

Oracle Hospitality Payment Interface OPERA V5 OPI Installation and Reference Guide



Release 20.4
F35751-04
February 2024

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

ORACLE®

Oracle Hospitality Payment Interface OPERA V5 OPI Installation and Reference Guide Release 20.4

F35751-04

Copyright © 2010, 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 Steps	1-1
<hr/>	
2 Installing the OPI	2-1
<hr/>	
Token Exchange Settings	2-10
Certificates	2-11
<hr/>	
3 OPERA Configuration	3-1
<hr/>	
Creating an EFT Interface	3-1
Configuring CHIP AND PIN (EMV)	3-2
Configuring the CC Vault	3-5
OPERA Payment Widget Configuration	3-6
Cashiering Overview	3-7
Overview of Credit Card Payment Types	3-8
Credit Card Type Payment Setup Information	3-8
Activating and Using the Payment Service Directive (PSD2) Control	3-18
Configuring the Workstation	3-22
Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC)	3-22
Configuring Authentication for the Hotel Property Interface (IFC8) with OPI	3-24
Perform Bulk Tokenization	3-26
Configuring OPI for Hotel Mobile or OWS/Kiosk Setup in OPERA	3-38
<hr/>	
4 Upgrading the OPI	4-1
<hr/>	
Upgrading OPI 6.2.0.0 to 20.3.0.0	4-1
Upgrading OPI 19.1.0.0 to 20.3.0.0	4-3
Upgrading OPI 20.1.0.0 to 20.3.0.0	4-4
Upgrading OPI 20.2.0.0 to 20.3.0.0	4-6
<hr/>	
5 OPERA Folio Print Receipt Setup for OPI	5-1
<hr/>	
Setup in OPERA PMS	5-1
OPERA Folio Print Receipt Setup for OPI	5-1
Verifying Folio information in OPERA PMS	5-5

Preface

Purpose

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

Audience

This document covers the installation of OPI, as well as the OPERA and IFC8 Configuration needed to support OPI.

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 Revision History

Date	Description
July 2020	<ul style="list-style-type: none">• Initial publication.
November 2020	<ul style="list-style-type: none">• Updated for release 20.3
April 2021	<ul style="list-style-type: none">• Added new feature Payment Services Directive (PSD2) control.• Updated Perform Bulk Tokenization section with content and screens.• Added new chapter OPERA Folio Print Receipt Setup for OPI.
October 2021	<ul style="list-style-type: none">• Updated the Certificates section with correct OPERA release versions

Date	Description
March 2022	<ul style="list-style-type: none">Updated content in Configuring the CC vault section
March 2023	<ul style="list-style-type: none">Updated content for IFC set up details in the Pre-Installation Steps chapter
May 2023	<ul style="list-style-type: none">Updated the Customer Support section with the new support portal name and URL
October 2023	<ul style="list-style-type: none">Removed the MySQL 5.6 version across the document as the OPI installer no longer supports
January 2024	<ul style="list-style-type: none">Updated content in Certificate Import using Microsoft Management Console
February 2024	<ul style="list-style-type: none">Added Windows 2022 in Pre-Installation Steps section

1

Pre-Installation Steps

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

- Minimum OPERA Property Management Systems (for V5 Hosted) releases you can integrate with OPI:
 - OPERA V5 Hosted 5.5.0.25.8 or higher
 - OPERA V5.6.6 or higher
 - OPERA V5 On Premise 5.5.0.24.4 or higher
- OPI 20.3 does not install a database. If you are doing a clean install of OPI, a database must be installed first.
- You cannot upgrade directly from OPI 6.1 to OPI 20.3.
- OPI upgrade functionality supports:
 - Upgrading OPI 6.2 (include patch releases) to OPI 20.3
 - Upgrading OPI 19.1 (include patch releases) to OPI 20.3
 - Upgrading OPI 20.1 (include patch releases) to OPI 20.3
 - Upgrading OPI 20.2 (include patch releases) to OPI 20.3
- OPI requires 64bit Operating System only.
- OPI requires at least 6 GB of free disk space and you must install OPI as a System Administrator.
- The Oracle Payment Interface Installer release 20.3 supports the following database connections:
 - MySQL Database 5.7 / 8.0
 - Oracle Database 11g / 12c / 19c

NOTE:

Stay current by upgrading your Java version as [Oracle CPUs/Alerts](#) are announced.

- The Oracle Payment Interface release 20.3 is compatible with the following operating systems:
 - Microsoft Windows 10 Professional
 - Microsoft Windows 10 Enterprise
 - Microsoft Windows 11 Professional
 - Microsoft Windows 11 Enterprise
 - Microsoft Windows Server 2012 R2

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

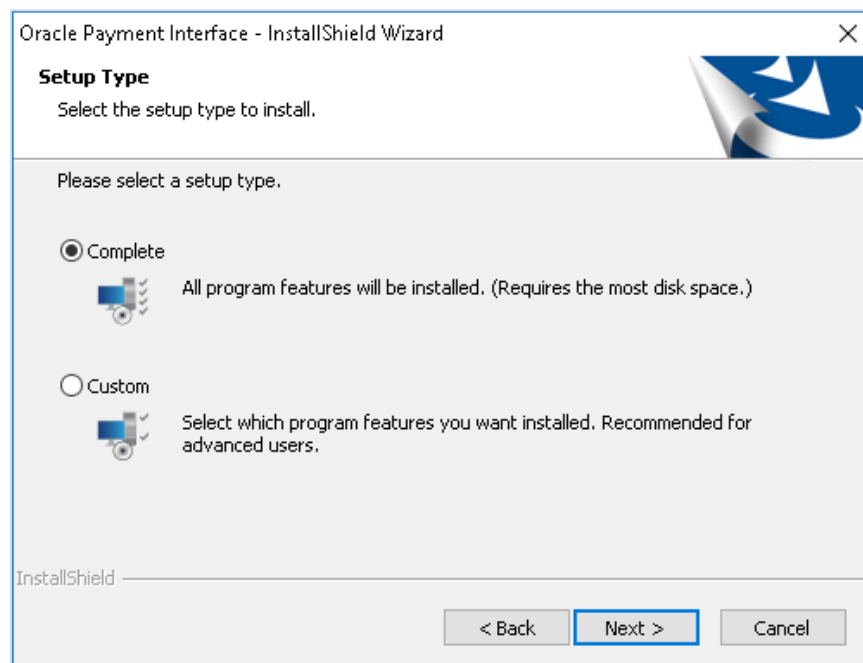
During the installation you must confirm the following:

- Merchant IDs
- IP address of the OPI Server
- The machine running the OPI Service must have a static IP Address
- The machine name running the OPI Service and IFC8 must not contain any special characters
- If there is an existing MySQL database installed, then the SQL root password is required.
- If there is an existing database installed, the root password is required.
- Workstation IDs and IPs that integrate with the PIN pad.

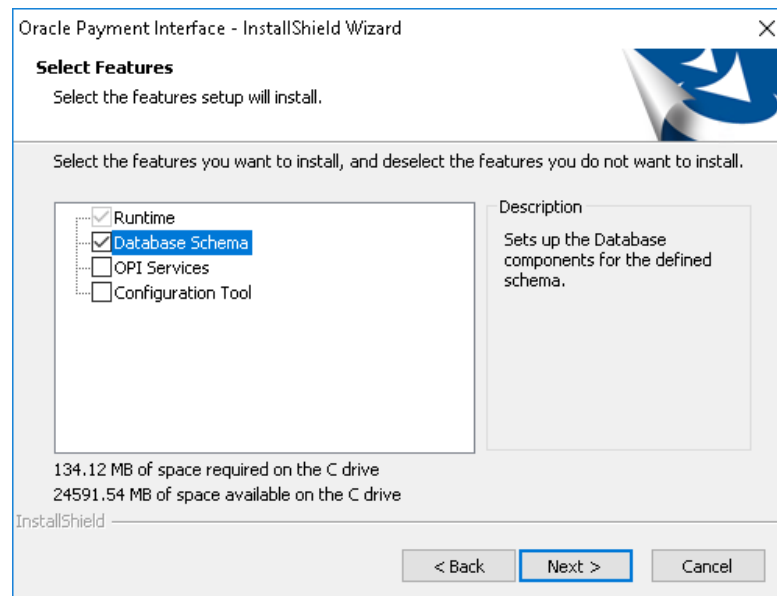
2

Installing the OPI

1. Right-click **OraclePaymentInterfaceInstaller_20.3.0.0.exe** file and select **Run as Administrator** to perform an installation.
2. Select your language from the drop-down list, and click **OK**.
3. Click **Next** twice.
4. Ensure all the prerequisites for the OPI installation are met.



5. Select either the **Complete** or **Custom** installation option:
 - a. **Complete:** All program features will be installed.
 - b. **Custom:** Select which program features you want to install. Recommended for advanced users only.
6. Make a selection (only for Custom install), and click **Next**. If you select Complete Install, it will go to the Step 8 directly.



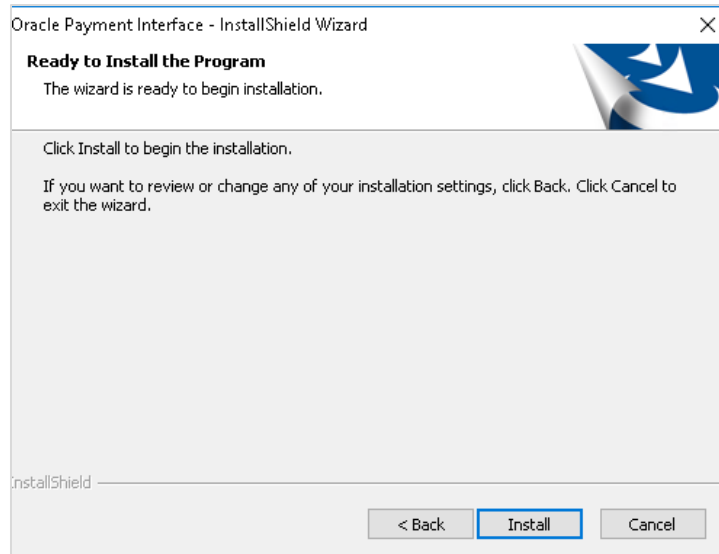
If you selected the Custom install option, the Select Features screen appears with the following options:

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

All these three features must be installed. Ensure whether they all are installed on the same computer or on separate computers.

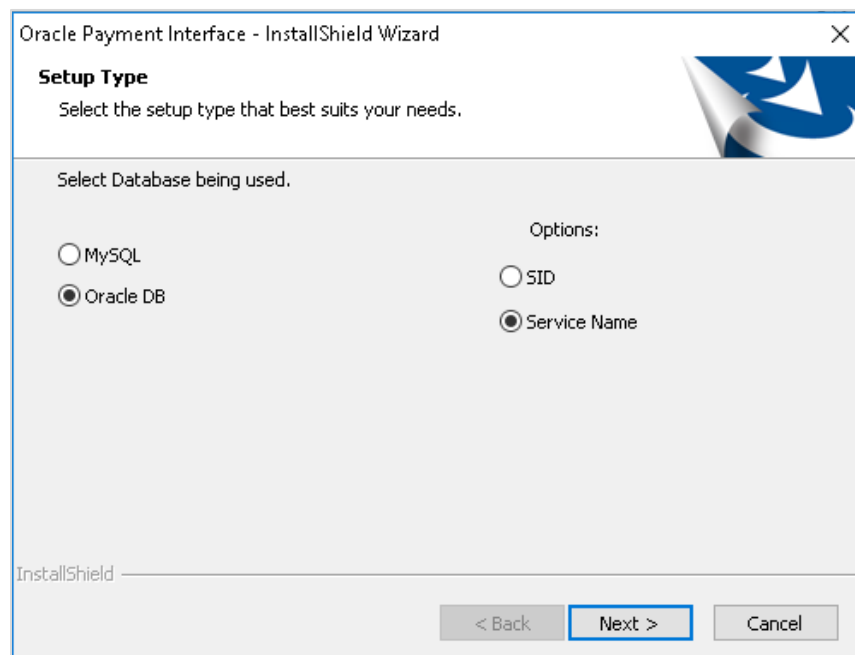
7. Select the features to install on this computer, and click **Next**.
8. Click **Change** to amend the installation drive or path, if required and click **Next**.
9. Click **Install** to begin installation.

When the file transfer is finished, Setup prompts for the next set of configuration settings.



10. Select your Database type:

- My SQL
- Oracle DB



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

 **NOTE:**

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

MySQL

- **Name/IP:** The Hostname or IP Address used for communication to the database. If you are using MySQL, then this can be left as localhost as the default value. If you cannot use localhost for the Name/IP field (because you have installed the database schema on another computer), then you should run some commands manually on the MySQL database before proceeding. See the **Granting Permission in MySQL** section in the OPI Installation and Reference guide for instructions. Setup will not be complete if this step is missed.
- **Port #:** The Port number used for communication to the database.

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.

12. 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.
13. Enter the username and password to create a new database user account. If the username already exists in the database, you are prompted to select a different username.
 - a. When creating the username for the database, the installer allows only alphanumeric characters and should start only with an alphabetic character, NOT a number.
 - b. Enter a password according to the requirements specified.

The installer attempts to connect to the database using the admin credentials provided and creates the OPI database user.

14. Enter the username and password to create a Super User System Admin level account that is used for configuring and maintaining the system.
15. Enter the **Host** and **Port**.

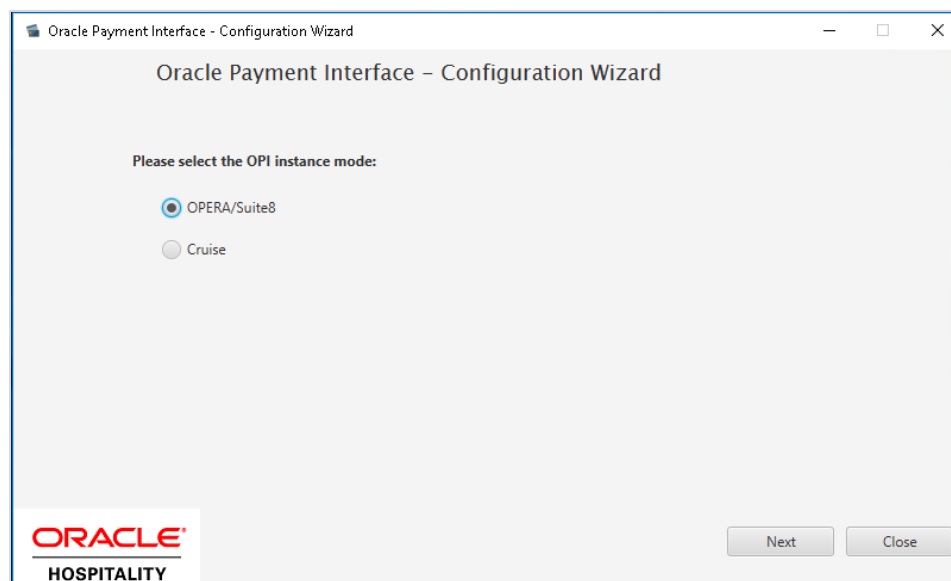
 **NOTE:**

In the previous step you are not configuring the port the service will listen on. Instead, it is prompting for the details on how to connect.

- The IP will depend on where the OPI Config Service is installed. If you are performing a complete installation, this can be left as the localhost address.
- The default port is 8090.

16. Set and confirm the passphrase value.

If the details entered for the connection to the **OPI Config Service** are correct, then the OPI installer launches the configuration wizard.



17. Select the OPI instance mode for Property Management System (PMS) merchants as **OPERA/Suite8**.

On the **OPI Interface** screen, the configuration screens displayed are same when the configuration wizard is launched manually.
(:\OraclePaymentInterface\v20.3\Config\LaunchWizard.bat)

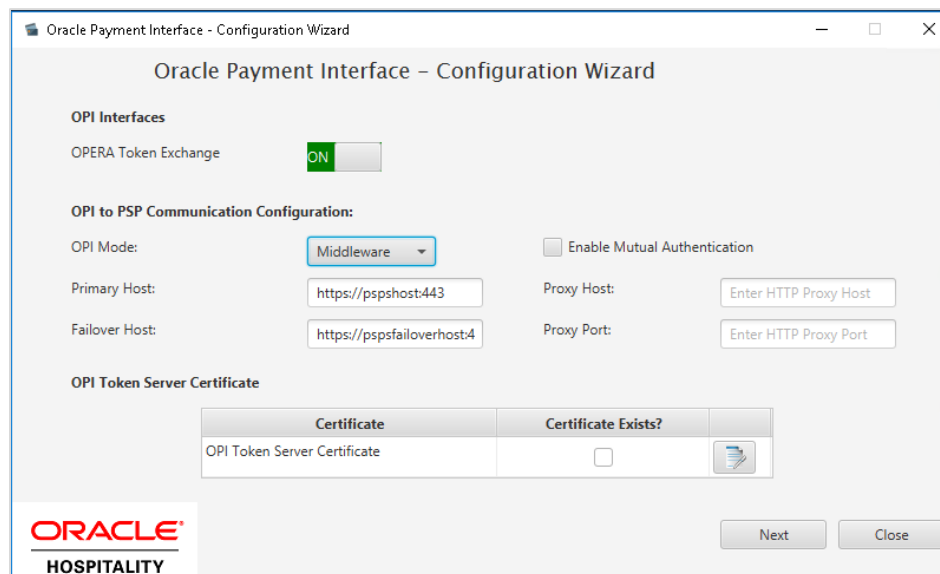
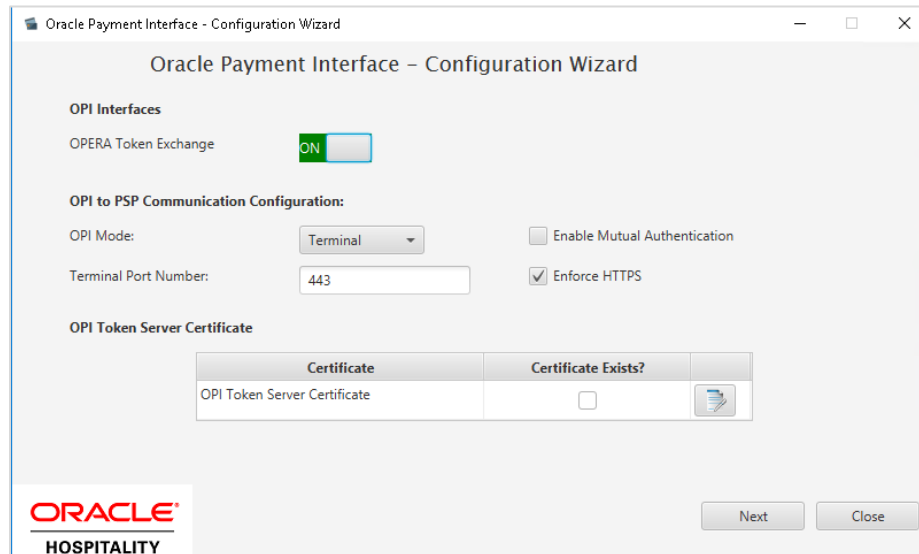
18. OPERA Token Exchange: This option is enabled by default for all OPERA token exchange services.

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.

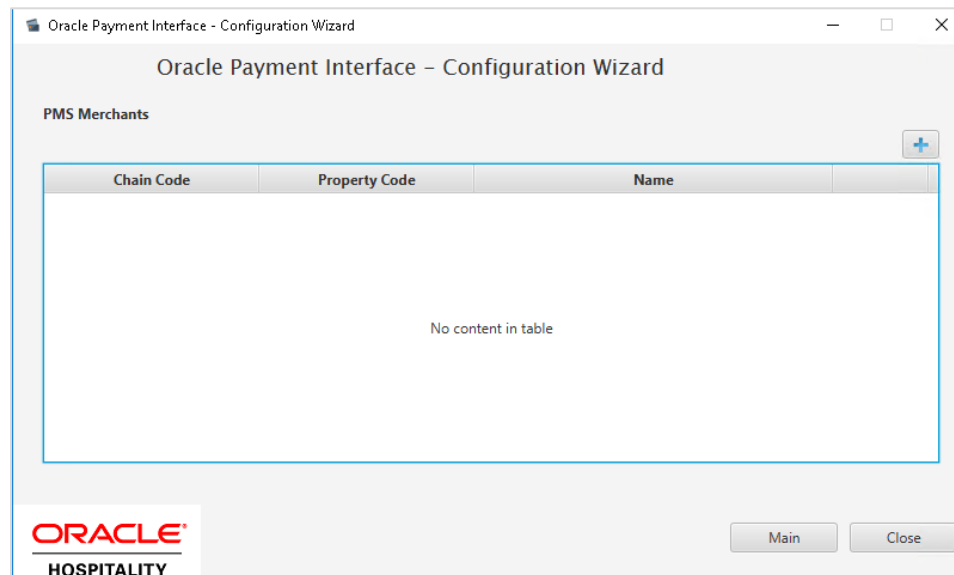
 **NOTE:**

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.



- **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.
- Enter the third-party payment service provider middleware Host address if **Middleware** mode is selected. If the **Terminal** mode is selected, OPI configuration will populate another window in further steps to input Workstation ID and IP address.

19. Click the **Add** () icon to add a new merchant configuration for OPERA.



20. To configure the OPERA merchant, enter the following information:
- a. The **OPERA Vault Chain Code** and **Property Code**; will form the **Siteld** value in the Token request messages.

 **NOTE:**

Chain Code and **Property Code** values need to be in upper case.

- b. Select **Generate Key**. Use to generate an IFC8 Communication key. The generated key will have the prefix **FidCrypt0S|** that is automatically added. Use this generated key when configuring the key in IFC8 software.
- c. Enter the **IFC8 IP address** and **port** number for the Hotel Property Interface (IFC8) server.
- d. Enter the Merchant **Name**, **City**, **State/Province** and **Country/Region** information.
- e. **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's 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. **Reset**: To reset the currency back to use country/region currency.
- f. Select the option **Only Do Refund** if you want to disable differentiating between void and refund from OPERA.

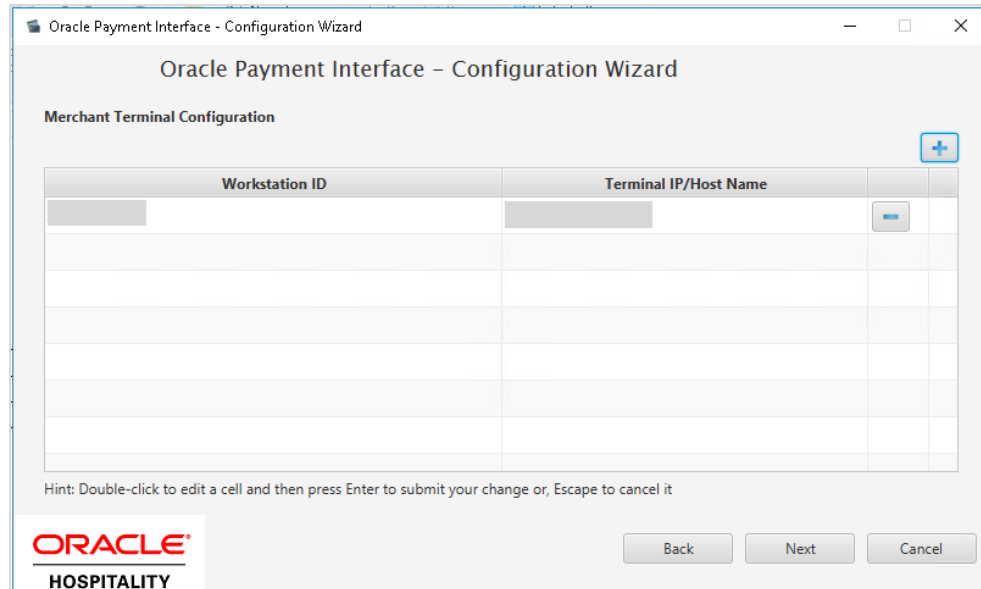
g. Click Next.

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

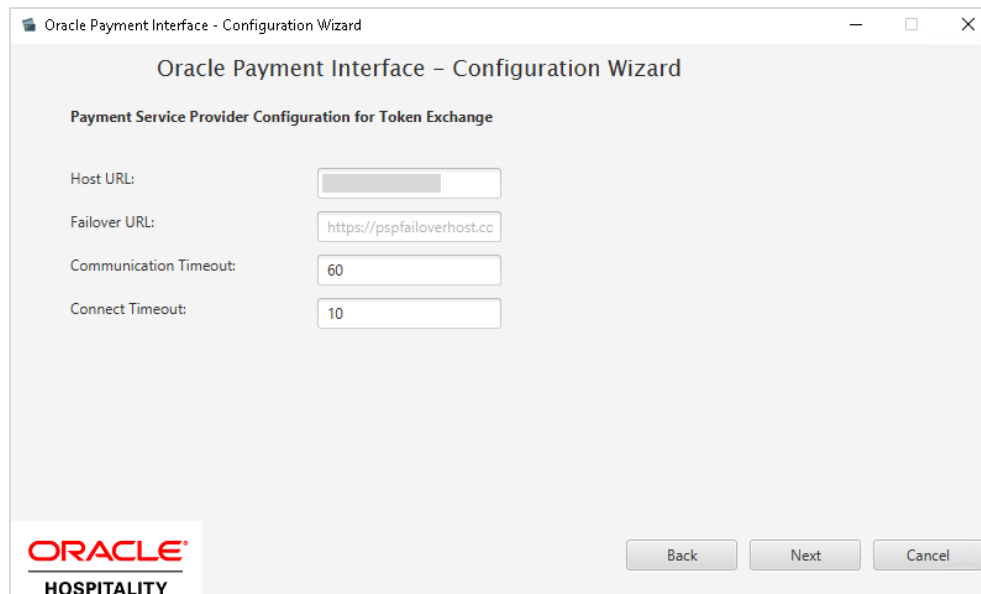
21. Enter the OPERA payment code for each card type, and click Next.

Card Type	Payment Code
Gift Card	GC
GiroCard	BC
JCB	JC
Maestro	ME
MasterCard	MC
MasterCard Debit	MD
MIR	MI
Paypal	PC
Reserve-01	ZZ

Below is terminal mapping if you select Terminal mode.



22. 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 click **Next**.



23. Click **Finish** to restart.

Token Exchange Settings

The Token Exchange Configuration settings allows you to configure the Authentication credentials used in communications from OPERA→OPI.

OPERA to OPI Communication Configuration

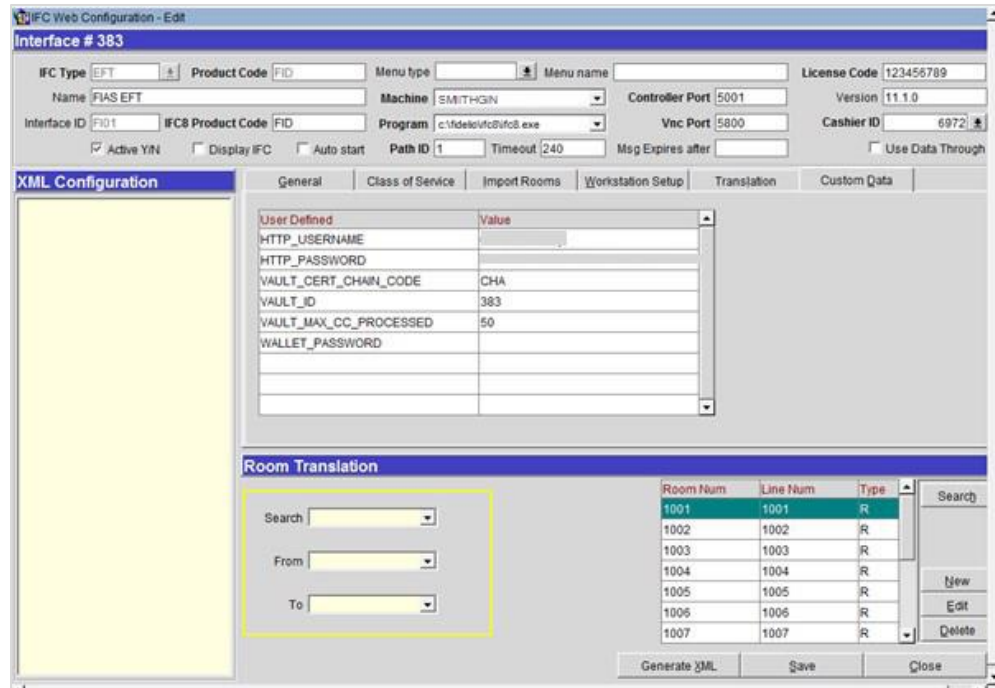
- Run `\\OraclePaymentInterface\v20.3\Config\LaunchConfiguration.bat`.
- Login with the Super user account created during OPI installation.
- Select **Merchants** tab, and click **Token Exchange Settings** subtab.

The screenshot shows the Oracle Payment Interface configuration page for a PMS Merchant. The 'Token Exchange Settings' subtab is active. It contains three password fields: 'Authentication User', 'Authentication Password', and 'Confirm Password'. Below these is a 'Certificates' section with a table:

Certificate	Certificate exists?
OPERA Token Certificate	<input type="checkbox"/>

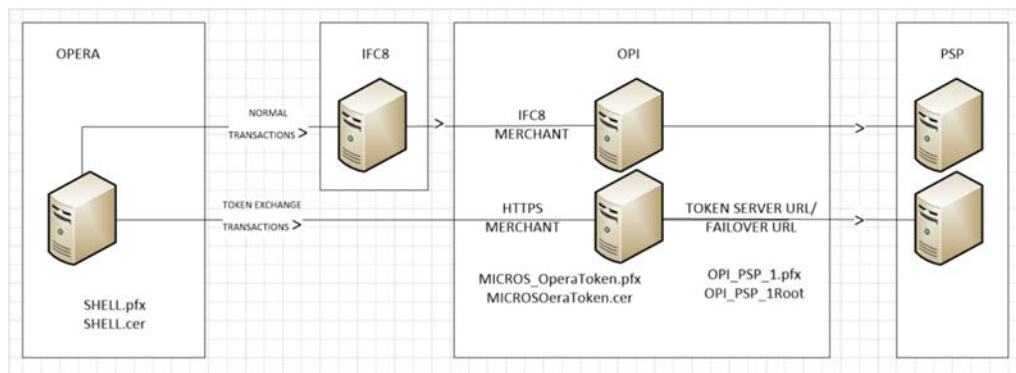
- **Authentication User:** The username for OPERA Authentication.
- **Authentication Password:** The password for OPERA Authentication.
- **Confirm Password:** The password for OPERA Authentication.

The details provided here 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.
- Click **Save**.

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 below sections for further details.

PSP - Client Side Certificates

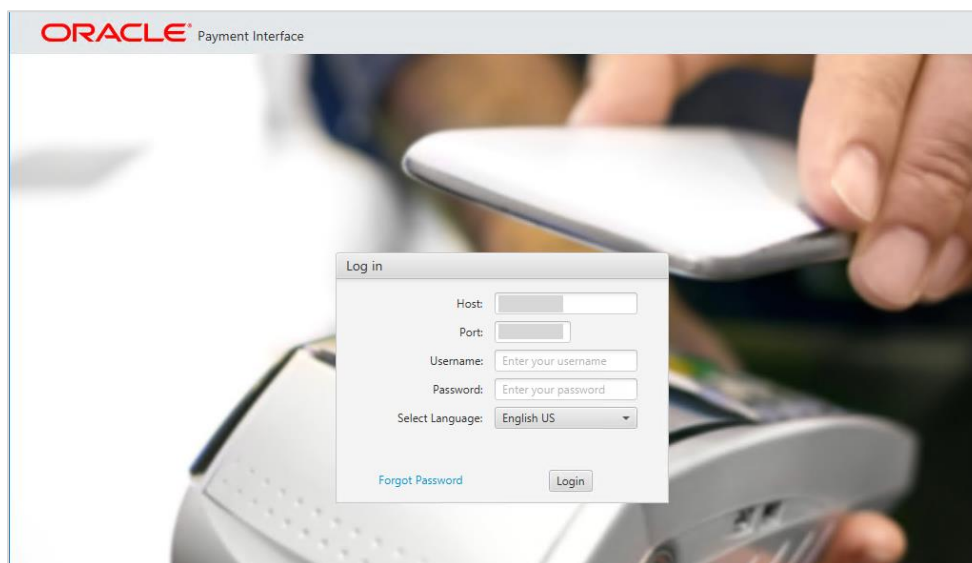
The communication from OPI to the PSP for the token exchange uses HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed on PSP (server side) for HTTPS communication, the PSP is also expected to provide a client side certificate to be deployed on OPI side. OPI provides the 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 on 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 on PSP side. The root certificate file provided by the PSP should be in the format of .cer or .crt.

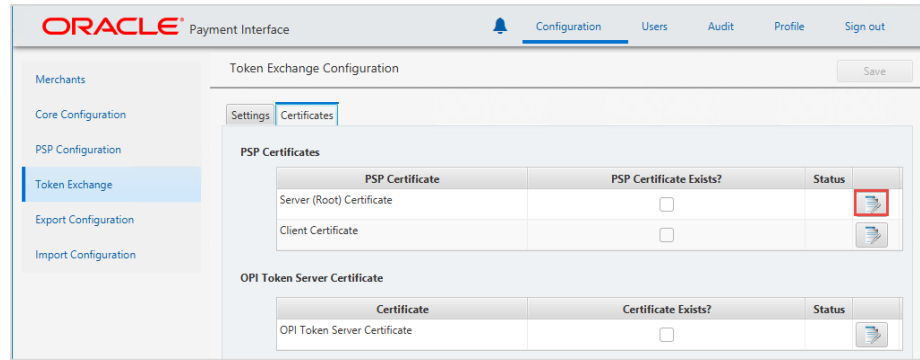
To deploy the client certificate on the OPI side:


1. Run `\\OraclePaymentInterface\20.3\Config\LaunchConfiguration.bat`
2. Login with the Super user account created during OPI installation.

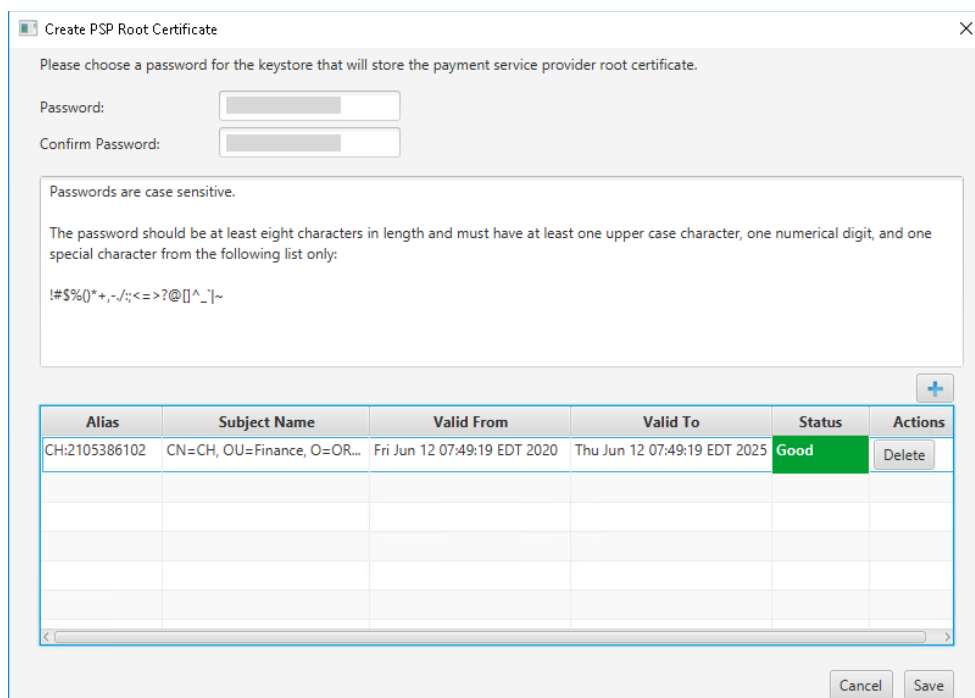


Handling the Root Certificate File by OPI Configuration Tool.

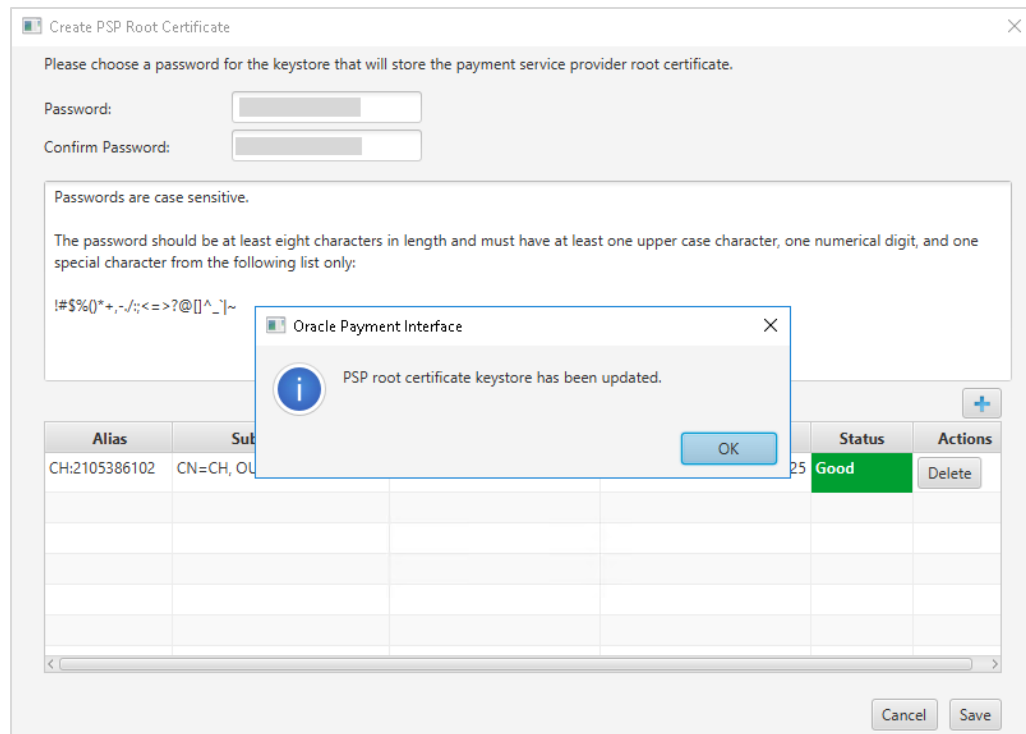
1. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Server (Root) Certificate**.



2. 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.



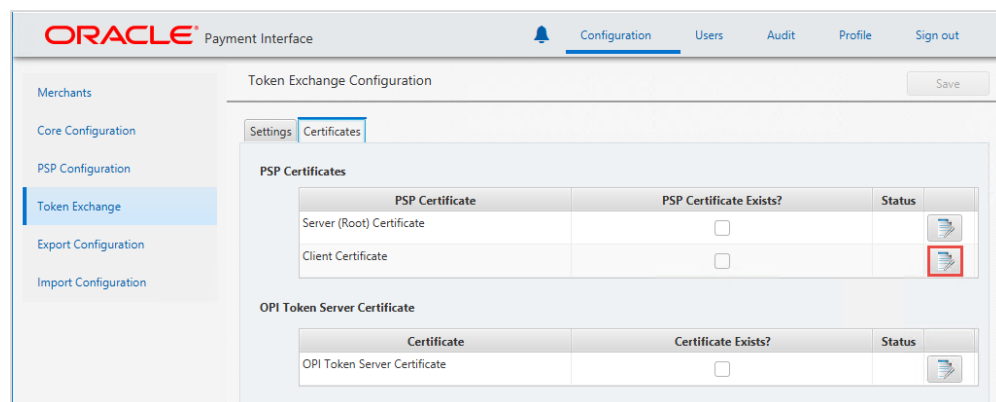
3. Click **Save**.



OPI_PSP_1Root is created under \OraclePaymentInterface\v20.3\Services\OPI\key

Handling the Client Side Certificate

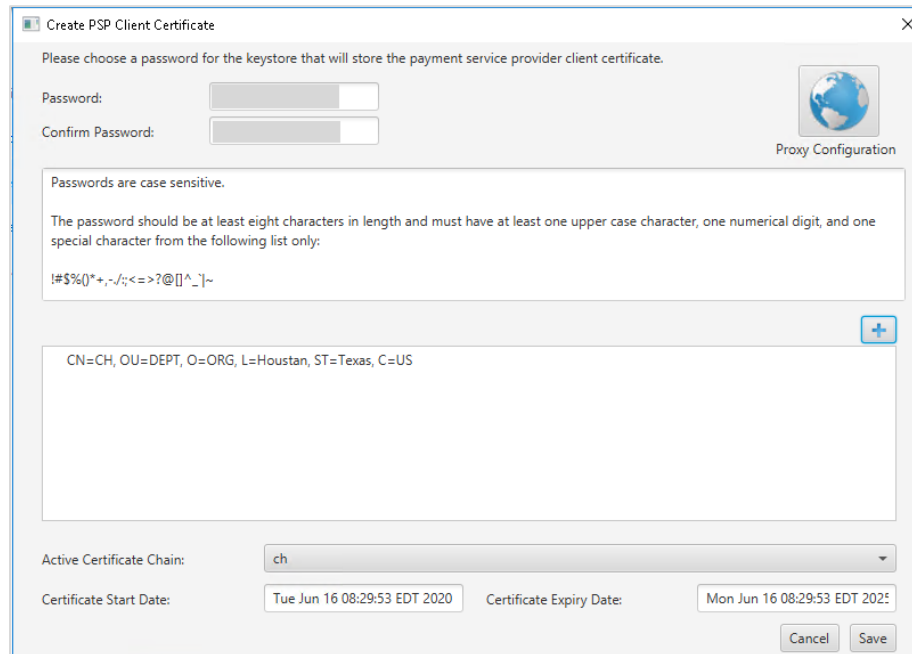
1. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Client Certificate**.



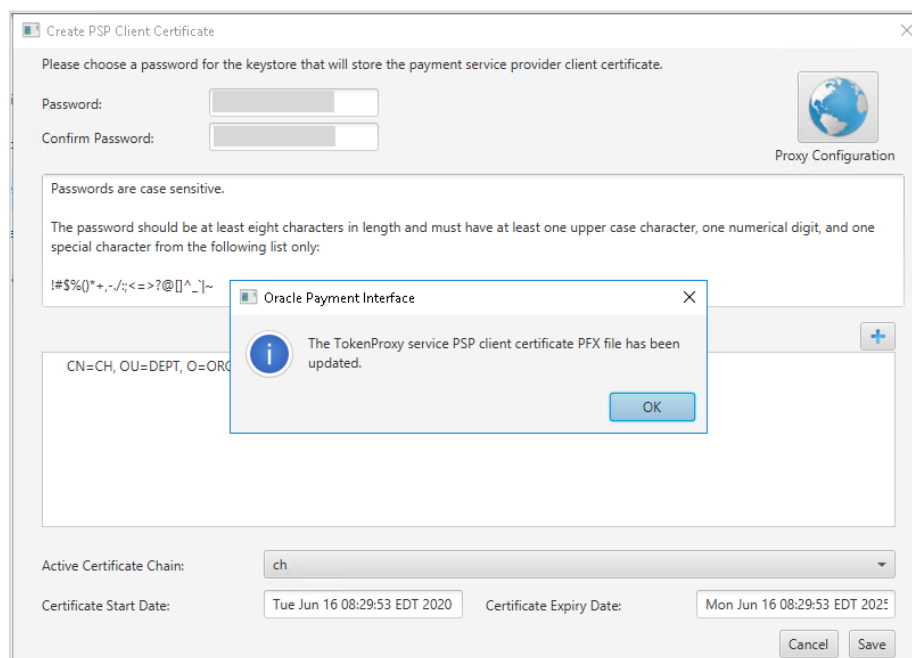
2. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** (+) icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements mentioned below 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.



3. Click Save.

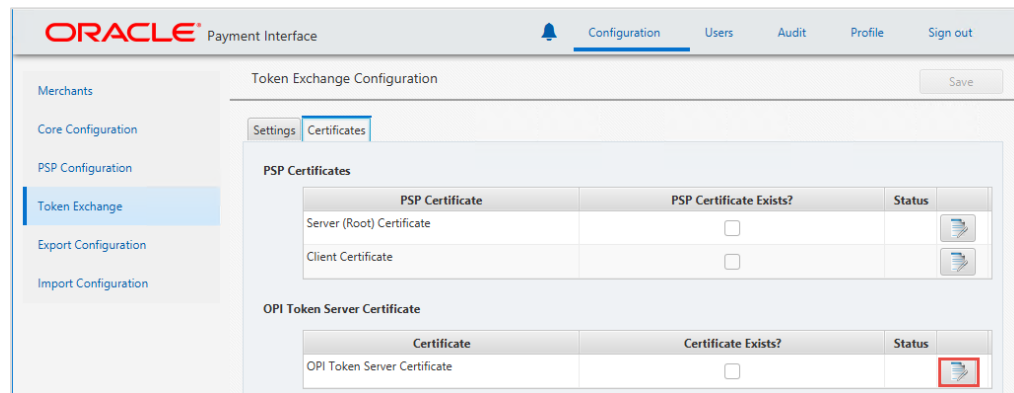


OPI_PSP_1.pfx is created under \OraclePaymentInterface\v20.3\Services\OPI\key folder.

OPI - Server Side Certificates

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

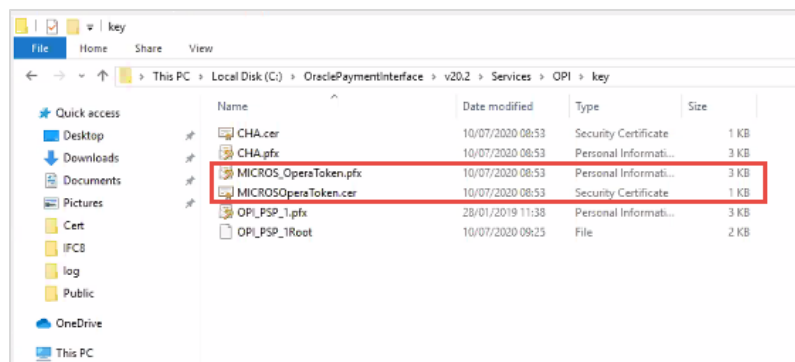
1. Select **Token Exchange** tab, click **Certificates** subtab and then click **Create OPI Token Server Certificate** to proceed.



2. Enter **City**, **State/Province**, **Country/Region**, **Create based on IP or FQDN**, **OPI Server IP**, **Password** and **Confirm Password**.

3. Click **Generate** to continue.

This process will generate the **MICROS_OPERAToken.pfx** and **MICROSOPERAToken.cer** files in the following folder:
\OraclePaymentInterface\v20.3\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** file to all the OPERA registered terminals that you want to 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 following OPERA versions, the Mutual Authentication requirement was removed for OPI TPS communication.

- OPERA V5.5.0.24.4 and V5.6.6.
- OPERA Cloud 19.4.0.0 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

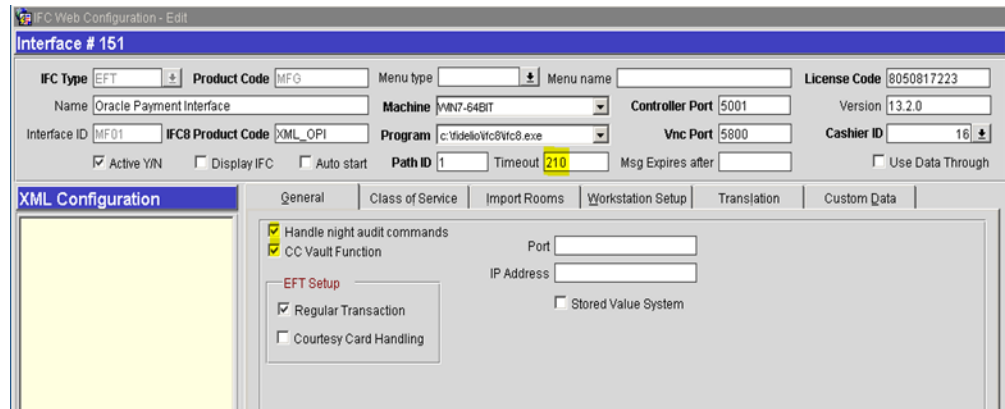
Communication: TCP/IP Serial

IP:

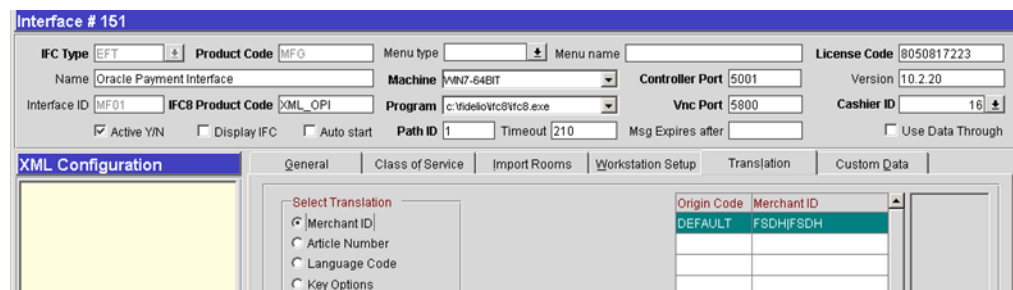
Port:

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.



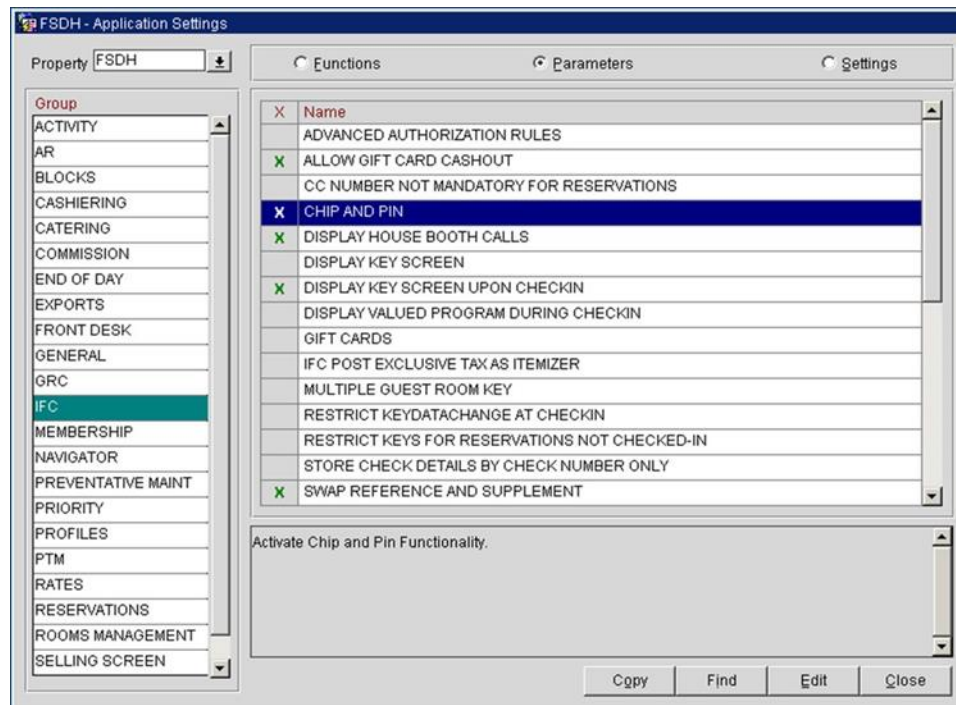
7. Select the **Translation** tab, and click **Merchant ID**.
8. Select **New** to add the Merchant ID. This must be the same as previously configured in OPI (MPG) Configuration.



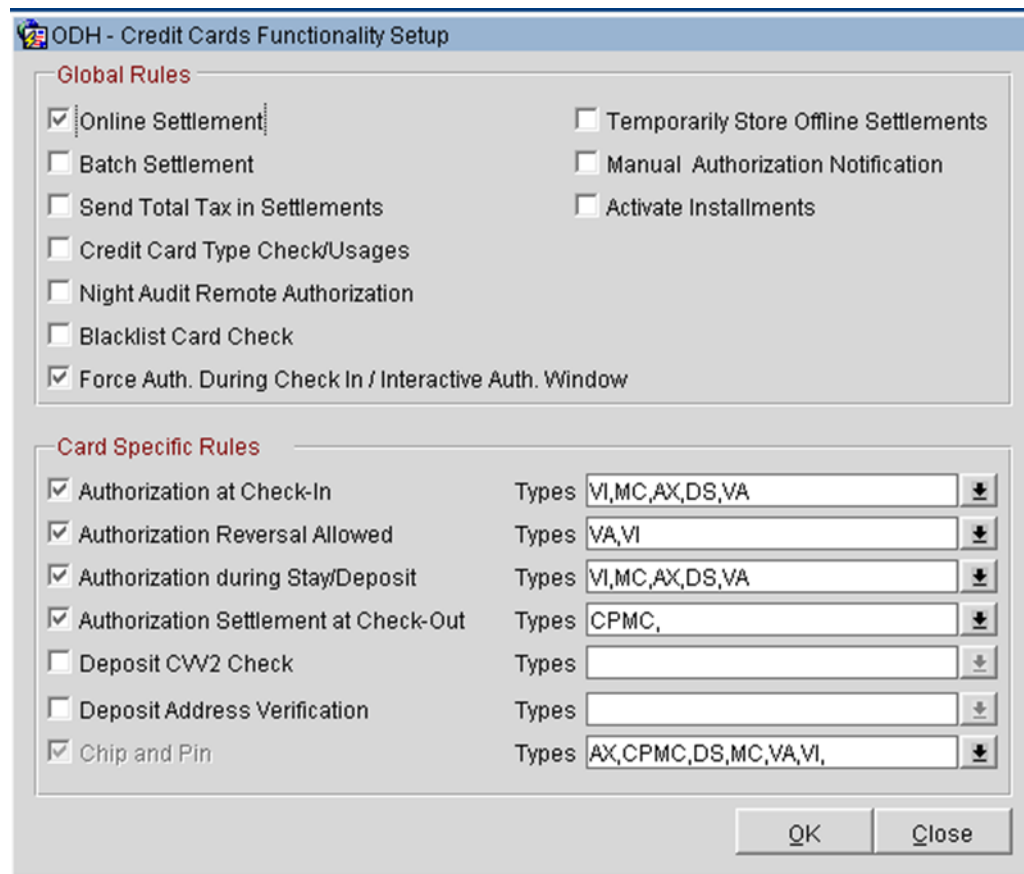
Configuring CHIP AND PIN (EMV)

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.**



- **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

These settings can be per property. Goto **Configuration | Setup | Property Interfaces | Interface Configuration | edit EFT IFC OPI | Custom Data** tab.

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

The screenshot displays the 'IFC Web Configuration - Edit' window for 'Interface # 12845'. The 'General' tab is selected, showing the following configuration details:

- IFC Type:** EFT
- Product Code:** FID
- Machine:** DEN00GDA
- Controller Port:** 5001
- Version:** 9.6.11
- Name:** OPI_EFT
- Interface ID:** FID01
- IFC8 Product Code:** FID
- Program:** c:\fdetel\ifc8\ifc8.exe
- Vnc Port:** 5800
- Cashier ID:** 34
- Path ID:** 1
- Timeout:** 210
- Msg Expires after:** (empty)
- Use Data Through:** (empty)

Under the 'EFT Setup' section, the following options are visible:

- Handle night audit commands
- CC Vault Function
- Regular Transaction
- Courtesy Card Handling

The 'Room Translation' section includes a search box and a table with the following structure:

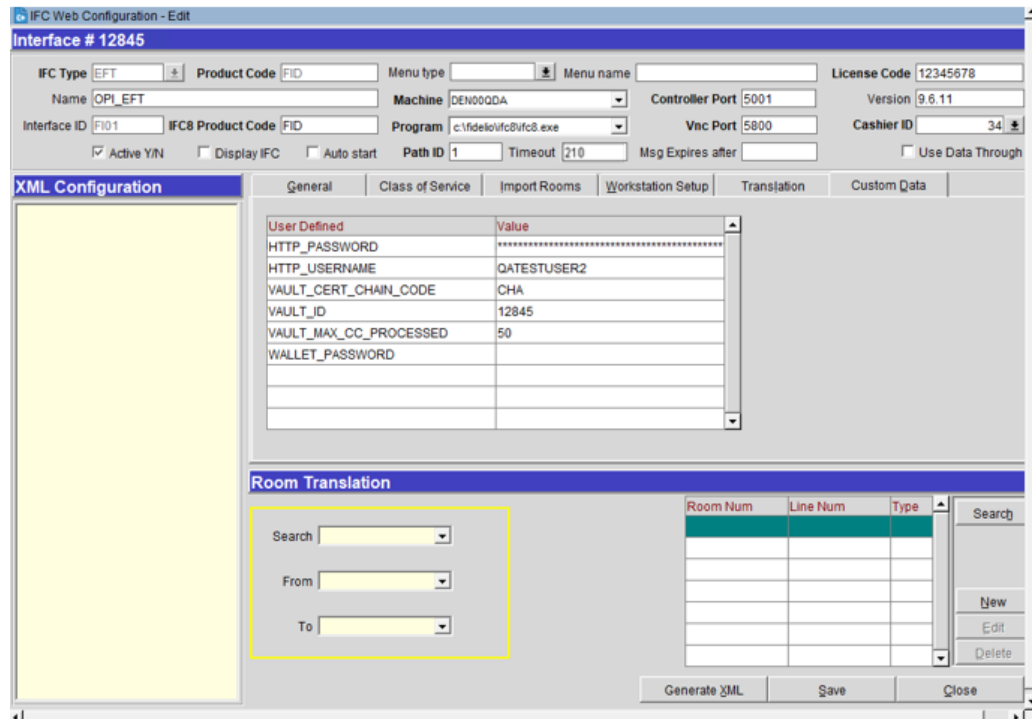
Room Num	Line Num	Type

The 'Token URL' field is highlighted with a yellow box and contains the text: `https://OPIHost/IP:OPITokenPortNumber/TokenOPERA`. Other fields include 'Port' (COM), 'IP Address' (empty), and 'Stored Value System' (unchecked).

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:

Example: <https://OPIHost> or address: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 (This is determined by Payment Partner/Vendor; please verify with Partner/Vendor, the number of credit cards that can be processed per batch).

The CREDIT CARD VAULT TIMEOUT is set to the timeframe to wait for a response from the Token Proxy Service. At least 240 is recommended.

OPERA Payment Widget Configuration

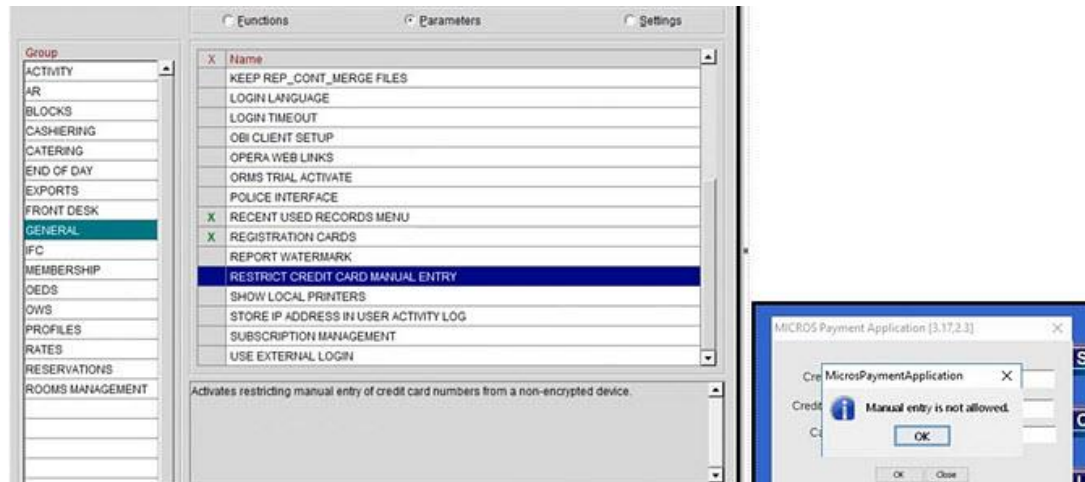
Activation / Inactivation Rules

- **Credit Card Vault** function and the **Chip and Pin** Parameter must be set active.

Application Settings

To configure this Application Settings:

1. Go to **Setup | Application Settings | General | Restrict Credit Card Manual Entry**
2. When Active this will deactivate the OPERA Payment Widget across the OPERA Property.



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.

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.

015 - Payment Types - Edit

Payment Type: VA Description: Visa Card Credit Limit: 1,000,000.00
 IFC CC Type: VA Trn. Code: 9600 Extra Percent: 0.00
 Cash Surcharge
 Merchant Number: No Post Reservation
 Authorization Receipt
 Display Sequence:

Algorithm Configuration Range

Card Length: 13,16 From: 4000000000000000 To: 4905249999999999
 Card Prefix: 4 From: 400000000000000000 To: 490524999999999999
 Validation Rule: Mod 10 From: 4905300000000000 To: 4910999999999999

Delete OK Close

Credit Card Type Payment Setup Information

To link the Card Types, the Credit Cards types mentioned below should be created and available in OPERA PMS.

Sample List of Card Types

Payment Types - Customer Present (Chip and PIN)	Description	Capture Method
VA	Visa	CP can be used. Transaction will go to the EMV (Chip and PIN) device.
MC	Mastercard	CP can be used. Transaction will go to the EMV (Chip and PIN) device.
AX	American Express	CP can be used. Transaction will go to the EMV (Chip and PIN) device.
DC	Diners Club	CP can be used. Transaction will go to the EMV (Chip and PIN) device.
JC	JCB	CP can be used. Transaction will go to the EMV (Chip and PIN) device.
CU	China Union Pay	CP can be used. Transaction will go to the EMV (Chip and PIN) device.
VD	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 and PIN) device.
MD	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 and PIN) device.
CD	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 and PIN) device.
MS	Maestro	CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip and PIN) device. Customer present ONLY!
VP	V-Pay	CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip and PIN) device. Customer present ONLY!
BC	GiroCard	CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip and PIN) device. Customer present ONLY!

Payment Types - Customer Present (Chip and PIN)	Description	Capture Method
AB	AliPay	CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip and PIN) device. Customer present ONLY!
MI	MIR (National Card for Russia)	CP can be used. Transaction will go to the EMV (Chip and PIN) device.

Payment Types – Customer NOT Present (Keyed)	Description	Capture Method
KVA	Visa Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
KMC	Mastercard Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
KAX	American Express Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
KDC	Diners Club Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
KJC	JCB Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
KCU	China Union Pay Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
KVD	Visa Debit Keyed	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
KMD	Mastercard Debit	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)
KCD	China Union Pay Debit	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)

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

Individual Card Functions

Payment Types - Customer Present (Chip and PIN)	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
VA	Y	N	N	Y	N
MC	Y	N	N	Y	N
AX	Y	N	N	Y	N
DC	Y	N	N	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
MI	Y	N	Y	Y	Y

Payment Types - Customer NOT Present (Keyed)	Authorization at Check-in	Pay Only (no Authorization)	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

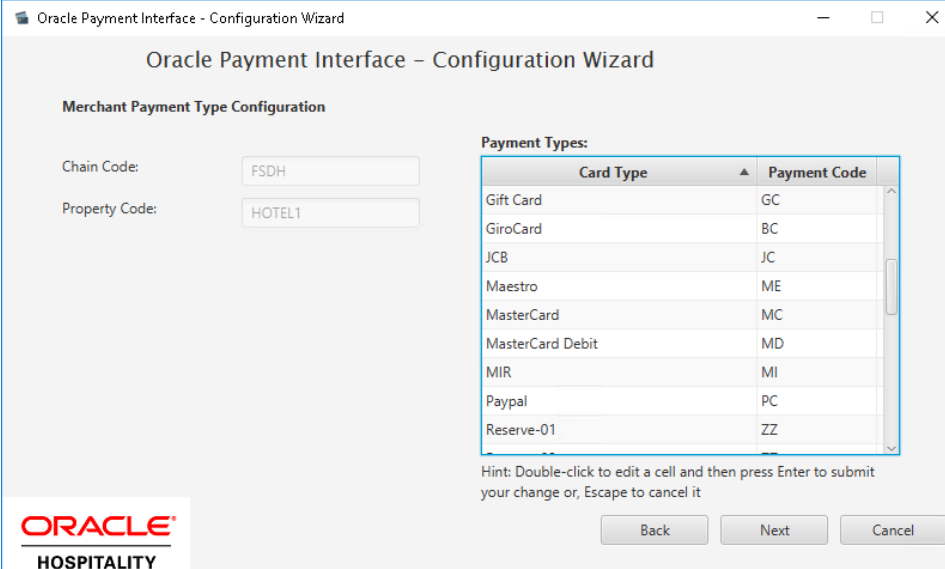
Payment Types – One Shot Cards (Keyed) OPTIONAL!!!	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
VVA	N	Y	N	Y	N
VMC	N	Y	N	Y	N
VAX	N	Y	N	Y	N

Important Considerations

- Transaction codes for Chip and 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 and PIN.

Update OPI Configuration Payment Types

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

Merchant Payment Type Configuration

Chain Code: FSDH

Property Code: HOTEL1

Payment Types:

Card Type	Payment Code
Gift Card	GC
GiroCard	BC
JCB	JC
Maestro	ME
MasterCard	MC
MasterCard Debit	MD
MIR	MI
Paypal	PC
Reserve-01	ZZ

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

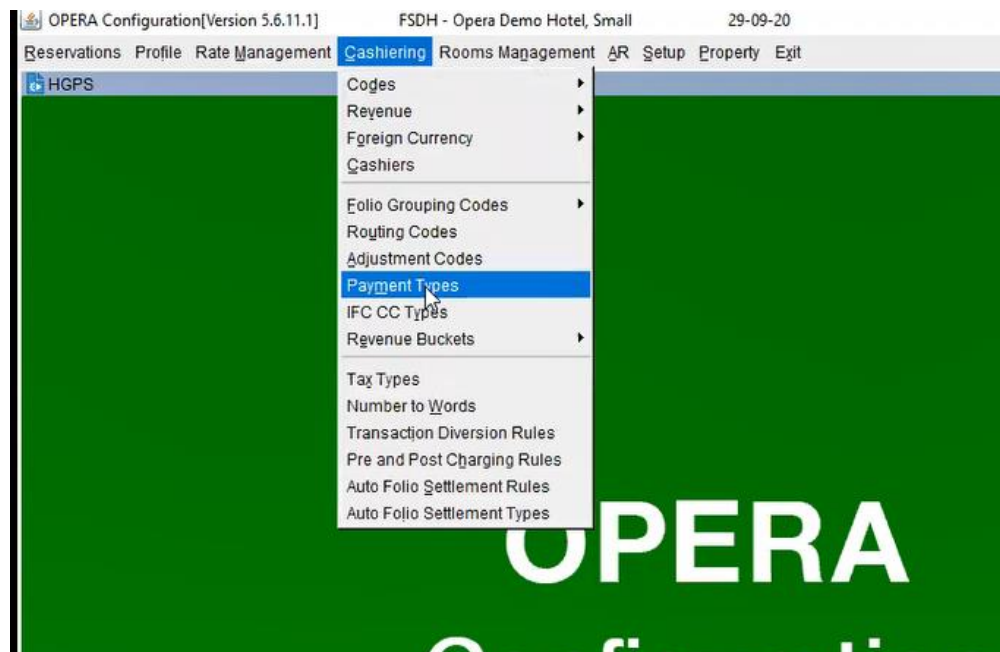
Pay Only Transaction Codes

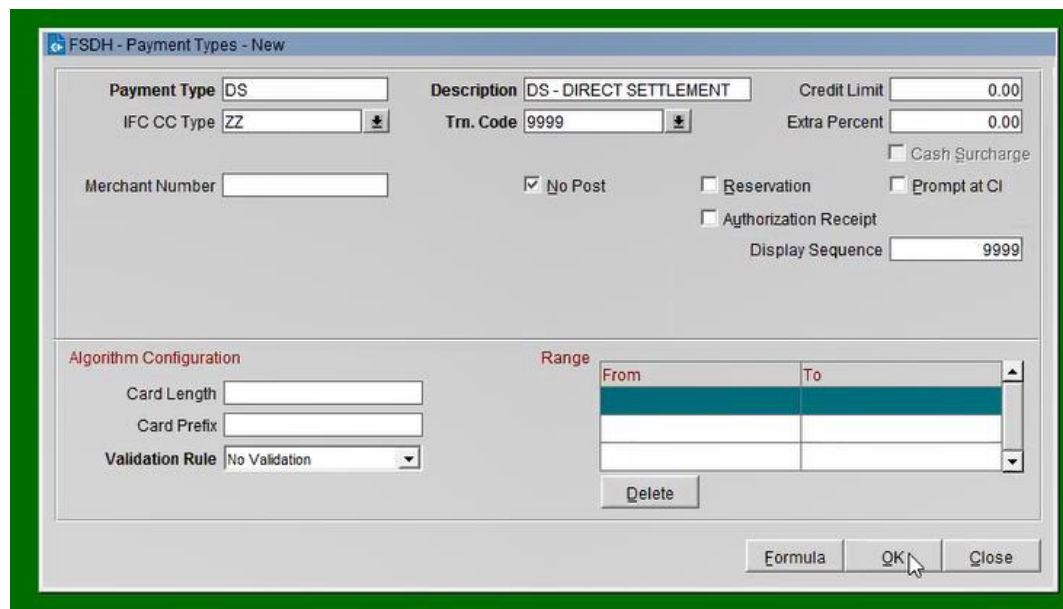
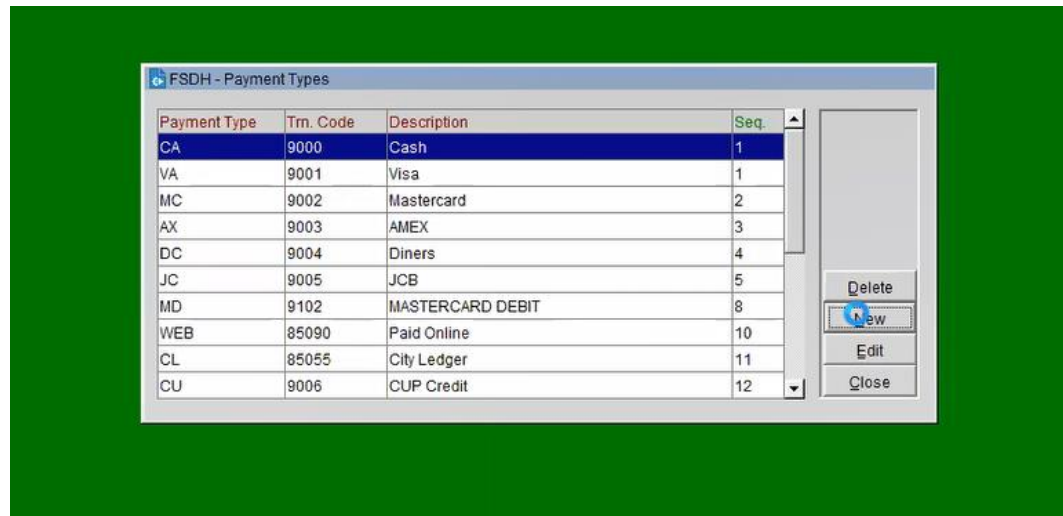
By default, OPERA will process a Pre-authorization following by a Sale Completion when processing a payment. At times, hotels will need to process transactions as a “Sale Transaction” – meaning a Sale Transaction only and no pre-authorization is processed. In OPERA we refer to this feature as “Pay Only” and this can be used to process payments for Debit Cards, Digital Wallets, or Virtual Credit Cards that do not support Pre-Authorizations.

To set up this type of transaction code, you will need to set up a new Transaction Code and Payment type for each of these Card types being processed at a property level.

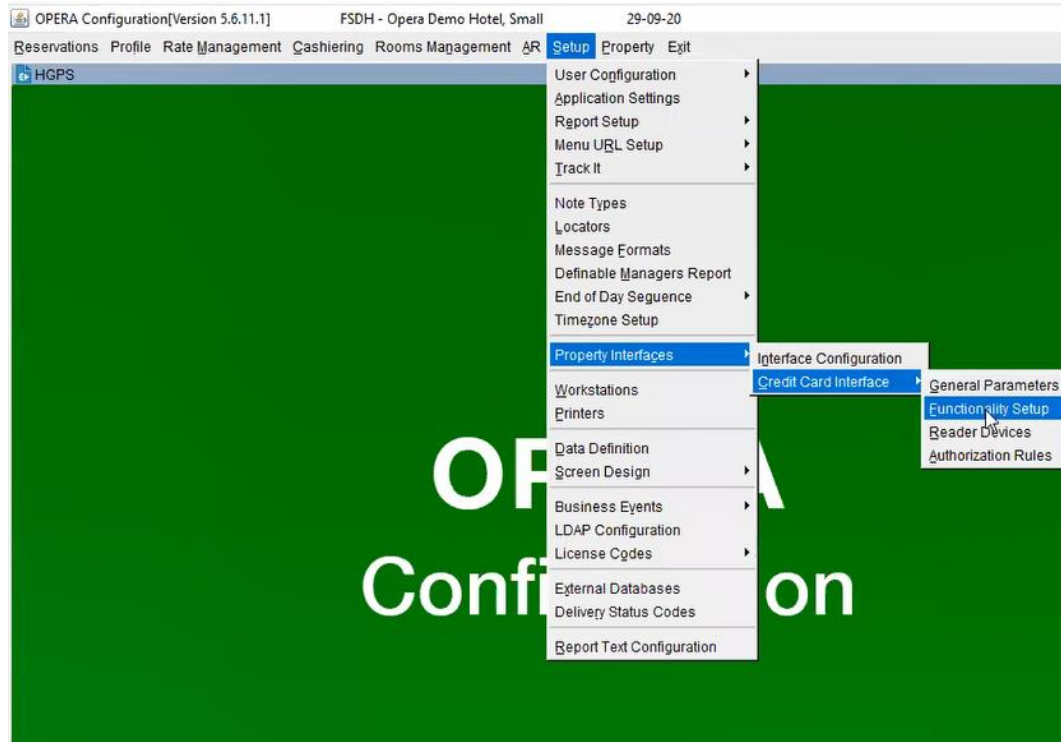
1. Go to **OPERA Configuration | Cashiering | Codes | Transaction |New**. Configure the code as shown in the screen shot below:

- Next go to OPERA PMS Configuration | Cashiering | Payment Types. Configure the payment types with the settings shown below:

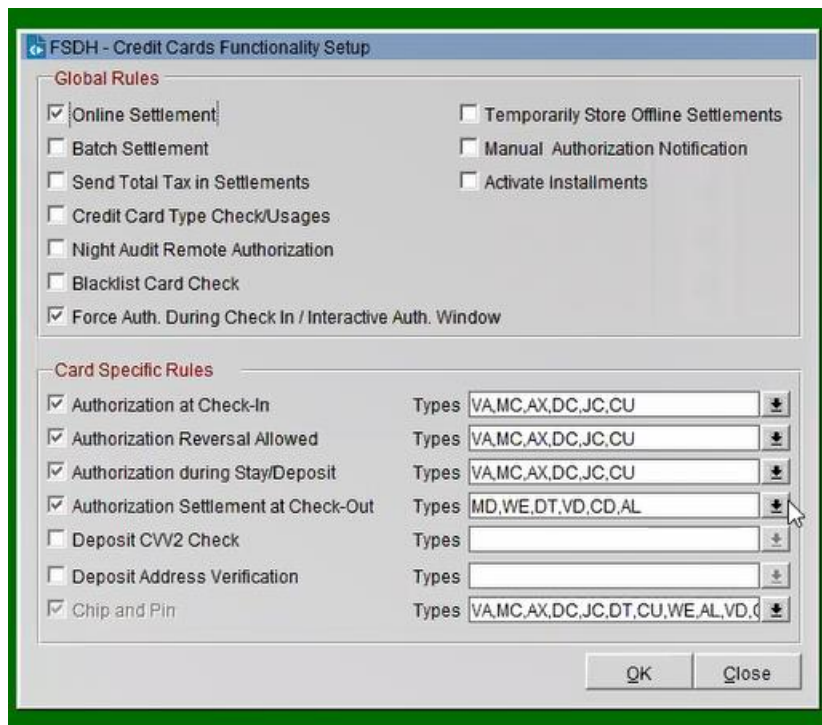


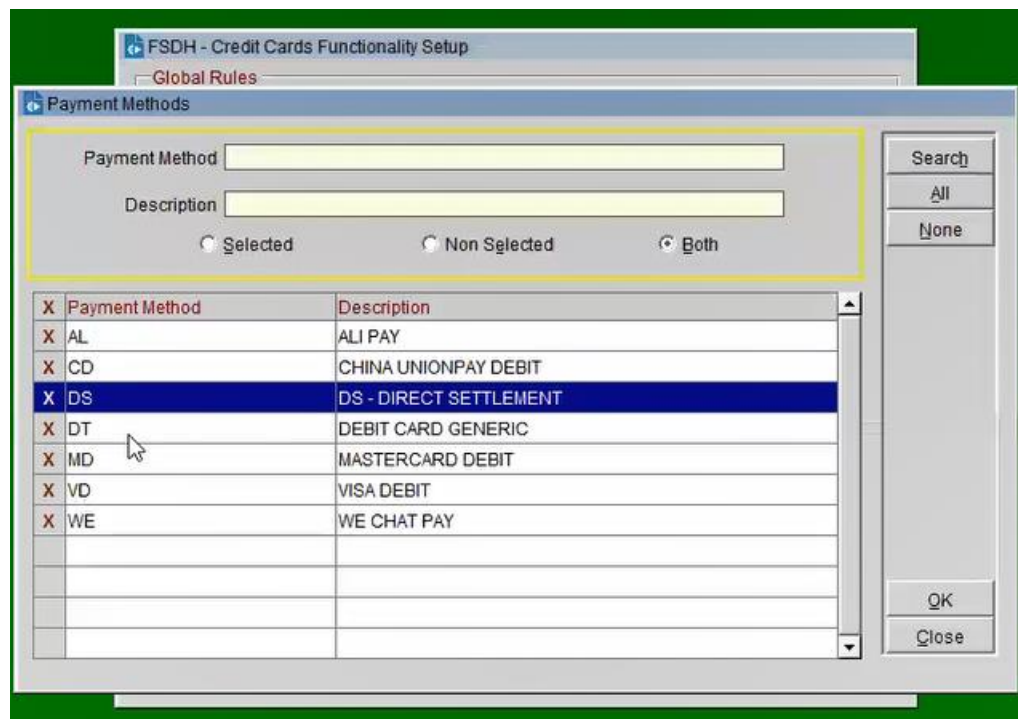
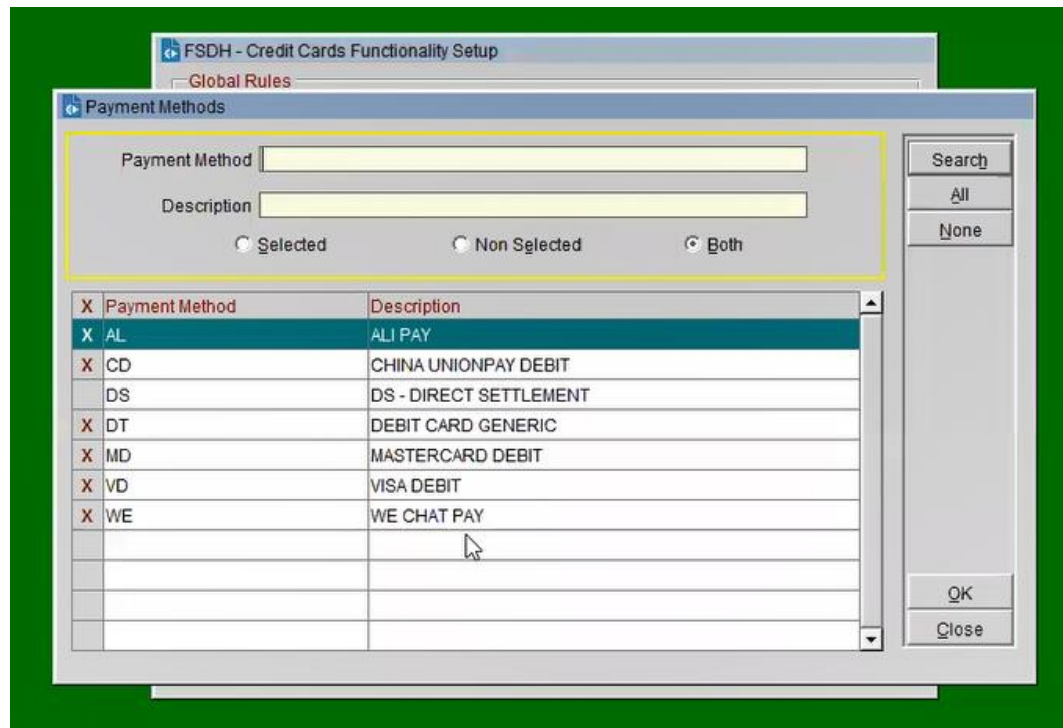


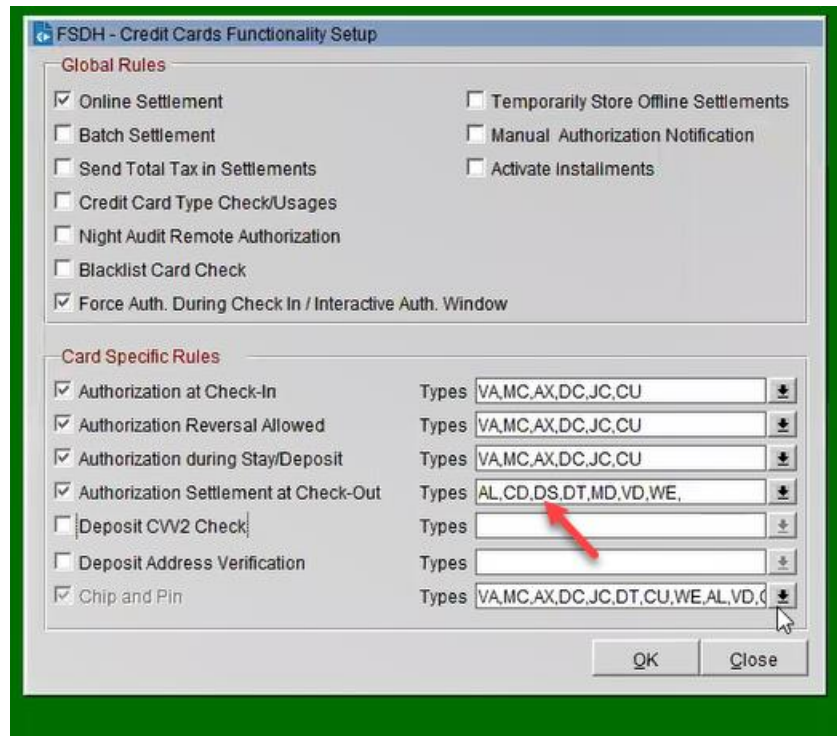
- Next go to OPERA **PMS Configuration | Setup | Property Interface | Credit Card Interface | Functionality Setup.**



4. Add the new payment types you created above to the following two settings:
 - a. Authorization Settlement at Check-out
 - b. Chip and Pin





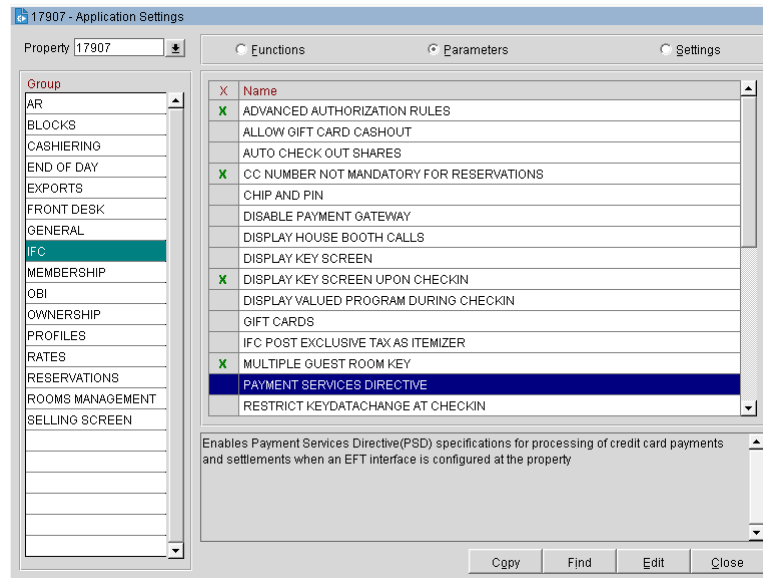


Activating and Using the Payment Service Directive (PSD2) Control

A Payment Service Directive OPERA Control is added for properties with payment integration to meet the requirements of the P2D2 European directive for card not present transactions.

The support of the **Customer Initiated Transaction (CIT)**, **Mail Order / Telephone Order (MOTO)** and **Merchant Initiated Transaction (MIT)** flags need the **Payment Service Directive** application parameter in OPERA PMS to be activated. Currently, the supported functions for OPERA V5 are CIT, MOTO, and MIT.

Activating the Payment Service Directive is available only once the credit card interface has been installed in OPERA and the Credit Card Vault function and the Chip and Pin is turned on. If this is completed follow the below sections to know the functions of CIT, MOTO and MIT:



Activating this parameter enables the Payment Services Directive (PSD2) specifications for the processing of credit card payments and settlements when an EFT interface is configured at the property.

Customer Initiated Transaction (CIT) Flag

The following OPERA screens receive and send out the CIT ID:

- Deposits
- Payments
- Reservation Main
- Credit Cards Authorization
- Post It Payments
- Passer By Payments
- Accounts Receivable Payments

OXI Incoming Messages for New or Update Reservation

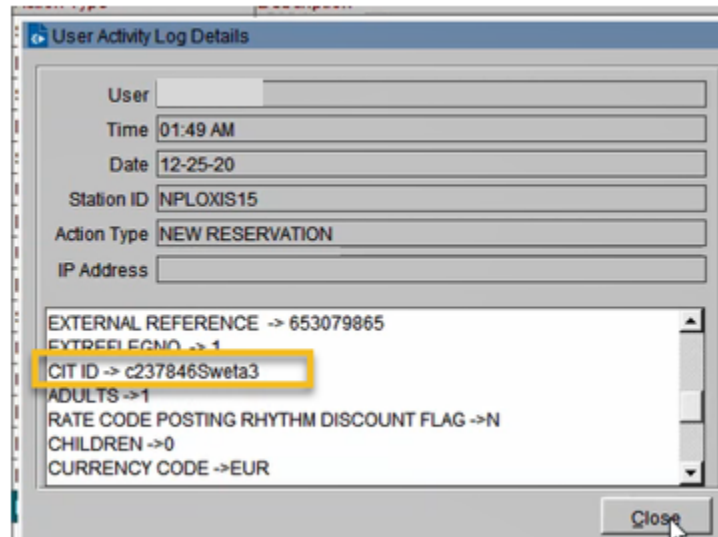
When OXI sends a new reservation or an update reservation message to OPERA that contains credit card information with a CIT ID, OPERA stores the CIT ID along with the credit card payment information. The incoming OXI message to OPERA includes the CIT ID in the "PaymentMethod" attribute.

OXI Outgoing Messages for Credit Card Transactions

When OXI sends outgoing messages for credit card authorizations and transactions to an IFC8 interface, OXI includes the CIT ID in the "PaymentMethod" attribute.

Viewing the CIT ID in OPERA

OPERA PMS users can view the CIT ID in the Reservation Changes Log in **NEW RESERVATION** and **UPDATE RESERVATION** Action type field by navigating to **Reservation > Options > Changes Log**. The CIT ID is read-only.



Mail Order / Telephone Order (MOTO) Flag

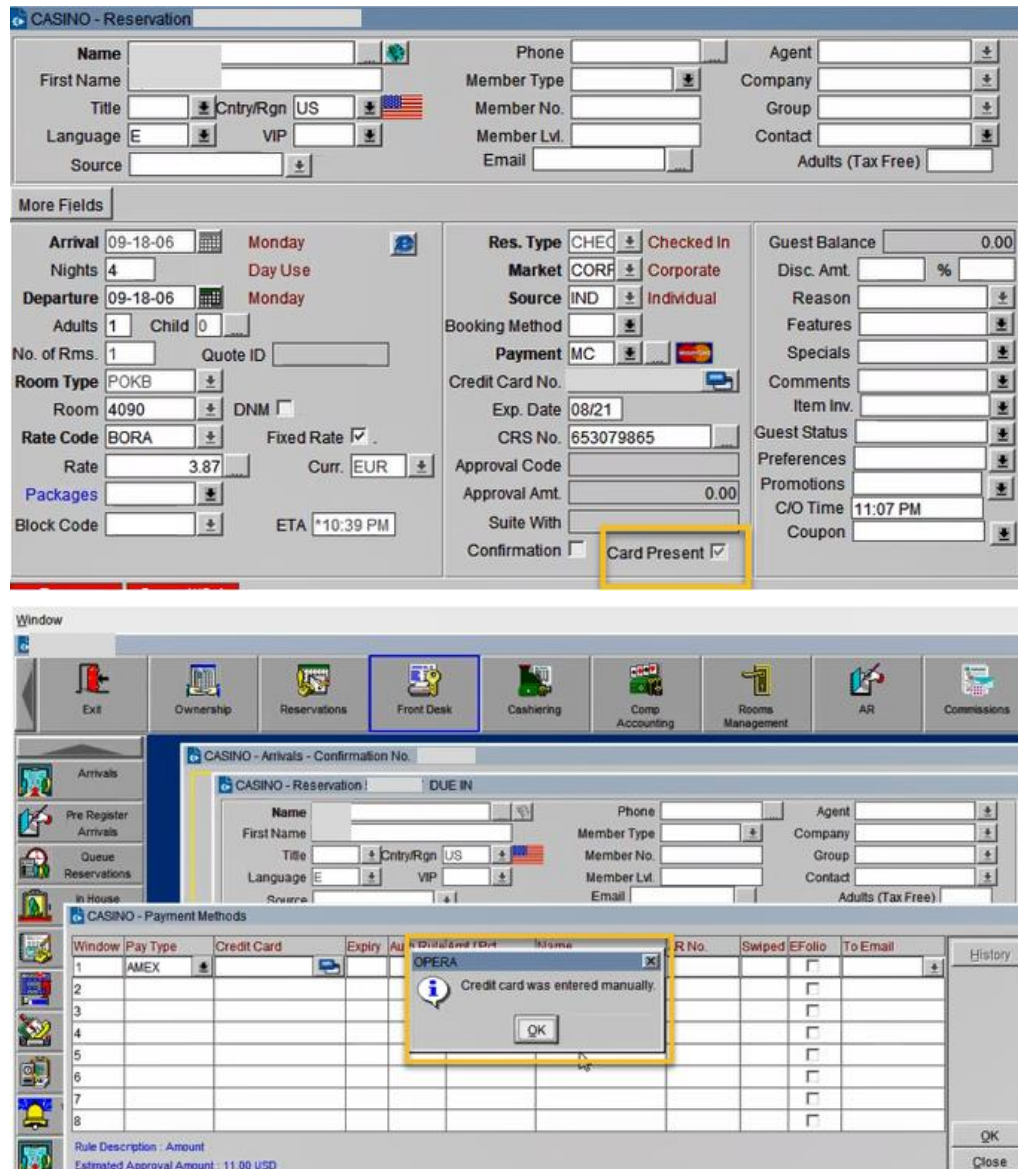
When **Payment Service Directive** is Active, the information sent from OPERA V5 to the interface will:

- Include a MOTO flag in the "PaymentMethod" tag indicating:
 - MOTO=0 indicates the Credit Card was NOT entered manually
 - MOTO=1 indicates that the Credit Card was entered manually

Sample:

`PaymentMethod="InitTrx:MIT2[Cc:][Moto:0]"cc:0"/>]`

- Display a new '**Card Present**' checkbox.
 - **Card Present** checkbox selected indicates the Credit Card was not entered manually.
 - **Card Present** checkbox not selected indicates that the Credit Card was entered manually (Entering Credit card manually will also prompt a message saying "**Credit card was entered manually**").



Merchant Initiated Transaction (MIT) Flag

When **Payment Service Directive** is active, the information sent from OPERA V5 to the interface will include the MIT flag in the 'PaymentsMethod' tag when sending payments to the Payment Service Provider for approval.

MIT Flag options include an MIT flag in the "PaymentMethod" tag indicating:

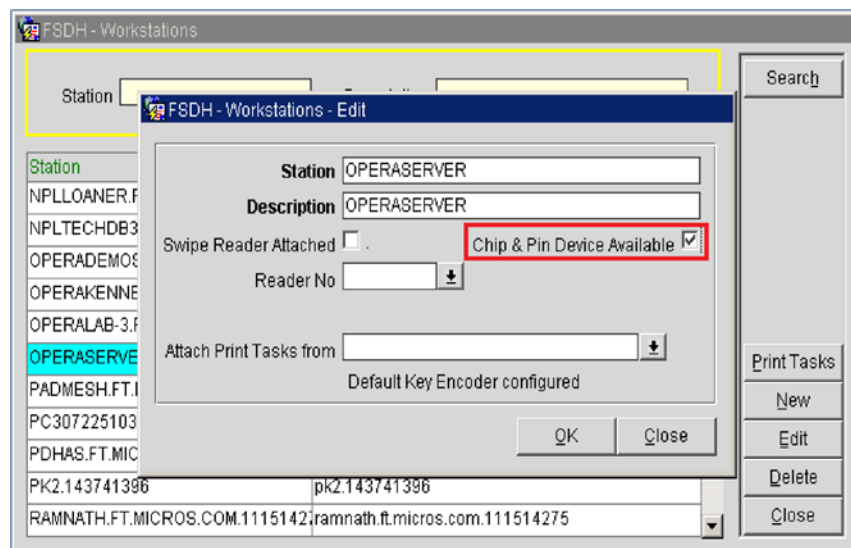
- **MIT1: NO SHOW** - used when processing credit card payment for **NO SHOW** fees.
- **MIT2: PRE-PAYMENT** - used when processing credit card **PRE-PAYMENT** for deposits.
- **MIT4: DELAYED CHARGE** - used when processing credit card payments for **POST-STAY CHARGES**.

PaymentMethod="InitTx:MIT2[Cit:|Moto:0|Vcc:0"/>]

Configuring the Workstation

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

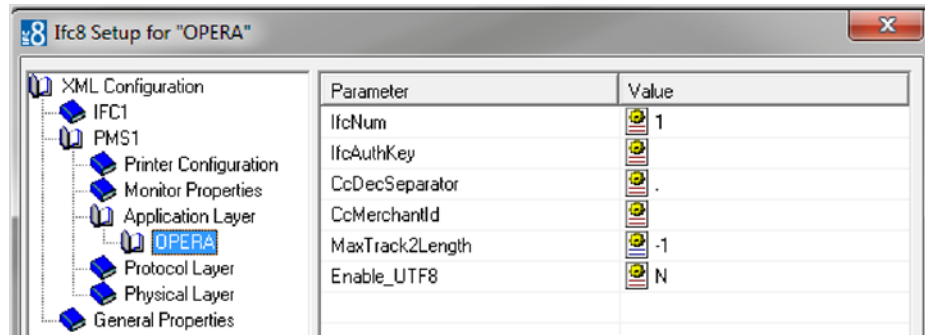
1. In OPERA | **Setup** | **Workstations** | edit your workstation.
2. Select the **Chip & Pin Device Available** check box to enable the device for this workstation (this allows the generic CP Payment Type to display in the LOV for a reservation).



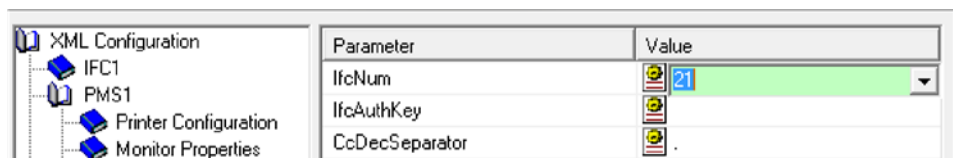
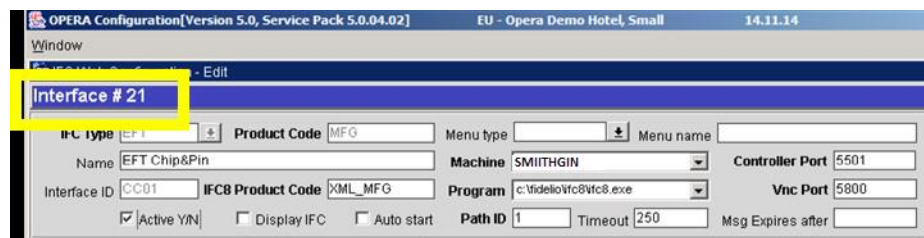
Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC)

To configure the link between the interfaces:

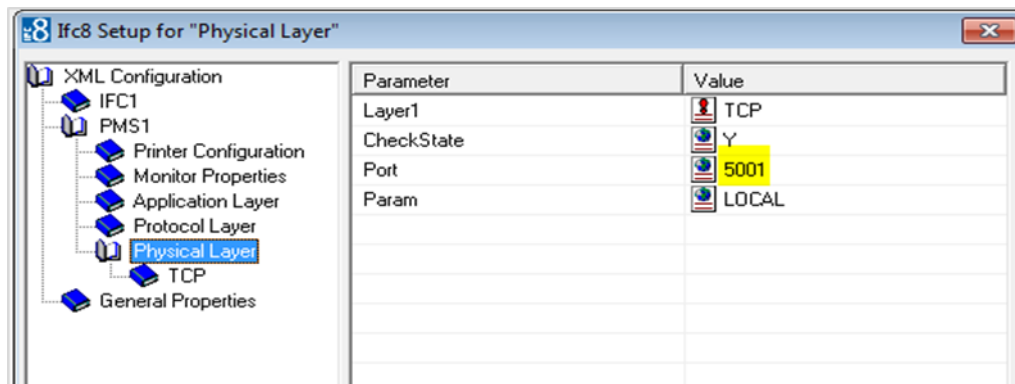
1. In the **Hotel Property Interface**, go to the **PMS1** tree and then select **OPERA** in the application layer.
2. Enter the **OPERA IFC** number in the parameter `lfcNum` value.



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



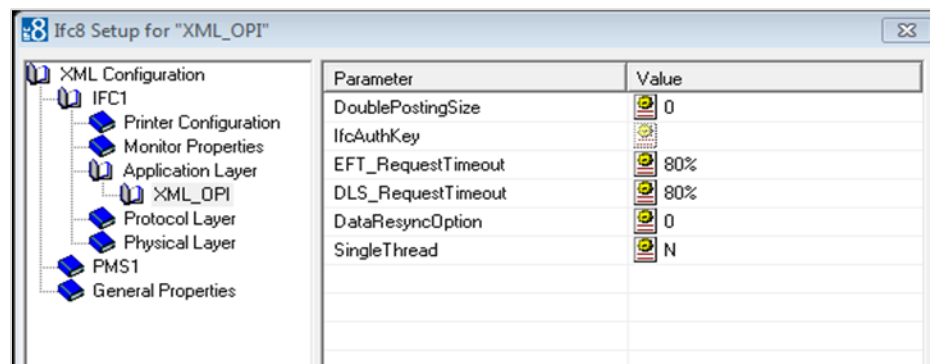
3. Go to the **PMS1** tree in the **Physical Layer**.
4. Enter the port number into Parameter value Port. This is the port IFC8 uses to communicate with the OPERA IFC controller.
5. Select **Enter** and **Apply** to re-initiate IFC8, and click **Save**.



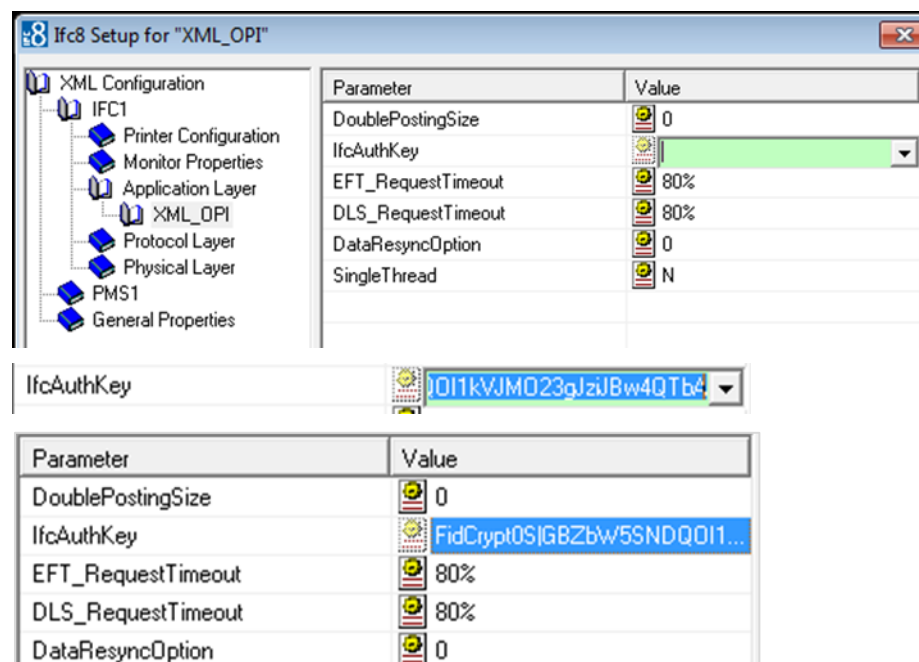
Configuring Authentication for the Hotel Property Interface (IFC8) with OPI

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.

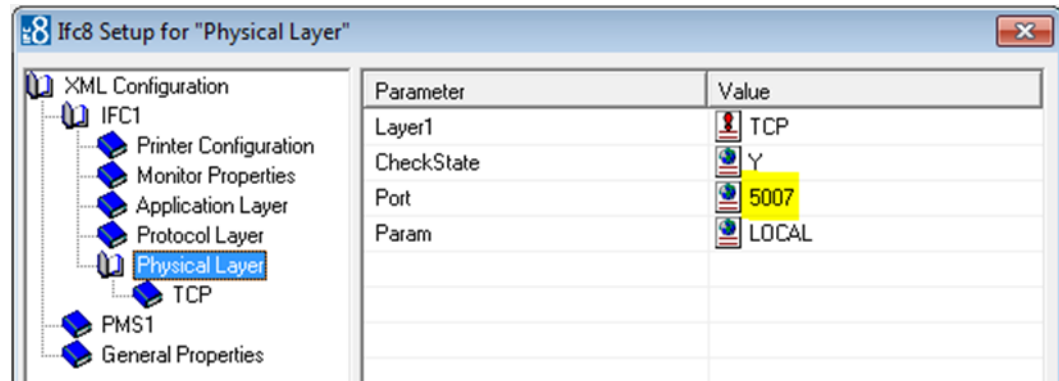
1. In the Hotel Property Interface (IFC8) configuration, go to the **IFC1** tree, and then in the **Application Layer**, select the **XML_OPI** option.



2. Copy the generated key from Configuring OPI - OPERA merchant step 3.
3. Copy this string into IFC8 Parameter **IfcAuthKey** value field.

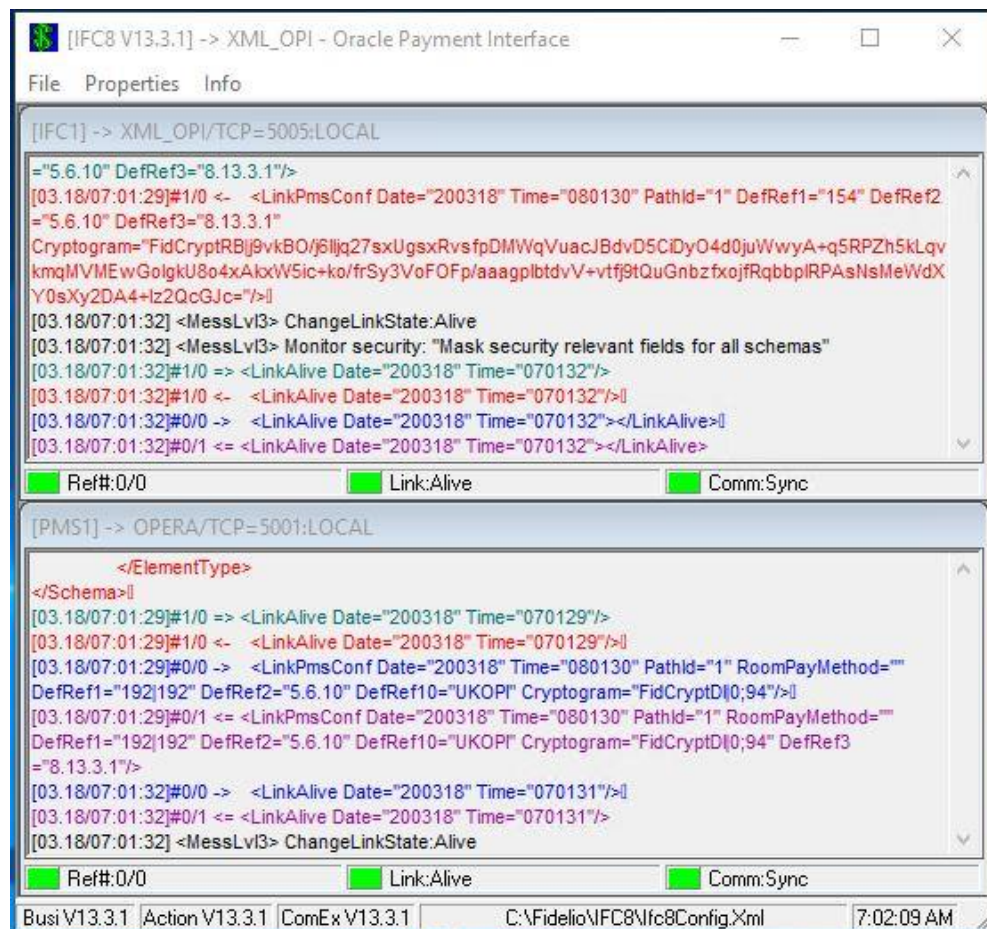


4. Go to **IFC1** tree and select the **Physical Layer**.
5. Enter the port number in port value. This is the same port that was configured in OPI.



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 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.

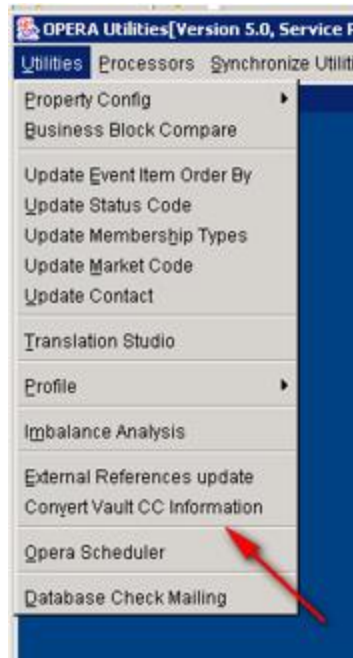


Perform Bulk Tokenization

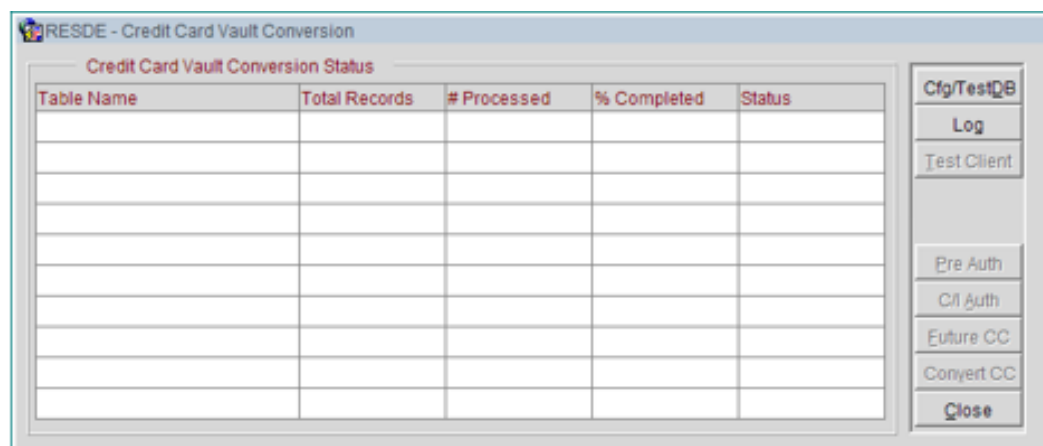
1. Test Connection. This is done from the **Utilities** Module.



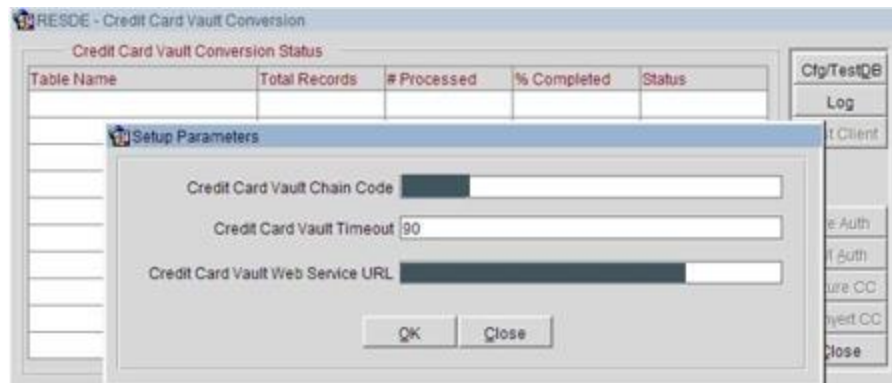
2. From the **Utilities** module, select the **Convert Vault CC Information** option.



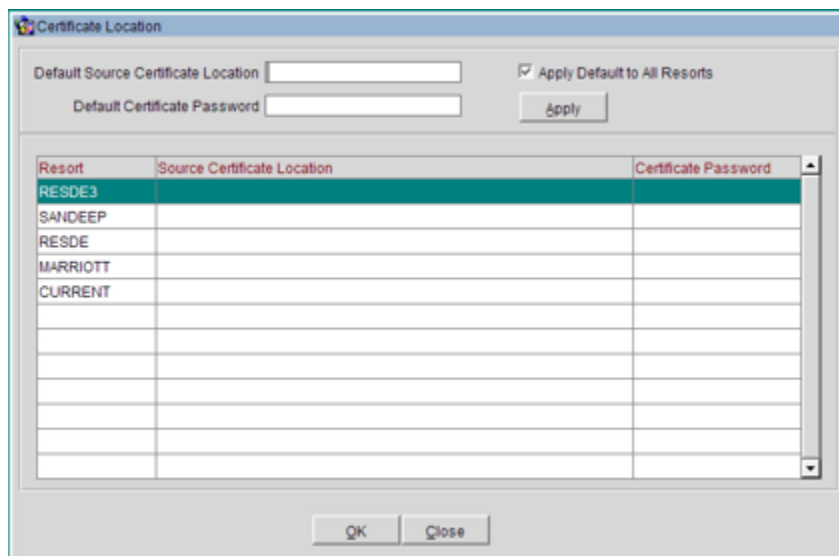
3. Click **Cfg/TestDB**.



This **Cfg/TestDB** option will perform a background check of the settings needed for Oracle Wallets. The next screen displays the existing Vault settings from Application Settings or if it is blank user can add the settings and it will update the Application Settings.

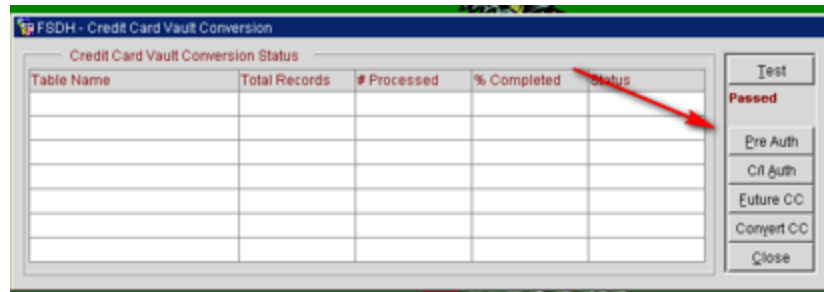


4. Click **OK** and the **Certificate Location** screen appears. The properties within the same chain that have an active Credit Card IFC will display. This is to indicate where the p12 is located and its password to be used in the Wallets. Enter a path where the p12 exists and the DB can access.



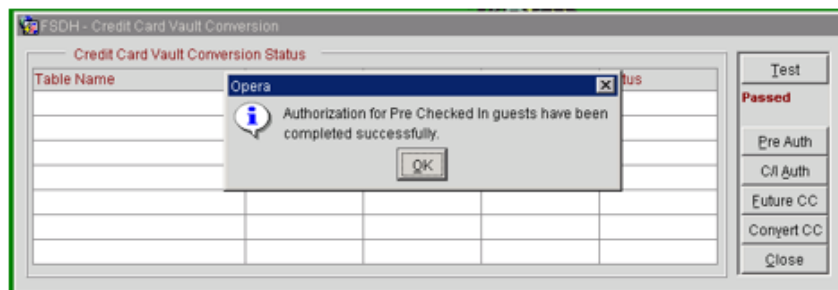
- a. Select **Default Source Certificate Location**.
- b. Click **Apply** and all the data is moved to the **Resort** column.
- c. Click **OK** and the process is initiated.
 - If the DB cannot access where the p12 is located the log will indicate a message: Unable to copy file/prop46logs/ewallet.p12: Source file does not exist.
- d. Click **Cfg/TestDB** button to navigate back to the **Credit Card Vault Conversion** screen. The **Test Client** option is now available.
- e. Click **Test Client** (this will verify that the certificate is loaded on this machine where OPERA is accessed). A credit card number is needed to verify that the token can be retrieved successfully. Once successful, the Vault Conversion process can be run.

“Passed” test will activate the **Pre auth**, **C/I auth**, **Future CC** and **Convert CC** options. If the test fails, refer to HTTP_TRANSACTION_LOG to check the reason for the failure.



- **Pre Auth**

- The Pre Auth option is used for instances where the hotel has reservations which contain authorizations on them but are not yet checked in. This option is available when the **Reservations>CC Pre Check in Authorization** application parameter is set to Y and a successful Test of the Credit Card Vault Web Service URL has passed.
- Click **Pre Auth** option to run through memo authorizations for reservations that are authorized and are not yet checked in. At the end of the process, a message is displayed stating, "Authorization for Pre Checked In guests have been completed successfully."
- Click **OK**.

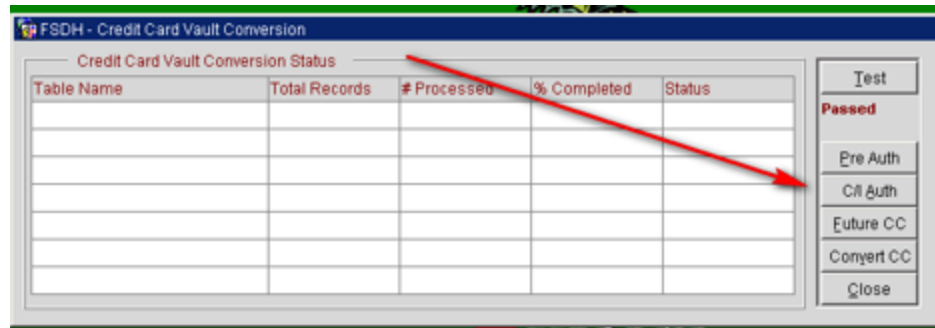


- **Convert In house guest (C/I Auth) Credit Cards**

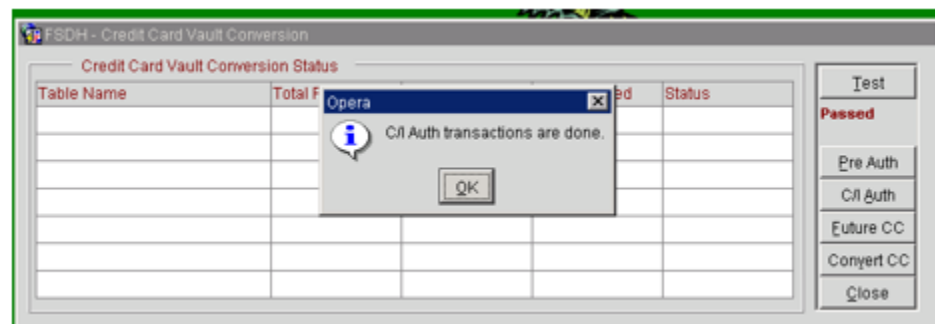
 **NOTE:**

The Pre Auth and C/I auth functions utilizes the wallets on the DB server and not local client certificates.

- This is the first conversion done. This will convert credit cards attached to reservations in house currently into tokens. This needs to take place first so that the hotel operations are not adversely affected by the conversion process. If in house guest is not converted, then there will be issues checking the guest out of the hotel.



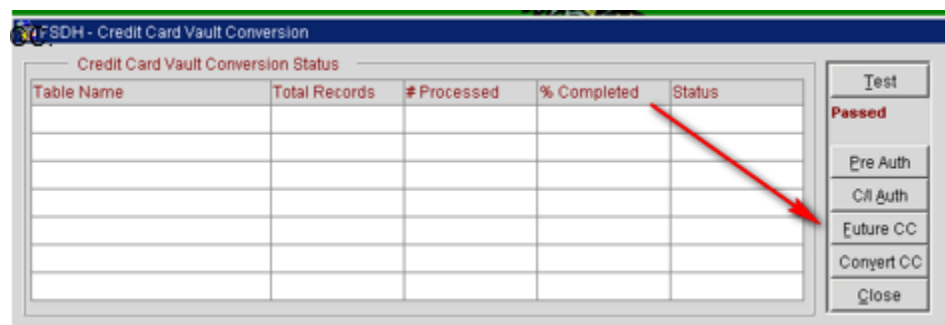
- Click **C/I Auth** to run through the checked in credit card authorizations for all properties. At the end of the process, a message is displayed stating, "C/I Auth transactions are done" to notify the user it has completed.
- Click **OK**.



 **NOTE:**

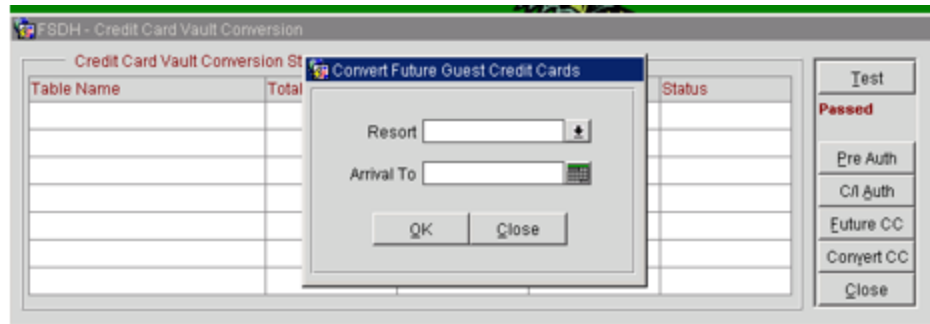
Inform Property(s) that they can now resume full PMS operations. However, OXI still needs to stay disabled.

- Convert Future Guest Credit Cards. Click **Future CC**.

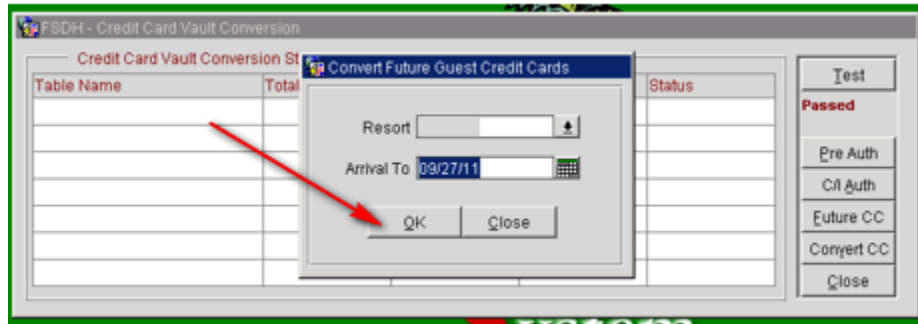


Populate the parameters as needed.

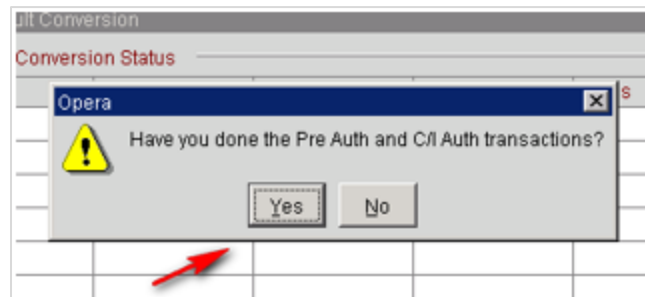
- **Resort:** This allows you to choose a specific resort to convert in a multi property environment. Leave blank if you are working on a single property or want to convert all resorts in the schema.
- **Arrival To:** This is the arrival date you want the system to convert out to. The next business date should suffice unless you are working in a multi property environment where the conversion might take several days.



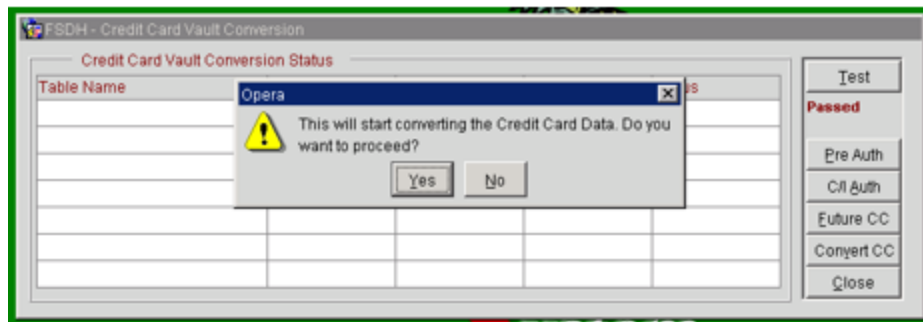
- Once the parameters are populated, click **OK**.



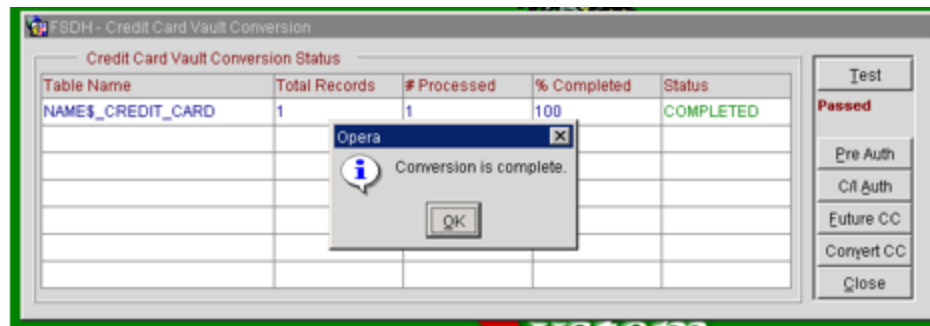
- You are prompted with a question concerning whether you have converted all pre auth and in house guest. If you have completed this step click **Yes**, if not click **No** and go to the previous step.



- You will receive one more prompt, if you are ready to continue click **Yes**.



- Once the conversion is complete, you will view the following message.



Credit Card Vault Conversion Status

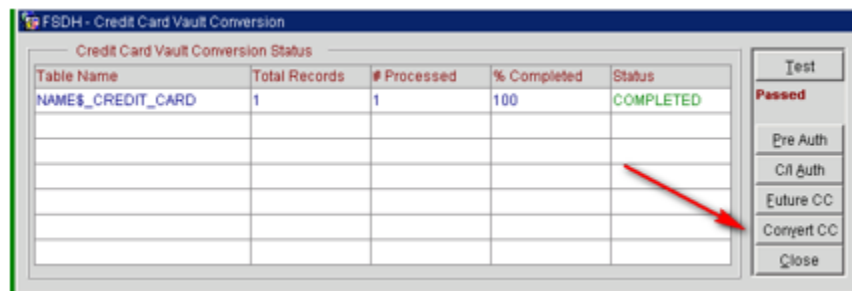
- **Table Name:** Name of the table that is currently having the credit card information converted.
- **Total Records:** Total records to be converted in this table.
- **# Processed:** Number of records that have been processed for the table.
- **% Completed:** Displays the percentage complete for converting the credit card information in the listed table.
- **Status:** Displays the status of the conversion, Running, Complete, or Failed.
- Credit cards are converted to tokens at a rate of 50 cards per batch.

- Convert remaining CC #'s

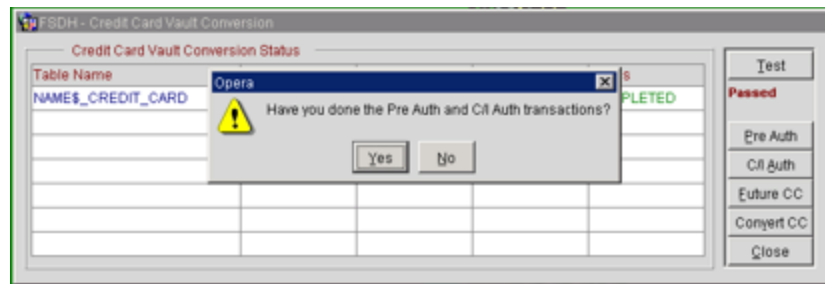
NOTE:

This will convert all the remaining Credit Cards which are stored in OPERA.

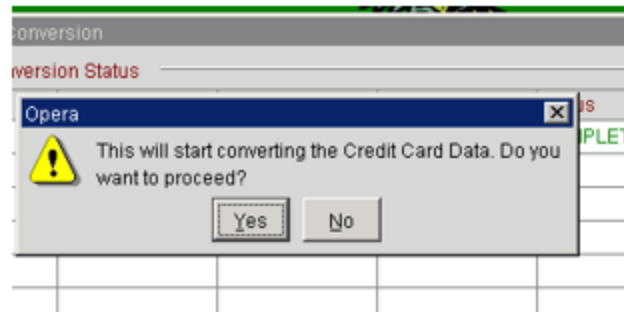
- Click **Convert CC.**



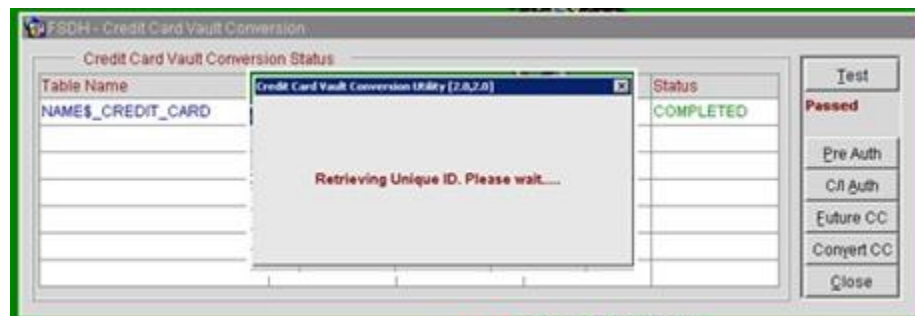
- You will receive a prompt requesting if you have completed the conversion of the pre auth and in house guest.
 - Yes – Initiates the conversion for the rest of the database.
 - No – Takes you back to the form to allow you to run the pre auth and C/I Auth process.



- You will receive another prompt requesting if you want to proceed. Click **Yes** if you want to proceed.

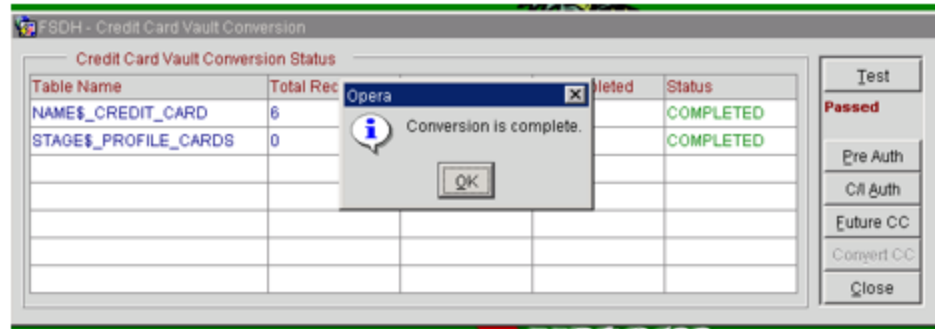


- The grid will start an update as the conversion proceeds. There will be a flashing "RUNNING" box as the process proceeds, and with each flash the grid will update the status.



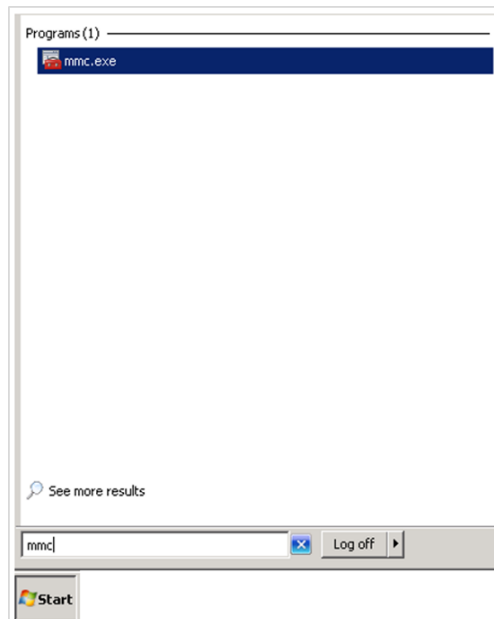
Credit Card Vault Conversion Status

- **Table Name:** Name of the table that is currently having the credit card information converted.
- **Total Records:** Total records to be converted in this table.
- **# Processed:** Number of records that have been processed for the table.
- **% Completed:** Displays the percentage complete for converting the credit card information in the listed table.
- **Status:** Displays the status of the conversion, Running, Complete, or Failed.
- The conversion processes 50 cards per transaction. Click **OK**.

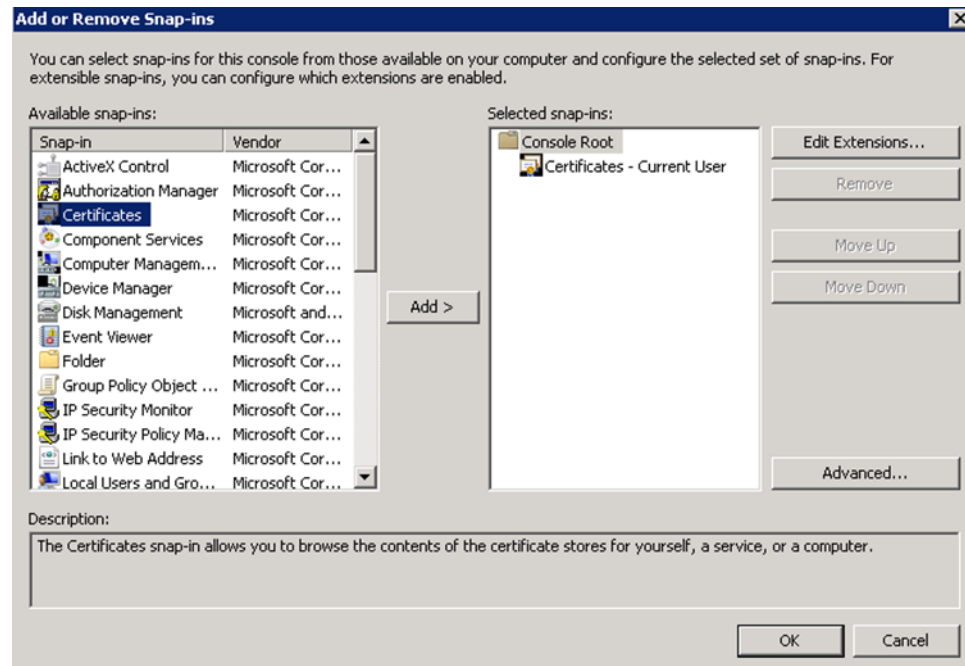


Certificate Import using Microsoft Management Console

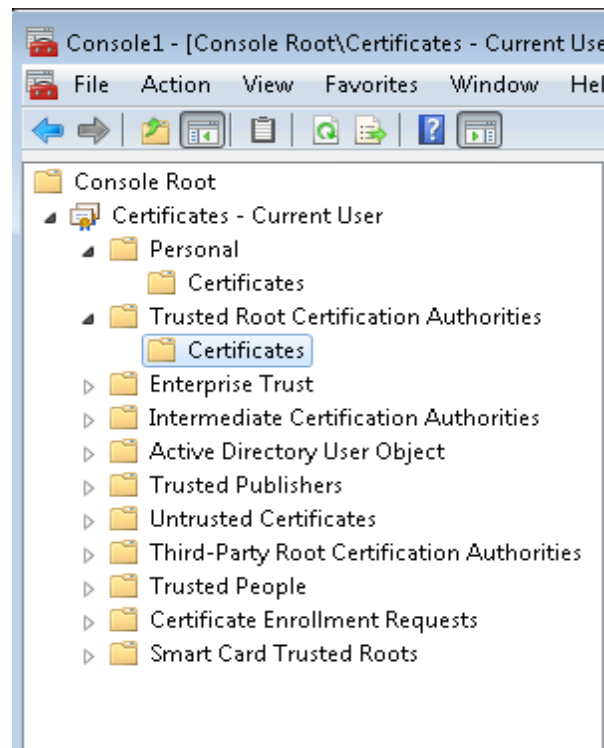
1. Find and open `mmc.exe` from Start menu.



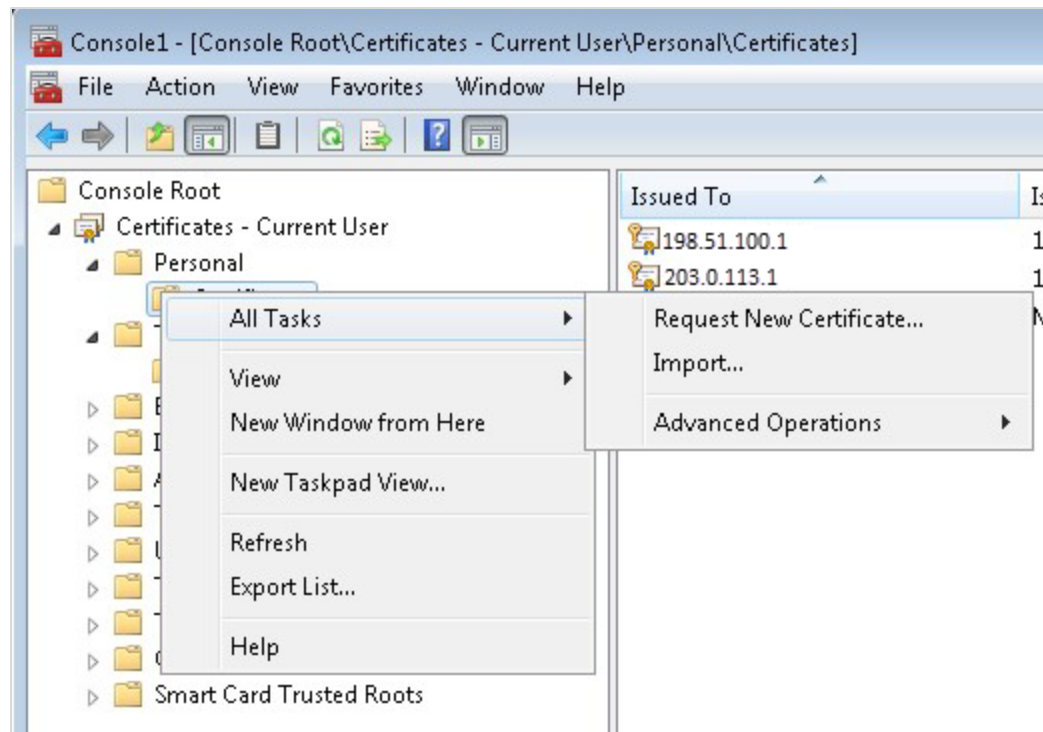
2. Go to **File | Add or Remove Snap-ins**, add certificates to **Selected snap-ins**, and click **OK**.



- Expand **Certificates**, expand **Personal** or **Trusted Root** as required, and 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 click **Next**.
- If required enter the password relevant to the certificate you are importing, and click **Next**.
- If the import is successful, then the certificates Common Name will be listed under the folder that was selected during import.

See the below matrix for information on what certificates are required to be imported and to which locations.

For OPERA V5.5.0.24 and lower

Applications	Certificate Name + Type	Import Location
OPERA Client – Imported onto every workstation that will key in CC details	MICROS_OperaToken.pfx	<ul style="list-style-type: none"> • Certificates – Current User – Personal • Certificates – Current User – Trusted Root Certification Authorities • Certificates (Local Computer) – Personal • Certificates (Local Computer) - Trusted Root Certification Authorities
OEDS – Imported for Tokenization	MICROSOperaToken.cer CHAIN.pfx	<ul style="list-style-type: none"> • Certificates – Current User – Personal

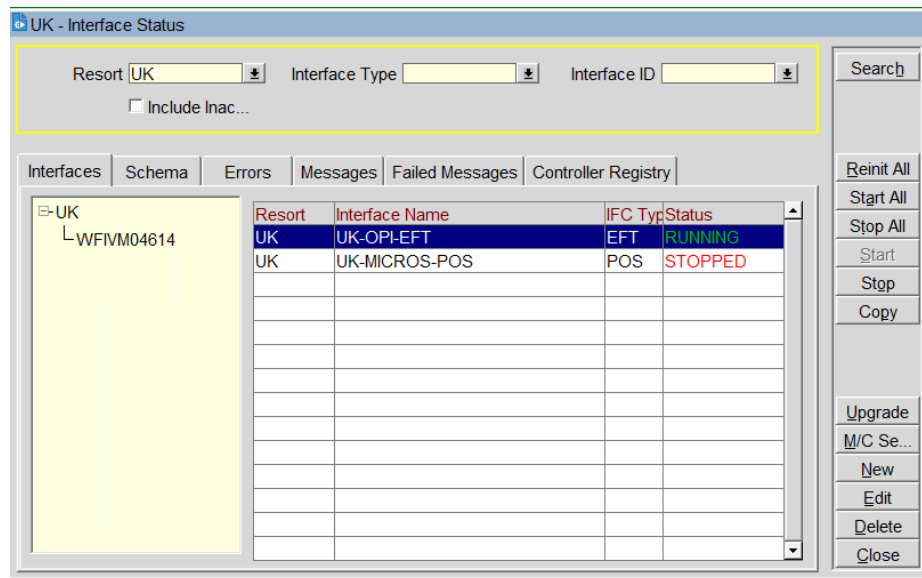
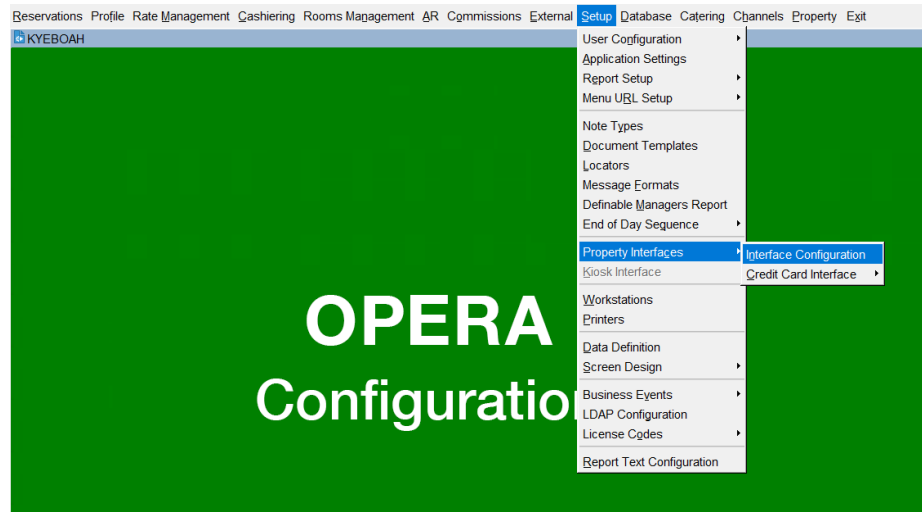
Applications	Certificate Name + Type	Import Location
	CHAIN.cer	<ul style="list-style-type: none"> • Certificates – Current User – Trusted Root Certification Authorities • Certificates – Current User – Intermediate Certification Authorities • Certificates (Local Computer) – Personal • Certificates (Local Computer) - Trusted Root Certification Authorities • Certificates (Local Computer) - Intermediate Certification Authorities
OXI - Imported for Tokenization	MICROS_OperaToken.pfx	<ul style="list-style-type: none"> • Certificates – Current User – Personal
	MICROSOperaToken.cer	<ul style="list-style-type: none"> • Certificates – Current User – Trusted Root Certification Authorities
	CHAIN.pfx	<ul style="list-style-type: none"> • Certificates – Current User – Intermediate Certification Authorities
	CHAIN.cer	<ul style="list-style-type: none"> • Certificates (Local Computer) – Personal • Certificates (Local Computer) - Trusted Root Certification Authorities • Certificates (Local Computer) - Intermediate Certification Authorities • Certificates Service (Opera interface for XXX) on Local Computer – Personal • Certificates Service (Opera interface for XXX) on Local Computer - Trusted Root Certification Authorities • Certificates Service (Opera interface for XXX) on Local Computer - Intermediate Certification Authorities

For OPERA V5.5.0.25 and higher

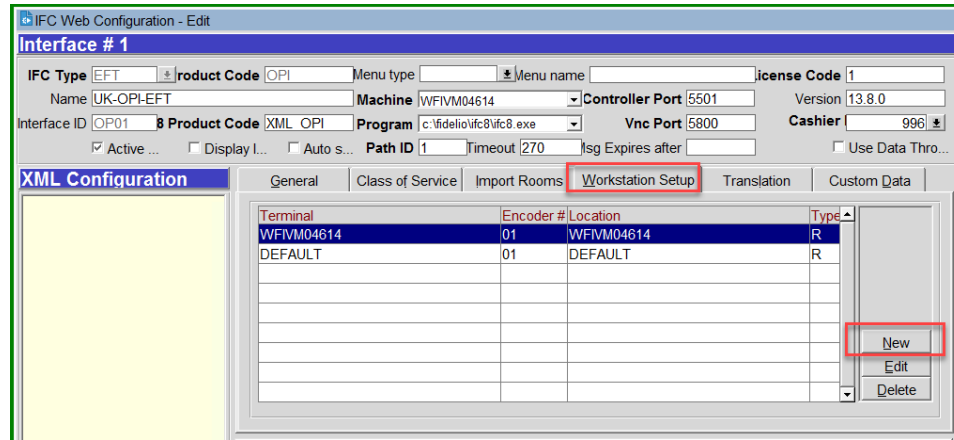
Applications	Certificate Name + Type	Import Location
OPERA Client – Imported onto every workstation that will key in CC details	MICROOperaToken.cer	<ul style="list-style-type: none"> • Certificates (Local Computer) - Trusted Root Certification Authorities
OEDS – Imported for Tokenization	MICROOperaToken.cer	<ul style="list-style-type: none"> • Certificates (Local Computer) - Trusted Root Certification Authorities
OXI - Imported for Tokenization	MICROOperaToken.cer	<ul style="list-style-type: none"> • Certificates (Local Computer) - Trusted Root Certification Authorities • Certificates Service (Opera interface for XXX) on Local Computer – Personal • Certificates Service (Opera interface for XXX) on Local Computer - Trusted Root Certification Authorities • Certificates Service (Opera interface for XXX) on Local Computer - Intermediate Certification Authorities

Configuring OPI for Hotel Mobile or OWS/Kiosk Setup in OPERA

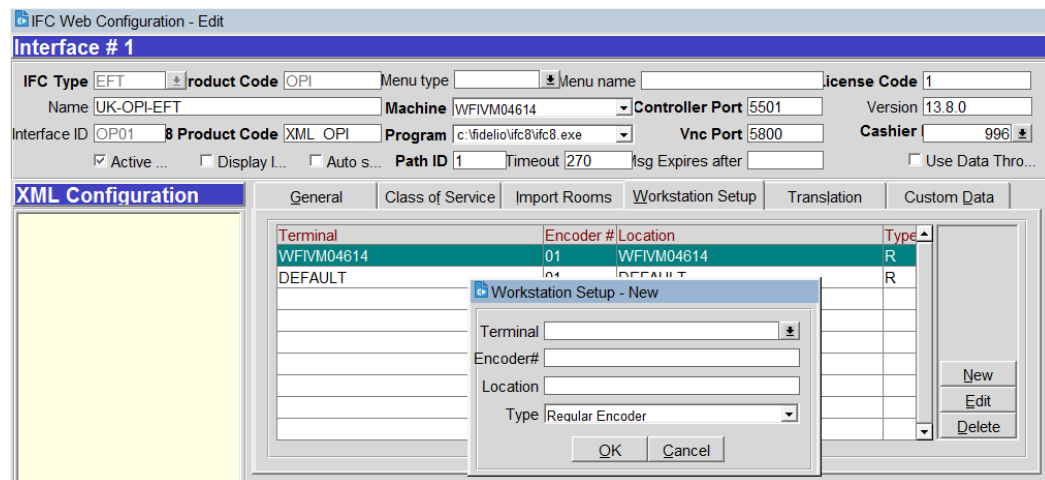
1. Go to **OPERA Configuration | Setup | Property Interfaces | Interface Configuration** | edit OPI Interface.



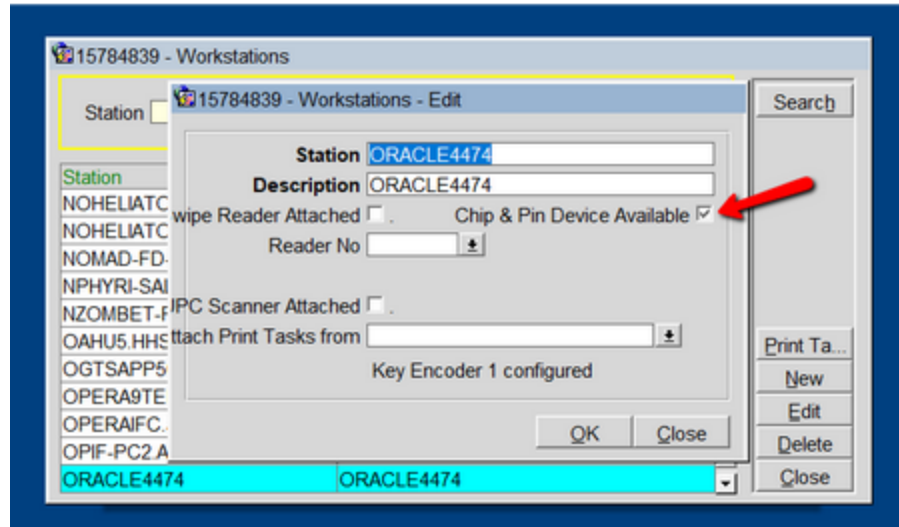
2. Select **New**.



3. Select the OPERA Workstation and enter the Encoder # provided by PSP Vendor.



4. Click **OK** to save.
5. Next go to OPERA Configuration | **Setup** | **Workstations** | to edit your workstation to allow for CP to be used from that workstations (Unless this was done prior).
6. 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).



4

Upgrading the OPI

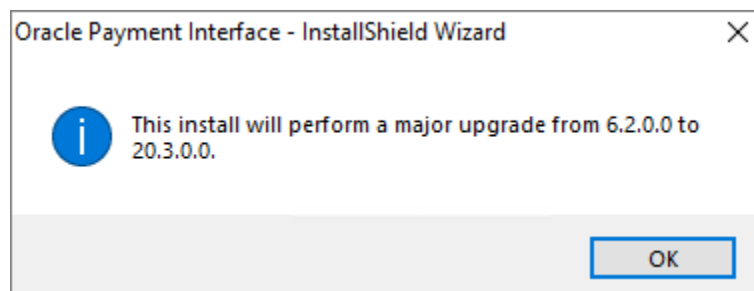
VERY IMPORTANT: Read and follow the upgrade directions.

 **NOTE:**

- OPI 6.1 cannot be upgraded to OPI 20.3. You will need to upgrade OPI 6.1 to either 6.2, 19.1 or 20.1,20.2 before upgrading it to 20.3
- OPI upgrade functionality supports:
 - Upgrading OPI 6.2 (include patch releases) to OPI 20.3
 - Upgrading OPI 19.1 (include patch releases) to OPI 20.3
 - Upgrading OPI 20.1 (include patch releases) to OPI 20.3
 - Upgrading OPI 20.2 (include patch releases) to OPI 20.3

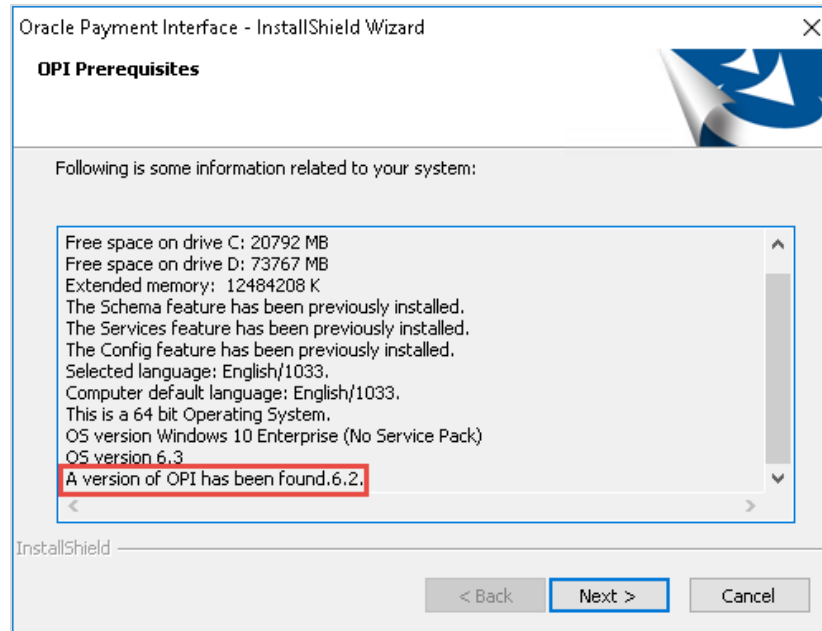
Upgrading OPI 6.2.0.0 to 20.3.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.3.0.0.exe** file and select **Run as Administrator** to perform an upgrade.
2. Select your language from the drop-down list, and click **OK**.
3. Click **Next**.
4. Click **OK**.



5. Click **Next**.

Ensure all the prerequisites for the OPI installation are met.



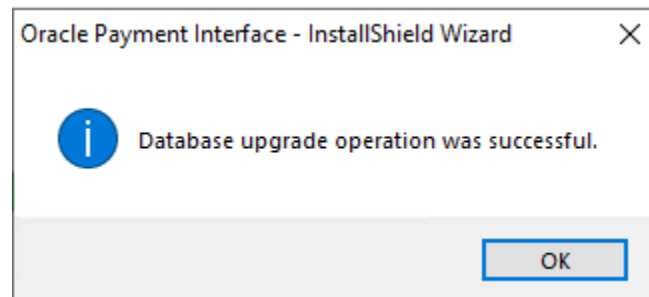
6. Choose a Destination Location. Accept the default installation location or click **Change...** to choose a different location.

7. Click **Next**.

The **Ready to Install the Program** screen appears.

8. Click **Install** to begin the installation.

9. Click **OK**.



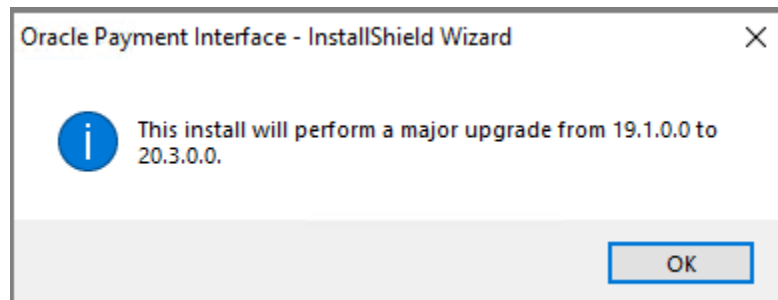
10. Enter the **Host** and **Port** that should be used to connect to the OPI Config Service for the Merchant Configuration.

11. Once the installation is complete, the installer will prompt for a reboot of the host machine.

12. Click **Finish** and reboot the system.

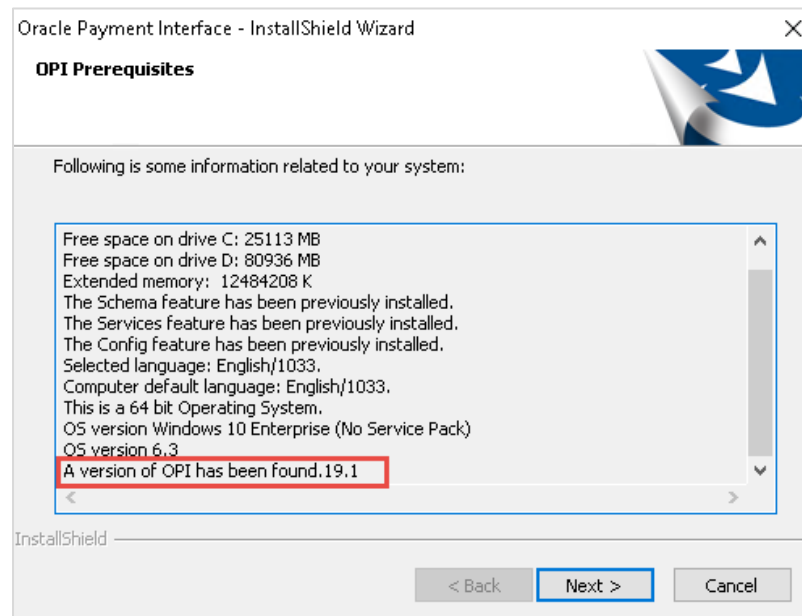
Upgrading OPI 19.1.0.0 to 20.3.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.3.0.0.exe** file and select **Run as Administrator** to perform an upgrade.
2. Select your language from the drop-down list, and click **OK**.
3. Click **Next**.
4. Click **OK**.



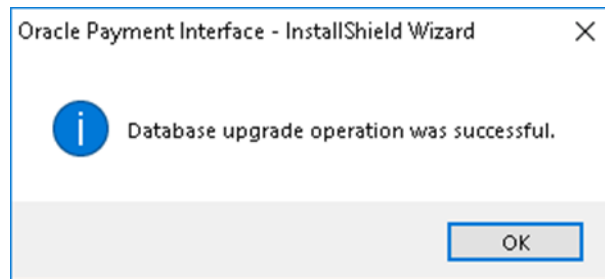
5. Click **Next**.

Ensure all the prerequisites for the OPI installation are met.



6. Choose a Destination Location. Accept the default installation location or click **Change...** to choose a different location.
7. Click **Next**.
The **Ready to Install the Program** screen appears.
8. Click **Install** to begin the installation.

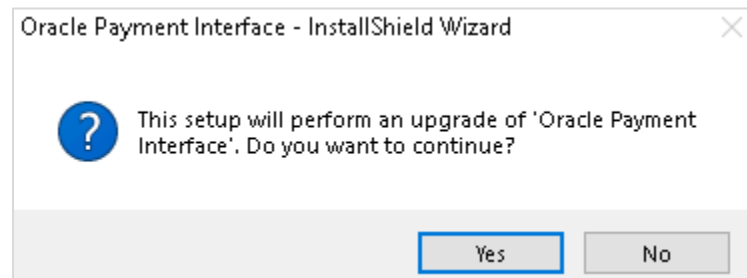
9. Click **OK**.



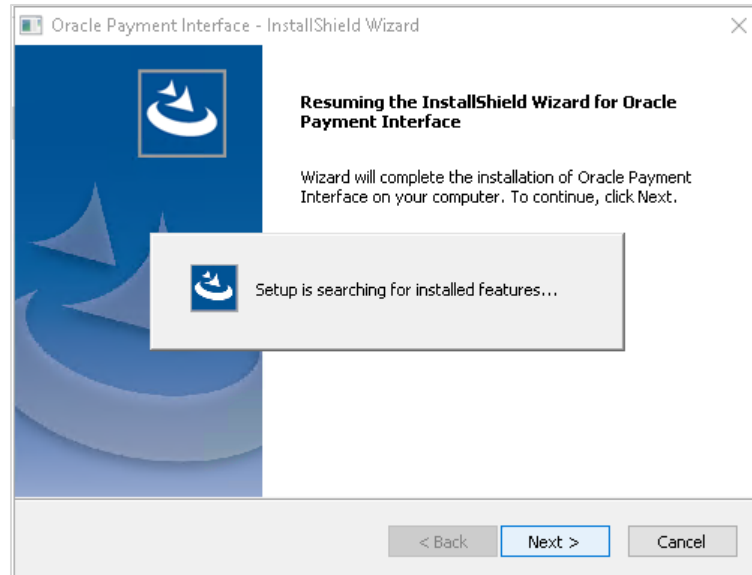
10. Enter the **Host** and **Port** that should be used to connect to the OPI Config Service for the Merchant Configuration.
11. Once the installation is complete, the installer will prompt for a reboot of the host machine.
12. Click **Finish** and reboot the system.

Upgrading OPI 20.1.0.0 to 20.3.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.3.0.0.exe** file and select **Run as Administrator** to perform an upgrade.

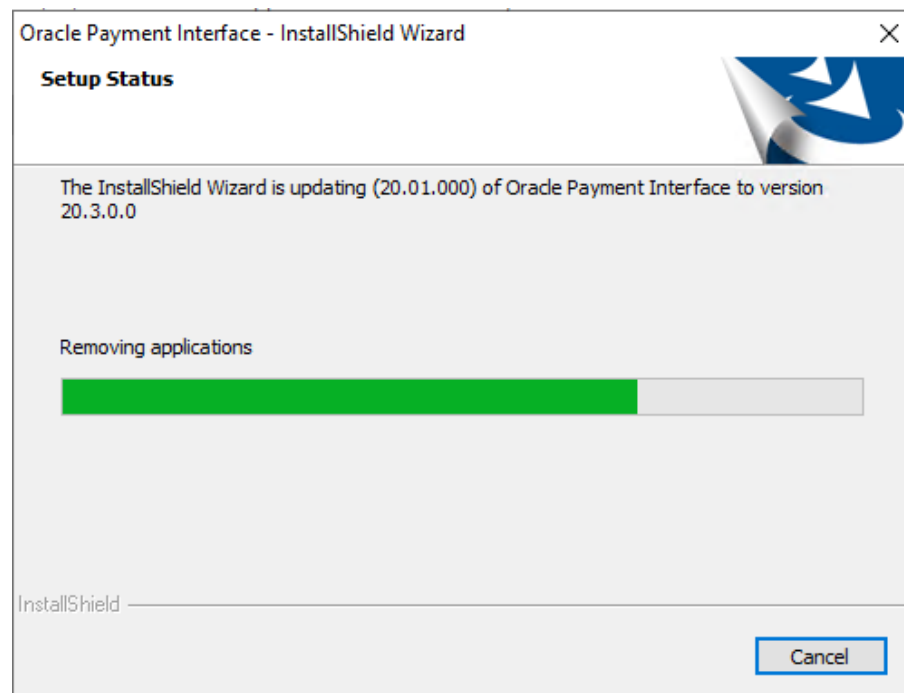


2. Click **Yes**.



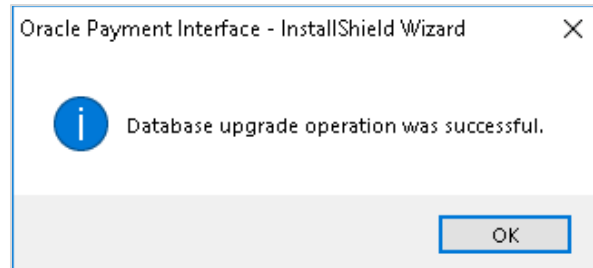
3. Click **Next**.

Setup is searching for installed features.

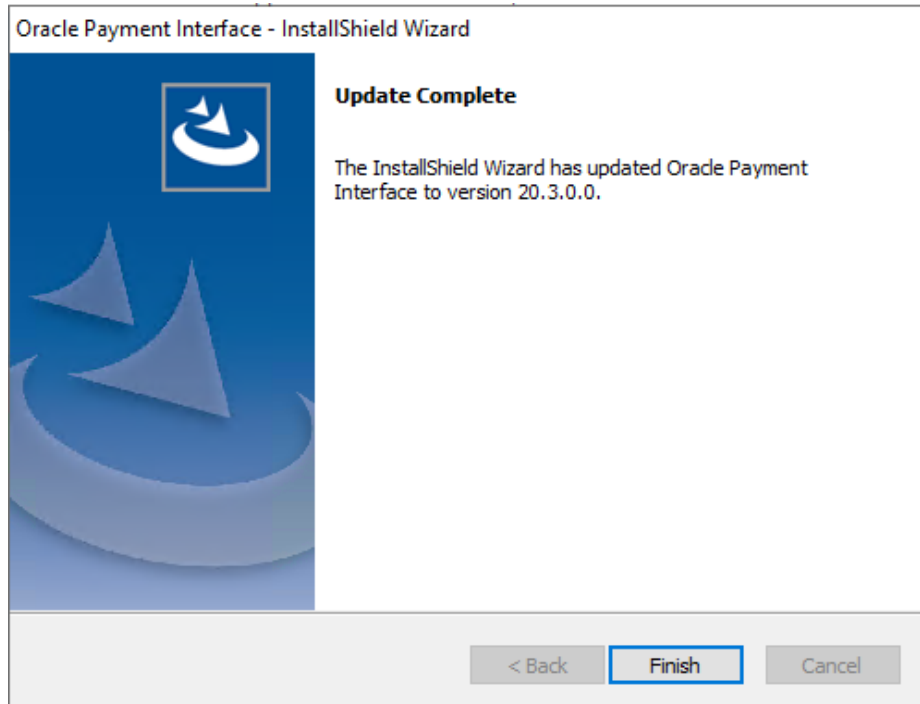


4. Click **Next**.

The Install wizard is updating from **OPI 20.1** to version **20.3**.



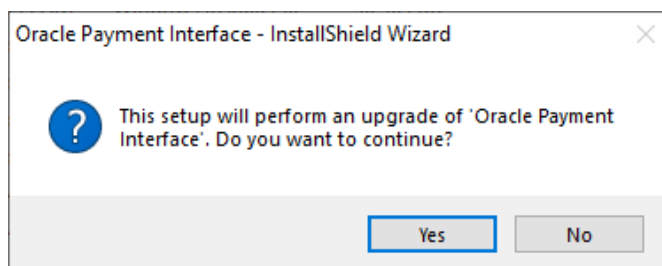
5. Click **OK**.



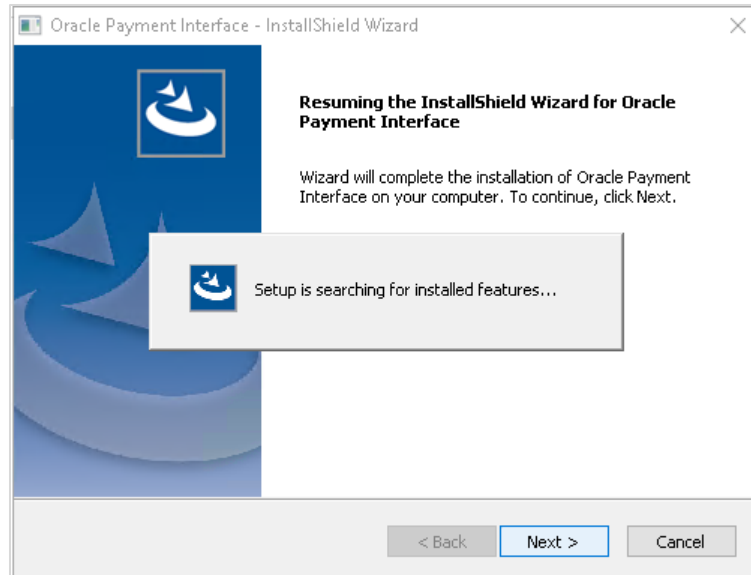
6. Click **Finish**.

Upgrading OPI 20.2.0.0 to 20.3.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.3.0.0.exe** file and select **Run as Administrator** to perform an upgrade.

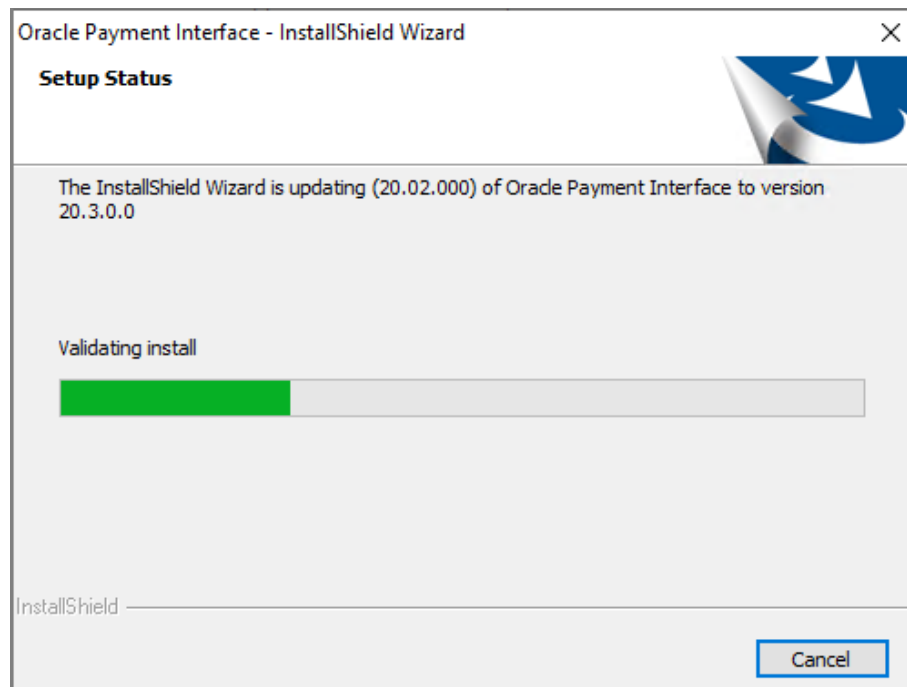


2. Click **Yes**.



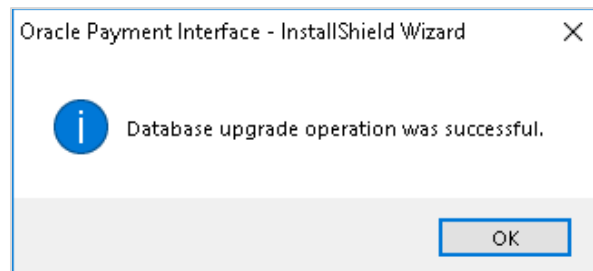
3. Click **Next**.

Setup is searching for installed features.

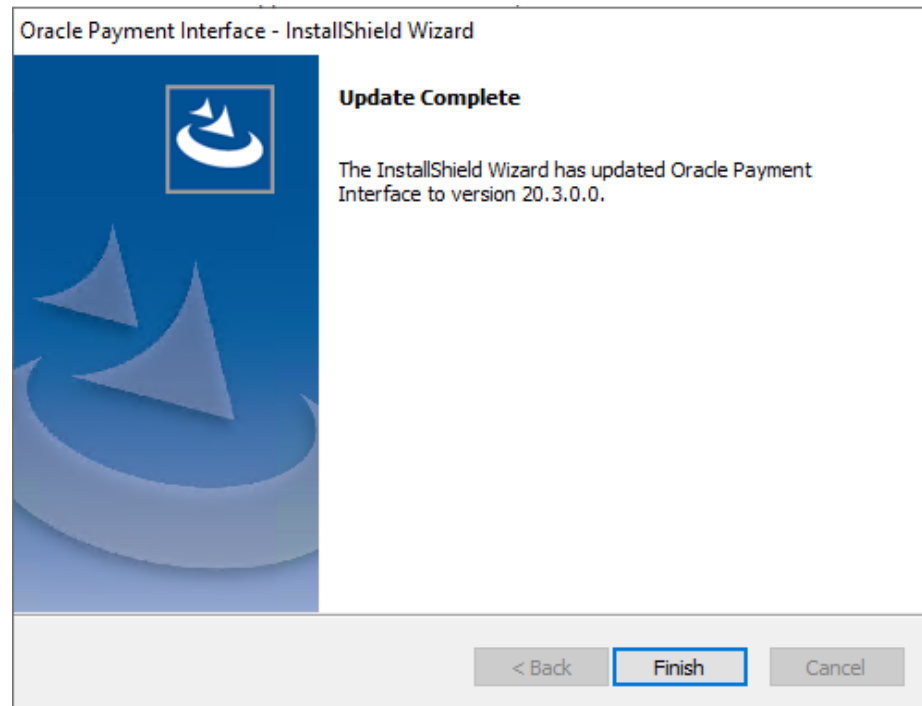


4. Click **Next**.

The Install wizard is updating from **OPI 20.2** to version **20.3**.



5. Click **OK**.



6. Click **Finish**.

5

OPERA Folio Print Receipt Setup for OPI

Setup in OPERA PMS

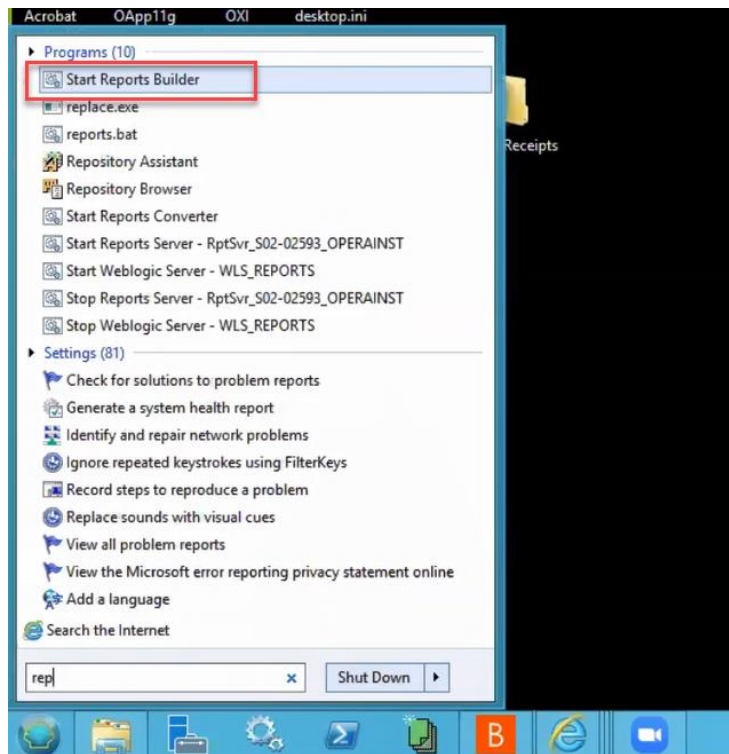
As part of the standard OPERA OPI configuration, the installers can follow the below process for updating the customers folio and receipt templates to show the OPI transaction details.

OPERA Folio Print Receipt Setup for OPI

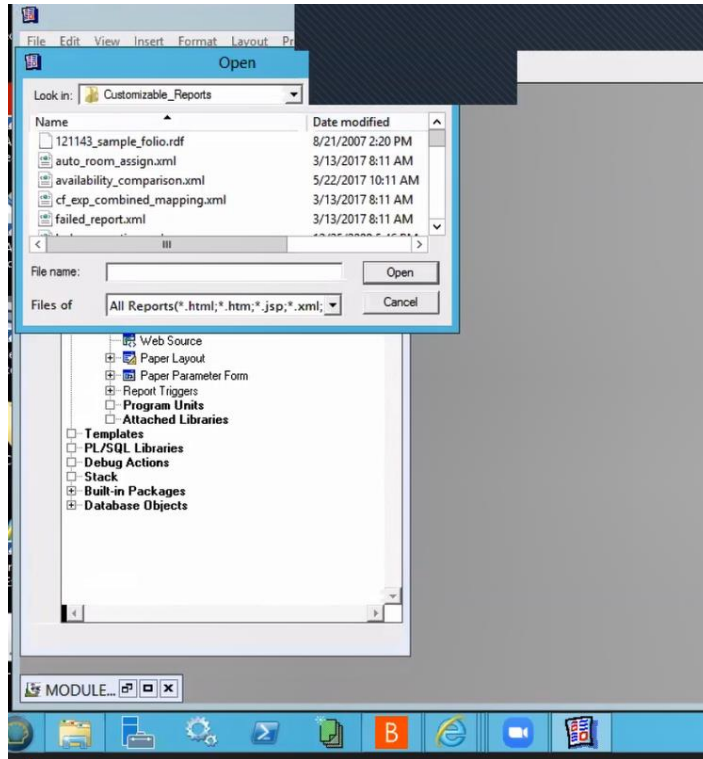
Included in this pack are copies of the sample folio and deposit/payment receipts. On the Data Model within these templates, there is a query called 'merchant info' with two files promotional_text1 and promotional_text2.

To access the screen, open the Oracle Reports Builder.

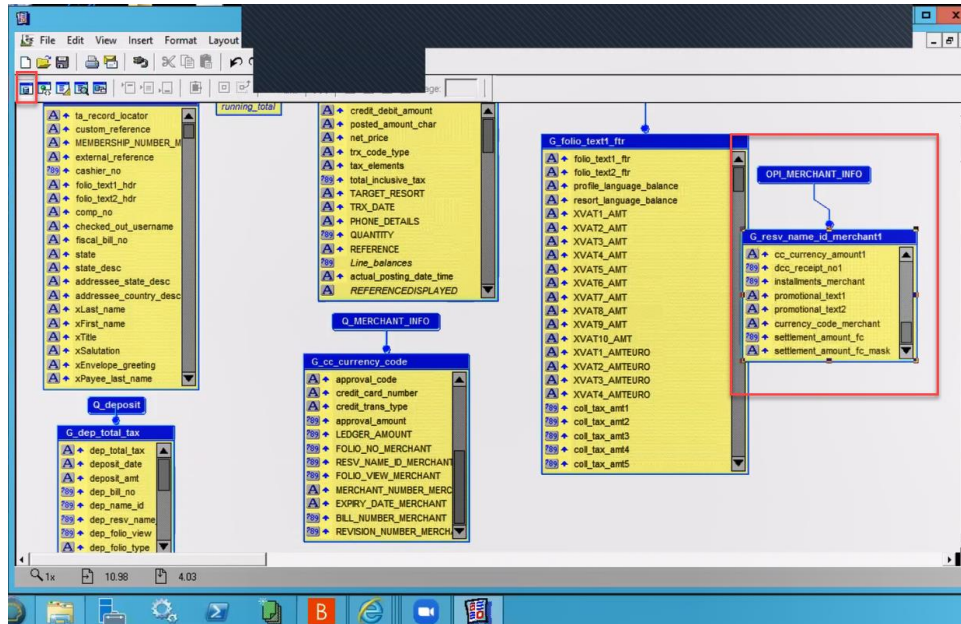
- Go to **Start > Programs > Start Report Builder**.



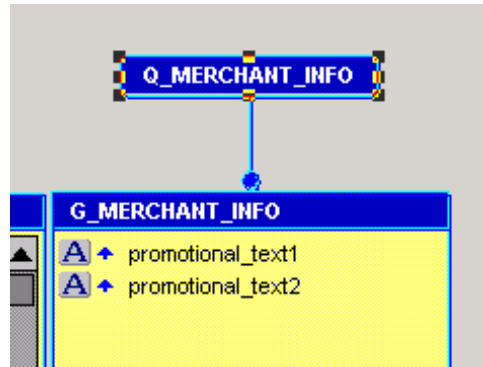
- Log into report builder.
- Open the file to be edited.



- Open the Module page.

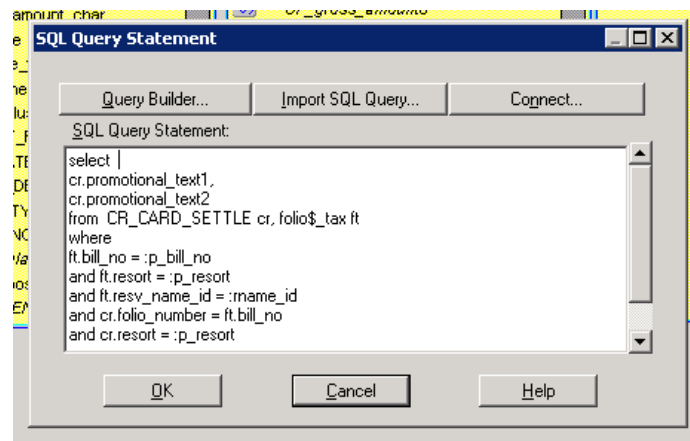


- Select the “promotional text” section.



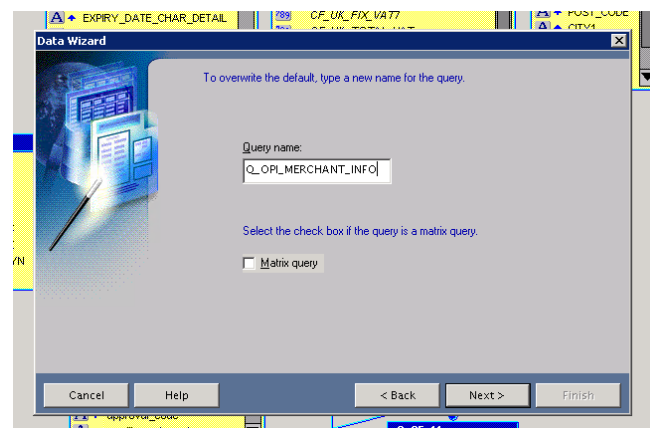
You need this query to copy over to the existing folio/receipt. For OPI, we need these fields as the database adds a 'picture' of the transactions into these fields.

- To copy the query:
 - Double-click the Q_MERCHANT_INFO to open the query statement field.
 - Select all the query and copy (ctrl+c).

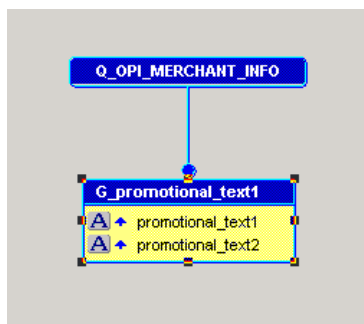


In the existing customer folio, on the Data Model:

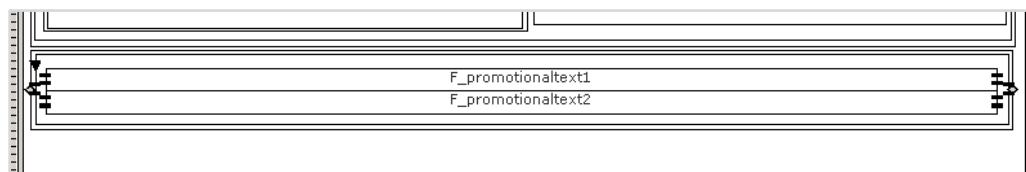
- Go to **Insert > Query** and follow the data wizard to add in the query. Name the query OPI_MERCHANT_INFO.



- Click **Next > select SQL Query > Next > paste the query > Next > Next > Finish**. Then you can move the query to a blank space on the Data Model:



- On the Page Layout you can replace the old credit card fields with the Promotional Text fields.
- Delete the existing fields and frames, add a new frame and link it to the OPI_MERCHANT_INFO query, then add two fields linked to the promo_text fields, as shown below:



 **NOTE:**

Ensure to set the frame and fields to expand on the Vertical axis.

- In the OPERA Standard Stationery folder on the DC there are two folio's already set up:
 - UK_FOLIO_OPI_ORACLE – standard VAT layout
 - UK_FOLIO_OPI_VAT_ORACLE – modified VAT layout (compatible with long term VAT functionality)
- There is also a deposit receipt and a payment receipt in the same folder.

Verifying Folio information in OPERA PMS

The PrintData information should be sent from the Payment Provider (Vendor) for ALL entry (Manual or via Chip & Pin).

In order to get the Print receipt data look organized, it is recommended to request the vendor to configure each fields separated by a pipe (|). Below example shows the before and after display of data in folio.

Display of Data in Folio

- Data sent without pipe separation:

```
2020/08/11 06:27:57
*****Sales Completion*****
MERC ID:00 [REDACTED]
REF No: 001[REDACTED]
CT No: *****8[REDACTED]
EXP: XX/XX
CARD: MASTERCARD
CheckNo:1[REDACTED]
APPROVAL CODE: 0[REDACTED]
EMV Receipt Section
TRANSACTION RECORD
IMPORTANT - RETAIN FOR YOUR RECORDS
01 APPROVED - THANK YOU 027
REF
66[REDACTED]M
CURRENCY:USD
CHECK-IN DATE:081020
```

- Data sent with a pipe separation:

```
Sample Data
MERC ID:003020XXXX469|REF No: 001031XXXXM |CT
No: *****3393
|EXP: XX/XX|CARD: MASTERCARD|CheckNo:136XXX7 End
result
```