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 ....................................................................................................... 8
    SafeNet Luna HSM (v7.x) ............................................................................................ 8
    SafeNet Luna HSM (v4.x/5.x/6.x) ................................................................................ 8
  Prerequisites ..................................................................................................................... 9
    Configuring PED Auth SafeNet Luna HSM (v6.1/v7.0) ............................................... 9
    Configuring PED Auth SafeNet Luna HSM (v6.2.x) .................................................... 10
    Configuring SafeNet Luna Network HSM 7.x .............................................................. 10
    Configuring SafeNet Luna Network HSM (v4.x/5.x/6.x) ........................................... 13
    Using Luna 6.x/7.x in FIPS Mode ................................................................................ 14

2 Oracle iPlanet Web Server Installation ....................................................................... 15

3 Oracle iPlanet Web Server Configuration with SafeNet Luna HSM .............................. 16
  Oracle iPlanet Web Server 7.0 with SafeNet Luna HSM ................................................ 16
  Oracle iPlanet Web Server 6.1 with SafeNet Luna HSM ................................................ 27
This document is intended to guide administrators through the steps for Oracle iPlanet Web Server and SafeNet Luna HSM integration. This guide provides the necessary information to install, configure, and integrate Oracle iPlanet with SafeNet Luna HSM.

Scope

This guide provides an overview of how to integrate Oracle iPlanet Web Server with SafeNet Luna HSM. It explains how to install and configure the Oracle iPlanet Web Server while storing 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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
</table>
| **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. |
Overview

This document covers the necessary information to install, configure, and integrate Oracle iPlanet Web Server with SafeNet Luna HSM.

SafeNet Luna HSMs integrate with the Oracle iPlanet Web Server to provide significant performance improvements by off-loading cryptographic operations from the Oracle iPlanet Web Server to SafeNet Luna HSMs. In addition, SafeNet Luna HSM provides extra security by protecting and managing the server’s high value SSL private key within a FIPS 140-2 certified hardware security module.

This integration between SafeNet Luna HSM and Oracle iPlanet Web Server uses the industry standard PKCS#11 interface.

The following is the procedure for installing and configuring the SafeNet Luna HSM with Oracle iPlanet Web Server.

The installation is performed in several steps:

- Install and configure the SafeNet Luna HSM.
- Install the Oracle iPlanet Web Server.
- Configure the Oracle iPlanet Web Server.

3rd Party Application Details

- Oracle iPlanet Web Server 7.0 SP24 RHEL 7 (64 bit)
- Oracle iPlanet Web Server 7.0 SP15 RHEL 6.5 (64 bit)
- Oracle iPlanet Web Server 6.1 SP14 SPARC (64bit)
## Supported Platforms

The following platforms are tested with SafeNet Luna HSM:

### SafeNet Luna HSM (v7.x)

**Oracle iPlanet Web Server 7.0 SP24 RHEL 7 (64 bit)**

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Network HSM Appliance Version</th>
<th>Firmware Version</th>
<th>SafeNet Luna Client Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 7 64-bit</td>
<td>7.2.0</td>
<td>7.2.0</td>
<td>7.2.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7 64-bit</td>
<td>7.1.0</td>
<td>7.1.0</td>
<td>7.1.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7 64-bit</td>
<td>7.0.0</td>
<td>7.0.1</td>
<td>7.0.0</td>
</tr>
</tbody>
</table>

### SafeNet Luna HSM (v4.x/5.x/6.x)

**Oracle iPlanet Web Server 7.0 SP24 RHEL 7 (64 bit)**

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Network HSM Appliance Version</th>
<th>Firmware Version</th>
<th>SafeNet Luna Client Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 7 64-bit</td>
<td>6.3.0</td>
<td>6.27.0</td>
<td>6.3.0</td>
</tr>
</tbody>
</table>

### Oracle iPlanet Web Server 7.0 SP15 RHEL 6.5 (64bit)

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>HSM</th>
<th>Firmware</th>
<th>Luna Client Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 6.5 64-bit</td>
<td>6.2.2</td>
<td>6.24.3</td>
<td>6.2.2</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6.5 64-bit</td>
<td>6.2.1</td>
<td>6.24.2</td>
<td>6.2.1</td>
</tr>
</tbody>
</table>
### Platforms Tested

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>HSM</th>
<th>Firmware</th>
<th>Luna Client Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 6.5 64-bit</td>
<td>6.0.0</td>
<td>6.22.0</td>
<td>6.x (v6.0, 6.1)</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6.5 64-bit</td>
<td>5.4.7</td>
<td>6.2.1</td>
<td>5.x (v5.0.x, 5.2.x, 5.3.x, 5.4.x)</td>
</tr>
</tbody>
</table>

**Oracle iPlanet Web Server 6.1 SP14 SPARC (64bit)**

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>HSM</th>
<th>Firmware</th>
<th>Luna Client Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris 10 SPARC (64-bit)</td>
<td>4.5</td>
<td>4.8.1</td>
<td>4.5.x</td>
</tr>
</tbody>
</table>

**NOTE:** Oracle iPlanet Web Server is also tested with Luna Clients in HA & FIPS Mode.

---

### Prerequisites

**Configuring PED Auth SafeNet Luna HSM (v6.1/v7.0)**

You need to obtain the following patch to work with PED based SafeNet Luna HSM when using the version 6.1 and 7.0:

**DOC ID:** DOW4166  
**Part No:** 630-010467-001 Alpha3  
**TITLE:** Luna 5 Compatibility Shim for Luna 6

---

**NOTE:** The below configuration is only applicable for Version 6.1/7.0 of PED based SafeNet Luna HSM.

---

**CONFIGURATION:**

1. Copy the libshim.so to `<lunaclient installation>/lib` directory. It is advised to first rename the previous shim.
2. Point the application to the libshim.so instead of the Cryptoki shared object library. To point it, open the `/etc/Chrystoki.conf` file and make the following changes:
   ```
   Chrystoki2 = {
   LibUNIX64 = /usr/safenet/lunaclient/lib/libshim.so;
   }
   Shim2 = {
   ```
LibUNIX64 = /usr/safenet/lunaclient/lib/libCryptoki2_64.so;
}
Misc = {
  :
  ApplicationInstance=SAS_COMPATIBILITY;
  FunctionBindLevel=2;
  :
}

Contact Customer Support if you need assistance regarding the above configuration.

### Configuring PED Auth SafeNet Luna HSM (v6.2.x)

For Ped based SafeNet Luna HSM make sure ProtectedAuthenticationPathFlagStatus is set to ‘1’ in Misc Section of Chrystoki.conf file.

Misc = {
  ProtectedAuthenticationPathFlagStatus = 1;
}

### Configuring SafeNet Luna Network HSM 7.x

SafeNet Luna Network HSM allows to create Per-Partition Security Officer (PPSO) partition. HSM Administrator is not Security Officer (SO) for PPSO partitions. The HSM SO/Administrator elects to create a partition as PPSO-type, which creates an empty structure that is handed to the new owner, who initializes the partition to create the Partition Security Officer (PSO) role or identity for management functions. The PSO in turn creates the partition Crypto Officer (CO) to control client cryptographic operations on the partition.

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX/Windows systems. Before you get started ensure the following:

- SafeNet Luna Network HSM appliance and a secure admin password.
- SafeNet Luna Network HSM, and a hostname, suitable for your network.
- SafeNet Luna Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Luna Network HSM appliance.
- Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
- Create a partition on the HSM that will be later used by Oracle iPlanet Web Server.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Luna HSM. The general form of command is "C:\Program Files\SafeNet\LunaClient>vtl verify" for Windows and "/usr/safenet/lunaclient/bin/vtl verify" for Unix.
- Initialize the Partition as mentioned in steps below for Password/PED based respectively
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Luna Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

### Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition

These instructions assume a password-authenticated SafeNet Luna Network HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer.
• **Initialize the Partition SO role**

  Set the active slot to the created, uninitialized, application partition:
  
  Type `slot set -slot <slot number>`
  
  lunacm:> slot set -slot 0
  
  Current Slot Id: 0  (Luna User Slot 7.0.0 (Password) Signing With Cloning Mode)
  
  Command Result: No Error

  Initialize the application partition, to create the partition's Security Officer (SO).
  
  Type `partition init -label <part_label>`
  
  lunacm:> par init -label <part_label> -password <part_password>
  
  You are about to initialize the partition.
  
  All partition objects will be destroyed.
  
  Are you sure you wish to continue?
  
  Type 'proceed' to continue, or 'quit' to quit now -> proceed
  
  Command Result: No Error

• **Initialize the Crypto Officer role**

  a. The SO of the application partition can now assign the first operational role within the new partition. Type `role login -name Partition SO`.
  
  lunacm:> role login -name Partition SO

  b. Type `role init -name Crypto Officer`.
  
  lunacm:> role init -name Crypto Officer

  c. The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.
  
  Type `role logout`.
  
  lunacm:> role logout

**Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition**

These instructions assume a PED-authenticated SafeNet Luna Network HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer.

Take the following steps to initialize the PSO and CO roles:

• **Initialize the Partition SO role**

  Set the active slot to the created, uninitialized, application partition.
  
  Type `slot set -slot <slot number>`
  
  lunacm:> slot set -slot 0
  
  Current Slot Id: 0  (Luna User Slot 7.0.0 (PED) Signing With Cloning Mode)
  
  Command Result: No Error

  Initialize the application partition, to create the partition's Security Officer (SO).
  
  Type `partition init -label <part_label>`
  
  lunacm:> par init -label <part_label>
  
  You are about to initialize the partition.
  
  All partition objects will be destroyed.
  
  Are you sure you wish to continue?
  
  Type 'proceed' to continue, or 'quit' to quit now -> proceed
  
  Please attend to the PED.
  
  Respond to SafeNet PED prompts...
Command Result : No Error

- **Initialize the Crypto Officer role**
  The SO of the application partition can now assign the first operational role within the new partition.
  
  Type `role login -name Partition SO`
  
  Type `role init -name Crypto Officer`.

  lunacm:> role init -name Crypto Officer
  Please attend to the PED.
  Respond to SafeNet PED prompts...
  Command Result: No Error

  The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.
  
  Type `role logout`.

  Now, the Crypto Officer, or an application using the CO’s challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto Officer logs in with `role login -name Crypto Officer`. However, the Crypto Officer can create, modify and delete crypto objects within the partition, in addition to merely using existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer, but cannot modify them.

  **NOTE**: The black Crypto Officer PED key/Crypto Officer Password (in case of PW-Ath) is valid for the initial login only. You must change the initial credential on the key using the command `role changepw` during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_EXPIRED error while performing role-dependent actions.

**Controlling User Access to the HSM**

By default, only the root user has access to the HSM. You can specify a set of non-root users that are permitted to access the HSM, by adding them to the `hsmusers` group. The client software installation automatically creates the hsmusers group. The hsmusers group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your hsmusers group configuration.

**Adding users to hsmusers group**

To allow non-root users or applications access to the HSM, assign the users to the `hsmusers` group. The users you assign to the hsmusers group must exist on the client workstation. Users you add to the hsmusers group are able to access the HSM. Users who are not part of the hsmusers group are not able to access the HSM.

- **Adding a user to hsmusers group**
  
  a. Ensure that you have `sudo` privileges on the client workstation.
  
  b. Add a user to the hsmusers group.

    `sudo gpasswd --add <username> hsmusers`

    where `<username>` is the name of the user you want to add to the hsmusers group.
Removing users from hsmusers group

To revoke a user's access to the HSM, you can remove them from the hsmusers group.

- **Removing a user from hsmusers group**
  a. Ensure that you have `sudo` privileges on the client workstation.
  b. Remove a user from the hsmusers group.

    ```
    sudo gpasswd -d <username> hsmusers
    ```

    Where `<username>` is the name of the user you want to remove from the hsmusers group. You must log in again to see the change.

    **NOTE:** The user you delete will continue to have access to the HSM until you reboot the client workstation.

Configuring SafeNet Luna Network HSM (v4.x/5.x/6.x)

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX systems. Before you get started ensure the following:

- SafeNet Luna Network HSM appliance and a secure admin password.
- SafeNet Luna Network HSM, and a hostname, suitable for your network.
- SafeNet Luna Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Luna Network HSM appliance.
- Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
- Create a partition on the HSM, remember the partition password that will be later used by Oracle iPlanet Web Server.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Luna Network HSM. The general form of command is "C:\Program Files\SafeNet\LunaClient> vtl verify" for Windows and "/usr/safenet/lunaclient/bin/vtl verify" for Unix.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Luna Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).
Using Luna 6.x/7.x in FIPS Mode

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

Misc = {
    RSAKeyGenMechRemap = 1;
}

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

NOTE: The above configuration is valid for Luna 7.x and Luna 6.x (F/W Version 6.22.0 and above only).
To install Oracle iPlanet Web Server, perform the following steps:

1. Login as the root user and unpack the .gz or .zip file to a temporary directory using gunzip filename or unzip filename.

2. Untar the unzipped file using tar –xvf filename.
   This command unpacks the server files and creates a temporary directory structure under the current directory. Unpacking the file may take a little time. Change to the directory where the files have been unpacked.

3. Execute the command "./setup" to start web server installation.

Refer the Oracle iPlanet Web Server documentation for more details.

After the installation follow the steps mentioned in the next Chapter for configuring Web Server with SafeNet Luna HSM.
Oracle iPlanet Web Server Configuration with SafeNet Luna HSM

Oracle iPlanet Web Server 7.0 with SafeNet Luna HSM

To configure the Web Server to recognize the Luna SA cryptographic device, perform the following steps:

1. Add the following in the LD_LIBRARY_PATH:
   
   ```
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<Path to Luna SA installation directory>/lib:<Path to Web Server installation directory>/lib
   ```

2. Change to the alias directory of the Web Server by using the command:
   
   ```
   cd <Path to Web Server installation directory>/https-localhost.localdomain/config
   ```

   Where the `<Path to Web Server installation directory>` is root directory of the Web Server.

   List the contents of the alias directory to see if the file `secmod.db` exists. If the file does not exist, follow the steps below. If the file exists go to step 4.

3. Create a security module database by using the `modutil` utility as below:
   
   ```
   /opt/oracle/webserver7/bin/modutil -create -nocertdb -dbdir .
   ```

   `modutil` displays the following warning:

   ```
   WARNING: Performing this operation while Communicator is running could cause corruption of your security databases. If Communicator is currently running, you should exit Communicator before continuing this operation. Type 'q <enter>' to abort, or <enter> to continue:
   ```

   Ensure that the web browser and communicator are not running and press Enter.

4. Disable the compliance with the FIPS 140-2 in the Web Server. To do this use the `modutil` utility as below:
   
   ```
   /opt/oracle/webserver7/bin/modutil -fips false -nocertdb -dbdir .
   ```

   `modutil` displays the following warning:

   ```
   WARNING: Performing this operation while Communicator is running could cause corruption of your security databases. If Communicator is currently running, you should exit Communicator before continuing this operation. Type 'q <enter>' to abort, or <enter> to continue:
   ```

   Ensure that the web browser and communicator are not running and press Enter.
5. If FIPS mode has already been disabled, modutil displays the following message: (default)
   FIPS mode already disabled.
   Otherwise, modutil will display the following message:
   Using database directory...
   FIPS mode disabled.

6. Add the Luna SA PKCS #11 library to the security database by using the command:
   For (32-bit):
   `/opt/oracle/webserver7/bin/modutil -add lunasa -libfile
   /usr/safenet/lunaclient/lib/libCryptoki2.so -nocertdb -dbdir`.
   For (64-bit):
   `/opt/oracle/webserver7/bin/modutil -add lunasa -libfile
   /usr/safenet/lunaclient/lib/libCryptoki2_64.so -nocertdb -dbdir`.
   modutil displays the following warning:

   **WARNING**: Performing this operation while Communicator is running could cause corruption of your security databases. If Communicator is currently running, you should exit Communicator before continuing this operation. Type 'q <enter>' to abort, or <enter> to continue:
   Ensure that the web browser and communicator are not running and press Enter.
   The following message will be displayed:
   Module "lunasa" added to database.

7. Ensure that the module has been added by executing the modutil utility as below:
   `/opt/oracle/webserver7/bin/modutil -list -nocertdb -dbdir`.
   
   Listing of PKCS #11 Modules
   
   1. NSS Internal PKCS #11 Module
      slots: 2 slots attached
      status: loaded
      slot: NSS Internal Cryptographic Services
      token: NSS Generic Crypto Services
      slot: NSS User Private Key and Certificate Services
      token: NSS Certificate DB
   2. lunasa
      library name: /usr/safenet/lunaclient/lib/libCryptoki2_64.so
      slots: 4 slots attached
      status: loaded
      slot: Net Token Slot
      token: part1
      slot: Luna UHD Slot
      token:
slot: Luna UHD Slot

token:

slot: Luna UHD Slot

token:

8. Start the web server using the following command:
   
   cd /opt/oracle/webserver7/admin-server/bin
   ./startserv

9. If you have configured Oracle on Non-SSL Port, then open the browser with the following URL:

   http://<ServerName or IP Address>:port

   For Example: http://<ServerName or IP Address>:8800

   If it is configured on SSL then open the browser with the following URL:

   https://<ServerName or IP Address>:port

   For Example: https://<ServerName or IP Address>:8989
10. Enter the username and password to log in to the server with the administrator password provided during the installation of the web server.

![Server Login](image)

11. Ensure that all the instances are running and no deployment is pending. To verify pending deployments, go to the Configurations tab, click `<Virtual Server name>` under the Configurations list.

Click **Pull and Deploy configuration from** in case it is pending.

12. Click **Server Certificates**.

![Server Certificates](image)
13. Click **Set Password**. And provide Luna SA partition/token password. Click **OK**.
14. On **Server Certificate** tab click **Request**... and follow the wizard. At step 2 select Luna HSM token, provide password and click **Next**.

15. On step 3 provide all information for certificate request. Click **Next**.
16. Provide Key Type details in the step 4.

17. Select **CA Signed Certificate** as Certificate Type. Click **Next**. It will return certificate request. Get it signed from third party CA.

18. Once you receive signed certificate go to **Server Certificates** tab click **Install**. Provide token details and paste certificate data or select signed certificate file. Click **Next**.
19. Provide the nickname for your certificate and select **http listener**.

![Certificate Details](image)

20. Verify the certificate details and click **Finish**.

![Review Details](image)
21. The following message displays, click **Close**.

![Install Server Certificate Wizard](image)

22. Go to the **Configuration** tab and click the configuration.

![Configuration Tab](image)
23. Go to the HTTP Listener tab and click listed listener. Select the Enabled check box for SSL and make sure that certificate that was installed in step 18 is listed as RSA Certificates. Click Apply.

24. Deployment pending message will get displayed. Click Deploy.
25. The message displays **The Configuration has been deployed successfully to all available nodes.**

   ![Configuration deployed successfully](image)

26. Once the SSL is enabled on the server open the browser and enter the URL that points the documents on an SSL-Enabled server:

   https://<ServerName or IP Address>:port

   If the SSL is enabled for the existing port number i.e., 80, type https://<ServerName or IP Address>:80

27. **Accept** the certificate.
Oracle iPlanet Web Server 6.1 with SafeNet Luna HSM

To configure the Web Server to recognize the SafeNet Luna HSM cryptographic device, perform the following steps:

1. Add the following in the LD_LIBRARY_PATH:
   ```bash
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<Path to Luna SA installation directory>/lib:<Path to Web Server installation directory>/bin/https/lib
   ```

2. Change to the alias directory of the Web Server by using the command:
   ```bash
   cd <Path to Web Server installation directory>/alias
   ```
   Where the `<Path to Web Server installation directory>` is root directory of the Web Server.
   
   List the contents of the alias directory to see if the file secmod.db exists. If the file does not exist, follow the steps below. If the file exists go to step 4.

3. Create a security module database by using the modutil utility as below:
   ```bash
   ../bin/https/admin/bin/modutil -create -nocertdb -dbdir .
   ```
   modutil displays the following warning:
   
   ![WARNING]
   Performing this operation while Communicator is running could cause corruption of your security databases. If Communicator is currently running, you should exit Communicator before continuing this operation. Type ‘q <enter>’ to abort, or <enter> to continue:
   
   Ensure that the web browser and communicator are not running and press Enter.

4. Disable the compliance with the FIPS 140-2 in the Web Server. To do this use the modutil utility as below:
   ```bash
   ../bin/https/admin/bin/modutil -fips false -nocertdb -dbdir .
   ```
   modutil displays the following warning:
   
   ![WARNING]
   Performing this operation while Communicator is running could cause corruption of your security databases. If Communicator is currently running, you should exit Communicator before continuing this operation. Type ‘q <enter>’ to abort, or <enter> to continue:
   
   Ensure that the web browser and communicator are not running and press Enter.

5. If FIPS mode has already been disabled, modutil displays the following message: (default)
   ```bash
   FIPS mode already disabled.
   ```
   Otherwise, modutil will display the following message:
   ```bash
   Using database directory...
   FIPS mode disabled.
   ```

6. Add the Luna SA PKCS #11 library to the security database by using the command:
   ```bash
   32-bit Library:
   ```
   ```bash
   ../bin/https/admin/bin/modutil -add lunasa -libfile /usr/lunasa/lib/libCryptoki2.so -nocertdb -dbdir .
   ```
64-bit Library:

```bash
../bin/https/admin/bin/modutil -add lunasa -libfile /usr/lunasa/lib/libCryptoki2_64.so -nocertdb -dbdir .
```

modutil displays the following warning:

```
WARNING: Performing this operation while Communicator is running could cause corruption of your security databases. If Communicator is currently running, you should exit Communicator before continuing this operation. Type ‘q <enter>’ to abort, or <enter> to continue:
Ensure that the web browser and communicator are not running and press Enter. The following message will be displayed:
Module "lunasa" added to database.
```

7. Ensure that the module has been added by executing the modutil utility as below:

```bash
../bin/https/admin/bin/modutil -list -nocertdb -dbdir .
```

<table>
<thead>
<tr>
<th>Listing of PKCS #11 Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. NSS Internal PKCS #11 Module</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>2. lunasa</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

8. Start the web server using the following command:

```bash
../startconsole
```

9. Open the browser with the following URL:

```
http://<ServerName or IP Address>:port
```

   If you have selected the default port then type `http://<ServerName or IP Address>:8888`

10. Enter the username and password to log in to the server with the administrator password provided during the installation of the web server.

11. Select the **web server**, click **Manage** and select the **Security tab**.
12. Click **Create Database** and provide the Database Password, click **OK**. The following message will be displayed, click **OK**:
   
   Success!
   Trust database has been successfully initialized.

13. Click **Apply** and then click **Apply Changes**, the following message will be displayed, click **OK**:
   
   Success!
   The server has started up.

14. Select **Request a Certificate** and enter the following details:
   
   - In the Cryptographic Module field, select Luna SA token.
   - In the **Key Pair File Password**, enter the Luna SA partition password.
   - Enter the details to generate certificate request.

15. Copy the certificate request and submit the request to CA, after receiving the response from CA save the response.

16. Select **Install Certificate** and enter the following details and click **OK**:
   
   - In the Cryptographic Module field, select Luna SA token.
   - In the **Key Pair File Password**, enter the Luna SA partition password.
   - Enter the **Certificate Name**.
   - Copy and paste the received CA response in the Message Text (with headers)

17. Verify the certificate details at the **Add Server Certificate** page and click **Add Server Certificate**, the following message will be displayed, click **OK**.
   
   Warning: Security Changes require Shutdown
   Although the certificate database has been updated, you must shutdown the server and start it up again to ensure that the changes take effect.

18. The following message will be displayed, click **OK**:
   
   Success
   Your certificate has been added
   You may now turn on encryption for your server
   Click **Apply** and **Apply Changes** to ensure that the changes take effect.

19. Select the **Administration Server** and click **Manage**.

20. Select **Preferences** tab and click **Edit Listen Sockets**.

21. Click **Listen Socket ID** and enter the Luna SA partition password and click **OK**.

22. Enter the details on the **Edit Listen Socket** page:
   
   - In the **Security** section, select security Enabled in the drop down list, click **OK** and click the **Apply**.
   - Select **Server Certificate Name** for the listen socket, select the certificate which you have installed and click **OK**.

23. Click **Apply** and **Apply Changes** to ensure that the changes take effect, it will ask password for listed Modules. Provide password and click **OK** to start the server.
Once the SSL enabled on the server open the browser and enter the URL that points the documents on an SSL-Enabled server:

https://<ServerName or IP Address>:port

If the SSL is enabled for the existing port number i.e., 80, type https://<ServerName or IP Address>:80

24. **Accept** the certificate.