THALES

IBM HTTP Server & IBM WebSphere Application Server: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-009320-001
Revision	AB
Release Date	8 January 2021

Trademarks, Copyrights, and Third-Party Software

Copyright © 2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

CONTENTS

Copyright © 2021 Thales Group

Overview

This document provides the necessary information to install, configure, and integrate IBM HTTP Server and IBM WebSphere Application Server with Luna HSM devices and Luna Cloud HSM services. IBM WebSphere Application Server is a software platform for deploying enterprise Java-based applications utilizing IBM HTTP Server. IBM WebSphere Application Server provides key management security for certificates and certificate-based authentication. With IBM WebSphere Application Server, users can import trusted CA certificates from a software-based keystore to a hardware-based keystore, and generate self-signed certificates and personal certificate requests using the IBM Key Management Utility (iKeyman). IBM WebSphere Application Server utilizes the following APIs:

- PKCS #11
- JCA/JCE
- IBM Java Secure Sockets Extension (JSSE)

The Luna HSM solutions for IBM WebSphere Application Server provide secure key management, accelerated signing for private keys associated with the IBM WebSphere Application Server, and secure SSL Acceleration. SSL acceleration is accomplished on the IBM WebSphere Application Server through implementing the Java Secure Sockets Extension (JSSE) Provider. Following are the benefits of using Luna HSM devices or Luna Cloud HSM services to generate the keys (RSA/ECDSA) and certificate for IBM HTTP Server and WebSphere Application Server:

- Secure generation, storage, and protection of the private keys on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- Access to the HSM audit trail*.
- Significant performance improvements by off-loading cryptographic operations from signing servers.

*Luna Cloud HSM services do not have access to the secure audit trail.

Certified Platforms

This integration is certified on the following platforms:

HSM Type	Platforms Certified
Luna HSM	RHEL AIX Solaris SPARC Windows Server

NOTE: This integration is tested with Luna HSM clients in HA Mode. IBM HTTP Server integration with Luna HSM in FIPS mode is supported from Luna HSM firmware 7.7.0 onwards.

Copyright © 2021 Thales Group

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. The Luna HSM on premise offerings include the Luna Network HSM, PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

HSM Type	Platforms Certified
Luna Cloud HSM	RHEL Windows Server

Luna Cloud HSM: Luna Cloud HSM is a cloud-based platform that provides on-demand HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective, and easy to manage because there is no hardware to buy, deploy, and maintain. As an Application Owner, you click and deploy services, generate usage reports, and maintain just the services you need.

Prerequisites

Before you begin this integration, complete the following tasks:

Configure Luna HSM

Configure Luna Cloud HSM Service

Set up IBM HTTP Server and WebSphere Application Server

Configure Luna HSM

If you are using Luna HSM:

1. Verify the HSM is set up, initialized, provisioned, and ready for deployment.
2. Create a partition that will be later used by IBM HTTP Server and IBM WebSphere Application Server.
3. If using a Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize the Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
# /usr/safenet/lunaclient/bin/lunacm

lunacm.exe (64-bit) v10.3.0-273. Copyright (c) 2020 SafeNet. All rights
reserved.

Available HSMs:

Slot Id -> 0

Label -> IBM
```

Copyright © 2021 Thales Group

```
Serial Number -> 1238696044952
Model -> LunaSA 7.4.0
Firmware Version -> 7.4.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> Non-FM
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

> **NOTE:** Refer to Luna HSM documentation for detailed steps about creating NTLS connection, initializing the partitions, and assigning various user roles.

Set up Luna HSM High-Availability

Refer to Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work so that if the primary goes down due to any reason all calls automatically route to the secondary until the primary recovers and starts up.

Set up Luna HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna HSM in FIPS mode, you have to make the following change in the configuration file:

```
[Misc]
RSAKeyGenMechRemap=1
```

The above setting redirects the older calling mechanism to a new approved mechanism when Luna HSM is in FIPS mode.

> **NOTE:** The above setting is not required for Universal Client. This setting is applicable only for Luna Client 7.x.

Copyright © 2021 Thales Group

Configure Luna Cloud HSM Service

You can configure Luna Cloud HSM Service in the following ways:

> Standalone Cloud HSM service using minimum client package

> Standalone Cloud HSM service using full Luna client package

> Luna HSM and Luna Cloud HSM service in hybrid mode

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

```
[Windows]
cvclient-min.zip
[Linux]
cvclient-min.tar
# tar -xvf cvclient-min.tar
```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

```
[Windows]
Right-click setenv.cmd and select Run as Administrator.
[Linux]
Source the setenv script.
# source ./setenv
```

5. Run the LunaCM utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

```
[Windows]
cvclient-min.zip
[Linux]
```

Copyright © 2021 Thales Group

```
cvclient-min.tar
# tar -xvf cvclient-min.tar
```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

```
[Windows]
Right-click setenv.cmd and select Run as Administrator.
[Linux]
Source the setenv script.
# source ./setenv
```

5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

Cloud HSM Certificates:

```
server-certificate.pem
partition-ca-certificate.pem
partition-certificate.pem
```

LunaClient Certificate Directory:

```
[Windows default location for Luna Client]
C:\Program Files\Safenet\Lunaclient\cert\
[Linux default location for Luna Client]
/usr/safenet/lunaclient/cert/
```

> **NOTE:** Skip this step for Luna Client v10.2 or higher.

6. Open the configuration file from the Cloud HSM service client directory and copy the XTC and REST section.

```
[Windows]
crystoki.ini
[Linux]
Chrystoki.conf
```

7. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.
8. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

[XTC]

```
. . .
PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
. . .
```

Copyright © 2021 Thales Group

```
[REST]
. . .
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
. . .
```

> **NOTE:** Skip this step for Luna Client v10.2 or higher.

9. Edit the following entry from the Misc section and update the correct path for the plugins directory:

```
Misc]
PluginModuleDir=<LunaClient_plugins_directory>

[Windows Default]

C:\Program Files\Safenet\Lunaclient\plugins\

[Linux Default]

/usr/safenet/lunaclient/plugins/
```

   Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.

10. Reset the ChrystokiConfigurationPath environment variable and point back to the location of the Luna Client configuration file.

    [Windows]

    In the Control Panel, search for "environment" and select Edit the system environment variables. Click Environment Variables. In both list boxes for the current user and system variables, edit ChrystokiConfigurationPath and point to the crystoki.ini file in the Luna client install directory.

    [Linux]

    Either open a new shell session, or export the environment variable for the current session pointing to the location of the Chrystoki.conf file:

```
# export ChrystokiConfigurationPath=/etc/
```

11. Run the LunaCM utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

> **NOTE:** Follow the Luna Cloud HSM documentation for detailed steps for creating service, client, and initializing various user roles.

Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the Standalone Cloud HSM service using full Luna client package section above.

> **NOTE:** Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Copyright © 2021 Thales Group

To use Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, enable the Allow non-FIPS approved algorithms check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Set up IBM HTTP Server and WebSphere Application Server

Install IBM HTTP Server and IBM WebSphere Application Server on the target machine to complete the integration process. Download and install IBM Agent to install and configure IBM HTTP Server and WebSphere Application Server. Refer to the IBM HTTP Server and IBM WebSphere Application Server Documentation for detailed installation procedures.

Integrate IBM HTTP Server and IBM WebSphere Application Server with Luna HSM

To integrate IBM HTTP Server and IBM WebSphere Application Server with Luna HSM, you need to complete the following tasks:

> Configure the iKeyman to recognize a Luna HSM
> Configure SSL using Luna HSM for IHS
> Configure IBM WebSphere Application Server using Luna HSM
> Configure SSL using Luna HSM for WAS

Configure the iKeyman to recognize a Luna HSM

Complete the following procedures as the root user to configure the IBM Key Management Utility (iKeyman) to recognize and use the Luna HSM or Luna Cloud HSM service for cryptographic operations:

1. Create a file named **luna.cfg** that contains the information about the Luna HSM partition or Luna Cloud HSM service.

   The required entries in **luna.cfg** are:

```
name = LUNA
library = <Path to Cryptoki library>
description = Luna config
slotListIndex = 0
attributes (*, *, *) = {
CKA_TOKEN= true
}
attributes (*, CKO_PRIVATE_KEY, *) = {
CKA_SENSITIVE = true
CKA_SIGN=true
CKA_DECRYPT=true
```

Copyright © 2021 Thales Group

```
}
attributes (*, CKO_PUBLIC_KEY, *) = {
CKA_VERIFY=true
CKA_ENCRYPT=true
}
attributes (*, CKO_SECRET_KEY, *) = {
CKA_SENSITIVE = true
CKA_ENCRYPT=true
CKA_DECRYPT=true
CKA_SIGN=true
CKA_VERIFY=true
}
disabledMechanisms = {
CKM_SHA1_RSA_PKCS
}
```

> **NOTE:** IBM HTTP Server 8.5.5 and earlier versions only support a 32-bit Cryptoki library version on Windows operating systems. Therefore, if you are using IBM HTTP Server 8.5.5 or an earlier version, use the 32-bit Cryptoki library path in the library field.
>
> IBM HTTP Server 9.0.0 and later versions support the 64-bit Cryptoki library version on Windows operating systems. Therefore, if you are using IBM HTTP Server 9.0.0 or a later version, use the 64-bit Cryptoki library path in the library field.

2. Update the **java.security** file located in the directory:

   UNIX: `<HTTP Server Installation Directory>/java/jre/lib/security`

   Windows: `<HTTP Server Installation Directory>\java\jre\lib\security`

   To include the following:

   ```
   security.provider.x=com.ibm.security.cmskeystore.CMSProvider
   security.provider.x=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl <Path of luna.cfg file>
   ```

   For example:

   ```
   # List of providers and their preference orders (see above):
   security.provider.1=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.2=sun.security.provider.Sun
   security.provider.3=com.ibm.crypto.provider.IBMJCE
   security.provider.4=com.ibm.jsse.IBMJSSEProvider
   security.provider.5=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.6=com.ibm.security.cert.IBMCertPath
   ```

Copyright © 2021 Thales Group

```
security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl <Path
of luna.cfg file>
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

If using UNIX, add the following entry to the Luna HSM configuration file **Chrystoki.conf** for HTTP Server:

```
Misc = {
Apache = 1;
}
```

3. Restart the HTTP Server.

   UNIX

   ```
   <HTTP Server Installation Directory>/bin/apachectl -k restart
   ```

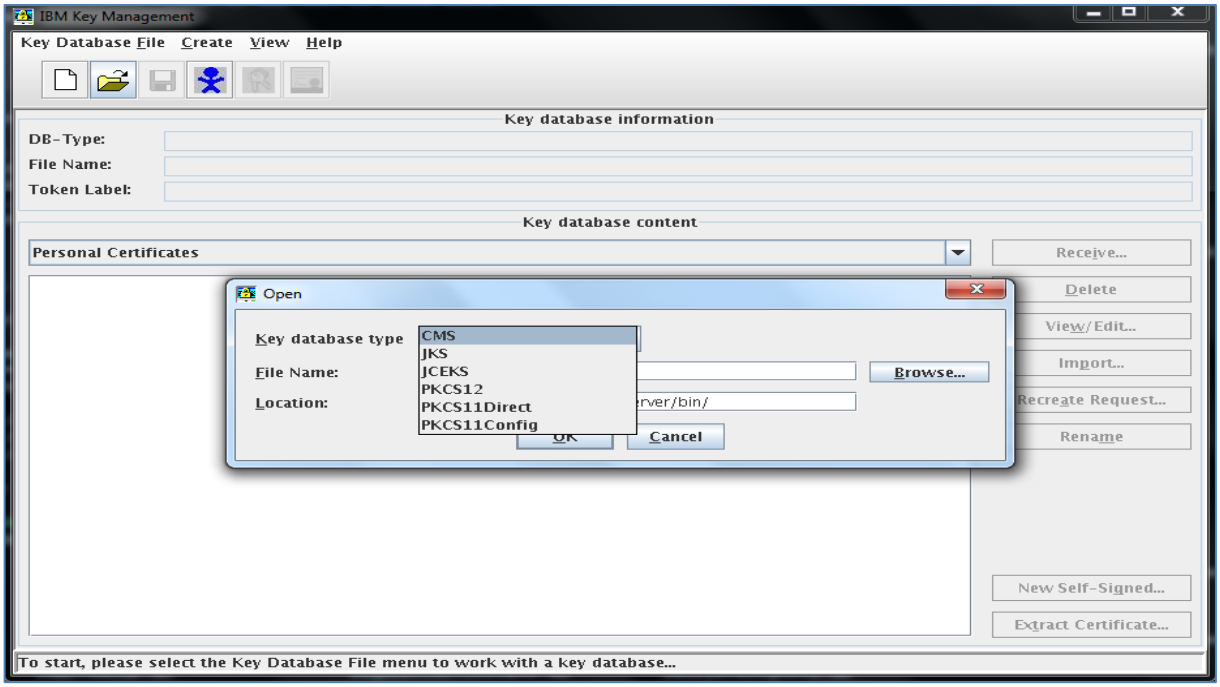
   Windows

   ```
   <HTTP Server Installation Directory>\bin\apache.exe -k restart
   ```

4. Run the **IBM Key Management Utility** (ikeyman) using the command below:

   ```
   # <HTTPServer-Installation-Directory>/bin/ikeyman.sh
   ```

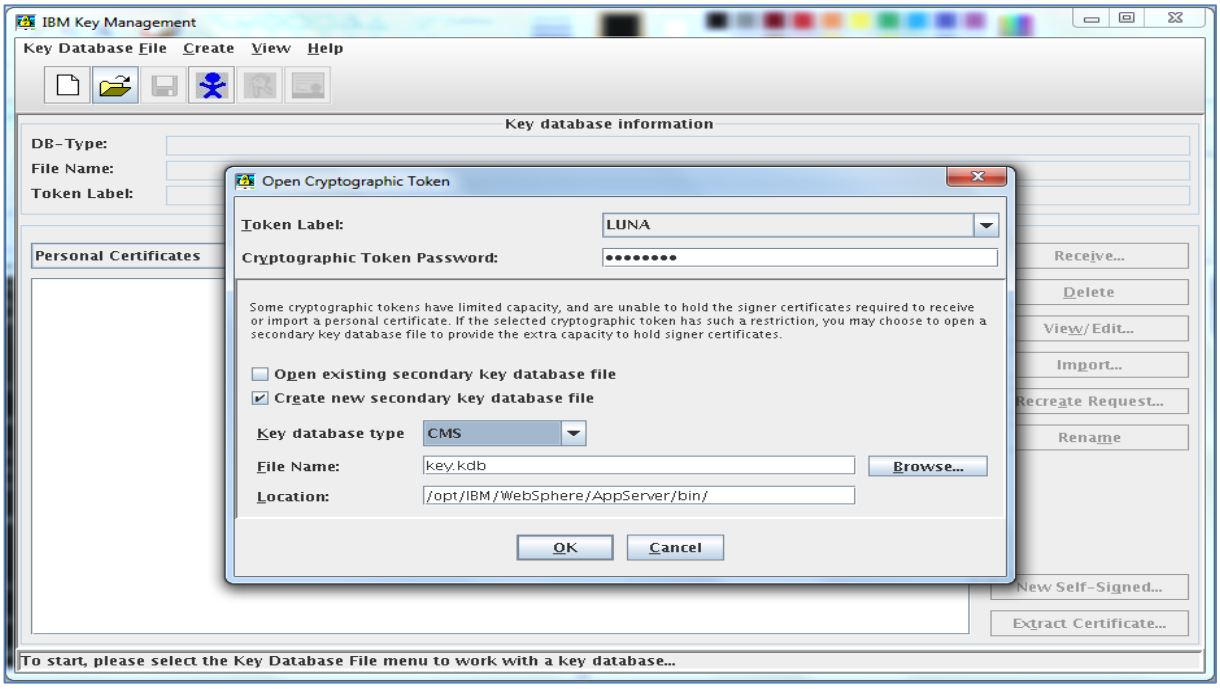
5. Click **Key Database File** > **Open** and select **PKCS11Config** from the **Key database type** drop-down menu.



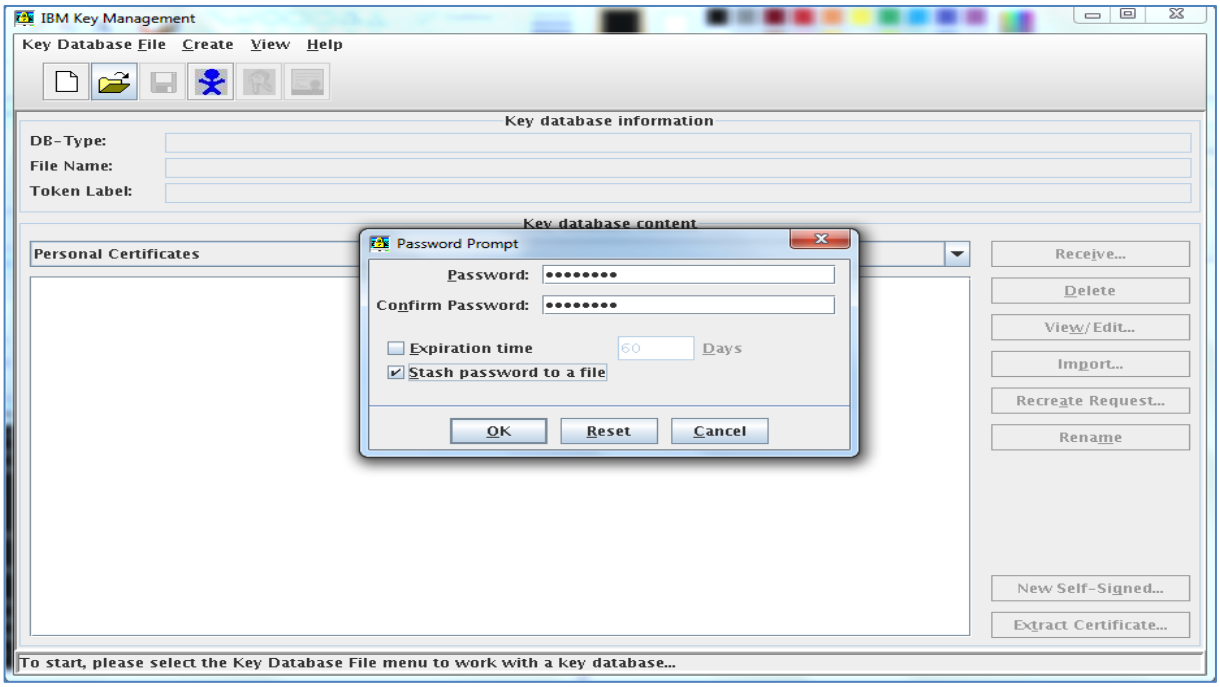
6. Select **LUNA** from the **Token Label** drop-down menu and enter the partition password in the **Cryptographic Token Password** field. Select the **Create new secondary key database file** check

Copyright © 2021 Thales Group

box, select **CMS** from the **Key database type** drop-down menu, browse the location where you want to save **key.kdb** file, and then click **OK**.

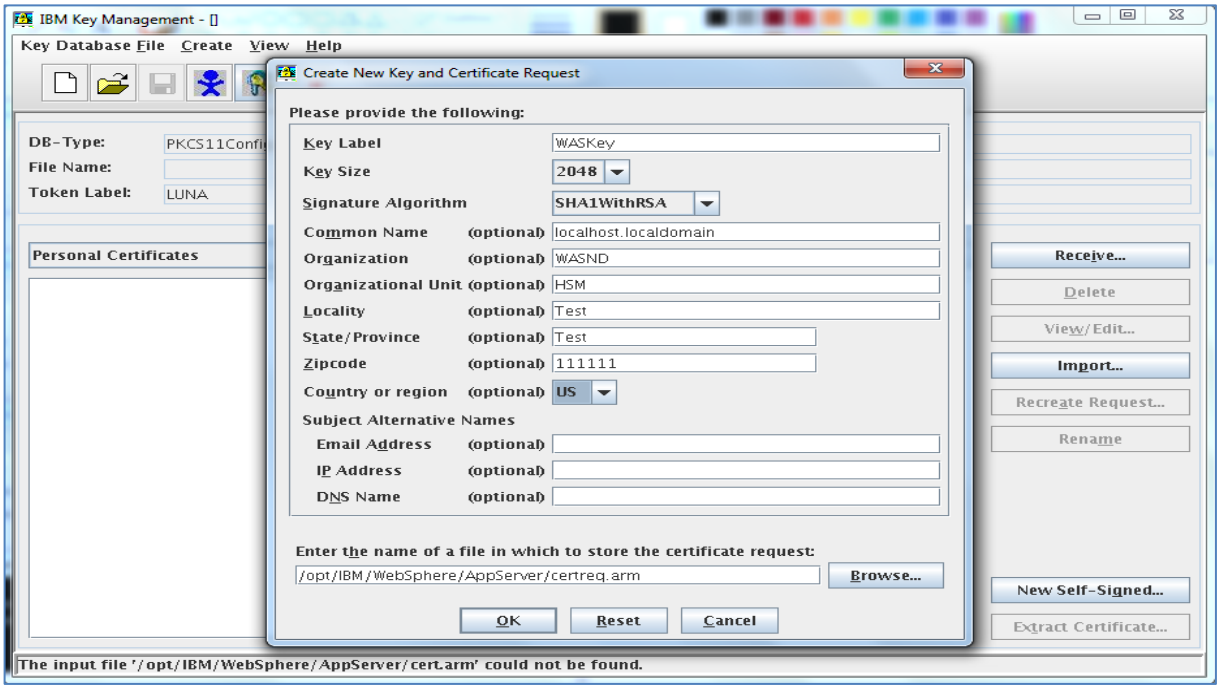


7. Enter the password for Key Database File in the **Password** and **Confirm Password** fields and select the **Stash password to a file** check box. Click **OK**.



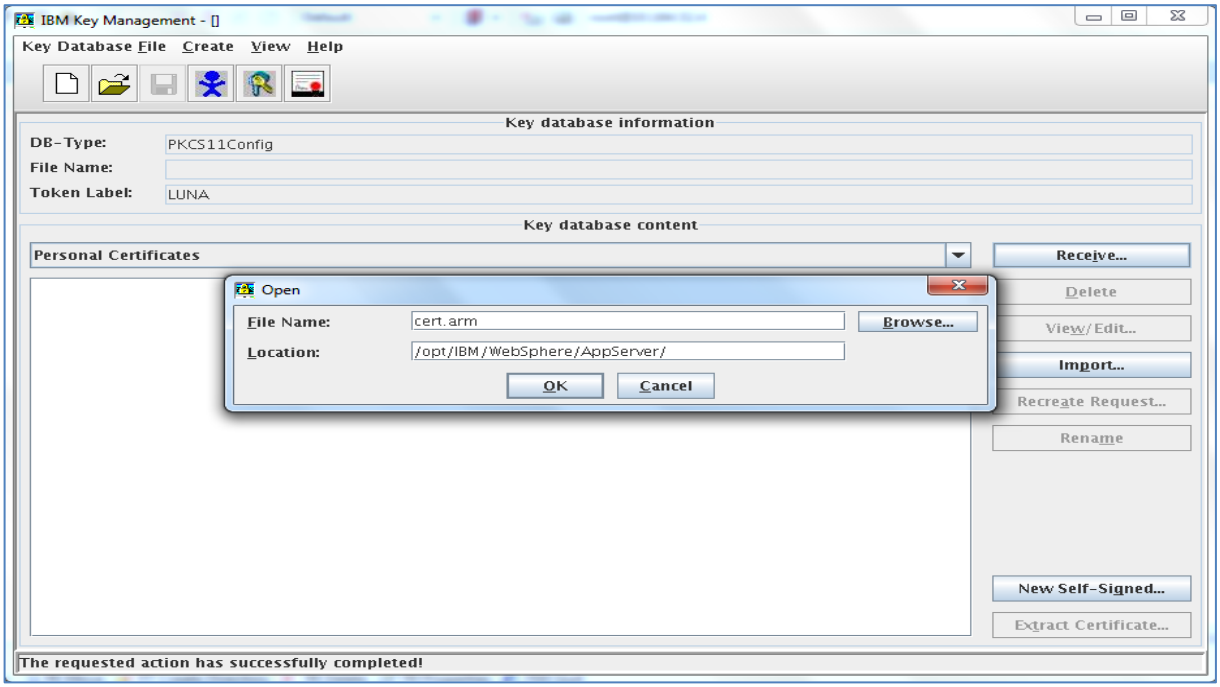
Copyright © 2021 Thales Group

8. Click **Create** > **New Certificate Request**, enter the certificate details, and browse the file in which you want to store the certificate request. Click **OK**.



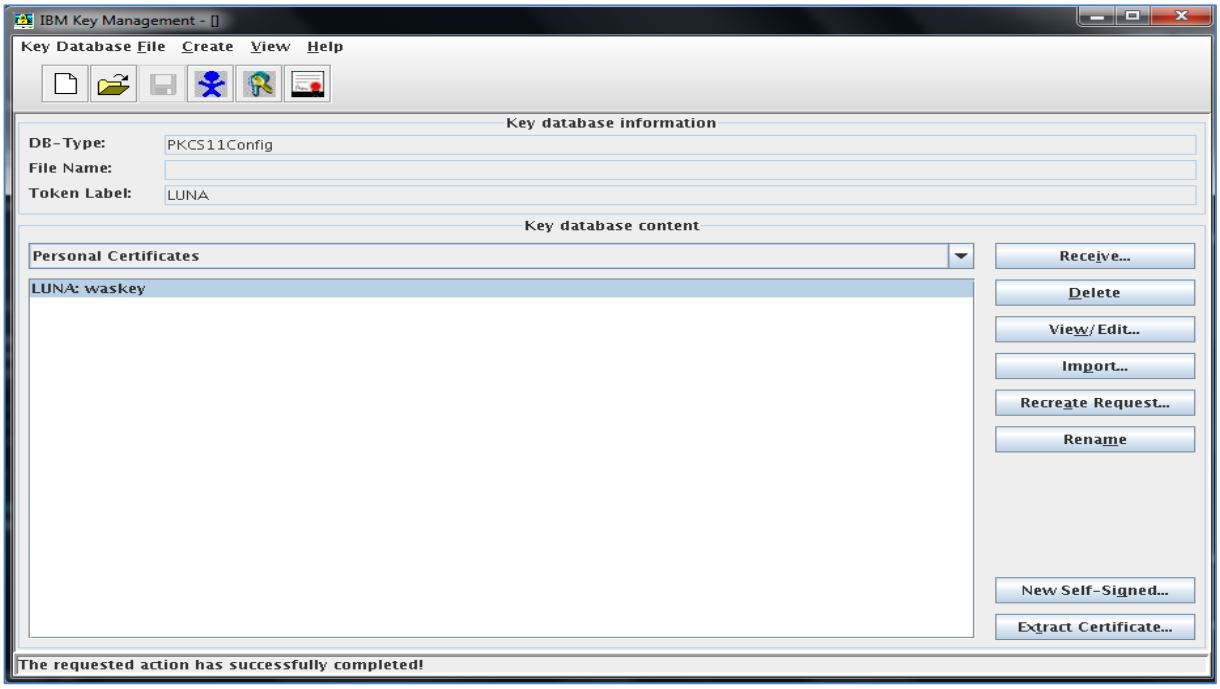
9. Minimize the **IBM Key Management** console and open the certificate request file. Copy the contents, and send the certificate request to the CA. Save the response received from the certificate authority.

10. Open the **IBM Key Management** console and select **Personal Certificates**. Click **Receive…**. **Browse** and select the signed certificate received from CA. Click **OK**.



Copyright © 2021 Thales Group

11. Verify that the certificate has been successfully stored on the Luna HSM partition or Luna Cloud HSM service with the label "**Token Label: Certificate Name**". Close the **IBM Key Management Utility**.



Configure SSL using Luna HSM for IHS

Follow these steps to enable the Secure Sockets Layer (SSL) using Luna HSM on the IBM HTTP Server:

1. Open the shell and navigate to directory `<HTTP Server Installation Directory>/bin`.
2. Save the Luna HSM partition password or Luna Cloud HSM service password using the `SSLStash` Utility and execute the following command:

   UNIX

   ```
   ./sslstash -c <IBM HTTP Server Installation Directory>/conf/ssl.passwd
           crypto "<partition-password>"
   ```

   Windows

   ```
   SSLStash.exe -c "<IBM HTTP Server Installation Directory>\conf\ssl.passwd"
           crypto "<partition password>"
   ```

3. Enable SSL Security for HTTP Server and execute the following command:

   UNIX

   ```
   ./gskcmd -keydb -stashpw -db key.kdb -pw <password>
   ./gskcapicmd -keydb -stashpw -db key.kdb -pw <password>
   ```

   Windows

   ```
   gskcmd.bat -keydb -stashpw -db key.kdb -pw <password>
   gskcapicmd -keydb -stashpw -db key.kdb -pw <password>
   ```

Copyright © 2021 Thales Group

4. Modify and add SSL Security settings to <HTTPServer-Installation-Directory>/conf/httpd.conf. Add or uncomment the appropriate lines throughout the file so that it appears as follows in the Virtual Host section:

```
LoadModule ibm_ssl_module  modules/mod_ibm_ssl.so
Listen *:443
<VirtualHost *:443>
SSLEnable
KeyFile <Path to key.kdb file>
SSLServerCert <partition name>:<key label>
SSLClientAuth None
SSLPKCSDriver <Path to Cryptoki library>
SSLStashfile <Path to ssl.passwd file>
</VirtualHost>
```

5. Restart the HTTP Server.

   UNIX

```
<HTTP Server Installation Directory>/bin/apachectl –k restart
```

   Windows

```
<HTTP Server Installation Directory>\bin\apachectl.exe –k restart
```

6. Open the browser and type the following web address: https://<hostname or ip address>:443.

   This will display the Welcome to the HTTP Server web page.

Configure IBM WebSphere Application Server using Luna HSM

After you have installed IBM WebSphere Application Server, complete the following procedure for configuration:

1. Create a file named luna.cfg containing information about the Luna HSM partition or Luna Cloud HSM service. The required entries in luna.cfg are:

```
name = LUNA
library = <Path to Cryptoki library>
description = Luna config
slotListIndex = 0
attributes (*, *, *) = {
CKA_TOKEN= true
}
attributes (*, CKO_PRIVATE_KEY, *) = {
CKA_SENSITIVE = true
CKA_SIGN=true
CKA_DECRYPT=true
```

Copyright © 2021 Thales Group

```
}
attributes (*, CKO_PUBLIC_KEY, *) = {
CKA_VERIFY=true
CKA_ENCRYPT=true
}
attributes (*, CKO_SECRET_KEY, *) = {
CKA_SENSITIVE = true
CKA_ENCRYPT=true
CKA_DECRYPT=true
CKA_SIGN=true
CKA_VERIFY=true
}
disabledMechanisms = {
CKM_SHA1_RSA_PKCS
}
```

> **NOTE:** IBM HTTP Server 8.5.5 and earlier versions only support a 32-bit Cryptoki library version on Windows operating systems. If using IBM HTTP Server 8.5.5 or an earlier version, use the 32-bit Cryptoki library path in the library field.
>
> IBM HTTP Server 9.0.0 and later versions support the 64-bit Cryptoki library version on Windows operating systems. If using IBM HTTP Server 9.0.0 or a later version, use the 64-bit Cryptoki library path in the library field.

2. Add the following text to the java.security file located in directory `<IBM WebSphere Installation Directory>/AppServer/java/jre/lib/security`:

```
security.provider.x=com.ibm.security.cmskeystore.CMSProvider
security.provider.x=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl <Path of luna.cfg file>
```

For example:

```
# List of providers and their preference orders (see above):
security.provider.1=com.ibm.security.jgss.IBMJGSSProvider
security.provider.2=sun.security.provider.Sun
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.jsse.IBMJSSEProvider
security.provider.5=com.ibm.jsse2.IBMJSSEProvider2
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl <Path of luna.cfg file>
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
```

Copyright © 2021 Thales Group

```
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

3. Restart WebSphere Application Server:

   UNIX

```
<IBM WebSphere Installation
        Directory>/AppServer/profiles/AppSrv01/bin/stopServer.sh
        <servername>

        <IBM WebSphere Installation
        Directory>/AppServer/profiles/AppSrv01/bin/startServer.sh
        <servername>
```

   Windows

```
<IBM WebSphere Installation

Directory>\AppServer\profiles\AppSrv01\bin\stopServer.bat <server_name>

<IBM WebSphere Installation

Directory>\AppServer\profiles\AppSrv01\bin\startServer.bat <server_name>
```

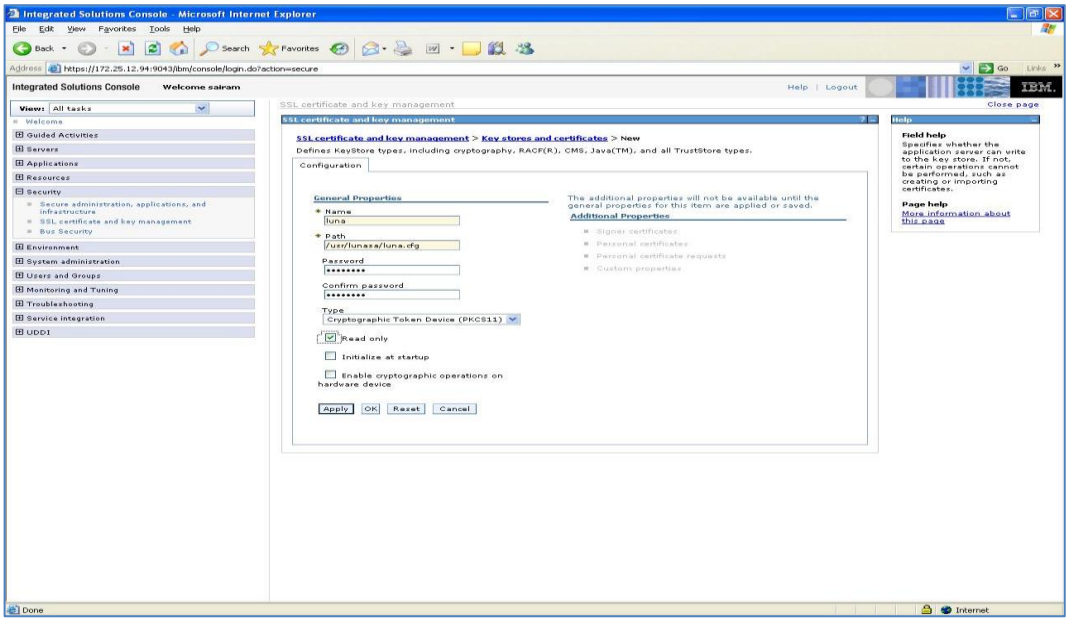
Configure SSL using Luna HSM for IBM WAS

After the server is set up and operational, you can configure it to use the Luna HSM for cryptographic operations. For this you need to complete the following steps in the administrative console http://<hostname or ipaddress>:9060/ibm/console:

1. Log in to the IBM WAS admin console.
2. Click **Security** > **SSL certificate and Key management** > **Key stores and certificates**.
3. Click **New**. Type a name to identify the keystore. This name is used to enable hardware cryptography in the Web services security configuration.
4. Type the path for the hardware device-specific configuration file **<Path to Luna cfg file>**.
5. Type a password if the token login is required. Select **Cryptographic Token Device (PKCS11)** as the type.

Copyright © 2021 Thales Group

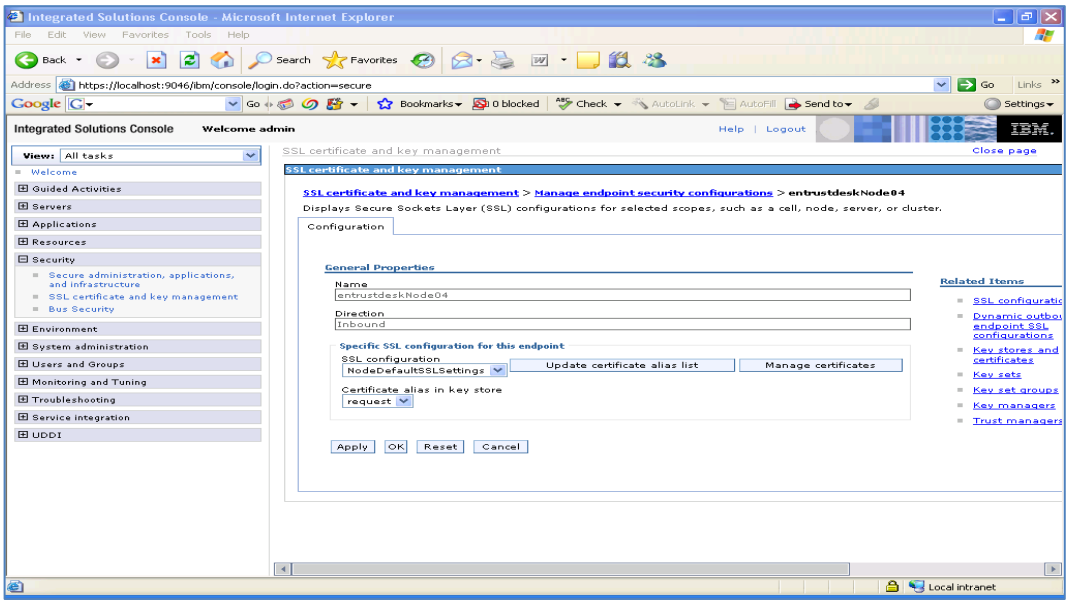
6. Select the **Read only** check box. Click **OK** and **Save**.



7. Click **Security** > **SSL Certificate and Key Management** > **SSL Configurations** > **Node Default SSLSettings**. For the keystore name, select the newly created keystore and click **Get Certificate Aliases**.

8. The **Default server certificate alias** and **Default client certificate alias** drop-down menu will list all certificates present on the Luna HSM. Select any one certificate. Click **OK** and **Save**.

9. Click **Security** > **SSL certificate and Key management** > **Manage endpoint security configurations** > **Inbound | Outbound** > **SSL_configuration_name**. Select **SSL configuration** as **NodeDefaultSSLSettings** and click **Update certificate alias list**. The **Certificate alias in keystore** drop-down box lists all the certificates present on the Luna HSM. Select the certificate. Click **OK** and **Save**.



Copyright © 2021 Thales Group

10. Restart WebSphere Application Server:

    UNIX

    ```
    <IBM WebSphere Installation
    Directory>/AppServer/profiles/AppSrv01/bin/stopServer.sh <servername>
    <IBM WebSphere Installation
    Directory>/AppServer/profiles/AppSrv01/bin/startServer.sh <servername>
    ```

    Windows

    ```
    <IBM WebSphere Installation
    Directory>\AppServer\profiles\AppSrv01\bin\stopServer.bat <server_name>
    <IBM WebSphere Installation
    Directory>\AppServer\profiles\AppSrv01\bin\startServer.bat <server_name>
    ```

11. Use the **Retrievesigners** Utility to add server certificate to the **ClientDefaulttrust** store from **CellDefaulttruststore**.

    UNIX

    ```
    <IBM WebSphere Installation
    Directory>/AppServer/profiles/AppSrv01/bin/retrieveSigners.sh
    <CellDefaulttruststore> <ClientDefaulttrust>
    ```

    Windows

    ```
    <IBM WebSphere Installation
    Directory>\AppServer\profiles\AppSrv01\bin\retrieveSigners.bat
    <CellDefaulttruststore> <ClientDefaulttrust>
    ```

12. Log out and log in to the administrative console on the configured secure port or https://<ipaddress>:9043/ibm/console.

13. The administrative console default page will be displayed.

This completes IBM HTTP Server and WebSphere Application Server Integration with Luna HSM by securing SSL private keys/certificate on Luna HSM.

Copyright © 2021 Thales Group

Contacting Customer Support

If you encounter a problem during this integration, contact your supplier or Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.

Copyright © 2021 Thales Group