

Oracle® Hospitality Payment Interface

Suite8 Property Management System Installation Guide



Release 20.2
F32294-01
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	2-9
Certificates	2-11
3 Suite8 Credit Card Configuration	3-1
General Credit Card Interface Setup	3-1
Payment Type Configuration	3-3
Tokenization Setup	3-7
Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC)	3-9
Configuring Encryption for the Hotel Property Interface (IFC8) with OPI	3-10
Perform a Tokenization	3-12
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 install Oracle Payment Interface (OPI) with the Suite8 Property Management System (PMS) and also explains how to configure Suite8 for OPI.

Audience

This document is intended for installers and system administrators of OPI to integrate with Suite8 PMS.

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 1-1 Revision History

Date	Description
July 2020	<ul style="list-style-type: none">• Initial Publication

1

Pre-Installation Steps

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

- Suite8 Property Management System release 8.12.0.0 is the minimum release you can integrate with OPI.
- 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.

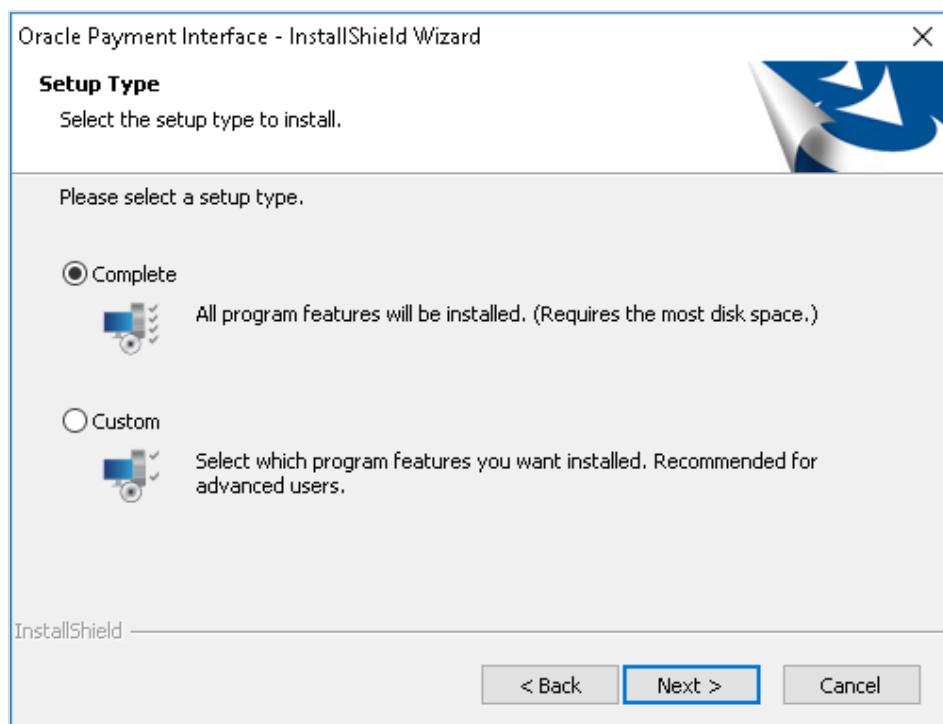
During the installation you must confirm the following:

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

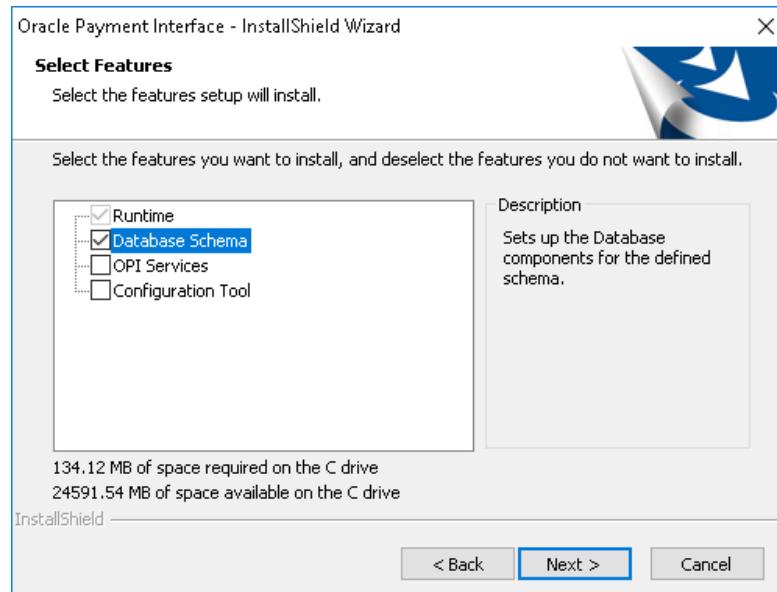
2

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 then click **Next**. If you select Complete Install, it will go to the Step 8 directly.



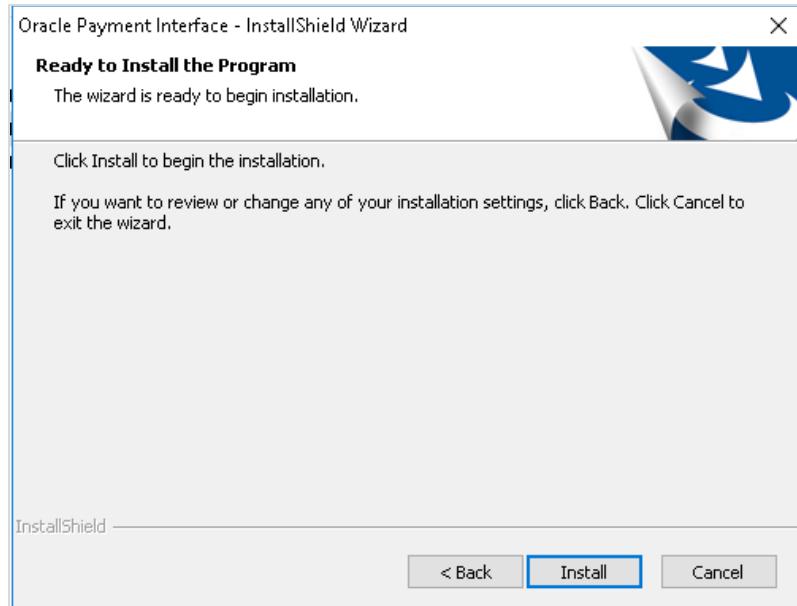
If you selected the Custom install option, the Select Features screen appears with the following options:

- 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. It is just a matter of whether they are all installed on the same computer or on separate computers.

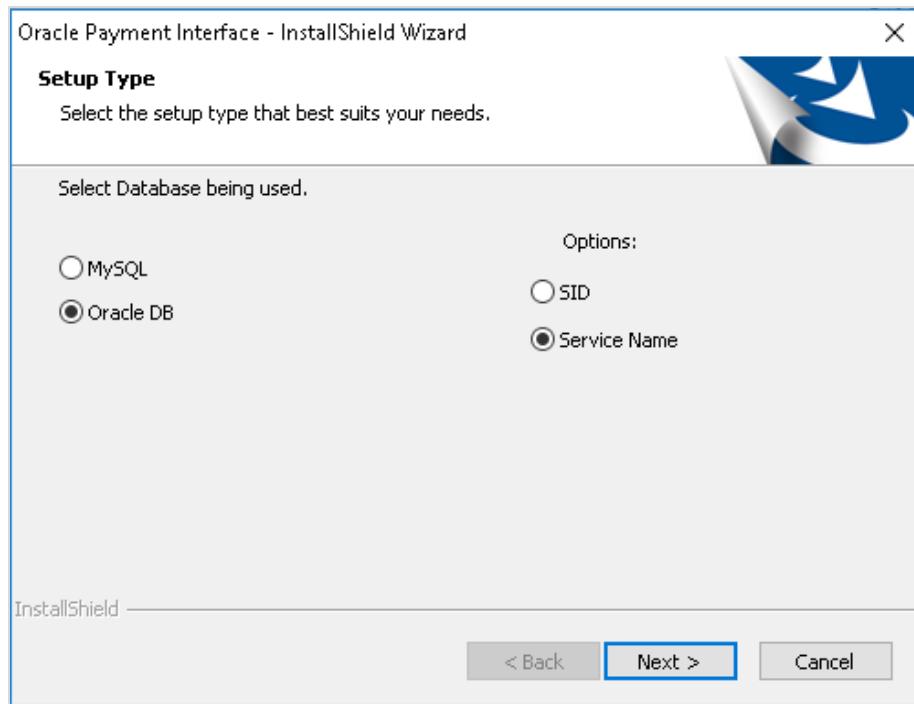
7. Select the features to install on this computer, and then click **Next**.
8. Click **Change** to amend the installation drive or path, if required and click **Next**.
9. Click **Install** to begin the installation.

When the file transfer is finished, Setup prompts you 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**.

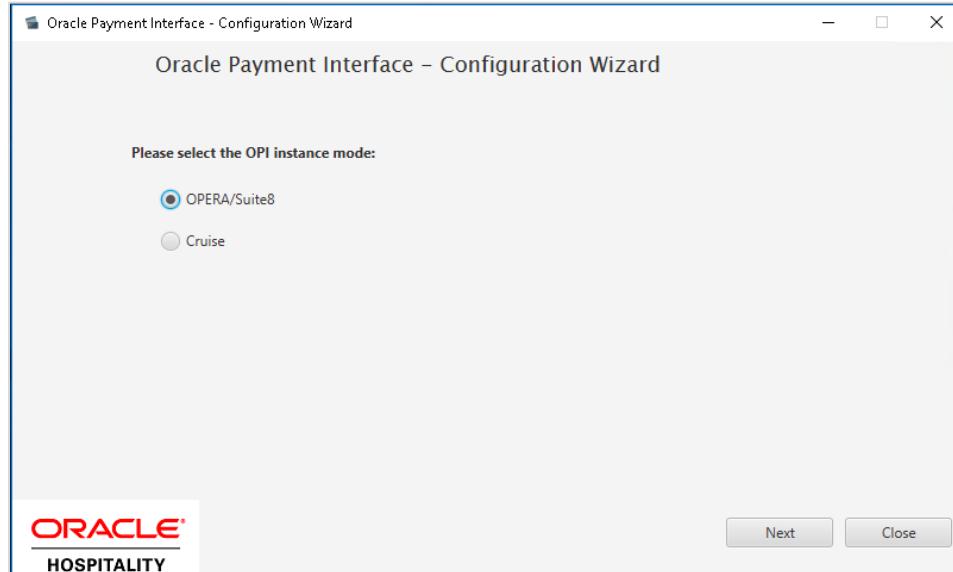
 **NOTE:**

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 PMS merchants as **OPERA/Suite8**.

On the **OPI Interface** screen, the configuration screens displayed are same as when the configuration wizard is launched manually.
(`:\OraclePaymentInterface\v20.2\Config\LaunchWizard.bat`)

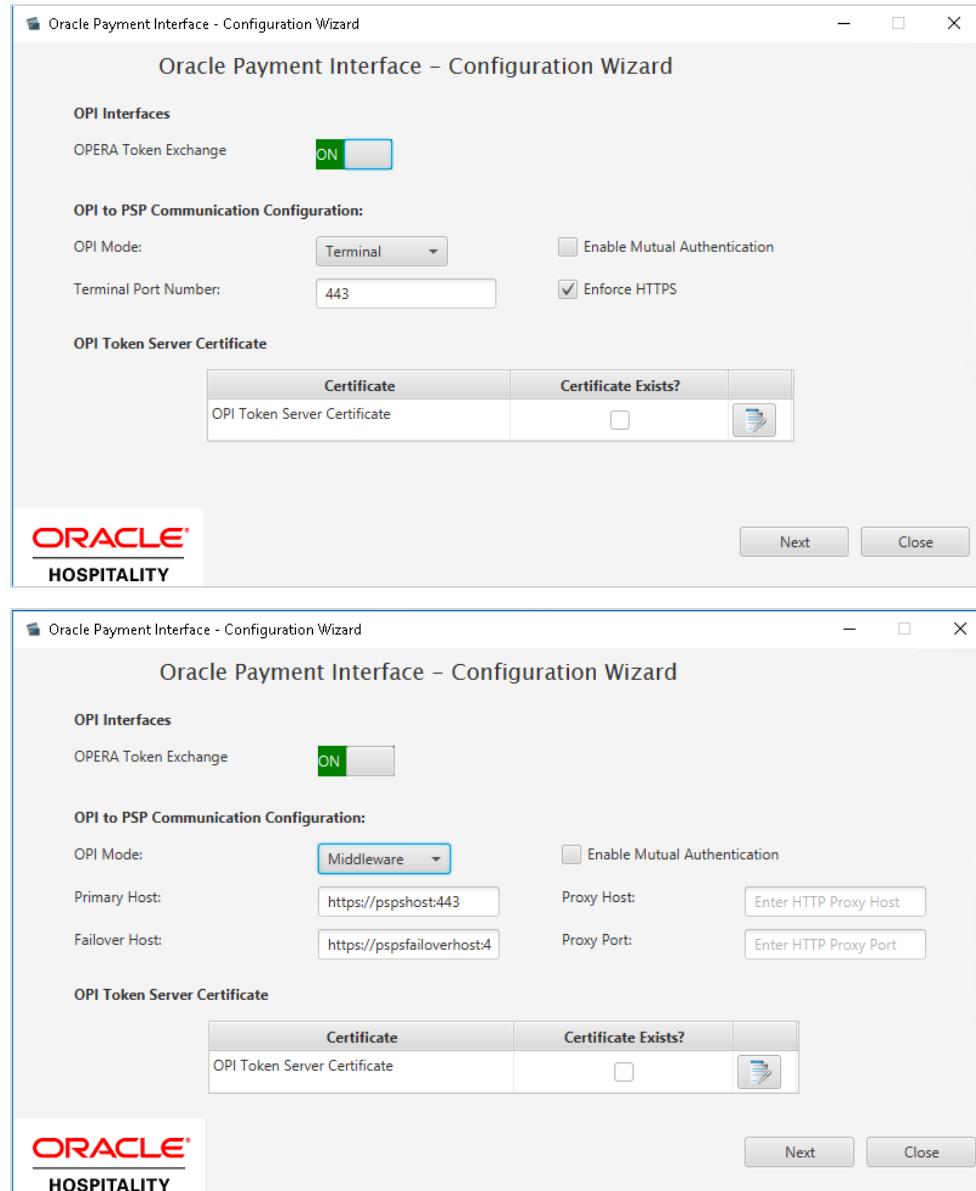
18. OPERA Token Exchange: This option is enabled by default for all OPERA token exchange services.

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.

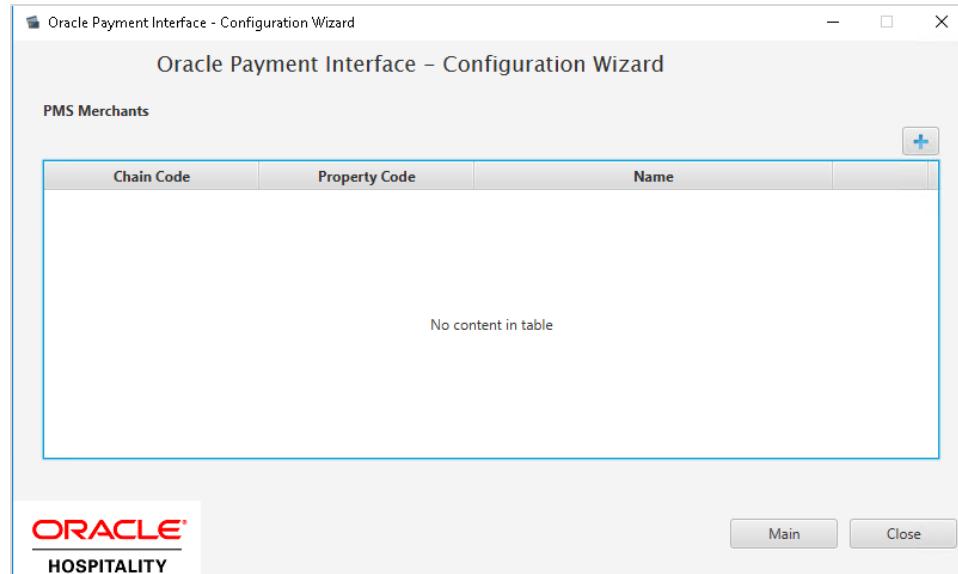
 **NOTE:**

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 Suite8.



20. To configure the Suite8 merchant, enter the following information:

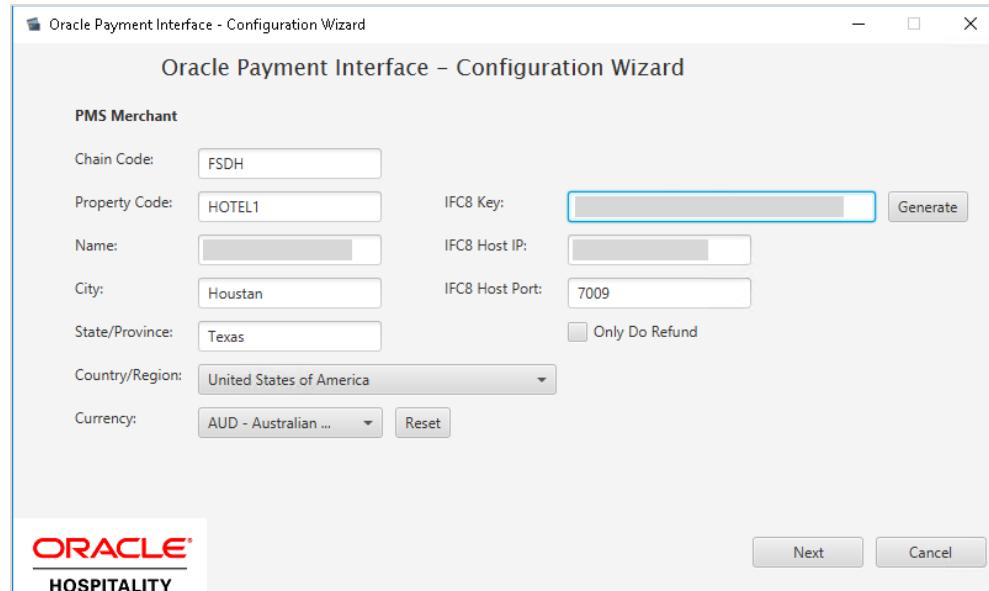
- The **Suite8 Vault Chain Code** and **Property Code**; will form the **SitId** value in the Token request messages.

 **NOTE:**

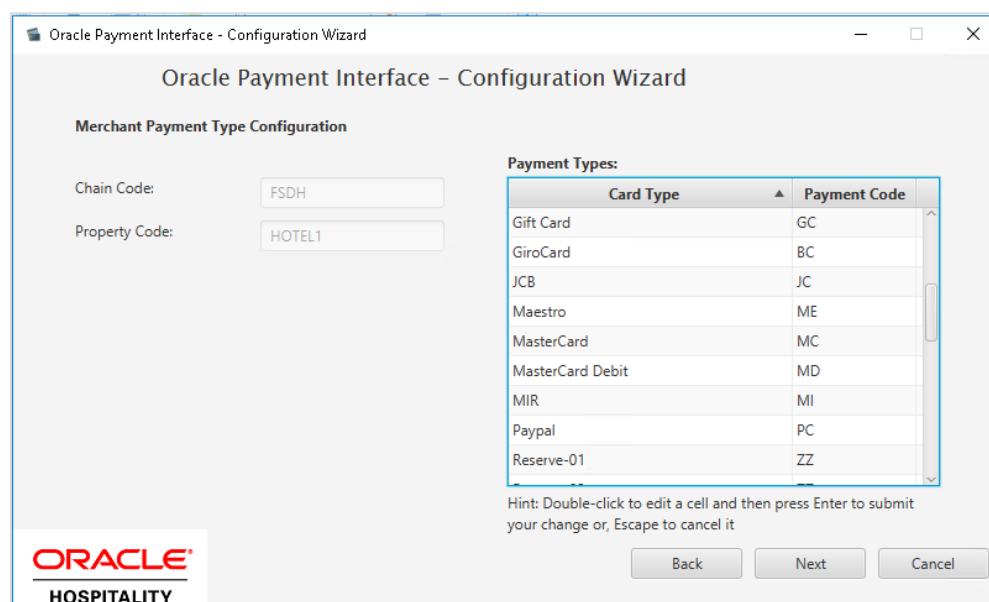
Chain Code and **Property Code** values need to be in upper case.

- 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**.

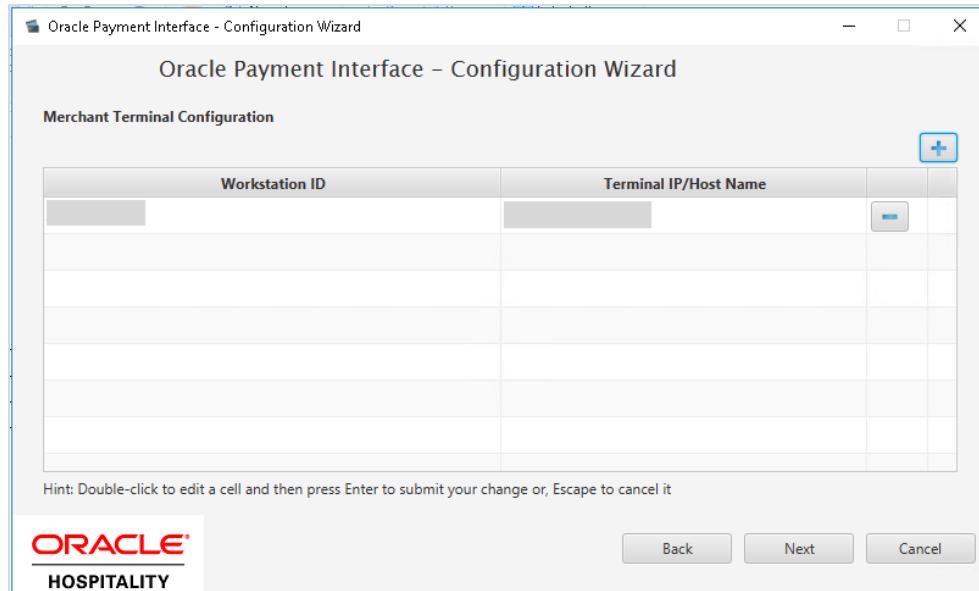
Although the other populated settings are not directly related to the Token Exchange Service configuration, Token Exchange is not possible if the IFC8 interface is not running, as OPI cannot progress past the IFC8 startup if the IFC8 connection is not possible.



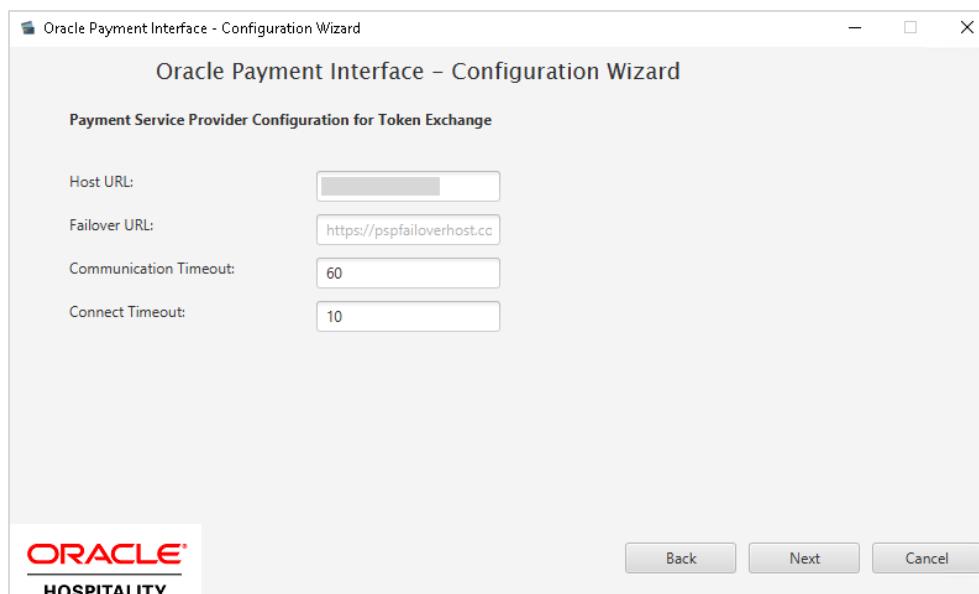
21. Enter the Suite8 payment code for each card type, and click **Next**.



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 then 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 with the 'Merchants' tab selected. The 'Token Exchange Settings' subtab is active. It contains fields for 'Authentication User', 'Authentication Password', and 'Confirm Password'. Below these is a 'Certificates' section with a table for 'OPERA Token Certificate' and a 'Certificate exists?' checkbox.

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

The details provided here must match the details entered in the OPERA Interface Custom Data page (**Suite8 PMS Configuration | Global Settings | Interfaces | 2Interface (IFC8) | Credit Card Interface | enable Tokenization ff.**)

The screenshot shows the Suite8 PMS Configuration | Global Settings | Interfaces | 2Interface (IFC8) | Credit Card Interface configuration page. It includes sections for 'Room Key Interface' and 'Credit Card Interface'. The 'Room Key Interface' section contains checkboxes for various key-related functions. The 'Credit Card Interface' section contains checkboxes for batch settlements, chip & pin authorization, dynamic credit card currency, and other payment-related options. It also includes fields for 'Token Server URL', 'User Name', 'Password', 'Chain Code', and 'Property code'.

- 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](#))
- Suite8 > OPI - ([OPI - Server Side Certificates](#))
- Suite8 > OPI - ([OPI - Client Side Certificates](#))

Refer to the sections below for further details.

PSP - Client Side Certificates

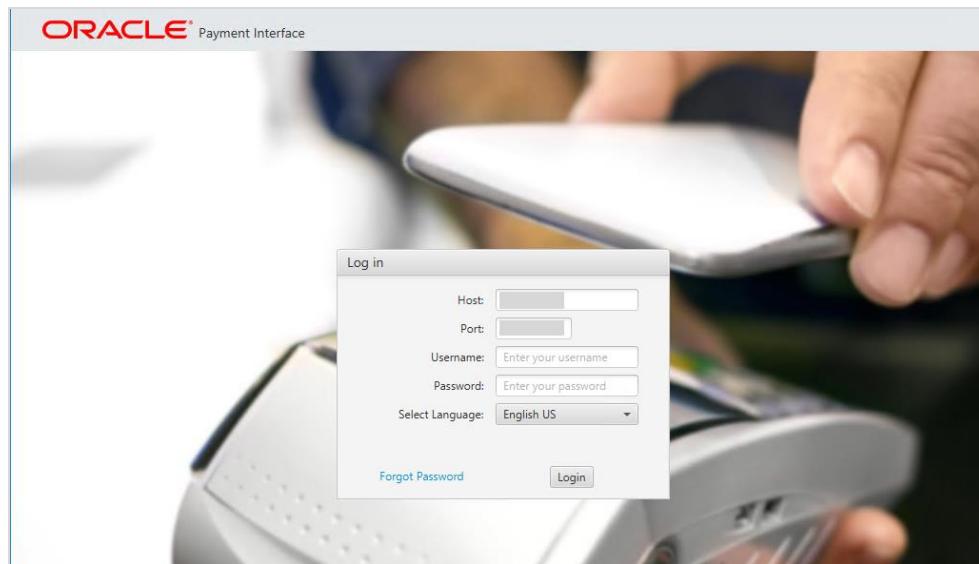
The communication from OPI to the PSP for the token exchange uses HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed on PSP (server side) for HTTPS communication, the PSP is also expected to provide a client side certificate 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:

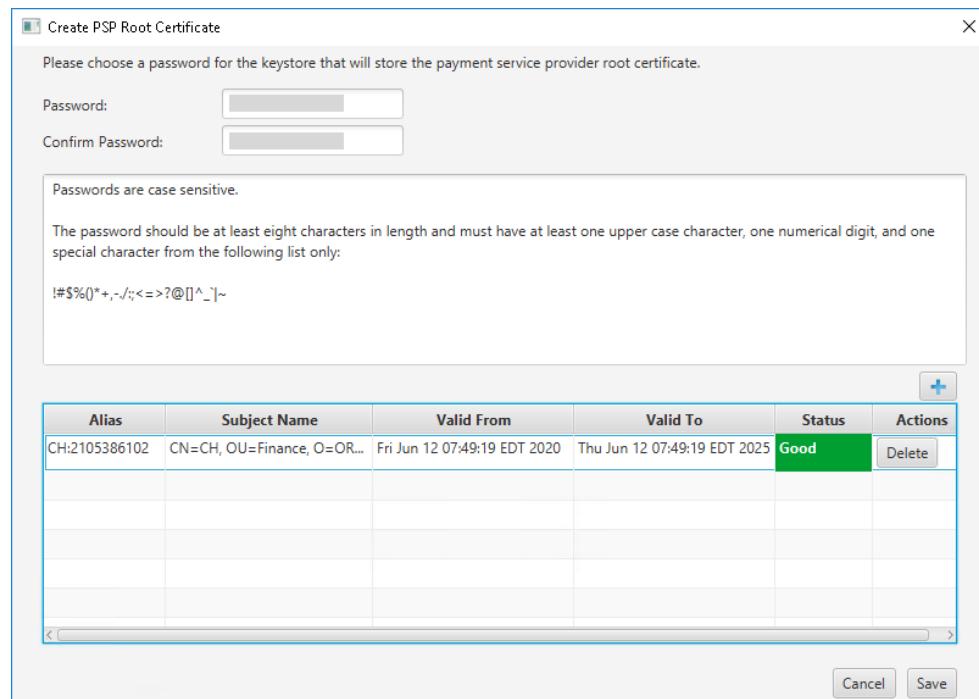
1. Run **\OraclePaymentInterface\v20.2\Config\LaunchConfiguration.bat**
2. Login with the Super user account created during OPI installation.



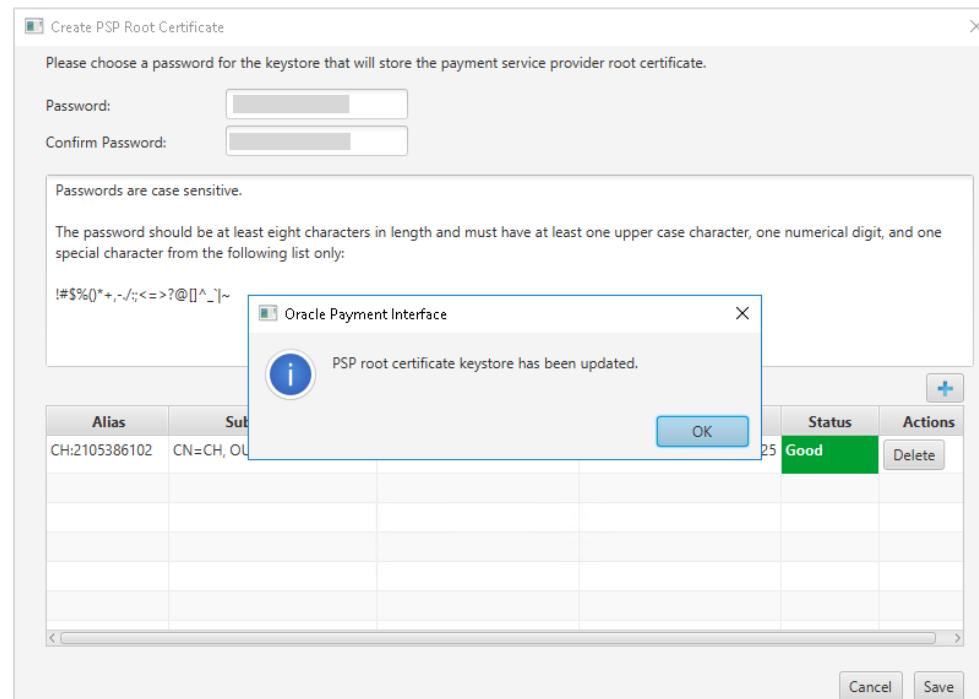
Handling the Root Certificate File by OPI Configuration Tool.

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.



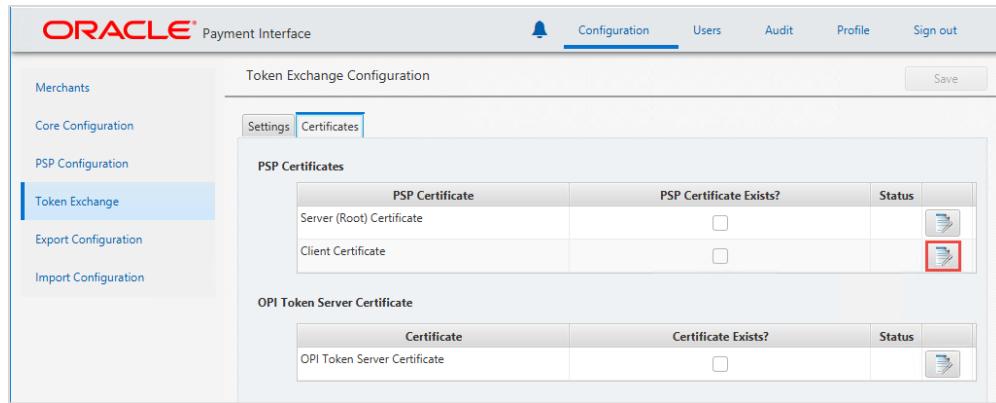
3. Click **Save**.



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**.



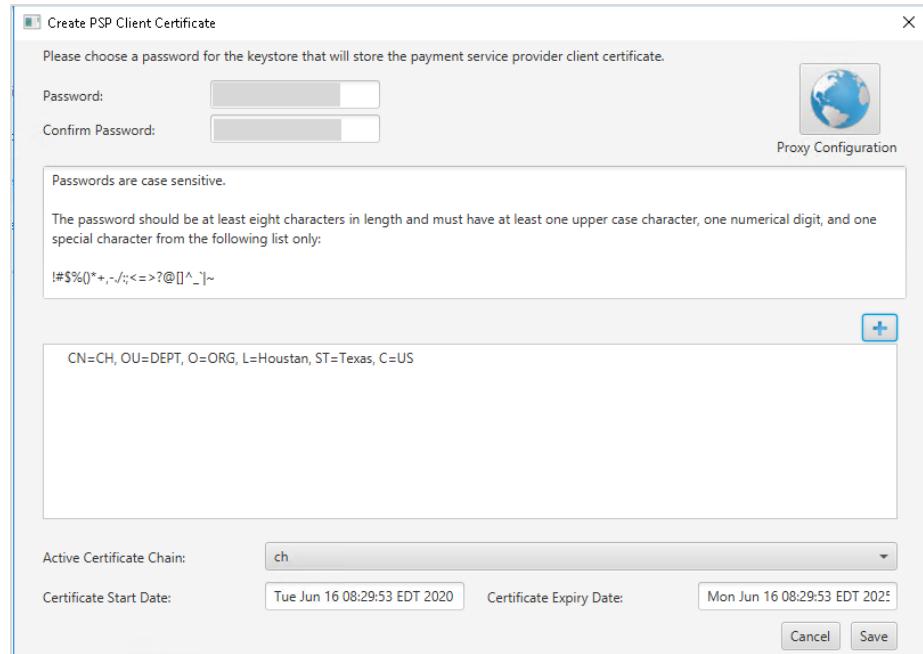
PSP Certificate	PSP Certificate Exists?	Status
Server (Root) Certificate	<input type="checkbox"/>	
Client Certificate	<input type="checkbox"/>	

Certificate	Certificate Exists?	Status
OPI Token Server Certificate	<input type="checkbox"/>	

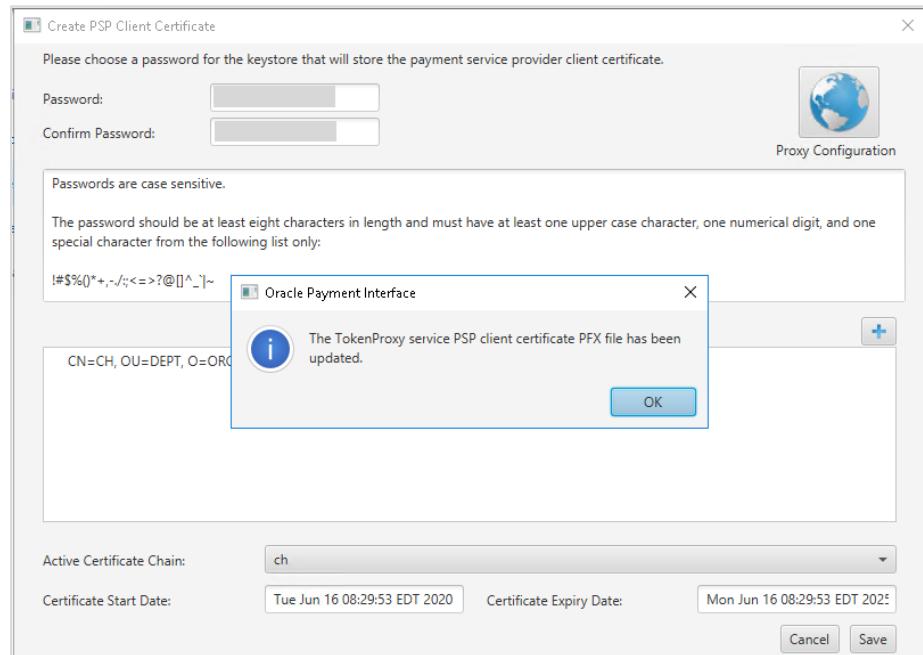
2. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** (+) icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below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

 **NOTE:**

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



3. Click Save.

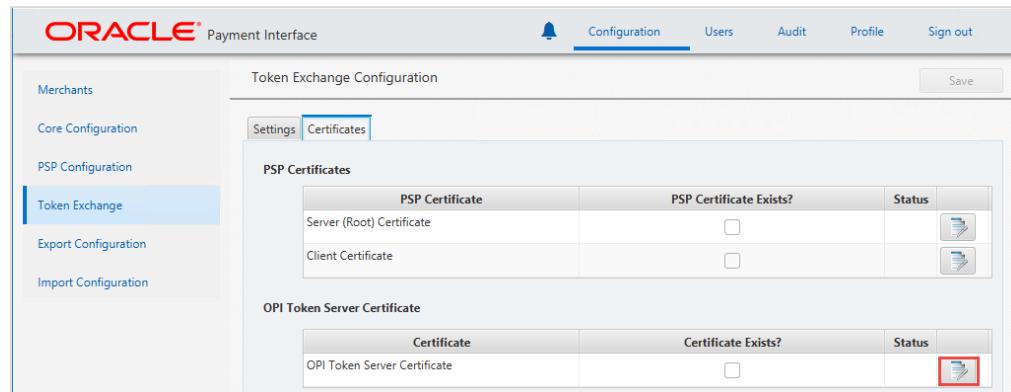


OPI_PSP_1.pfx is created under **\OraclePaymentInterface\20.2\Services\OPI\key** folder.

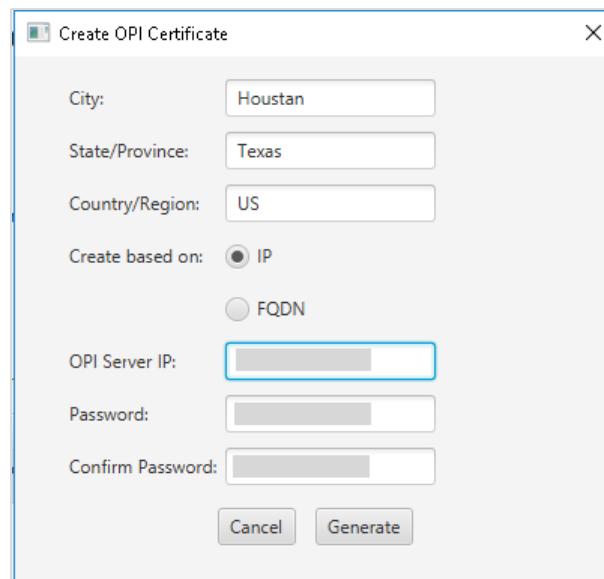
OPI - Server Side Certificates

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.

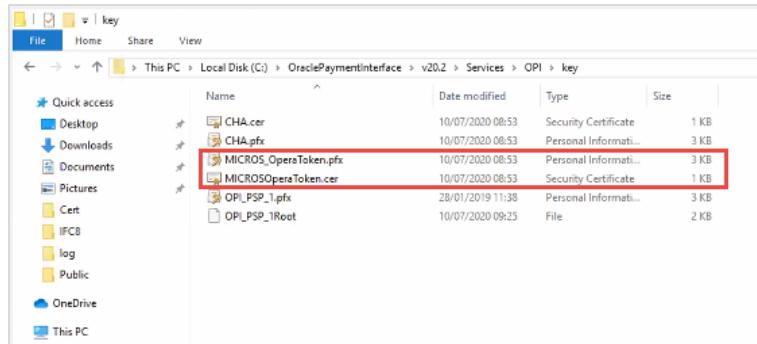


2. Enter **City, State/Province, Country/Region, Create based on IP or FQDN, OPI Server IP, Password and Confirm Password**.



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:**

- OPI does not differentiate from OPERA PMS or Suite8 PMS. Therefore the name of the certificate will always be MICROSOptToken.xxx
- 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.

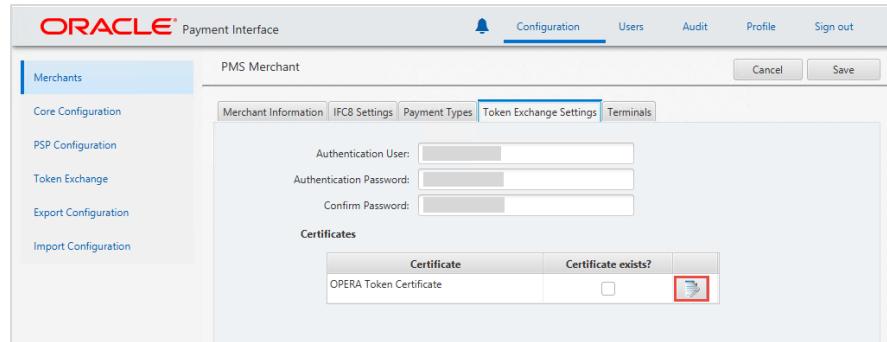
Copy the **MICROSOptToken.cer** file to all the OPERA registered terminals that you want to run the Token Exchange process from and then Import to Trusted Root Certification Authorities, using **mmc.exe** (Refer to section [Certificate Import using Microsoft Management Console](#) for more details)

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

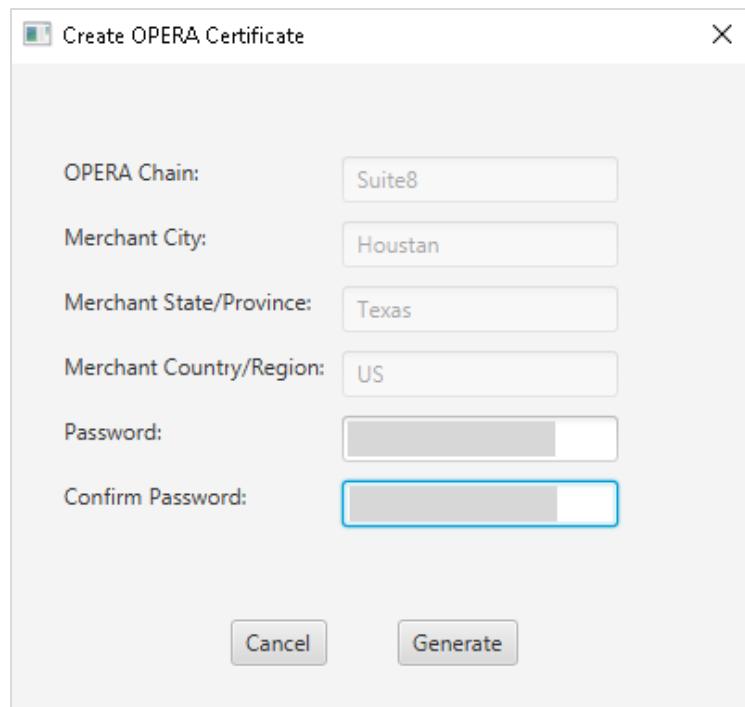
OPI - Client Side Certificates

For communication from OPERA to OPI, the OPI Client Certificates at the Suite8 side are also required.

1. Select **MERCHANTS** tab, click **Token Exchange Settings** subtab and then click the **Create OPERA Token Certificate** to proceed. There is no specific name for Suite8, so the names in the forms always refer to OPERA.

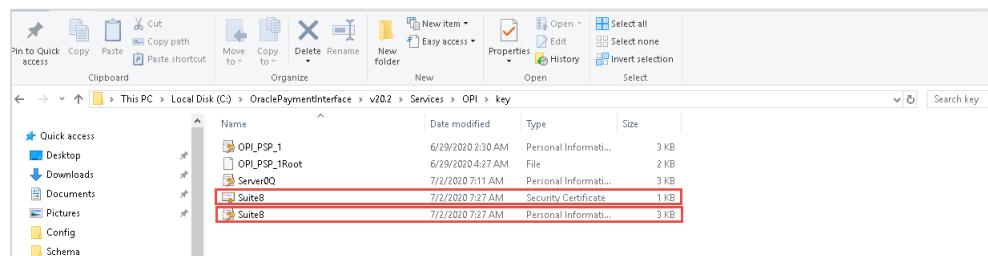


2. **OPERA Chain, Merchant City, Merchant State/Province and Merchant Country/Region** fields are automatically populated based on the Merchant Information.
3. Enter the **Password** and confirm it.



4. Click **Generate** to continue.

This process will generate the **Suite8.pfx** and **Suite8.cer** files in the following folder:
\OraclePaymentInterface\v20.2\Services\OPI\key



In the above example, the certificates are named Suite8, which is picked up from the Chain Code entered in previous steps. The certificates you create may be named differently specific to the environment in which they are being installed.

Copy the created **Suite8.pfx** and **Suite8.crt** files to all the Suite8 terminals that you want to run the Token Exchange transactions from. Import the certificates using mmc.exe (Refer to section [Certificate Import using Microsoft Management Console](#) for more details)

- **Suite8.pfx** import to Personal – you will need the password used during the creation in the previous steps.
- **Suite8.crt** import to Trusted Root Certification Authorities.

 **NOTE:**

- The OPI Client Side Certificates have a default expiry date of five years from the date of creation. Check the expiry date in the properties of the certificate files.
- The OPI Client Side Certificates must be updated prior to the expiration date to avoid downtime to the interface.

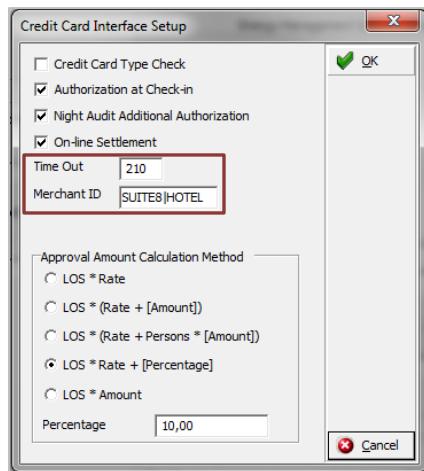
5. You must restart the OPI service for the update to take effect.

3

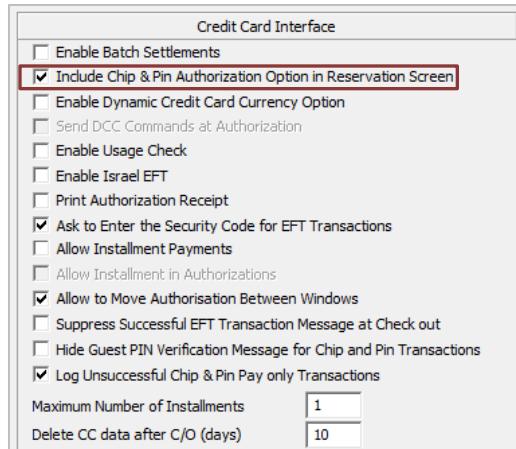
Suite8 Credit Card Configuration

General Credit Card Interface Setup

1. Log in to **Suite8** and go to **Configuration**.
2. Select the menu option **Global Settings| Interface | 1Interfaces (IFC8) | Credit Card Interface**.
3. Ensure the **Merchant ID** and **EFT Timeout** are correctly set in Suite8 PMS Configuration.



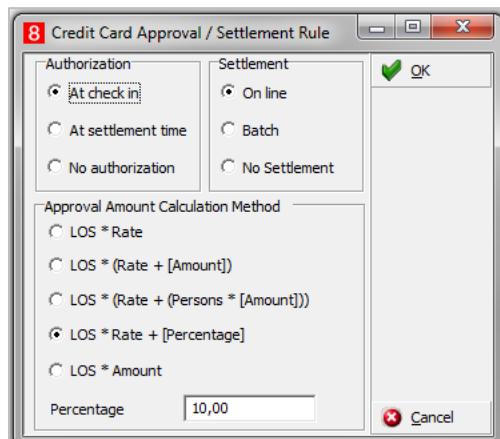
4. **Timeout:** Must be greater than 168 seconds as IFC8 will use 80% of this PMS timeout and send the value to OPI. OPI requires a minimum of 150 seconds, else it will stop connection with IFC8.
5. **MerchantID:** Must be set in format [Chain Code] | [Property Code] as Suite8 has not pre-set Chain Code or Property Code the user needs to define its own value.
6. Go to **Global Settings | Interface| 2Interfaces (IFC8) | Credit Card Interface** and ensure that the Credit Card Interface **Chip&Pin functionality** is enabled.



Card Type Functionality Setup

Define Credit card type functionality to handle authorization requests and settlement requests as per card type. EFT functionality with OPI requires following settings for all common **Credit Card types** (MasterCard, Visa, Amex, Diners/those card types who support amount authorization).

- Set **Authorization = At check in** in order to automatically send out an authorization request of a defined amount to OPI at check in of a reservation.
- Set **Settlement = On line** to enable functionality to send Payment request at the time of checkout/at the time when a payment shall be performed.



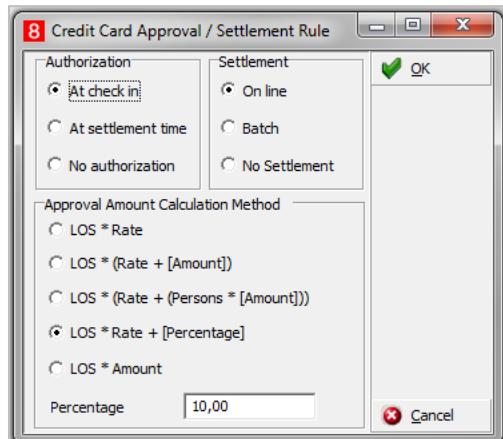
EFT functionality with OPI requires following settings for all common **Debit Card types** (Maestro, V-Pay, Local bank cards/those card types who do not support amount authorization).

- Set **Authorization = No Authorization**. No authorization amount will be possible for this Card type.
- Set **Settlement = On Line** to enable functionality to send Payment request at the time of checkout/at the time when a payment shall be performed. Authorization of the payment amount will be done at same process than the payment itself.



Authorization Amount Calculation Method

Common setup is one authorization rule with amount calculation per length of stay (LOS) and/or multiplied with Rate per Night.



Authorization Amount calculation methods can vary based on the Card type. Choose one of the define calculation methods in the Payment Type Configuration.

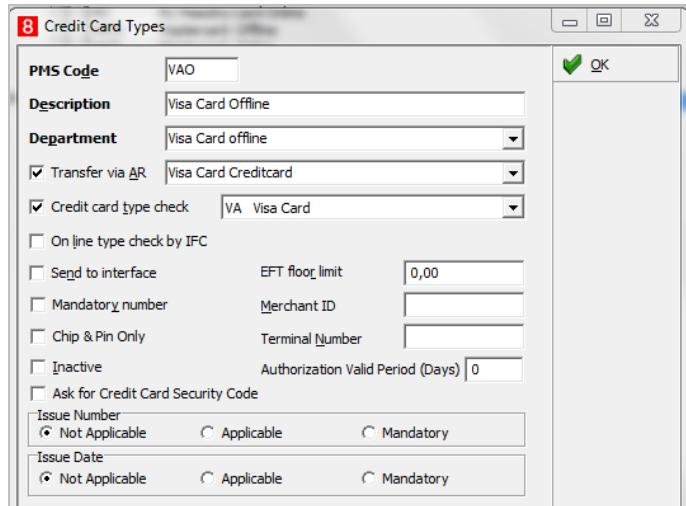
Payment Type Configuration

Offline Credit Card Type

This is used for credit card numbers which will not be sent to an EFT system through EFT Interface. This is usually used in case EFT Interface is not operating or it is not intended to send transaction to EFT System.

Suite8 Code = free definable 3 letter code

Send to Interface = unticked – no message sent to IFC.



Online/Present Credit Card Type

This is used for credit cards which are present at front desk. You or the guest is able to enter the credit card into EMV Device at time of authorization payment.

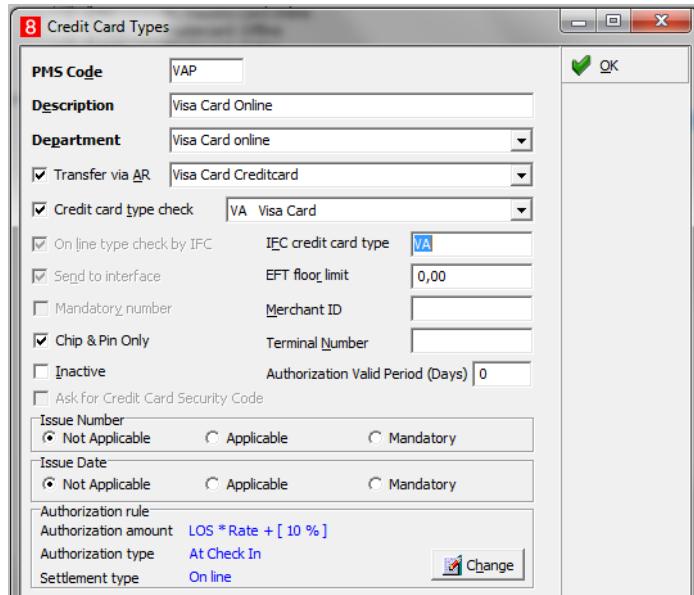
PMS Code = free definable 3-letter code

IFC Credit card type = 2-letter code as setup in OPI (for example, VA for VISA)

Chip & Pin only = active for Chip & Pin transaction

Authorization rule:

- **Authorization type** = At check-in - will use CpAuthor messages to IFC8
- **Settlement type** = Online - will use CpSettl messages to IFC8



Not Present Card Type

This is used for credit cards which are not present (such as card provided by phone, letter, mail, fax, external system) = card is not able to be entered into the pin pad by you or a guest. The card number needs to be entered directly into the related field in Suite8.

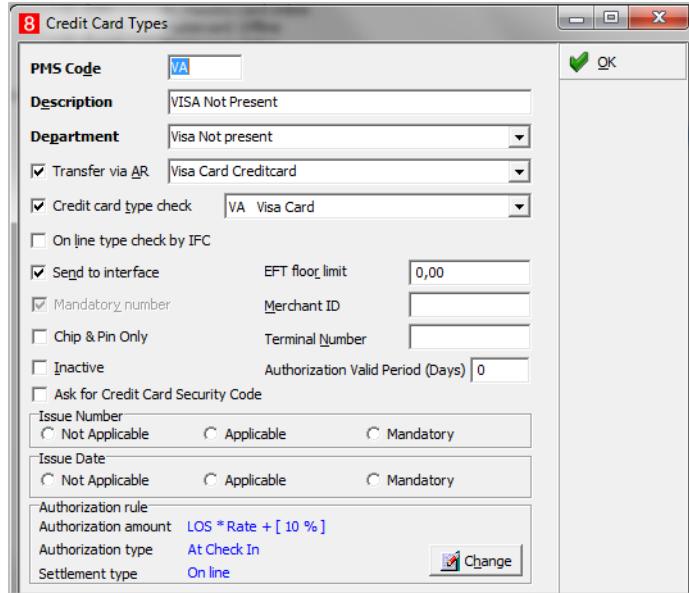
PMS Code = 2-letter code as setup in OPI (for example, VA for VISA)

Send to Interface = ticked

Chip & Pin Only = unticked

Authorization rule:

- **Authorization type** = At check in - will use CcAuthor messages to IFC8
- **Settlement type** = On line - will use CcSettl messages to IFC8



Debit Card Type

This is used for card types where the authorization will not be allowed, usually for Debit cards, Maestro, Girocard, V-Pay, any Mobile Payment card type (AliPay, PayPal) and so on.

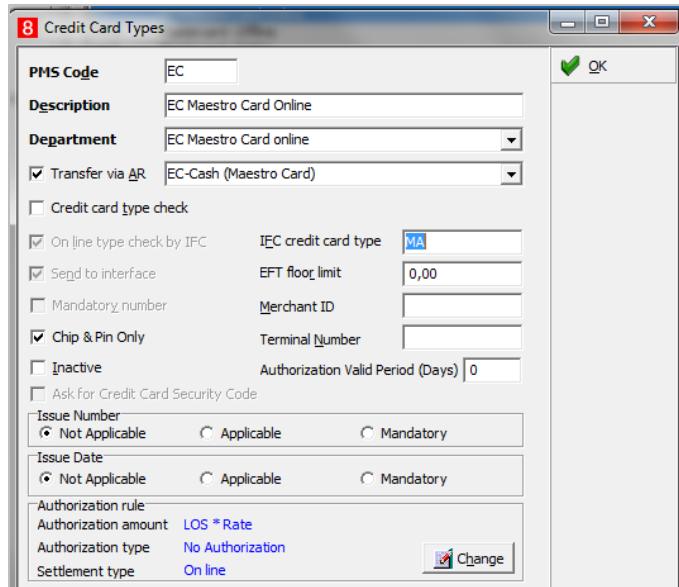
PMS Code = 2-letter code – freely definable

IFC Credit card type = 2-letter code as setup in OPI (for example, MD for Maestro Debit)

Chip & Pin only = active for Chip&Pin transaction

Authorization rule:

- **Authorization type** = No Authorization
- **Settlement type** = Online - will use CpPayOnly messages to IFC8



Tokenization Setup

User Right to Enable the Tokenization Feature

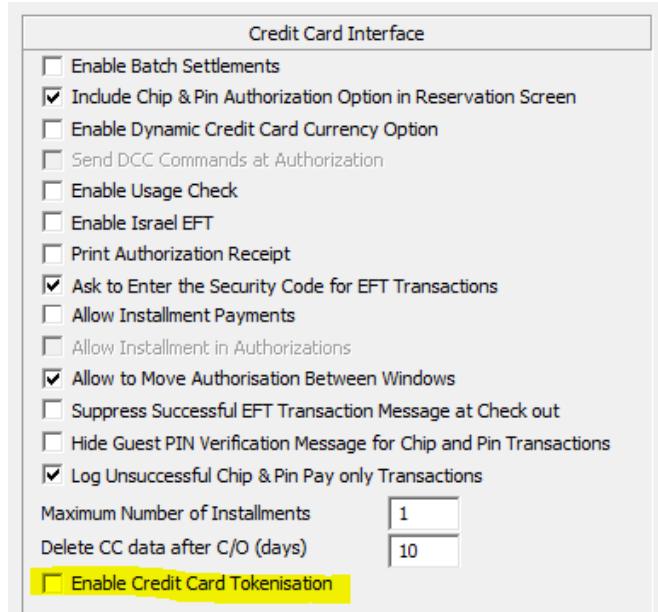
Activate the user rights under **Setup | Configuration | User Rights | Configuration | Global settings** security related to enable the activation of the guest anonymization.

NOTE:

This user right is not only required for this specific feature but also for other items in configuration.

Tokenization Functionality Settings

1. Activate the setting and **Enable Credit Card Tokenisation** under **Global Settings | Interface | 2 Interfaces (IFC8) | Credit Card Interface**.



2. As soon as you have activated the setting additional fields will populate.
3. Configure the connection to the OPI token proxy service which is typically installed with the OPI service on a computer on-premise. Suite8 PMS will always send a token ID request through this connection whenever a credit card number is being entered into the credit card number field within Suite8 application (card not present) or a credit card is received from external systems (CRS). It is also used to request token ID when the bulk tokenization function is executed.

Table 3-1 – Microsoft Windows Task Scheduler Settings

Parameter Name	Value	Description
Token Server URL	<code>https://IP Address of PC OPI is installed on:5012 /TokenOPERA</code>	URL of the OPI on-premise Token Proxy Service Values displayed in black font are hardcoded values.
Version	3.2	This is a hardcoded value.
Timeout	30	The timeout time waiting for response from OPI Token Proxy. Enter the value in seconds.
Chain Code	SUITE8 (Example)	As defined in OPI configuration
Max Requests	50	The number of credit cards to be sent in one bulk tokenization request. Enter a value between 1 and 50
Property Code	HOTEL (Example)	As defined in OPI configuration

Example:

Token Server URL	https://192.0.2.69:501/TokenOPERA		
User Name	OPITEST	Version	3.2
Password	*****	Time out	30
Chain Code	SUITE8	Max Requests	5
Property code	HOTEL		

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

To configure the link between the interfaces:

1. In the **Hotel Property Interface**, go to the **PMS1** tree and select **SERV** in the application layer.
2. Enter the **Suite8 IFC** number in the parameter **IfcNum** value. You can find the Suite8 IFC number in the IFC8 Database Configuration (ICFG_ID).

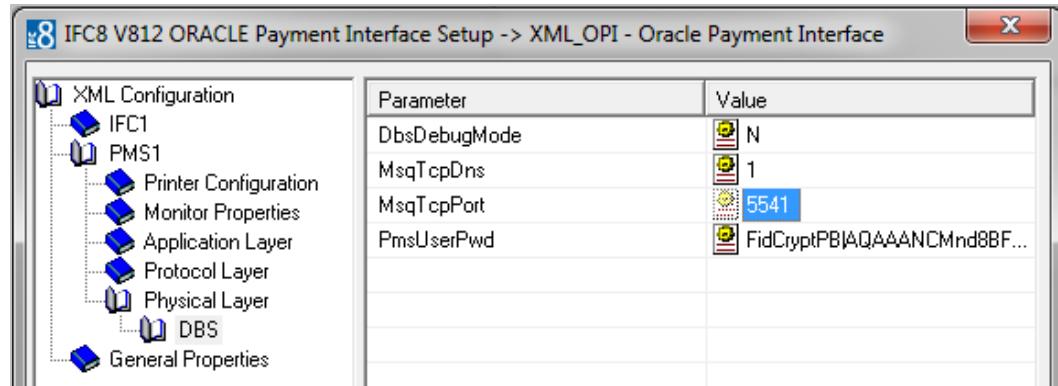
Ifc8 Database Configuration for "ICFG" (select Ifc & FktLogo)

ICFG_Setup	ICFG_FKT_LOGO-	ICFG_TYPE	ICFG_ID-	ICFG_HOTEL_ID	ICFG_ACTIVE	ICFG_LONGDESC
	XML_POS	PO	12	1	0	XML_POS
	XML_OPI	EF	18	1	1	V812 OPI Local

Ifc8 IFC8 V812 ORACLE Payment Interface Setup -> XML_OPI - Oracle Payment Interface

XML Configuration	Parameter	Value
IFC1	IfcNum	18
PMS1		
Printer Configuration		
Monitor Properties		
Application Layer		
SERV		
Protocol Layer		
Physical Layer		
General Properties		

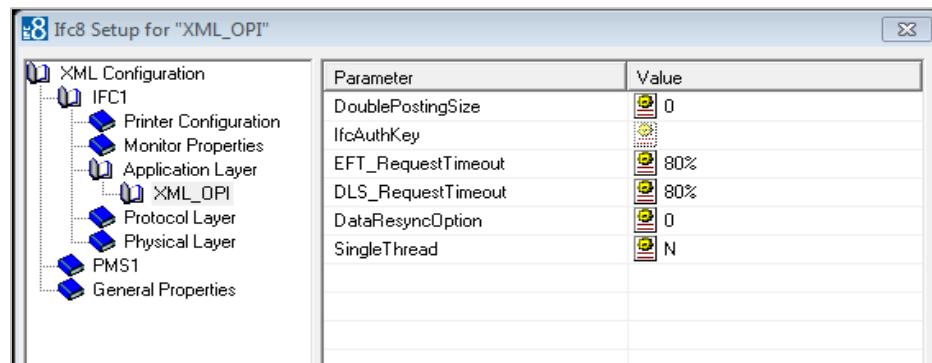
3. Go to the **PMS1 | Physical Layer | DBS**.
4. Enter the port number into Parameter value **MsqTcpPort**. This is the port IFC8 uses to communicate with Suite8 PMS.
5. Select **Enter** and **Apply** to re-initiate IFC8, and then click **Save**.



Configuring Encryption 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.

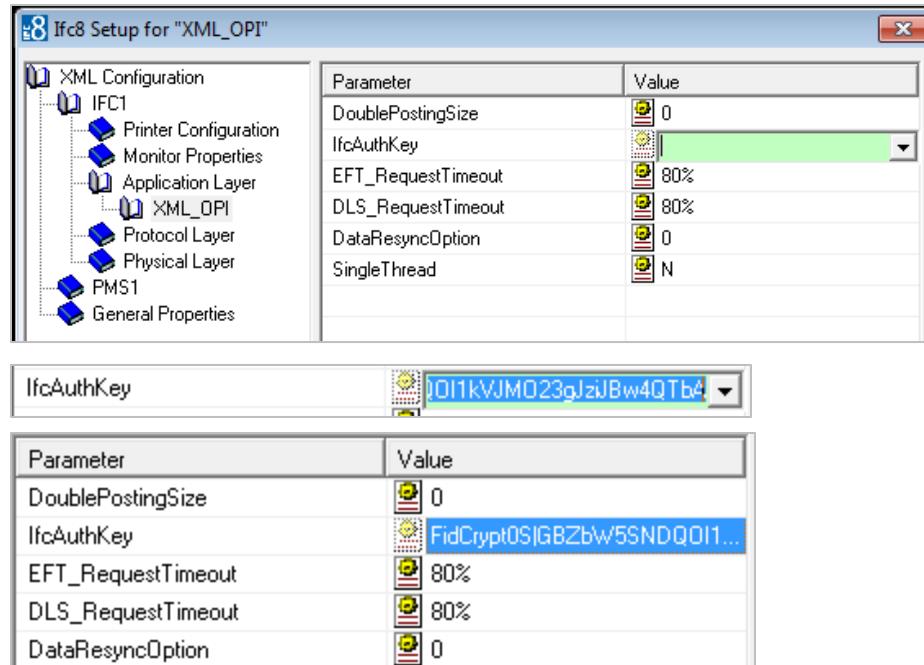
1. In the Hotel Property Interface (IFC8) configuration, go to the **IFC1** tree, and then in the **Application Layer**, select the **XML_OPI** option.



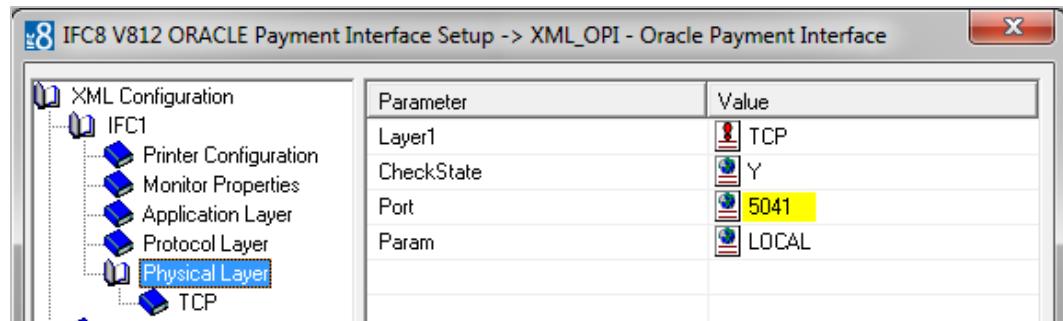
2. Copy the generated key from Configuring OPI - OPERA merchant step 3, and add "FidCrypt0S|" to the generated key as prefix.

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.

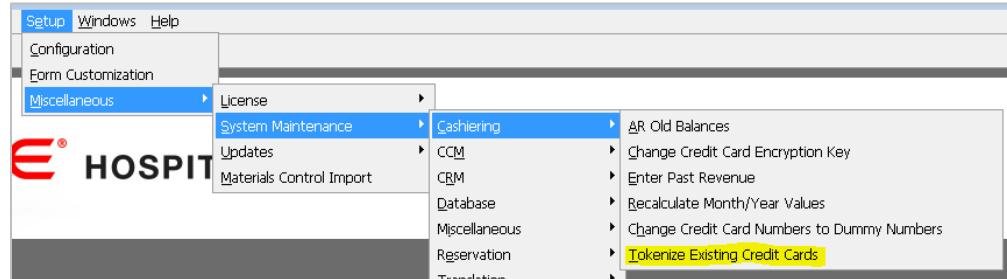


6. Click **Apply**, IFC8 reinitiates.
7. The **IfcAuthKey** value now shows an encrypted key and the entered string is now encrypted by IFC8.
8. Click **Save**, and then click **OK** to close the IFC8 Configuration form.

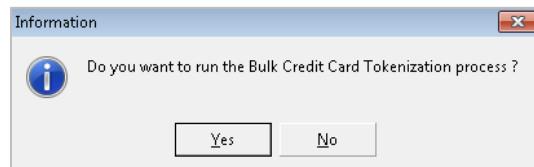
IFC8 now connects with OPI to verify IFC8 successful status, confirm that all 6 status indicators are green.

Perform a Tokenization

1. Go to **Setup | Miscellaneous | System Maintenance | Cashiering** and select **Tokenize Existing Credit Cards** to replace all existing credit cards with token ID's.



2. A new window will open.



3. Select **Yes** to start the process and all existing credit card numbers stored in the Suite8 database will be exchanged with a token ID. The process will send out a request message to OPI containing max 50 credit card numbers (depending on the defined values in global settings) and Expiry Date and expects a response message with a token ID. In case a credit card will not receive a token ID, the existing credit card will be masked automatically and stored without a token ID. A credit card which

is already expired retrieves no token ID but will be also masked automatically and stored without a token ID.

NOTE:

After the successful replacement of credit card numbers with token ID's the process should NOT be executed again.

4. Go to user rights and deny the user right **Run bulk Credit card Tokenization** as this process should only be executed at the time of activation of EFT tokenization handling.

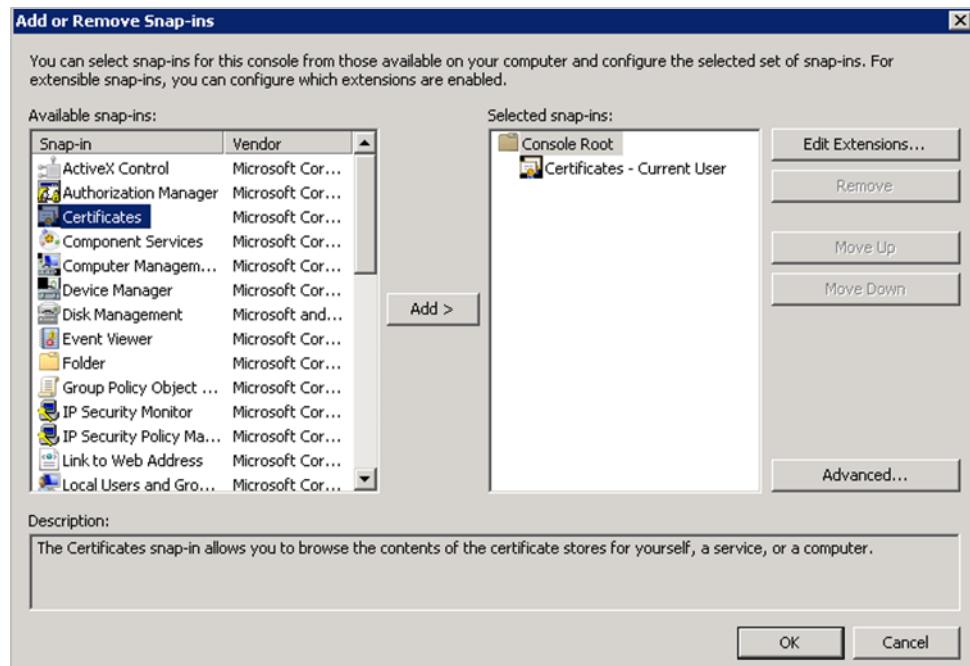
OPI only supports the **Convert CC** function; the other conversion options are not currently supported.

Certificate Import using Microsoft Management Console

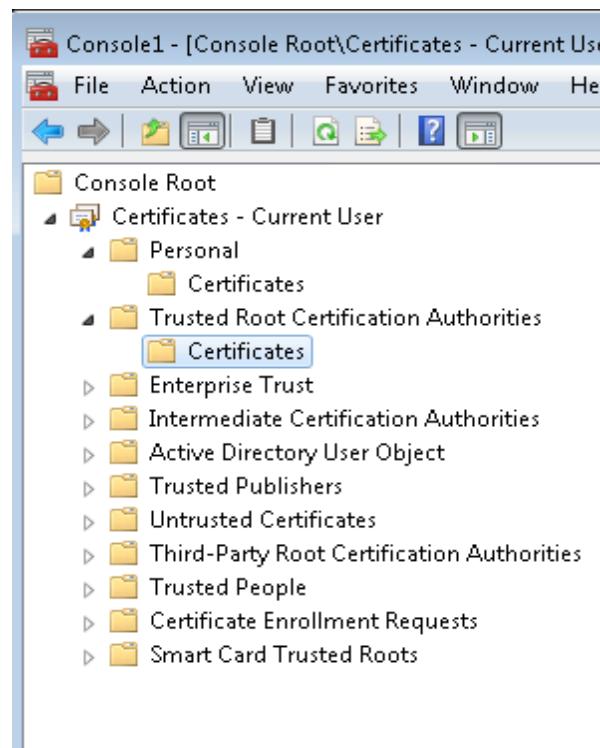
1. Find and open **mmc . exe** from Start menu.



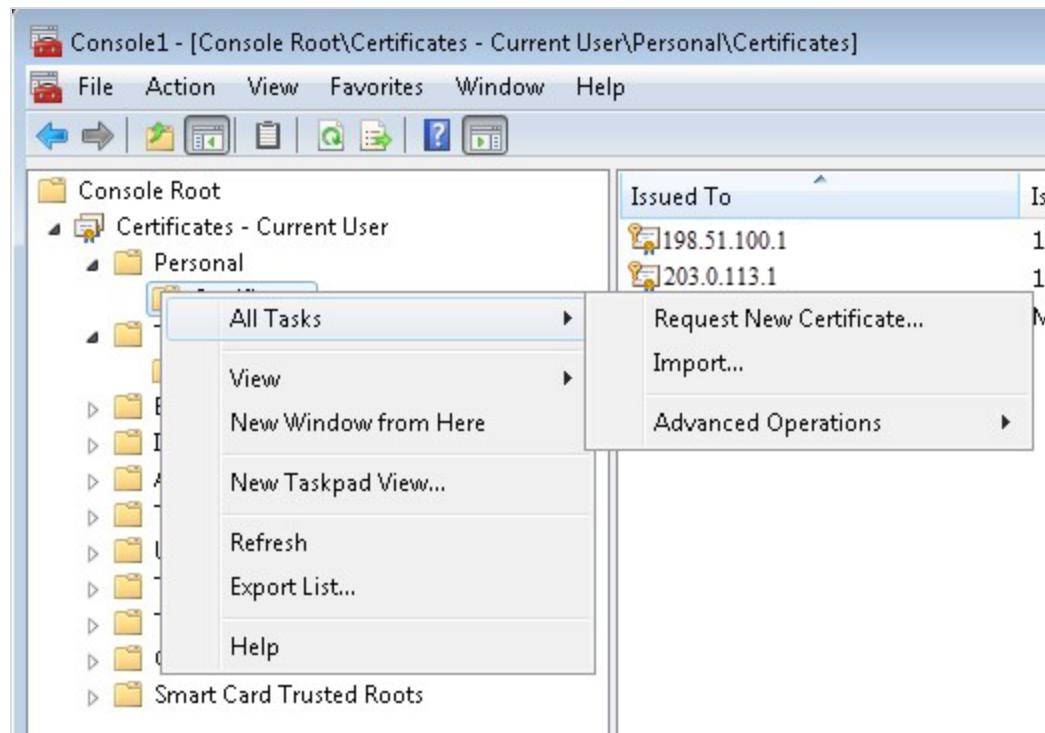
2. Go to **File | Add or Remove Snap-ins**, add certificates to **Selected snap-ins**, and then click **OK**.



3. Expand Certificates, expand Personal or Trusted Root as required, and then 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 then click **Next**.
- If the import is successful, then the certificates Common Name will be listed under the folder that was selected during import.

4

Upgrading the OPI

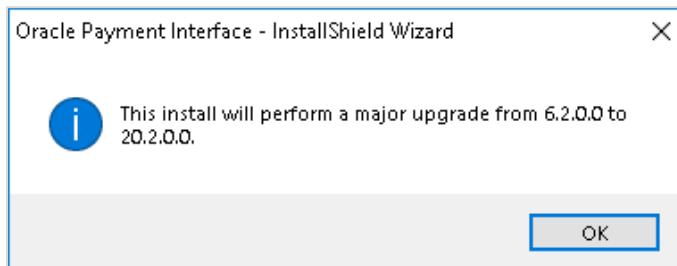
VERY IMPORTANT: Read and follow the upgrade directions.

NOTE:

- OPI 6.1 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

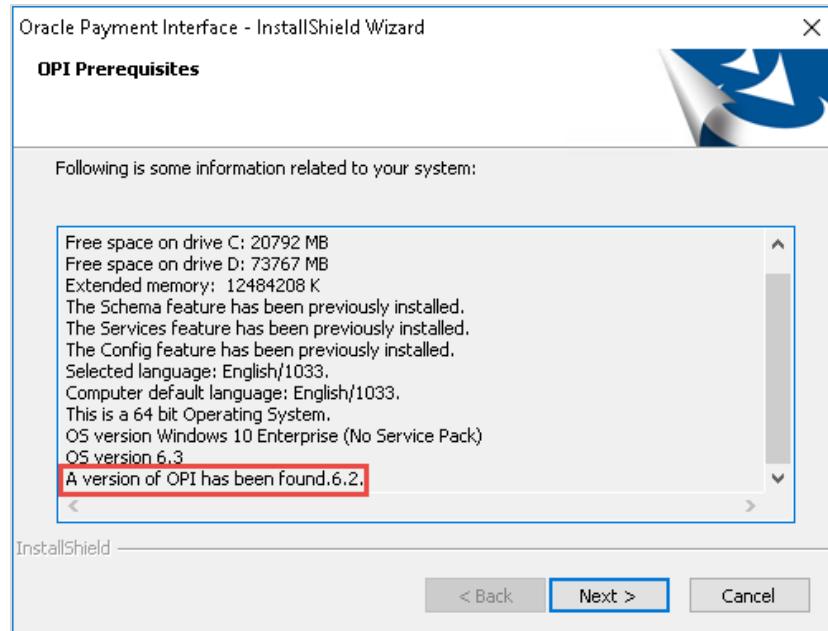
Upgrading OPI 6.2.0.0 to 20.2.0.0

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.



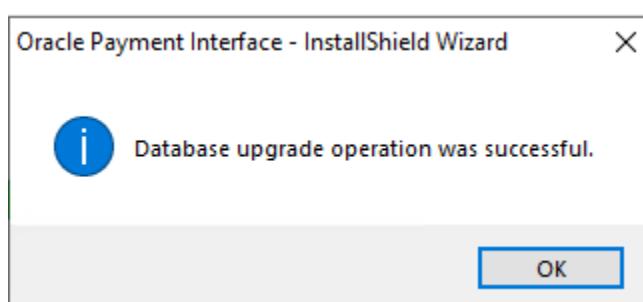
6. Choose a Destination Location. Accept the default installation location or click **Change...** to choose a different location.

7. Click **Next**.

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

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

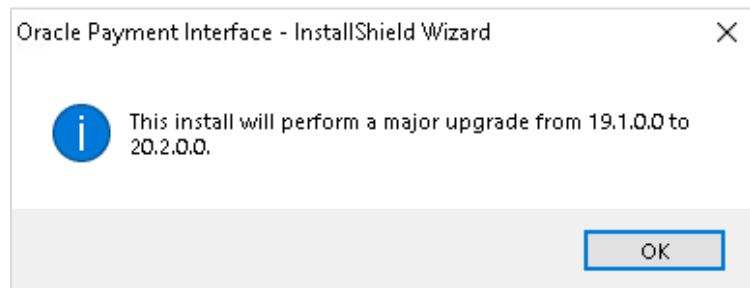
9. Click **OK**.



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.

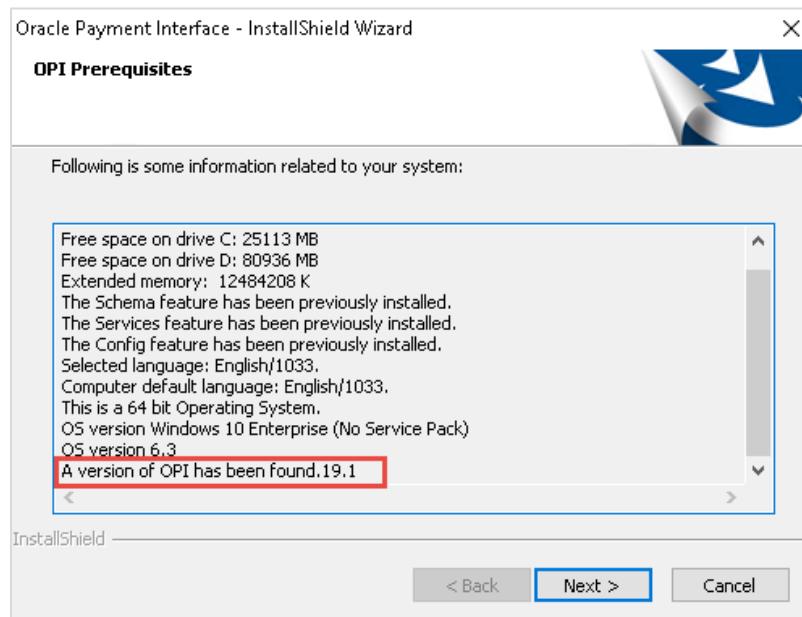
Upgrading OPI 19.1.0.0 to 20.2.0.0

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**.

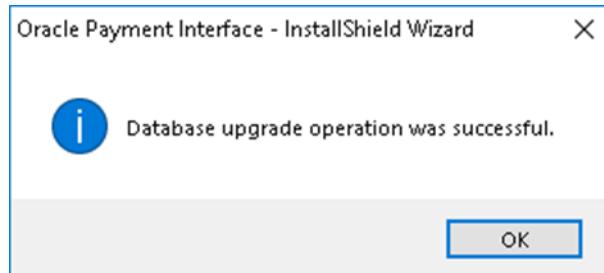
Ensure all the prerequisites for the OPI installation are met.



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.

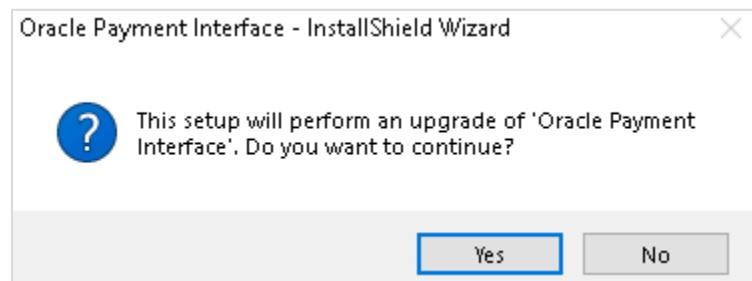
8. Click **Install** to begin the installation.
9. Click **OK**.



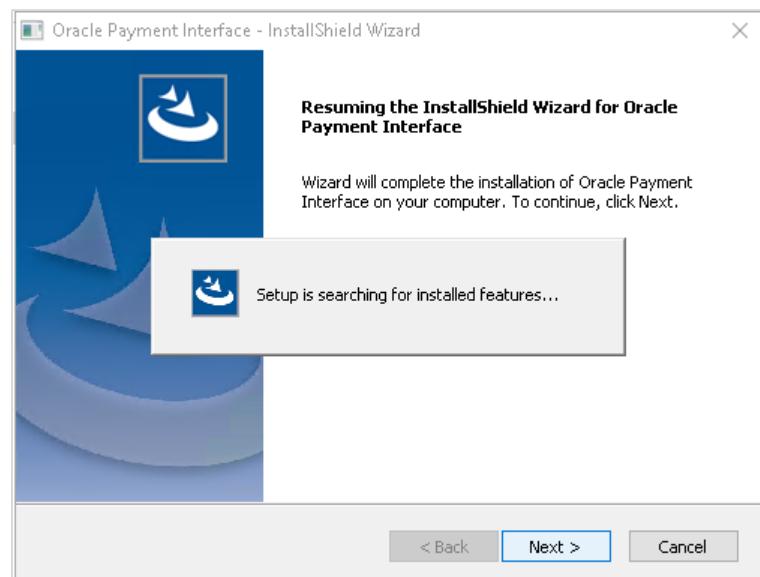
10. Enter the **Host** and **Port** that should be used to connect to the OPI Config Service for the Merchant Configuration.
11. Once the installation is complete, the installer will prompt for a reboot of the host machine.

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.

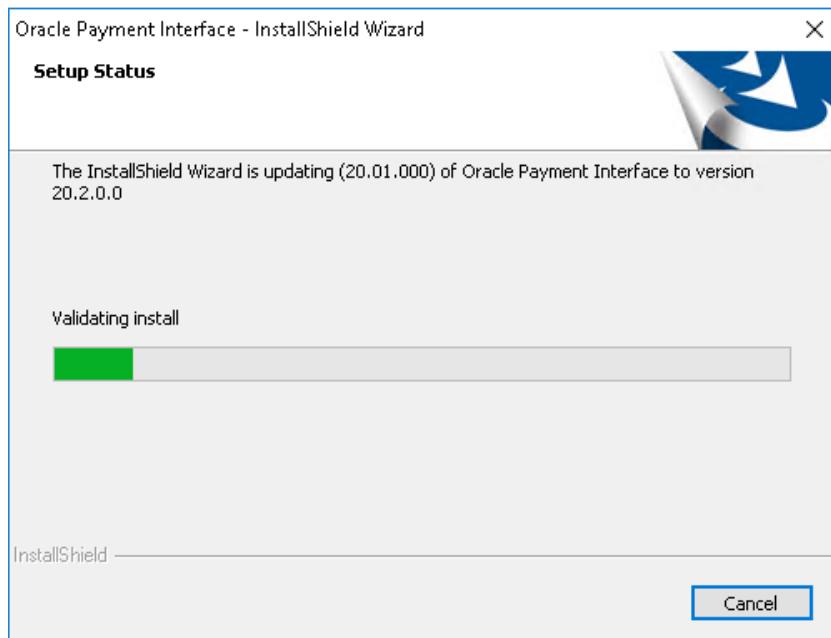


2. Click **Yes**.



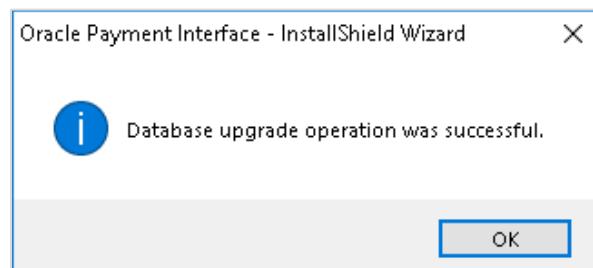
3. Click **Next**.

Setup is searching for installed features.



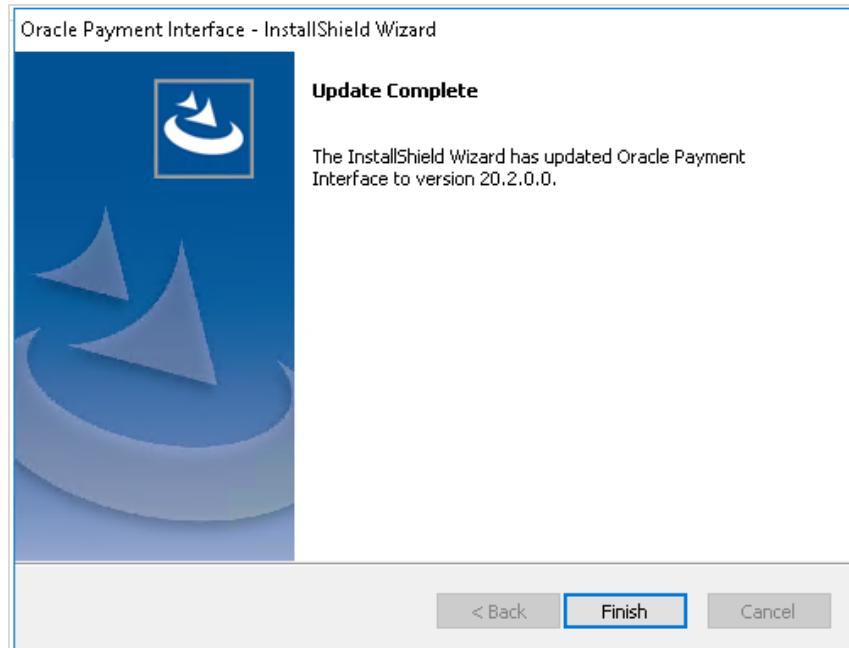
4. Click **Next.**

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.