

# Oracle® Payment Interface

## Oracle Hospitality OPERA Property Management System Installation Guide



Release 19.1  
F14989-02  
July 2020

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

ORACLE®

Oracle Payment Interface Oracle Hospitality OPERA Property Management System Installation Guide, Release 19.1

F14989-02

Copyright © 2001, 2020, 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

Preface	4
<hr/>	
1 Pre-Installation Steps	1-1
<hr/>	
2 Installing the OPI	2-1
<hr/>	
Certificates	2-13
<hr/>	
3 OPERA Configuration	3-1
<hr/>	
Creating an EFT Interface	3-1
Configuring CHIP AND PIN (EMV)	3-2
Configuring the CC Vault	3-4
Cashiering Overview	3-6
Overview of Credit Card Payment Types	3-7
Credit Card Type Payment Setup Information	3-7
Configuring the Workstation	3-12
Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC)	3-13
Configuring Authentication for the Hotel Property Interface (IFC8) with OPI	3-14
Perform a Tokenization	3-16
<hr/>	
4 Upgrading the OPI	4-1
<hr/>	
OPI 6.1 to 19.1.0.0 Upgrade Steps	4-1
OPI 6.2 to 19.1.0.0 Upgrade Steps	4-3

# Preface

## Purpose

This document describes how to configure the Oracle Payment Interface On Premise Token Exchange Service.

## Audience

This document is intended to cover the additional steps required to setup OPI to handle the On Premise Token Exchange functionality.

This document covers only the configuration of the additional On Premise Token Exchange functionality, it does not cover in detail, installation of the OPI software and IFC8 merchant configuration, separate documentation already exists to cover this.

## Customer Support

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

<https://support.oracle.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 and any associated log files
- Screenshots of each step you take

## Documentation

Product documentation is available on the Oracle Help Center at

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

## Revision History

Date	Description of Change
February 2019	Initial publication.
April 2019	<ul style="list-style-type: none"> <li>• Updated formatting and cover page with new template.</li> <li>• Updated screenshot and minor content changes in <b>Chapter 2 Installing the OPI</b> and <b>Chapter 3 OPERA Configuration</b>.</li> </ul>
July 2019	Updated security bugs in few chapters.
November 2019	Updated content in Terminal section.
December 2019	Updated OPERA client side certificates section and added content for Credit Card Payment Types.
July 2020	Added note in Installing the OPI section.

# 1

## Pre-Installation Steps

Consider the following guidelines before installing Oracle Payment Interface (OPI):

**IF UPGRADING OPI, YOU MUST READ THE [UPGRADING THE OPI SECTION](#) FIRST.**

- OPERA Property Management Systems releases you can use to integrate with OPI:
  - OPERA V5 Hosted 5.5.25 or higher
  - OPERA V5.6.4 or higher
- OPI 19.1 does not install a database. If doing a clean install of OPI, a database must be installed first.
- Upgrading to OPI 19.1 from OPI 6.1 and higher is supported but MPG versions are not supported. Prior to upgrading from OPI 6.1 to OPI 19.1 all credit card transactions must be finalized and closed as the schema upgrade will not include the migration of old transaction data to OPI side. Finalizing and closing credit card transactions is not a requirement for upgrading from OPI 6.2 to OPI 19.1 as no schema migration is expected in this case.
- Any previous version of MPG should be uninstalled prior to installing OPI 19.1
- The application requires Microsoft.NET Framework version 4.0 or higher.
- Confirm Java Platform, Standard Edition Runtime Environment (JRE) version 1.8.152 or higher but below 1.9 is installed on the computer where OPI is installed.
- OPI requires at least 6 GB of free disk space and you must install OPI as a System Administrator.

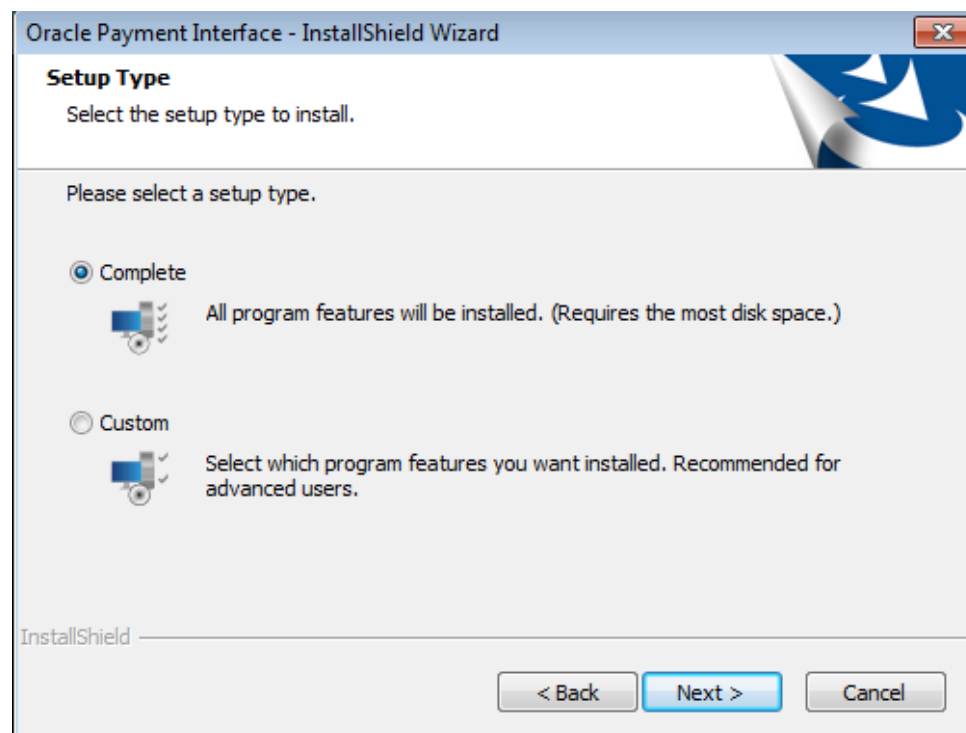
During the installation you must confirm the following:

- Merchant IDs
- IP address of the OPI Server
- If there is an existing MySQL database installed, then the SQL root password is required.
- Workstation IDs and IPs that integrate with the PIN pad.

# 2

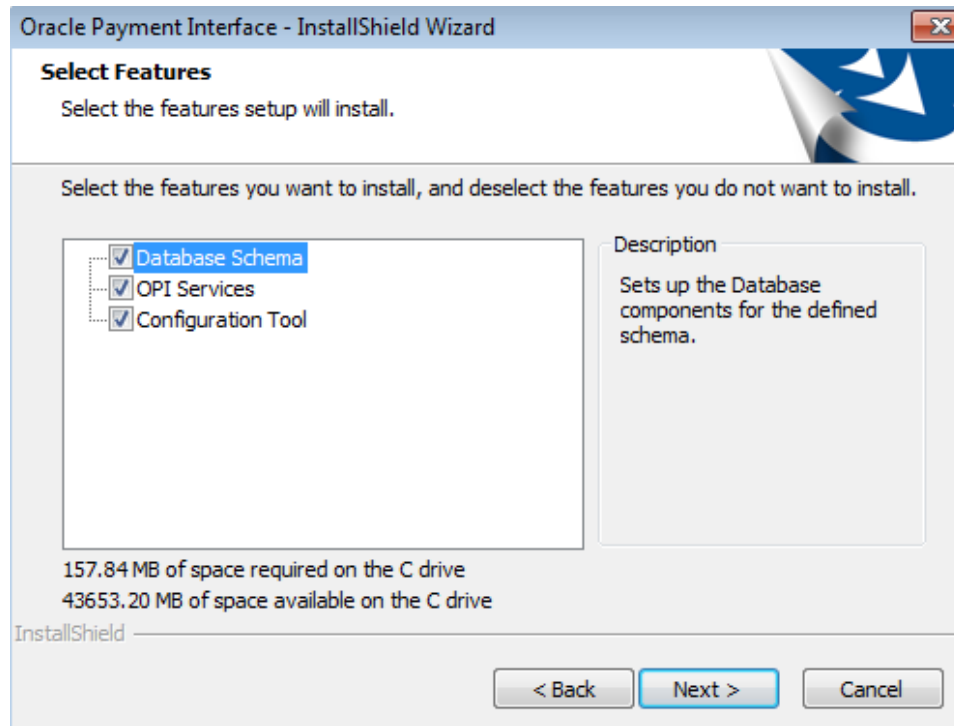
## Installing the OPI

1. Copy `OraclePaymentInterfaceInstaller_19.1.0.0.exe` to the Server and double-click it to launch the install.
2. Select a language, and then click **OK**.
3. Click **Next** on the Welcome to the InstallShield Wizard for Oracle Payment Interface screen.
4. Click **Next** on the OPI Prerequisites screen.



The Setup Type screen appears.

- **Complete:** All program features will be installed.
  - **Custom:** Select which program features you want installed. Recommended for advanced users only.
5. Make a selection (only for Custom install), and then click **Next**. If you select Complete Install, it will go to the Step 7 directly.



If you selected the Custom install option, the Select Features screen appears with the following options:

- a. Database Schema
- b. OPI Services
- c. Configuration Tool

All three of these features must be installed. It is just a matter of whether they are all installed on the same computer or on separate computers.

6. Select the features to install on this computer, and then click **Next**.

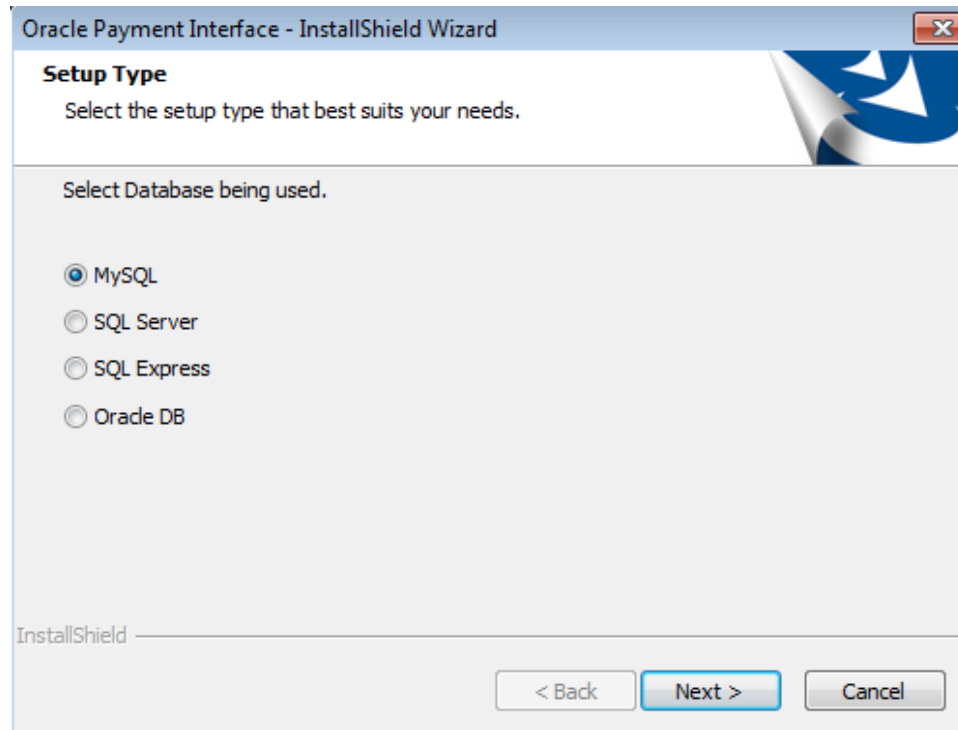
The Choose Destination Location screen appears.

7. Accept the default installation location or click **Change...** to choose a different location, and then click **Next**.

8. Click **Install** on the Ready to Install the Program screen.

The Setup Status screen displays for a few minutes.

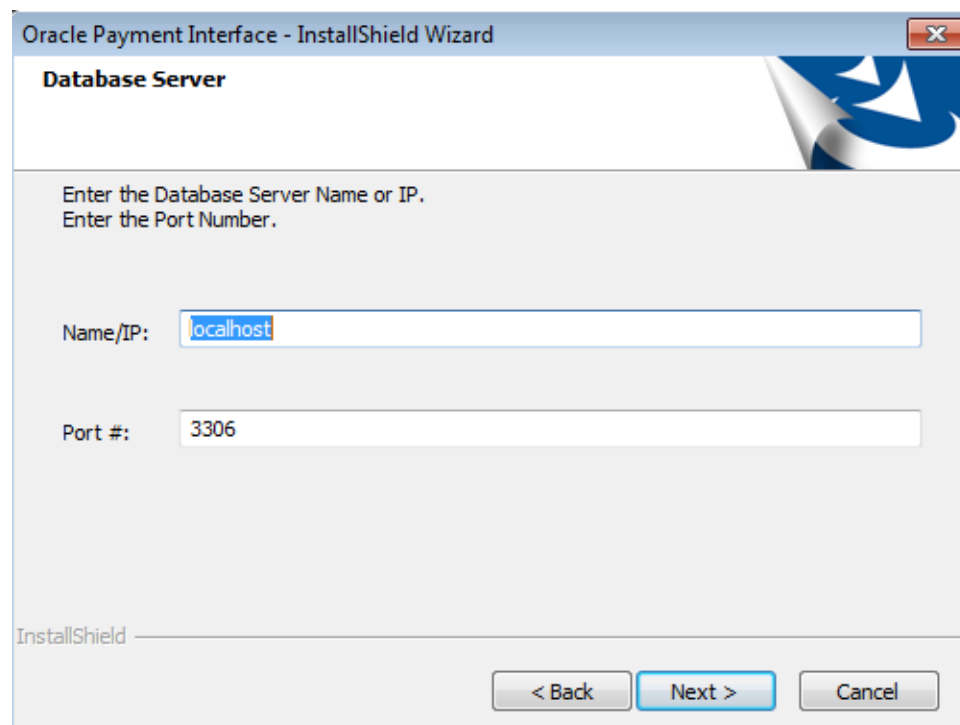
9. The Setup Type screen appears.



10. Select the database type being used, and then click **Next**.

 **NOTE:**

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





The Database Server screen appears.

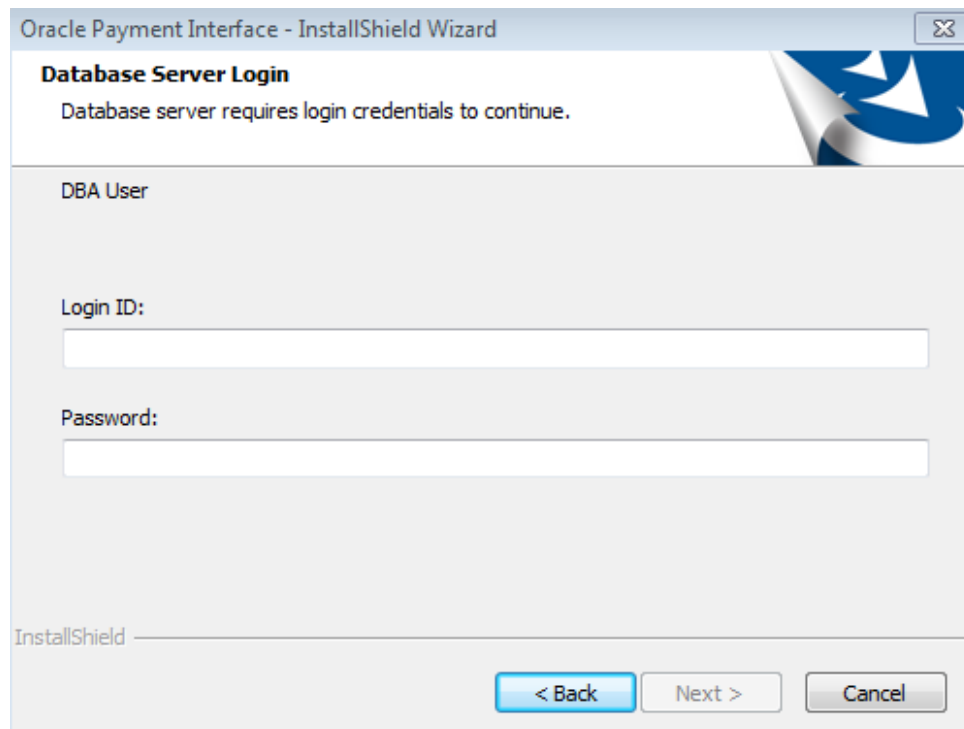
11. **The Name/IP:** field defaults to localhost. This should be left as localhost if the OPI database is installed on the same computer. If the database is installed on another computer, the Name or IP address of that machine should be entered here.

 **NOTE:**

If the database type is MySQL, and you cannot use localhost for the Name/IP field, then some commands must be run manually on that MySQL database before proceeding. See MySQL command link in the OPI Basic Install doc for instructions. Setup will not complete if this is not done.

12. Accept the default **Port #** of 3306 (for MySQL), and then click **Next**.

The Database Server Login screen appears.



13. Enter the credentials for the DBA user of the database type selected, and then click **Next**.

- For MySQL the Login ID: = root
- For other database types the DBA user name/Login ID may be different.
- Enter the correct password for the DBA user.

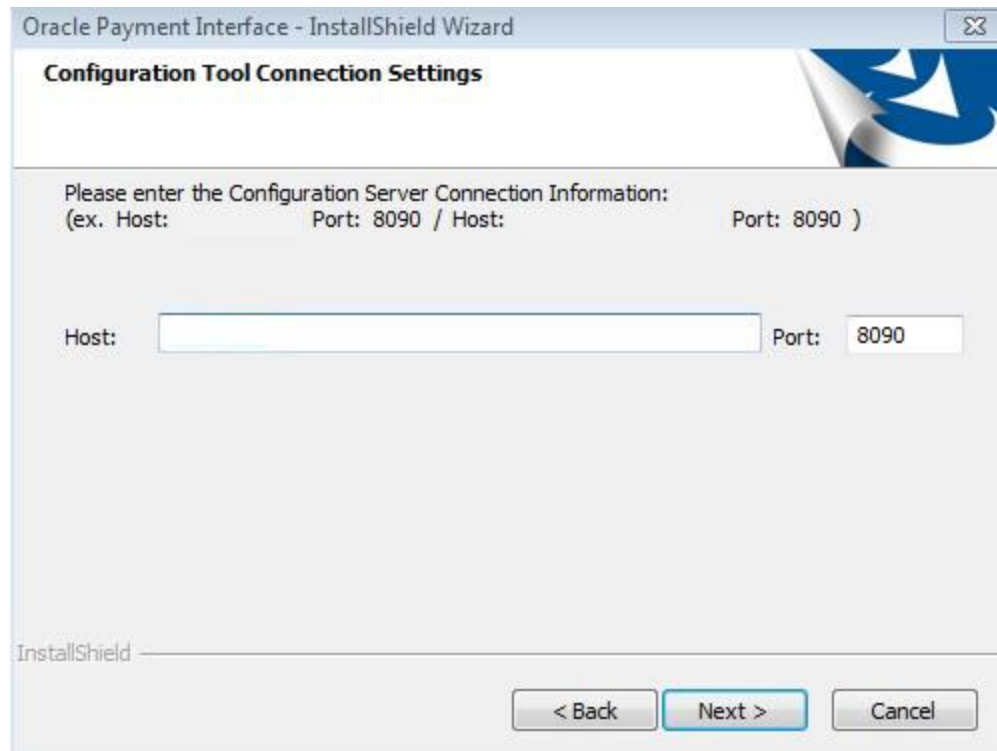
The Database User Credentials screen appears.

The screenshot shows a dialog box titled "Oracle Payment Interface - InstallShield Wizard" with a sub-header "Database User Credentials". The dialog contains the following text: "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: !@#\$\$%^&\*". Below this text are three input fields labeled "User Name:", "Password:", and "Confirm Password:". At the bottom of the dialog are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog.

14. **User Name:** Create a new user.
15. **Password:** Create a password. 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: !@#\$\$%^&\*.
16. Confirm the password, and then click **Next**.
17. Click **OK** on the Database connection successful dialog.
18. Click **OK** on the Database Configuration operation successful dialog.  
The Configuration Tool Superuser Credentials screen appears.

The screenshot shows a dialog box titled "Oracle Payment Interface - InstallShield Wizard" with a close button in the top right corner. The main heading is "Configuration Tool Superuser Credentials". Below the heading is a blue graphic of a document with a white arrow pointing to the right. The text inside the dialog reads: "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: !@#\$%^&\*". There are three input fields: "User Name:", "Password:", and "Confirm Password:". At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog.

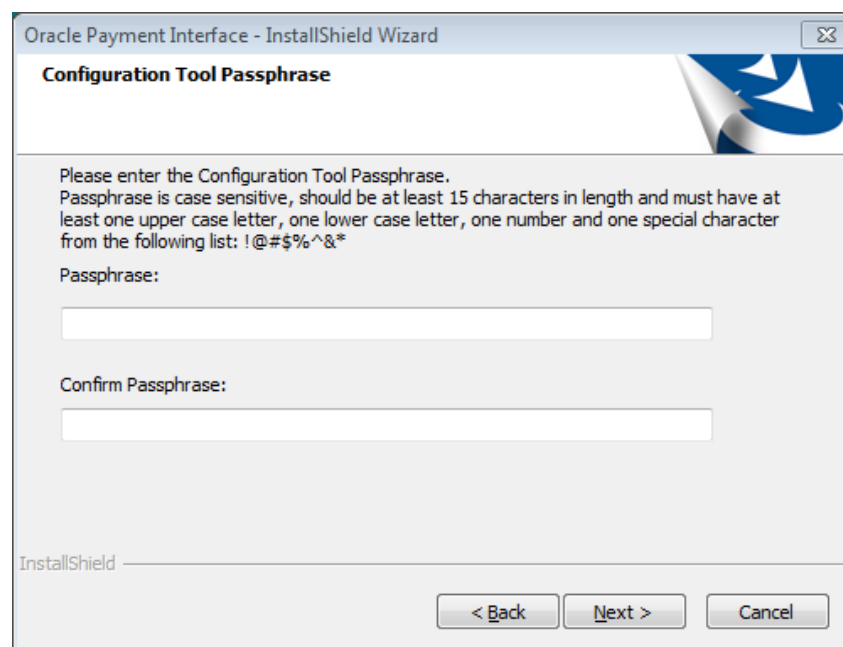
19. **User Name:** This can be any user name. It does not have to be a Windows account user.
20. **Password:** Create a password. Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#\$%^&\*.
21. Confirm the password, and then click **Next**.
22. Click **OK** on the Create SuperUser operation successful dialog.  
The Configuration Tool Connection Settings screen appears.



- **Host:** Enter the IP address or server name of the PC where the OPI Config Service is installed. This will be the PC where you selected “OPI Services” to be installed.
- Leave the default Port of 8090.

23. Click **Next**.

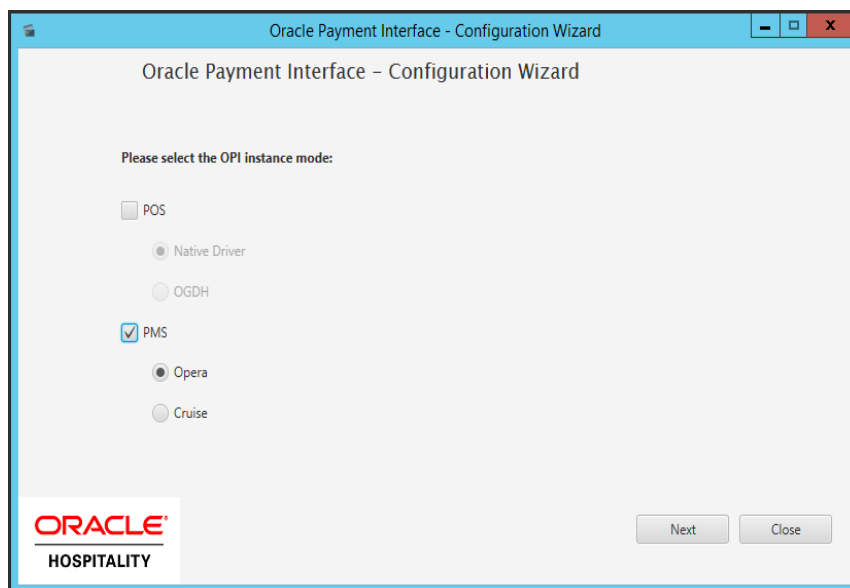
The Configuration Tool Passphrase screen appears.



24. **Passphrase:** The passphrase is case sensitive, should be at least 15 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: !@#%&^\*.

25. Enter a passphrase, confirm it, and then click **Next**.

After a brief pause, the Configuration Wizard launches.



26. Select **PMS**, select **OPERA**, and then click **Next**.

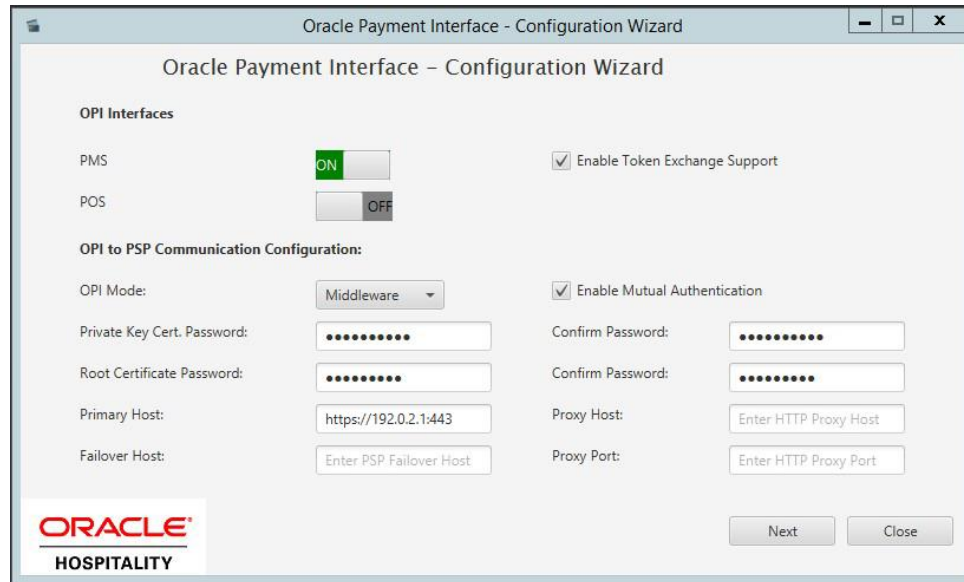
27. **OPI Interface:** Turn PMS on, and select the **Enable Token Exchange Support** box. The Token Exchange functionality is separate to the IFC8 merchant functionality.

### OPI to PSP Communication Configuration

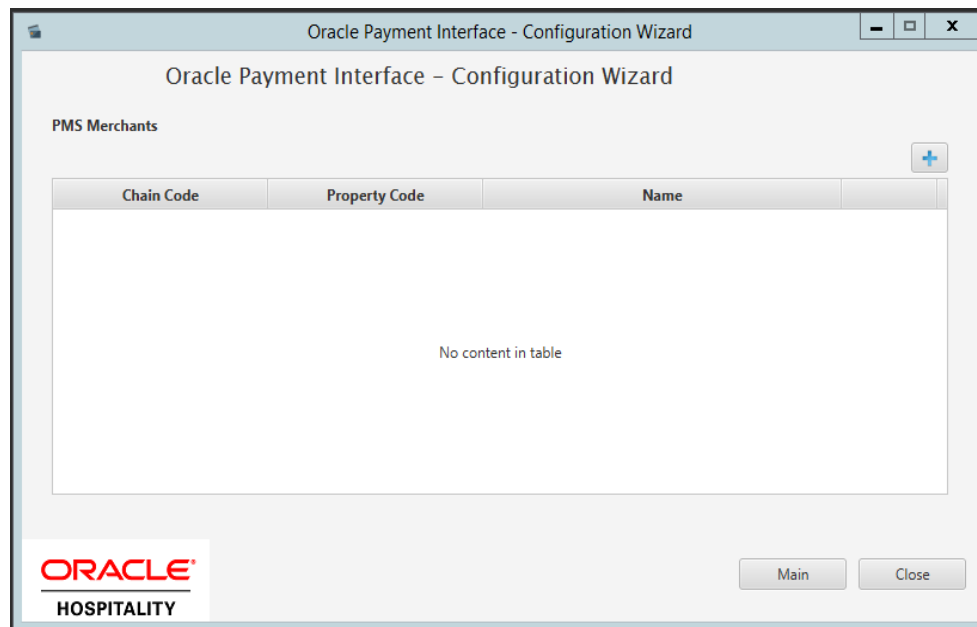
- From the OPI Mode drop-down list, select the Terminal for the PED direct connection or select Middleware for middleware connection.
- Enable Mutual Authentication, this supports two-way authentication. The PSP partner needs to provide a set of .cer and .pfx files. Load the .cer file into JKS, and copy both root certificate and pfx to the key folder of OPI. Put the relative password here for Private key and root certificate key.
- Enter the third-party payment service provider middleware Host IP address if Middleware mode is selected. If Terminal mode is selected OPI configuration will populate another window in further steps to input Workstation ID and IP address.

#### **NOTE:**

For Terminal Mode setup, special characters including "\_", "|", and "=" cannot be used in the CHAINCODE or PROPERTYCODE. This will cause the EOD to fail in OPI.



28. Click the blue + icon to add a new merchant configuration for OPERA.



29. To configure the OPERA merchant, enter the following information:

- The *OPERA Vault Chain Code* & *Property Code*; will form the **Siteld** value in the Token request messages.
- Select **Generate Key**. You must use this key to configure the Hotel Property Interface (IFC8). Add "FidCrypt0S|" to the generated key as prefix. For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxxxx
- Enter the **IFC8 IP address** and **port** number for the Hotel Property Interface (IFC8) server.
- Enter the **Merchant name**, **city**, and **country** information.

- Select the option of **Only Do Refund** if you want to disable differentiating between void and refund from OPERA.
- Click **Next**.

Although the other populated settings are not directly related to the Token Exchange Service configuration, Token Exchange will not be possible if the IFC8 interface is not running, as OPI will not progress past the IFC8 startup if the IFC8 connection is not possible.

30. Enter the OPERA payment code for each card type, and then click **Next**.

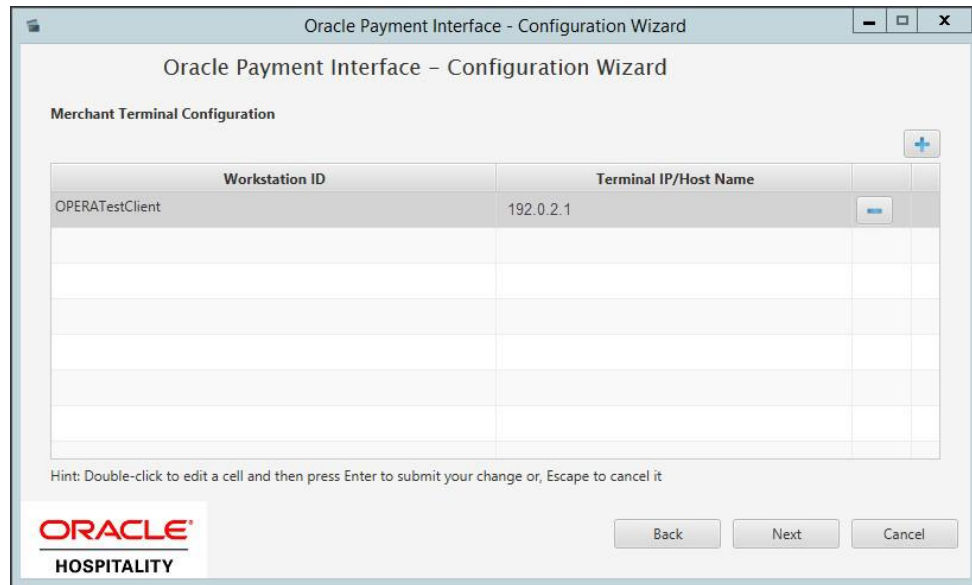


**NOTE:**

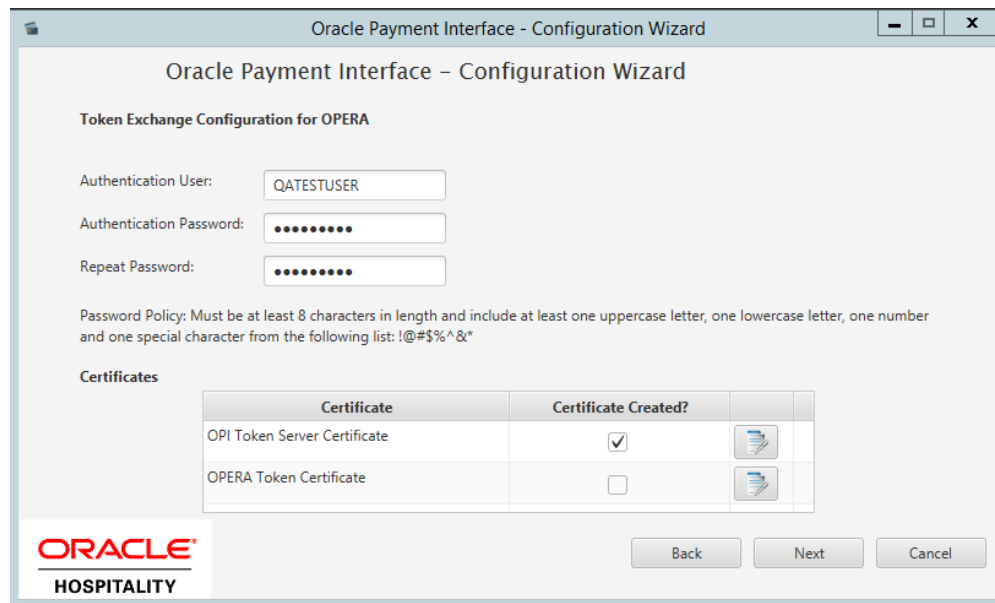
OPI Payment Code must match the IFC CC Type configured in OPERA.

Card Type	Payment Code
AliPay	AB
Alliance	AL
American Express	AX
China UnionPay	CU
China UnionPay Debit	CD
Debit	DD
Diners Club	DC
Discover	DS
EC Chip	EC

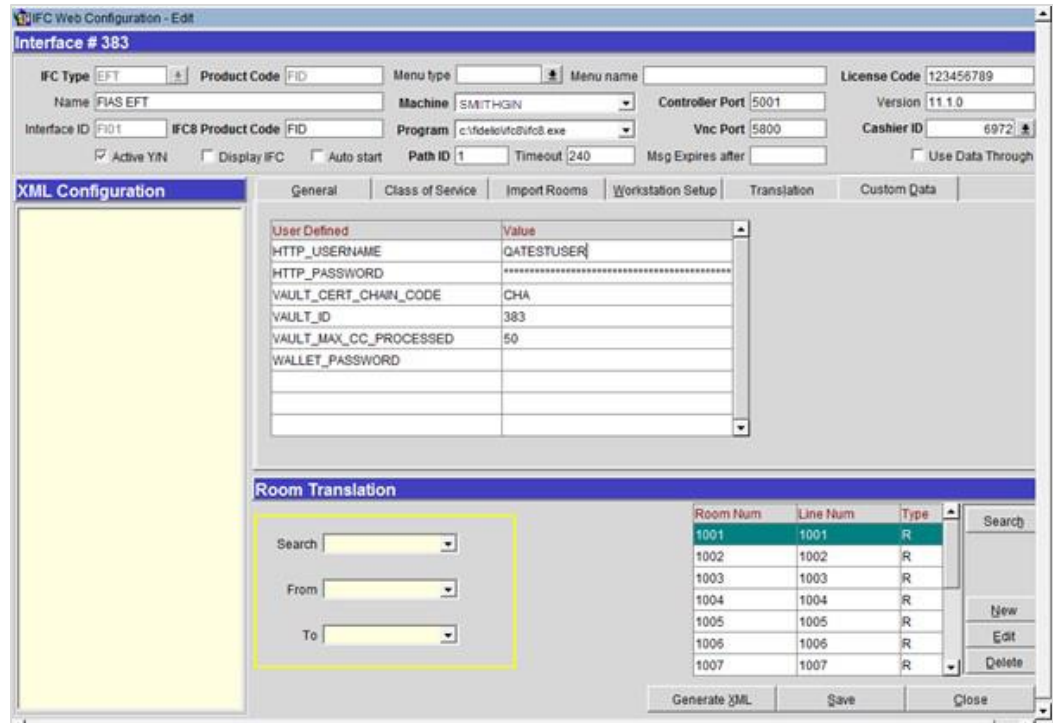
Below is terminal mapping if you select terminal mode.



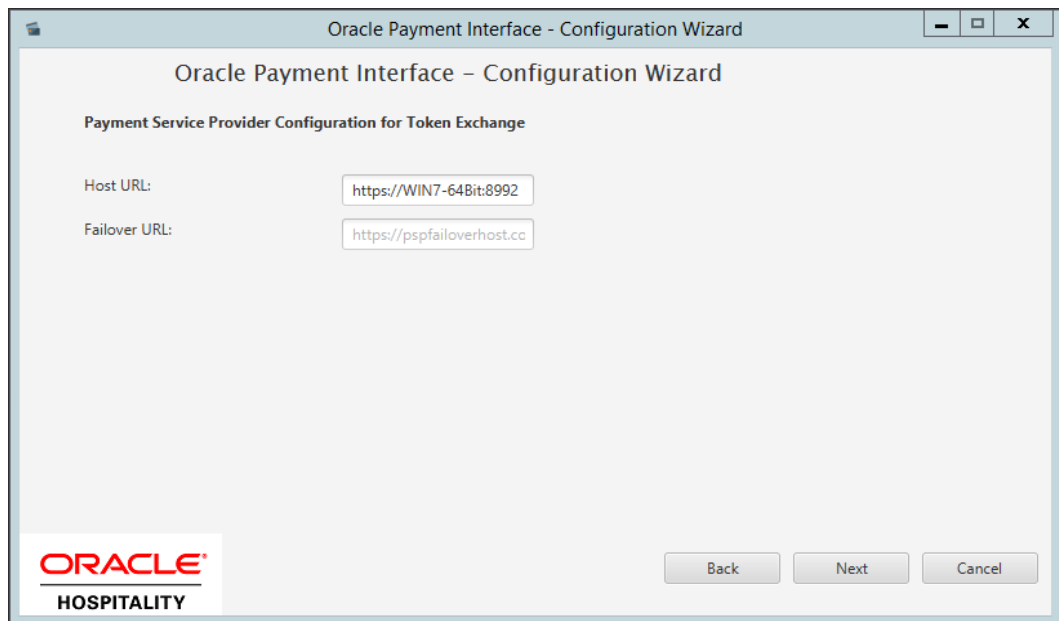
31. The top half of the *Token Exchange Configuration* screen allows you to configure the Header Authentication credentials used in communications from OPERA->OPI.
  - The details entered must match the details entered in the OPERA Interface Custom Data page (**OPERA PMS Configuration | Setup | Property Interfaces | Interface Configuration | edit EFT IFC OPI | Custom Data tab**)





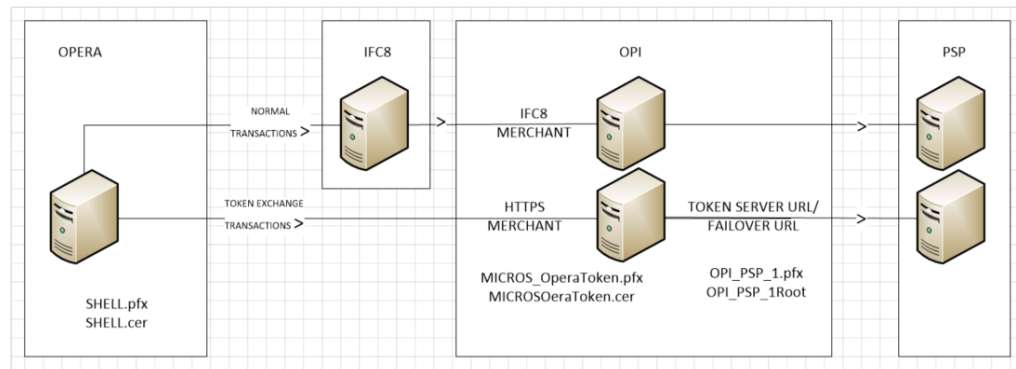


- Certificates are explained in the [Certificates](#) section.
32. The next configuration relates to communication from OPI to the PSP host for Token Exchange, enter the PSP host name with port in the URL, and then click **Next**.



33. Click **Finish** to restart.

# Certificates



OPI on Premise Token Exchange requires the below sets of certificates:

- OPI > PSP - (PSP - Client Side Certificates)
- OPERA > OPI - (OPI - Server Side Certificates)

Refer to the sections below for further details.

## PSP - Client Side Certificates

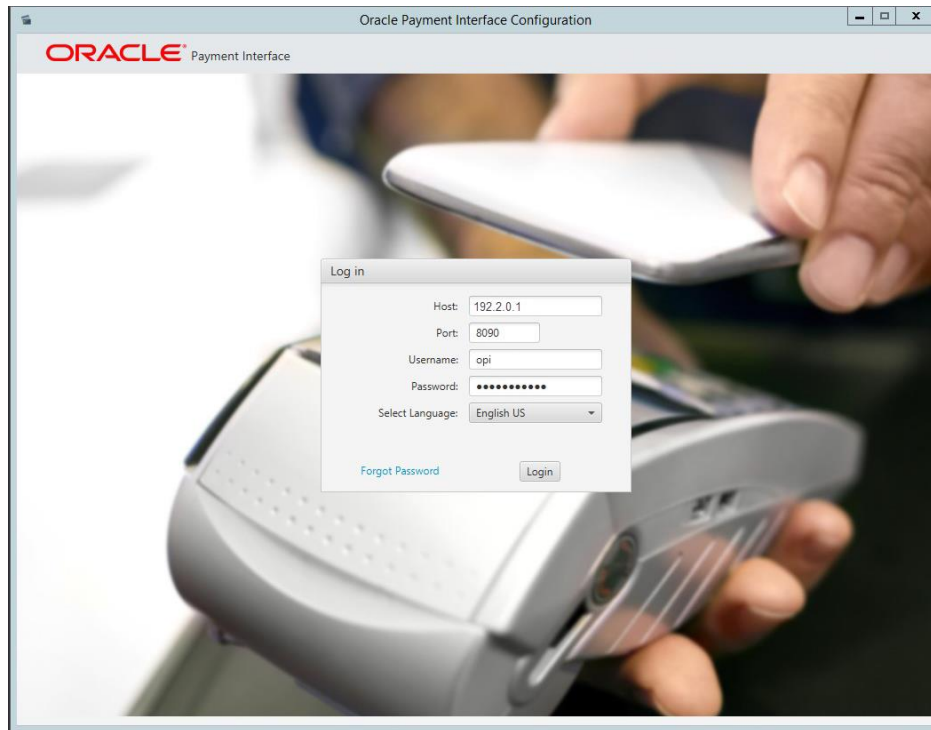
The communication from OPI to the PSP for token exchange uses HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed at PSP (server side) for HTTPS communication, PSP is also expected to provide a client side certificate to be deployed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

In order to achieve this, PSP is required to provide two files:

- A client side certificate file, this is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password.
- The root certificate file for the server side certificate that is deployed at PSP side. OPI needs to load this root certificate file into the Java Key store so that OPI can properly recognize and trust the server side certificate deployed at PSP side. The root certificate file provided by the PSP should be in the format of .cer or .crt.

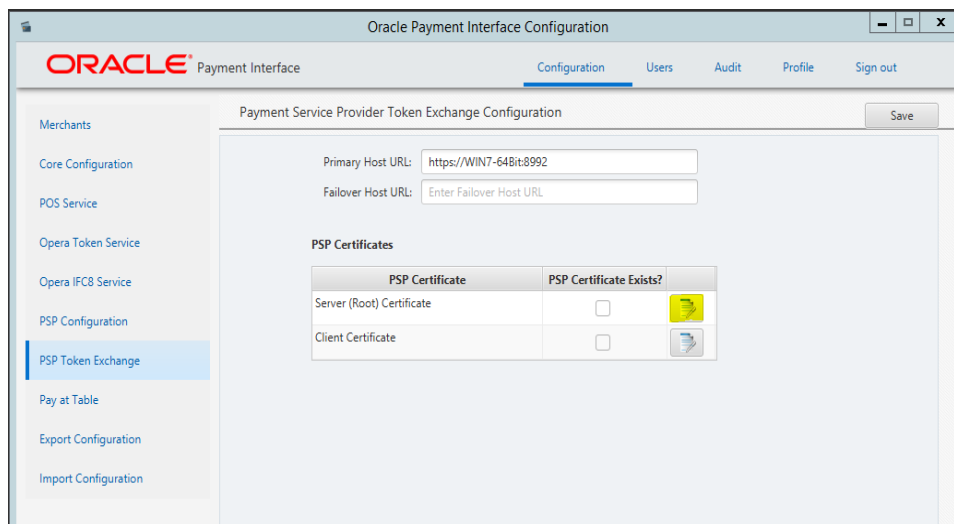
**To deploy the client certificate on the OPI side:**

1. Run `\OraclePaymentInterface\19.1\Config\LaunchConfiguration.bat`
2. Log in as the Super user you created during OPI installation.

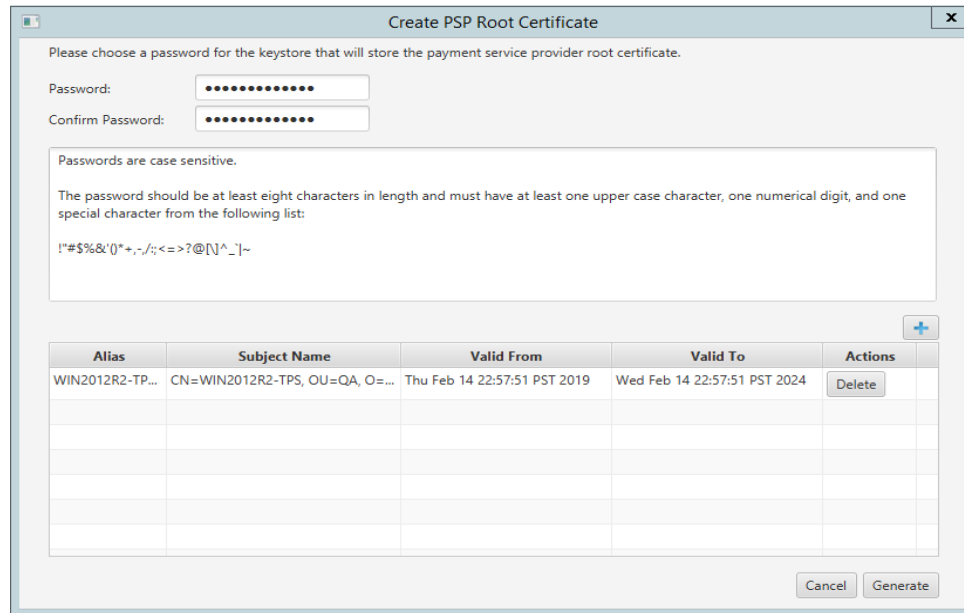


### Handling the Root Certificate File by OPI Configuration Tool.

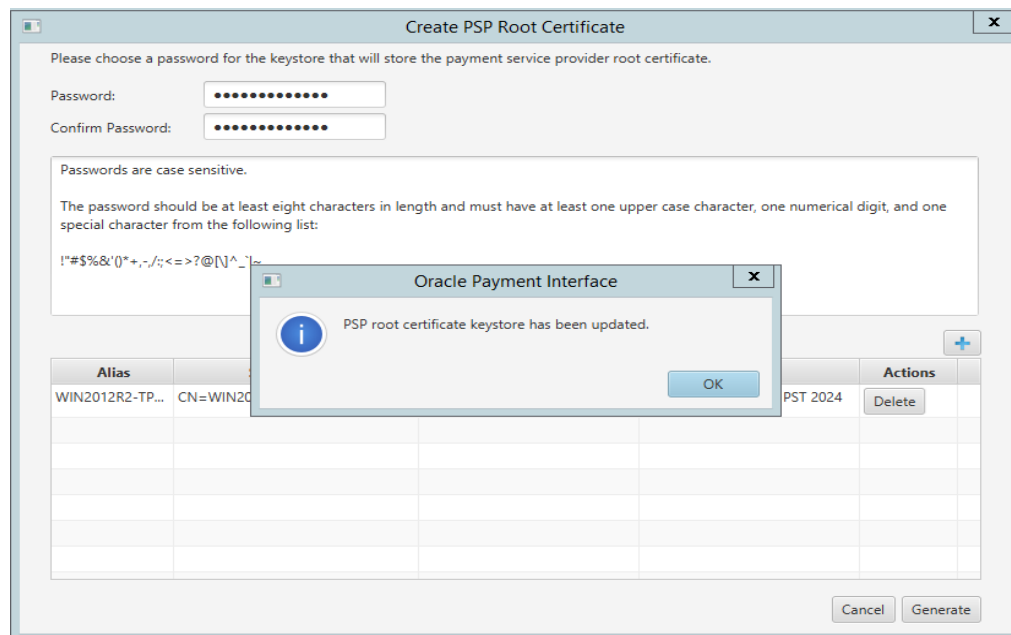
1. Select **PSP Token Exchange**, and then edit the **Server (Root) Certificate**.



2. Enter the password for the keystore, and then browse to the location of the certificate you wish to import from add icon available or drag and drop the .cer or.crt.



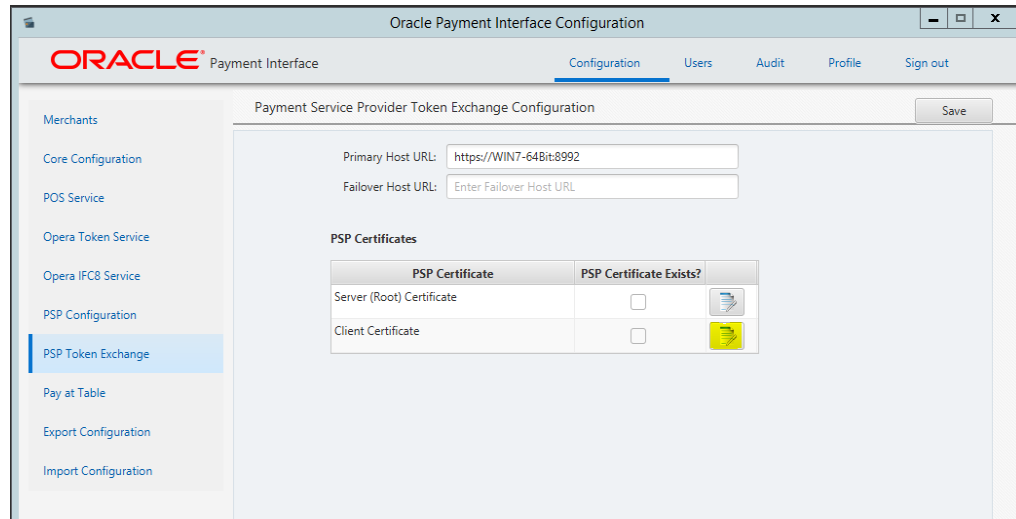
3. Click **Generate**.



**OPI\_PSP\_1Root** is created under `\OraclePaymentInterface\19.1\Services\OPI\key`

### Handling the Client Side Certificate

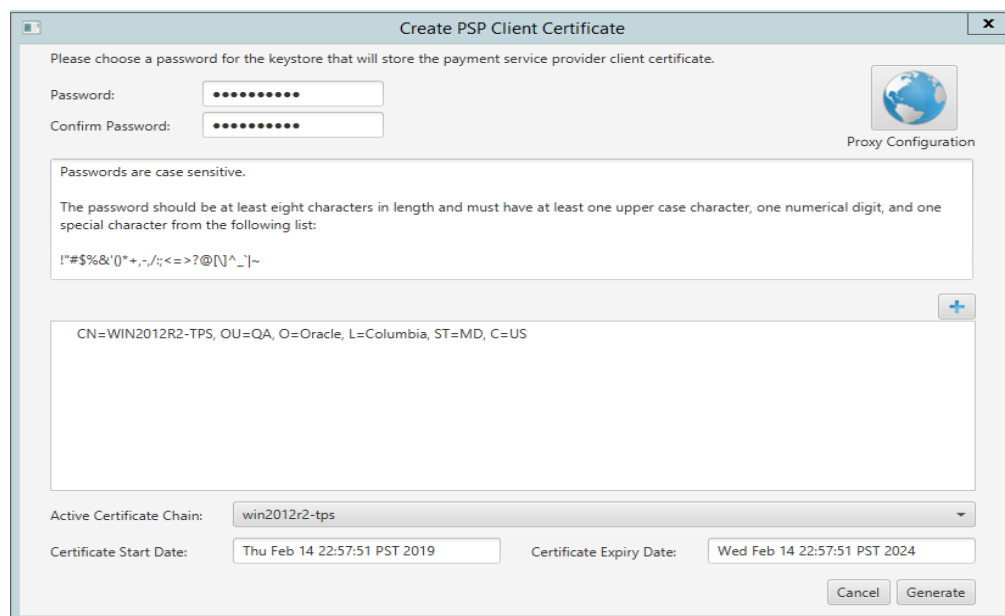
1. Select **PSP Token Exchange**, and then edit the **Client Certificate**.



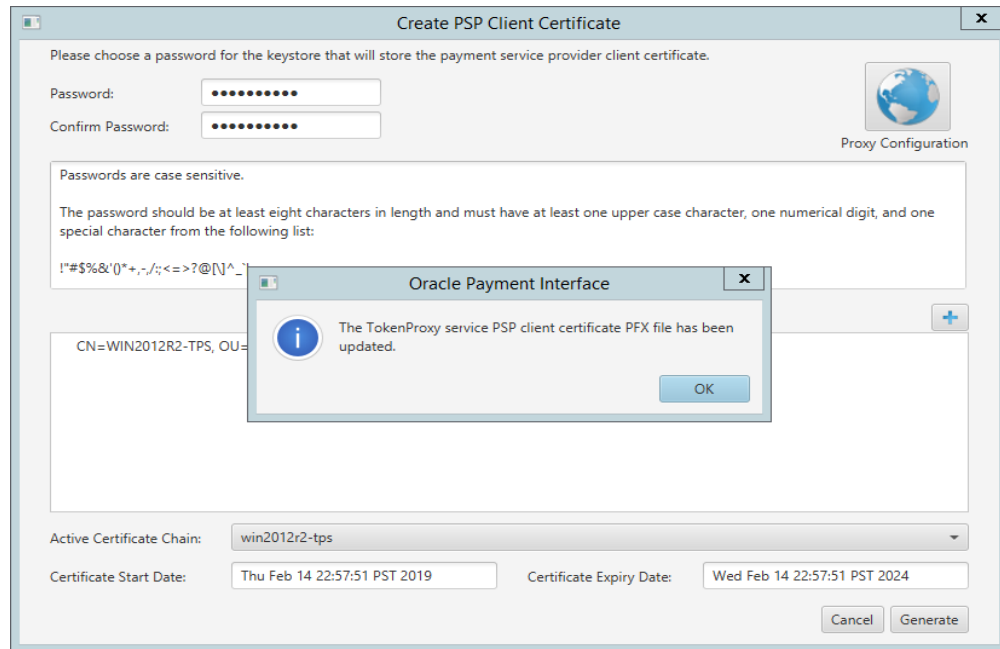
2. Enter the password for the keystore then browse to the location of the certificate you wish to import from add icon available or drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below or it will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

**NOTE:**

The PSP Client Side Certificates expiration date will vary depending on what the PSP 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.



3. Click **Generate**.

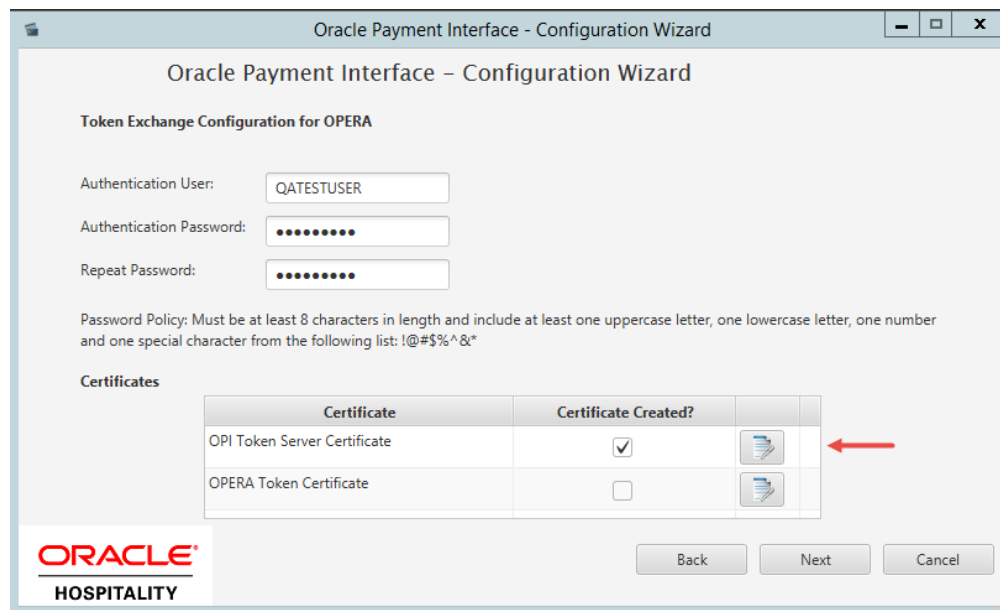


OPI\_PSP\_1.pfx is created under \OraclePaymentInterface\19.1\Services\OPI\key folder.

## OPI - Server Side Certificates

The lower half of the page relates to generating server side certificate used in communication from OPERA to OPI.

1. Click **Create OPI Token Server Certificate** to proceed.



- Populate the fields with the relevant information. The password fields validate the passwords are complex, so the passwords will need to meet these requirements;
  - Min 8 characters in length

- Min 1 Alpha Character
- Min 1 Numeric Character
- Min 1 Special Character from the following list !@#\$\$%^&\*

Merchant City: Columbia

Merchant State/Province: MD

Merchant Country/Region: US

OPI Server IP: 192.2.0.1

Password: .....

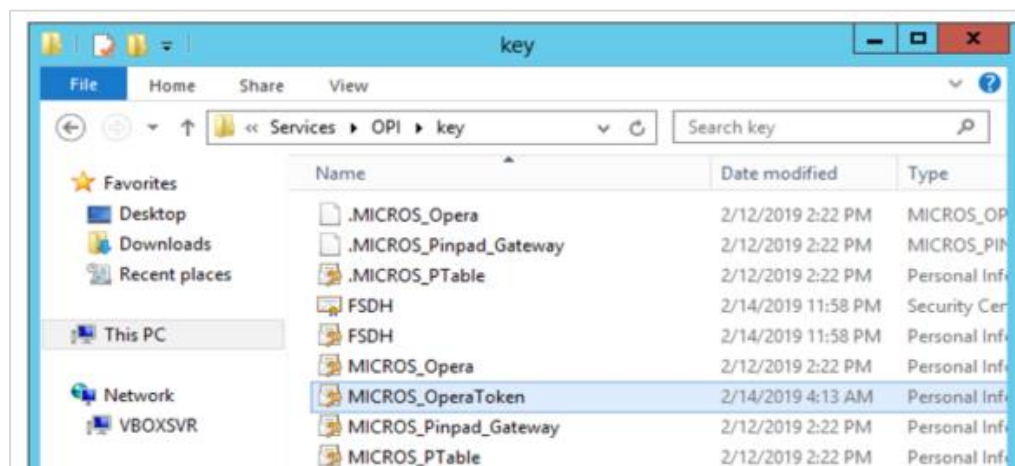
Confirm Password: .....

Cancel Generate

3. Click **Generate** to continue.

This process will generate the `MICROS_OPERAToken.pfx` & `MICROSOPERAToken.cer` files in the following folder:

`\OraclePaymentInterface\v19.1\Services\OPI\key\`



 **NOTE:**

The OPI Server Side Certificates have a default expiration date of five years from the date of creation. Check the expiration date in the properties of the certificate files.

The OPI Server Side Certificates must be updated prior to the expiration date to avoid downtime to the interface.

Copy the `MICROSOPERAToken.cer` files to all of the OPERA registered terminals that you will run the Token Exchange process from, and then import to Trusted Root Certification Authorities, using `mmc.exe` (Refer to section [Certificate Import using Microsoft Management Console](#) for more details)

Close the Certificate generation screen. You should now see  under Certificate created.

## OPI - Client Side Certificates

 **NOTE:**

For the below OPERA versions, the Mutual Authentication requirement was removed for an OPI TPS communication.

- OPERA V5.5.0.23 and V5.6.4.0.
- OPERA Cloud 19.2.0.0 and 1.20.16.0.



# 3

## OPERA Configuration

### Creating an EFT Interface

1. Log in to OPERA and go to **Configuration**.
2. Select the menu option **Setup | Property Interfaces | Interface Configuration**. If there is no active EFT or CCW IFC Type, select New to add configuration for a new EFT interface.
3. Enter the following options, and then click **OK**:
  - **IFC Type**: EFT
  - **Name**: Oracle Payment Interface
  - **Product Code**: OPI
  - **Machine**: Select the machine
  - **License Code**: License code for interface
  - **IFC8 Prod Cd**: XML\_OPI

IFC Web Configuration - New

IFC Type: EFT Name: Oracle Payment Interface

Product Code: OPI Machine: SMIITHGIN

License Code: 987654 IFC8 Prod Cd: XML\_OPI

Generate XML

Communication:  TCP/IP  Serial

IP: [ ] Port: [ ]

OK Close

4. Select the check box to enable the **Handle night audit commands**.
5. Select the check box to enable the **CC Vault Function**.
6. Define the **Timeout** value as 210.

IFC Web Configuration - Edit

Interface # 151

IFC Type: EFT Product Code: MFG Menu type: [ ] Menu name: [ ] License Code: 8050817223

Name: Oracle Payment Interface Machine: WIN7-64BIT Controller Port: 5001 Version: 13.2.0

Interface ID: MF01 IFC8 Product Code: XML\_OPI Program: c:\ndelo\lrc8\lrc8.exe Vnc Port: 5800 Cashier ID: 16

Active Y/N  Display IFC  Auto start Path ID: 1 Timeout: 210 Msg Expires after: [ ]  Use Data Through

XML Configuration

General Class of Service Import Rooms Workstation Setup Translation Custom Data

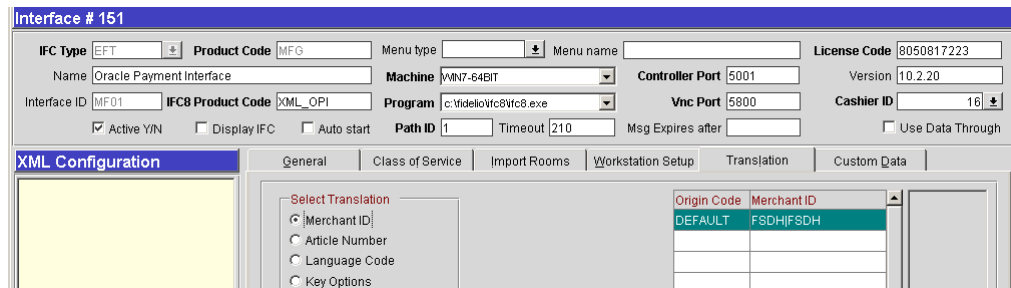
Handle night audit commands  CC Vault Function

EFT Setup

Regular Transaction  Courtesy Card Handling

Port: [ ] IP Address: [ ]  Stored Value System

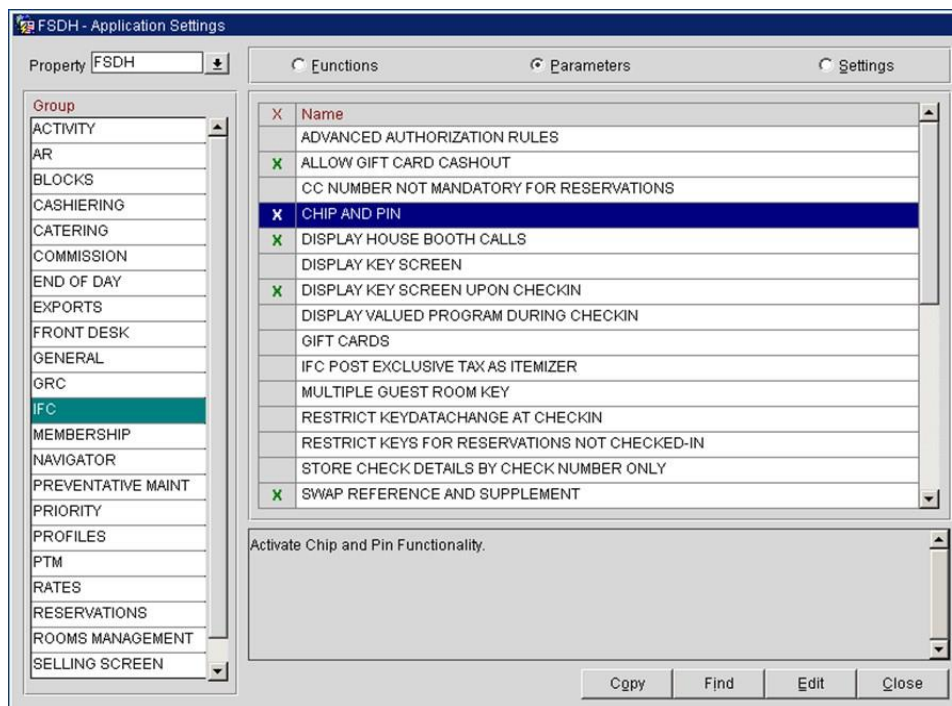
7. Select the **Translation** tab, and then click **Merchant ID**.
8. Select **New** to add the Merchant ID. This must be the same as previously configured in OPI (MPG) Configuration.



## Configuring CHIP AND PIN (EMV)

To configure the Functionality Setup:

1. Go to **Setup | Application Settings | IFC Group > Parameters**, and enable **CHIP AND PIN**.



2. Go to **Setup | Property Interfaces | Credit Card Interface | Functionality Setup**.

**ODH - Credit Cards Functionality Setup**

**Global Rules**

- Online Settlement
- Batch Settlement
- Send Total Tax in Settlements
- Credit Card Type Check/Usages
- Night Audit Remote Authorization
- Blacklist Card Check
- Force Auth. During Check In / Interactive Auth. Window
- Temporarily Store Offline Settlements
- Manual Authorization Notification
- Activate Installments

**Card Specific Rules**

- Authorization at Check-In      Types: VI,MC,AX,DS,VA
- Authorization Reversal Allowed      Types: VA,VI
- Authorization during Stay/Deposit      Types: VI,MC,AX,DS,VA
- Authorization Settlement at Check-Out      Types: CPMC,
- Deposit CW2 Check      Types:
- Deposit Address Verification      Types:
- Chip and Pin      Types: AX,CPMC,DS,MC,VA,VI,

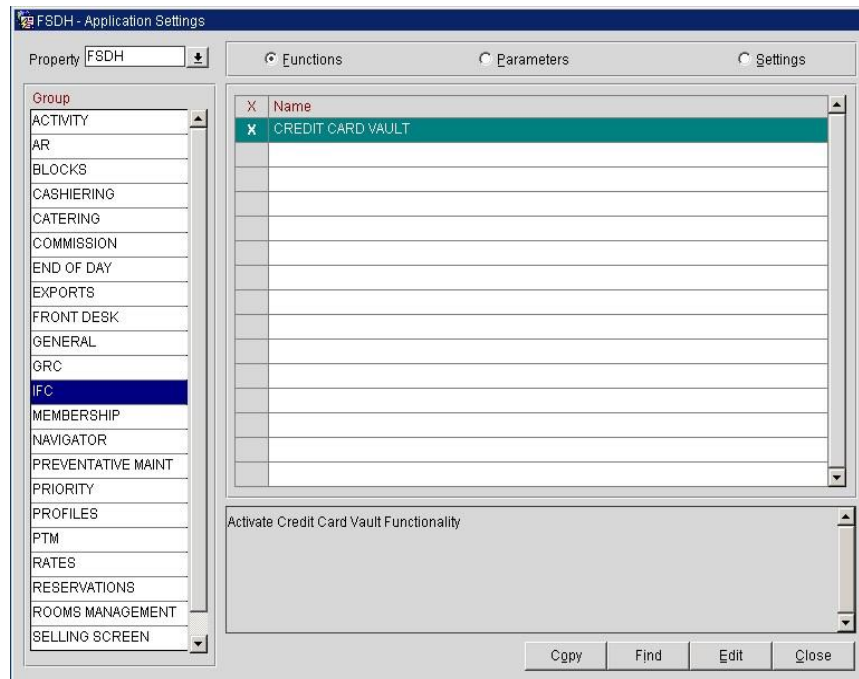
OK      Close

- **Online Settlement:** Select this check box to allow online settlement. OPI is an online settlement. This must be checked to activate the Chip and PIN Application Setting.
- **Authorization at Check-In:** Select the payment methods that will trigger an automatic credit card authorization at check-in.
- **Authorization Reversal Allowed:** Select the payment methods that can process authorization reversals. This provides a request transaction to the Payment Partner to remove the existing authorization on a guest credit card or debit card if the folio payment type is changed or at check-out a different payment method is used. For example, a guest checks in on a reservation for a 5-night stay using a Visa credit card for payment type. At the time of authorization, a hold is put on the Visa credit card for the total cost of the stay. If the payment type is changed to another type on the reservation or the guest checks out using cash or a different brand of credit card, OPERA will send a reversal request for the originally selected Visa credit card authorization. A partial reverse authorization is not supported.
- **Authorization During Stay/Deposit:** Select the payment methods that allow manual and automatic authorizations following check-in and prior to check-out and settlement. This option must be enabled in order to allow authorizations by the end-of-day routine.
- **Authorization Settlement at Check-Out:** Select the payment types that use credit card authorization and settlement in one transaction request. These are payment types that do not allow an authorization separate from the settlement/sale.

- The payment types that are available in the multi-select list of values are only payment types configured as EFT payment types. Any one payment type can be selected for credit card specific rules of Authorization at check-in, Authorization Reversal, and Authorization during Stay/Deposit. If they are selected for these card specific rules, then the payment types will not be available for Authorization During Stay/Deposit.
- **Chip and PIN Enabled Payment Types:** When the **IFC | Chip and PIN** application parameter is set to Y, this option is visible and selected by default. You may not unselect the check box. Select the LOV to choose the credit card payment types that will trigger a Chip and PIN message with or without credit card data to the EMV Device. Payment types that are configured here will not require that a credit card number or expiration date to be entered when selected as a payment method on the Reservation screen or on the Payment screen. This data can be provided in the response message from the Payment Partner.

## Configuring the CC Vault

Go to **Setup | Application Settings | IFC Group | Functions**, and enable **CREDIT CARD VAULT**.



*Configuration -> Setup -> Application Settings -> IFC -> Settings*

OPERA uses the CREDIT CARD VAULT CHAIN CODE for the certificate lookup and should be populated with what was entered during the OPI configuration for PMS.

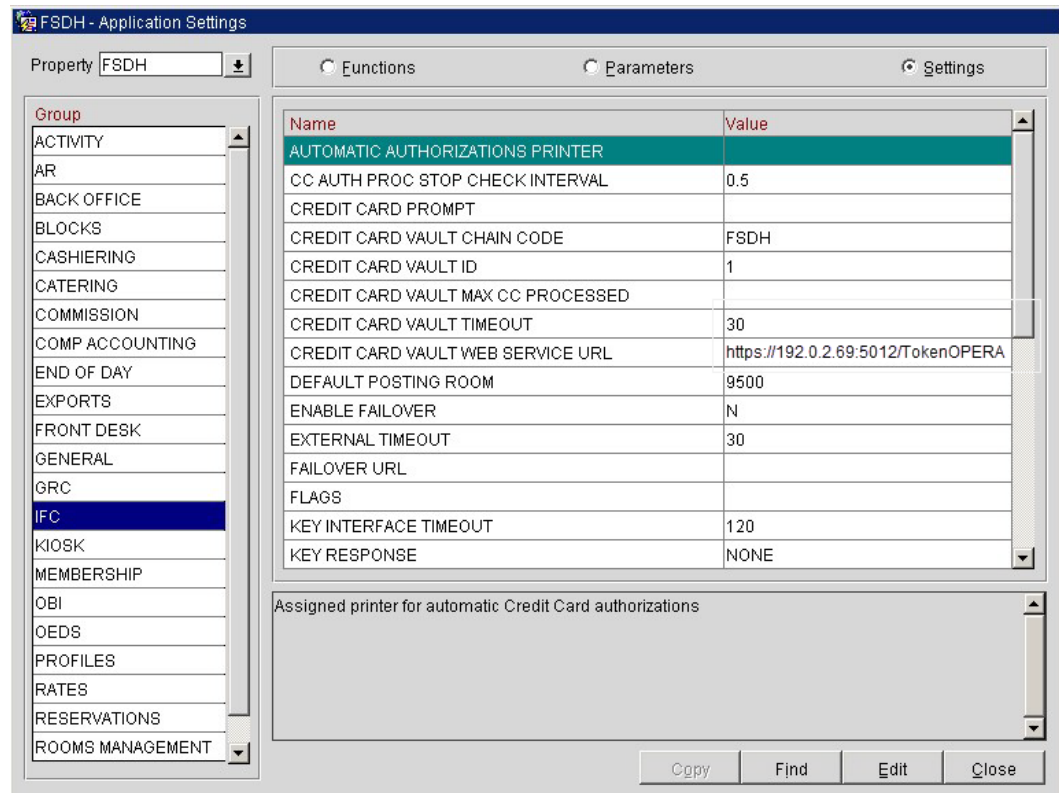
The CREDIT CARD VAULT WEB SERVICE URL should be in the format:

<https://OPIHostIP:OPITokenPortNumber/TokenOPERA>

The CREDIT CARD VAULT ID is currently not used.

The CREDIT CARD MAX CC PROCESSED is set to what the Payment Partner can support for the number of rows sent in one Token (GetID/GetCC) request. This is used during the bulk tokenization process and when multiple folio windows exist on OPERA Reservations. 50 is the default used when nothing is set here.

The CREDIT CARD VAULT TIMEOUT is set to the timeframe to wait for a response from the Token Proxy Service. At least 45 is recommended.



Application settings are changed based on the OPERA Version 5.5.0.18.1, 5.5.0.19 and 5.6.1.0 above.

These settings can be per property and these are moved to **Configuration | Setup | Property Interfaces | Interface Configuration | edit EFT IFC OPI | Custom Data tab.**

Token URL is moved to **Configuration | Setup | Property Interfaces | Interface Configuration | edit EFT IFC OPI | General.**

# Cashiering Overview

## Credit Card Payment Transaction Codes

1. In OPERA, go to **Configuration | Cashiering | Codes | Transaction Codes** to view the Credit Card Payments transaction codes setup.

The screenshot shows the '015 - Transaction Codes - Edit' window. The fields are as follows:

- Code: 9600
- Description: Visa Card
- Subgroup: CRED (Credit Cards)
- Group: Payments
- Trn. Type: [Dropdown]
- Adjustment Code: [Dropdown]
- Minimum Amount: [Text Box]
- Maximum Amount: [Text Box]
- Radio buttons: Credit Card (selected), Cash, Check, Others
- Radio buttons: EFT (selected), Manual
- CC Code: VA (Visa Card)
- AR Account: [Dropdown]
- CC Commission: 0.00 %
- Checkboxes:
  - Revenue Group: [ ]
  - Paidout: [ ]
  - Cashier Payments (1-8): [x]
  - Include in Deposit/CXL Rule: [ ]
  - Inactive: [ ]
  - Membership: [x]
  - Generates Inclusive: [ ]
  - AR Payments: [x]
  - Check No. Mandatory: [ ]
  - Manual Posting: [ ]
  - Deposit Payments: [x]
- Display Code: [Text Box]
- Buttons: Generates, OK, Close

2. Information for credit card payment transaction codes:
  - **EFT** selection is necessary to send credit card transactions out to the integrated payment partner for the specific Payment type.
  - **Manual** selection will not send out any transactions to the integrated payment partner.
  - **CC Code** will auto-populate once the transaction code is associated to a Payment Type.
  - **Display Code** can be populated to display a button when payment screen is accessed in OPERA PMS.

## Overview of Credit Card Payment Types

The credit card payment types link with the transaction code:

- In OPERA, go to **Configuration | Cashiering | Payment Types**.
  - The **IFC CC Type** field has the credit card code used such as MC, VA, AX.
  - The **Trn Code** field has the credit card transaction code.

## Credit Card Type Payment Setup Information

In order to link Card Types, the Credit Cards types below will need to be created and available in OPERA PMS.

### Sample List of Card Types

Payment Types - Customer Present (Chip & PIN)	Description	Capture Method
VA	Visa	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
MC	Mastercard	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
AX	American Express	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
DC	Diners Club	CP can be used. Transaction will go to the EMV (Chip & PIN) device.

<b>Payment Types - Customer Present (Chip &amp; PIN)</b>	<b>Description</b>	<b>Capture Method</b>
<b>JC</b>	JCB	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
<b>CU</b>	China Union Pay	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
<b>VD</b>	Visa Debit	CP cannot be used, manual card type selection is required. If CP is used, OPERA will default to Visa. Transaction will go to the EMV (Chip & PIN) device.
<b>MD</b>	Mastercard Debit	CP cannot be used, manual card type selection is required. If CP is used, OPERA will default to Mastercard. Transaction will go to the EMV (Chip & PIN) device.
<b>CD</b>	China Union Pay Debit	CP cannot be used, manual card type selection is required. If CP is used, OPERA will default to China Union Pay. Transaction will go to the EMV (Chip & PIN) device.
<b>MS</b>	Maestro	CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip & PIN) device. Customer present ONLY!
<b>VP</b>	V-Pay	CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip & PIN) device. Customer present ONLY!
<b>BC</b>	GiroCard	CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip & PIN) device. Customer present ONLY!
<b>AB</b>	AliPay	CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip & PIN) device. Customer present ONLY!

<b>Payment Types - Customer NOT Present (Keyed)</b>	<b>Description</b>	<b>Capture Method</b>
<b>KVA</b>	Visa Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>KMC</b>	Mastercard Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>KAX</b>	American Express Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)



<b>Payment Types - Customer NOT Present (Keyed)</b>	<b>Description</b>	<b>Capture Method</b>
<b>KDC</b>	Diners Club Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>KJC</b>	JCB Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>KCU</b>	China Union Pay Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>KVD</b>	Visa Debit Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>KMD</b>	Mastercard Debit	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>KCD</b>	China Union Pay Debit	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)

<b>Payment Types – One Shot Cards (Keyed) OPTIONAL!!!</b>	<b>Description</b>	<b>Capture Method</b>
<b>VVA</b>	Visa Virtual	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>VMC</b>	Mastercard Virtual	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
<b>VAX</b>	American Express Virtual	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)

## Individual Card Functions

<b>Payment Types - Customer Present (Chip &amp; PIN)</b>	<b>Authorization at Check-in</b>	<b>Pay Only (no Authorization)</b>	<b>Deposit Y/N</b>	<b>Cashier Payment Y/N</b>	<b>A/R Payment Y/N</b>
<b>VA</b>	Y	N	N	Y	N
<b>MC</b>	Y	N	N	Y	N
<b>AX</b>	Y	N	N	Y	N
<b>DC</b>	Y	N	N	Y	N

Payment Types - Customer Present (Chip & PIN)	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
JC	Y	N	N	Y	N
CU	Y	N	N	Y	N
VD	N	Y	N	Y	N
MD	N	Y	N	Y	N
CD	N	Y	N	Y	N
MS	N	Y	N	Y	N
VP	N	Y	N	Y	N
BC	N	Y	N	Y	N
AB	N	Y	N	Y	N

Payment Types - Customer <b>NOT</b> Present (Keyed)	Authorization at Check-in	Pay Only (no Auth)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
KVA	Y	N	Y	Y	Y
KMC	Y	N	Y	Y	Y
KAX	Y	N	Y	Y	Y
KDC	Y	N	Y	Y	Y
KJC	Y	N	Y	Y	Y
KCU	Y	N	Y	Y	Y
KVD	N	Y	Y	Y	Y
KMD	N	Y	Y	Y	Y
KCD	N	Y	Y	Y	Y

Payment Types – <b>One Shot Cards</b> (Keyed) <b>OPTIONAL!!!</b>	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
VVA	N	Y	N	Y	N
VMC	N	Y	N	Y	N
VAX	N	Y	N	Y	N

## Important Considerations

- Transaction codes for Chip & PIN, KEYED and VIRTUAL cannot be the same!
- SOLO cards does not exist anymore, and cannot be used.
- VISA ELECTRON and VISA DELTA should not be created as separate transaction / payments codes, these cards will fall under VISA.
- DISCOVER cards now fall under DINERS CLUB.
- VIRTUAL cards can only be VISA, MASTERCARD and AMERICAN EXPRESS.
- V-Pay, GiroCard and AliPay can only be Chip & PIN.

## Update OPI Configuration Merchant Tenders

Enter the OPERA payment code for each card type, and then click **Next**.

Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface - Configuration Wizard

Merchant Tender Configuration

OPERA Chain Code: FSDH

Property Code: FSDH

Tenders:

Card Type	Payment Code
AliPay	AB
Alliance	AL
American Express	AX
China UnionPay	CU
China UnionPay Debit	CD
Debit	DD
Diners Club	DC
Discover	DS
EC Chip	EC

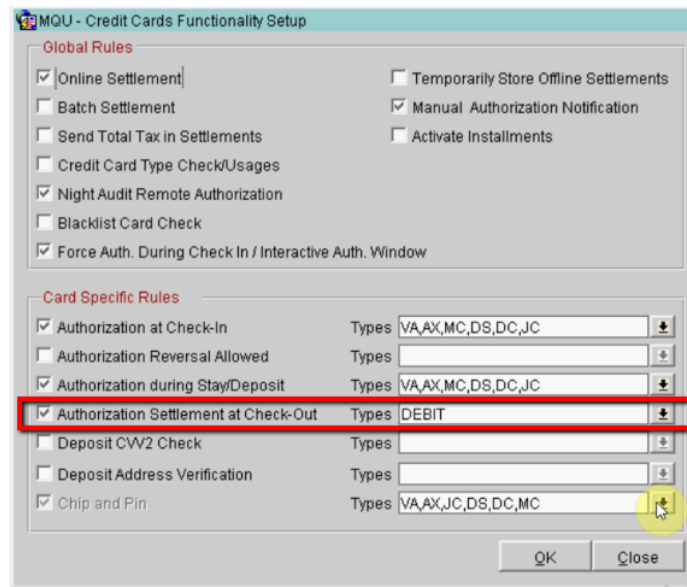
Hint: Double-click to edit a cell and then press Enter to submit your change or, Escape to cancel it

Back Next Cancel

ORACLE HOSPITALITY

## Update Functionality settings for Chip & Pin and PayOnly

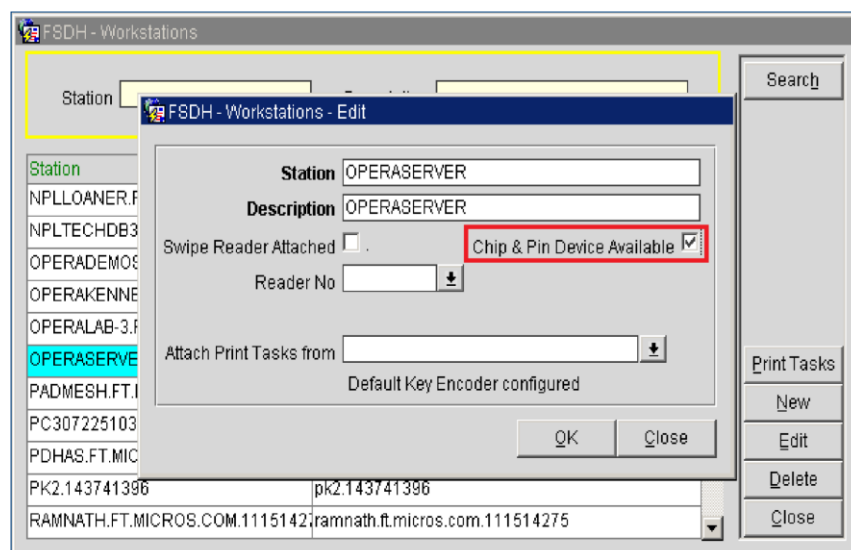
- Selection for Chip & Pin and PayOnly cards



## Configuring the Workstation

If the workstation is connected to a Chip & Pin terminal, the Chip & Pin Device Available check box must be enabled.

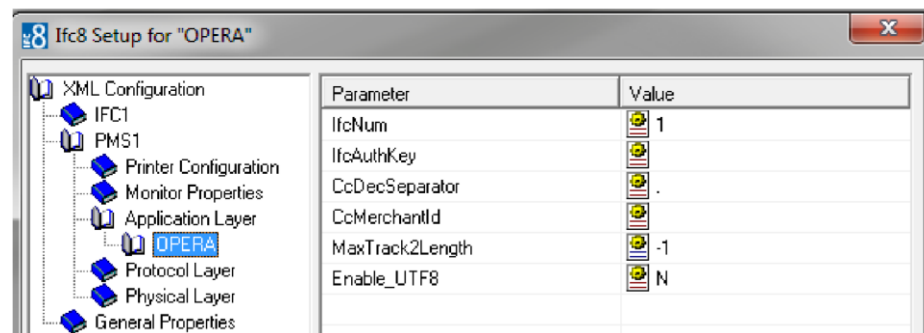
1. In OPERA | **Setup** | **Workstations** | edit your workstation.
2. Select the **Chip & Pin Device Available** check box to enable the device for this workstation (this allows the generic CP Payment Type to display in the LOV for a reservation).



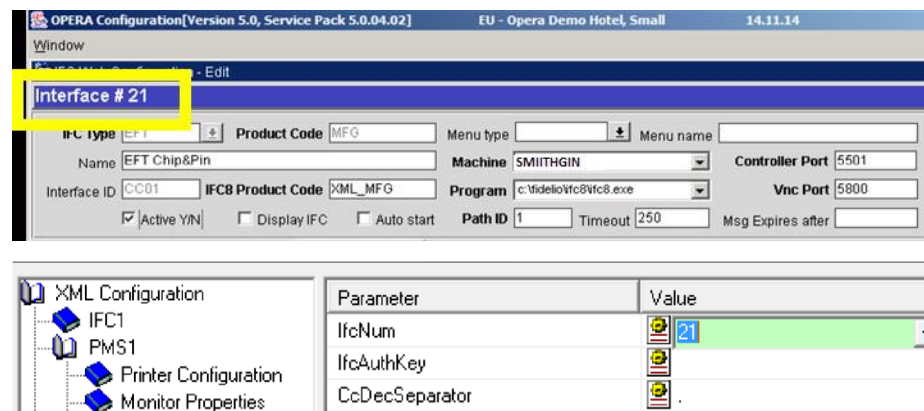
## Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC)

To configure the link between the interfaces:

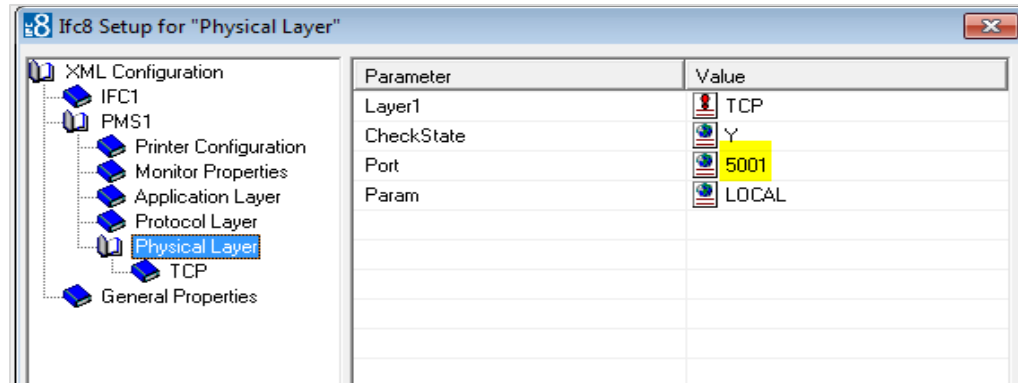
1. In the **Hotel Property Interface**, go to the **PMS1** tree and select **OPERA** in the application layer.
2. Enter the **OPERA IFC** number in the parameter **IfcNum** value.



You can find the OPERA IFC number in OPERA on the IFC Configuration of the related Hotel Property Interface (IFC) (Row\_ID).



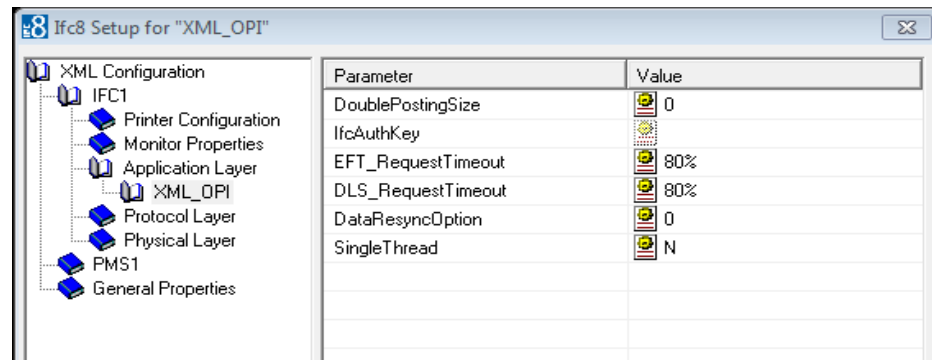
3. Go to the **PMS1** tree in the **Physical Layer**.
4. Enter the port number into Parameter value **Port**. This is the port IFC8 uses to communicate with the OPERA IFC controller.
5. Select **Enter** and **Apply** to re-initiate IFC8, and then click **Save**.



## Configuring Authentication for the Hotel Property Interface (IFC8) with OPI

You must secure the connection between OPI and Hotel Property Interface (IFC8) by exchanging encryption keys at startup. This authentication key must be defined by OPI. The corresponding key must be entered in the Hotel Property Interface (IFC8) configuration.

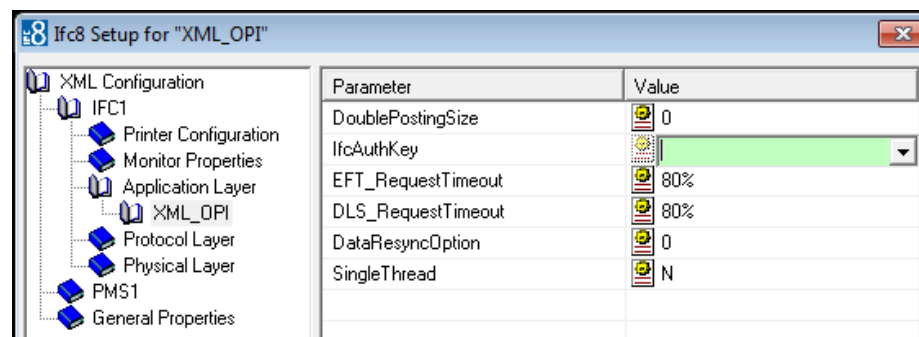
1. In the Hotel Property Interface (IFC8) configuration, go to the **IFC1** tree, and then in the **Application Layer**, select the **XML\_OPI** option.



2. Copy the [generated key](#) from Configuring OPI - OPERA merchant step 3, and add "FidCrypt0S|" to the generated key as prefix.

For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

3. Copy this string into IFC8 Parameter **IfcAuthKey** value field.



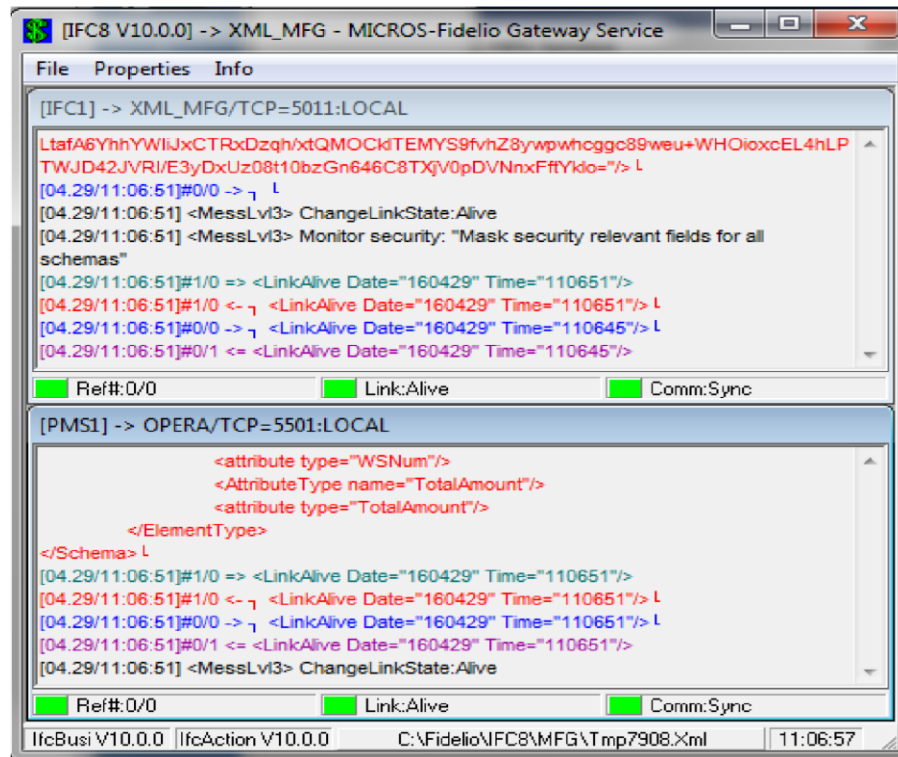
IfcAuthKey	j011kVJMO23gJzjBw4QTb4
Parameter	Value
DoublePostingSize	0
IfcAuthKey	FidCrypt0SjG8Zbw5SNDQ0I1...
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0

4. Go to **IFC1** tree and select the **Physical Layer**.
5. Enter the port number in port value. This is the same port that was configured in OPI.

Parameter	Value
Layer1	TCP
CheckState	Y
Port	5007
Param	LOCAL

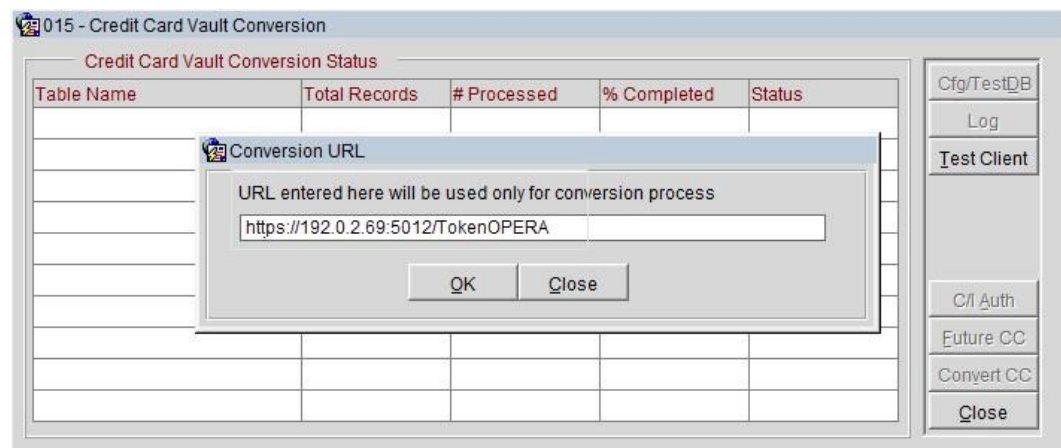
6. Click **Apply**, IFC8 reinitiates.
7. The **IfcAuthKey** value now shows an encrypted key and the entered string is now encrypted by IFC8.
8. Click **Save**, and then click **OK** to close the IFC8 Configuration form.

IFC8 now connects with OPI and OPERA IFC Controller. To verify IFC8 successful status, confirm that all 6 status indicators are green.



## Perform a Tokenization

*Utilities -> Convert CC -> Convert Vault CC Information -> Test Client*

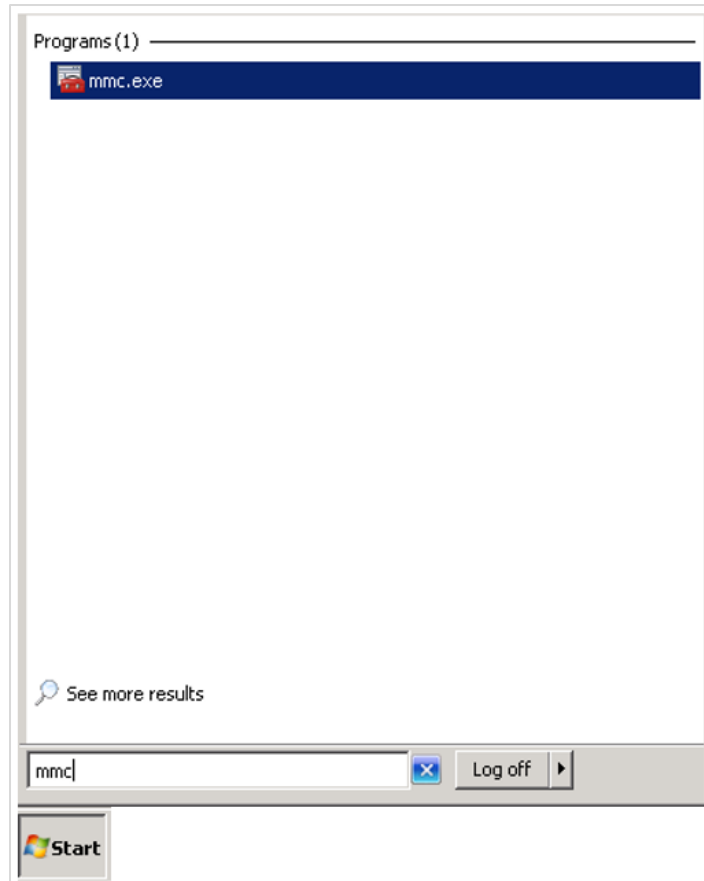


Complete the **Test Client** conversion to enable the **Credit Card Vault Conversion** functions.

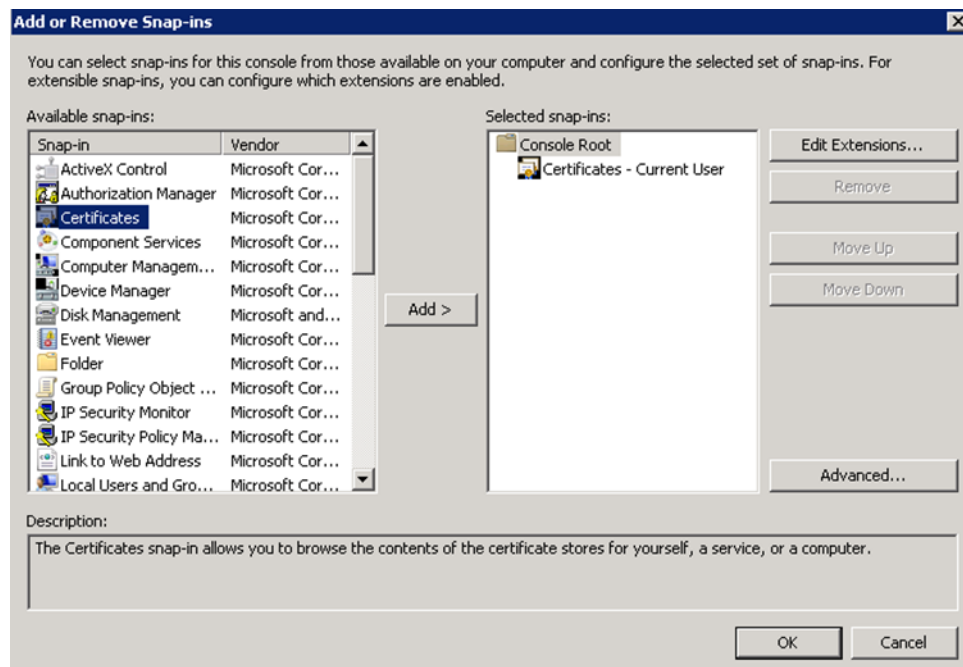
## Certificate Import using Microsoft Management Console

1. Find and open mmc.exe from Start menu.

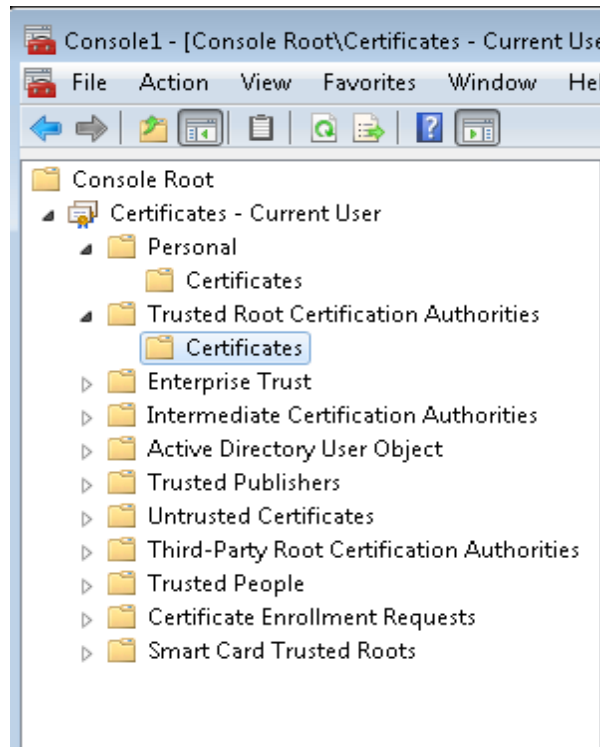




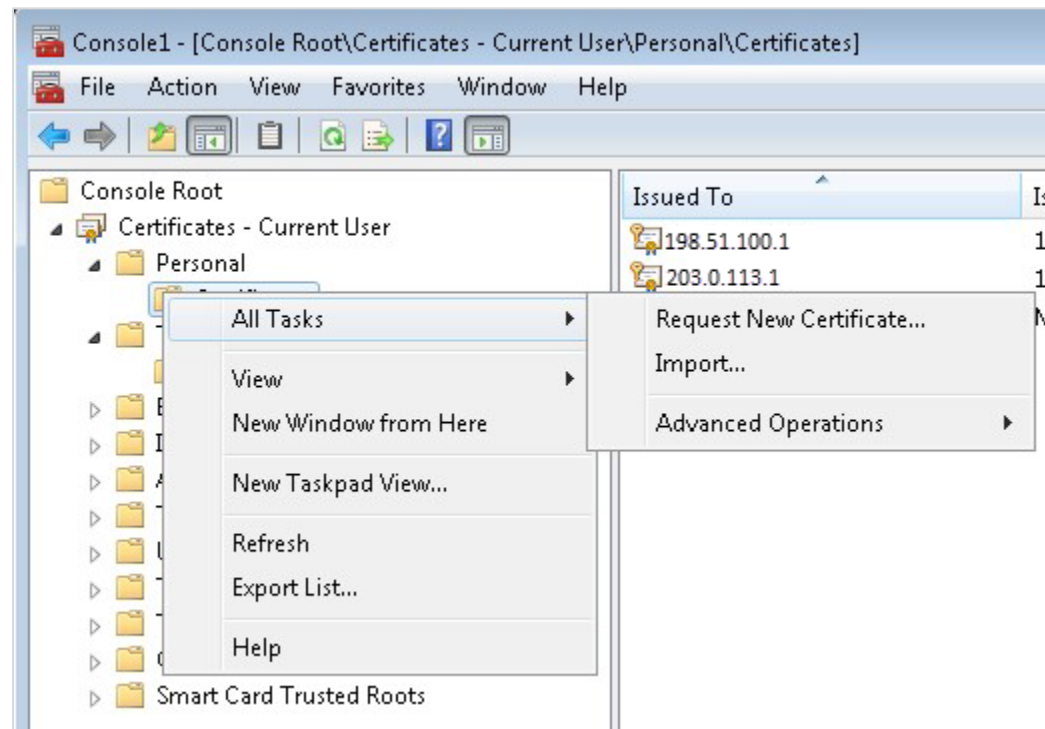
2. Go to **File | Add or Remove Snap-ins**, add certificates to **Selected snap-ins**, and then click **OK**.



- Expand Certificates, expand Personal or Trusted Root as required, and then select **Certificates**.



- Right-click **Certificates**, select **All Tasks**, and then select **Import**.



- On the Certificate Import Wizard Welcome page, click **Next**.

- Browse to the location of the certificate file, and then click **Next**.
- If required enter the password relevant to the certificate you are importing, and then click **Next**.
- If the import is successful, then the certificates Common Name will be listed under the folder that was selected during import.

# 4

## Upgrading the OPI

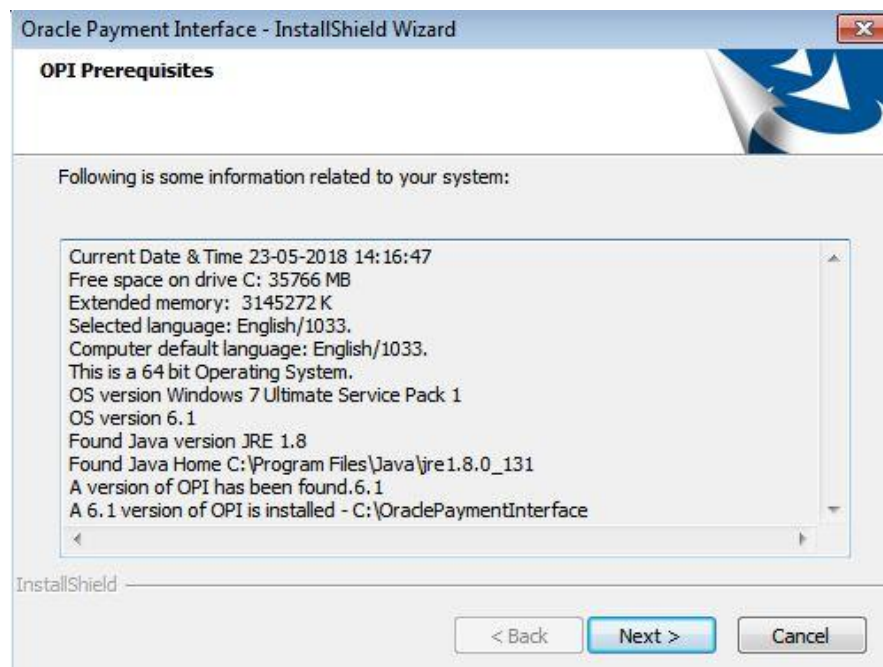
**VERY IMPORTANT:** Read and follow the upgrade directions.

 **NOTE:**

OPI 6.1 and higher can be upgraded to OPI 19.1

### OPI 6.1 to 19.1.0.0 Upgrade Steps

1. Right-click and Run as Administrator the `OraclePaymentInterfaceInstaller_19.1.0.0.exe` file to perform an upgrade.
2. Select a language from the drop-down list, and then click **OK**.
3. Click **Next** on the Welcome screen to proceed with the installation.  
Prerequisites for the installation will be checked, including the required free drive space, details of the host environment, and the Java version that is present.
4. Click **Next** on the OPI Prerequisites screen.



5. Click **OK** on the OPI Upgrade screen.



**6. WARNING!** You must click **Yes**.

IF YOU CLICK NO, YOU WILL HAVE BOTH OPI 6.1 AND OPI 19.1 INSTALLED AND NEITHER WILL WORK.

**Explanation:** OPI will migrate the existing MySQL configuration information, but all previous OPI applications will be removed before the new files are installed.

**7.** Choose a Destination Location. Accept the default installation location or click **Change...** to choose a different location.

**8.** Click **Next**.

The Ready to Install the Program screen displays.

**9.** Click **Install**.

The Setup Status screen displays for a few minutes.

### Setup Type

For database type, select MySQL. No other database type is supported for upgrades.

### Database Server

Name/IP: The Hostname or IP Address used for communication to the MySQL database. This must be left at the default of localhost.

Port #: The Port number used for communication to the database

### Database Server Login

DBA user

Login ID: root

Password: root user password for MySQL database.

### Database User Credentials

User Name: This must be a new user name. It cannot be the same user from the 6.1 install.

Password: Password for the new database user.

### Configuration Tool Superuser Credentials

User Name: This can be any user name. It does not have to be a Windows account user.

Password: Create a password, and then confirm it.

### Configuration Tool Connection Settings

Host: Enter the IP address or server name of the PC where the OPI Config Service is installed. This will be the PC where you selected “OPI Services” to be installed.

Port: Leave at 8090.

### Configuration Tool Passphrase

Enter and confirm a passphrase.

Click **Next**.

The Configuration Wizard launches.

Continue to follow on-screen directions, verifying settings as you go.

### PMS Merchants

On the Merchants screen, click the wrench icon to the right of the existing merchant.

Verify the merchant settings are correct.

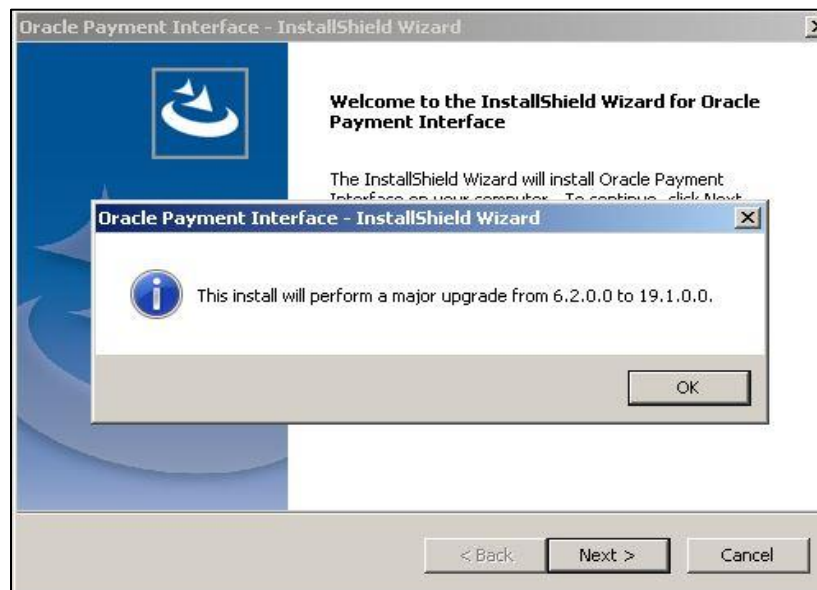
### InstallShield Wizard Complete

Click **Finish** to allow a reboot.

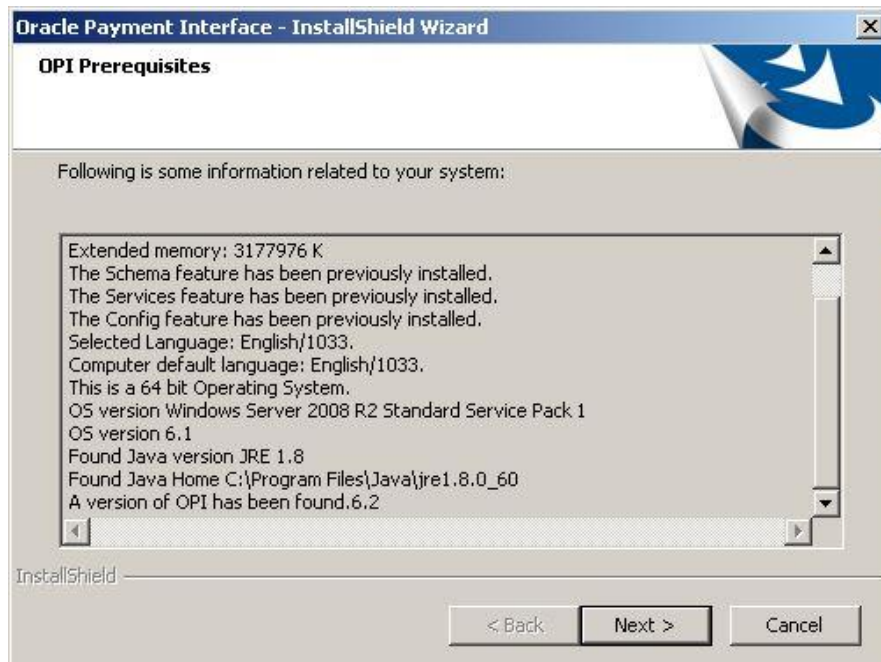
If you cannot immediately reboot, you must stop and then start the OPI Service for the current settings to take effect.

## OPI 6.2 to 19.1.0.0 Upgrade Steps

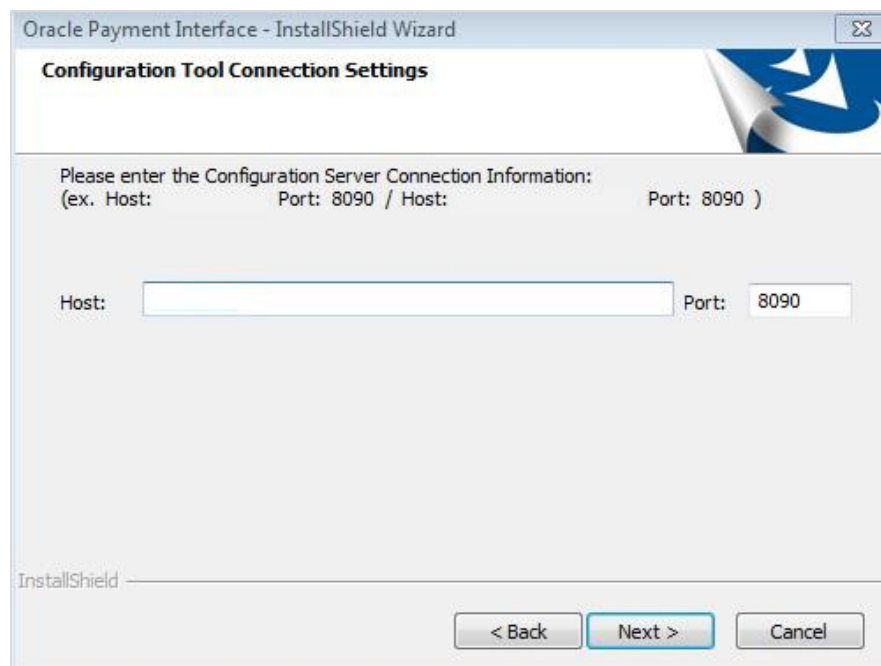
1. Right-click and Run as Administrator the OraclePaymentInterfaceInstaller\_19.1.0.0.exe file to perform an upgrade.
2. Select a language from the drop-down list, and then click **OK**.
3. Click **Next** on the Welcome screen to proceed with the installation.



4. Click **Next** on the OPI Prerequisites screen.



5. Choose a Destination Location. Accept the default installation location or click **Change...** to choose a different location and click **Next**.
6. Click **Install**. When The Ready to Install the Program screen displays.
7. Click **OK** when The Database upgrade operation was successful screen displays.
8. Enter the configuration Server connection information.



9. Click **Finish** to restart your computer.

