Oracle iPlanet Web Server

Integration Guide

All information herein is either public information or is the property of and owned solely by Gemalto 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 publicly accessible 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.

Document Number: 007-012078-001, Rev. J

Release Date: May 2018

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

Preface

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

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

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)

Platforms Tested	SafeNet Luna Network HSM Appliance Version	Firmware Version	SafeNet Luna Client Software Version
Red Hat Enterprise Linux 7 64-bit	7.2.0	7.2.0	7.2.0
Red Hat Enterprise Linux 7 64-bit	7.1.0	7.1.0	7.1.0
Red Hat Enterprise Linux 7 64-bit	7.0.0	7.0.1	7.0.0

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

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

Platforms Tested	SafeNet Luna Network HSM Appliance Version	Firmware Version	SafeNet Luna Client Software Version
Red Hat Enterprise Linux 7 64-bit	6.3.0	6.27.0	6.3.0

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

Platforms Tested	HSM	Firmware	Luna Client Software Version
Red Hat Enterprise Linux 6.5 64-bit	6.2.2	6.24.3	6.2.2
Red Hat Enterprise Linux 6.5 64-bit	6.2.1	6.24.2	6.2.1

Platforms Tested	HSM	Firmware	Luna Client Software Version
Red Hat Enterprise Linux 6.5 64-bit	6.0.0	6.22.0	6.x (v6.0, 6.1)
Red Hat Enterprise Linux 6.5 64-bit	5.4.7	6.2.1	5.x (v5.0.x, 5.2.x, 5.3.x, 5.4.x)

Oracle iPlanet Web Server 6.1 SP14 SPARC (64bit)

Platforms Tested	HSM	Firmware	Luna Client Software Version
Solaris 10 SPARC (64-bit)	4.5	4.8.1	4.5.x

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=SA5_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-Auth) 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).

2
Oracle iPlanet Web Server Installation

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.

3

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 .

   [root@localhost config]# /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:
   ```

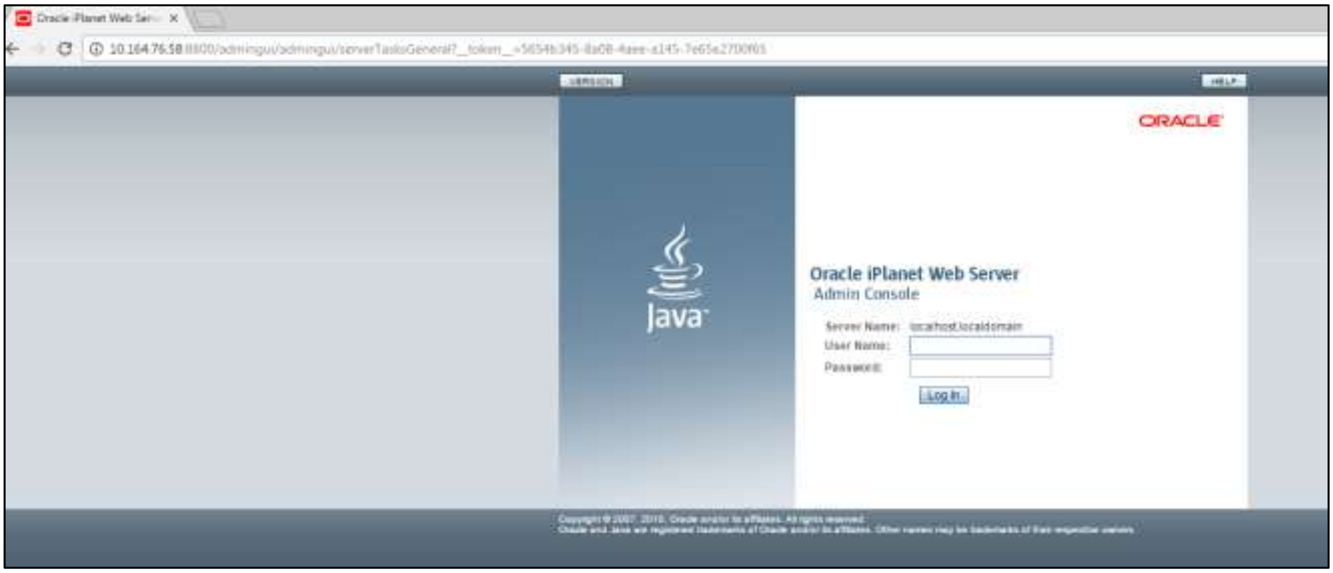
```
                slot: Luna UHD Slot
                token:

                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
```



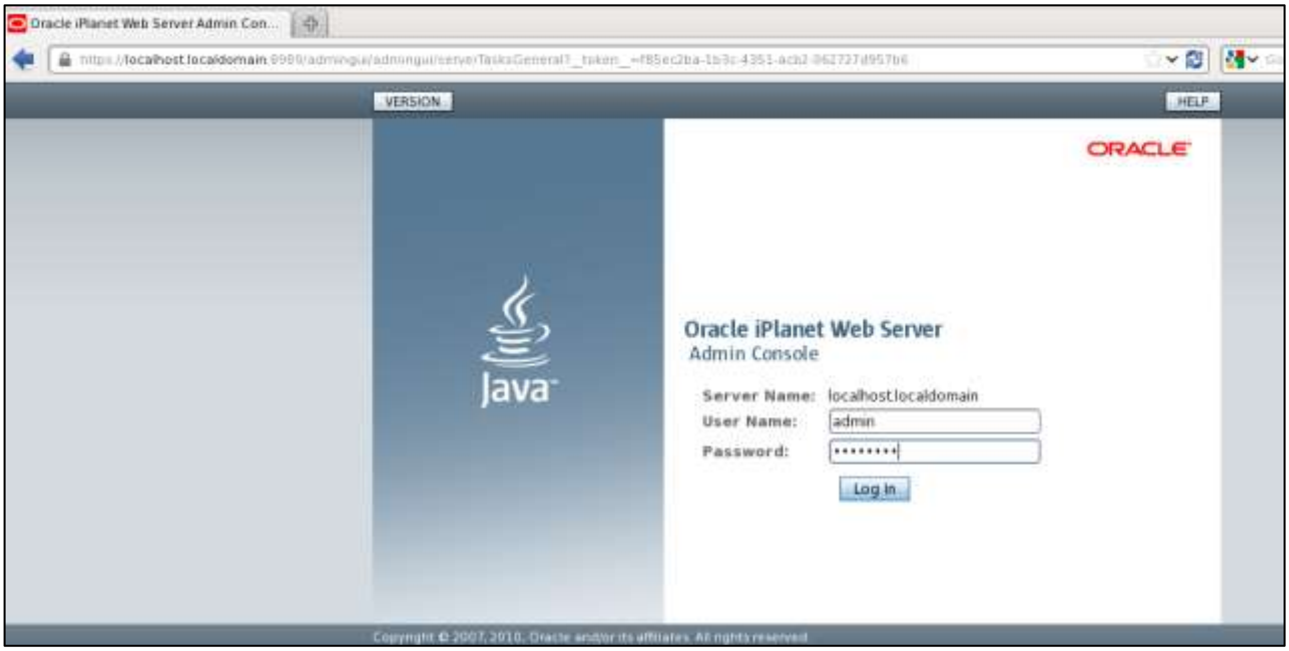
Oracle iPlanet Web Ser...
10.164.76.58:8800/admingui/admingui/serverTasksGeneral?__token__=5654b345-8a08-4aee-a145-7e65e2700f65
VERSION
HELP
ORACLE
Java
Oracle iPlanet Web Server
Admin Console
User Name:
Password:
Log In

Server Name: localhost.localdomain

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.



Oracle iPlanet Web Server
Admin Console

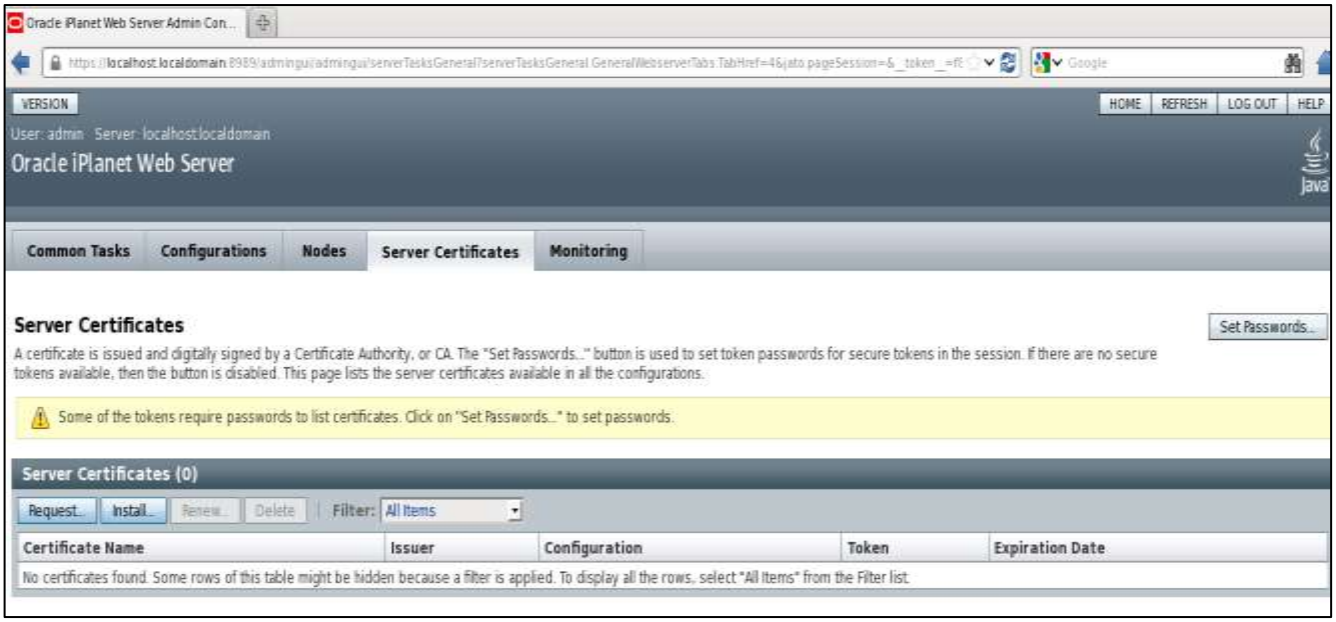
Server Name: localhost.localdomain
User Name: admin
Password: ••••••••

Copyright © 2007, 2010, Oracle and/or its affiliates. All rights reserved.

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 if it is pending.

12. Click **Server Certificates**.



User: admin Server: localhost.localdomain

Oracle iPlanet Web Server

Server Certificates

A certificate is issued and digitally signed by a Certificate Authority, or CA. The "Set Passwords..." button is used to set token passwords for secure tokens in the session. If there are no secure tokens available, then the button is disabled. This page lists the server certificates available in all the configurations.

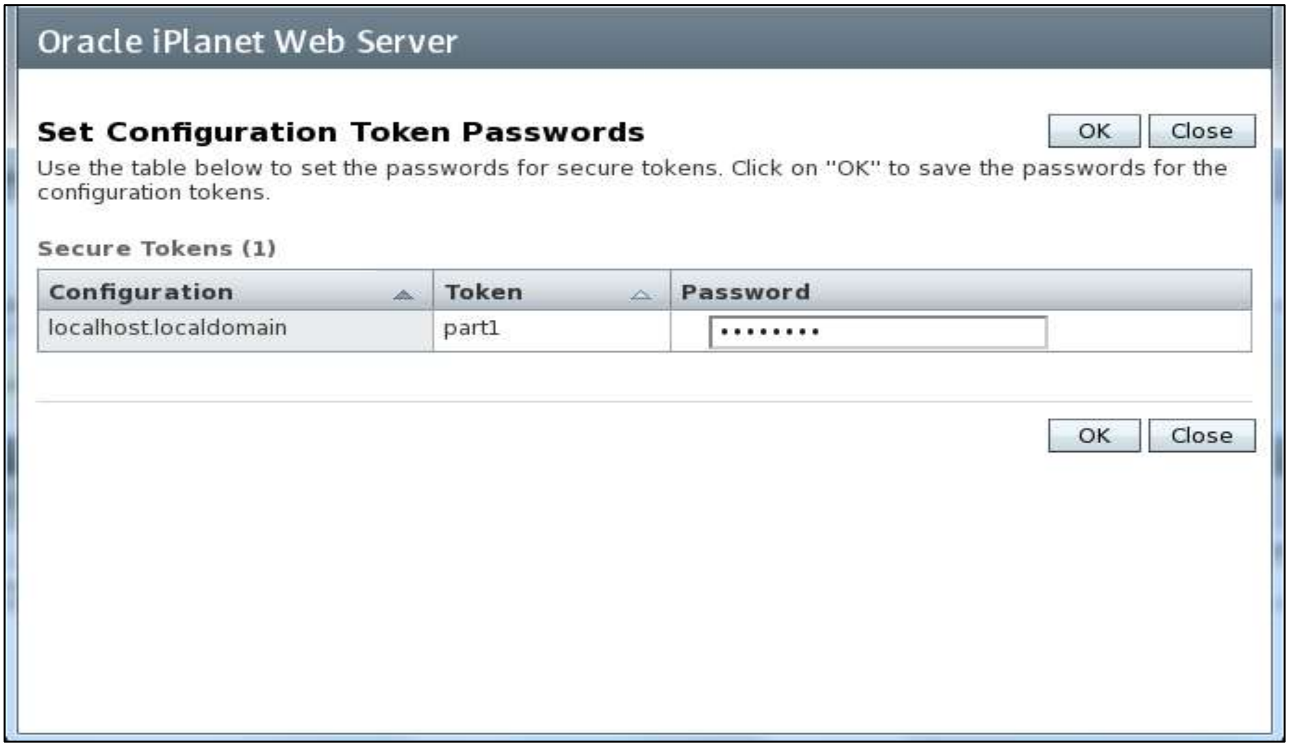
Some of the tokens require passwords to list certificates. Click on "Set Passwords..." to set passwords.

Server Certificates (0)

Filter: All Items

Certificate Name	Issuer	Configuration	Token	Expiration Date
No certificates found. Some rows of this table might be hidden because a filter is applied. To display all the rows, select "All Items" from the Filter list.				

13. Click **Set Password**. And provide Luna SA partition/token password. Click **OK**.



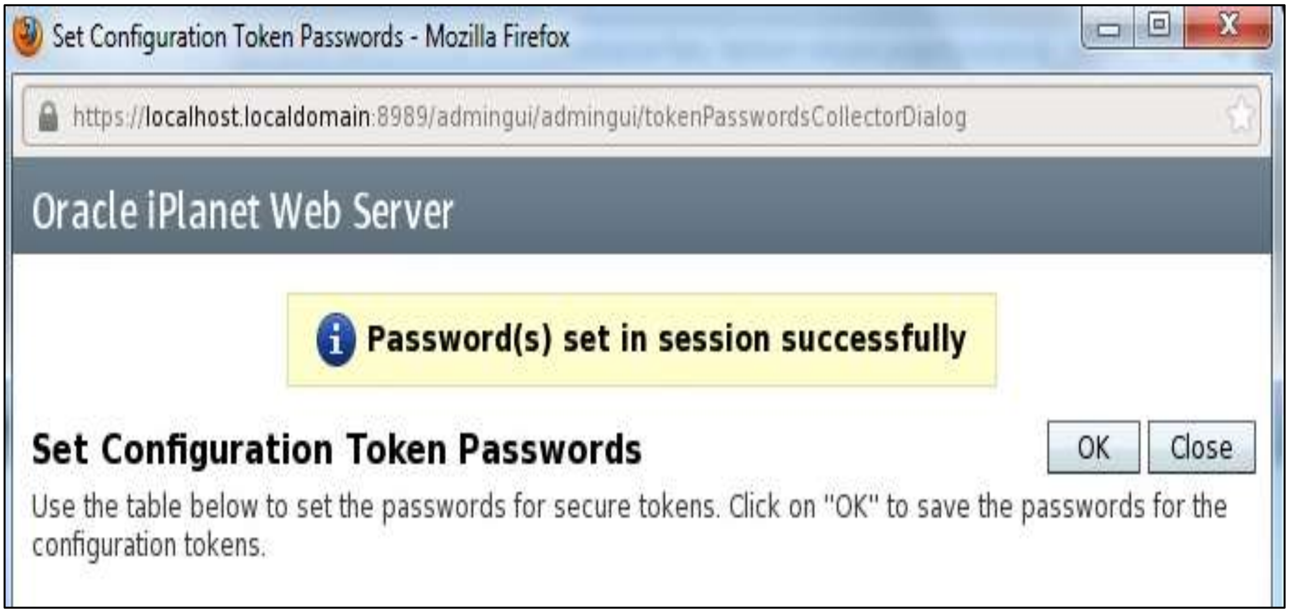
Oracle iPlanet Web Server

Set Configuration Token Passwords

Use the table below to set the passwords for secure tokens. Click on "OK" to save the passwords for the configuration tokens.

Secure Tokens (1)

Configuration	Token	Password
localhost.localdomain	part1	•••••••••



Set Configuration Token Passwords - Mozilla Firefox

https://localhost.localdomain:8989/admingui/admingui/tokenPasswordsCollectorDialog

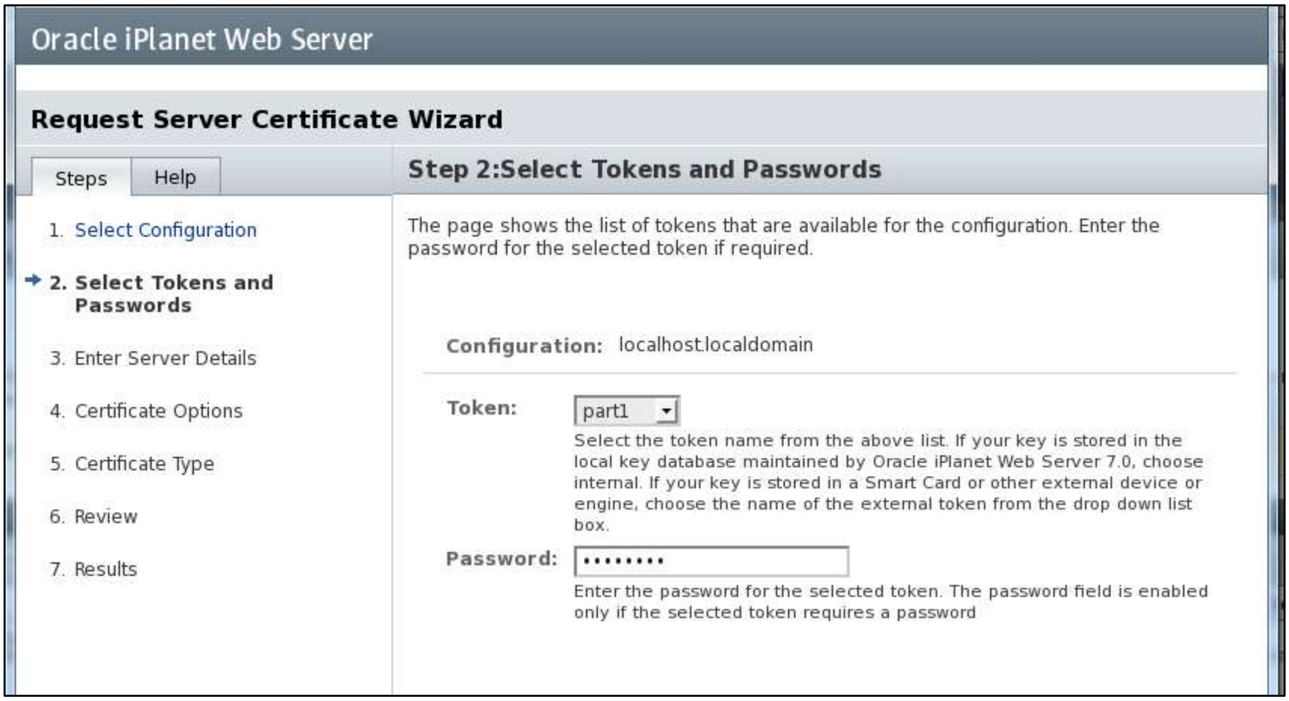
Oracle iPlanet Web Server

Password(s) set in session successfully

Set Configuration Token Passwords

Use the table below to set the passwords for secure tokens. Click on "OK" to save the passwords for the configuration tokens.

14. On **Server Certificate** tab click **Request…** and follow the wizard. At step 2 select Luna HSM token, provide password and click **Next**.



Oracle iPlanet Web Server

Request Server Certificate Wizard

1. Select Configuration
2. **Select Tokens and Passwords**
3. Enter Server Details
4. Certificate Options
5. Certificate Type
6. Review
7. Results

Step 2:Select Tokens and Passwords

The page shows the list of tokens that are available for the configuration. Enter the password for the selected token if required.

Configuration: localhost.localdomain

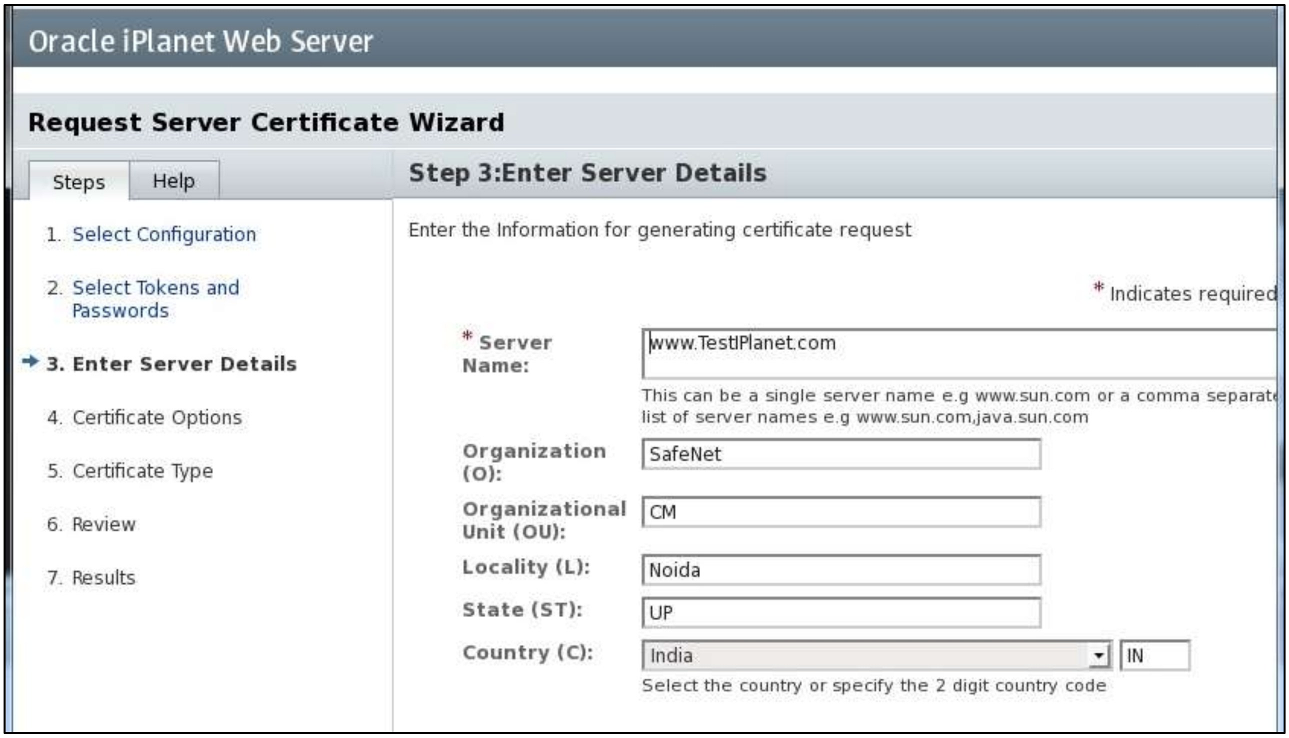
Token: part1

Select the token name from the above list. If your key is stored in the local key database maintained by Oracle iPlanet Web Server 7.0, choose internal. If your key is stored in a Smart Card or other external device or engine, choose the name of the external token from the drop down list box.

Password: ••••••••

Enter the password for the selected token. The password field is enabled only if the selected token requires a password

15. On step 3 provide all information for certificate request. Click **Next.**



Oracle iPlanet Web Server

Request Server Certificate Wizard

1. Select Configuration
2. Select Tokens and Passwords
3. **Enter Server Details**
4. Certificate Options
5. Certificate Type
6. Review
7. Results

Step 3:Enter Server Details

Enter the Information for generating certificate request

* Indicates required

* **Server Name:** www.TestPlanet.com

This can be a single server name e.g www.sun.com or a comma separat list of server names e.g www.sun.com,java.sun.com

Organization (O): SafeNet

Organizational Unit (OU): CM

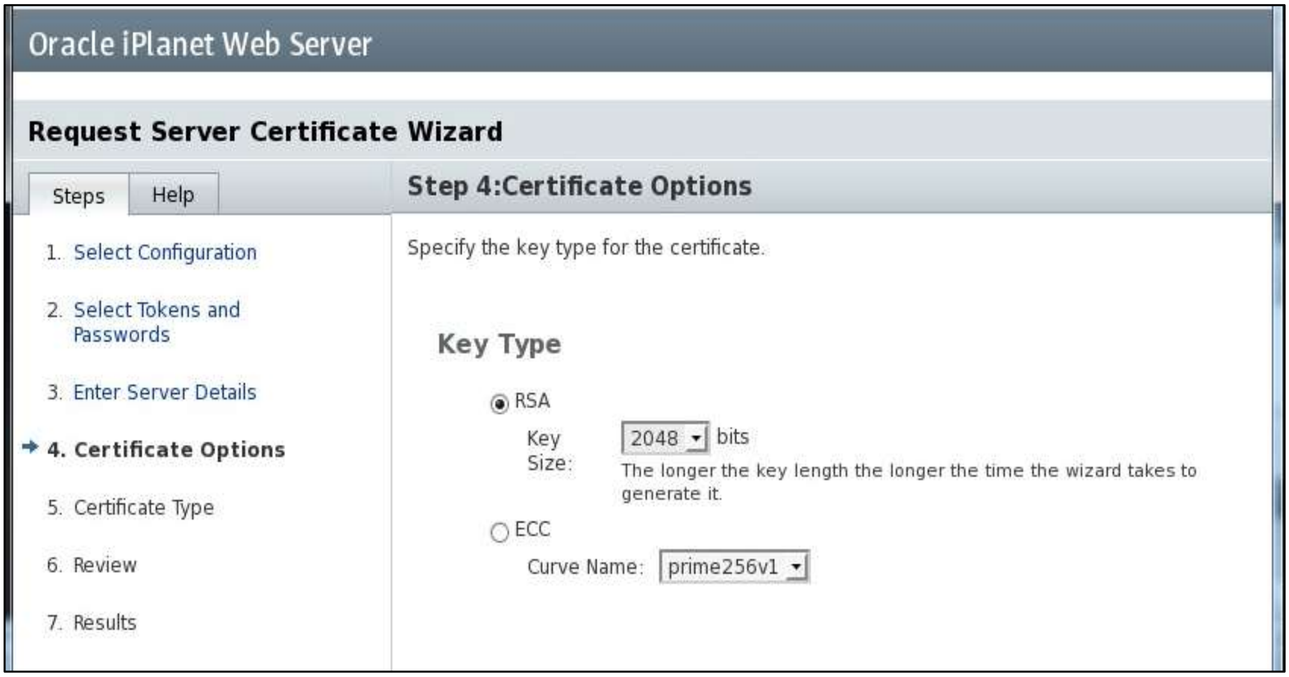
Locality (L): Noida

State (ST): UP

Country (C): India IN

Select the country or specify the 2 digit country code

16. Provide Key Type details in the step 4.



Request Server Certificate Wizard

1. Select Configuration
2. Select Tokens and Passwords
3. Enter Server Details
4. Certificate Options
5. Certificate Type
6. Review
7. Results

Step 4:Certificate Options

Specify the key type for the certificate.

Key Type

● RSA

Key Size: 2048 bits

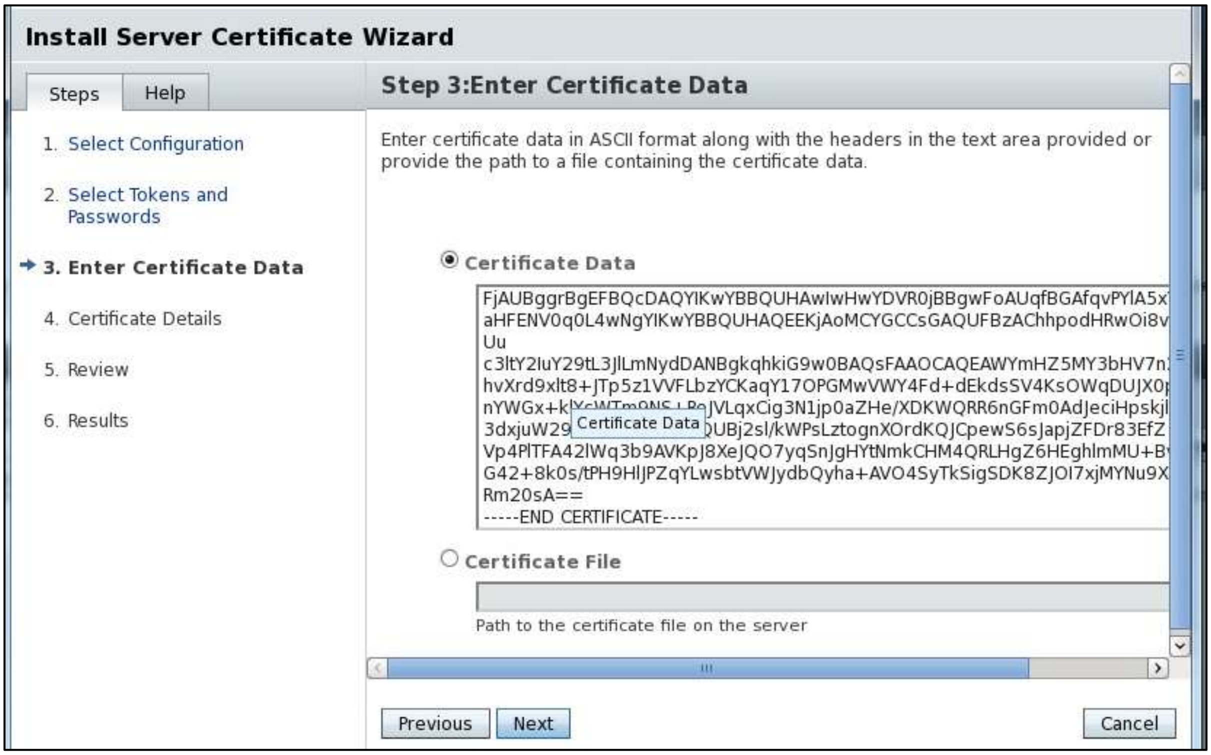
The longer the key length the longer the time the wizard takes to generate it.

○ ECC

Curve Name: prime256v1

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**.



Install Server Certificate Wizard

1. Select Configuration
2. Select Tokens and Passwords
3. Enter Certificate Data
4. Certificate Details
5. Review
6. Results

Step 3:Enter Certificate Data

Enter certificate data in ASCII format along with the headers in the text area provided or provide the path to a file containing the certificate data.

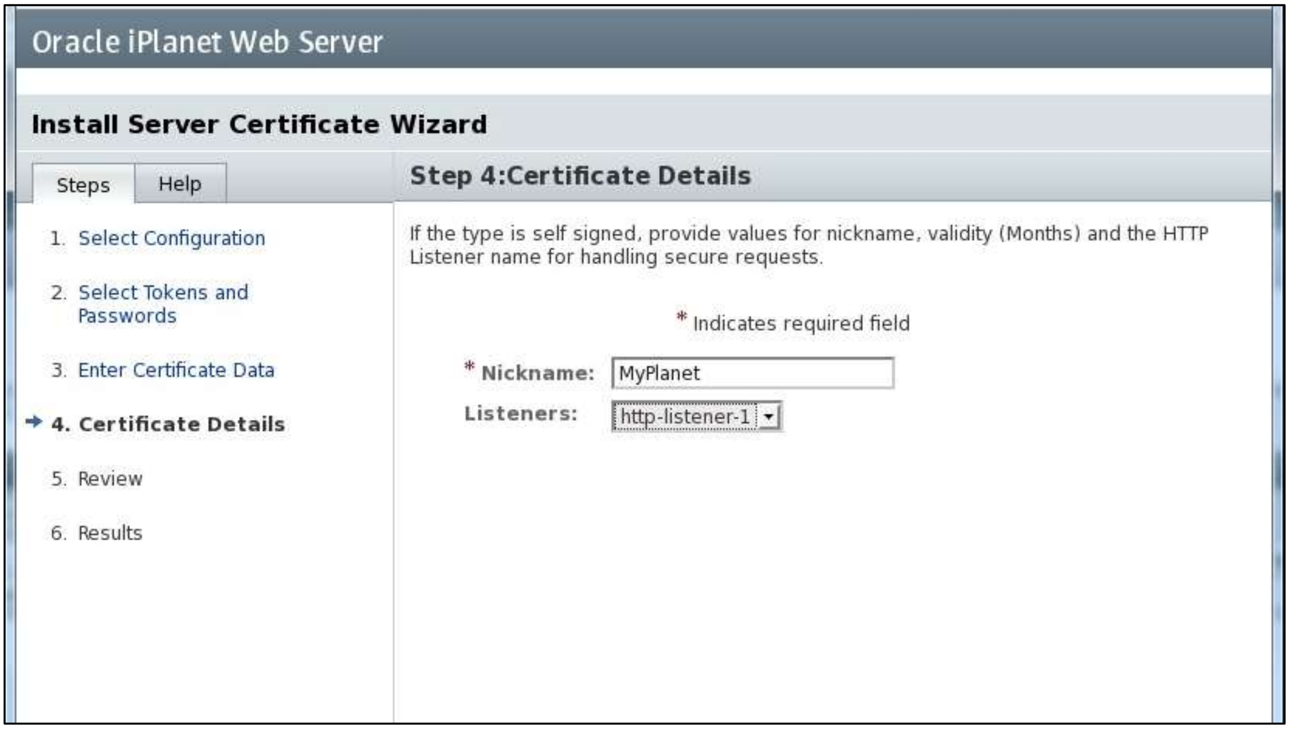
● Certificate Data

```
FjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYDVR0jBBgwFoAUqfBGAfqvPYlA5x
aHFENV0q0L4wNgYIKwYBBQUHAQEEKjAoMCYGCCsGAQUFBzAChhpodHRwOi8v
Uu
c3ltY2luY29tL3JlLmNydDANBgkqhkiG9w0BAQsFAAOCAQEAWYmHZ5MY3bHV7n
hvXrd9xlt8+JTp5z1VVFLbzYCKaqY17OPGMwVWY4Fd+dEkdsSV4KsOWqDUJX0
nYWGx+k            JVLqxCig3N1jp0aZHe/XDKWQRR6nGFm0AdJeciHpskjl
3dxjuW29            QUBj2sl/kWPsLztognXOrdKQJCpewS6sJapjZFDr83EfZ
Vp4PlTFA42lWq3b9AVKpJ8XeJQO7yqSnJgHYtNmkCHM4QRLHgZ6HEghlmMU+B
G42+8k0s/tPH9HlJPZqYLwsbtVWJydbQyha+AVO4SyTkSigSDK8ZJOI7xjMYNu9X
Rm20sA==
-----END CERTIFICATE-----
```

○ Certificate File

Path to the certificate file on the server

19. Provide the nickname for your certificate and select **http listener.**


Oracle iPlanet Web Server
Install Server Certificate Wizard
Steps
Help
1. Select Configuration
2. Select Tokens and Passwords
3. Enter Certificate Data
4. Certificate Details
5. Review
6. Results

Step 4:Certificate Details

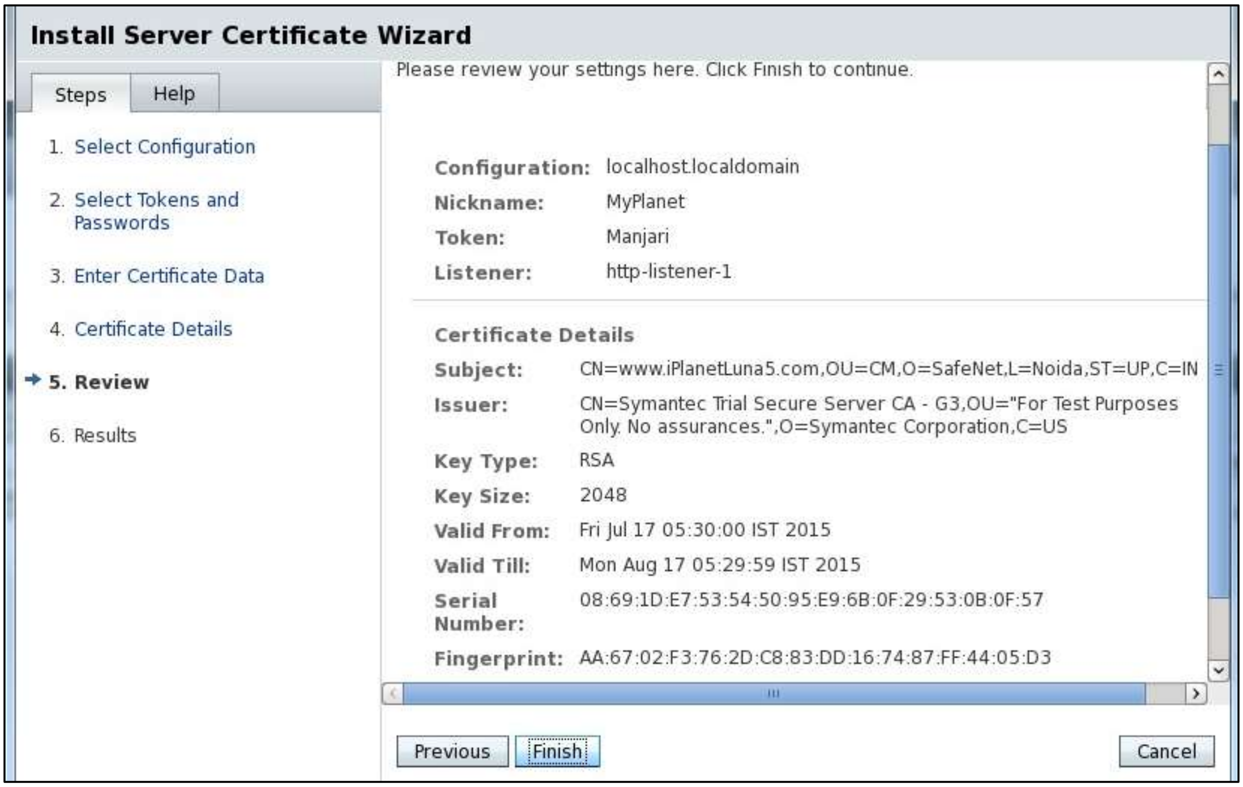
If the type is self signed, provide values for nickname, validity (Months) and the HTTP Listener name for handling secure requests.

* Indicates required field

* Nickname: MyPlanet

Listeners: http-listener-1

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



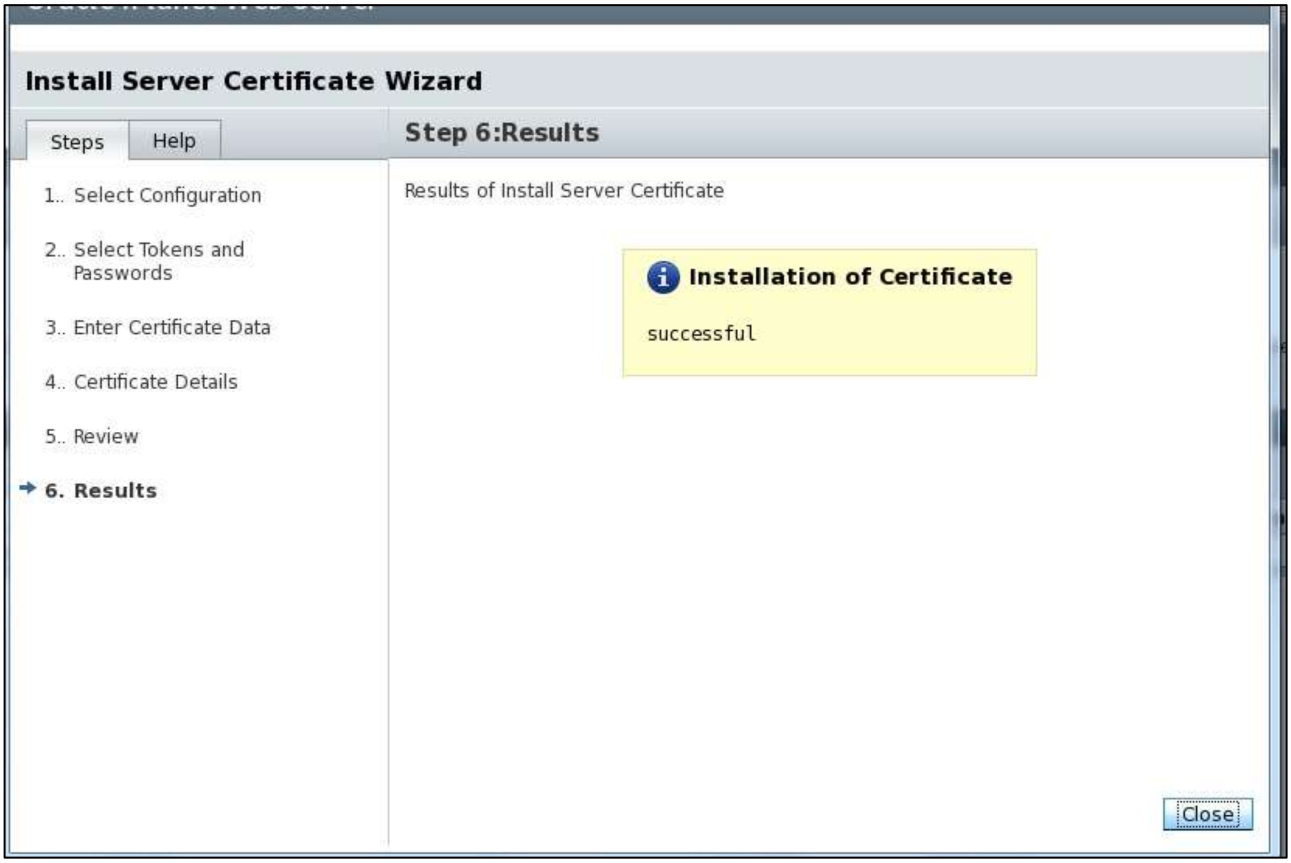
Please review your settings here. Click Finish to continue.

Configuration: localhost.localdomain
Nickname: MyPlanet
Token: Manjari
Listener: http-listener-1

Certificate Details

Subject: CN=www.iPlanetLuna5.com,OU=CM,O=SafeNet,L=Noida,ST=UP,C=IN
Issuer: CN=Symantec Trial Secure Server CA - G3,OU="For Test Purposes Only. No assurances.",O=Symantec Corporation,C=US
Key Type: RSA
Key Size: 2048
Valid From: Fri Jul 17 05:30:00 IST 2015
Valid Till: Mon Aug 17 05:29:59 IST 2015
Serial Number: 08:69:1D:E7:53:54:50:95:E9:6B:0F:29:53:0B:0F:57
Fingerprint: AA:67:02:F3:76:2D:C8:83:DD:16:74:87:FF:44:05:D3

21. The following message displays, click **Close**.



Install Server Certificate Wizard

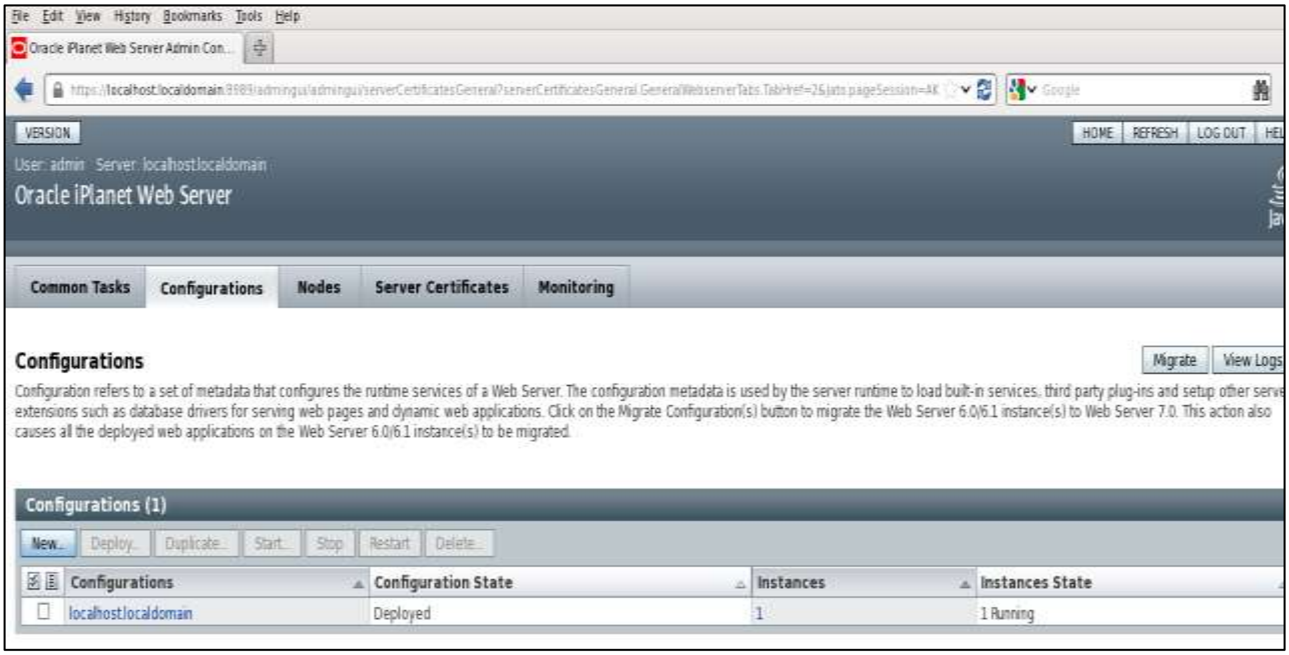
Step 6:Results

Results of Install Server Certificate

Installation of Certificate

successful

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



User: admin Server: localhost.localdomain

Oracle iPlanet Web Server

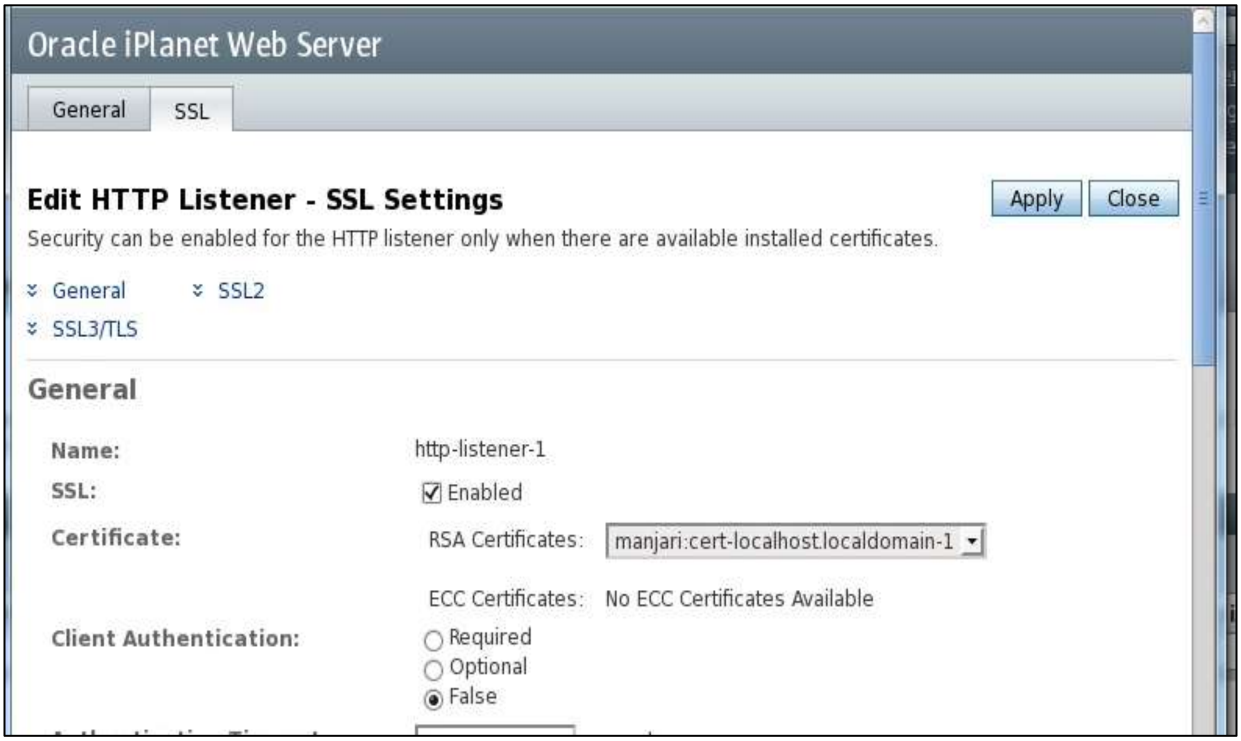
Configurations

Configuration refers to a set of metadata that configures the runtime services of a Web Server. The configuration metadata is used by the server runtime to load built-in services, third party plug-ins and setup other serve extensions such as database drivers for serving web pages and dynamic web applications. Click on the Migrate Configuration(s) button to migrate the Web Server 6.0/6.1 instance(s) to Web Server 7.0. This action also causes all the deployed web applications on the Web Server 6.0/6.1 instance(s) to be migrated.

Configurations (1)

	Configurations	Configuration State	Instances	Instances State
□	localhost.localdomain	Deployed	1	1 Running

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.**



Edit HTTP Listener - SSL Settings

Security can be enabled for the HTTP listener only when there are available installed certificates.

General

Name: http-listener-1

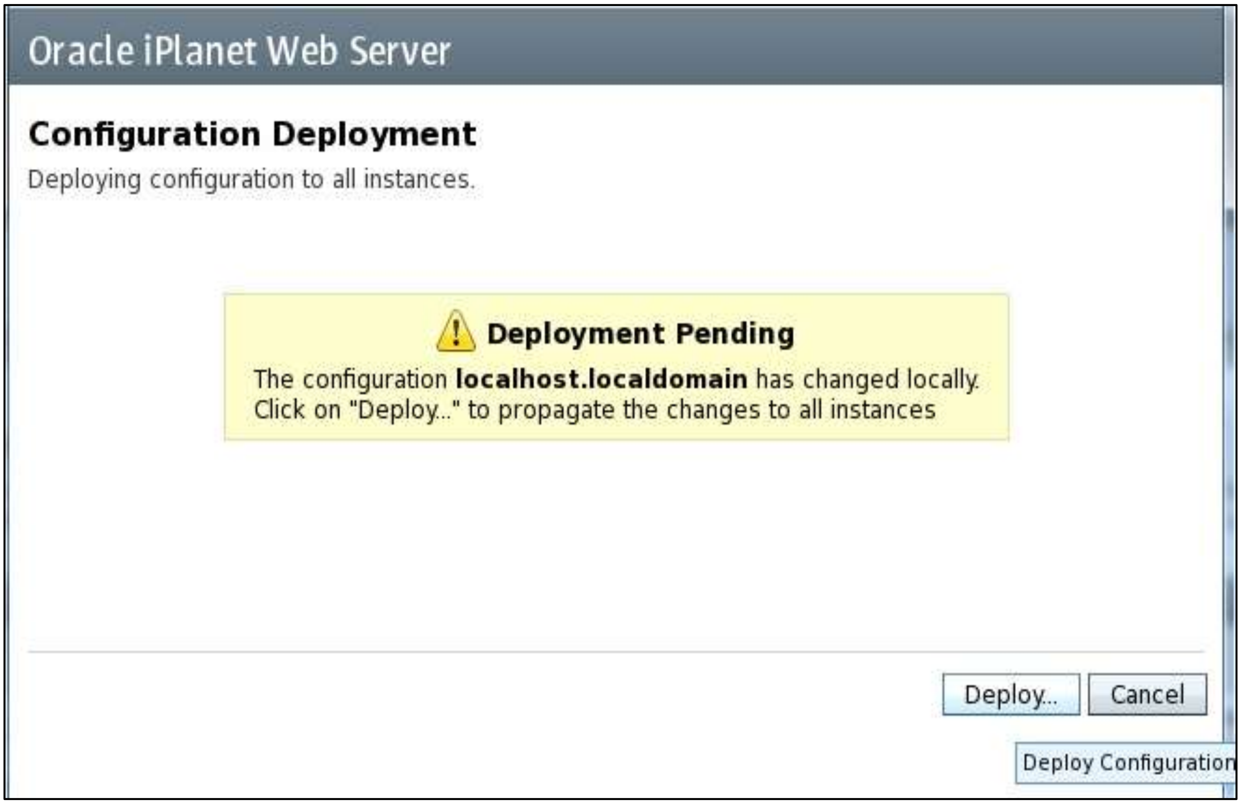
SSL: ☑ Enabled

Certificate: RSA Certificates: manjari:cert-localhost.localdomain-1

ECC Certificates: No ECC Certificates Available

Client Authentication: ○ Required ○ Optional ● False

24. Deployment pending message will get displayed. Click **Deploy**.



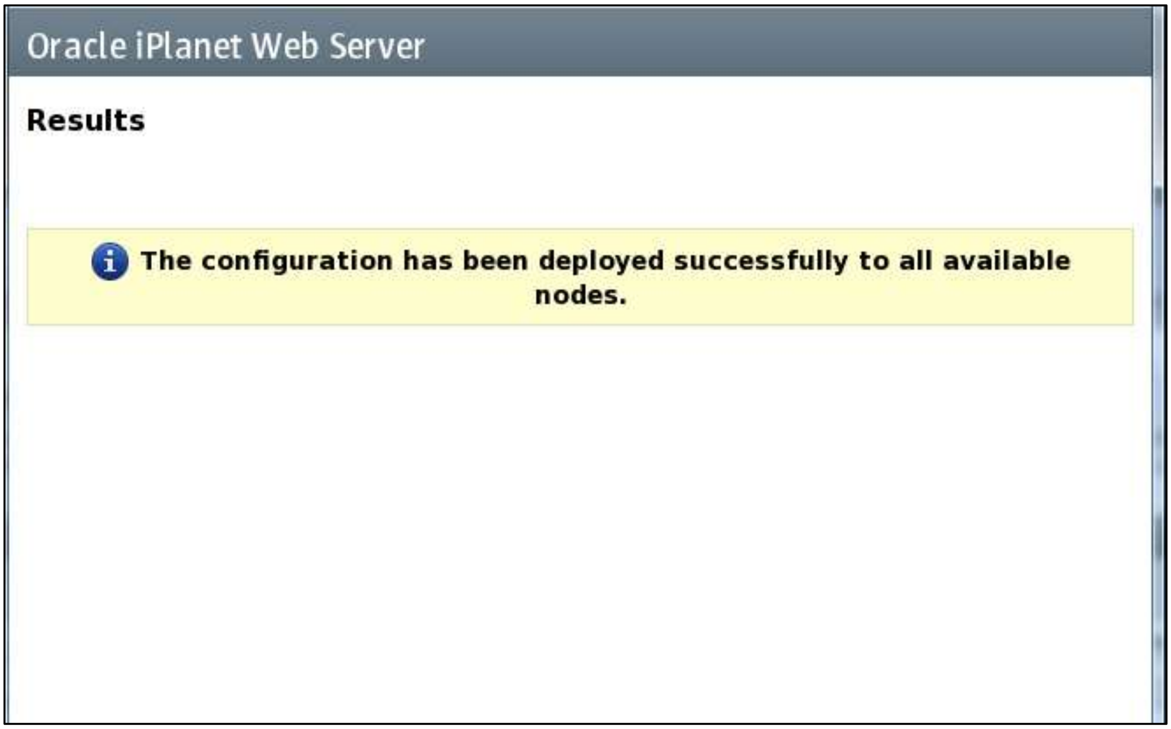
Configuration Deployment

Deploying configuration to all instances.

Deployment Pending

The configuration **localhost.localdomain** has changed locally. Click on "Deploy..." to propagate the changes to all instances

25. The message displays **The Configuration has been deployed successfully to all available nodes**.



Results

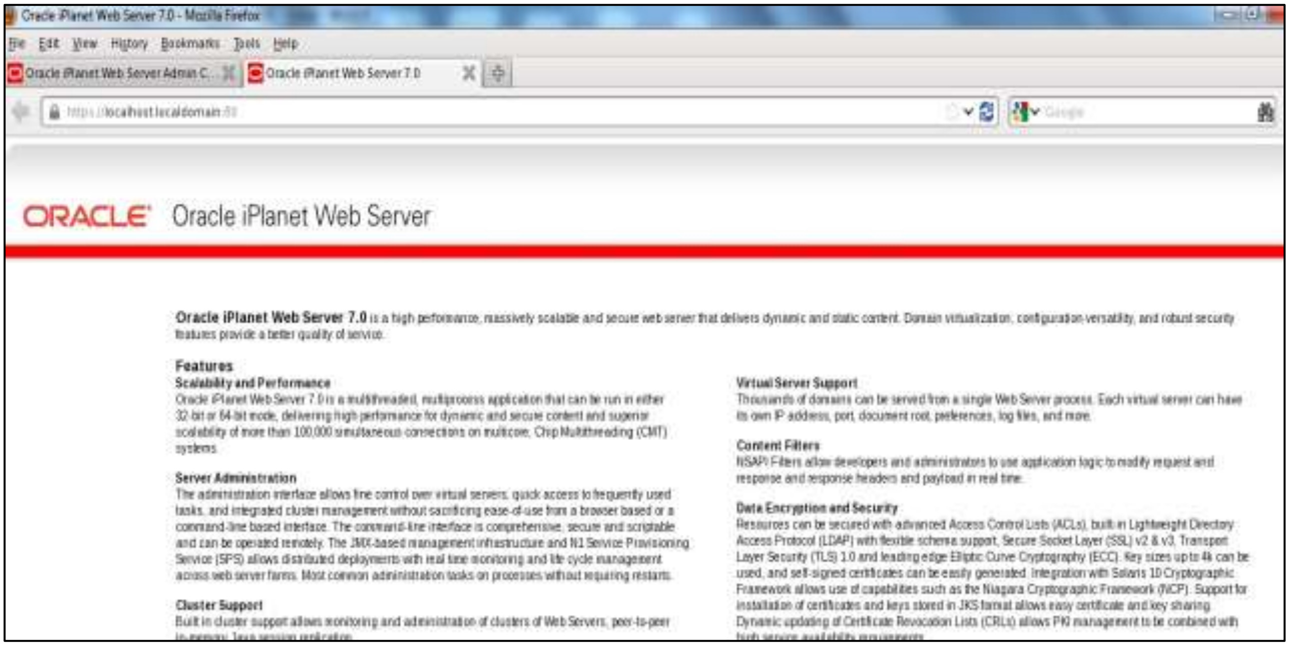
The configuration has been deployed successfully to all available nodes.

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 7.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Oracle iPlanet Web Server Admin C...
Oracle iPlanet Web Server 7.0
https://localhost.localdomain:80
Google
ORACLE
Oracle iPlanet Web Server

Oracle iPlanet Web Server 7.0 is a high performance, massively scalable and secure web server that delivers dynamic and static content. Domain virtualization, configuration versatility, and robust security features provide a better quality of service.

Features

Scalability and Performance
Oracle iPlanet Web Server 7.0 is a multithreaded, multiprocess application that can be run in either 32-bit or 64-bit mode, delivering high performance for dynamic and secure content and superior scalability of more than 100,000 simultaneous connections on multicore, Chip Multithreading (CMT) systems.

Server Administration
The administration interface allows fine control over virtual servers, quick access to frequently used tasks, and integrated cluster management without sacrificing ease-of-use from a browser based or a command-line based interface. The command-line interface is comprehensive, secure and scriptable and can be operated remotely. The JMX-based management infrastructure and N1 Service Provisioning Service (SPS) allows distributed deployments with real time monitoring and life cycle management across web server farms. Most common administration tasks on processes without requiring restarts.

Cluster Support
Built in cluster support allows monitoring and administration of clusters of Web Servers, peer-to-peer in-memory Java session replication

Virtual Server Support
Thousands of domains can be served from a single Web Server process. Each virtual server can have its own IP address, port, document root, preferences, log files, and more.

Content Filters
NSAPI Filters allow developers and administrators to use application logic to modify request and response and response headers and payload in real time.

Data Encryption and Security
Resources can be secured with advanced Access Control Lists (ACLs), built-in Lightweight Directory Access Protocol (LDAP) with flexible schema support, Secure Socket Layer (SSL) v2 & v3, Transport Layer Security (TLS) 1.0 and leading edge Elliptic Curve Cryptography (ECC). Key sizes up to 4k can be used, and self-signed certificates can be easily generated. Integration with Solaris 10 Cryptographic Framework allows use of capabilities such as the Niagara Cryptographic Framework (NCP). Support for installation of certificates and keys stored in JKS format allows easy certificate and key sharing. Dynamic updating of Certificate Revocation Lists (CRLs) allows PKI management to be combined with high service availability requirements

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:

   ```
   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:

   ```
   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:

   ```
   ../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:

   ```
   ../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)

   ```
   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:

   32-bit Library:

   ```
   ../bin/https/admin/bin/modutil -add lunasa -libfile /usr/lunasa/lib/libCryptoki2.so -nocertdb -
   dbdir .
   ```

64-bit Library:

```
../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:

```
../bin/https/admin/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/lunasa/lib/libCryptoki2.so
         slots: 1 slot attached
        status: loaded

         slot: LunaNet Slot
        token: part1
-----------------------------------------------------------
```

8. Start the web server using the following command:

   `../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.