# JBoss Application Server

Integration Guide

security to be free

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.

**Document Part Number:** 007-012123-001, Rev. G

**Release Date:** September 2016

# Contents

# Preface

This document is intended to guide administrators through the steps for JBoss Application Server and SafeNet Luna HSM integration, and also covers the necessary information to install, configure, and integrate JBoss Application Server with SafeNet Luna HSM.

## Scope

This guide will teach you to install and get started with the JBoss Application Server and configure the SSL connection while securing the SSL keys and certificate on the Luna HSM. Installing JBoss Application Server is simple and easy. You can have it installed and running in no time.

## Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

| Old product name | New product name |
|---|---|
| Luna SA HSM | SafeNet Network HSM |
| Luna PCI-E HSM | SafeNet PCI-E HSM |
| Luna G5 HSM | SafeNet USB HSM |
| Luna Client | SafeNet HSM Client |

**NOTE:** These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

## 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

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

## 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.

| Contact Method | Contact Information | |
|---|---|---|
| **Address** | Gemalto<br>4690 Millennium Drive<br>Belcamp, Maryland  21017, USA | |
| **Phone** | US | 1-800-545-6608 |
| | International | 1-410-931-7520 |
| **Technical Support Customer Portal** | https://serviceportal.safenet-inc.com<br>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. | |

# 1
# Introduction

## Overview

This document is intended to guide security administrators through the steps for JBoss Application Server and SafeNet Luna HSM integration, and also covers the necessary information to install, configure, and integrate JBoss with SafeNet Luna Hardware Security Modules (HSMs).

The SafeNet Luna HSMs integrates with the JBoss to provide significant performance improvements by off-loading cryptographic operations from the JBoss server to the Luna HSMs and protecting the server's high value SSL private key and certificate within a FIPS 140-2 certified hardware security module.

## Understanding the JBoss Application Server

JBoss Application Server is the open source implementation of the Java EE suite of services. It comprises a set of offerings for enterprise customers who are looking for preconfigured profiles of JBoss Enterprise Middleware components that have been tested and certified together to provide an integrated experience. It's easy-to-use server architecture and high flexibility makes JBoss the ideal choice for users just starting out with J2EE, as well as senior architects looking for a customizable middleware platform.

Because it is Java-based, JBoss Application Server is cross-platform, easy to install and use on any operating system that supports Java. The readily available source code is a powerful learning tool to debug the server and understand it. It also gives you the flexibility to create customized versions for your personal or business use.

Installing JBoss Application Server is simple and easy. You can have it installed and running in no time. This guide will teach you to install and get started with the JBoss Application Server.

## 3rd Party Application Details

- JBoss EAP 6.3.0
- JBoss Application Server v7.1.1

  You can download the above servers from JBoss community site: http://www.jboss.org/jbossas/downloads/

# Supported Platforms

| JBoss Application Server | Platforms Tested | SafeNet Luna HSM Appliance version and Firmware | SafeNet Luna HSM Client Software version |
|---|---|---|---|
| JBoss AS7.1.1 | RHEL 6.5(64 bit) | 6.2.1f/w 6.10.9,<br>6.2.1f/w 6.24.2 | 6.x<br>(v6.2.1) |
| JBoss AS7.1.1 | RHEL 6.5(64 bit) | 6.1f/w 6.23 | 6.x<br>(v6.1.0) |
| JBoss AS7.1.1 | CentOS | 5.4.1/w 6.21.0 | 5.x<br>(v5.4.1) |
| JBoss EAP 6.3 | RHEL 6.5(64 bit) | 5.4.1 f/w 6.21.0 | 5.x<br>(v5.4.1) |
| JBoss AS7.1.1 | RHEL 6.0(64 bit) | 5.1 f/w 6.2.1 | 5.x<br>(v5.1.1) |

# 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.
- Initialize the SafeNet Network HSM appliance.
- Create and exchange certificates between the SafeNet Network HSM and your Client system.
- Create a partition on the HSM, remember the partition password that will be later used by JBoss. Register the Client with the partition.
- Execute "`/usr/safenet/lunaclient/bin/vtl verify`" command on the client system to display a partition from Luna SA.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SafeNet HSM with Trusted Path Authentication [i.e; FIPS 140-2 level 3] only)

## Java Setup

Set the following variables of Java to use Jboss & Java KEYTOOL utility.

```
export JAVA_HOME=path to the java installation directory, for example:

export JAVA_HOME=/usr/lib/jvm/java-1.7.0-openjdk-1.7.0.45.x86_64 (For JDK 7)

export PATH=$JAVA_HOME/bin:$PATH
```

## JBoss Setup

JBoss must be installed on the target machine to carry on with the integration process. For the installation of JBoss server refer the JBoss documentation. To install the JBoss, perform the following steps:

- Run the following command to install the JBoss from the downloaded file.

  ```
  # tar -zxvf jboss-as-7.x.x.Final.tar.gz -C /usr/local/
  ```

  It will install the JBoss as /usr/local/jboss-as-7.x.x.Final (where 7.x.x matches the version you downloaded).
- Set the JBOSS_HOME variable and provide the path of JBoss installation directory.

  ```
  # export JBOSS_HOME=/usr/local/jboss-7.1.1
  ```
- Run the following command to start the JBoss Server.

  ```
  # sh $JBOSS_HOME/bin/standalone.sh
  ```

  JBoss is installed and running. Browse http://localhost:8080/ to verify the server has started properly.

# 2 JBoss Server Integration with SafeNet Luna HSM

## Integration of JBoss Application Server with SafeNet Luna HSM

### Configure SafeNet HSM Client for SSL acceleration

1. Copy `libLunaAPI.so` and `LunaProvider.jar` from `/usr/safenet/lunaclient/jsp/lib` location to `$JAVA_HOME/jre/lib/ext/`.

   **Example:**

   ```
   cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so $JAVA_HOME/jre/lib/ext/

   cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar $JAVA_HOME/jre/lib/ext/
   ```

2. Modify the java.security file to include the Luna Provider. It is available at `$JAVA_HOME/jre/lib/security` location.

   ```
   security.provider.1=sun.security.pkcs11.SunPKCS11 ${java.home}/lib/security/nss.cfg

   security.provider.2=sun.security.provider.Sun

   security.provider.3=sun.security.rsa.SunRsaSign

   security.provider.4=sun.security.ec.SunEC

   security.provider.5=com.sun.net.ssl.internal.ssl.Provider

   security.provider.6=com.sun.crypto.provider.SunJCE

   security.provider.7=com.safenetinc.luna.provider.LunaProvider

   security.provider.8=sun.security.jgss.SunProvider

   security.provider.9=com.sun.security.sasl.Provider

   security.provider.10=org.jcp.xml.dsig.internal.dom.XMLDSigRI

   security.provider.11=sun.security.smartcardio.SunPCSCCSC
   ```

### Configuration Required for SafeNet Network HSM 6.1.0

Customer can request for SafeNet release Patch with Doc ID **DOW4088** from SafeNet.

Replace your patch shim (/usr/safenet/lunaclient/lib) with the SafeNet release patch and make the below changes in Chrystoki.conf file:

### Chrystoki with Logs

```
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;
}
```

Add the following line in Misc section of Chrystoki.conf file:

```
Misc = {
ApplicationInstance = RSA_SIGN_RAW;
FunctionBindLevel = 2;
}
```

### Chrystoki without Logs

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

Add the following line in Misc section of Chrystoki.conf file:

```
Misc = {
ApplicationInstance = RSA_SIGN_RAW;
FunctionBindLevel = 2;
}
```

**NOTE: Above changes are only applicable for SafeNet Network HSM 6.1.0**

## Generate trusted certificate on SafeNet Network HSM

1. Modify the /etc/Chrystoki.conf to include the following:

   ```
   Misc = {
   AppIdMajor=1;
   ```

```
AppIdMinor=1;
}
```

2. Open the session on Luna SA using application ID 1:1 with salogin utility

   ```
   /usr/lunasa/bin/salogin -o -i 1:1 -s <slot id> -p <password>
   ```

   **NOTE:** slot id is the slot number and password is SafeNet Network HSM partition password. Above two steps is needed for SafeNet Network HSM 5.1 only. No need to execute the above 2 steps for SafeNet Network HSM 5.2.1 onwards.

3. Change the directory where you want to create your keystore, if you want to use the JBoss configuration directory then

   ```
   cd $JBOSS_HOME/standalone/configuration/
   ```

4. Create a keystore file manually and enter the “tokenLabel:<Partition_Name>” entry in it. <PartitionName> is the SafeNet Luna HSM partition name, which is already registered.

5. Generate a new keystore using the java keytool utility that uses the luna provider to generate key and certificate

   **For RSA Keys:**

   ```
   keytool -genkey -keystore mykeystore -storepass password -alias jboss -keypass password -keyalg
   RSA -keysize 2048 -sigalg SHA1withRSA -validity 365 -storetype luna
   ```

   **For ECDSA Keys:**

   ```
   keytool -genkey -keystore mykeystore -storepass password -alias jboss -keypass password -keyalg
   EC -keysize 256 -sigalg SHA1withECDSA -validity 365 -storetype luna
   ```

   **NOTE:** password in the above command should be your partition pin.

   **NOTE:** It will ask you to provide the details to generate the self-signed certificate. Provide the details and your key and certificate will be generated in the SafeNet Network HSM and key store in the current directory.

   **NOTE:** When you want to use ECDSA keys then you must use JDK 7 (above 1.7.0_8). ECDSA Key support is not available in JDK 6.

   **NOTE:** When HSM is in FIPS mode, replace SHA1withRSA and SHA1withECDSA with **SHA256withRSA** and **SHA256withECDSA** respectively as a signature algorithm.

6. Create a Certificate Signing Request (CSR) using the generated key

   **For RSA Keys:**

```
keytool -certreq -alias jboss -file cert.csr -keypass password -keystore mykeystore -storepass
password -sigalg SHA1withRSA -storetype luna
```

**For ECDSA Keys:**

```
keytool -certreq -alias jboss -file cert.csr -keypass password -keystore mykeystore -storepass
password -sigalg SHA1withECDSA -storetype luna
```

**NOTE:** When HSM is in FIPS mode, replace SHA1withRSA and SHA1withECDSA with **SHA256withRSA** and **SHA256withECDSA** respectively as a signature algorithm.

7. Copy the contents of the generated CSR and submit it to the CA to sign the certificate request.
8. Obtain the signed certificate and root certificate from the Certificate Authority and import it to the key store.
9. Import the CA root certificate in the key store

```
keytool -import -trustcacerts -alias rootCA -file RootCA.cer -keystore mykeystore -storepass
password -storetype luna
```

10. Import the signed certificate in the key store.

```
keytool -import -trustcacerts -alias jboss -keypass password -file jboss.cer -keystore
mykeystore -storepass password -storetype luna
```

**NOTE:** Before importing the certificate in key store you must import the CA Root certificate and Intermediate certificate also if any.

## Configure JBoss to use the trusted certificate

1. By default JBoss uses the APR\Native library instead of Java library. To use the Java library you need to rename or remove the lib folder from the following location:

```
$JBOSS_HOME/modules/org/jboss/as/web/main/                          (JBoss AS 7.0.1)

$JBOSS_HOME/modules/system/layers/base/org/jboss/as/web/main        (JBoss EAP 6.3.0)
```

```
# mv $JBOSS_HOME/modules/system/layers/base/org/jboss/as/web/main/lib
$JBOSS_HOME/modules/system/layers/base/org/jboss/as/web/main/lib.bkp
```

Or

```
# rm -rf $JBOSS_HOME/modules/org/jboss/as/web/main/lib
```

2. Modify the connector setting in the $JBOSS_HOME/standalone/configuration/standalone.xml file, add the following:

```
<connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">

<ssl name="ssl"

    keystore-type="luna"

    key-alias="jboss"

    password="password"

    certificate-key-file="<jboss install directory path>/standalone/configuration/mykeystore"

    verify-client="false"
    ca-certificate-file="<jboss install directory path>/standalone/configuration/mykeystore"/>
</connector>
```

3. Start the JBoss server using the command

   ```
   sh $JBOSS_HOME/bin/standalone.sh
   ```

4. Open the browser and enter the URL that points the SSL enabled server:

   ```
   https://<ip address>:8443/
   ```

   Accept the certificate and it will open the JBoss Application Server Console.

   You have successfully configured the SSL configuration on JBoss whereas Private Key and SSL Certificate are secured on SafeNet Luna HSM.

# 3 Troubleshooting Tips

## Problem

“SSL ERROR” received on accessing JBoss on HTTPS as Sun JDK used with JBoss and generated the ECDSA keys on SafeNet Luna HSM.

## Solution

1. Sun PKCS11 provider must be present in the java.security file ($JAVA_HOME/jre/lib/security.) and Luna Provider must be above on SunEC provider.

   ```
   security.provider.1=sun.security.pkcs11.SunPKCS11 ${java.home}/lib/security/nss.cfg
   security.provider.2=sun.security.provider.Sun
   security.provider.3=sun.security.rsa.SunRsaSign
   security.provider.4=com.safenetinc.luna.provider.LunaProvider
   security.provider.5=sun.security.ec.SunEC
   security.provider.6=com.sun.net.ssl.internal.ssl.Provider
   security.provider.7=com.sun.crypto.provider.SunJCE
   security.provider.8=sun.security.jgss.SunProvider
   security.provider.9=com.sun.security.sasl.Provider
   security.provider.10=org.jcp.xml.dsig.internal.dom.XMLDSigRI
   security.provider.11=sun.security.smartcardio.SunPCSC
   ```

2. Save the java.security file after making above changes and make sure that nss.cfg file is present and if not present create it manually in the $JAVA_HOME/jre/lib/security along with java.security file and must have the following entries for hardware token to support SSL/TLS encryption:

   ```
   name = NSS
   nssLibraryDirectory = /usr/lib64
   nssDbMode = noDb
   attributes = compatibility
   ```

3. Development libraries for PKCS #11 (Cryptoki) using NSS must be installed on the system. Use the following command to install the binaries:

   ```
   # sudo yum install nss-pkcs11-devel
   ```

4. Restart JBoss Application Server after making all the above changes and then access the page using HTTPS.