

Oracle® Hospitality Payment Interface

OPERA V5 OPI Installation and Reference Guide



Release 20.2
F32295-01
July 2020



Copyright © 2010, 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

Contents	3
Preface	4
1 Pre-Installation Steps	1-1
2 Installing the OPI	2-1
Token Exchange Settings	2-10
Certificates	2-11
3 OPERA Configuration	3-1
Creating an EFT Interface	3-1
Configuring CHIP AND PIN (EMV)	3-2
Configuring the CC Vault	3-5
Cashiering Overview	3-6
Overview of Credit Card Payment Types	3-7
Credit Card Type Payment Setup Information	3-8
Configuring the Workstation	3-14
Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC)	3-14
Configuring Authentication for the Hotel Property Interface (IFC8) with OPI	3-16
Perform a Tokenization	3-18
4 Upgrading the OPI	4-1
Upgrading OPI 6.2.0.0 to 20.2.0.0	4-1
Upgrading OPI 19.1.0.0 to 20.2.0.0	4-3
Upgrading OPI 20.1.0.0 to 20.2.0.0	4-4

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 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
- 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.

1

Pre-Installation Steps

IF UPGRAADING 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 20.2 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 20.2.
- OPI upgrade functionality supports:
 - Upgrading OPI 6.2 (include patch releases) to OPI 20.2
 - Upgrading OPI 19.1 (include patch releases) to OPI 20.2
 - Upgrading OPI 20.1 (include patch releases) to OPI 20.2
- 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.
- OPI 20.2 supports Oracle Database 19c.

 **NOTE:**

Stay current by upgrading your Java version as Oracle CPUs/Alerts are announced.

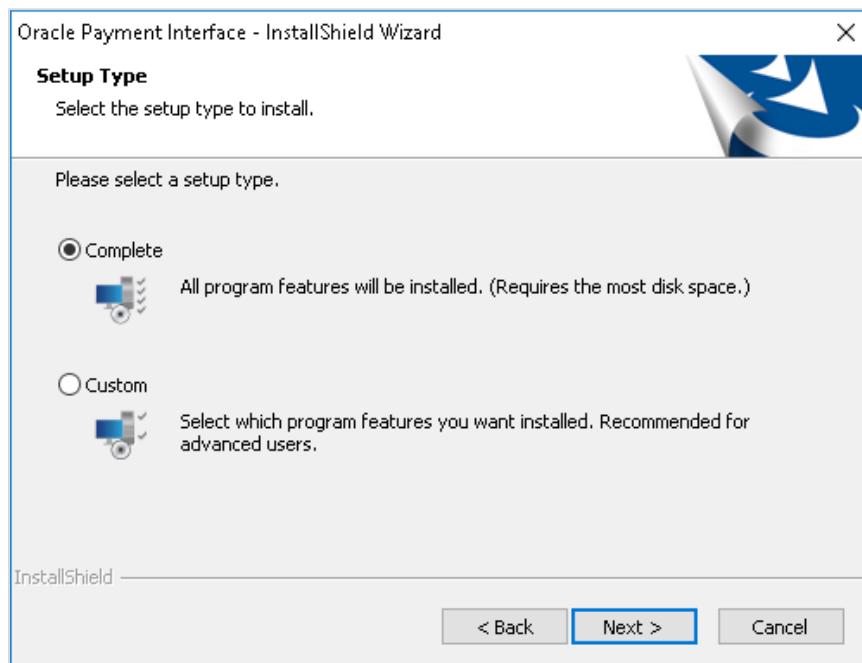
During the installation you must confirm the following:

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

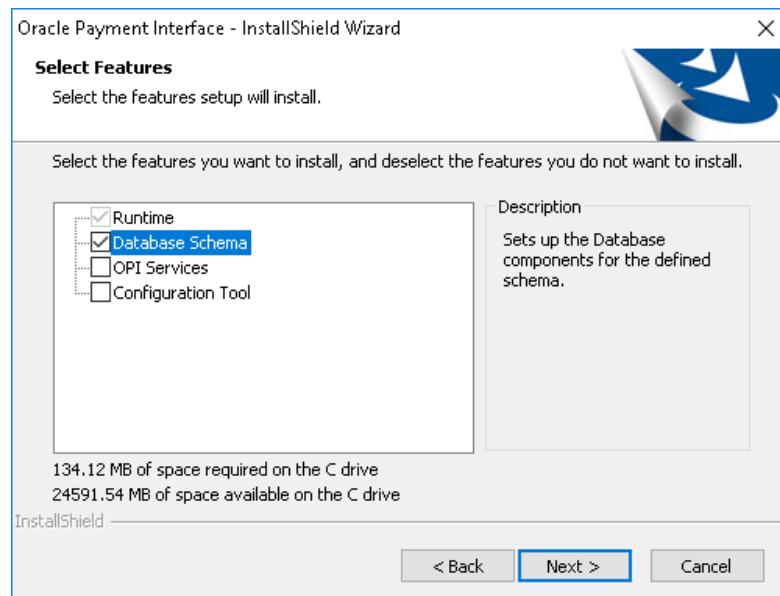
2

Installing the OPI

1. Right-click **OraclePaymentInterfaceInstaller_20.2.0.0.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.



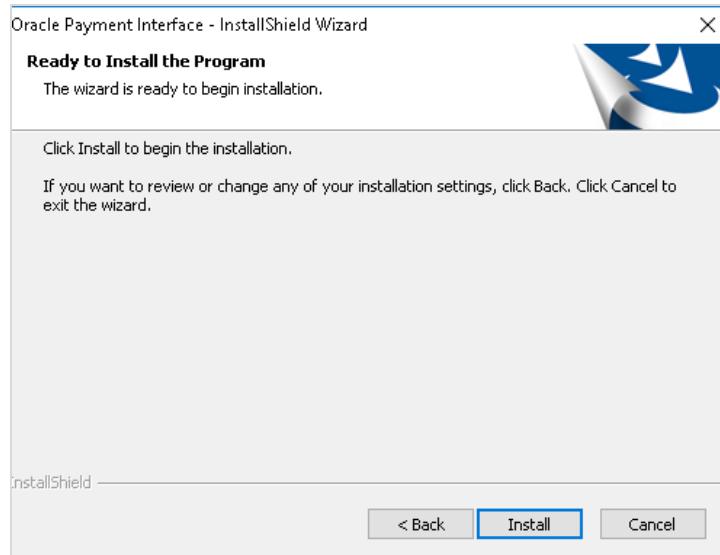
If you selected the Custom install option, the Select Features screen appears with the following options:

- 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.

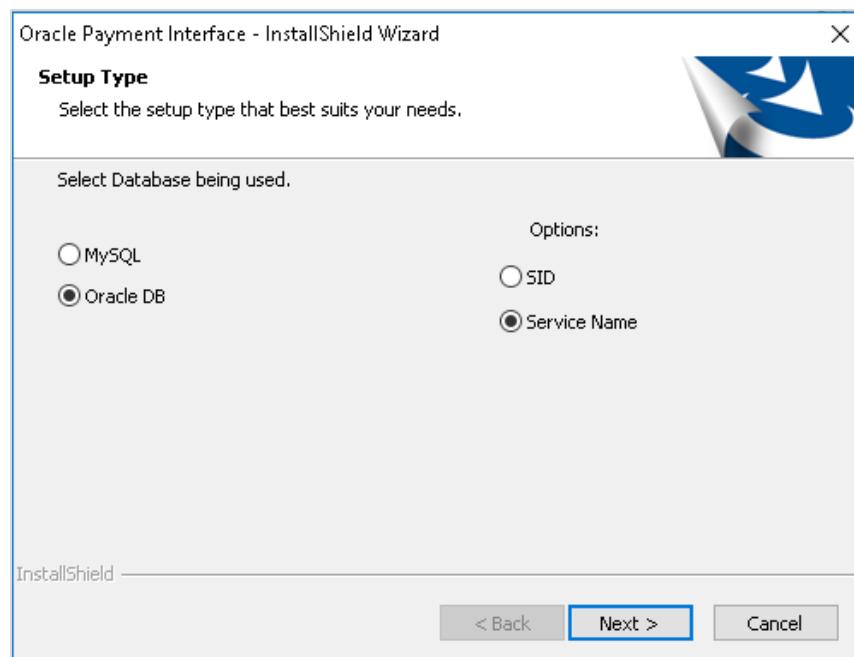
7. Select the features to install on this computer, and click **Next**.
8. Click **Change** to amend the installation drive or path, if required and click **Next**.
9. Click **Install** to begin installation.

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



10. Select your Database type:

- MySQL
- 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.

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**.

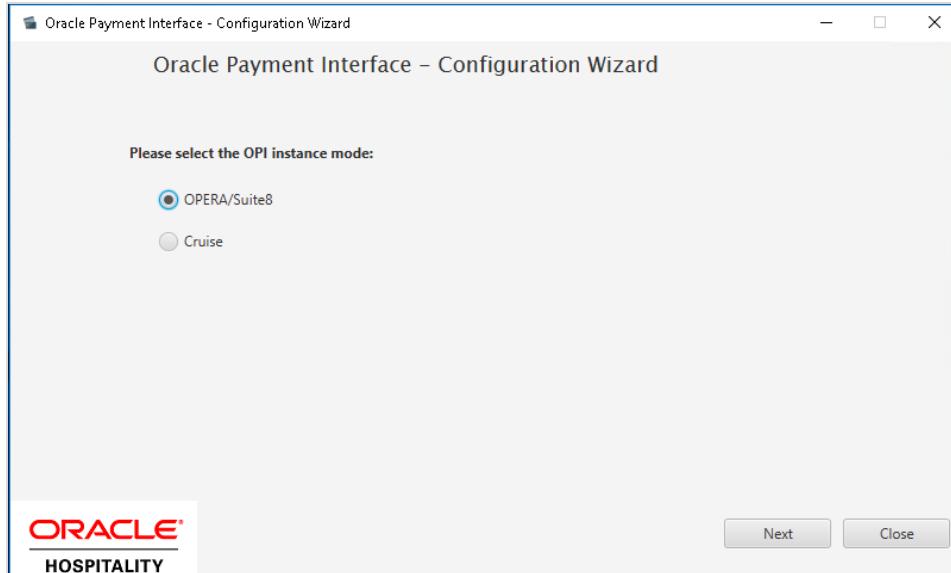
NOTE:

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\v20.2\Config\LaunchWizard.bat)

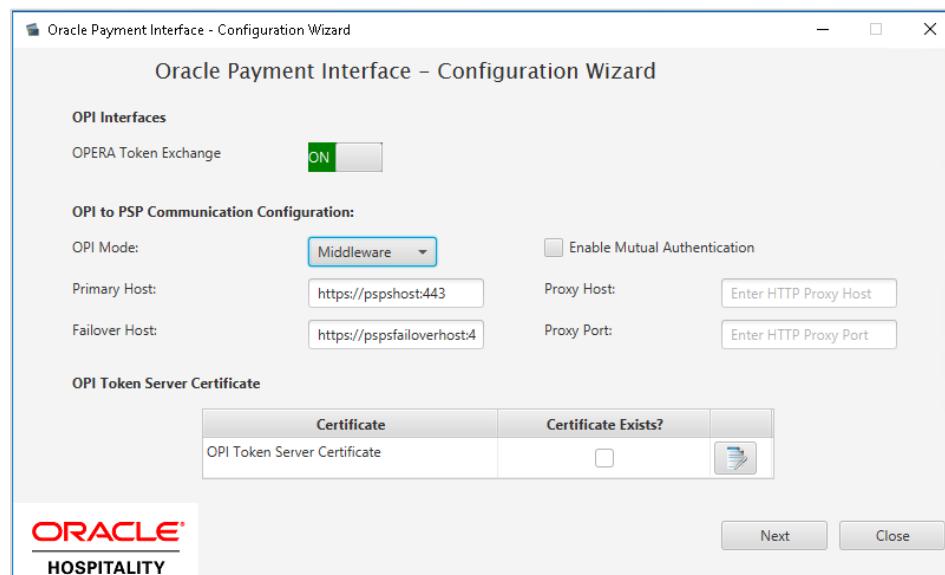
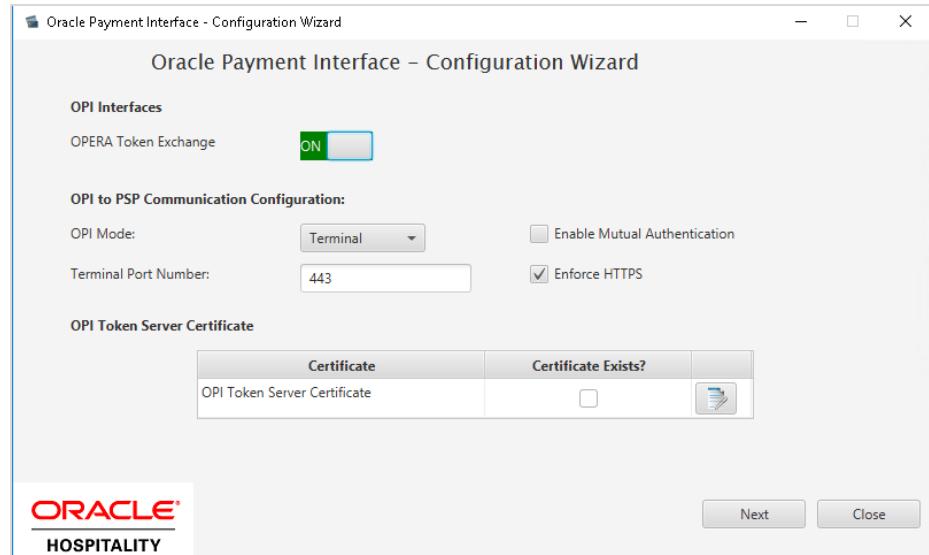
18. **OPERA Token Exchange:** This option is enabled by default for all OPERA token exchange services.

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.

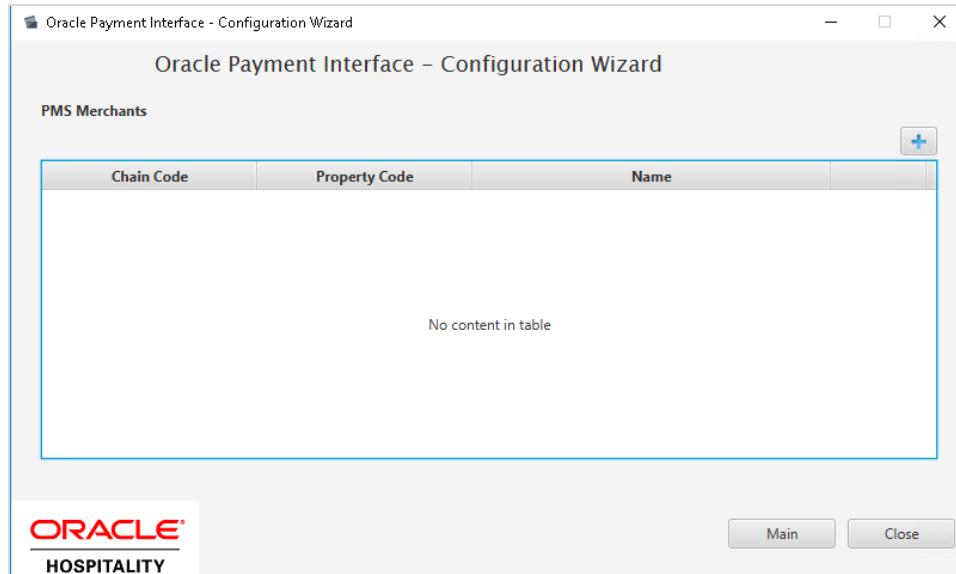
NOTE:

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:

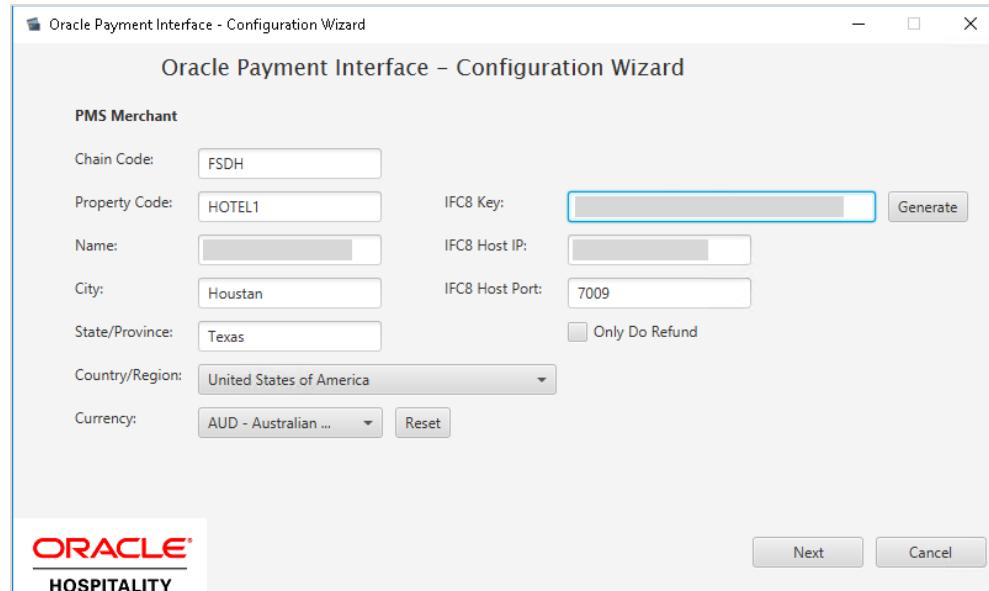
- The **OPERA Vault Chain Code** and **Property Code**; will form the **SitId** value in the Token request messages.

 **NOTE:**

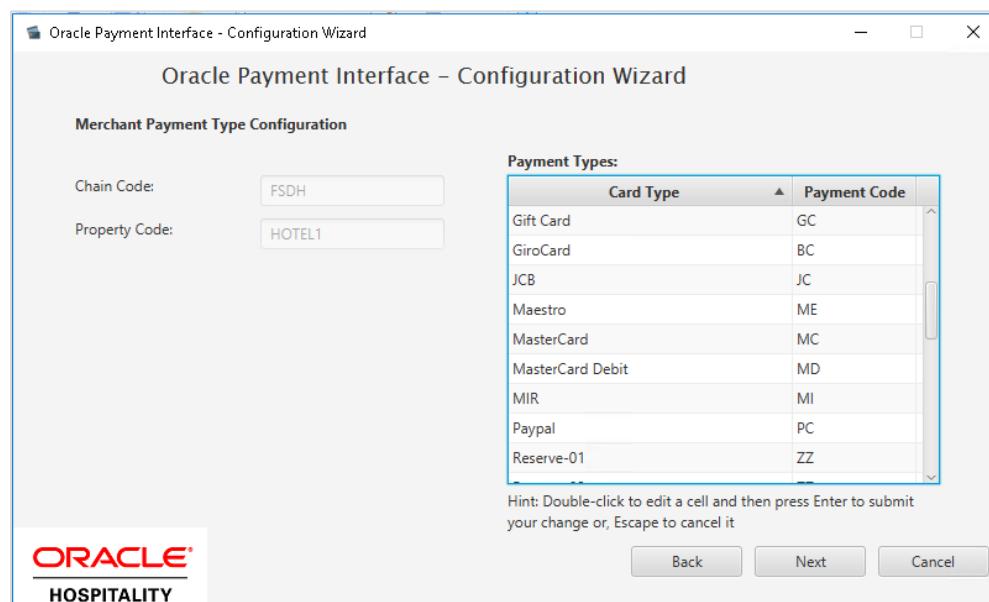
Chain Code and **Property Code** values need to be in upper case.

- 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**, **State/Province** and **Country/Region** information.
- 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.
- Select the option **Only Do Refund** if you want to disable differentiating between void and refund from OPERA.
- Click **Next**.

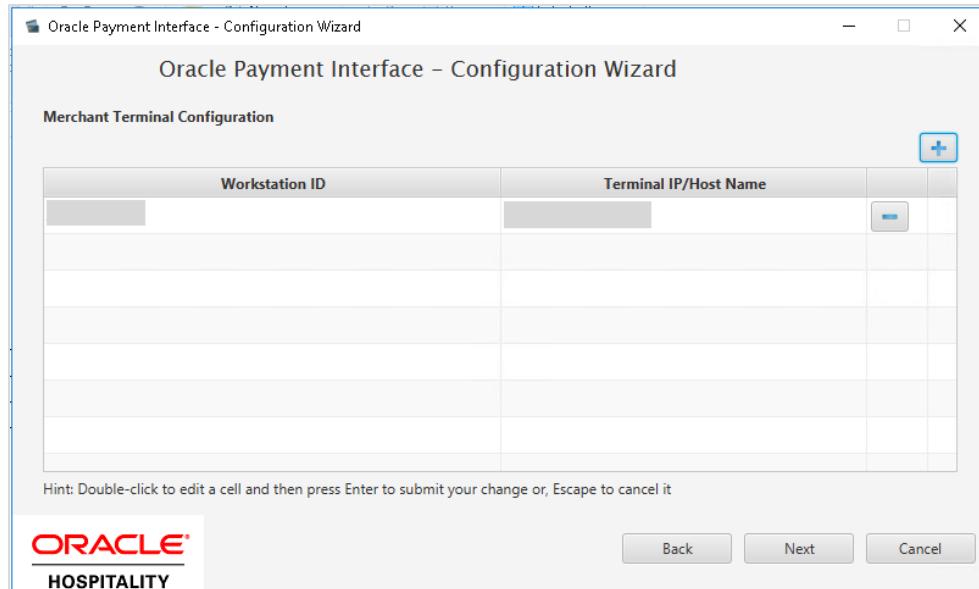
Although the other populated settings are not directly related to the Token Exchange Service configuration, Token Exchange is not possible if the IFC8 interface is not running, as OPI cannot progress past the IFC8 startup if the IFC8 connection is not possible.



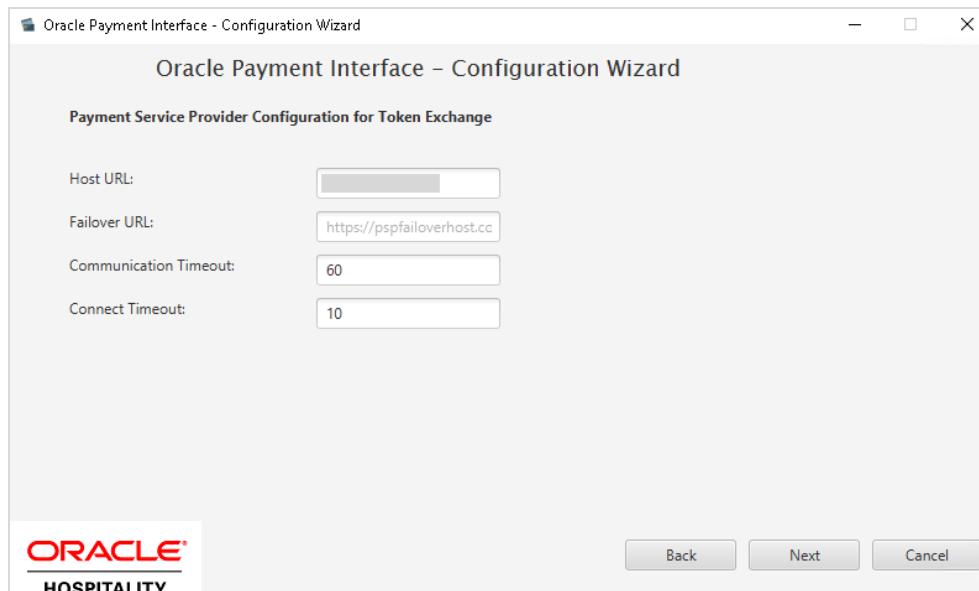
21. Enter the OPERA payment code for each card type, and click **Next**.



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**.



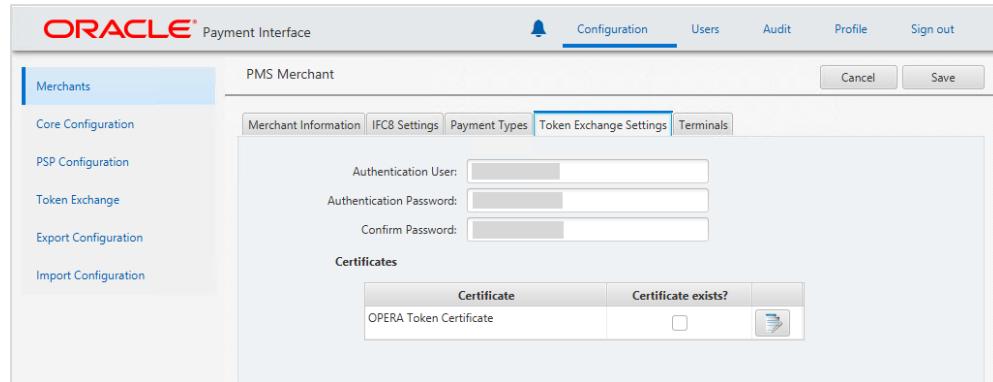
23. Click **Finish** to restart

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

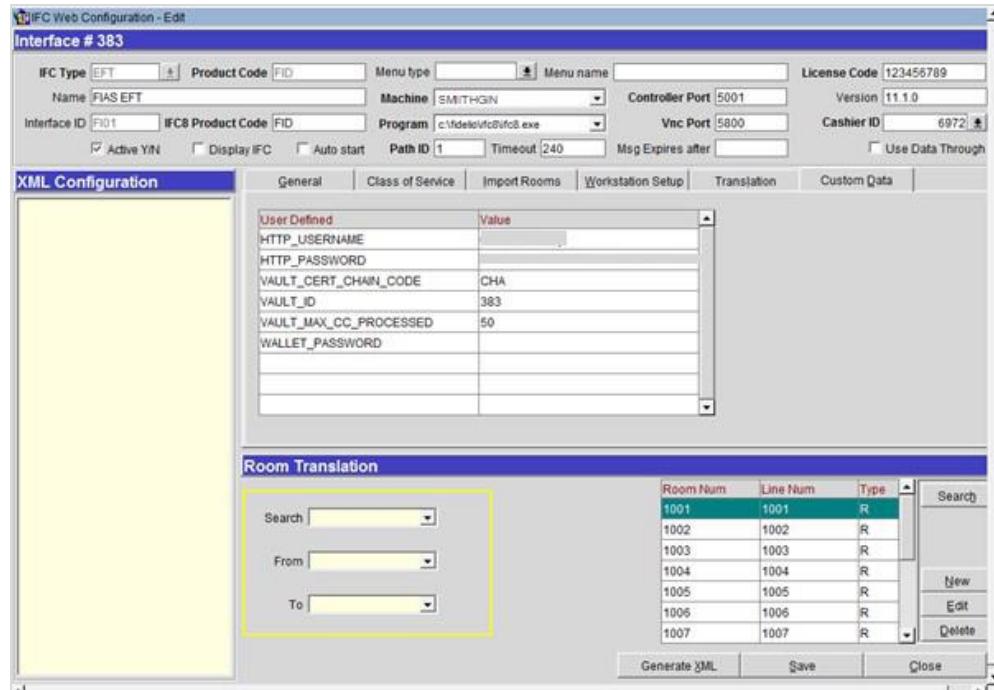
- Run **\OraclePaymentInterface\v20.2\Config\LaunchConfiguration.bat**
- Login with the Super user account created during OPI installation.
- Select **MERCHANTS** tab, and click **Token Exchange Settings** subtab.



The screenshot shows the Oracle Payment Interface configuration interface. The top navigation bar includes links for Configuration, Users, Audit, Profile, and Sign out. The main menu on the left has sections for Core Configuration, PSP Configuration, Token Exchange, Export Configuration, and Import Configuration. The 'Merchants' section is currently selected. Within the 'Merchants' section, the 'PMS Merchant' sub-section is active. The 'Token Exchange Settings' subtab is selected within the 'Merchant Information' tab group. The configuration form includes fields for Authentication User, Authentication Password, and Confirm Password. Below these fields is a 'Certificates' section with a table for managing certificates, showing one entry for 'OPERA Token Certificate'.

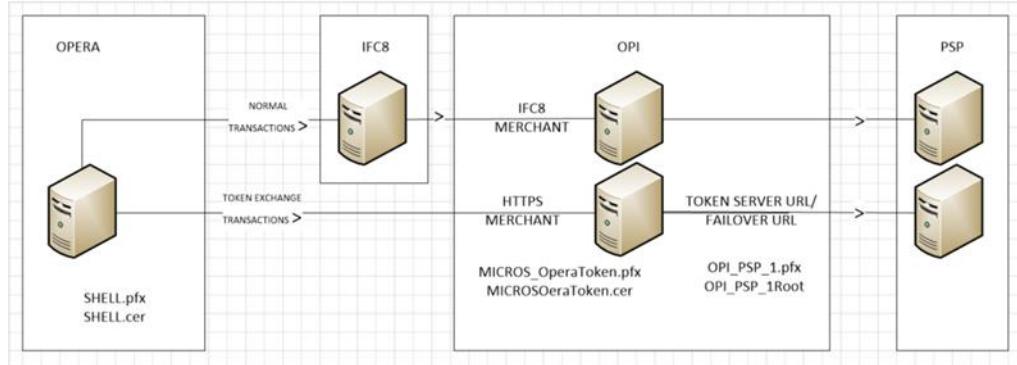
- **Authentication User:** The username for OPERA Authentication.
- **Authentication Password:** The password for OPERA Authentication.
- **Confirm Password:** The password for OPERA Authentication.

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

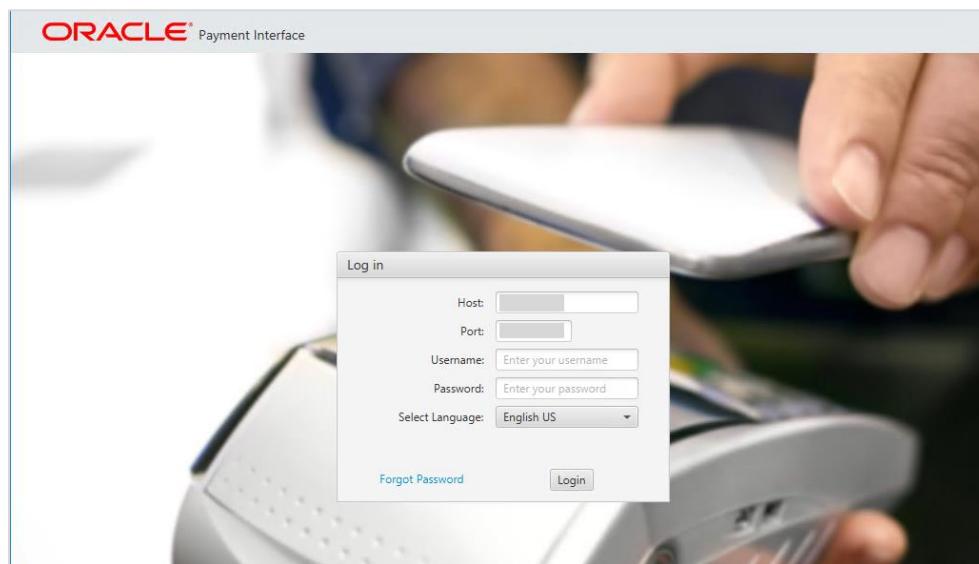
The communication from OPI to the PSP for the token exchange uses HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed on PSP (server side) for HTTPS communication, the PSP is also expected to provide a client side certificate 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\20.2\Config\LaunchConfiguration.bat**
2. Login with the Super user account created during OPI installation.



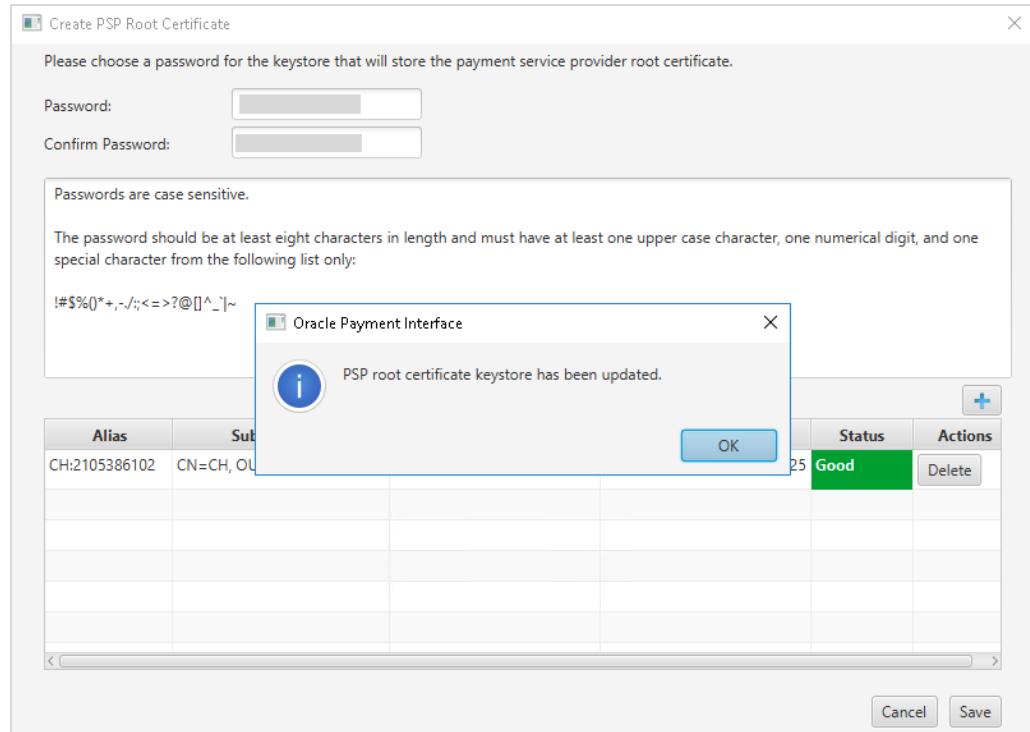
Handling the Root Certificate File by OPI Configuration Tool.

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.

Alias	Subject Name	Valid From	Valid To	Status	Actions
CH:2105386102	CN=CH, OU=Finance, O=OR...	Fri Jun 12 07:49:19 EDT 2020	Thu Jun 12 07:49:19 EDT 2025	Good	Delete

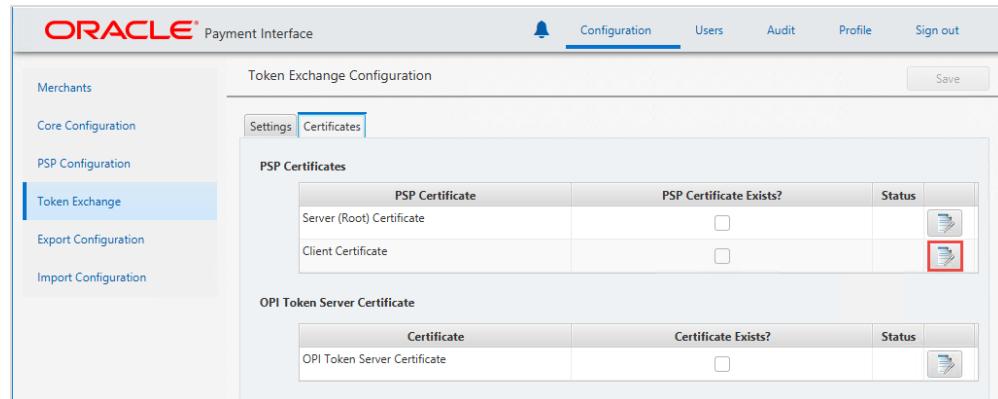
3. Click **Save**.



OPI_PSP_1Root is created under **\OraclePaymentInterface\v20.2\Services\OPI\key**

Handling the Client Side Certificate

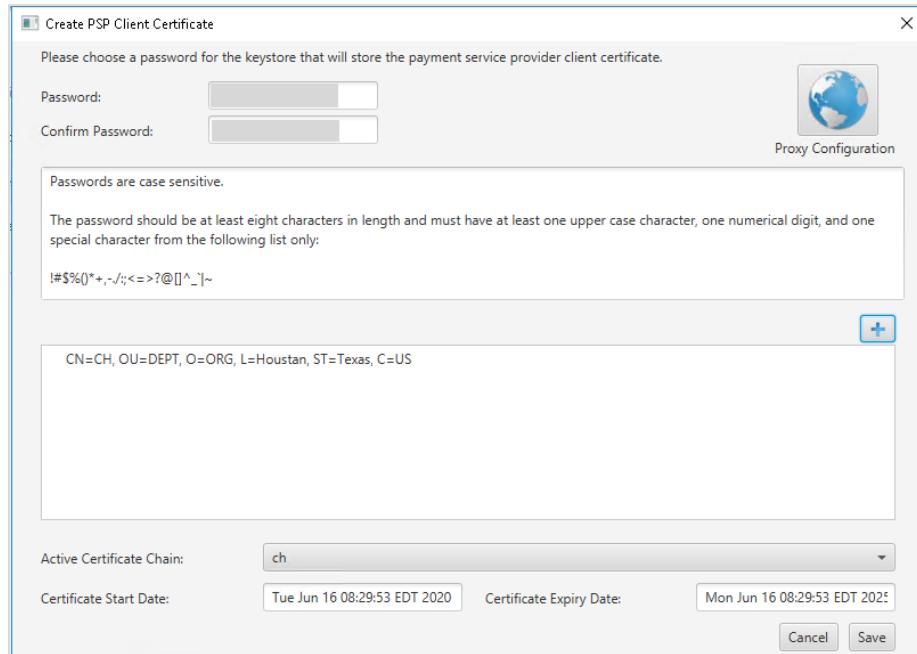
1. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Client Certificate**.



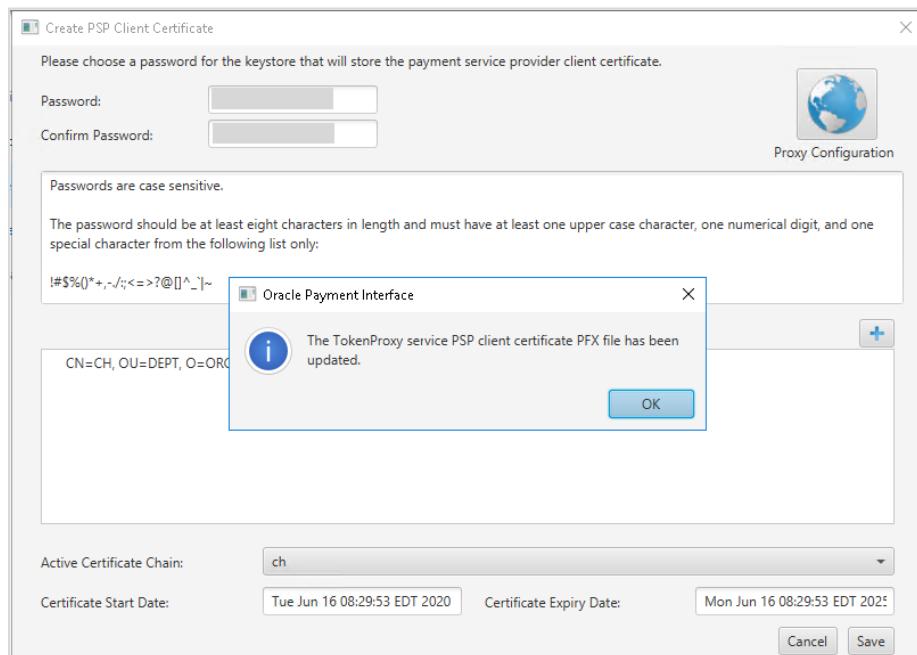
2. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** (+) icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements mentioned below 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\v20.2\Services\OPI\key** folder.

OPI - Server Side Certificates

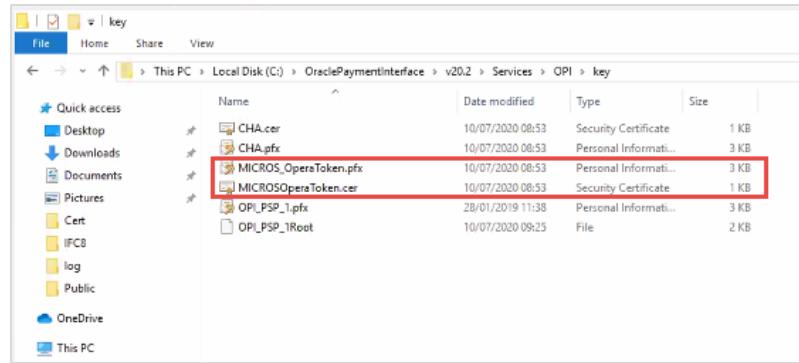
The lower half of the page relates to generating server side certificate used in communication from OPERA to OPI.

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\v20.2\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 **MICROSOOPERAToken.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.

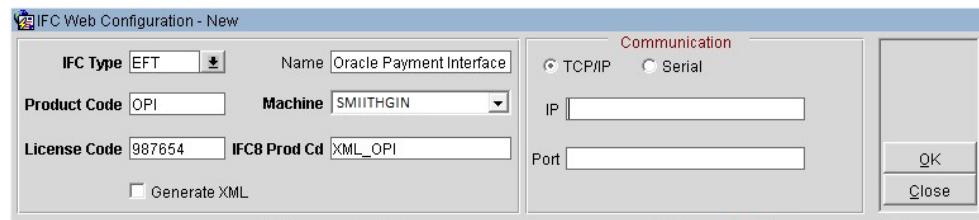
- OPERA V5.5.0.23 and V5.6.4.0.
- OPERA Cloud 19.2.0.0 and 1.20.16.0.

3

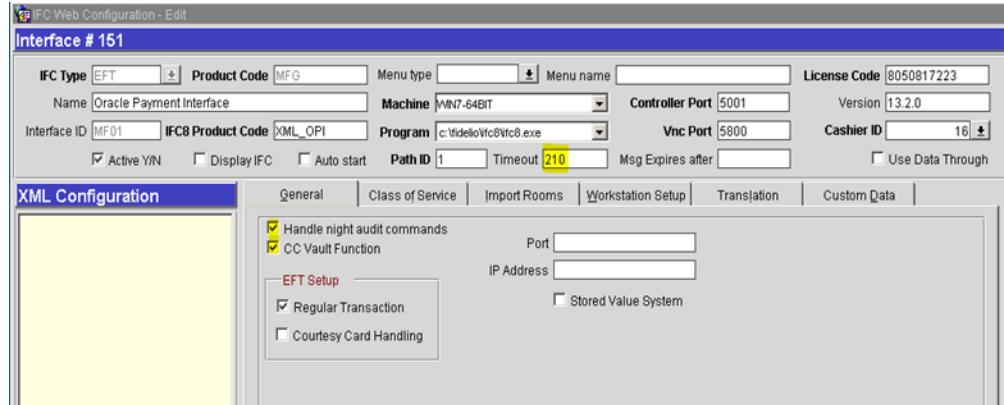
OPERA Configuration

Creating an EFT Interface

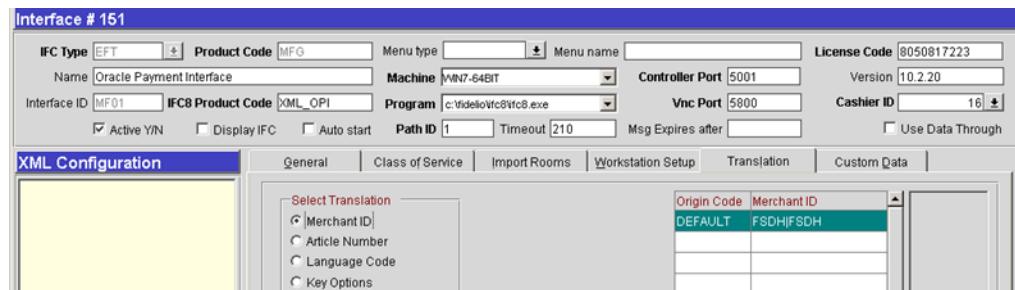
1. Log in to OPERA and go to **Configuration**.
2. Select the menu option **Setup | Property Interfaces | Interface Configuration**. If there is no active EFT or CCW IFC Type, select **New** to add configuration for a new EFT interface.
3. Enter the following options, and then click **OK**:
 - **IFC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



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.



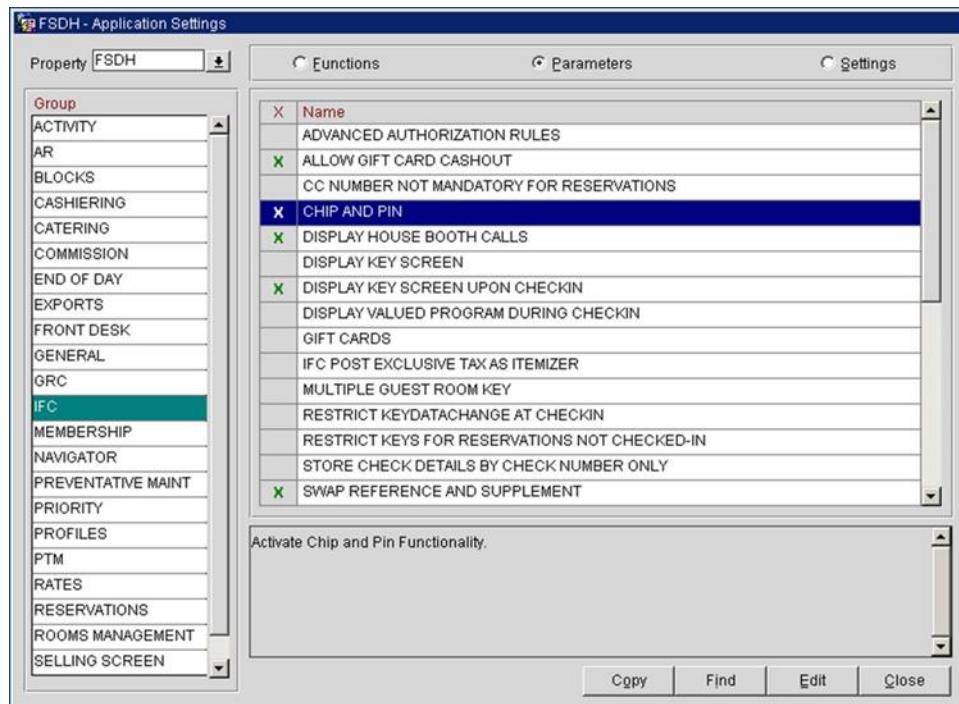
7. Select the **Translation** tab, and click **Merchant ID**.
8. Select **New** to add the Merchant ID. This must be the same as previously configured in OPI (MPG) Configuration.



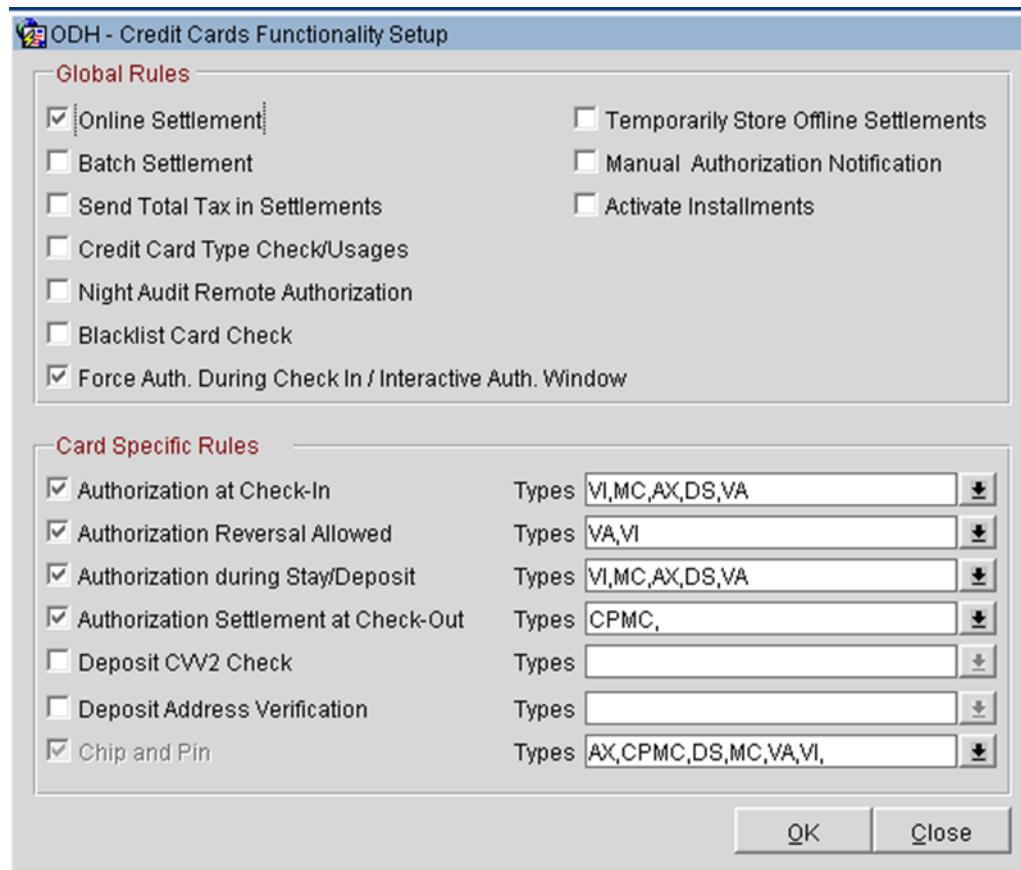
Configuring CHIP AND PIN (EMV)

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.**

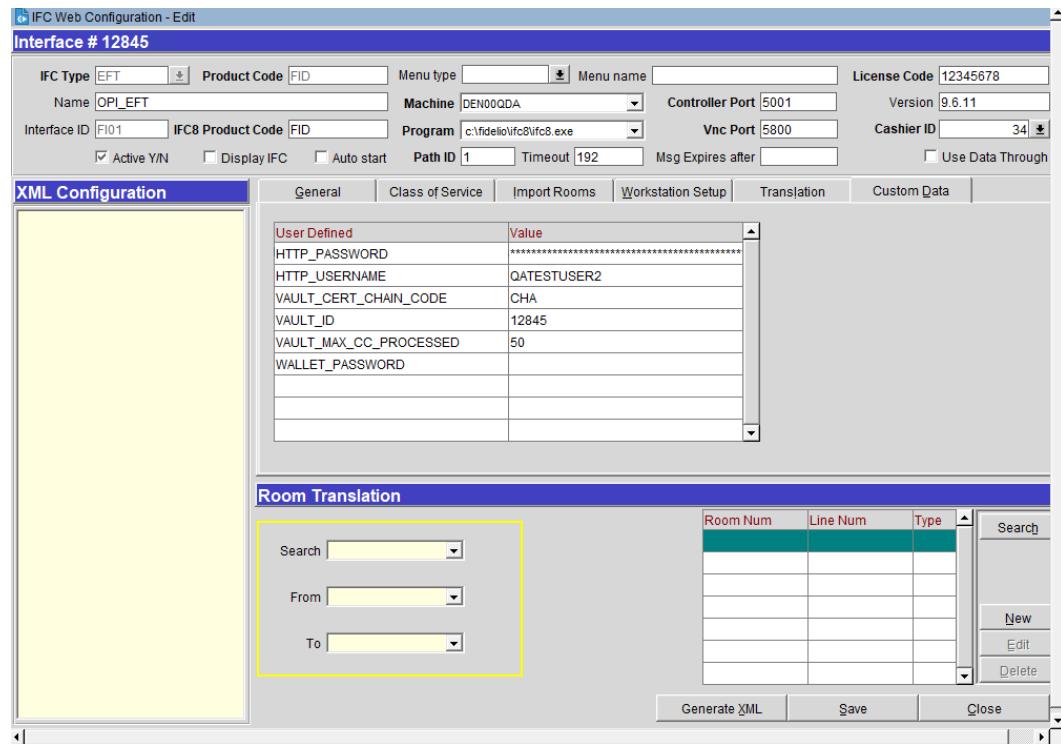


- **Online Settlement:** Select this check box to allow online settlement. OPI is an online settlement. This must be checked to activate the Chip and PIN Application Setting.
- **Authorization at Check-In:** Select the payment methods that will trigger an automatic credit card authorization at check-in.
- **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**.

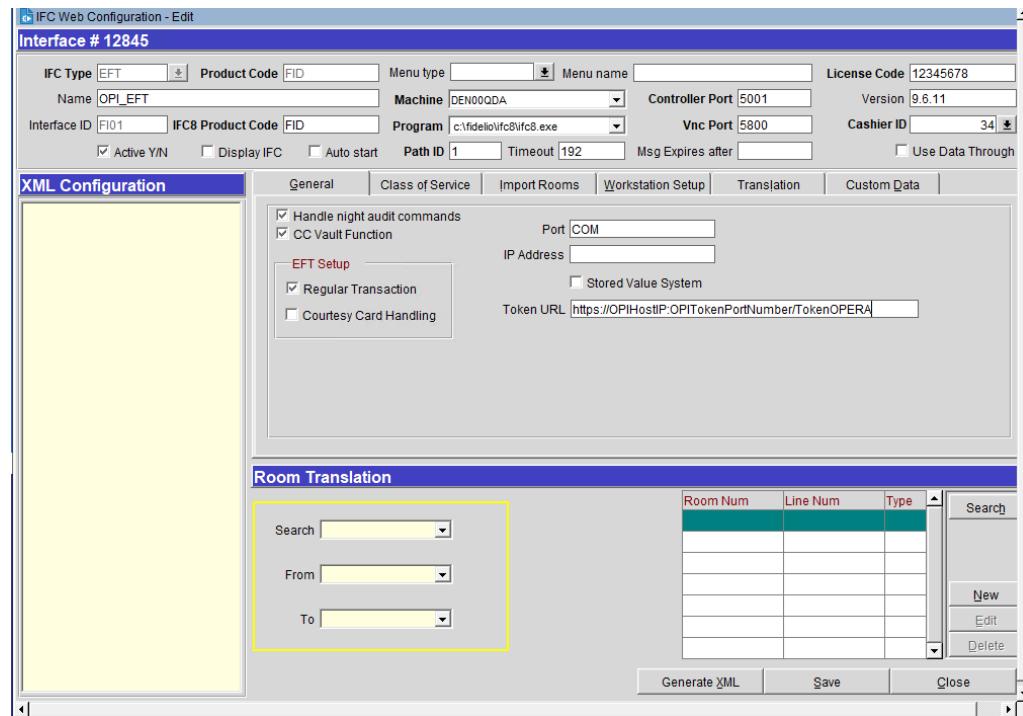
Token URL is accessible from **Configuration | Setup | Property Interfaces | Interface Configuration | edit EFT IFC OPI | General**.



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.

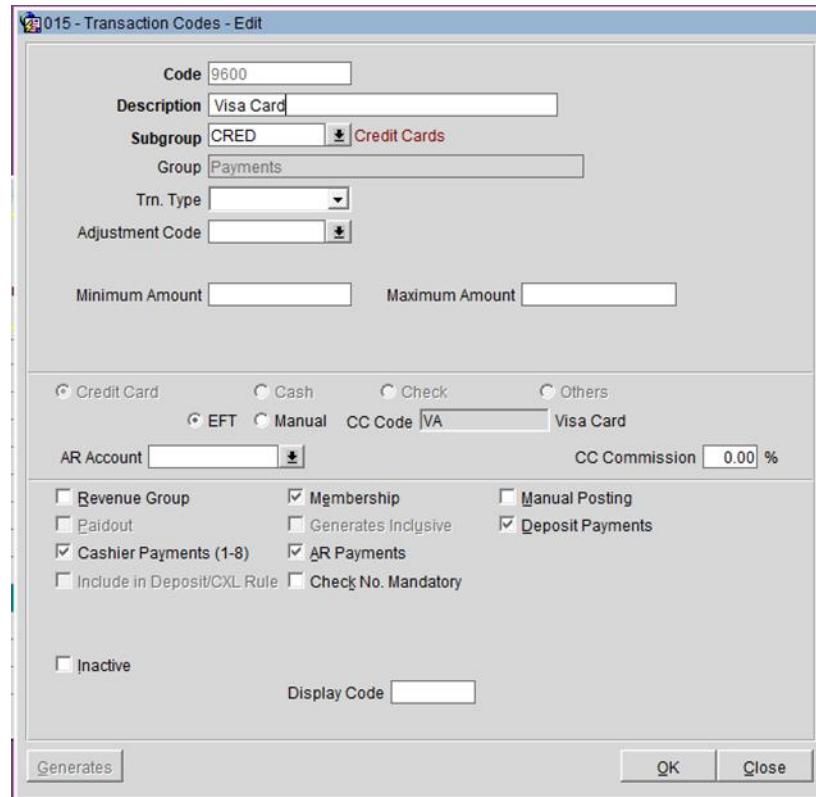
The CREDIT CARD MAX CC PROCESSED is set to what the Payment Partner can support for the number of rows sent in one Token (GetID/GetCC) request. This is used during the bulk tokenization process and when multiple folio windows exist on OPERA Reservations. 50 is the default used when nothing is set here (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 45 is recommended.

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.



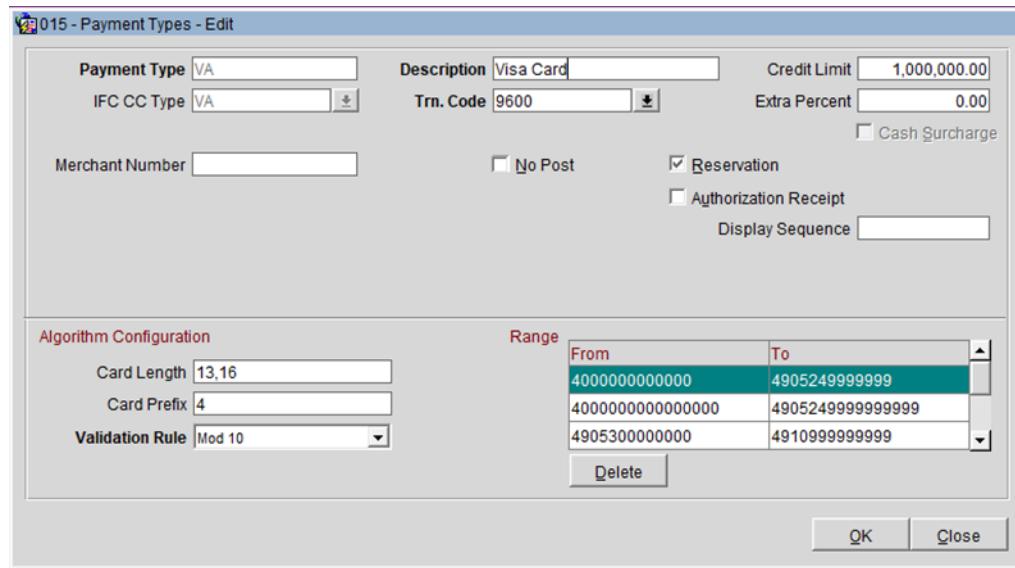
2. Information for credit card payment transaction codes:

- **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.



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.

Payment Types - Customer Present (Chip and PIN)	Description	Capture Method
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!
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)

Payment Types – Customer NOT Present (Keyed)	Description	Capture Method
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

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
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

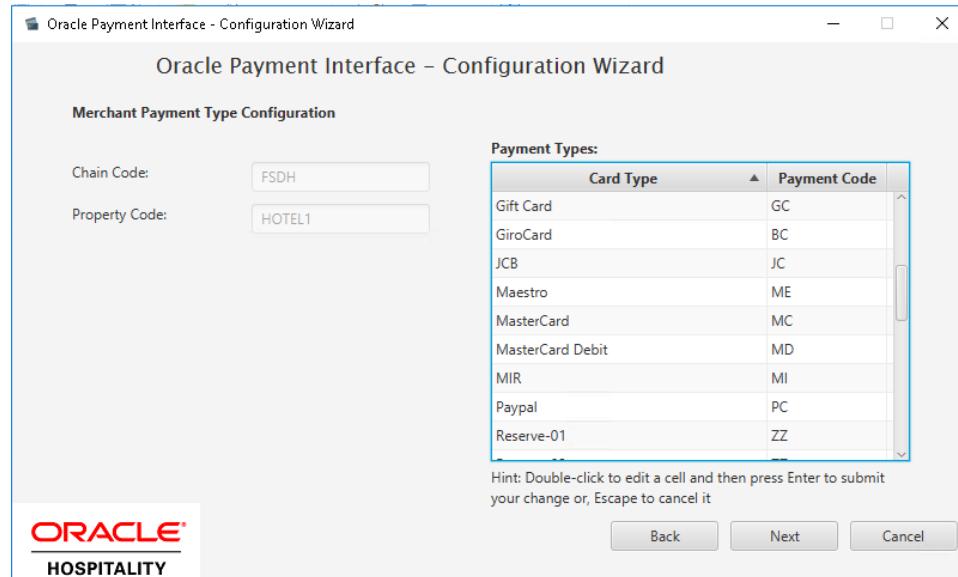
Payment Types – One Shot Cards (Keyed) OPTIONAL!!!	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
VVA	N	Y	N	Y	N
VMC	N	Y	N	Y	N
VAX	N	Y	N	Y	N

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.

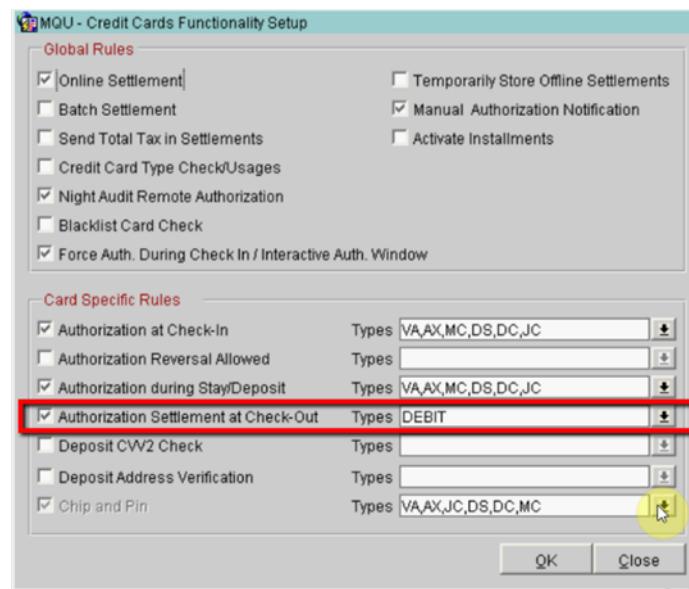
Update OPI Configuration Payment Types

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



Update Functionality settings for Chip and Pin and PayOnly

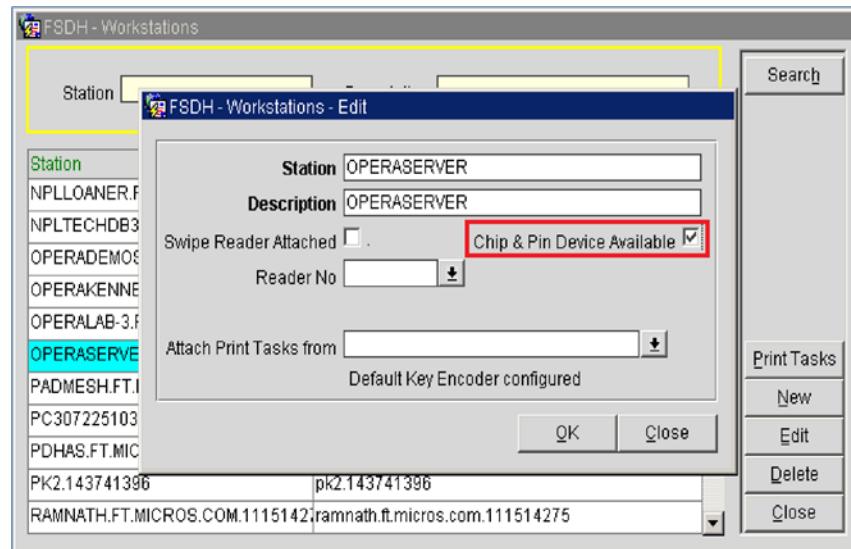
- Selection for Chip and Pin and PayOnly cards.



Configuring the Workstation

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

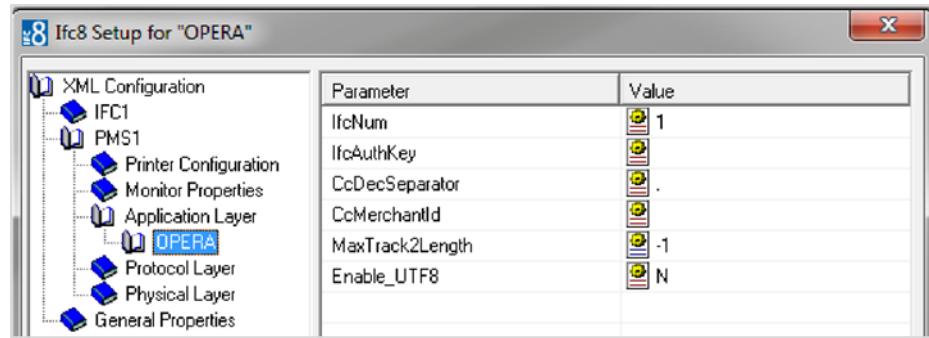
1. In OPERA | **Setup | Workstations** | edit your workstation.
2. Select the **Chip & Pin Device Available** check box to enable the device for this workstation (this allows the generic CP Payment Type to display in the LOV for a reservation).



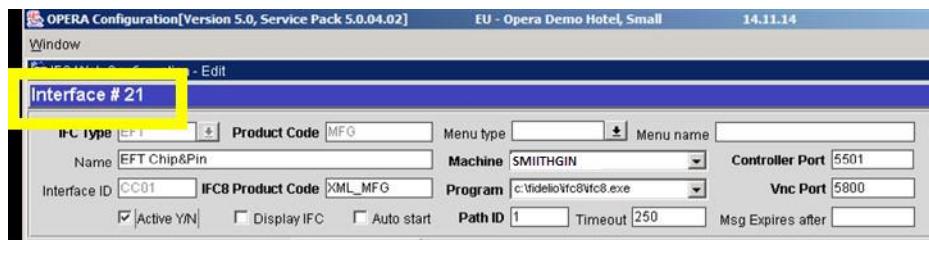
Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC)

To configure the link between the interfaces:

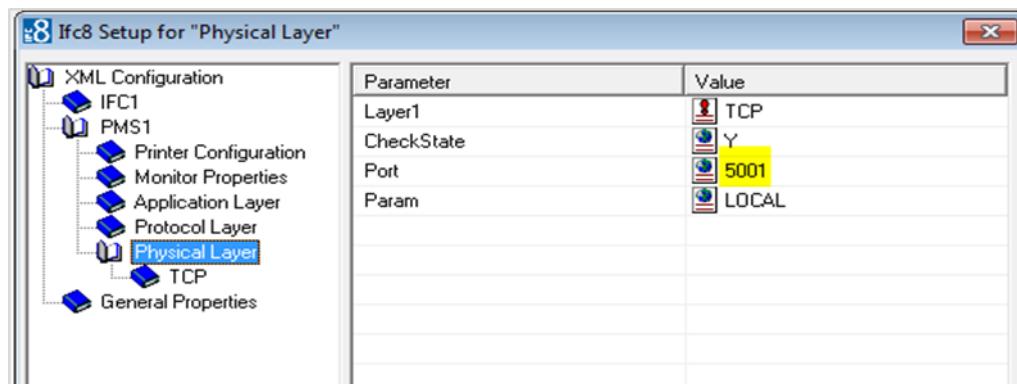
1. In the **Hotel Property Interface**, go to the **PMS1** tree and then select **OPERA** in the application layer.
2. Enter the **OPERA IFC** number in the parameter **IfcNum** value.



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



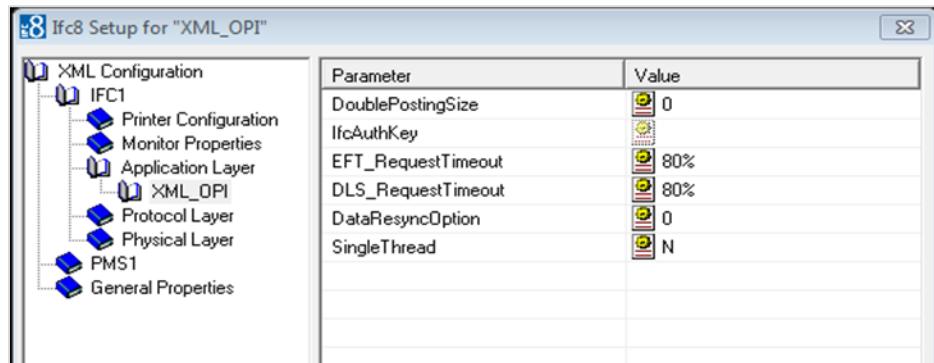
3. Go to the **PMS1** tree in the **Physical Layer**.
4. Enter the port number into Parameter value Port. This is the port IFC8 uses to communicate with the OPERA IFC controller.
5. Select **Enter** and **Apply** to re-initiate IFC8, and click **Save**.



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.

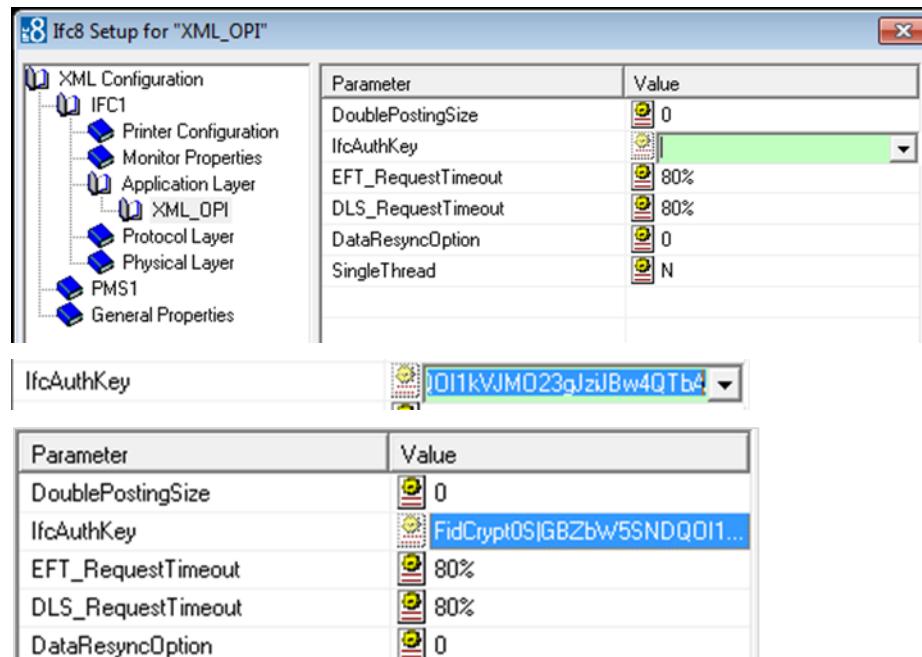
1. In the Hotel Property Interface (IFC8) configuration, go to the **IFC1** tree, and then in the **Application Layer**, select the **XML_OPI** option.



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

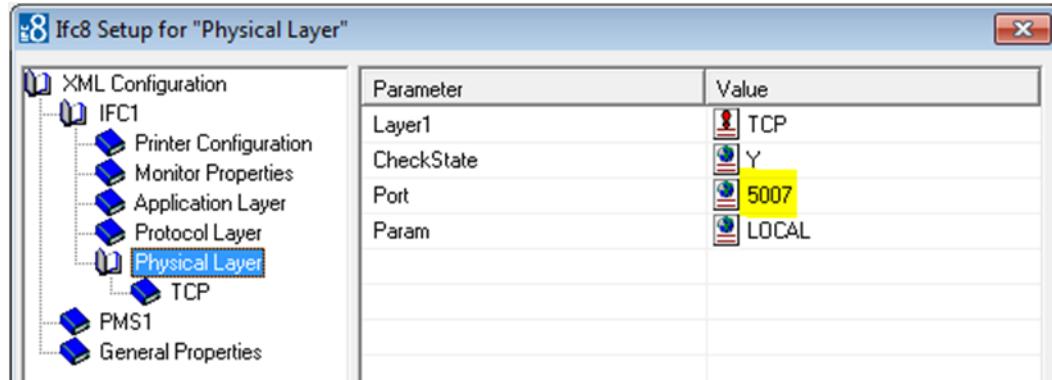
For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxxxx

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



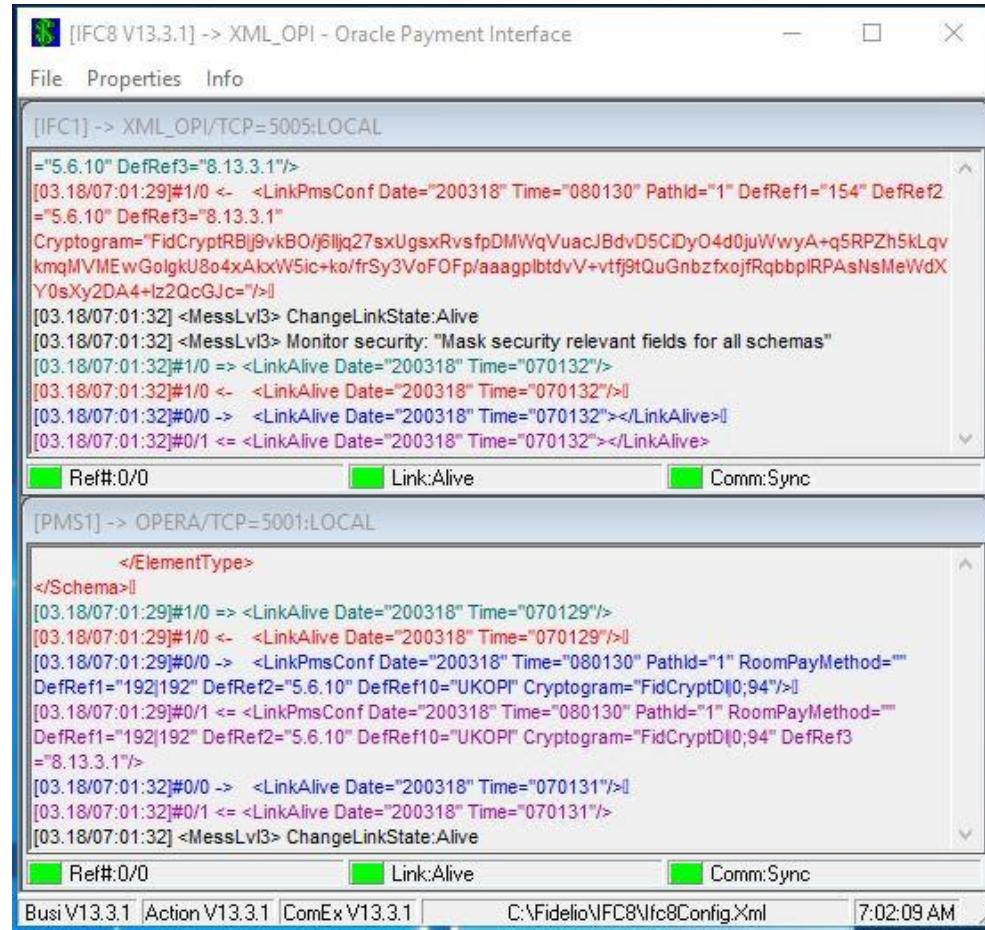
4. Go to **IFC1** tree and select the **Physical Layer**.

5. Enter the port number in port value. This is the same port that was configured in OPI.



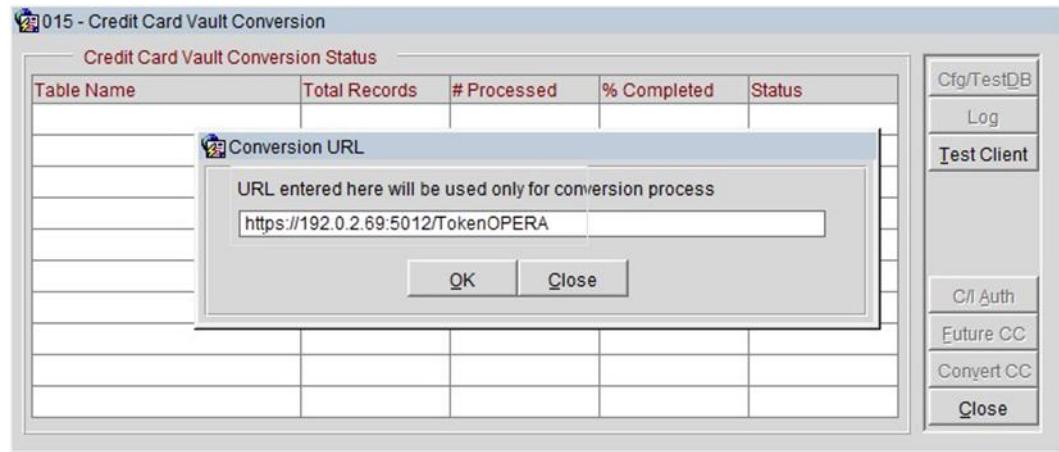
6. Click **Apply**, IFC8 reinitiates.
 7. The **IfcAuthKey** value now shows an encrypted key and the entered string is now encrypted by IFC8.
 8. Click **Save**, and click **OK** to close the IFC8 Configuration form.

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



Perform a Tokenization

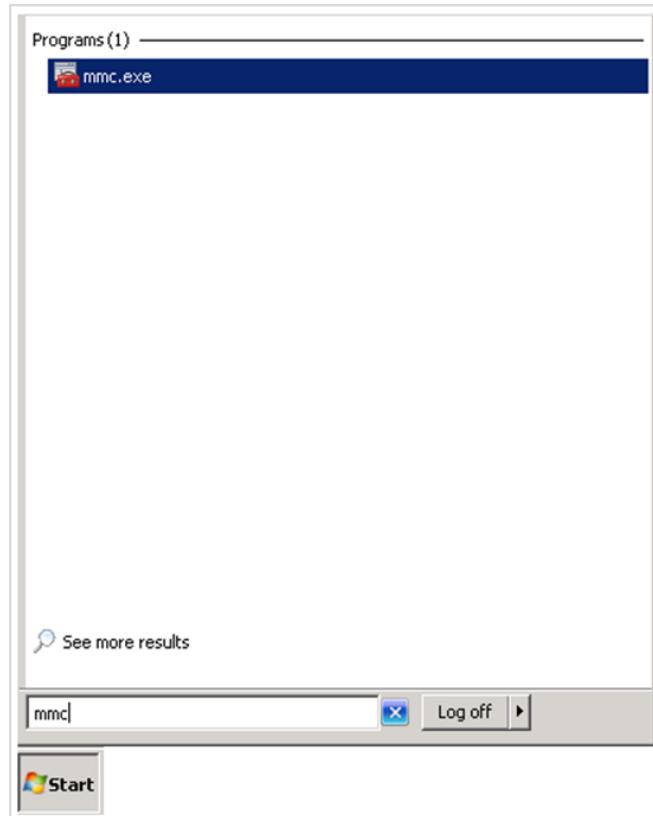
Utilities → Convert CC → Convert Vault CC Information → Test Client



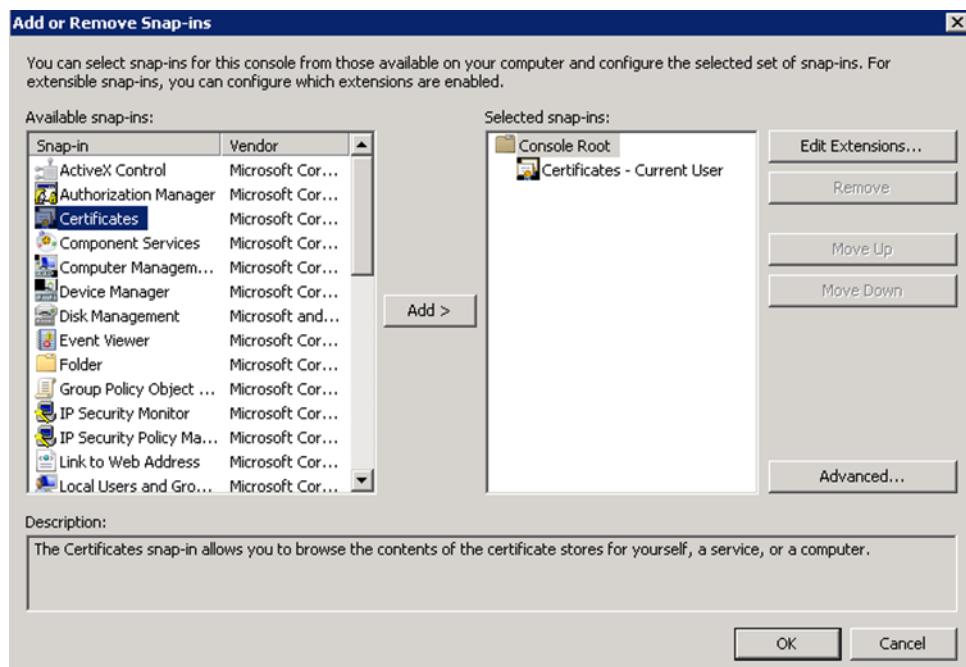
Complete the **Test Client** conversion to enable the **Credit Card Vault Conversion** functions.

Certificate Import using Microsoft Management Console

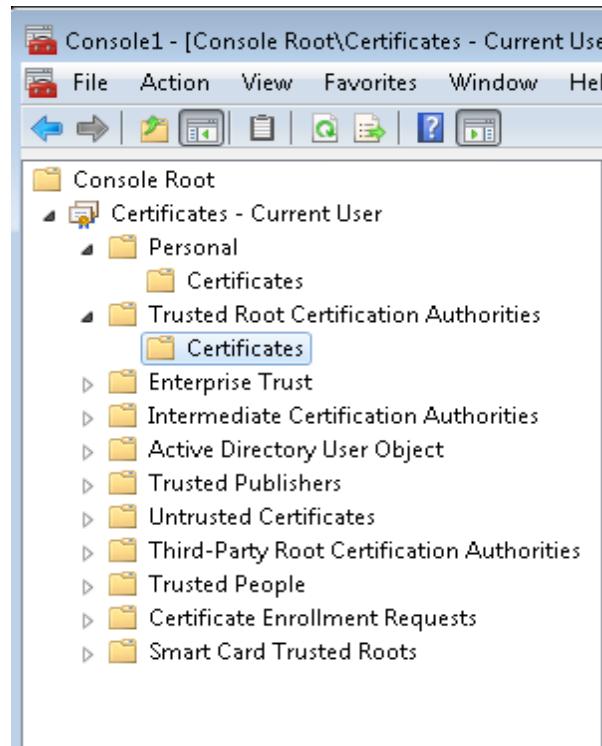
1. Find and open `mmc.exe` from Start menu.



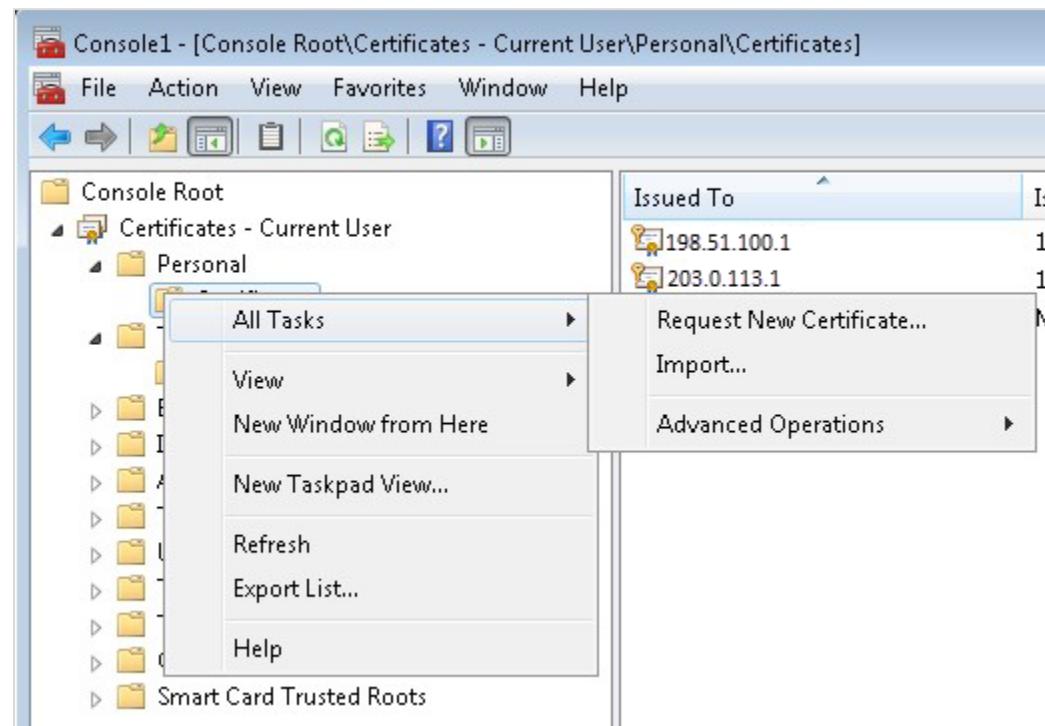
2. Go to **File | Add or Remove Snap-ins**, add certificates to **Selected snap-ins**, and click **OK**.



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



4. 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.

4

Upgrading the OPI

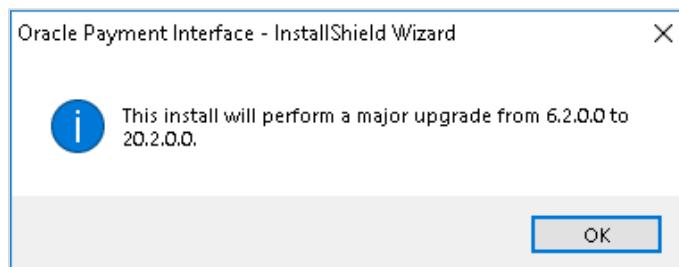
VERY IMPORTANT: Read and follow the upgrade directions.

NOTE:

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

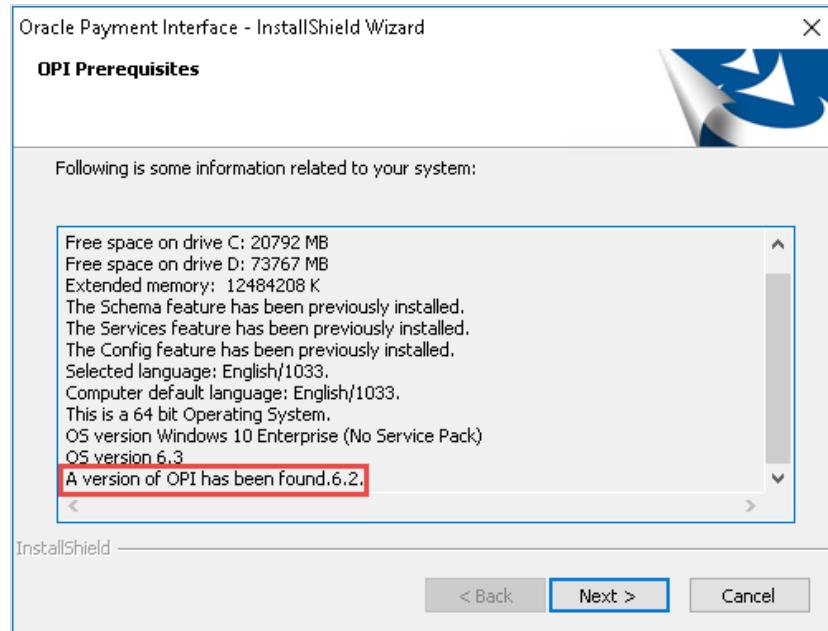
Upgrading OPI 6.2.0.0 to 20.2.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.2.0.0.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.

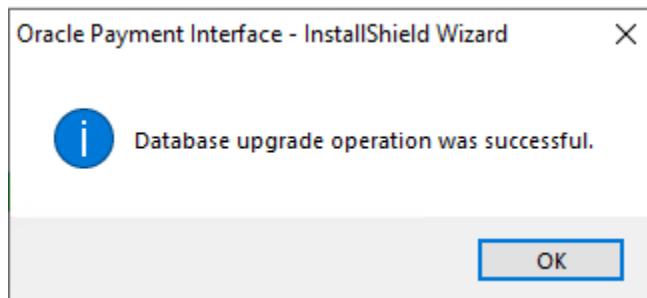


6. Choose a Destination Location. Accept the default installation location or click **Change...** to choose a different location.

7. Click **Next**.

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

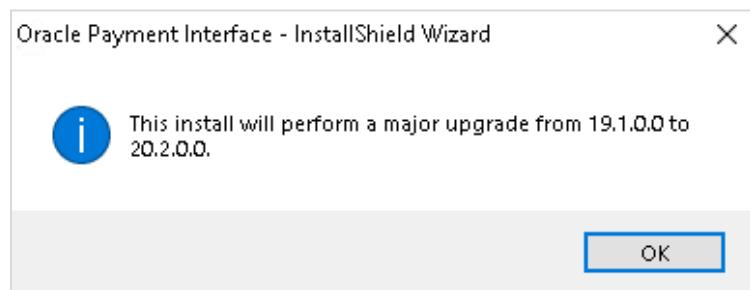
8. Click **Install** to begin the installation.
9. Click **OK**.



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.

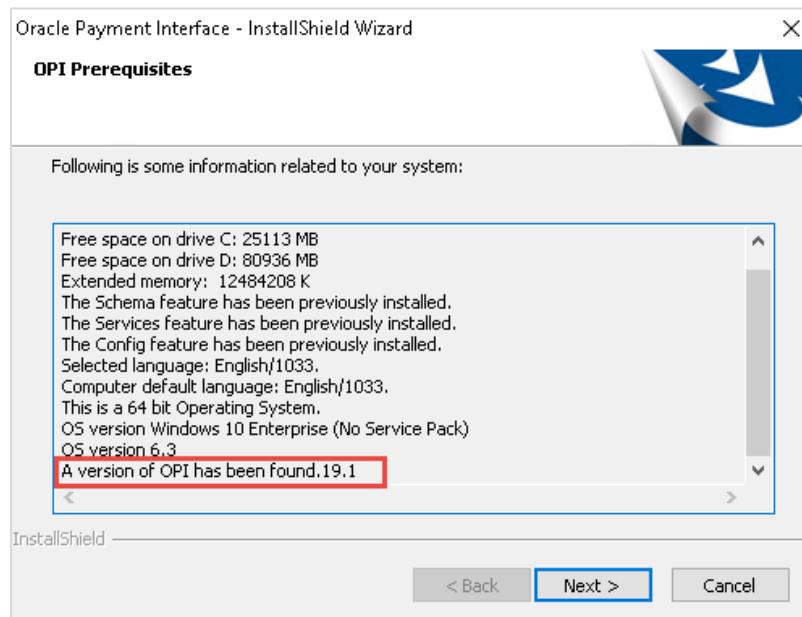
Upgrading OPI 19.1.0.0 to 20.2.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.2.0.0.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**.

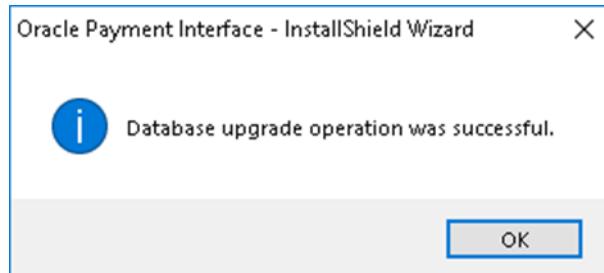
Ensure all the prerequisites for the OPI installation are met.



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.

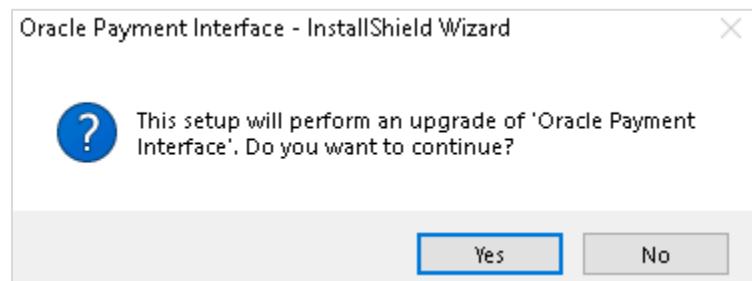
8. Click **Install** to begin the installation.
9. Click **OK**.



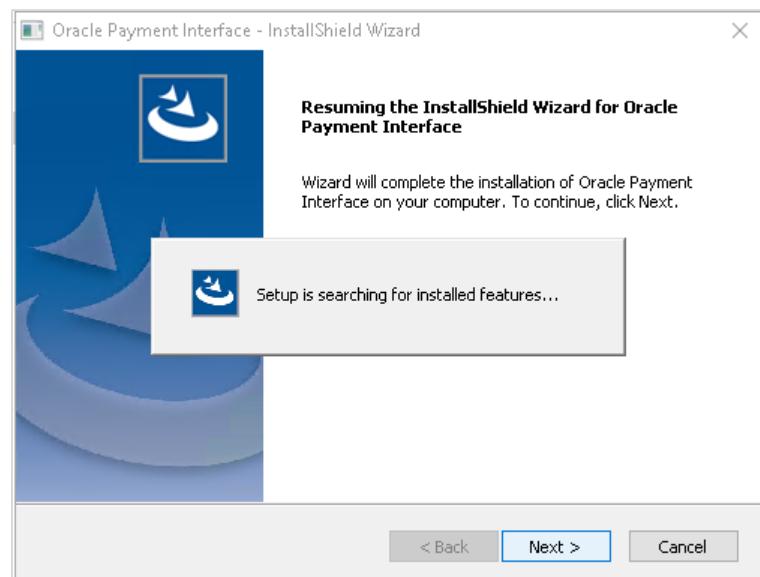
10. Enter the **Host** and **Port** that should be used to connect to the OPI Config Service for the Merchant Configuration.
11. Once the installation is complete, the installer will prompt for a reboot of the host machine.

Upgrading OPI 20.1.0.0 to 20.2.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.2.0.0.exe** file and select **Run as Administrator** to perform an upgrade.

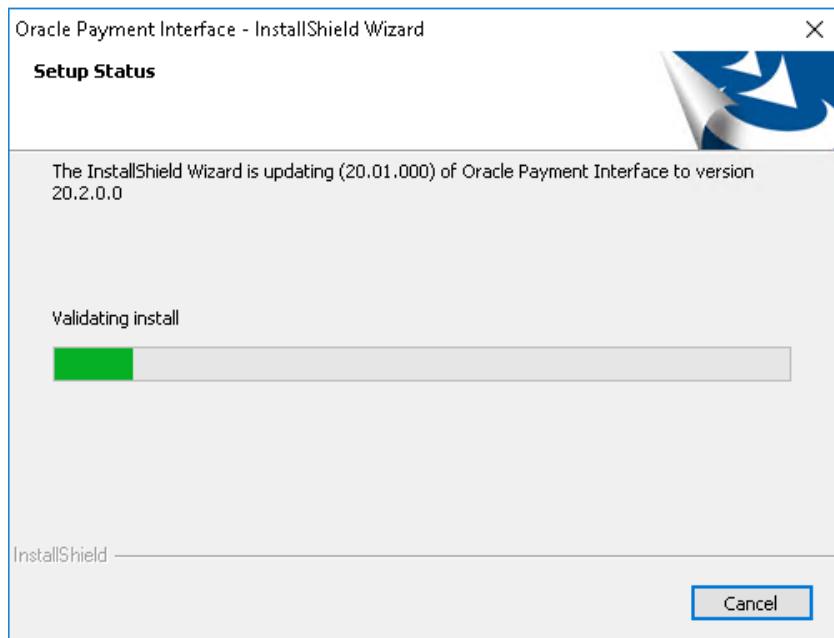


2. Click **Yes**.



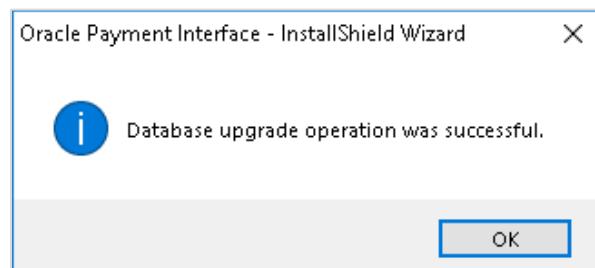
3. Click **Next**.

Setup is searching for installed features.



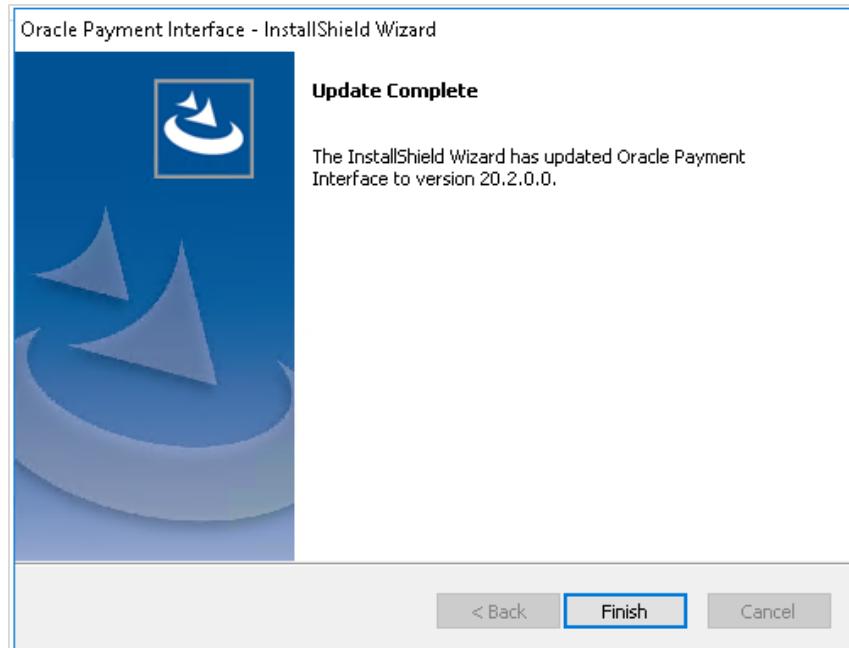
4. Click **Next.**

The Install wizard is updating from **OPI 20.1** to version **20.2**.



5. Click **OK on the OPI database upgrade screen.**

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



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