Oracle HTTP Server

Integration Guide

gemalto
security to be free

Document Part Number: 007-012181-001, Rev. F

Release Date: September 2018

Contents

Preface

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

Scope

This technical information guide provides instructions for setting up Oracle HTTP Server running with SafeNet Luna HSM for securing the SSL certificate private key. This guide explains how to install and configure the Oracle HTTP Server while storing the certificate private key on SafeNet Luna 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

Convention	Description
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type **dir /p**.) • Button names (Click **Save As**.) • Check box and radio button names (Select the **Print Duplex** check box.) • Window titles (On the **Protect Document** window, click **Yes**.) • Field names (**User Name:** Enter the name of the user.) • Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) • 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

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://supportportal.gemalto.com 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

Oracle HTTP Server is the Web server component for Oracle Fusion Middleware. It provides an HTTP listener for Oracle Web Logic Server and the framework for hosting static pages, dynamic pages, and applications over the Web. Oracle HTTP Server is beneficial because it serves both dynamic and static content, and can integrate with both Oracle and non-Oracle products.

Oracle HTTP Server is based on the proven, open source technology of Apache. Oracle HTTP Server Apache infrastructure, includes all base Apache modules and modules developed specifically by Oracle.

This guide demonstrates how to complete Oracle HTTP Server Integration using a SSL key generated on a SafeNet Luna HSM.

Using a SafeNet Luna HSM to generate the RSA keys for Oracle HTTP Server provides the following benefits:

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

3rd Party Application Details

- Oracle HTTP Server 12c

  You can download the Oracle HTTP Server from the Oracle Support site.

NOTE: If you are using an earlier version of Oracle HTTP Server you will require a previous version of the Integration Guide.

Access *OracleHTTPServer_SafeNetLunaHSM_Integration Guide_RevE*.

Supported Platforms

List of the platforms which are tested with the following HSMs:

SafeNet Luna HSM: is a standalone network-attached appliance that physically and logically secures cryptographic keys and cryptographic processing. The purpose of an HSM is to protect sensitive data from being stolen by providing a highly secure operation structure. HSMs are fully contained and complete solutions for cryptographic processing, key generation, and key storage.

This integration is supported/verified with SafeNet Luna HSM on the following operating system:

- RHEL

Prerequisites

Before starting the integration of Oracle HTTP Server with SafeNet Luna Network HSM, complete the following:

Configuring SafeNet Luna Network HSM

Before you get started with SafeNet Luna HSM ensure the following:

1. SafeNet Luna Network HSM appliance and a secure admin password.
2. SafeNet Luna Network HSM, and a hostname, suitable for your network.
3. SafeNet Luna Network HSM network parameters are set to work with your network.
4. Initialize the HSM on the SafeNet Luna Network HSM appliance.
5. Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
6. Create a partition on the HSM that will be later used for Oracle HTTP Server.
7. Register a client for the system and assign the client to the partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
8. Ensure that the partition is successfully registered and configured. The command to see the registered partition is:

```
# /usr/safenet/lunaclient/bin/lunacm
LunaCM v7.1.0-379. Copyright (c) 2006-2017 SafeNet.

Available HSMs:
Slot Id ->              1
Label ->                OHS
Serial Number ->        1213475834492
Model ->                LunaSA 7.1.0
Firmware Version ->     7.1.0
Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning Mode
Slot Description ->     Net Token Slot
```

NOTE: Follow the SafeNet Luna Network HSM documentation for detailed steps for creating NTLS connection, initializing the partitions and various user roles.

Constraints on SafeNet Luna Network HSM

Verify SafeNet Luna HSM <slot> value

SafeNet Luna HSM needs to be edited for slot id because by default it is set to 0. Set the slot id to 1 by making the following changes in the **Chrystoki.conf** configuration file:

```
Presentation = {
OneBaseSlotId = 1;
}
```

SafeNet Luna HSM in FIPS mode

If you are using the FIPS Mode, edit the **Chrystoki.conf** file as follows to generate the RSA keys:

```
Misc = {
RSAKeyGenMechRemap = 1;
}
```

For PED based HSM

Edit the **Chrystoki.conf** file as follows for PED based HSM:

```
Misc = {
ProtectedAuthenticationPathFlagStatus = 1;
}
```

Installing Oracle HTTP Server

It is recommended that you should have knowledge of the *Oracle HTTP Server*. Refer to the Oracle documentation for more information on installation requirements and installation process. This integration guide uses the default installation directory PATH for this integration i.e. "**/u01/app/oracle/Oracle/Middleware/Oracle_Home"** and presumes that the Oracle HTTP Server software is already installed and configured on the system.

Adding Oracle user to hsmusers group

To allow non-root users or applications access to the HSM, add the users to the **hsmusers** group.

1. Ensure that you have **sudo** or **root** privileges on the workstation.
2. Add the **oracle** user to the hsmusers group.

   ```
   # sudo gpasswd --add oracle hsmusers
   ```

2

Integrating Oracle HTTP Server with SafeNet Luna HSM

This section demonstrates the steps to generate SSL keys and certificate on a SafeNet Luna HSM. Additionally, it provides procedural materials for creating the PKCS#11 wallet and configuring the PKCS#11 wallet to access the keys and certificate on the SafeNet Luna HSM.

Creating the Oracle HTTP Server Keys and Certificate

Access the system as the **root** user and complete the following procedure to create the RSA keys and certificate for the Oracle HTTP Server on the SafeNet Luna HSM.

To open the application connection with HSM partition

1. Sautil utility is used to allow a login state to be persisted for a given application connection, which is part of our OpenSSL Toolkit. Download the OpenSSL Toolkit (GemEngine) from Gemalto support portal.

   NOTE: Doc IDs for downloading the GemEngine v1.2 from support portal is KB0016309.

2. After downloading unzip the file in a directory, let say **/home**, and copy the **sautil** to **/usr/bin** directory.

   ```
   # cp /home/gemengine-1.2/builds/linux/rhel/64/1.0.2/sautil /usr/bin/
   ```

3. Open the **/etc/Chrystoki.conf** file in a text editor and add the following in **Misc** Section:

   ```
   Misc = {
   AppIdMajor = 10;
   AppIdMinor = 11;
   Apache = 1;
   }
   ```

   NOTE: There should be other settings **Misc** section please do not remove them and you can choose any random major/minor id as per your choice.

4. Open the application connection and persist the login state for Oracle HTTP Server using the command below and provide the Crypto Officer password when prompts.

   ```
   # sautil -o -s 1 -i 10:11 -v -q
   Copyright 2009-2018 SafeNet. All rights reserved.
   sautilis the property of SafeNet and is provided to our customers for
   ```

```
the purpose of diagnostic and development only.  Any re-distribution of this
program in whole or in part is a violation of the license agreement.

Config file: /etc/Chrystoki.conf.
Will use application ID [10:11].
Application ID [10:11] opened.
Open ok.
Session opened. Handle 1.
HSM Slot Id is 1.
HSM Label is "OHS                          ".
Enter Crypto-Officer Password:
**********************************************************************************************
**********************************************************************************************
************************************************************

WARNING: Application Id 10:11 has been opened for access. Thus access will
         remain open until all sessions associated with this Application Id are
         closed or until the access is explicitly closed.
```

NOTE: The sautil utility is provided to assist clients that do not include the requisite HSM login and logout capability within the client application.

To create the Oracle HTTP Server keys and certificate

1. Execute the following to generate a RSA key pair. Enter the partition password, select the RSA Mechanism Type, and specify the public exponent when prompted:

   ```
   # ./cmu generatekeypair -labelPublic=OHSpub -labelPrivate=OHSpriv -keytype=RSA -modulusbits=2048
   -publicExponent=65537 -sign=T -verify=T -encrypt=T -decrypt=T -wrap=T -unwrap=T
   Please enter password for token in slot 1 : ********
   Select RSA Mechanism Type -
   [1] PKCS [2] FIPS 186-3 Only Primes [3] FIPS 186-3 Auxiliary Primes : 1
   Select public exponent - [1] 3 [2] 17 [3] 65537 : 3
   ```

2. Both the Public Key and Private Key handle are required to create the certificate request. Execute the following command to list the generated key pair.

   ```
   # ./cmu list
   Please enter password for token in slot 1 : ********
   handle=258      label=OHSpriv
   handle=267      label=OHSpub
   ```

   Copy both the Public Key and Private Key handles.

3. Create a certificate request using key pair generated on HSM. Execute the following command and respond to the prompts:

   ```
   # ./cmu requestCertificate -publichandle=267 -privatehandle=258 -outputFile=cert.req
   ```

```
Please enter password for token in slot 1 : ********
Enter Subject 2-letter Country Code (C) : IN
Enter Subject State or Province Name (S) : Uttar Pradesh
Enter Subject Locality Name (L) : Noida
Enter Subject Organization Name (O) : Gemalto
Enter Subject Organization Unit Name (OU) : OHSM
Enter Subject Common Name (CN) : localhost
Enter EMAIL Address (E) :
```

Submit the certificate request to a CA to obtain the signed certificate and signing certificate from your CA.

4. After obtaining the signed certificate and signing certificate from the CA, import the CA certificate and signed certificate to the partition using the following command:

```
# ./cmu import -inputfile=root.cer -label hsmintg-CA
# ./cmu import -inputfile=OHSCert.cer -label OHSCert
```

5. Verify that the keys and certificates are stored on the SafeNet Luna HSM partition. Execute:

```
# ./cmu list
Please enter password for token in slot 1 : ********
handle=201      label=OHSCert
handle=178      label=hsmintg-CA
handle=258      label=OHSpriv
handle=267      label=OHSpub
```

The Keys and Certificate required for Oracle HTTP Server are available on the HSM. Next, you must create the Oracle HTTP Server wallet and configure it to access the keys and certificates stored on the SafeNet Luna HSM.

Creating Oracle HTTP Server PKCS#11 Wallet

Create the HTTP Server's PKCS$11 wallet and configure the wallet to access the keys and certificates stored externally on the SafeNet Luna HSM.

To create the Oracle HTTP Server PKCS#11 Wallet

1. The following environment variables are necessary for creating the Oracle wallet. Export the following environment variables:

```
# export ORACLE_HOME=/u01/app/oracle/Oracle/Middleware/Oracle_Home
# export LD_LIBRARY_PATH=$ORACLE_HOME/lib:/usr/safenet/lunaclient/lib
# export JAVA_HOME=$ORACLE_HOME/oracle_common/jdk/jre
```

2. The Oracle wallet is available in the following location in your <Oracle Home Installation Directory>. Locate the Oracle wallet.

   For example:
   `$ORACLE_HOME/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/<component name>/keystores/default/`

3. Rename the **cwallet.sso** file before creating the PKCS#11 wallet. Navigate to the default wallet location and rename the available wallet.

```
# cd
$ORACLE_HOME/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/keystores/default/

# mv cwallet.sso cwallet.bkp
```

4. Navigate to the directory containing the **orapki** utility and create the Oracle wallet for accessing the HSM.

```
# cd $ORACLE_HOME/oracle_common/bin

# ./orapki wallet create -wallet
$ORACLE_HOME/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/keystores/default/ -auto_login

Oracle PKI Tool : Version 12.2.1.3.0

Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights reserved.

Enter password:********

Enter password again:********

Operation is successfully completed.
```

   The system will prompt you to enter the wallet password. Set the wallet password to be the same as your SafeNet Luna HSM partition password.

5. Add the PKSC#11 information required to access the HSM contents by executing the command below:

```
# ./orapki wallet p11_add -wallet
$ORACLE_HOME/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/keystores/default/ -p11_lib /usr/safenet/lunaclient/lib/libCryptoki2_64.so -p11_tokenlabel OHS -p11_tokenpw userpin1 -p11_certlabel OHSCert -pwd userpin1

Oracle PKI Tool : Version 12.2.1.3.0

Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights reserved.
```

   Where **-p11_lib** is PKCS#11 library, **-p11_tokenlabel** is your HSM partition label, **-p11_tokenpw** is the partition password, **-p11_certlabel** is your certificate label, and **-pwd** is the Oracle wallet password.

6. After adding the PKCS#11 information, verify that Oracle is accessing the HSM partition objects by executing the following command:

```
# ./orapki wallet p11_verify -wallet
$ORACLE_HOME/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/keystores/default/ -pwd userpin1

Oracle PKI Tool : Version 12.2.1.3.0

Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights reserved.

Cert with label: OHSCert and subject name: CN=localhost,OU=OHS-HSM,O=Gemalto-HSM,L=Noida,ST=Uttar Pradesh,C=IN has a matching private key on token.

Cert with subject name: CN=hsmintg-CA,DC=hsmintg,DC=com has NO matching private key on token.
Added to wallet as a CA cert.

Cert with subject name: CN=localhost,OU=OHS-HSM,O=Gemalto-HSM,L=Noida,ST=Uttar Pradesh,C=IN
installed as user cert in wallet.
```

7. Add the CA certificate to the Oracle wallet as a Trusted Certificate that was used to sign the Oracle HTTP Server certificate.

```
# ./orapki wallet add -wallet
$ORACLE_HOME/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/keystores/default/ -cert /usr/safenet/lunaclient/bin/root.cer -trusted_cert -pwd userpin1

Oracle PKI Tool : Version 12.2.1.3.0

Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights reserved.
```

```
Operation is successfully completed.
```

8. Verify that the Oracle wallet is displaying the PKCS#11 information and the trusted certificate by executing the following command:

```
# ./orapki wallet display -wallet
$ORACLE_HOME/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/ke
ystores/default/

Oracle PKI Tool : Version 12.2.1.3.0

Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights reserved.

PKCS11 token information:

Library:/usr/safenet/lunaclient/lib/libCryptoki2_64.so

Token label:OHS

Token passphrase:<...>

Certificate label:OHSCert

Requested Certificates:

User Certificates:

Trusted Certificates:

Subject:        CN=hsmintg-CA,DC=hsmintg,DC=com
```

9. Navigate to the directory containing the Node Manager and OHS Components scripts and run them to start the Oracle HTTP Server.

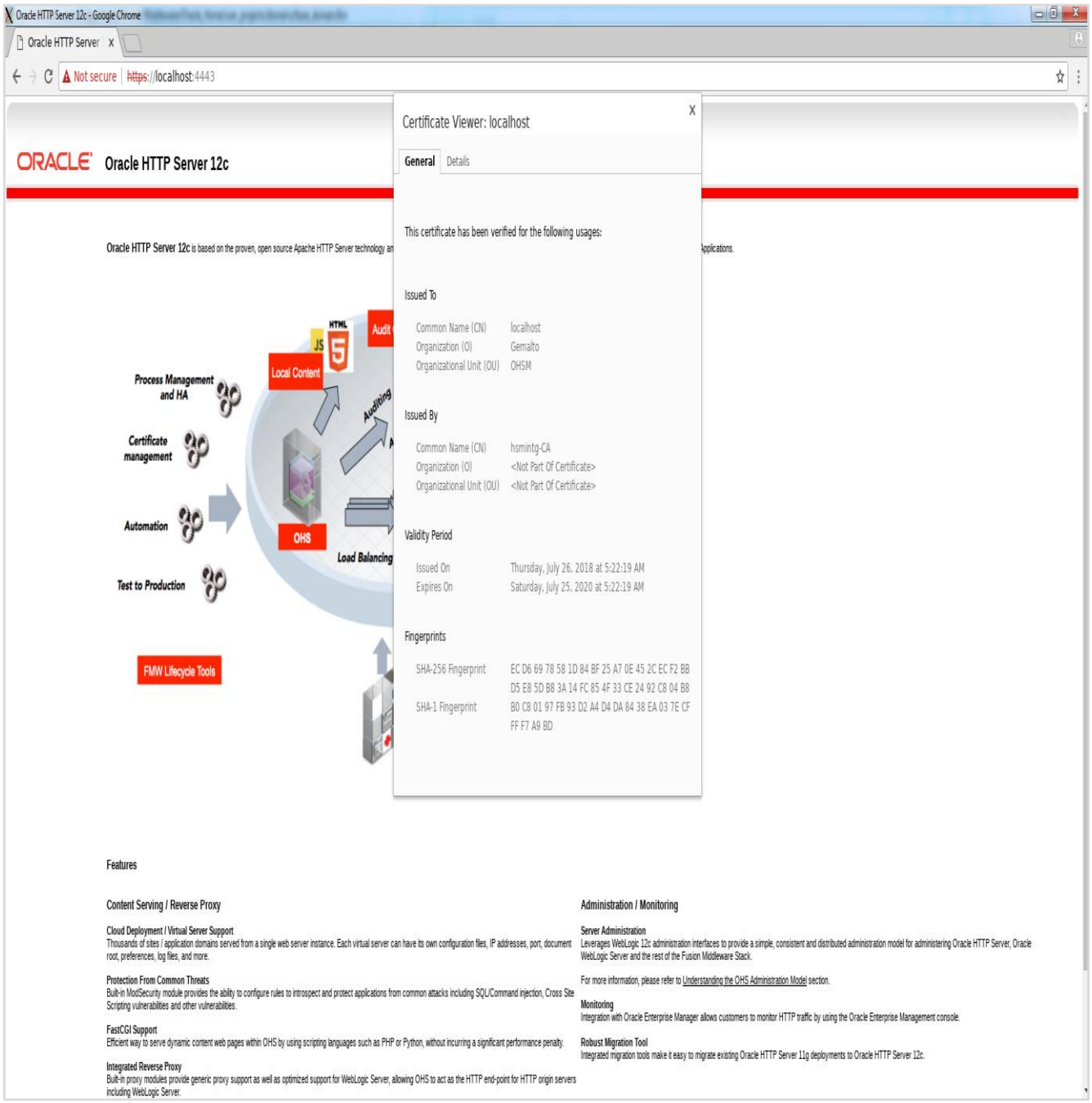
```
# cd $ORACLE_HOME/user_projects/domains/base_domain/bin

# ./startNodeManager.sh

# ./startComponent.sh ohs1
```

When prompted, provide the password for Node Manager Admin to connect the OHS component to Node Manager. The Node Manager Admin password was set during the Oracle HTTP Server installation.

10. Open the web browser and access the Oracle HTTP Server SSL page, it will prompt you to accept the certificate.

https://localhost:4443

11. Verify that the certificate you are going to accept is the same as the certificate you recently generated on the HSM partition.



This completes the Oracle HTTP Server integration with the SafeNet Luna HSM. The Oracle HTTP Server's SSL private key and certificate is secured by the SafeNet Luna HSM.