contains 2 entries

ibmec, null, keyEntry,
Certificate fingerprint (SHA1): E2:88:E4:36:A6:29:23:3E:A1:B5:28:FE:EE:E3:88:D0:69:53:AC:D4
ibmeccert0, null, trustedCertEntry,
Certificate fingerprint (SHA1): E2:88:E4:36:A6:29:23:3E:A1:B5:28:FE:EE:E3:88:D0:69:53:AC:D4

C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>
```

Figure 24 : Keytool list command output

3. List the objects using p11tool2.

›_ Console

```
C:\Program Files\Utimaco\SecurityServer\Administration>p11tool2 Slot=0
 LoginUser=ask ListObjects
```

Enter user PIN when prompted.

```
C:\Program Files\Utimaco\SecurityServer\Administration>p11tool2 Slot=0 LoginUser=ask ListObjects
Enter normal user PIN:


CKO_CERTIFICATE:

+ 1.1
  CKA_CERTIFICATE_TYPE          = CKC_X_509
  CKA_UNIQUE_ID                 = 298166CD-1C0F-449B-AC3C-C1E5B217DD7F
  CKA_LABEL                     = ibmec
  CKA_ID                        =

  CKA_SUBJECT                   =
               0x3060310B 30090603 55040613 02494E31 |0`1 0   U    IN1|
                 0B300906 03550408 13024D48 310D300B | 0   U    MH1 0 |
                 06035504 07130470 756E6531 10300E06 |  U    pune1 0  |
                 0355040A 13077574 696D6163 6F311130 | U    utimaco1 0|
                 0F060355 040B1308 73656375 72697479 |   U    security|
                 3110300E 06035504 03130765 63206465 |1 0   U    ec de|
                 6D6F                               |mo             |



CKO_PUBLIC_KEY:

+ 2.1
  CKA_KEY_TYPE                  = CKK_ECDSA
  CKA_UNIQUE_ID                 = 293A1C3B-53A5-46D6-8F96-69EA354CE013
  CKA_LABEL                     =
  CKA_ID                        =
```

Figure 25 : ListObjects output using p11tool2

```
CKO_PRIVATE_KEY:

+ 3.1
  CKA_KEY_TYPE                  = CKK_ECDSA
  CKA_UNIQUE_ID                 = 92393DEB-A830-49F1-ADFE-A1B4C0CEBB37
  CKA_SENSITIVE                 = CK_TRUE
  CKA_EXTRACTABLE               = CK_FALSE
  CKA_LABEL                     =
  CKA_ID                        =


+ 3.2
  CKA_KEY_TYPE                  = CKK_ECDSA
  CKA_UNIQUE_ID                 = B2AF3E8D-4AEB-4C4B-A2DD-33E059FB3DA0
  CKA_SENSITIVE                 = CK_TRUE
  CKA_EXTRACTABLE               = CK_FALSE
  CKA_LABEL                     = ibmec
  CKA_ID                        =


C:\Program Files\Utimaco\SecurityServer\Administration>
```

4. Generate a CSR using Keytool command.

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool -certreq -alias ibmec -keystore NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer -fil
e ec.csr
Enter keystore password:

C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>
```

Figure 26 : Generate CSR command output

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- Provide the keystore password when prompted
- IBMPKCS11Impl-CryptoServer is the provider name
- ibmec is the key name
- ec.csr is the CSR file name that will be generated

Provide the keystore password when prompted.

5. Get this CSR signed by CA.
6. Copy the signed certificate and root CA certificate on the IBM WebSphere application server.
7. Import Root CA certificate into HSM keystore.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool.exe importcert
-alias rootca -file C:\Users\Downloads\RootCA.crt -storetype PKCS11IMPLKS
-keystore NONE -providername IBMPKCS11Impl-CryptoServer
```

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool.exe -importcert -alias rootca -file C:\Users\Downloads\RootCA.crt -storetype PKCS11IMPLKS -keystore NONE -
providername IBMPKCS11Impl-CryptoServer
Enter keystore password:
Owner: CN=RootCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Issuer: CN=RootCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Serial number: 49d6e0dcbb688792
Valid from: 5/31/23 12:19 PM until: 5/31/33 12:19 PM
Certificate fingerprints:
        MD5:  03:10:2E:20:56:73:46:C7:1D:7F:C8:57:34:7B:FC:85
        SHA1: 0A:B0:CE:87:FA:21:54:32:D7:A5:4A:F2:B9:74:B9:08:B1:C5:DE:58
        SHA256: 74:23:C5:23:08:B8:18:56:2A:E5:71:0C:31:C5:65:39:73:2C:9F:5C:3A:AA:C4:28:02:D2:88:83:A8:95:94:DE
        Signature algorithm name: SHA256withRSA
        Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL CA
   S/MIME CA
   Object Signing CA]

#2: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 0F 78 63 61 20 63 65  72 74 69 66 69 63 61 74  ..xca.certificat
0010: 65                                                 e


#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]
```

Figure 27 : Importing root CA certificate into keystore

```
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: d0 a3 b6 f4 72 6e 7f b9  7d cf a1 51 79 55 da 1b  ....rn.....QyU..
0010: 6f f8 46 8c                                       o.F.
]
]

#5: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]

Trust this certificate? [no]:  yes
Certificate was added to keystore

C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>
```

8. Import the signed certificate reply using the command below.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool -importcert
-alias ibmec -file C:\Users\Downloads\ec_demo.p7b -storetype PKCS11IMPLKS
keystore NONE -providername IBMPKCS11Impl-CryptoServer
```

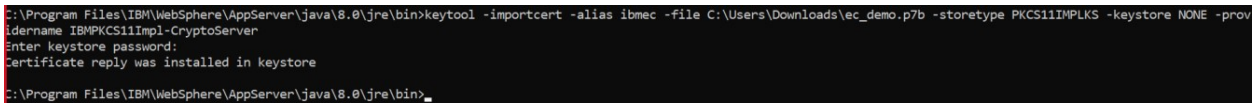


Figure 28 : Importing user certificate into keystore

9. Verify that the keytool command shows the signed certificate as well as root CA certificate.

›_ Console

```
C:\Program Files\IBM\WebSphere\AppServer\java\8.0\jre\bin>keytool -list keystore
NONE -storetype PKCS11IMPLKS -providername IBMPKCS11Impl-CryptoServer
```

Here:

- NONE is the keystore for HSM
- PKCS11IMPLKS is the storetype
- IBMPKCS11Impl-CryptoServer is the provider's name

Provide the keystore password when prompted.

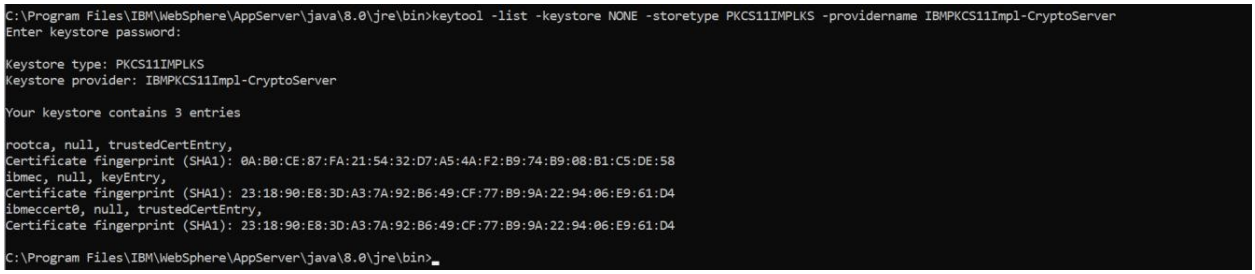


Figure 29 : Keytool list output showing signed certificate as well as root CA certificate

6.3 Configuring WebSphere Application Server for SSL

6.3.1 Configuring Keystore for Utimaco HSM

1. Access IBM WebSphere Application server Admin console: http://<IPADDRESS:9043/ibm/console> using web browser
2. Provide username and password to login.

3. Click on **Security** -> **SSL certificate and key management** -> under **Related Items** section select **Key stores and certificates**.

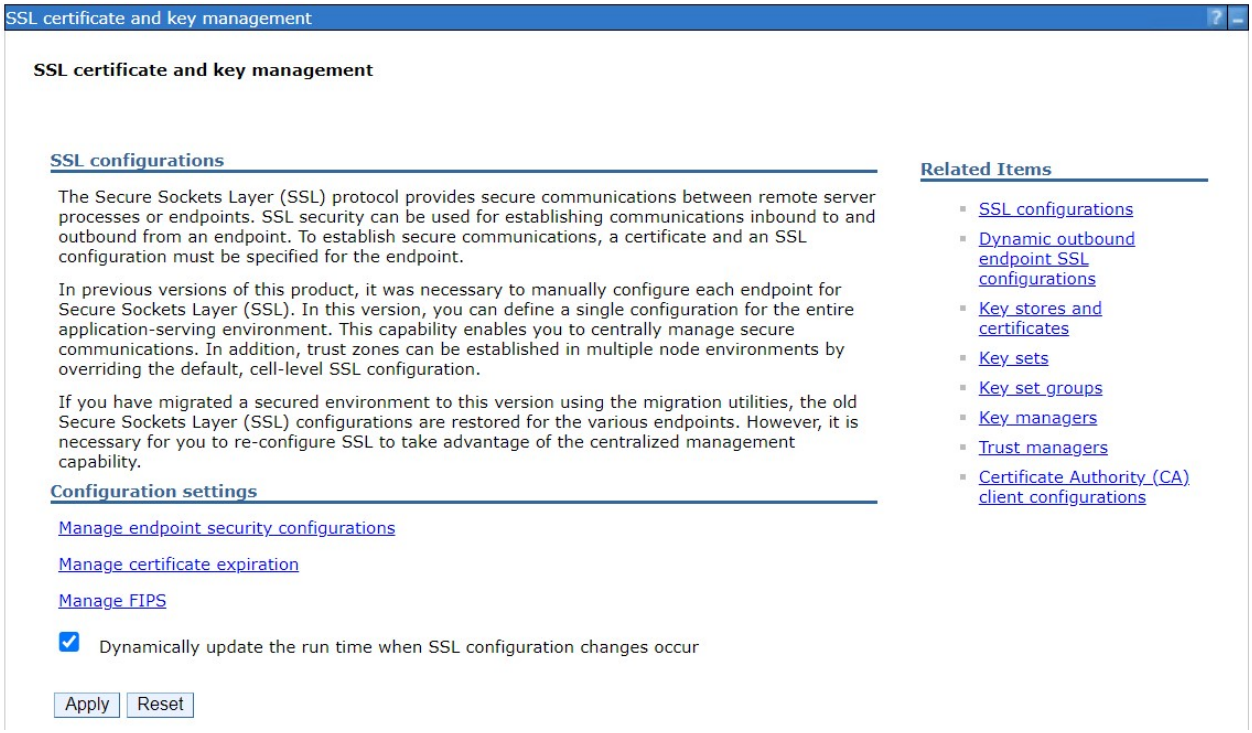


Figure 30 : SSL certificate and key management page

4. Click on **New...** button.

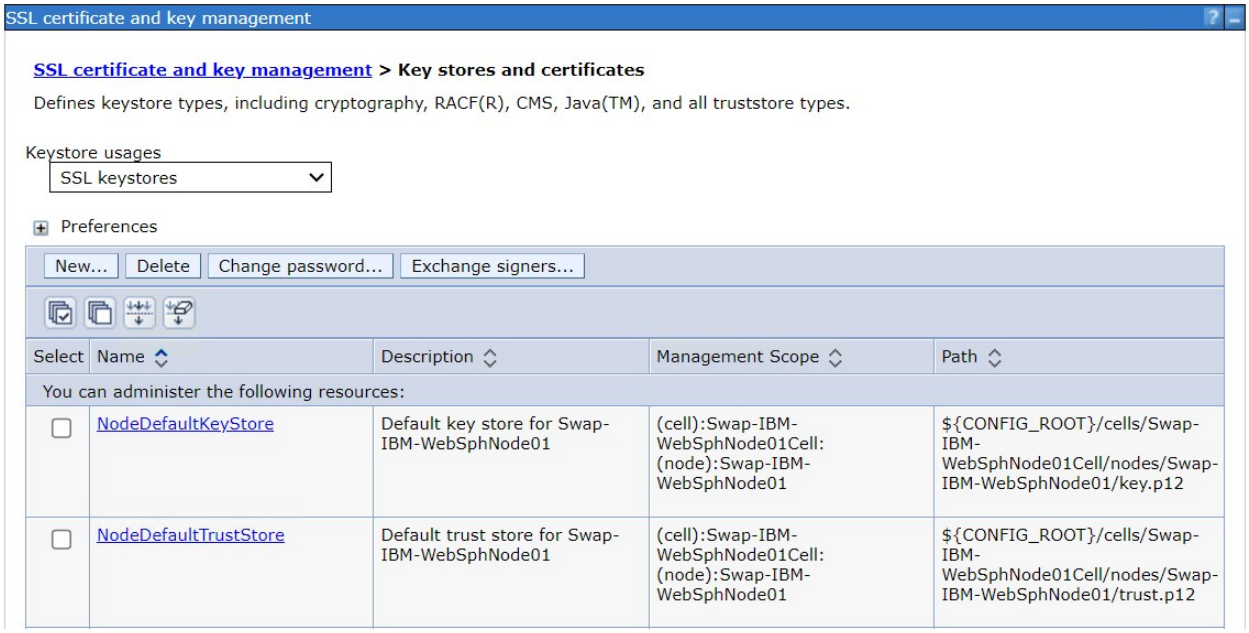


Figure 31 : Key stores and certificates page

5. Provide the following details related to Utimaco HSM in the below fields:

    a. Name: Name of the keystore for example Utimaco

    b. Path: Path to library. For example /etc/utimaco/pkcs11.cfg for Linux and C:\ \Program Files\\Utimaco\\pkcs11.cfg for Windows

    c. Password: Slot PIN

    d. Confirm Password : Enter Slot PIN again

    e. Type : Select Cryptographic Token Device (PKCS11)

    f. Read Only : Check this option

On Linux

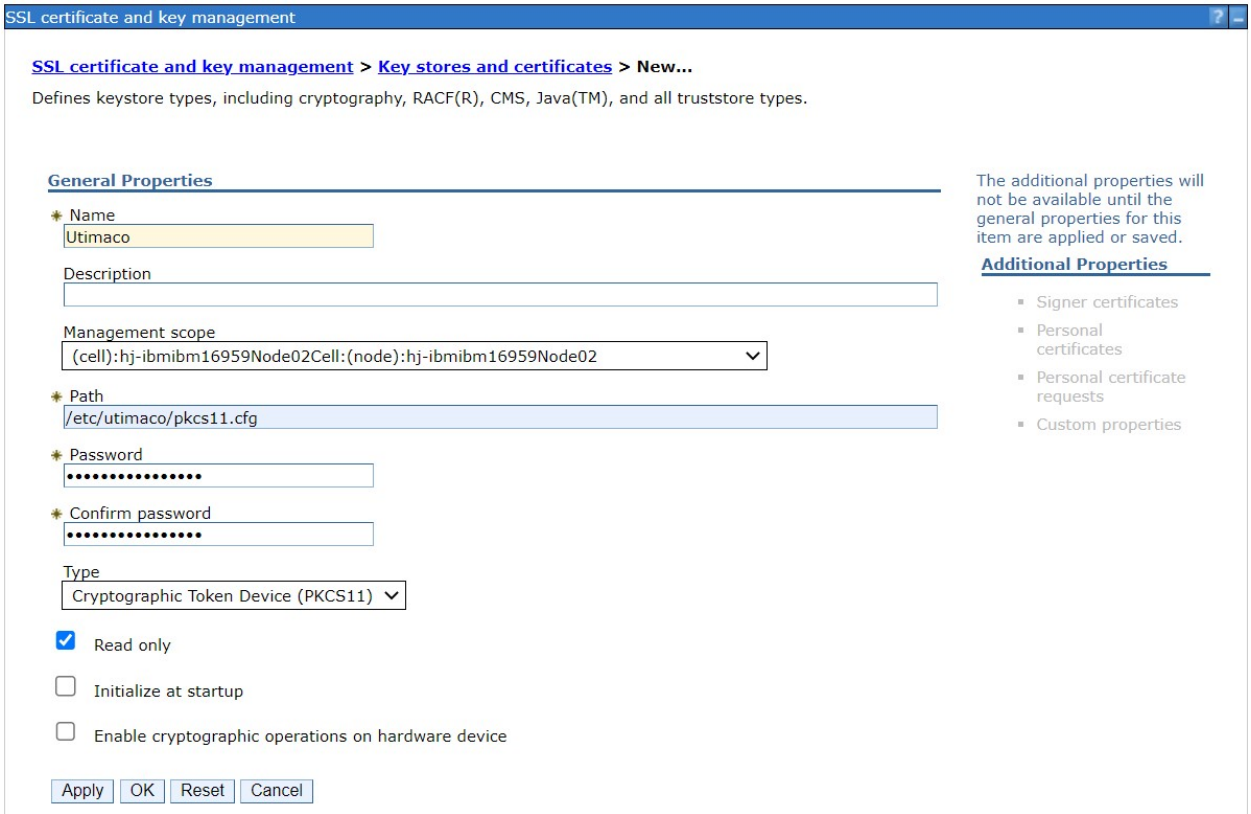


Figure 32 : Creating keystore for Utimaco HSM on Linux

On Windows

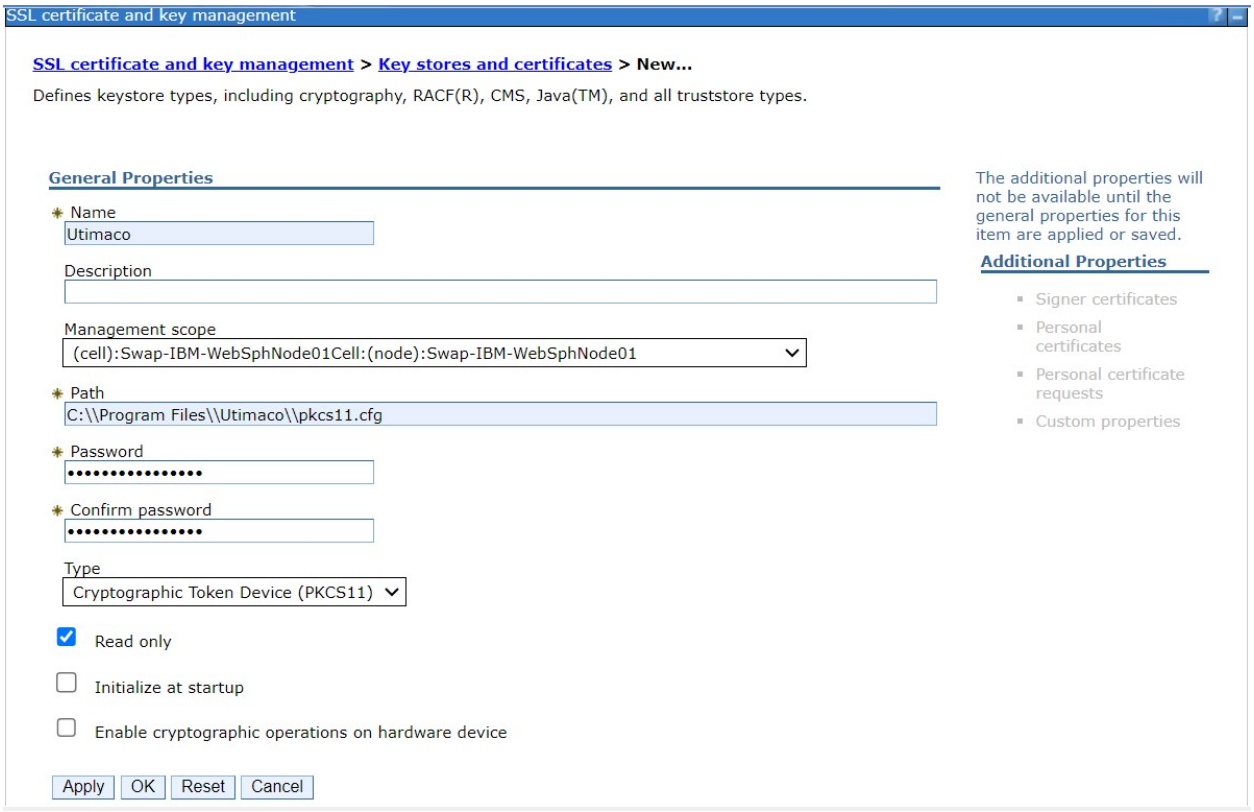


Figure 33 : Creating keystore for Utimaco HSM on Windows

6. Click on **Apply** and **OK**.

7. Click on **Save** to save the changes when the message pops up.

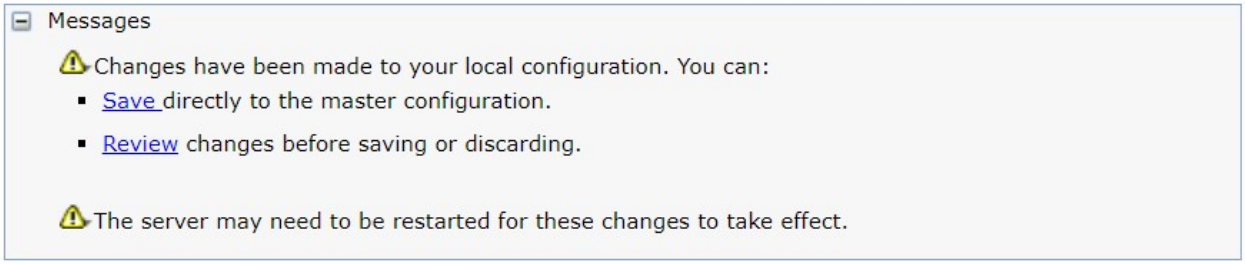


Figure 34 : Messages to save/review the changes

6.3.2 Node Default SSL Configuration

1. From the Admin console Click on **Security** -> **SSL certificate and key management** -> under **Related Items** section select **SSL configuration**.

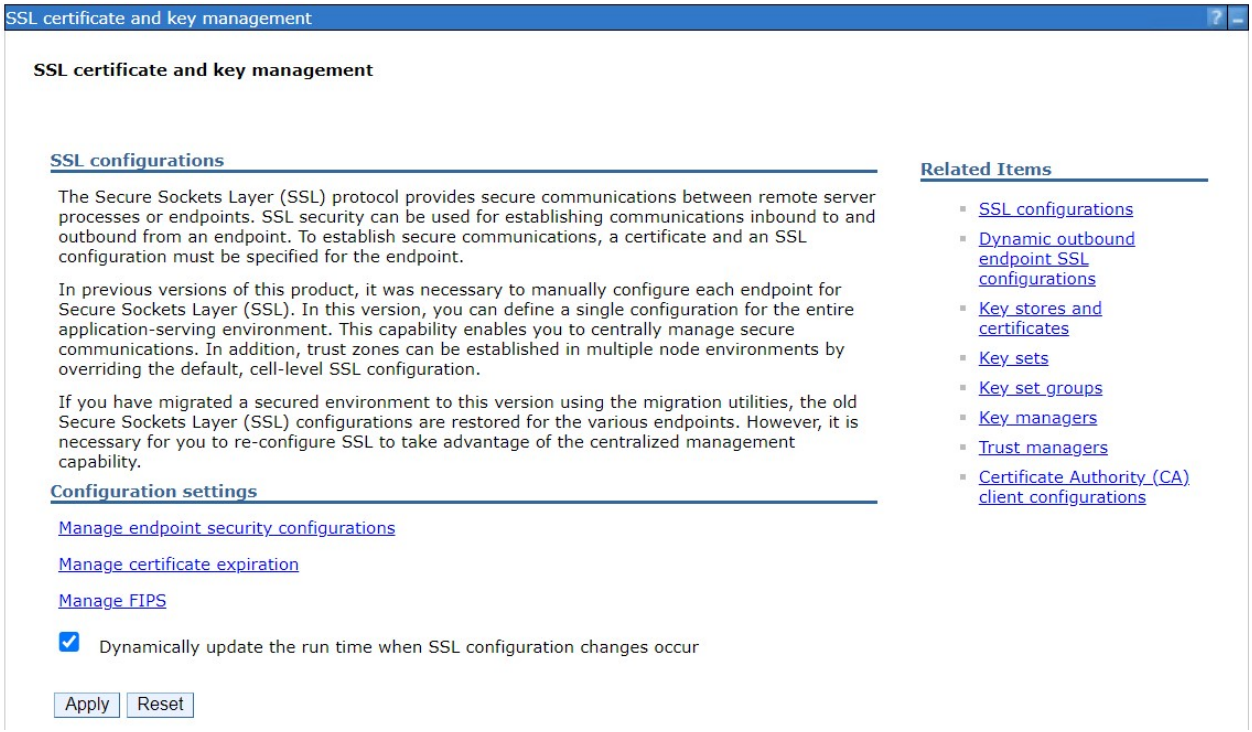


Figure 35 : SSL certificate and key management page

2. Select **NodeDefaultSSLSettings**.

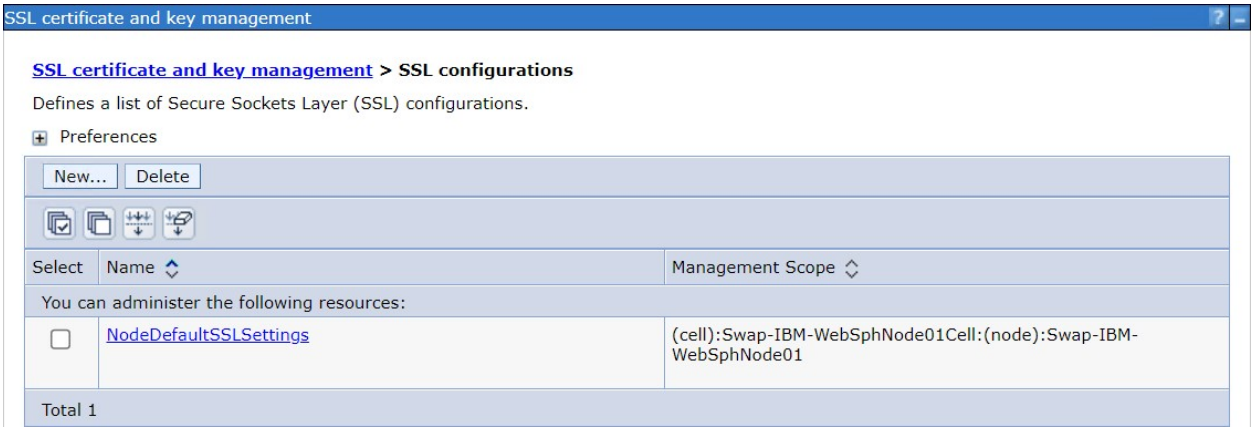


Figure 36 : SSL configuration page

3. In Trust store name field select Utimaco from dropdown.

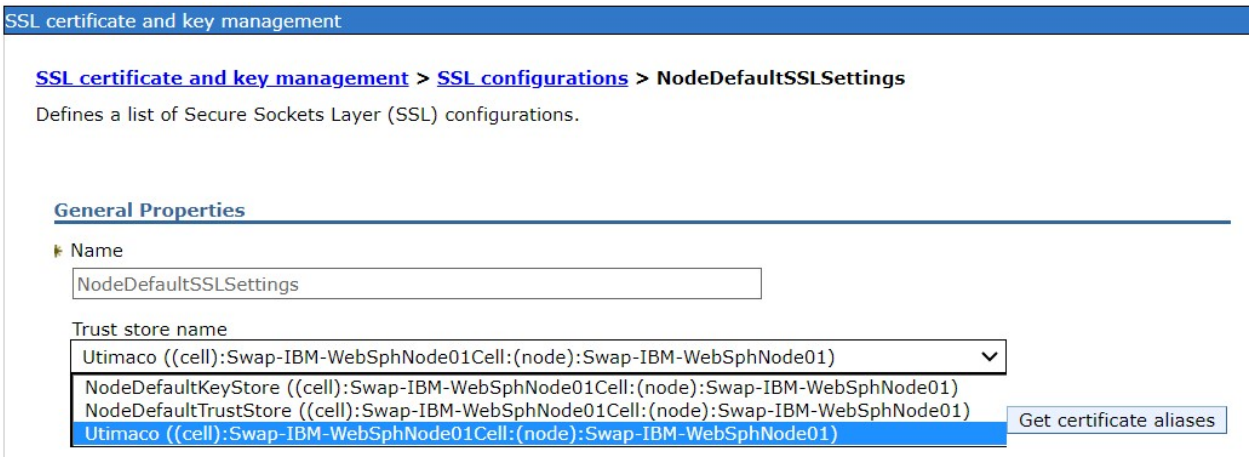


Figure 37 : Selecting Trust store name

4. Similarly, in **Keystore name** field select Utimaco from dropdown.

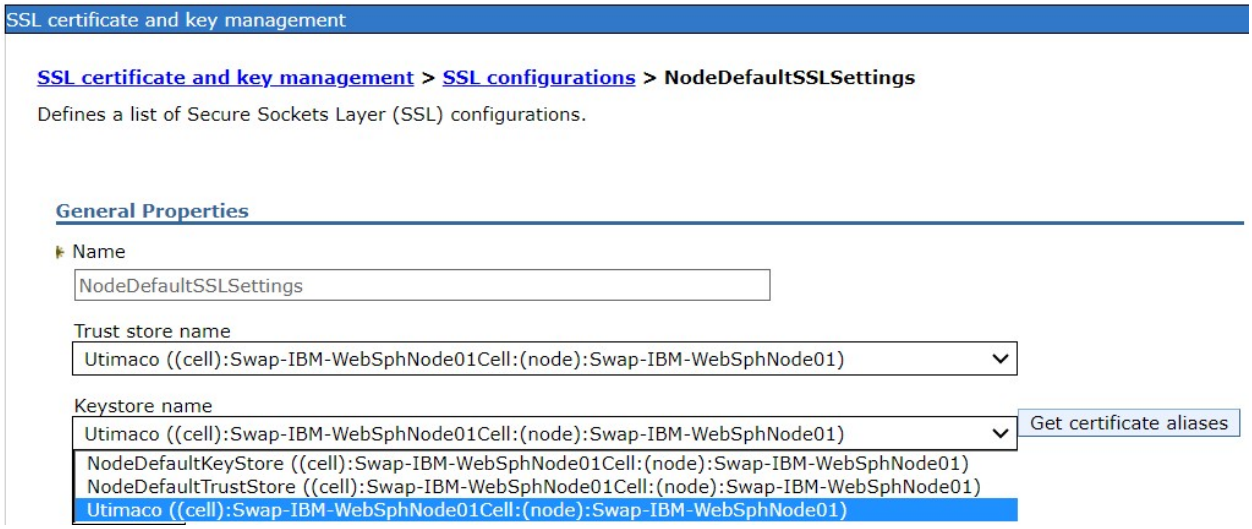


Figure 38 : Selecting keystore name

5. Click on **Get Certificate aliases** button to get the t server certificate and client certificate.
6. Select the **Default server certificate alias** from the dropdown.
7. Select the **Default client certificate alias** from the dropdown.
8. Click Apply and OK.

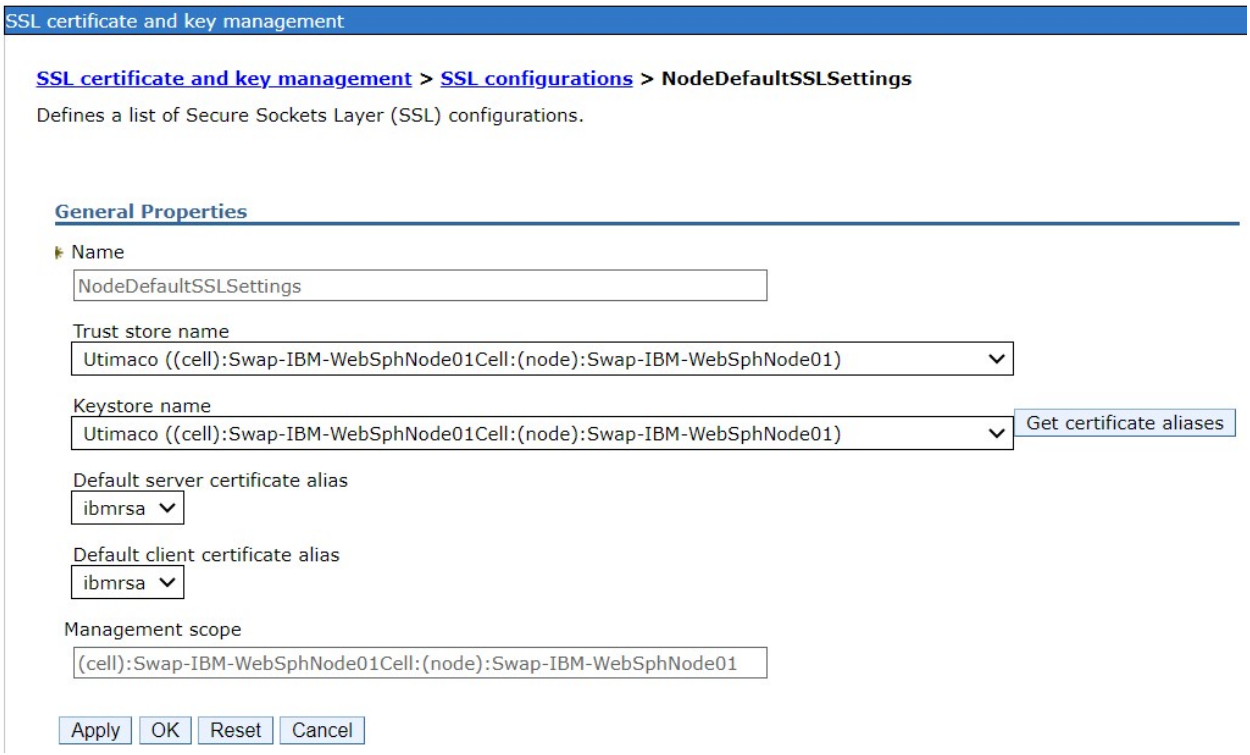


Figure 39 : NodeDefaultSSLSettings page

9. Click on Apply -> OK and save.
10. Restart the WebSphere application server.

In Linux you can use commands stopserver.sh <servername> and startserver.sh <servername>to stop/start the service. In windows click on start and select IBM WebSphere Application Service utility to stop/start the service.

6.3.3 Application Server SSL Configuration

You can configure SSL for IBM WebSphere application server by following the below steps:

1. From the Admin console Click on **Security** -> **SSL certificate and key management** -> **Manage endpoint security configurations**.

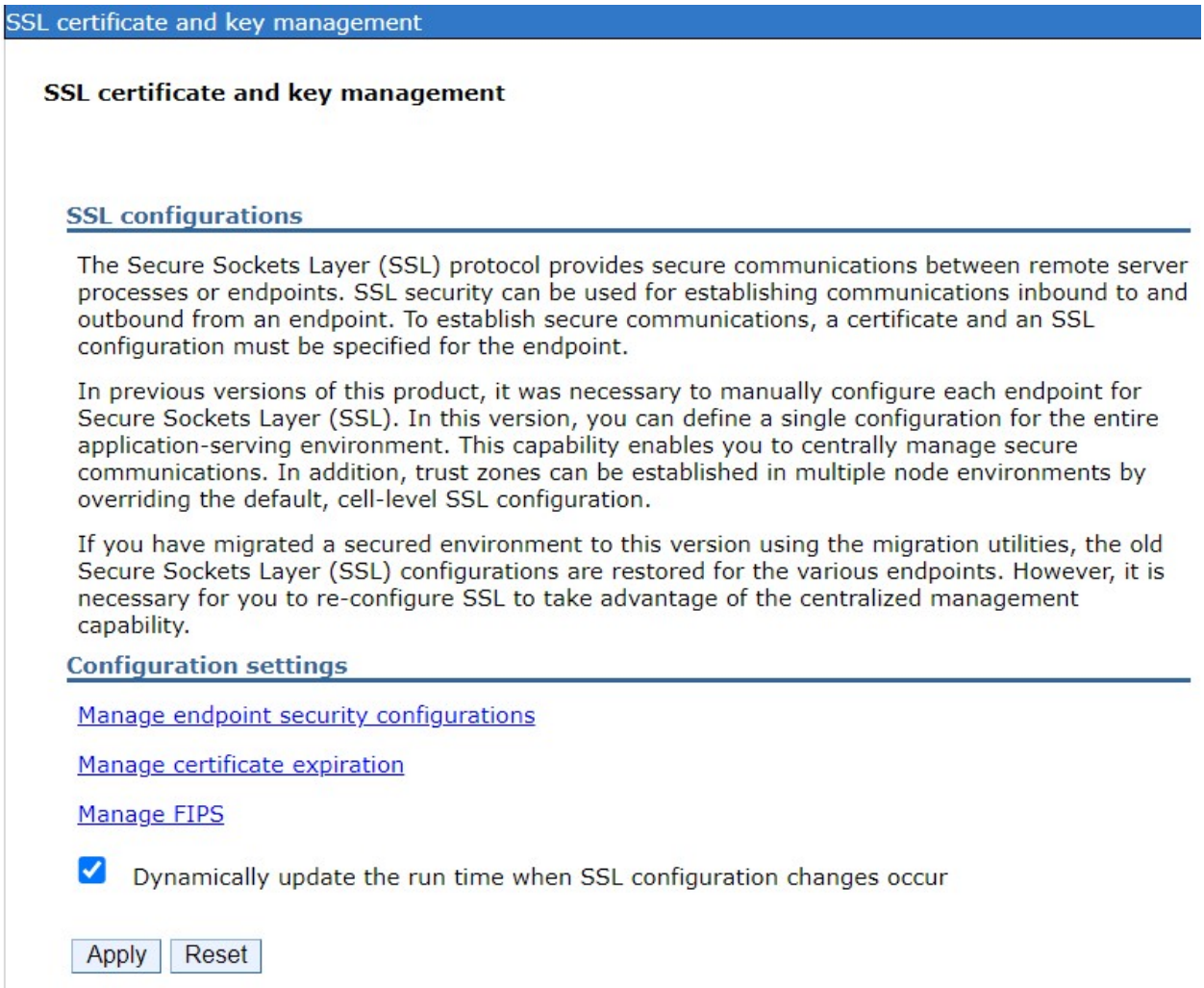


Figure 40 : SSL certificate and key management page

2. In the inbound local topology tree, click the server's name for example server1 below.

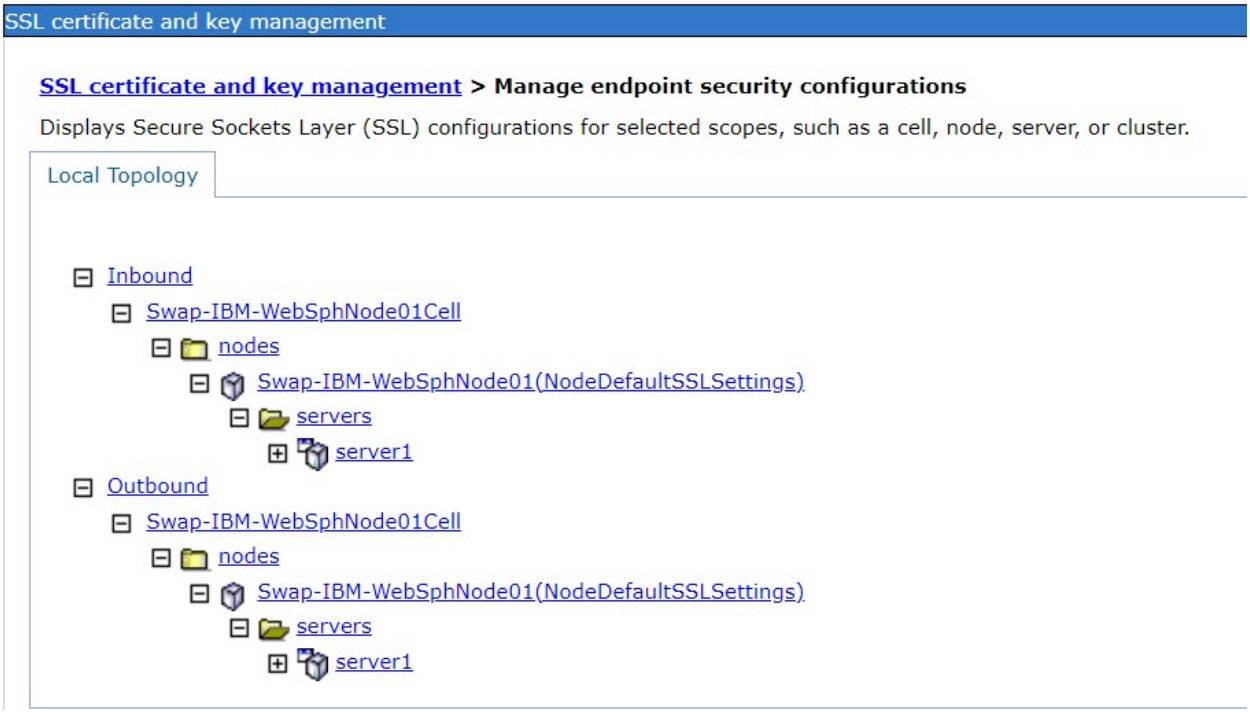


Figure 41 : Manage endpoint security configurations page

3. Under **Specific SSL configuration for this endpoint**, enable **Override inherited values**.
4. Select **NodeDefaultSSLSettings** from within the **SSL configuration** field.
5. Click **Update certificate alias list**.
6. Specify the certificate alias in the keystore from the drop-down list for example **ibmrsa.**

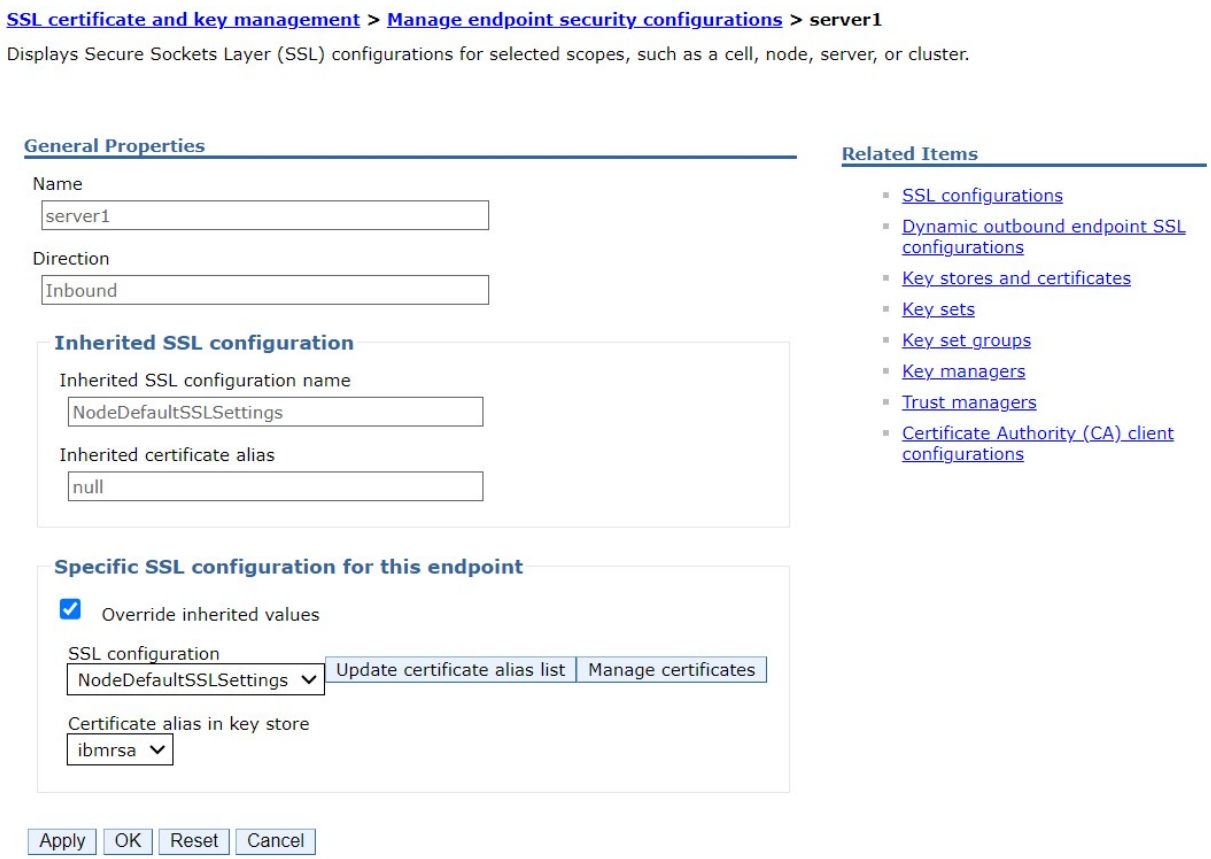


Figure 42 : Selecting Certificate alias for SSL

7. Click **OK** and save the changes.

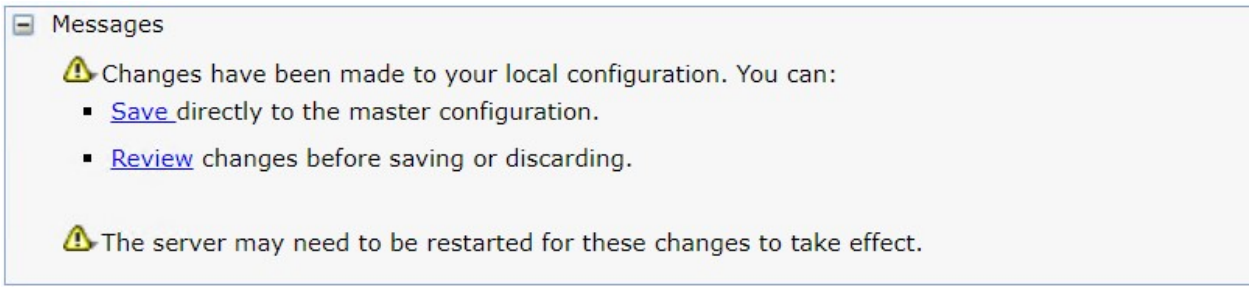


Figure 43 : Messages to Save/Review the changes

8. From the Admin console Click on **Security** -> **SSL certificate and key management**.
9. Make sure to select to **Dynamically update the run time when SSL configuration changes occur** if not selected.

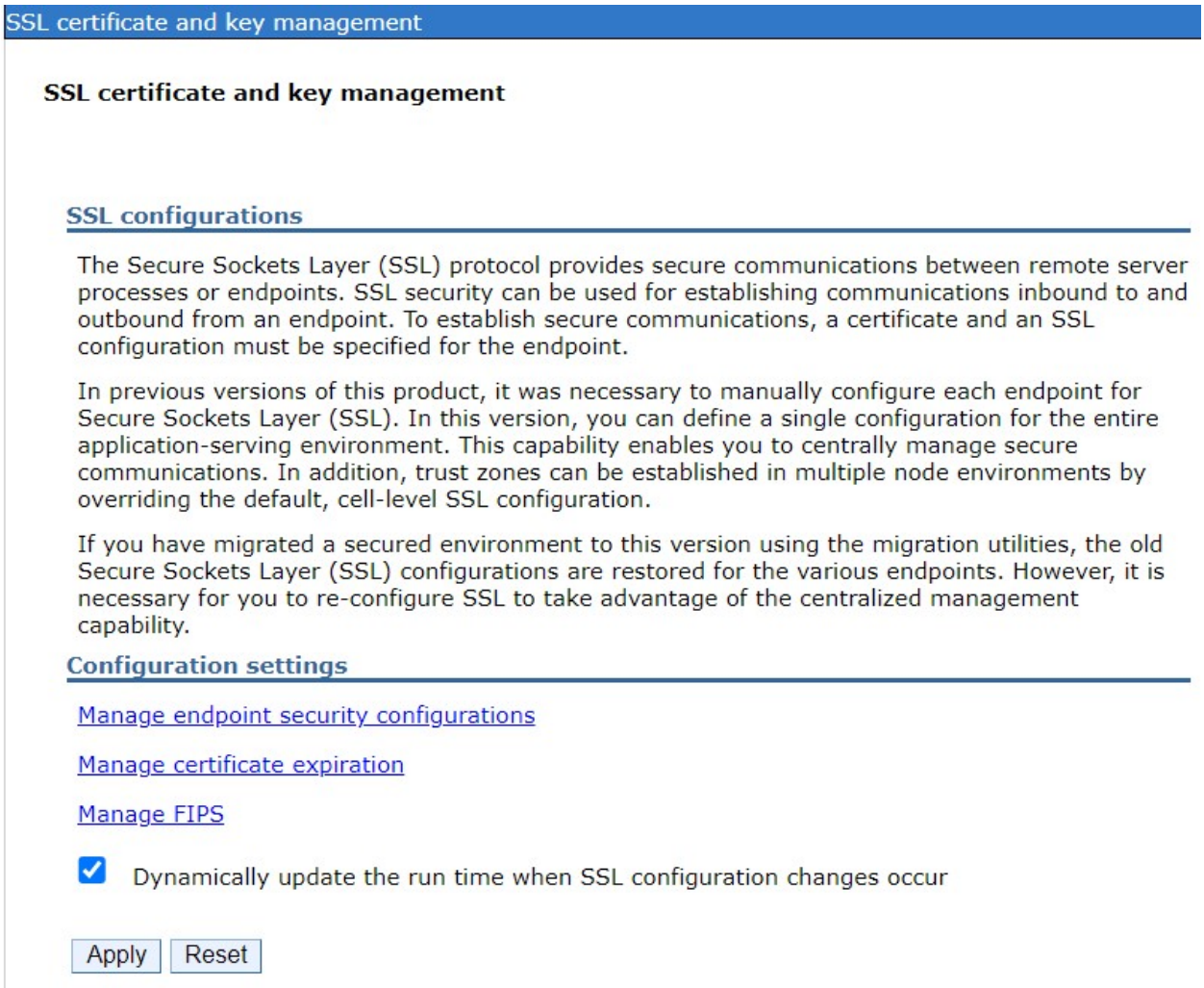


Figure 44 : SSL certificate and key management page

10. Click **Apply** and save the changes.
11. Restart the WebSphere application server.

In Linux you can use commands stopserver.sh <servername> and startserver.sh <servername>to stop/start the service. In windows click on start and select IBM WebSphere Application Service utility to stop/start the service.

12. Now the access the web page https://<ServerIPAddress>:9043/ibm/console over https from browser.

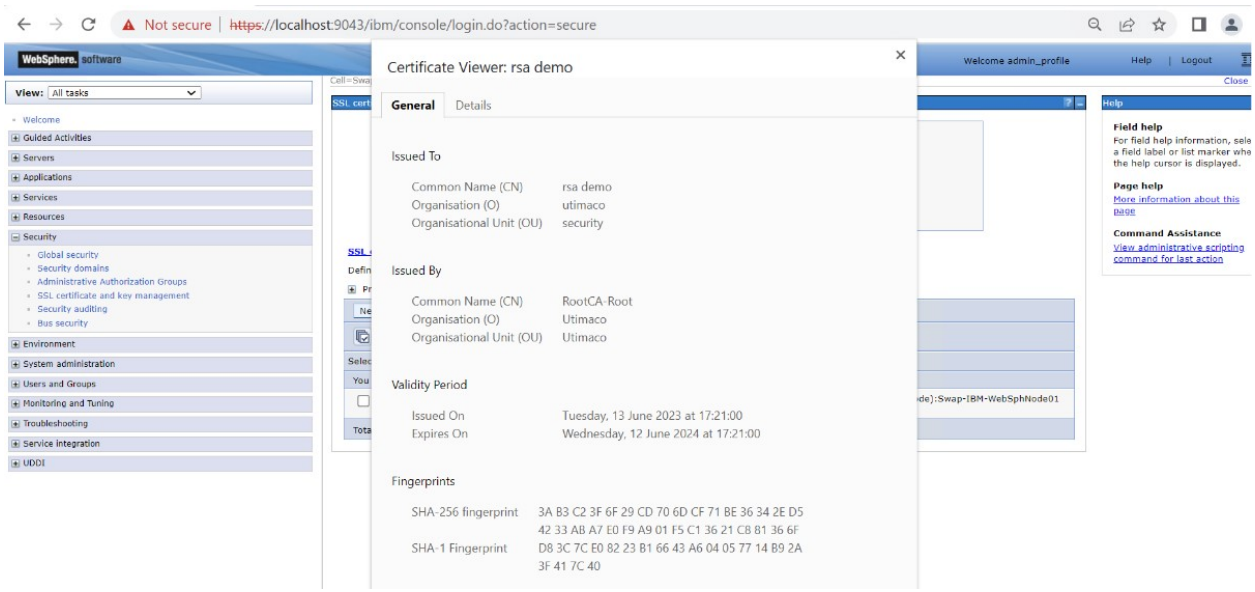


Figure 45 : Loading page over https

This completes the Integration for IBM WebSphere Application Server with Utimaco SecurityServer.

7 Troubleshooting

Error	Diagnosis
LoginUser= failed: 22.05.2023 09:58:41 src/p11adm_R2.c[429] p11_login: C_Login [type=1] returned Error 0x00000032 (CKR_DEVICE_REMOVED)	Check if HSM is reachable from host machine and HSM is up and running.
The CryptoServer PKCS#11 Library R3 is not initialized. Error CKR_CRYPTOKI_NOT_INITIALIZED occurred	PKCS#11 Slot is not initialized.

Table 6: List of Errors and their Diagnoses

8 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website: https://utimaco.com/.

9 References

Reference	Title/Company	Document No.
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSTrSh]	CryptoServer Troubleshooting/Utimaco IS GmbH	M011-0008-en
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSP11Tool2]	CryptoServer_p11tool2_Manual.pdf	2012-0004
[CSPKCSM]	CryptoServer - PKCS#11 P11CAT Manual	M013-0001-en
[CSLAN5]	CryptoServerLAN_Manual_Systemadministrators.pdf	2018-0004

Table 7: References

10 Contact Information and Support

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.