

Oracle Payment Interface

Hospitality Cruise Shipboard Property Management System Installation Guide



Release 20.4
F95686-01
June 2024

The Oracle logo, consisting of the word "ORACLE" in white, uppercase, sans-serif font, centered within a solid red square.

ORACLE®

Oracle Payment Interface Hospitality Cruise Shipboard Property Management System Installation Guide
Release 20.4

F95686-01

Copyright ©2020, 2024, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Contents	3
<hr/>	
Preface	4
<hr/>	
1 Pre-Installation	1-1
<hr/>	
Supported Database Types and Operating Systems	1-1
Downloading the OPI 20.4 Installer	1-1
2 Installing OPI 20.4	2-1
<hr/>	
3 Token Exchange Handling	3-1
<hr/>	
PSP Certificates	3-1
4 Financial Transaction Handling	4-1
<hr/>	
5 SPMS Configuration	5-1
<hr/>	
OHC OPI Web Service	5-1
OHC OPI Daemon Service Configuration	5-1
OHC OPI Manager	5-2

Preface

Purpose

This guide explains the setup required to configure and use Oracle Payment Interface (OPI) with Shipboard Property Management System (SPMS).

Audience

This document is intended to cover the steps required to setup OPI to handle the integration with Shipboard Property Management System.

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at the following URL:

<https://iccp.custhelp.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at

<http://docs.oracle.com/en/industries/hospitality/>

Table 1-1 Revision History

Date	Description
June 2024	<ul style="list-style-type: none">• Initial Publication

1

Pre-Installation

Consider the following guidelines before installing OPI with SPMS:

- SPMS Release 8.0.8 is the minimum release you can integrate with OPI (19.1, 20.1, and 20.2 versions onwards).
- SPMS Release 8.0.17 is the minimum release you can integrate with OPI 20.4 version.
- OPI 20.4 does not install a database. If you are performing a fresh install of OPI, a database must be installed first.
- From OPI 20.1, OPI no longer uses Java installed on the host system. Instead, OPI includes its own Java runtime environment. The OPI runtime folder includes Java Development Kit 11.0.8.
- OPI requires at least 6 GB of free disk space, 1024 MB Memory and you must install OPI using a System Administrator account.
- A database is still required to hold the OPI configuration and audit event data but must be installed separately before installing OPI.
- Root access to the database is required during the OPI installation, only to create a dedicated OPI database user, which can have a lower level of privilege than the Root user, and is used for OPI tasks once the installation is complete.

Supported Database Types and Operating Systems

See [Supported Database Types and Operating Systems](#) section in the OPI Installation and Reference guide for database and operating systems with Oracle Payment Interface Installer release 20.4.

Downloading the OPI 20.4 Installer

The OPI 20.4 Installer is available for download from Oracle Software Delivery Cloud, search by:

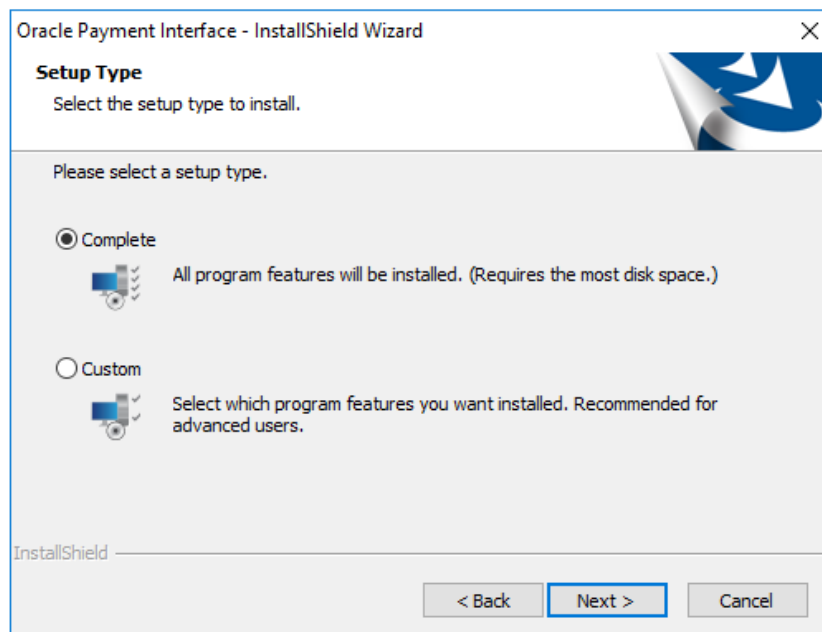
- **Release:** Oracle Payment Interface.
- **Select:** DLP: Oracle Payment Interface Without TPS 20.4
- During the installation of OPI, you must confirm the following:
 - Chain Code and Property Code.

- IP address of the OPI Server.
- Ensure you have the SQL root/Oracle user password for OPI database.

2

Installing OPI 20.4

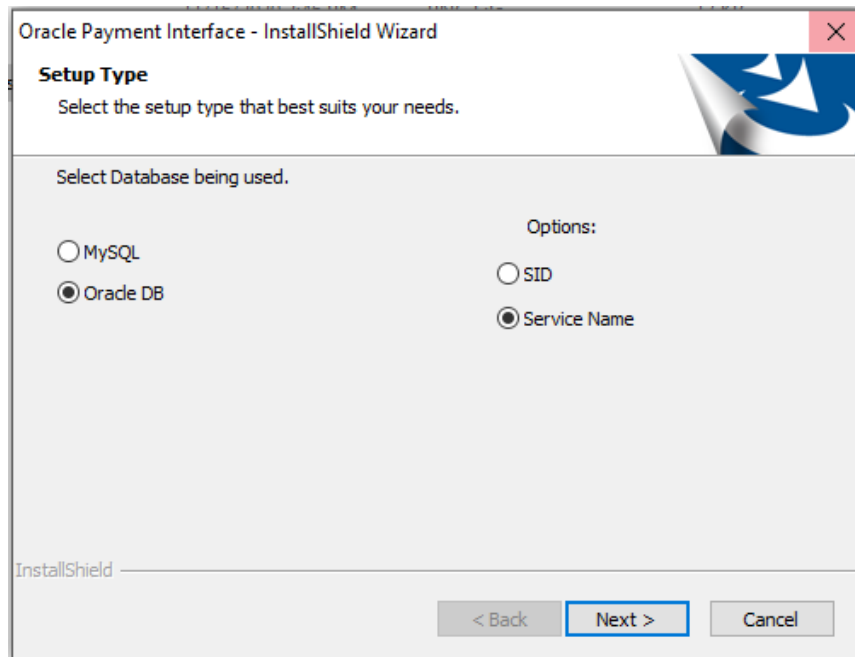
1. Copy the downloaded **OraclePaymentInterfaceInstaller_20.4.0.0**, to c:\temp folder.
2. Right-click and select **Run as Administrator** to launch the InstallShield.
3. Select your language preference, and then click **OK**.
4. Click **Next** on the Welcome to the InstallShield Wizard for Oracle Payment Interface window.
5. Click **Next** on the OPI Prerequisites window.



6. At the Setup Type window, select the **Complete** option to install all program features, and then click **Next**.
7. At the Choose a Destination Location window, accept the default installation location and then click **Next**.
8. Click **Install** on the Ready to Install the Program window.
9. At the Setup Type window, select the database type used and click **Next**.

 **NOTE:**

OPI does not install any database, so the database must already be installed.



10. Enter the relevant connection details for your database type. Details are provided by the individual who installed or configured the database software.

 **NOTE:**

OPI uses the string OPIDB as a tablespace name, so OPIDB should not be used in the installation path or service names/IDs of any of the databases. Otherwise, conflicts may occur and the installation is likely to fail.

Oracle DB

SID

- **Name/IP:** The Hostname or IP Address used for communication to the database.
- **Port #:** The Port number used for communication to the database.
- **SID:** The unique name that uniquely identifies the Oracle database.

Service Name

- **Name/IP:** The Hostname or IP Address used for communication to the database.
- **Port #:** The Port number used for communication to the database.
- **Service:** The TNS alias used to connect to the Oracle database.

11. Confirm the database admin user used to connect to the database. The database admin user is used to create an OPI database user, which is used once the installation completes.

12. On the Database User Credentials window, input the following and click **Next**.

- **User Name:** Create a new user.

- **Password:** Create a password.
- Confirm password

The screenshot shows a dialog box titled "Oracle Payment Interface - InstallShield Wizard" with a close button (X) in the top right corner. The main heading is "Database User Credentials". Below the heading is a blue graphic with a white arrow pointing right. The text inside the dialog reads: "Enter the user name and password to create a new database user account that will be used by the Oracle Payment Interface application. Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list only: !#\$%()*+,-./:;<=>?@[]_ '~". Below this text are three input fields: "User Name:" with a text box containing a vertical bar, "Password:" with a text box, and "Confirm Password:" with a text box. At the bottom left, it says "InstallShield". At the bottom right, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

13. Click **OK** on the Database connection successful dialog.
14. The system will configure the schema and may take some time before the next prompt. Do not close the window.
15. On the Database Configuration operation successful dialog, click **OK**.
16. On the Configuration Tool Super user Credentials window, enter the following information and click **Next**.
 - **User Name:** To Create the super user account to access OPI configuration tools
 - **Password:** Create a password.
 - Confirm the password

Oracle Payment Interface - InstallShield Wizard

Configuration Tool Super User Credentials

Enter the user name and password to create the Super User account for the configuration tool.
Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list only: !#\$%()*+,-./;<=>?@[]_`|~

User Name:

Password:

Confirm Password:

InstallShield

< Back **Next >** Cancel

17. Click **OK** on the 'Create Super User operation successful' dialog.
18. On the Configuration Tool Connection Settings window, enter the Host IP and click **Next**.
 - **Host:** You may leave this as 127.0.0.1 if the OPI configuration server is installed on this PC. Otherwise, specify the name or IP address of the PC where the OPI configuration server will be installed.
 - Leave the default **Port** as 8090.

Oracle Payment Interface - InstallShield Wizard

Configuration Tool Connection Settings

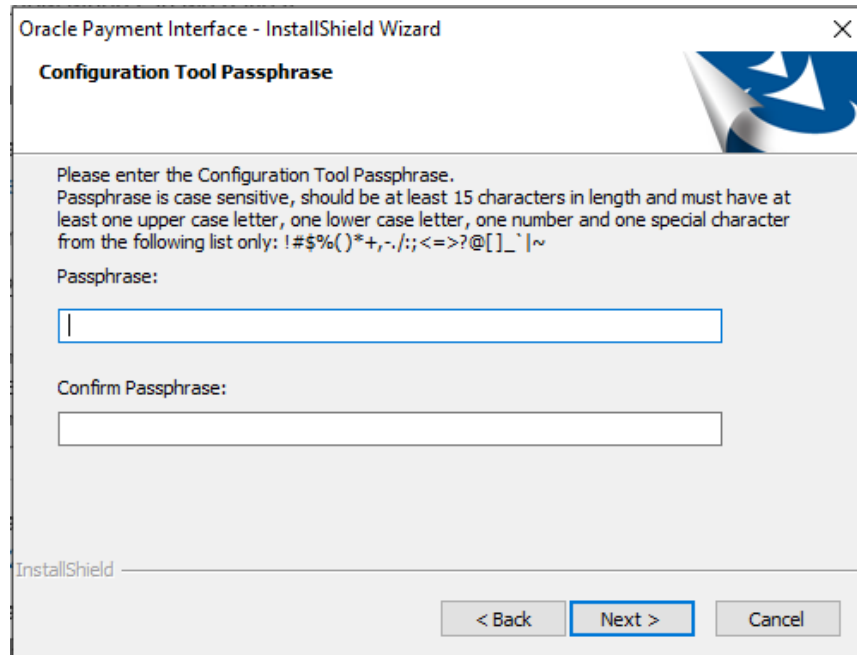
Please enter the Configuration Server Connection Information:
(ex. Host: 192.0.2.1 Port: 8090 / Host: example.com Port: 8090)

Host: Port:

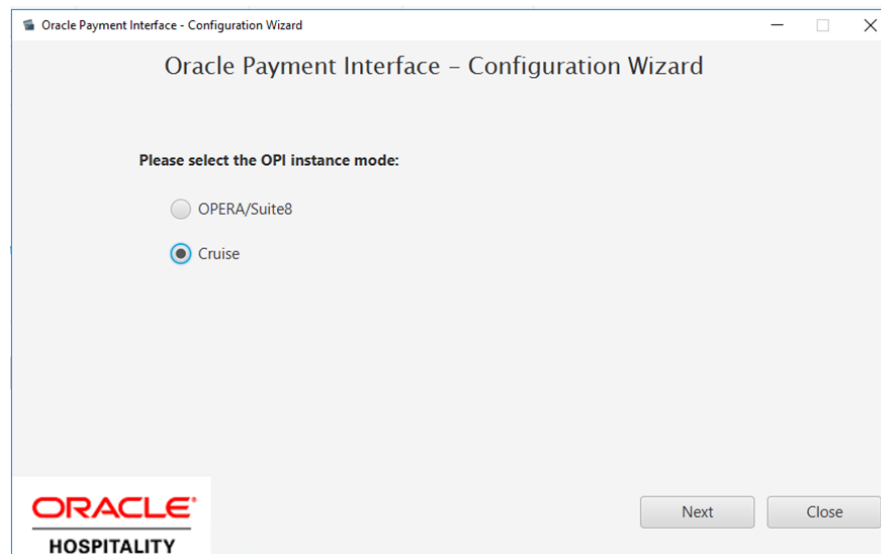
InstallShield

< Back **Next >** Cancel

19. On the Configuration Tool Passphrase window, enter the Passphrase and click **Next**.

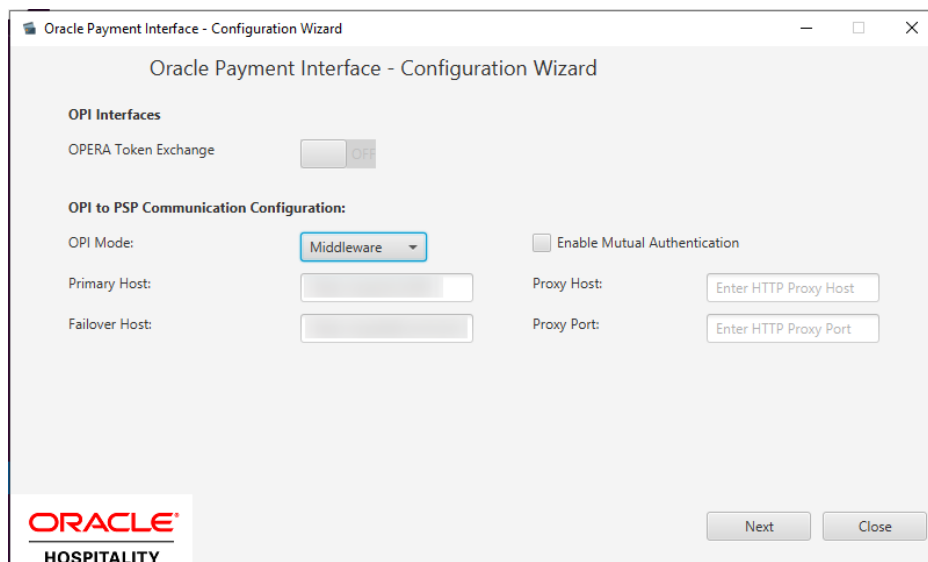


20. The following are the steps to configure OPI. At the Oracle Payment Interface – Configuration Wizard screen, choose **Cruise** and click **Next**.

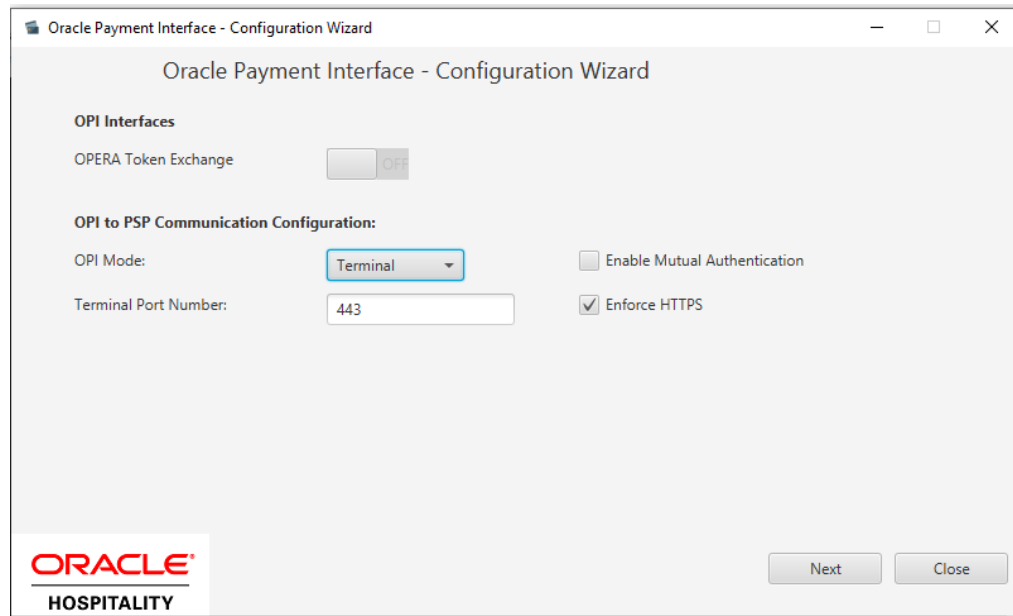


21. **Middleware Mode:** Choose Middleware as OPI Mode and fill in Primary host and Failover host under section **OPI to PSP communication configuration**.
- a. **Select OPI Mode:** Middleware
 - b. **Primary Host:** Specify the middleware server information.
 - c. **Failover Host:** Specify the failover middleware server information.
 - d. **Proxy Host:** The proxy host name or IP. If no proxy is needed, leave this field.
 - e. **Proxy Port:** The proxy port. If no proxy is needed, leave this field empty.

- f. **Enable Mutual Authentication:** Enable this option only if the PSP requests two-way authentication for financial transactions and has provided the certificates and passwords for it.



- 22. **Terminal Mode:** Choose **Terminal** as OPI Mode under section **OPI to PSP communication configuration**.
 - a. **Select OPI Mode:** Terminal
 - b. **Terminal Port Number:** This is the port number for PSP devices.
 - c. **Enable Mutual Authentication:** Enable this option only if the PSP requests two-way authentication for financial transactions and has provided the certificates and passwords for it.
 - d. **Enforce HTTPS:** This is enabled by default for all installations.



23. Click **Next**.
24. On the PMS Merchant window, click the blue **(+)** button and input the following, then click **Next**.
 - a. **Chain Code:** SPMS Chain code for the Merchant.
 - b. **Property Code:** SPMS Property code for the Merchant.
 - c. **Name:** Name of the Merchant.
 - d. **City:** City location of the Merchant.
 - e. **State or Province:** State or Province location of the Merchant.
 - f. **Country or Region:** Country location of the Merchant, this will indicate which currency it will operate when selected.
 - g. **IFC8 Key:** This key will be inserted into OHC OPI Daemon for validation between OPI with SPMS.
 - h. **IFC8 Host IP:** OHC OPI Daemon machines Hostname or IP Address.
 - i. **IFC8 Host Port:** OHC OPI Daemon port number.
 - j. **Currency:** The currency selection by the merchant in which the transactions are to be processed. Merchants can override selected transaction currency irrespective of country/region selection.
For example: If a merchant selects country as 'United States of America', then they can select the currency from the list of all available currencies (AUD, AED, AFN and so on) and this currency is used for transaction currency.

Oracle Payment Interface - Configuration Wizard

PMS Merchant

Chain Code:

Property Code: IFC8 Key:

Name: IFC8 Host IP:

City: IFC8 Host Port:

State/Province: Only Do Refund

Country/Region:

Currency:

ORACLE
HOSPITALITY

25. On the Merchant Payment Type Configuration window, the payment type accepted is shown. Click **Next** to proceed.

Oracle Payment Interface - Configuration Wizard

Merchant Payment Type Configuration

Chain Code:

Property Code:

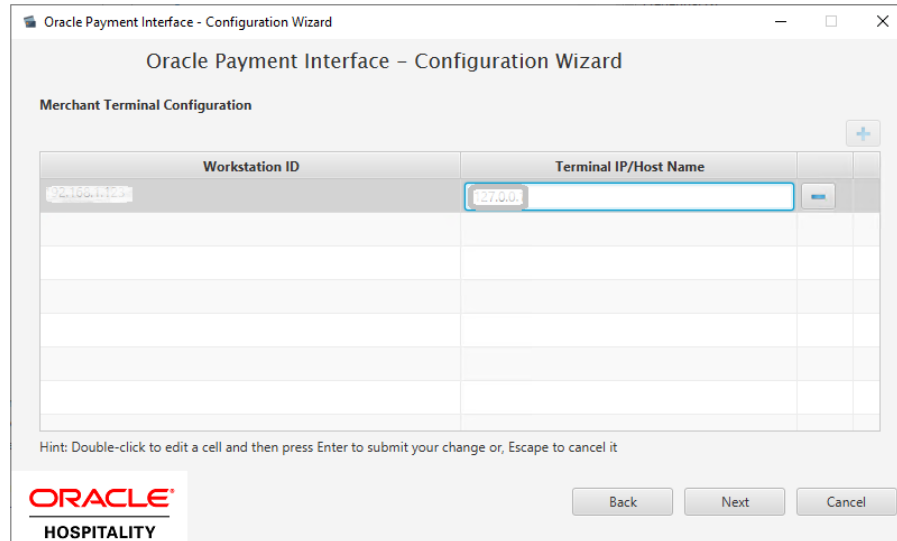
Payment Types:

Card Type	Payment Code
AliPay	AB
Alliance	AL
American Express	AX
Bank Card	LC
China UnionPay	CU
China UnionPay Debit	CD
Debit	DD
Debit Card	DE
Debit SMS	DL

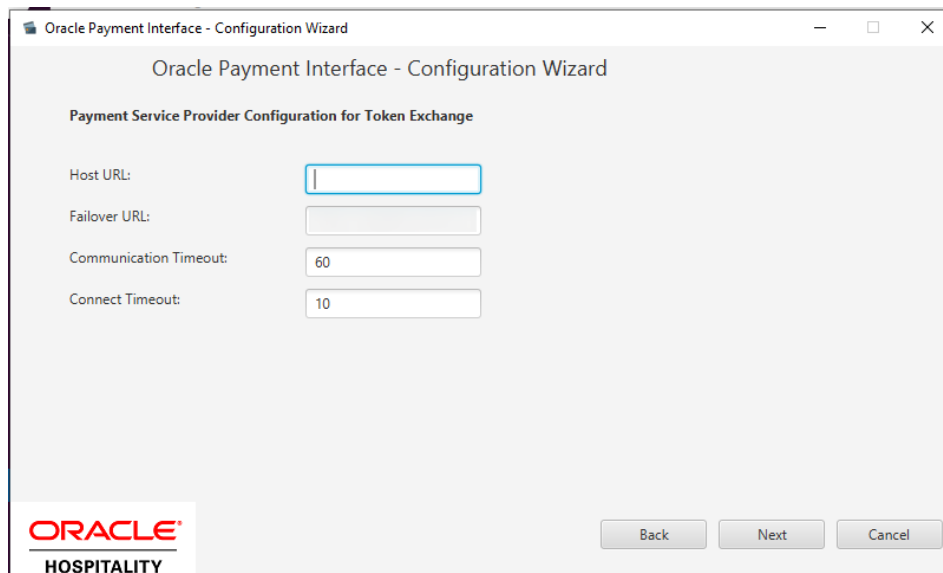
Hint: Double-click to edit a cell and then press Enter to submit your change or, Escape to cancel it

ORACLE
HOSPITALITY

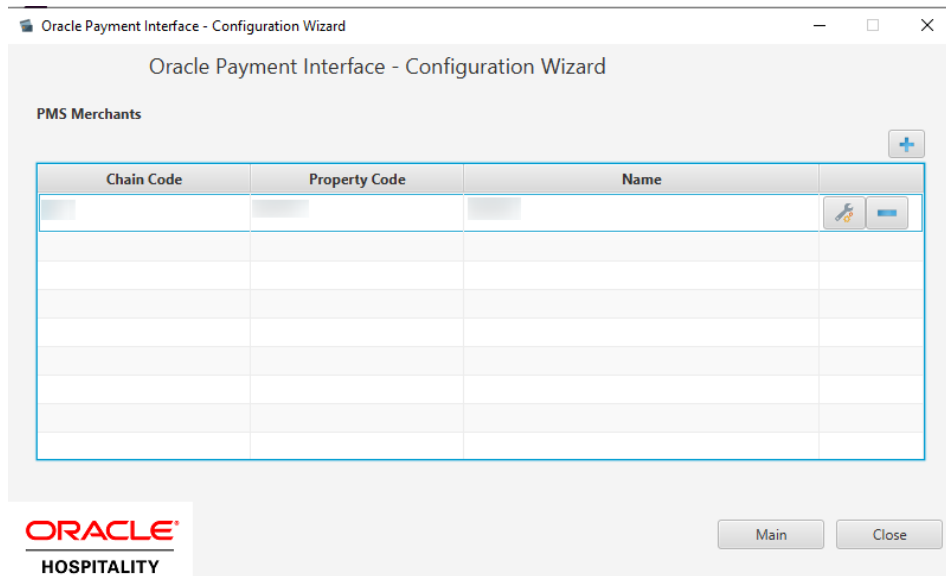
26. At the Merchant Terminal Configuration window, fill in the terminal details and click **Next**.
- Workstation ID:** IP address of the client with terminal connect to.
 - Terminal IP/ Host Name:** OHC OPI Daemon IP Address.



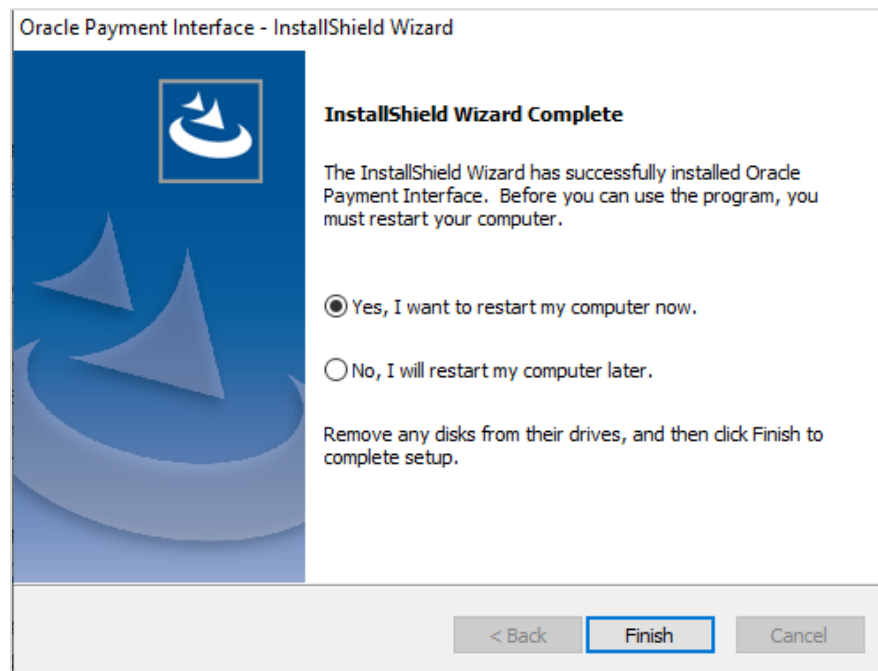
27. At the Payment Service Provider Configuration for Token Exchange window, fill in the details and click **Next**.
- Host URL:** Specify the middleware server information.
 - Failover URL:** Specify the failover middleware server information.
 - Communication Timeout:** Default to 60 seconds
 - Connect Timeout:** Default to 10 seconds



28. At the PMS Merchant window, verify that the PMS Merchant is created successfully.



29. Restart the machine when InstallShield Wizard complete.



NOTE:

The OPI installer saves detailed upgrade logs in the `OraclePaymentInterface_TempLogs` folder on the OPI drive. You can delete this folder if it is not needed.

3

Token Exchange Handling

This section describes the settings required for token exchange handling between OPI and PSP.

The Payment Service provider will need to provide the PSP root certificate and the client certificate.

PSP Certificates

The communication from OPI to the PSP for token exchange uses HTTPS with a client certificate for client authentication. That is, while a server-side certificate is expected to be deployed at PSP (server-side) for HTTPS communication, PSP is also expected to provide a client-side certificate to be deployed at OPI side. OPI will present this client certificate during HTTPS communication with PSP so that PSP can authenticate OPI properly.

To achieve this, the PSP is required to provide two files:

- A client-side certificate file: a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password. We expect the client certificate file provided by PSP to be in the format of .pfx or .jks.
- A root certificate file: a server-side certificate that is deployed at the PSP side. We expect the root certificate file provided by PSP to be in the format of .cer or .crt.

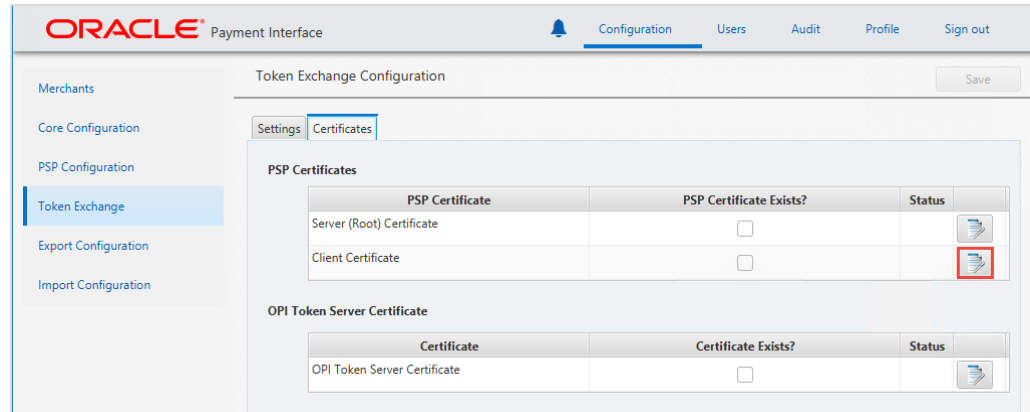
Handling the Client-Side Certificate


Certificates for Token Exchange

To import PSP Client certificates for token exchange:

You can import client certificates for Token exchange.

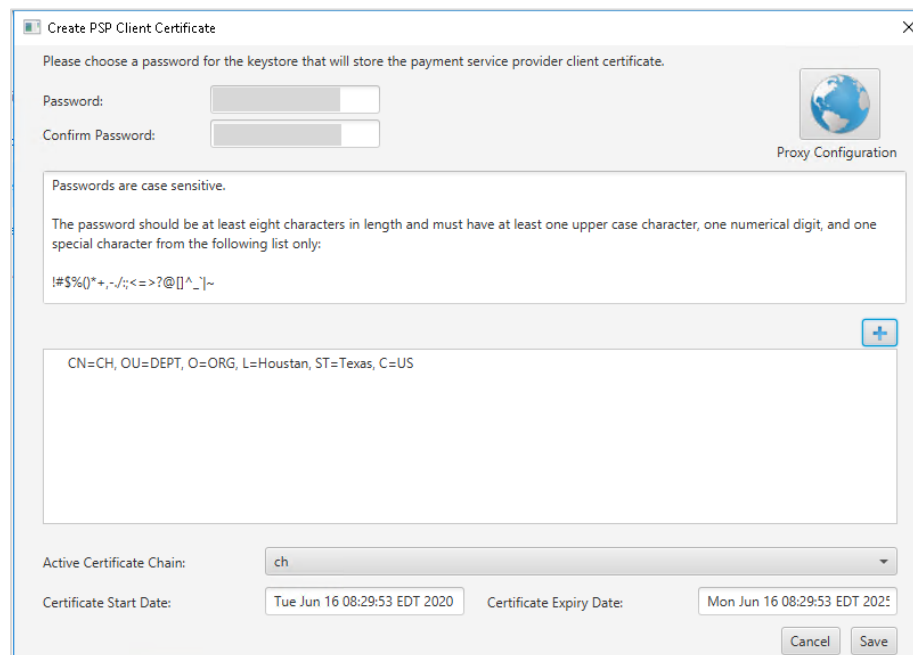
1. Log in to the OPI Configuration tool.
2. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Client Certificate**.



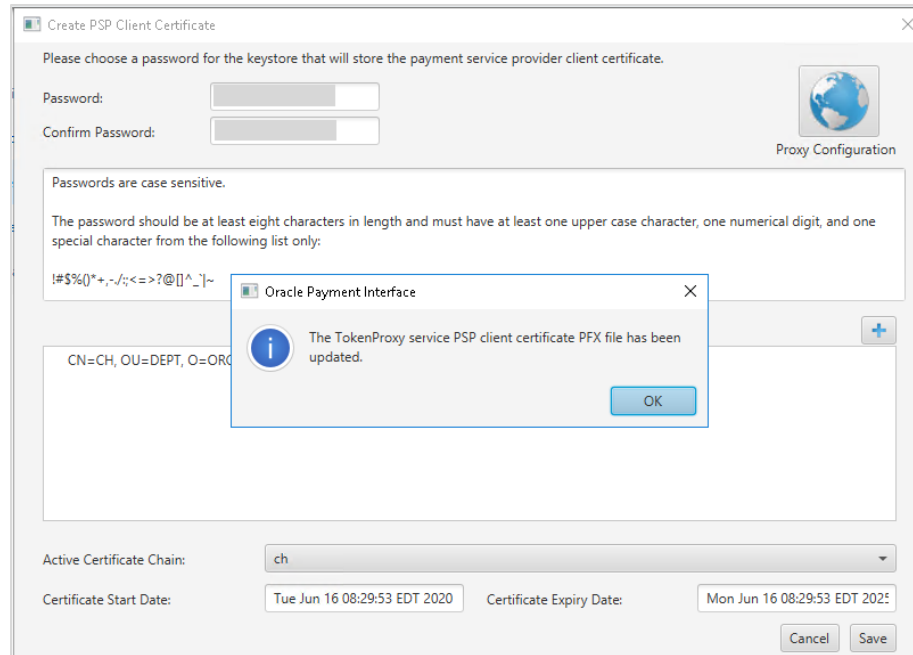
3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** () icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below or it will not be possible to enter the details to the OPI configuration.

 **NOTE:**

The PSP Client Side Certificates expiration date depends on what the PSP is set during the creation of the certificate. Check the expiration date in the properties of the certificate files. Be aware the PSP certificates must be updated before the expiration date to avoid downtime to the interface.



4. Click **Save**.



5. Click **OK**.

OPI_PSP_1.pfx is created under **\OraclePaymentInterface\v20.4\Services\OPI\key** folder.

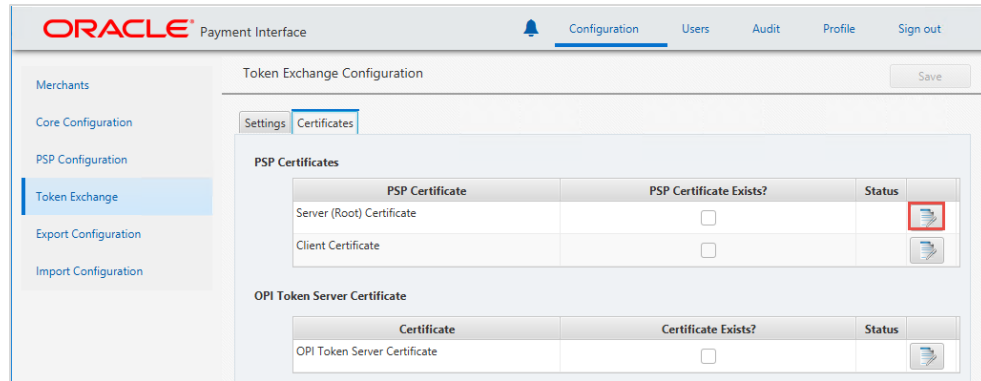
Handling the Root Certificate File


Certificates for Token Exchange

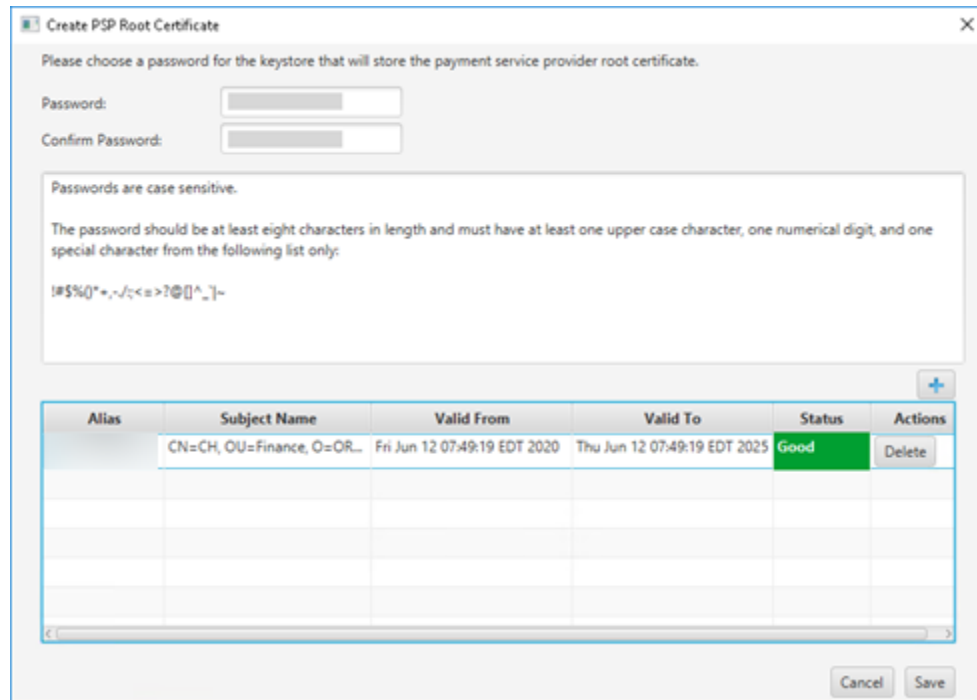
You can import certificates for Token exchange.

To import PSP Server (Root) certificates for token exchange:

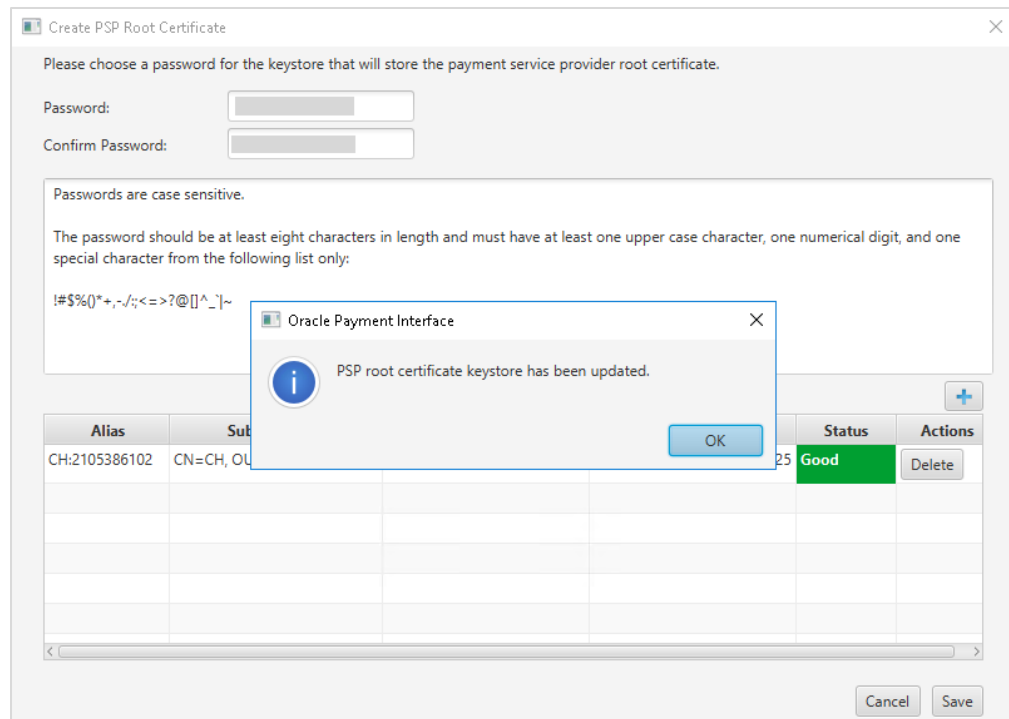
1. Log in to the OPI Configuration tool.
2. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Server (Root) Certificate**.



3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** () icon or you can also drag and drop the .cer or.crt.



4. Click **Save**.

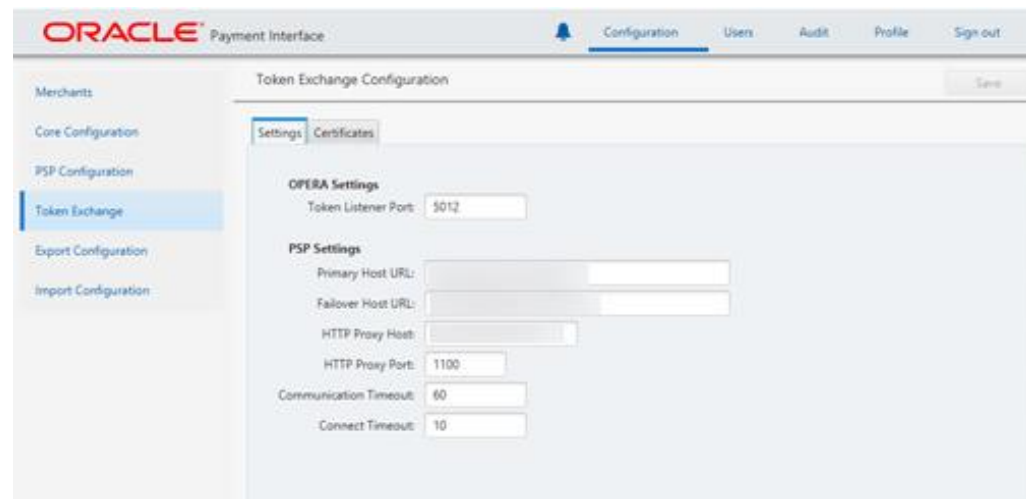


5. Click **OK**.

OPI_PSP_1Root is created under **\OraclePaymentInterface\v20.4\Services\OPI\key** folder.

Configuring Token Exchange

1. At OPI Configuration, go to **Token Exchange tab** and set below for SPMS uses:



- a. **Token Listener Port:** The listener port number for OPERA.
- b. **Primary Host URL:** The PSP Host URL for Token Exchange.

- c. **Failover Host URL:** The PSP Failover Host URL for Token Exchange. If a failover URL is not available, leave this blank.
 - d. **HTTP Proxy Host:** The proxy host name or IP. If no proxy is needed, leave this field empty.
 - e. **HTTP Proxy Port:** The proxy port. If no proxy is needed, leave this field empty.
 - f. **Communication Timeout:** The number of seconds OPI will wait for a response from the PSP Host or Terminal before timing out.
 - g. **Connect Timeout:** The number of seconds OPI will wait when initiating a connection to the PSP Host or Terminal before timing out.
2. Click **Save**.
 3. Restart the OPI Services.

4

Financial Transaction Handling

If Mutual Authentication is supported by the PSP and has been enabled within the OPI configuration, communication from OPI to the PSPs will require pair of private and public keys in a PKCS#12 – a .pfx file and a root certificate (both provided by the PSP).

- Server0Q.pfx: Used for client authentication of OPI to the PSP.
- Server0QRoot: Validates the public certificate(s) received from the PSPs.

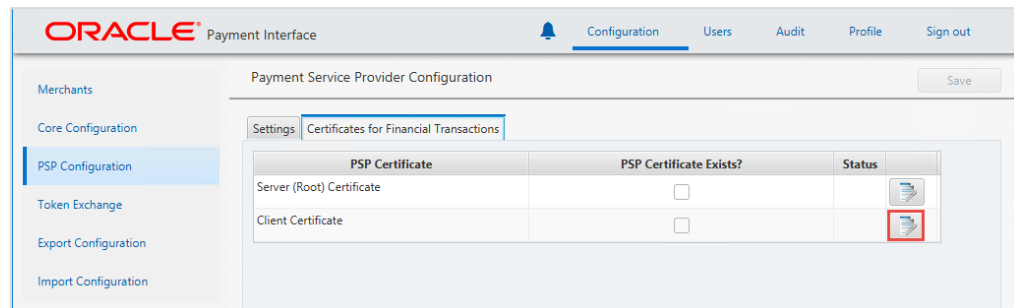
Handling the Client-Side Certificate


PSP Certificates for Financial Transaction

You can import client certificates for financial transactions.

To import PSP Client certificates for financial transactions:

1. Log in to the OPI Configuration tool.
2. Select **PSP Configuration** tab, click **Certificates for Financial Transactions** subtab and then edit the **Client Certificate**.



3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** () icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below or it will not be possible to enter the details to the OPI configuration.

NOTE:

The PSP Client Side Certificates expiration date depends on what the PSP is set during creation of the certificate. Check the expiration date in the properties of the certificate files. Be aware the PSP certificates must be updated prior to the expiration date to avoid downtime to the interface.

Create PSP Client Certificate for Financial Transactions

Please choose a password for the keystore that will store the payment service provider client certificates.

Password:

Confirm Password:

Proxy Configuration

Passwords are case sensitive.

The password should be at least eight characters in length and must have at least one upper case character, one numerical digit, and one special character from the following list only:

!#\$%()*+,-./:;<=>?@[^_`~

+

CN=CH, OU=Finance, O=ORG, L=Houston, ST=Texas, C=US

Active Certificate Chain: ch

Certificate Start Date: Fri Jun 12 07:49:19 EDT 2020

Certificate Expiry Date: Thu Jun 12 07:49:19 EDT 2025

Cancel Save

4. Click **Save**.

Create PSP Client Certificate for Financial Transactions

Please choose a password for the keystore that will store the payment service provider client certificates.

Password:

Confirm Password:

Proxy Configuration

Passwords are case sensitive.

The password should be at least eight characters in length and must have at least one upper case character, one numerical digit, and one special character from the following list only:

!#\$%()*+,-./:;<=>?@[^_`~

+

CN=CH, OU=Finance, O=ORG, L=Houston, ST=Texas, C=US

Active Certificate Chain: ch

Certificate Start Date: Fri Jun 12 07:49:19 EDT 2020

Certificate Expiry Date: Thu Jun 12 07:49:19 EDT 2025

Cancel Save

Oracle Payment Interface

The Financial Transaction's PSP client certificate PFX file has been updated.

OK

5. Click **OK**.

Server0Q.pfx is created under **\\OraclePaymentInterface\20.4\Services\OPI\key** folder.

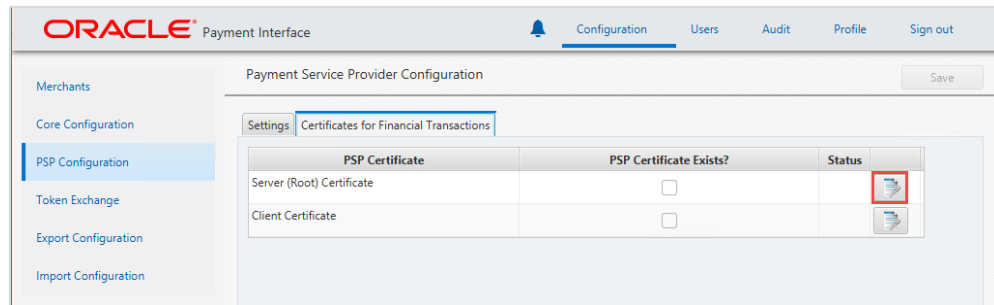
Handling the Root Certificate File


PSP Certificates for Financial Transaction

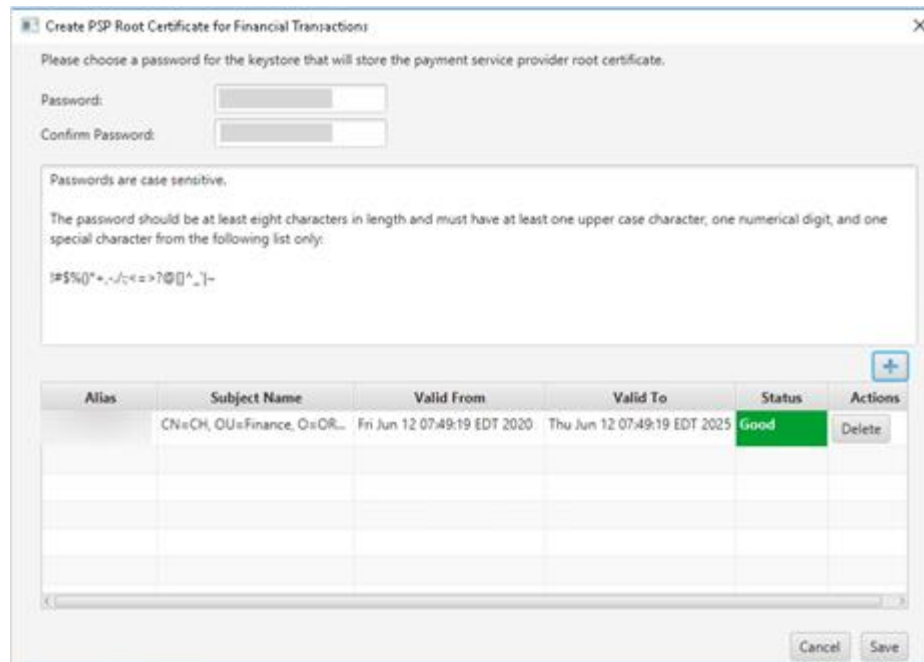
You can import server (root) certificates for financial transactions.

To import PSP Server (Root) certificates for financial transactions:

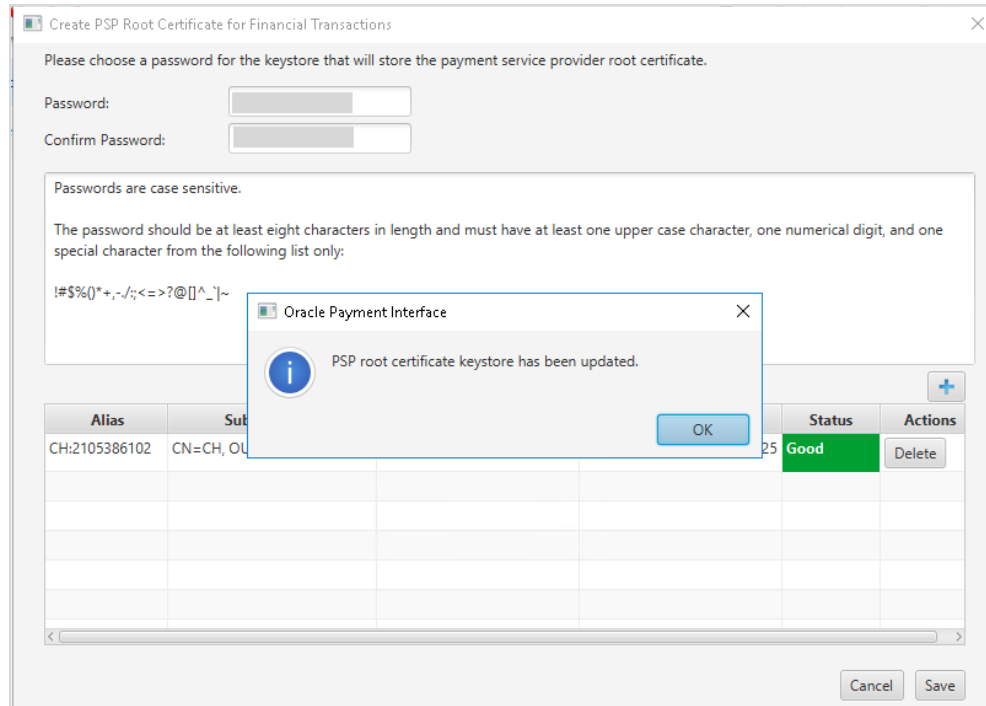
1. Log in to the OPI Configuration tool.
2. Select **PSP Configuration** tab, click **Certificates for Financial Transactions** subtab and then edit the **Server (Root) Certificate**.



3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** () icon or you can also drag and drop the .cer or.crt.



4. Click **Save**.



5. Click **OK**.

Server0QRoot is created under **\OraclePaymentInterface\20.4\Services\OPI\key**

5

SPMS Configuration

To enable the OPI Handling, login to the **Administration module**, go to **System Setup** menu, then **Database Parameters**, and set the Parameter value to “OPI” under ‘**Not Specified**’ group, **CC Transfer Format**.

OHC OPI Web Service

Refer to *SPMS Installation Guide Setting Up SPMS Web Server* section at [Oracle Help Center](#) for steps to install OHC OPI Web Services and OHC OPI Daemon Service.

NOTE:

If the SPMS Webserver is installed on a different machine, you need to copy the below two parameters into your `C:\Users\Public\Documents\Oracle Hospitality CruiseOHCSettings.par`, and ensure that there is a new line at the end of the file.

```
[#OPI Interface.Parameter.OPIInterfaceURL=#]
```

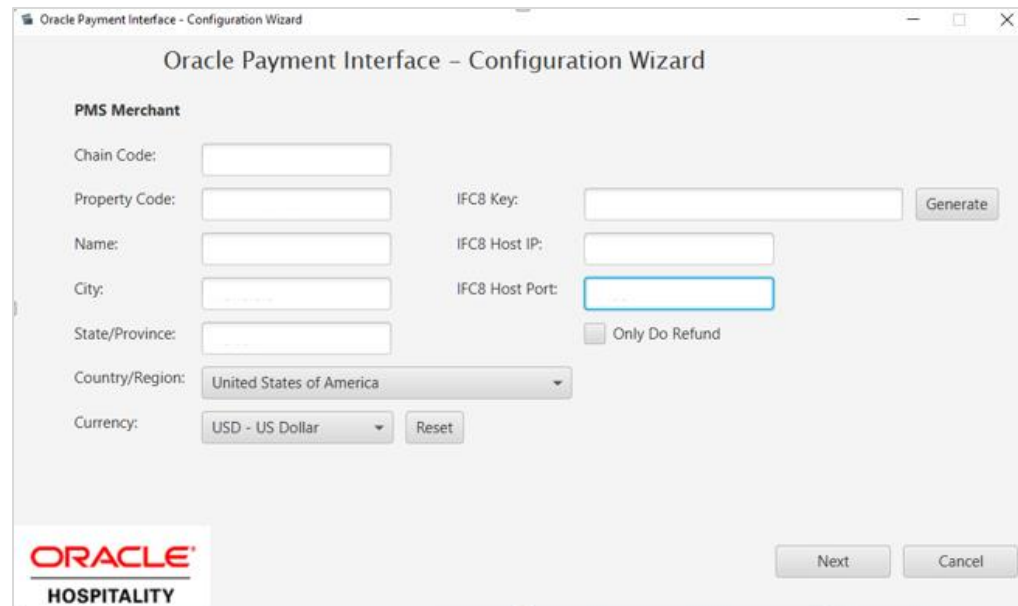
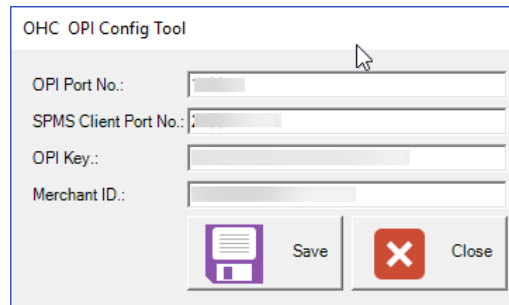
```
[#OPI Interface.Parameter.ClientPort=#]
```

OHC OPI Daemon Service Configuration

To configure the Daemon Services, run `C:\OHCOPIDaemonService\OHCOPIDaemonConfigTool.exe` and insert the fields accordingly.

Table 5-1 - OPI Daemon Service Configuration Field

Field	Description
OPI Port No.	The OPI Port Number.
SPMS Client Port No.	The SPMS Client Port Number.
OPI Key	The Key generated in OPI Configuration – IFC 8 Key.
Merchant ID	The Merchant ID set up in OPI Configuration.



OHC OPI Manager

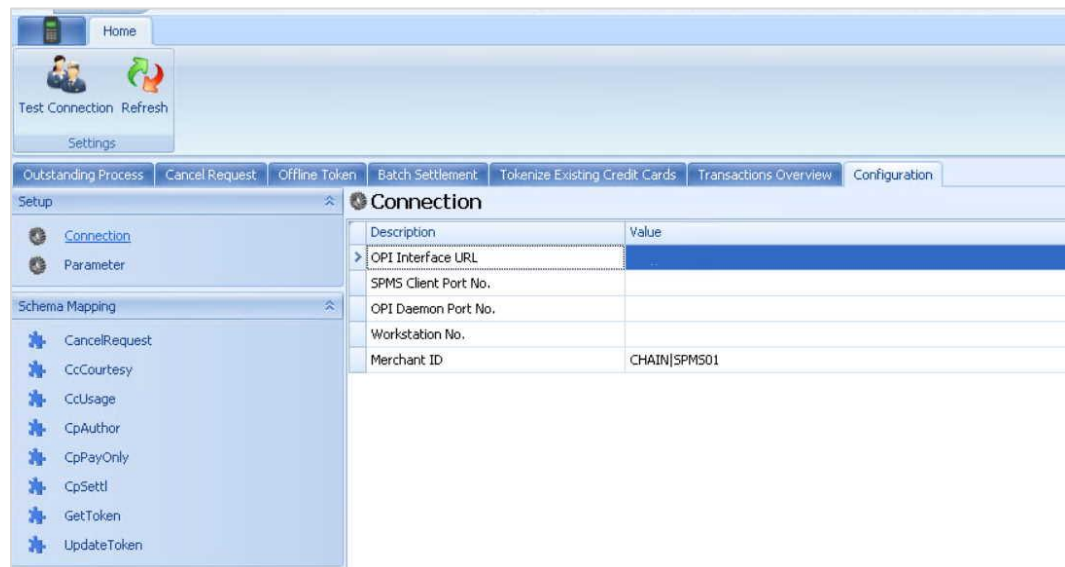
1. Run **OHC OPI Manager.exe** from C:\Program Files (x86)\Oracle Hospitality Cruise.
2. Navigate to the **Configuration** tab.
3. Click **Connection** under Setup pane.
4. Enter the following options:

Table 5-2 - OPI Manager Connection Settings

Description	Value
OPI Interface URL	This is where OHC OPI Daemon is installed (in format ws://ip address:)
SPMS Client Port No.	The same SPMS client Port Number that defined in OPI Daemon Config Tool.

Description	Value
OPI Daemon Port No.	The same OPI Daemon Port Number that defined in OPI Daemon Config Tool.
Workstation No.	Workstation Number of the client.
Merchant ID	Combination of OPERA Chain and Property Code values defined in OPI Configuration, for example, CHAIN PROP1.

5. Click the **Test Connection** to confirm the connection to OHC OPI Daemon is established.



6. Click on **Parameter** under Setup pane, select **OPI Web API Service URL** and insert the hostname or IP with port number where the OHC OPI Web Service is installed, for example, `https://localhost:<PortNo>/`.