All information herein is either public information or is the property of and owned solely by Gemalto NV, and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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.

Document Part Number: 007-009320-001, Rev. L

Release Date: March 2016
Contents

Preface .................................................................................................................................. 4
Scope ........................................................................................................................................... 4
Document Conventions ................................................................................................................. 4
Command Syntax and Typeface Conventions .............................................................................. 5
Support Contacts ......................................................................................................................... 6

1 Introduction ...................................................................................................................... 7
Overview ...................................................................................................................................... 7
3rd Party Application Details ........................................................................................................ 7
Supported Platforms .................................................................................................................... 7
Prerequisites .................................................................................................................................. 8
SafeNet Network HSM Setup ...................................................................................................... 8

2 IBM WebSphere & HTTP Server V8.0.0/8.5.5 with SafeNet Luna HSM ...................... 10
Installation Overview ................................................................................................................... 10
RHEL 6.5/AIX7.1 ........................................................................................................................ 10
Windows 2008 R2 ...................................................................................................................... 21

3 IBM WebSphere & HTTP Server V7.0 with SafeNet Luna HSM ................................... 26
Solaris 10 SPARC (64-bit) ......................................................................................................... 26

4 IBM WebSphere & HTTP Server V6.1 with SafeNet Luna HSM ................................... 40
Installation Overview ................................................................................................................... 40
AIX ............................................................................................................................................... 40
Windows XP SP2 (32-bit) .......................................................................................................... 55
RHEL 5 (32-bit) ......................................................................................................................... 69

5 Integration of WebSphere Network Deployment with SafeNet Luna HSM ............... 82
Deploying an application to the cluster ......................................................................................... 91

6 Troubleshooting ............................................................................................................. 94
Troubleshooting ........................................................................................................................ 94
Problem ...................................................................................................................................... 94
Solution ...................................................................................................................................... 94
Preface

This document covers the necessary information to install, configure, and integrate IBM HTTP Server and IBM WebSphere Application Server with SafeNet Luna Hardware Security Module.

Scope

This technical integration guide provides an overview of how to integrate IBM HTTP Server and IBM WebSphere Application Server with SafeNet HSM.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.
## Command Syntax and Typeface Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>The bold attribute is used to indicate the following: Command-line commands and options (Type <code>dir /p</code>.) Button names (Click <strong>Save As</strong>.) Check box and radio button names (Select the <strong>Print Duplex</strong> check box.) Window titles (On the <strong>Protect Document</strong> window, click <strong>Yes</strong>.) Field names (<strong>User Name</strong>: Enter the name of the user.) Menu names (On the <strong>File</strong> menu, click <strong>Save</strong>.) (Click <strong>Menu &gt; Go To &gt; Folders</strong>.) User input (In the <strong>Date</strong> box, type <strong>April 1</strong>.)</td>
</tr>
<tr>
<td><strong>italic</strong></td>
<td>The italic attribute is used for emphasis or to indicate a related document. (See the <strong>Installation Guide</strong> for more information.)</td>
</tr>
<tr>
<td><strong>Consolas</strong></td>
<td>Denotes syntax, prompts, and code examples.</td>
</tr>
</tbody>
</table>
Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>US</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>
Overview

IBM WebSphere Application Server is a software platform for deploying enterprise Java-based applications utilizing IBM HTTP Server. We provide Key Management security for Certificates and certificate-based authentication, including import of trusted CA certificates from software-based keystore to hardware-based keystore, generation of self-signed certificates and personal certificate requests via IBM Key Management Utility. In addition, the IBM HTTP Server can be configured to use our HSM for SSL connectivity. IBM WebSphere Application Server utilizes the following APIs: PKCS #11, JCA/JCE and their own JSSE implementation that makes calls to the PKCS #11 library.

The SafeNet HSM solutions for IBM WebSphere Application Server provide secure key management and accelerated signing for private keys associated with the IBM WebSphere Application Server as well as secure SSL Acceleration. SSL acceleration is accomplished by IBM WebSphere Application Server through JSSE (Java Secure Sockets Extension) Provider.

3rd Party Application Details

- IBM HTTP Server
- IBM WebSphere Application Server

Supported Platforms

<table>
<thead>
<tr>
<th>IBM WAS</th>
<th>IBM HTTP Server</th>
<th>Platforms Tested</th>
<th>Luna Client Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS 8.5.5</td>
<td>IHS 8.5.5 FP2</td>
<td>RHEL 6.5</td>
<td>Luna 6.1 with patch (630-010487-001_SW_Patch_WebspHERE_Issue_Luna_Clint_6.1_Alpha1) on firmware version 6.23 and Luna 6.2 with patch (630-010487-001_SW_Patch_WebspHERE_Issue_Luna_Clint_6.1_Alpha1) on firmware version 6.24</td>
</tr>
<tr>
<td>IBM WAS</td>
<td>IBM HTTP Server</td>
<td>Platforms Tested</td>
<td>Luna Client Software version</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>WAS 8.5.5</td>
<td>IHS 8.5.5 FP2</td>
<td>AIX 7.1</td>
<td>Luna 5.x (v5.3) Apply Luna SA patch 630-010372-001 SW PATCH, LUNASA, TO CLIENT 5.3.1, SHIM HTTPD AIX, ALPHA</td>
</tr>
<tr>
<td>WAS 8.0.0</td>
<td>NA</td>
<td>Windows 2008R2</td>
<td>5.x (v5.2.1)</td>
</tr>
<tr>
<td>WAS 7.0 FP11</td>
<td>IHS7.0 FP29 (32 bit), Java version 1.6.0_45</td>
<td>AIX 6.1</td>
<td>5.x (v5.1.1, 5.2.1)</td>
</tr>
<tr>
<td>WAS 7.0 FP21 (32bit)</td>
<td>IHS7.0 with FP 21,25,29 (32 bit)</td>
<td>Solaris SPARC 10</td>
<td>5.x (v5.2.1)</td>
</tr>
<tr>
<td>WAS 6.1</td>
<td>IHS 6.1</td>
<td>AIX 5.3(64-bit) RHEL 5, Windows XP</td>
<td>4.x (v4.2)</td>
</tr>
<tr>
<td>WAS Network Deployment 8.5.5</td>
<td>NA</td>
<td>RHEL 6.0</td>
<td>Luna 5.x (v5.4.2)</td>
</tr>
</tbody>
</table>

**NOTE:** For Luna SA 5.3 on Aix please apply Luna SA patch 630-010372-001 SW PATCH, LUNASA, TO CLIENT 5.3.1, SHIM HTTPD AIX, ALPHA, contact SafeNet Support for the patch.

**Prerequisites**

**SafeNet Network HSM Setup**

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started ensure the following:

- SafeNet Network HSM appliance and a secure admin password
- SafeNet Network HSM, and a hostname, suitable for your network
- SafeNet Network HSM network parameters are set to work with your network
- Initialized the HSM on the SafeNet Network HSM appliance.
- Created and exchanged certificates between the SafeNet Network HSM and your Client system.
• Created a partition on the HSM, remember the partition password that will be later used by IBM. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Network HSM.

• Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).
IBM WebSphere & HTTP Server V8.0.0/8.5.5 with SafeNet Luna HSM

Installation Overview

Below is the list of supported platforms tested with 8.5.5 (FP2):

- RHEL6.5
- AIX 7.1

RHEL 6.5/AIX 7.1

Integrating IBM HTTP Server V8.5.5 (FP2) with SafeNet Luna HSM

To configure the IBM Key Management Utility to recognize the SafeNet Luna HSM cryptographic device:

1. Ensure that the file `libshim.so` is in the directory `/usr/safenet/lunaclient/lib`. For Luna 6.1.0, use the shim provided by SafeNet(630-010487-001_SW_Patch_Websphere_Issue_Luna_Clnt_6.1_Alpha2)

2. For IBM HTTP Server Modify the java.security file located in directory: `/opt/IBM/HTTPServer/java/jre/lib/security` to include the following entry:

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

# List of providers and their preference orders (see above):
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
security.provider.4=com.ibm.security.cert.IBMCertPath
security.provider.5=com.ibm.security.cmskeystore.CMSProvider
security.provider.6=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl <Path of luna.cfg file>
security.provider.7=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.8=com.ibm.security.sasl.IBMSASL
security.provider.9=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.10=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.11=org.apache.harmony.security.provider.PolicyProvider

The required entries in luna.cfg are:

```
name = LUNA
library = <Path to Cryptoki Library> for Ex /usr/safenet/lunaclient/lib/libcklog2.so
description = Luna config
tokenLabel = <partition name>
attributes (*, CKO_PRIVATE_KEY, *) = {
    CKA_SENSITIVE = true
}
```
attributes (*,CKO_PUBLIC_KEY, *) = {
  CKA_VERIFY = true
  CKA_ENCRYPT = true
}

3. Add the following to the SafeNet Luna HSM configuration (/etc/Chrystoki.conf) file for HTTP Server Shim Support:

```
Misc = {
  ApplicationInstance=RSA_SIGN_RAW;
  AppIdMajor=1;
  AppIdMinor=1;
}
```

4. Verify the following in the Chrystoki.conf under /etc.

**Cryptoki with Logging using Shim**

```
Chrystoki2 = {
  LibUNIX64 = /usr/safenet/lunaclient/lib/libcklog2.so;
}
CkLog2 = {
  LibUNIX64=/usr/safenet/lunaclient/lib/libshim.so;
  Enabled=1;
  File=/tmp/cklog.txt;
  Error=/tmp/error.txt;
  NewFormat=1;
  LoggingMask=ALL_FUNC;
}
Shim2 = {
  LibUNIX64=/usr/safenet/lunaclient/lib/libCryptoki2_64.so;
}
```

**Cryptoki without Logging using shim**

```
Chrystoki2 = {
  LibUNIX64 = /usr/safenet/lunaclient/lib/libshim.so;
}
Shim2 = {
  LibUNIX64=/usr/safenet/lunaclient/lib/libCryptoki2_64.so;
}
```

LibUNIX should be path to your SafeNet Luna HSM client library/ log library, path may differ from shown in above example

---

**NOTE**: Please contact SafeNet for the shim patch (630-010487-001_SW_Patch_Websphere_Issue_Luna_Cln_6.1_Alpha2). Above changes are only applicable for Luna SA 6.1.0

5. Set the JAVA_HOME environment variable.

   `<IBM HTTP Server installation Directory/AppServer/java>`

   `/opt/IBM/HTTPServer/AppServer/java`

6. Stop and start the HTTP Server.

   `/opt/IBM/HTTPServer/bin/apachectl stop`
   `/opt/IBM/HTTPServer/bin/apachectl start`
7. Open the **IBM Key Management Utility**.  
   Traverse to the directory `/opt/IBM/HTTPServer/bin/`  
   Execute `/ikeyman`.  
   The Cryptographic Token menu option displays.

8. Run the **IBM Key Management Utility** (`ikeyman`) from `<IBM HTTP Server installation directory>/bin/ikeyman.sh`, click **Key Database File** -> Open and select **PKCS11Config**.
9. 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 box.

Select **CMS** from the **key database type** drop-down menu. By default, the file name will be key.kdb. To create a file with a different name, enter new name for the file and click **OK**.
10. It will prompt for password for the key database file. Enter the **Password** and **Confirm Password** and select the **Stash password to a file** check box. Click **OK**.
11. Click **Create -> New Certificate Request**: enter the details to generate the certificate and certificate request name to save the certificate request. Click **OK**.

![Image of Certificate Request Generation](image)

12. Minimize the **IBM Key Management** console and open the certificate request file and copy the contents, send the certificate request to the CA and save the response received from certificate authority.
13. Open the **IBM Key Management** console and select **Personal Certificates** click **Receive...**, Browse and select the signed certificate received from CA. Click **OK**.
14. Verify the certificate saved successfully stored on the partition with “Token Label: Certificate Name”. Close the **IBM Key Management Utility**.

To enable SSL Security

To enable SSL security, perform the following steps:

1. Open the shell and change to directory `/opt/IBM/HTTPServer/bin`.

2. To save the SafeNet LUNA HSM partition password using the SSLStash Utility, type the following command at shell:

   ```
   ./sslstash -c /opt/IBM/HTTPServer/conf/ssl.passwd crypto “partition password”
   ```

3. To enable SSL Security, you must modify and add settings to the file located at:

   `/opt/IBM/HTTPServer/conf/httpd.conf`

4. Add or uncomment the appropriate lines throughout the file, as explained below. In the VIRTUAL HOST section, add or uncomment the line as shown in the given example:

   ```
   LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
   Listen localhost:443
   <VirtualHost localhost:443>
   SSLEnable
   KeyFile /opt/IBM/HTTPServer/bin/key.kdb
   SSLServerCert <partition name>:<key label >
   SSLClientAuth None
   SSLPKCSDriver <Path to Luna crypto lib>
   SSLStashfile /opt/IBM/HTTPServer/conf/ssl.passwd
   </VirtualHost>
   ```
5. Stop and start the HTTP Server.

Open the browser and type the following web address: https://<machinename>. You should receive a message similar to the following:

![Security Alert Window]

6. Click Yes. The Welcome to the HTTP Server web page displays.

Integrating IBM WebSphere Application Server V8.5.5 with SafeNet Luna HSM

Once you have installed IBM WebSphere Application Server, you must complete the following POST Installation instructions:

1. Modify the java.security file located in directory<IBM HTTP Server Installation Directory>/AppServer/java/jre/lib/security> for Ex- /opt/IBM/Websphere/AppServer/java/jre/lib/security to include the following:

   ```
   security.provider.1=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.2=sun.security.provider.Sun
   security.provider.3=com.ibm.crypto.provider.IBMJCEFIPS
   security.provider.4=com.ibm.crypto.provider.IBMJCE
   security.provider.5=com.ibm.jss2.IBMJSSEProvider2
   security.provider.6=com.ibm.security.cert.IBMCertPath
   security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
   security.provider.8=com.ibm.security.cmskeystore.CMSProvider
   security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
   security.provider.10=com.ibm.crypto.pkcs11.provider.IBM PKCS11
   ```

   Create configuration file luna.cfg. The required entries in luna.cfg are:

   ```
   name = LUNA
   library = /usr/lunasa/lib/ libCryptoki2.so or <Path to Luna crypto lib>
   description = Luna config
   tokenLabel = <partition name>
   attributes (*, CKO_PRIVATE_KEY, *) = {
     CKA_SENSITIVE = true
   }
   ```
attributes (*,CKO_PUBLIC_KEY, *) = {
    CKA_VERIFY = true
    CKA_ENCRYPT = true
}

2. Restart IBM WebSphere Application Server.

**Configuring a hardware cryptographic keystore**

Complete the following steps in the administrative console:

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

6. Click **Security > SSL Certificate and Key Management > SSL Configurations > Node Default SSLSettings.** Select Keystore name as new created keystore and click **Get Certificate Aliases.**

7. **Default server certificate alias** and **Default client certificate alias** drop-down box will list all the certificates present on hardware. Select any one certificate. Click **OK** and **Save.**
8. 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**. **Certificate alias in keystore** drop-down box will list all the certificates present on the hardware. Select a certificate. Click **OK** and **Save**.

9. Use **Retrievesigners Utility** to add server certificate to the **ClientDefaulttrust store** from **CellDefaulttruststore**. The utility is located under:

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/retrieveSigners.sh
```
10. Logout and restart the server. The following page is displayed before the Logging page:

![Security Alert]

11. View certificate and check. It should be same as that selected in step 8 and 9. If yes, click Yes to continue.

Windows 2008 R2

Integrating IBM WebSphere Application Server V8.0 with SafeNet Luna HSM

Once you have installed IBM WebSphere Application Server, you must complete the following POST Installation instructions

1. Modify the java.security file located in directory.
   C:\ProgramFiles(x86)\IBMWebSphere\AppServer\java\relib\security\ to include the following:

   ```
   # list of providers and their preference orders (see above):
   security.provider.1=com.ibm.crypto.provider.IBMJCE
   security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.4=com.ibm.security.cert.IBMCertPath
   ```
security.provider.5=com.ibm.security.cmskeystore.CMSProvider
security.provider.6=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl c:\luna.cfg
security.provider.7=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.8=com.ibm.security.sasl.IBMSASL
security.provider.9=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.10=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.11=org.apache.harmony.security.provider.PolicyProvider# Default keystore type.
keystore.type=jks

NOTE: The above step is required to initialize IBMPKCS11 provider.

Details of the the `luna.cfg` file are given in the configuring a hardware cryptographic keystore section.

2. Restart the IBM WebSphere Application Server.

**Configuring a hardware cryptographic keystore**

Complete the following steps in the administrative console:

1. Click **Security > SSL certificate and Key management > Key stores and certificates.**
2. Click **New.** Type a name to identify the keystore. This name is used to enable hardware cryptography in the Web services security configuration.
3. Type the path for the hardware device-specific configuration file (`luna.cfg`). The configuration file is a text file that contains entries in the following format: `attribute = value.C:\luna.cfg`
4. The configuration file should also include device-specific configuration data. Navigate to the `PKCS11ImplConfigSamples.jar` file, which contains sample configuration files, under the heading "PKCS 11 Implementation Provider" on the Java technology site. [http://www.ibm.com/developerworks/java/jdk/security/50/](http://www.ibm.com/developerworks/java/jdk/security/50/). The required entries in `luna.cfg` are:

   ```
   name = LUNA
   library = C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll
   description = Luna config
   tokenLabel = part1
   attributes (*., CKO_PRIVATE_KEY, *) = {
      CKA_SENSITIVE = true
   }
   attributes (*.,CKO_PUBLIC_KEY, *) = {
      CKA_VERIFY = true
      CKA_ENCRYPT = true
   }
   ```
5. Type a password if the token login is required. Select the type as **Cryptographic Token Device (PKCS11).**
6. Select the Read only check box. Click OK and Save.


8. Default server certificate alias and Default client certificate alias drop down box will list all the certificates present on hardware. 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**. Certificate alias in keystore drop-down box will list all the certificates present on the hardware. Select a certificate. Click **OK** and **Save**.

10. Use **Retreivesigners Utility** to add server certificate to the **ClientDefaulttrust store** from **CellDefaulttruststore**. The utility is located under **C:\Program Files (x86)\IBM\WebSphere\AppServer\bin\retrieveSigners.bat**
11. Logout and restart the server. Before Logging page following page should be displayed:

12. View Certificate and check. It should be same as that selected in previous steps. If yes, click Yes to continue.
IBM WebSphere & HTTP Server V7.0 with SafeNet Luna HSM

Solaris 10 SPARC (64-bit)

Integrating IBM HTTP Server V7.0 with SafeNet Luna HSM

To configure the IBM Key Management Utility to recognize the SafeNet Luna HSM cryptographic device:

1. Ensure that the file libCryptoki2.so is in the <Path to LunaClient installation>/lib.
2. Traverse to the directory /opt/IBM/HTTPServer/gsk7/classes.
3. Rename ikmuser.sample to ikmuser.properties.
4. Uncomment and edit the following setting to use the cryptographic lib
   DEFAULT_CRYPTOGRAPHIC_MODULE=<Path to LunaClient installation>/lib.
5. Verify the following in the Chrystoki.conf under /etc.

   Cryptoki with Logging
   
   Chrystoki2 = {
   LibUNIX=/usr/lunasa/lib/libcklog2.so;
   }  
   Cklog2 = {
   LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
   NewFormat=1;
   Enabled=1;
   Error=/tmp/ErrorLunaSA2.txt;
   File=/tmp/LogLunaSA2.txt;
   }

   Cryptoki without Logging
   
   Chrystoki2 = {
   LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
   }

6. Set the JAVA_HOME environment variable /opt/IBM/HTTPServer/java.
7. Stop and start the HTTP Server.
   /opt/IBM/HTTPServer/bin/apachectl stop
   /opt/IBM/HTTPServer/bin/apachectl start
8. Modify the java.security file located in directory /opt/IBM/HTTPServer/java/jre/lib/security to include the following:
security.provider.1=com.ibm.security.jgss.IBMJGSSProvider
security.provider.2=sun.security.provider.Sun
#security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
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 /usr/lunasa/luna.cfg
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
#security.provider.10=com.ibm.crypto.pkcs11.provider.IBMPKCS11

Create configuration file luna.cfg. The required entries in luna.cfg are as follows:

```java
name = LUNA
library = <Path to Luna crypto lib>/libcryptoki2.so
description = Luna config
tokenLabel = <partition name>
attributes (*, CKO_PRIVATE_KEY, *) = {
  CKA_SENSITIVE = true
}
attributes (*,CKO_PUBLIC_KEY, *) = {
  CKA_VERIFY = true
  CKA_ENCRYPT = true
}
```

9. Open **IBM Key Management Utility**. Traverse to the directory `/opt/IBM/HTTPServer/bin/`. Execute `/ikeyman`. 
10. Select **Key Database File** and **Open**. Specify **Key Database Type** as **PKCS11Config**. Click **OK**.
11. The **Open Cryptographic Token** window displays, where **Cryptographic Token Label** represents the Partition in which objects will be created. Specify the SafeNet Luna HSM partition password for **Cryptographic Token Password**. You should check on the PED device if the password/key is required to be entered.
12. Check the **Create new secondary key database file** to create the CMS Key Database key.kdb. You are prompted to create a password to access this file. In addition, check **Stash the password to a file**.

![Password Prompt]

- **File Name:** /usr/IBM/HTTPServer/bin/key1.kdb
- **Password:** ********
- **Confirm Password:** ********
- **Set expiration time?** 60 Days
- **Stash the password to a file?**

13. The IBM Key Management window displays. Select **Signer Certificates** from the drop down in **Key Database Content** block. Select one of the Signer certificates (except for the "... - Persona Not Validated" certificates) and click **Extract**…

14. When the Extract Certificate to a File dialog appears, make the filename unique such that you can later recall the name of the certificate, and select Binary DER data, and click **OK**. Repeat for each certificate in the list, (except for the "... - Persona Not Validated" certificates).

15. Next, import each .Der Certificate to the HSM, by selecting the certificate in the list, clicking **Add** and selecting **Binary DER Data**. Click **OK**, which opens a label dialog, and enter the label. Repeat for each certificate.
16. Signer Certificates appear as:
<token label>:<certificate label>

17. For example, if the token label is "HTTP Server" and the certificate label is "Verisign Class 3 Primary Certification Authority" then you will see the "Signer Certificate" as:
HTTP Server: Verisign Class 3 Primary Certification Authority. For example, it is also shown in the above figure (highlighted one).

18. Click Create -> New Self Signed Certificate.... Specify the mandatory settings for Key Label and Organization. Click OK. RSA public and private keys as well as self-signed certificate now exist on the SafeNet Luna HSM Partition. Self Signed Certificate will also appear in the form <token label>:<key label>.
19. Select **Personal Certificate Request** and click **New**....

20. Give the appropriate details as required (as shown above) and the name of the file (*.arm) in which the certificate request will be stored.

21. Generate the CA signed certificate from a CA with this request. (By visiting to CA website and pasting the request where required). Save the generated certificate also in .arm format.

22. Add the root certificate to the HSM.

23. Select Signer Certificates and click **Add**.

24. Select **Data Type** as **Binary DER data**.

25. Enter the certificate file name in the **Certificate file name** field. Click **OK**.
26. The root certificate now exists on SafeNet Luna HSM partition.

27. Select **Personal Certificates** and click **Receive**.

28. Select **Data type** as **Base64-encoded ASCII data**.
29. Enter the certificate file name in the **Certificate file name** field. Click **OK**.

RSA Public and Private Keys as well as Self Signed Certificate and CA certified certificate now exist on the SafeNet Luna HSM Partition.

**To enable SSL Security**

To enable SSL security, perform the following steps:

1. Open the shell and change to directory `/usr/IBM/HTTPServer/bin`.
2. To Save the SafeNet Luna HSM partition password using the SSLStash Utility, type the following at shell:
   ```bash
   ./sslstash -c /opt/IBM/HTTPServer/conf/ssl.passwd crypto "partition password"
   ```
3. To enable SSL Security, you must modify and add settings to the file located at:
   ```bash
   /opt/IBM/HTTPServer/conf/httpd.conf
   ```
4. Add or uncomment the appropriate lines throughout the file, as explained below. In the VIRTUAL HOST section, add or uncomment the line as shown in the given example:
   ```bash
   LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
   Listen localhost:443
   <VirtualHost localhost:443>
      SSLEnable
      KeyFile  /opt/IBM/HTTPServer/bin/key.kdb
      SSLServerCert  <partition name>:<key label >
      SSLClientAuth None
      SSLPKCSDriver  <Path to Luna crypto lib>
   </VirtualHost>
   ```
SSLStashfile /opt/IBM/HTTPServer/conf/ssl.passwd
</VirtualHost>

5. Stop and start the HTTP Server.

Open the browser and type the following web address: https://<machinename>. You should receive a message similar to the following:

![Security Alert]

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

- The security certificate date is valid.

- The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

[Yes] [No] [View Certificate]

6. Click Yes. The Welcome to the HTTP Server web page displays.

Integrating IBM WebSphere Application Server V7.0 with SafeNet Luna HSM

Once you have installed IBM WebSphere Application Server, you must complete the following POST Installation instructions:

1. Modify the java.security file located in directory /opt/IBM/Websphere/AppServer/java/jre/lib/security to include the following:

   ```
   security.provider.1=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.2=sun.security.provider.Sun
   #security.provider.3=com.ibm.crypto.flips.provider.IBMJCEFIPS
   security.provider.3=com.ibm.crypto.provider.IBMJCE
   security.provider.4=com.ibm.jsse.IMBJ SSEProvider
   security.provider.5=com.ibm.jsse2.IBMJ SSEProvider2
   security.provider.6=com.ibm.cert.IBMCertPath
   security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
   security.provider.8=com.ibm.security.cmskeystore.CMSProvider
   security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
   #security.provider.10=com.ibm.crypto.pkcs11.provider.IBMPKCS11
   ```
Create configuration file luna.cfg. The required entries in luna.cfg are:

```
name = LUNA
library = /usr/lunasa/lib/ libCryptoki2.so
description = Luna config
tokenLabel = <partition name>
attributes (*, CKO_PRIVATE_KEY, *) = {
    CKA_SENSITIVE = true
}
attributes (*, CKO_PUBLIC_KEY, *) = {
    CKA_VERIFY = true
    CKA_ENCRYPT = true
}
```

2. Restart IBM WebSphere Application Server.

**Configuring a hardware cryptographic keystore**

Perform the following steps in the administrative console:

1. Click **Security > SSL certificate and Key management > Key stores and certificates**.
2. Click **New**. Type a name to identify the keystore. This name is used to enable hardware cryptography in the Web services security configuration.
3. Type the path for the hardware device-specific configuration file, `<Path to luna.cfg file>/luna.cfg`.
4. Type a password if the token login is required. Select the type as Cryptographic Token Device (PKCS11).
5. Select the Read only check box. Click OK and Save.


7. Default server certificate alias and Default client certificate alias drop down box will list all the certificates present on hardware. Select any one certificate. Click OK and Save.
8. 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. Certificate alias in keystore drop-down box will list all the certificates present on the hardware. Select a certificate. Click OK and Save.

9. Use **Retrievesigners Utility** to add server certificate to the ClientDefaulttrust store from CellDefaulttruststore. The utility is located under

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/retrieveSigners.sh
```
10. Logout and restart the server. The following page is displayed before the Logging page:

![Image of Security Alert dialog box]

11. View certificate and check. It should be same as that selected in step 7 and 8. If yes, click Yes to continue.
IBM WebSphere & HTTP Server V6.1 with SafeNet Luna HSM

4

Installation Overview

IBM HTTP Server and IBM WebSphere Application Server must be installed on the target machine to carry on with the integration process. For a detailed installation procedure, refer to the HTTP Server and WebSphere documentation.

This Chapter includes the steps for IBM WebSphere and HTTP Server V6.1 with SafeNet Luna HSM

AIX

Below is the list of supported platforms tested with IBM WebSphere and HTTP Server V6.1:

- AIX 5.3 (64-bit)
- AIX 6.1 (64-bit)
- AIX 7.1 (64-bit)

Integrating IBM HTTP Server V6.1 with SafeNet Luna HSM

To configure the IBM Key Management Utility to recognize the SafeNet Luna HSM cryptographic device:

1. Ensure that the file \texttt{libshim.so} is in the directory \texttt{/usr/lunasa/lib}. For Luna SA v5.2.1/5.3 and later versions ensure that library files are in \texttt{/usr/safenet/lunaclient/lib}.

2. For IBM HTTP Server Modify the java.security file located in directory:\texttt{/usr/IBM/HTTPServer/java/jre/lib/security} to include the following entry:

\begin{verbatim}
security.provider.x=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
\end{verbatim}

The required entries in luna.cfg are

\begin{verbatim}
name = LUNA
library = /usr/lunasa/lib/libCryptoki2.so
description = Luna config
tokenLabel = <partition name>
attributes (*, CKO_PRIVATE_KEY, *) = {
  CKA_SENSITIVE = true
}
attributes (*,CKO_PUBLIC_KEY, *) = {
  CKA_VERIFY = true
  CKA_ENCRYPT = true
\end{verbatim}
Please ensure entry in java. Security file should point to the correct location of luna.cfg file.

3. Traverse to the following directory:
   `<Path to IBM Installation Directory/gskta/classes>` For Ex:/usr/opt/ibm/gskta/classes/
   For IBM HTTP Server 7.0, traverse to the following directory:
   /export/home/IBM/HTTPServer/gsk7/classes
4. Rename ikmuser.sample to ikmuser.properties.
5. Uncomment and edit the following setting to use the cryptographic lib
   ```
   DEFAULT_CRYPTOGRAPHIC_MODULE=<Path to SafeNet Luna HSM client library>
   ```
6. Add the following to the SafeNet Luna HSM configuration (/etc/Chrystoki.conf) file for HTTP Server Shim Support
   ```
   Misc = {
   ApplicationInstance=HTTP_SERVER;
   AppIdMajor=1;
   AppIdMinor=1;
   }
   ```
7. Verify the following in the Chrystoki.conf under /etc.
   ```
   Cryptoki with Logging
   Chrystoki2 = {
   LibUNIX=/usr/lunasa/lib/libcklog2.so;
   }
   Cklog2 = {
   LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
   NewFormat=1;
   Enabled=1;
   Error=/tmp/ErrorLunaSA2.txt;
   File=/tmp/LogLunaSA2.txt;
   }
   Cryptoki without Logging
   Chrystoki2 = {
   LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
   }
   ```
   LibUNIX should be path to your SafeNet Luna HSM client library/ log library, path may differ from shown in above example
8. Set the JAVA_HOME environment variable.
   ```
   /usr/IBM/ HTTPServer/AppServer/java
   ```
9. Stop and start the HTTP Server.
   ```
   /usr/IBM/HTTPServer/bin/apachectl stop
   /usr/IBM/HTTPServer/bin/apachectl start
10. Open IBM Key Management Utility.

   Traverse to the directory: /usr/IBM/HTTPServer/bin/

   Execute ./ikeyman.

   The Cryptographic Token menu option displays.

11. Select **Key Database File** and **Open**. Specify **Key Database Type** as CMS Cryptographic Token, **File Name** as libshim.so and **Location** as /usr/lunasa/lib. Click **OK**.

   For IBM HTTP Server 8.5.5 select **PKCS11config** as **Key database type** and it will read file name and location automatically from config file.
12. The **Open Cryptographic Token** window displays, where **Cryptographic Token Label** represents the Partition in which objects will be created. Specify the SafeNet Luna HSM partition password for the **Cryptographic Token Password** field. You should check on the PED device if the password/key is required to be entered.
13. Check the Create new secondary key database file to create the CMS Key Database key.kdb. You are prompted to create a password to access this file. In addition, check Stash the password to a file.

![Password Prompt](image)

14. The IBM Key Management window displays. Select Signer Certificates from the drop-down in Key Database Content block. Select one of the Signer certificates (except for the "... - Persona Not Validated" certificates) and click Extract…

15. When the Extract Certificate to a File window displays, it is advised to make the filename unique such that you can later recall the name of the certificate. Select Binary DER data, and click OK. Repeat for each certificate in the list, (except for the "... - Persona Not Validated" certificates).

16. Next, import each .Der Certificate to the HSM, by selecting the certificate in the list, clicking Add and selecting Binary DER Data. Click OK, which opens a label dialog, and enter the label. Repeat for each certificate.
17. Signer Certificates appear as:
<token label>:<certificate label>

For example, if the token label is "WebSphere" and the certificate label is "Verisign Class 3 Primary Certification Authority" then you will see the "Signer Certificate" as:
WebSphere: Verisign Class 3 Primary Certification Authority. As an example, it is also shown in the above figure (highlighted one).

18. Click Create -> New Self Signed Certificate.... Specify the mandatory settings for Key Label and Organization. Click OK. RSA public and private keys as well as self-signed certificate now exist on the SafeNet Luna HSM Partition. Self Signed Certificate will also appear in the form <token label>:<key label>
19. Select **Personal Certificate Request** and click **New**

![Create New Key and Certificate Request](image)

Give the appropriate details as required (as shown above) and the name of the file (*.arm) in which the certificate request will be stored.

Generate the CA signed certificate from a CA with this request. (By visiting to CA website and pasting the request where required). Save the generated certificate also in .arm format.

20. Add the root certificate to the HSM.

21. Select Signer Certificates and click **Add**.

22. Select **Data Type** as **Binary DER data**.
23. Enter the certificate file name in the **Certificate file name** field. Click **OK**.
   The root certificate now exists on SafeNet Luna HSM partition.

24. Select **Personal Certificates** and click **Receive**.

25. Select **Data type** as **Base64-encoded ASCII data**.
26. Enter the certificate file name in the **Certificate file name** field. Click **OK**.

![Certificate Management](image)

RSA public and private keys as well as self-signed certificate and CA certified certificate now exist on the SafeNet Luna HSM Partition.

27. Install the patch 2.0.47.1-PK29827 for IBM HTTP Server V6.1.

**NOTE:** Download 2.0.47.1-PK29827.aix.tar patch from the IBM website (tar file) and untar it into the `/usr/IBM/HTTPServer`.

**To enable SSL Security:**

To enable SSL security, perform the following steps:

1. Open the shell and change to directory `/usr/IBM/HTTPServer/bin`.

2. To Save the SafeNet Luna HSM partition password using the SSLStash Utility, type the following command at shell:

   ```
   ./sslstash -c /usr/IBM/HTTPServer/conf/ssl.passwd crypto "partition password"
   ```

3. To enable SSL security, you must modify and add settings to the file located at:

   ```
   /usr/IBM/HTTPServer/conf/httpd.conf
   ```

   Add or uncomment the appropriate lines throughout the file, as explained below. In the VIRTUAL HOST section, add or uncomment the line as shown in the given example.
4. Stop and start the HTTP Server.
5. Open the browser and type the following web address: https://<machinename>. You should receive a message similar to the following:

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠️ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✔️ The security certificate date is valid.

⚠️ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Yes  No  View Certificate

6. Click Yes. The Welcome to the HTTP Server web page displays.

Integrating IBM WebSphere Application Server V6.1 with SafeNet Luna HSM

Once you have installed IBM WebSphere Application Server, you must complete the following POST Installation instructions:

1. Modify the java.security file located in directory /usr/IBM/WebSphere/AppServer/java/jre/lib/security to include the following:

   security.provider.6=com.ibm.crypto.pkcs11impl.provider.IBMFKCS11Impl /usr/lunasa/luna.cfg

For Example:

   # List of providers and their preference orders (see above):
   #security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.1=com.ibm.crypto.provider.IBMJCE
   security.provider.2=com.ibm.jsse.IBMJSSEProvider
   security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
security.provider.7=com.ibm.security.cmskeystore.CMSProvider
security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO

# Default keystore type.
keystore.type=jks

NOTE: The above step is required to initialize IBMPKCS11 provider.

Details of luna.cfg are given in section, configuring a hardware cryptographic keystore.

2. Restart IBM Websphere Application Server.

Configuring a hardware cryptographic keystore

Complete the following steps in the administrative console

1. Click **Security > SSL certificate and Key management > Key stores and certificates.**
2. Click **New.** Type a name to identify the keystore. This name is used to enable hardware cryptography in the Web services security configuration.
3. Type the path for the hardware device-specific configuration file (luna.cfg). The configuration file is a text file that contains entries in the following format: attribute = value./usr/lunasa/
4. The configuration file should also include device-specific configuration data. Navigate to the PKCS11implConfigSamples.jar file, which contains sample configuration files, under the heading "PKCS 11 Implementation Provider" on the Java technology site. http://www.ibm.com/developerworks/java/jdk/security/50/. The required entries in luna.cfg are:

```java
name = LUNA
library = /usr/lunasa/lib/libCryptoki2.so
description = Luna config
tokenLabel = <partition name>
attributes (*, CKO_PRIVATE_KEY, *) = {
    CKA_SENSITIVE = true
}
attributes (*,CKO_PUBLIC_KEY, *) = {
    CKA_VERIFY = true
    CKA_ENCRYPT = true
}
```
5. Type a password if the token login is required. Select the **Type** as **Cryptographic Token Device (PKCS11).**
6. Select the Read only check box. Click OK and Save.

![Image showing Integrated Solutions Console with SSL certificate and key management configuration]

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

**NOTE:** You can utilize the same certificate used for IBM HTTP Server integration.
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**. Certificate alias in keystore drop-down box will list all the certificates present on the hardware. Select a certificate. Click **OK** and **Save**.

**NOTE:** This Certificate should be same as that selected in step 8.

10. Use **RetrieveSigners Utility** to add server certificate to the ClientDefaulttrust store from CellDefaulttruststore. The utility is located under: `/usr/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/retrieveSigners.sh`
11. Logout and restart the server. The following page is displayed before the Logging page:

12. View certificate and check. It should be same as that selected in step 8 and 9. If yes, click Yes to continue.
Windows XP SP2 (32-bit)

Integrating IBM HTTP Server V6.1 with SafeNet Luna HSM

To configure the IBM Key Management Utility to recognize the SafeNet Luna HSM cryptographic device:

1. Ensure that the file shim.dll is in the directory C:\Program Files\LunaSA
2. Traverse to the directory C:\Program Files\IBM\gsk7\classes.
3. Rename ikmuser.sample to ikmuser.properties.
4. Uncomment and edit the following settings to use the cryptographic shim (libshim):
   
   ```
   DEFAULT_CRYPTOGRAPHIC_MODULE= C:\\Program Files\\LunaSA\\shim.dll
   ```
   
   Add the following to the SafeNet Luna HSM configuration (C:\Program Files\LunaSA\crystoki.ini) file for HTTP Server Shim Support
   
   ```
   [Misc]
   ApplicationInstance=HTTP_SERVER
   AppIdMajor=1
   AppIdMinor=1
   ```
5. Verify the following in the crystoki.ini under C:\Program Files\LunaSA.

   **Cryptoki with Logging**
   
   ```
   [Chrystoki2]
   LibNT=C:\Program Files\LunaSA\cklog201.dll
   ```

   ```
   [CkLog2]
   LibNT=C:\Program Files\LunaSA\cryptoki.dll
   Enabled=1
   NewFormat=1
   File=C:\Program Files\LunaSA\Log.txt
   Error=C:\Program Files\LunaSA\Err.txt
   ```

   **Cryptoki without Logging**
   
   ```
   [Chrystoki2]
   LibNT=C:\Program Files\LunaSA\cryptoki.dll
   ```
6. Set the JAVA_HOME environment variable C:\Program Files\IBM\WebSphere\AppServer\java.
7. Stop and start the HTTP Server. Go to Control Panel -> Services.
9. Select **Key Database File** and **Open**. Specify **Key database type** as **CMS Cryptographic Token**, **File Name** as **shim.dll**, and **Location** as **C:\Program Files\LunaSA**. Click **OK**.
10. The **Open Cryptographic Token** window displays, where **Cryptographic Token Label** represents the Partition in which objects will be created. Specify the SafeNet Luna HSM partition password for the **Cryptographic Token Password** field. You should check on the PED device if the password/key is required to be entered.
11. Check the **Create new secondary key database file** to create the CMS Key Database key.kdb. You are prompted to create a password to access this file. In addition, click **Stash the password to a file**.

![Password Prompt](image)

12. The **IBM Key Management** window displays. Select the Signer Certificates from the drop-down in **Key Database Content** block. Select one of the Signer certificates (except for the "... - Persona Not Validated" certificates) and click **Extract**.

13. The **Extract Certificate to a File** window displays. Make the filename unique such that you can later recall the name of the certificate, and select **Binary DER data**, and click **OK**. Repeat for each certificate in the list, (except for the "... - Persona Not Validated" certificates).

14. Next, import each .Der Certificate to the HSM, by selecting the certificate in the list, clicking **Add** and selecting **Binary DER Data**. Click **OK**, which opens a label dialog, and enter the label. Repeat for each certificate.
15. Signer Certificates appear as: 
<token label>:<certificate label>

For example, if the token label is "Web sphere" and the certificate label is "Verisign Class 3 Primary Certification Authority" then you will see the "Signer Certificate" as: Websphere:Verisign Class 3 Primary Certification Authority. As an example, it is also shown in the above figure (highlighted one).

16. Click Create -> New Self Signed Certificate.... Specify the mandatory settings for Key Label and Organization. Click OK. RSA public and private keys as well as self-signed certificate now exist on the SafeNet Luna HSM Partition. Self-signed certificate will also appear in the form <token label>:<key label>. 

17. Select **Personal Certificate Request** and click **New**.

![Create New Key and Certificate Request](image)

Give the appropriate details as required (as shown above) and the name of the file (*.arm) in which the certificate request will be stored.

Generate the CA signed certificate from a CA with this request. (By visiting to CA website and pasting the request where required). Save the generated certificate also in .arm format.

18. Add the root certificate to the HSM.

19. Select **Signer Certificates** and click **Add**.

20. Select **Data Type** as **Binary DER data**.
21. Enter the certificate file name in the **Certificate file name** field. Click **OK**. The root certificate now exists on SafeNet Luna HSM partition.

22. Select **Personal Certificates** and click **Receive**.

23. Select **Data type** as **Base64-encoded ASCII data**.
24. Enter the Certificate file name and click OK.

![Image of Key Management with Certificate Import](image.png)

RSA public and private keys as well as self-signed certificate and CA certified certificate now exist on the SafeNet Luna HSM Partition.

25. Install the patch 2.0.47.1-PK29827 for IBM HTTP Server V6.1

**NOTE:** Download 2.0.47.1-PK29827.nt patch from the IBM website (tar file) and untar it into the C:\Program Files\IBM\HTTPServer.

---

**To enable SSL Security**

To enable SSL security, perform the following steps:

1. Open the shell and change to directory C:\Program Files\IBM\HTTPServer\bin.

2. To save the SafeNet Luna HSM Partition Password using the SSLStash Utility, type the following at shell:

   ```
   Sslstash -c "C:\Program Files\IBM\HTTPServer\conf\ssl.passwd" crypto "partition password"
   ```

3. To enable SSL Security, you must modify and add settings to the file located at:

   ```
   C:\ProgramFiles\IBM\HTTPServer\conf\httpd.conf
   ```
Add or uncomment the appropriate lines throughout the file, as explained below. In the VIRTUAL HOST section, add or uncomment the line as shown in the given example:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen localhost:443
<VirtualHost localhost:443>
SSLEnable
KeyFile "C:\Program Files\IBM\HTTPServer\key.kdb"
SSLServerCert <partition name>:<key label >
SSLClientAuth None
SSLPKCSDriver "C:\Program Files\LunaSA\shim.dll"
SSLStashfile "C:\Program Files\IBM\HTTPServer\conf\ssl.passwd"
</VirtualHost>
```

4. Stop and start the HTTP Server.

5. Open the Browser and type the following web address: `https://<machinename>`. You should receive a message similar to the following:

![Security Alert Dialog](image)

```
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠️ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✅ The security certificate date is valid.

⚠️ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?
```

6. Click **Yes**. The **Welcome to the HTTP Server** web page displays.
Integrating IBM WebSphere Application Server V6.1 with SafeNet Luna HSM

Once you have installed IBM WebSphere Application Server, you must complete the following POST Installation instructions:

1. Modify the `java.security` file located in directory `C:\ProgramFiles\IBM\Websphere\AppServer\java\jre\lib\security\` to include the following:

   ```
   # List of providers and their preference orders (see above):
   security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.2=com.ibm.crypto.provider.IBMJCE
   security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.5=com.ibm.security.cert.IBMCertPath
   security.provider.6=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
   security.provider.7=com.ibm.security.cmskeystore.CMSProvider
   security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
   # Default keystore type.
   keystore.type=jks
   ```

   **NOTE:** The above step is required to initialize IBMPKCS11 provider.

   Details of the `luna.cfg` file are given in the configuring a hardware cryptographic keystore section.

2. Restart IBM WebSphere Application Server.

Configuring a hardware cryptographic keystore

Complete the following steps in the administrative console

1. Click **Security > SSL certificate and Key management > Key stores and certificates.**
2. Click **New.** Type a name to identify the keystore. This name is used to enable hardware cryptography in the Web services security configuration.
3. Type the path for the hardware device-specific configuration file (`luna.cfg`). The configuration file is a text file that contains entries in the following format: attribute = value. `C:\Program Files\LunaSA\`
4. The configuration file should also include device-specific configuration data. Navigate to the `PKCS11ImplConfigSamples.jar` file, which contains sample configuration files, under the heading “PKCS 11 Implementation Provider” on the Java technology site. `http://www.ibm.com/developerworks/java/jdk/security/50/`. The required entries in `luna.cfg` are mentioned below.

   ```
   name = LUNA
   library = C:\Program Files\LunaSA\cryptoki.dll
   description = Luna config
   tokenLabel = <partition name>
   ```

5. Type a password if the token login is required. Select the type as Cryptographic Token Device (PKCS11).
6. Select the **Read only** check box. Click **OK** and **Save**.

7. Click **Security > SSL Certificate and Key Management > SSL Configurations > Node Default SSLSettings**. Select Keystore as new created keystore and click **Get Certificate Aliases**.
8. Default server certificate alias and Default client certificate alias drop-down box will list all the certificates present on hardware. Select any one certificate. Click OK and Save.

NOTE: You can utilize the same certificate used for IBM HTTP Server integration.
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**. Certificate alias in keystore drop-down box will list all the certificates present on the hardware. Select a certificate. Click **OK** and **Save**.

**NOTE:** This Certificate should be same as that selected in step 8.

10. Use **Retrievesigners Utility** to add server certificate to the ClientDefaulttrust store from CellDefaulttruststore. The utility is located under

    C:\ProgramFiles\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\retrieveSigners.bat
11. Logout and restart the server. The following page is displayed before the logging page:

![Security Alert](image)

12. View certificate and check. It should be same as that selected in step 8 and 9. If yes, click Yes to continue.
RHEL 5 (32-bit)

Integrating IBM HTTP Server V6.1 with SafeNet Luna HSM

To configure the IBM Key Management Utility to recognize the Luna SA 4.2 cryptographic device

1. Ensure that the file libshim.so is in the directory /usr/lunasa/lib
2. Traverse to the directory /usr/local/ibm/gsk7/classes/
3. Rename ikmuser.sample to ikmuser.properties.
4. Uncomment and edit the following setting to use the cryptographic shim (libshim)
   DEFAULT_CRYPTOGRAPHIC_MODULE=/usr/lunasa/lib/libshim.so
   Add the following to the SafeNet Luna HSM configuration (/etc/Chrystoki.conf) file for HTTP Server Shim Support
   Misc = {
     ApplicationInstance=HTTP_SERVER;
     AppIdMajor=1;
     AppIdMinor=1;
   }
5. Verify the following in the Chrystoki.conf under /etc.

Cryptoki with Logging

Chrystoki2 = {
  LibUNIX=/usr/lunasa/lib/libcklog2.so;
}

Cklog2 = {
  LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
  NewFormat=1;
  Enabled=1;
  Error=/tmp/ErrorLunaSA2.txt;
  File=/tmp/LogLunaSA2.txt;
}

Cryptoki without Logging

Chrystoki2 = {
  LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
}

6. Set the JAVA_HOME environment variable /opt/IBM/WebSphere/AppServer/java
7. Stop and start the HTTP Server.
   /opt/IBM/HTTPServer/bin/apachectl stop
   /opt/IBM/HTTPServer/bin/apachectl start
9. Select **Key Database File** and **Open**. Specify **Key database type** as **CMS Cryptographic Token**, **File Name** as **libshim.so**, **Location** as **/usr/lunasa/lib**. Click **OK**.
10. The **Open Cryptographic Token** window displays, where **Cryptographic Token Label** represents the Partition in which objects will be created. Specify the SafeNet Luna HSM partition password for the **Cryptographic Token Password** field. You should check on the PED device if the password/key is required to be entered.

![Open Cryptographic Token Window]

Some cryptographic tokens have limited capacity, and are unable to hold the signer certificates required to receive or import a personal certificate. If the selected cryptographic token has such a restriction, you may choose to open a secondary key database file to provide the extra capacity to hold signer certificates.

- **Open existing secondary key database file**
- **Create new secondary key database file**

**Key database type**: CMS

**File Name**: `key.kdb`

**Location**: `/opt/IBM/HTTPServer/bin/`

![Password Prompt Window]

11. Check the **Create new secondary key database file** to create the CMS Key Database `key.kdb`. You are prompted to create a password to access this file. In addition, click **Stash the password to a file**.
12. The **IBM Key Management** window displays. Select the Signer Certificates from the drop-down menu in the **Key Database Content** block. Select one of the Signer certificates (except for the "... - Persona Not Validated" certificates) and click **Extract**.

13. The **Extract Certificate to a File** window displays. Make the filename unique such that you can later recall the name of the certificate. Select **Binary DER data** and click **OK**. Repeat for each certificate in the list, (except for the "... - Persona Not Validated" certificates).

14. Next, import each .Der Certificate to the HSM, by selecting the certificate in the list, clicking **Add** and selecting **Binary DER Data**. Click **OK**, which opens a label dialog, and enter the label. Repeat for each certificate.

15. Signer Certificates appear as:

\(<\text{token label}>:<\text{certificate label}>\)

For example, if the token label is "Web sphere" and the certificate label is "Verisign Class 3 Primary Certification Authority" then you will see the "Signer Certificate" as:

Websphere: Verisign Class 3 Primary Certification Authority. As an example, it is also shown in the above figure (highlighted one).

16. Click **Create -> New Self Signed Certificate**.... Specify the mandatory settings for **Key Label** and **Organization**. Click **OK**. RSA public and private keys as well as self-signed certificate now exist on the SafeNet Luna HSM partition. Self-signed Certificate will also appear in the form \(<\text{token label}>:<\text{key label}>\).
17. Select **Personal Certificate Request** and click **New**.

![Image of Key Management interface]

Give the appropriate details as required (as shown above) and the name of the file (*.arm) in which the certificate request will be stored.

Generate the CA signed certificate from a CA with this request. (By visiting to CA website and pasting the request where required). Save the generated certificate also in .arm format.

18. Add the root certificate to the HSM.
19. Select **Signer Certificates** and click **Add**.
20. Select **Data Type** as **Binary DER data**.
21. Enter the certificate file name in the **Certificate file name** field. Click **OK**.

The root certificate now exists on SafeNet Luna HSM partition.

22. Select **Personal Certificates** and click **Receive**.

23. Select **Data type** as **Base64-encoded ASCII data**.
24. Enter the certificate file name in the **Certificate file name** field. Click **OK**.

RSA Public and Private Keys as well as Self Signed Certificate and CA certified certificate now exist on the SafeNet Luna HSM Partition.

25. Install the patch 2.0.47.1-PK29827 for IBM HTTP Server V6.1.

**NOTE:** Download 2.0.47.1-PK29827.linux.tar patch from the IBM website (tar file) and untar it into the /opt/IBM/HTTPServer

---

**To enable SSL Security**

To enable SSL security, perform the following steps:

1. Open the shell and change to directory `/opt/IBM/HTTPServer/bin`.

2. To save the SafeNet Luna HSM Partition Password using the SSLStash Utility, type the following command at shell:
   
   ```
   ./sslstash -c /opt/IBM/HTTPServer/conf/ssl.passwd crypto "partition password"
   ```

3. To enable SSL Security, you must modify and add settings to the file located at:
   
   `/opt/IBM/HTTPServer/conf/httpd.conf`
   
   Add or uncomment the appropriate lines throughout the file, as explained below. In the **VIRTUAL HOST** section, add or uncomment the line as shown in the given example:
   
   ```
   LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
   Listen localhost:443
   ```
<VirtualHost localhost:443>
  SSLEnable
  KeyFile /opt/IBM/HTTPServer/bin/key.kdb
  SSLServerCert <partition name>:<key label>
  SSLClientAuth None
  SSLPKCSDriver /usr/lunasa/lib/libshim.so
  SSLStashfile /opt/IBM/HTTPServer/conf/ssl.passwd
</VirtualHost>

4. Stop and start the HTTP Server.
5. Open the browser and type the following web address: https://<machinename>. You should receive a message similar to the following:

![Security Alert]

- Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
- The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- The security certificate date is valid.
- The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

- Yes
- No
- View Certificate

6. Click Yes. The Welcome to the HTTP Server web page displays.
Integrating IBM WebSphere Application Server V6.1 with SafeNet Luna HSM

Once you have installed IBM WebSphere Application Server, you must complete the following POST Installation instructions:

1. Modify the java.security file located in directory /opt/IBM/Websphere/AppServer/java/jre/lib/security to include the following:

   ```
   # List of providers and their preference orders (see above):
   #security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.1=com.ibm.crypto.provider.IBMJCE
   security.provider.2=com.ibm.jsse.IBMJSSEProvider
   security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.5=com.ibm.security.cert.IBMCertPath
   security.provider.6=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
   security.provider.7=com.ibm.security.cmskeystore.CMSProvider
   security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
   # Default keystore type.
   keystore.type=jks
   ```

   **NOTE:** The above step is required to initialize IBMPKCS11 provider.

   Details of the luna.cfg file are given in the configuring a hardware cryptographic keystore section.

2. Restart IBM WebSphere Application Server.

Configuring a hardware cryptographic keystore

Complete the following steps in the administrative console

1. Click **Security > SSL certificate and Key management > Key stores and certificates**.

2. Click **New**. Type a name to identify the keystore. This name is used to enable hardware cryptography in the Web services security configuration.

3. Type the path for the hardware device-specific configuration file (luna.cfg). The configuration file is a text file that contains entries in the following format: attribute = value./usr/lunasa/.

4. The configuration file should also include device-specific configuration data. Navigate to the PKCS11ImplConfigSamples.jar file, which contains sample configuration files, under the heading "PKCS 11 Implementation Provider" on the Java technology site. [http://www.ibm.com/developerworks/java/jdk/security/50/](http://www.ibm.com/developerworks/java/jdk/security/50/). The required entries in luna.cfg are:

   ```
   name = LUNA
   library = /usr/lunasa/lib/libCryptoki2.so
   description = Luna config
   tokenLabel = <partition name>
   ```

5. Type a password if the token login is required. Select the **Type as Cryptographic Token Device (PKCS11)**.
6. Select the **Read only** check box. Click **OK** and **Save**.

7. Click **Security > SSL Certificate and Key Management > SSL Configurations > Node Default SSLSettings**. Select Keystore as new created keystore and click **Get Certificate Aliases**.
8. **Default server certificate alias** and **Default client certificate alias** drop-down box will list all the certificates present on hardware. Select any one certificate. Click **OK** and **Save**.

**NOTE:** You can utilize the same certificate used for IBM HTTP Server integration.
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. Certificate alias in keystore drop-down box will list all the certificates present on the hardware. Select a certificate. Click OK and Save.

NOTE: This Certificate should be same as that selected in step 8.

10. Use RetrieveSigners Utility to add server certificate to the ClientDefaulttrust store from CellDefaulttruststore. The utility is located under /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/retrieveSigners.sh
11. Logout and restart the server. The following page is displayed before the Logging page:

12. View certificate and check. It should be same as that selected in step 8 and 9. If yes, click Yes to continue.
Integration of WebSphere Network Deployment with SafeNet Luna HSM

Before integrating the WebSphere Network Deployment (WAS ND) with SafeNet Luna HSM Luna we need to install WebSphere Network Deployment software and setup cluster having at least two nodes. To install and configure nodes in WAS ND cluster refer the IBM WebSphere Network Deployment Installation guide.

It is assumed that you have successfully installed WebSphere Network Deployment and setup the cluster with two nodes.

You need to generate the keys and certificate on SafeNet Luna HSM using IBM Key Management Utility. Perform the following steps to configure the IBM Key Management utility to use with SafeNet Luna HSM:

1. For IBM WAS ND Server v8.5.5, Modify the java.security file located in directory
   /opt/IBM/WebSphere/AppServer/java/jre/lib/security/java.security to include the following entry

   security.provider.x=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /home/luna.cfg

   The java.security file looks like the following:

   security.provider.1=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
   security.provider.2=com.ibm.crypto.provider.IBMJCE
   security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.5=com.ibm.security.cert.IBMCertPath
   
   security.provider.6=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /home/luna.cfg
   security.provider.7=com.ibm.security.cmskeystore.CMSProvider
   security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
   security.provider.9=com.ibm.security.sasl.IBMSASL
   security.provider.10=com.ibm.xml.crypto.IBMXMLCryptoProvider
   security.provider.11=com.ibm.xml.enc.IBMXMLEncProvider
   security.provider.12=org.apache.harmony.security.provider.PolicyProvider

   The required entries in luna.cfg are:

   name = LUNA
   library = /usr/safenet/lunaclient/lib/libCryptoki2_64.so
   description = Luna config
   tokenLabel = <SafeNet Luna HSM partition name>
   attributes (*, CKO_PRIVATE_KEY, *) = {
     CKA_SENSITIVE = true
   }
   attributes (*,CKO_PUBLIC_KEY, *) = {
     CKA_VERIFY = true
     CKA_ENCRYPT = true
   }
2. Run the IBM Key Management Utility (ikeyman) from \<WAS ND installation directory\>/bin/ikeyman.sh, click **Key Database File -> Open** and select **PKCS11Config**.
3. 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 box.

Select CMS from the *key database type* drop-down menu. By default, the file name will be key.kdb. To create a file with a different name, enter a new name for the file, and click **OK**.
4. It will prompt for password for the key database file. Enter the password and confirm password. Select the **Stash password to a file** check box. Click **OK**.
5. Click **Create -> New Certificate Request**: enter the details to generate the certificate and certificate request name to save the certificate request. Click **OK**.

![Certificate Request Window](image)

6. Minimize the IBM Key Management console and open the certificate request file and copy the contents, send the certificate request to the CA and save the response received from certificate authority.
7. Open the **IBM Key Management** console and select **Personal Certificates**. Click **Receive**... A new window will pop up. Click **Browse** and select the signed certificate file received from the CA. Click **OK**.
8. Verify the certificate saved successfully stored on the partition with "Token Label: Certificate Name". Close the IBM Key Management Utility.

9. Open the browser and enter the URL http://localhost:9060/ibm/console into the address bar. Click Login.
10. Click on Security -> SSL certificate and key management -> Key stores and certificate. It will show you the Cell and Node default key store and trust store for cell and nodes respectively.
11. Click CellDefaultKeyStore and enter the location of the luna.cfg file in the Path field. Enter the partition password in the Password field and select Cryptographic Token Device (PKCS11) in the Type field. Click OK and Save.
12. Repeat the above steps for CellDefaultTrustStore, NodeDefaultKeyStore and NodeDefaultTrustStore. You need to select luna.cfg for all nodes and cell added into the WAS ND cluster. Enter partition password and select Cryptographic Token Device (PKCS11) in the Type field.
13. Click on Security -> SSL certificate and key management -> SSL Configurations. It will show you the list of Cell and Node default SSL settings.
14. Select **CellDefaultSSLSettings**, click the **Get certificate aliases** button and select the certificate stored on the Luna partition in Default server certificate alias and Default client certificate alias. Click **OK** and **Save**.

15. Repeat the above step for NodeDefaultSSLSettings for all nodes added in to the cell.

16. Click on **Security -> SSL certificate and key management -> Manage end point security configurations**.

17. Expand **Inbound** and click **cell01 (CellDefaultSSLSettings)**. Click **Update certificate alias list** and select the same certificate stored on the partition that you selected in the step 14. Click **OK** and **Save**.

18. Expand **Outbound** and click **cell01 (CellDefaultSSLSettings)**. Click **Update certificate alias list** and select the same certificate stored on the partition that you selected in the step 14. Click **OK** and **Save**.

19. Log out from IBM Management Console and restart the cluster (all nodes in the cluster).
20. Open the browser and enter URL: https://localhost:9043/ibm/console.

21. Add Exception and Confirm security exception and click Login. You will be logged in securely in the IBM Management console. Verify the certificate that you have generated on the Luna partition in step 5.

22. If you have selected the sample application during the installation of WAS ND then you can open the “snoop” application on both nodes using their respective ports. You can access the application with the following URLs:
Deploying an application to the cluster

In this section, we will deploy an application called the “Default application” which is located in the “<was_root>/installableapps” folder to verify the cluster. After deploying the application it must be accessible with all nodes of the cluster.

1. Within the Administration console navigate to Applications -> Application Types -> WebSphere enterprise applications.
2. Click Install to begin the application deployment.
3. Click the Remote file system option to install the DefaultApplication.EAR file from the server file-system.
4. Select the deployment manager node, and scroll down to the appropriate folder path.
5. Select DefaultApplication.ear file. Click OK and then Next.
6. In the next screen, which is the Preparing for the application installation screen, select the Fast Path option and click Next.
7. In Step 1: Select installation options, set the logical name of the application by typing “Default Application” into the Application name field. By default the Application name is set to the EAR file’s name.
8. Click Next to move to the Step 2: the Map modules to Servers screen. Here the wizard has detected that there is a Web module and EJB contained within the EAR file and so there need to be an explicit mapping of which JVM or cluster each component is to run on. If you want both to be run as a separate instances within each member of the cluster (this is the default setting set by the wizard).
9. Click Next to review the summary and then click Finish. Save to complete the deployment to the cluster.
10. Navigate to Applications -> Application Types -> WebSphere enterprise applications to view the newly installed (deployed) application.
11. Start the application by clicking the Start button. The console will report that the Default Application has been started successfully on both nodes.

For appsrv01- https://localhost:9443/snoop
For appsrv02- https://localhost:9444/snoop

If you have not installed the application, you need to follow the steps mentioned in the next section to deploy the application.
12. To test the application, you need to find out what port values the web container is running on for both servers in the cluster. Navigate to **Servers -> Server types -> WebSphere application servers** and you will see two servers. For example, click on server1 to enter the server’s properties screen. Locate the Communication section and expend the Ports section. Look for the port called WC_defaulthost_secure. This port is server1’s Web container port and in this example it is port 9443.

![WebSphere application servers](image)

13. Using the same process as above, locate the same port for server2. In this example it is port 9444.

14. Now you have two port numbers and you can access the snoop servlet via a browser to confirm that the application is running on the both nodes.

15. Navigate to **https://<host_name or IP>:9443/snoop**

You might get the following error:

SRVE0255E: A WebGroup/Virtual Host to handle /snoop has not been defined.

SRVE0255E: A WebGroup/Virtual Host to handle localhost:9443 has not been defined.

It means that the virtual host definition have not yet been set. When you deployed the application you mapped the Default Application’s web module to the default_host. Each web module within an application must be mapped to a virtual host.

16. To configure virtual hosts, navigate to **Environment -> Virtual hosts** and click **default_host**.

17. The next screen presented will allow you to locate the Host aliases assigned to the default host. Click **Host Aliases**.

18. There will now be a list of virtual hosts alias. Some are identified by “**”, other are identified by a host name. When a host alias is identified with a “**” it means any host can connect. If a named host is set as an alias, then only that host name can be used in the URL of a browser (i.e. the Browser will present that hostname in its host header) to connect to any resources in web apps bound to that virtual host.

19. Add a new host alias for both ports 9443 and 9444. These are the two ports of the Web containers in each server. Click the **New** button to enter the add alias screen.
20. Enter "*" in the **Host name** field and enter the value 9443 in the **Port** field. Click **OK**. Create a new alias for port 9444, and click **OK** and save both changes.

21. Ensure your cluster is restarted and retry the URLs above. You will be able to access the snoop servlet on the port 9443 and port 9444.

Below is an example of what the snoop servlet will produce for server1. Notice that the Server port is 9443 as expected.

Below is the snoop output for server2. Notice that the server port is 9444 as expected.
Troubleshooting

Problem

“CMS Cryptographic Token” is not available as Token Key Database Type option in IKEYMAN available with IBM HTTP Server version 7.0

Solution

In IBM HTTP Server 7.0, two different versions of IKEYMAN are provided. The native Tivoli Global Security Kit (GSKit) that is bundled with IBM HTTP Server 7.0 contains IKEYMAN Version 7, but the JVM that is bundled with IBM HTTP Server includes IKEYMAN Version 8. IKEYMAN Version 8 is enabled by default.

Users of operating systems other than Solaris and HP-UX who desire to use the traditional IKEYMAN Version 7 interface (for example to use older PKCS11 dialogues) can configure the system to use IKEYMAN Version 7.

To use IKEYMAN Version 7.0, move the `<ihsinst>/java/jre/lib/ext/gskikm.jar` file to a directory that is not in the JDK class path, extdirs path, or the bootclasspath environment variable.

For example, use the following command to move the file:

```
mv <his_install_path>/java/jre/lib/ext/gskikm.jar <his_Install_path>/libgskikm.jar
```

To use default version i.e. IKEYMAN 8 for Cryptographic Token,

Modify the java.security file located in directory `/opt/IBM/HTTPServer/java/jre/lib/security` to include the following entry:

```
security.provider.x=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
```

For example:

**On Solaris 10 SPARC x64**

```
security.provider.1=com.ibm.security.jgss.IBMJGSSProvider
security.provider.2=sun.security.provider.Sun
security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.jsse.IBMJSSEPProvider
security.provider.5=com.ibm.jsse2.IBMJSSEPProvider2
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
```
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
#security.provider.10=com.ibm.crypto.pkcs11.provider.IBMPKCS11

On AIX 6.1 x64

#security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ibm.jsse.IBMJSSEProvider
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
security.provider.7=com.ibm.security.cmskeystore.CMSProvider
security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO

The required entries in lunacfg are:

define (name = LUNA)
  library = /usr/lunasa/lib/libCryptoki2.so
  description = Luna config
  tokenLabel = <partition name>
  attributes (*, CKO_PRIVATE_KEY, *) = {
    CKA_SENSITIVE = true
  }
  attributes (*,CKO_PUBLIC_KEY, *) = {
    CKA_VERIFY = true
    CKA_ENCRYPT = true
  }