Oracle Hospitality Payment Interface

Suite8 PMS OPI Installation Guide

Release 20.4
F95649-01
June 2024

Oracle Hospitality Payment Interface Suite8 PMS OPI Installation Guide Release 20.4

F95649-01

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 3-6
Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC) 3-8
Configuring Encryption for the Hotel Property Interface (IFC8) with OPI 3-9
Perform a Tokenization 3-11

4 Upgrading the OPI 4-1

Upgrading OPI 19.1.0.0 to 20.4.0.0 4-1
Upgrading OPI 20.1.0.0 to 20.4.0.0 4-4
Upgrading OPI 20.2.0.0 to 20.4.0.0 4-6
Upgrading OPI 20.3.0.0 to 20.4.0.0 4-8

Preface

Purpose

This document describes how to install Oracle Payment Interface (OPI) with the Suite8 Property Management System (PMS) and 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 the Customer Support Portal at the following URL:

https://iccp.custhelp.com

When contacting Customer Support, please provide the following:

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

Documentation

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

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

Table 1-1 Revision History

Date	Description
June 2024	• 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 20.4 does not install a database. If you are doing a clean install of OPI, a database must be installed first.
- OPI upgrade functionality supports:
  - Upgrading OPI 19.1 (include patch releases) to OPI 20.4
  - Upgrading OPI 20.1 (include patch releases) to OPI 20.4
  - Upgrading OPI 20.2 (include patch releases) to OPI 20.4
  - Upgrading OPI 20.3 (include patch releases) to OPI 20.4
- OPI requires 64bit Operating System only.
- OPI requires at least 6 GB of free disk space and you must install OPI as a System Administrator.
- The Oracle Payment Interface Installer release 20.4 supports the following database connections:
  - MySQL Database 5.7 and 8.0
  - Oracle Database 11g / 12c / 19c

> **NOTE:**
>
> Stay current by upgrading your Java version as Oracle CPUs/Alerts are announced.

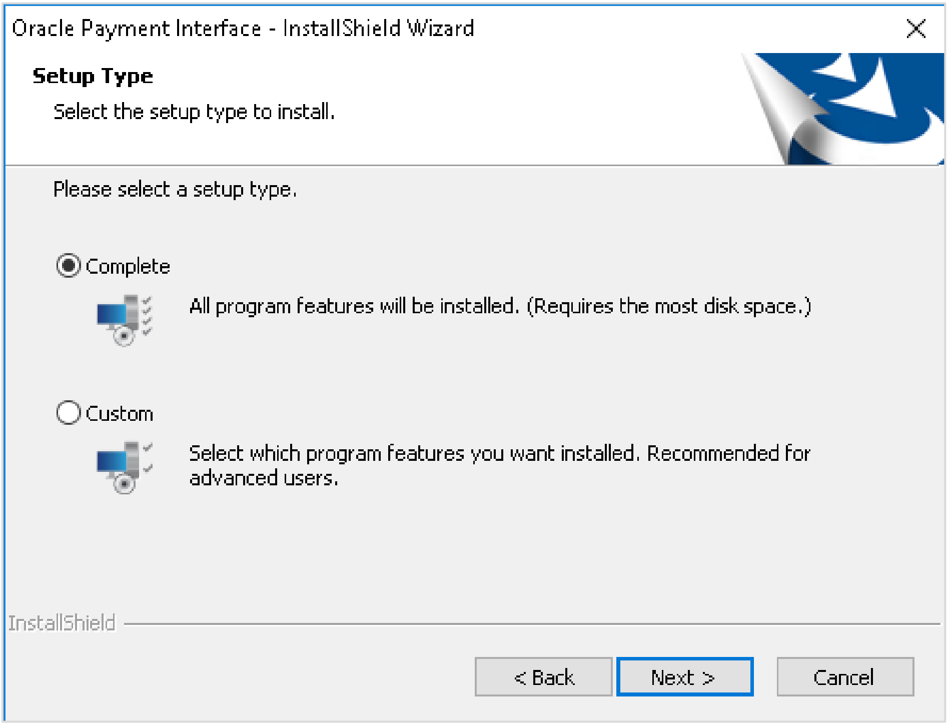
- The Oracle Payment Interface release 20.4 is compatible with the following operating systems:
  - Microsoft Windows 10 Professional
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 11 Professional
  - Microsoft Windows 11 Enterprise
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022

During the installation you must confirm the following:

- Merchant IDs
- IP address of the OPI Server
- 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_20.4.0.0.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.



Oracle Payment Interface - InstallShield Wizard

Setup Type

Select the setup type to install.

Please select a setup type.

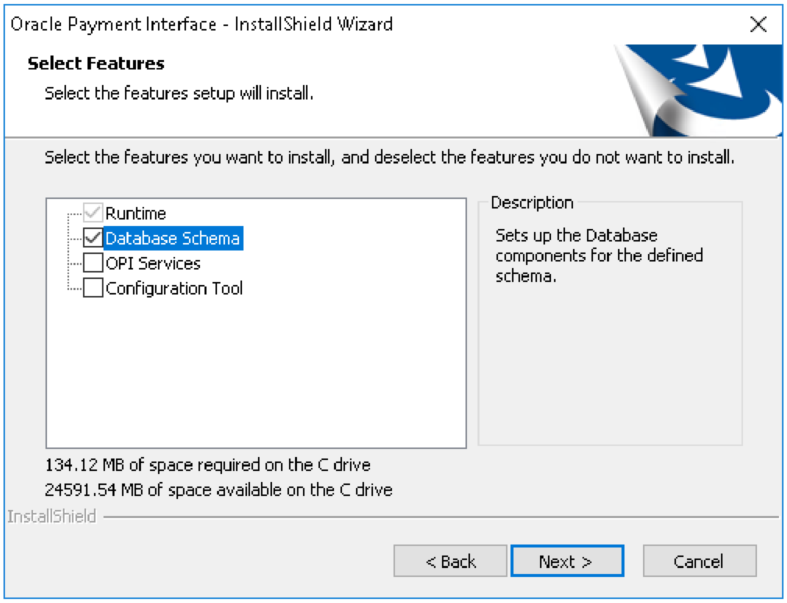
● Complete

All program features will be installed. (Requires the most disk space.)

○ Custom

Select which program features you want installed. Recommended for advanced users.

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.



Oracle Payment Interface - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☑ Runtime
☑ Database Schema
□ OPI Services
□ Configuration Tool

Description

Sets up the Database components for the defined schema.

134.12 MB of space required on the C drive
24591.54 MB of space available on the C drive

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

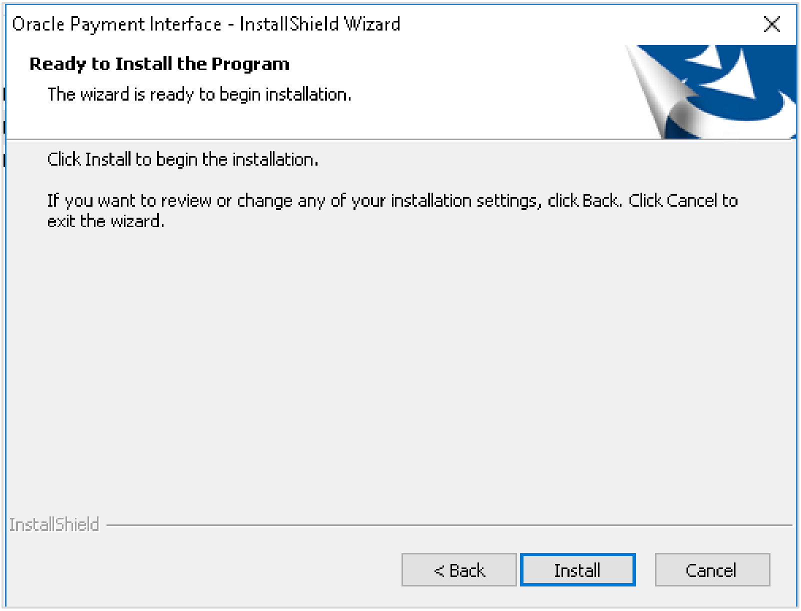
All these three features must be installed. Ensure whether they all are installed on the same computer or on separate computers. It is just a matter of whether they are all installed on the same computer or on separate computers.

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.



Oracle Payment Interface - InstallShield Wizard

Ready to Install the Program

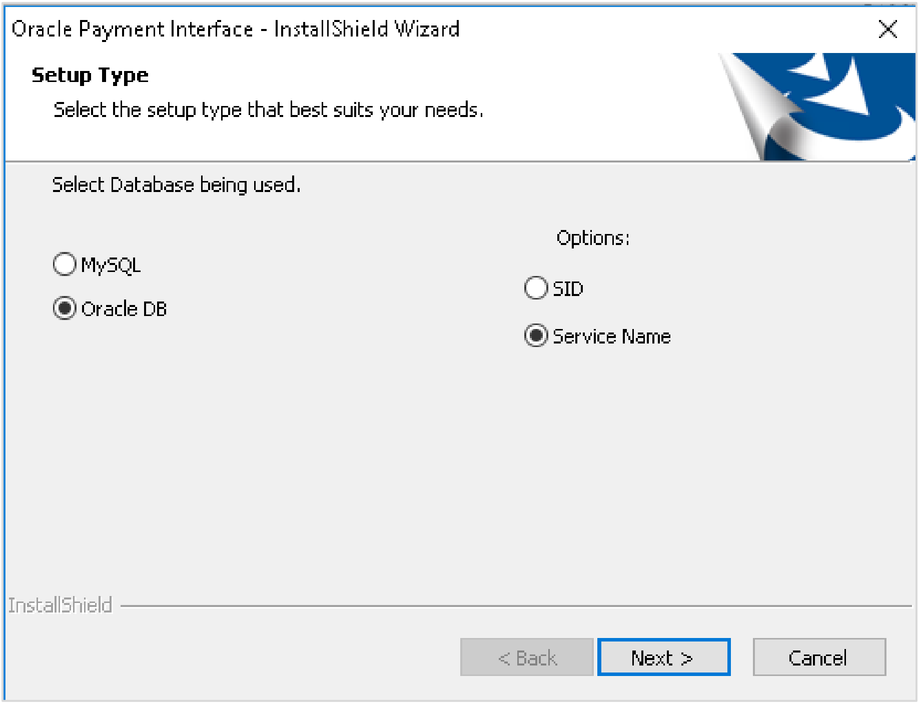
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

10. Select your Database type:

- My SQL
- Oracle DB



Oracle Payment Interface - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Select Database being used.

○ MySQL
● Oracle DB

Options:

○ SID
● Service Name

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

> **NOTE:**
>
> OPI does not install any database, so the database must already be installed.

MySQL

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

Oracle DB

SID

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

Service Name

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

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

13. Enter the username and password to create a new database user account. If the username already exists in the database, you are prompted to select a different username.

    a. When creating the username for the database, the installer allows only alphanumeric characters and should start only with an alphabetic character, NOT a number.

    b. Enter a password according to the requirements specified.

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

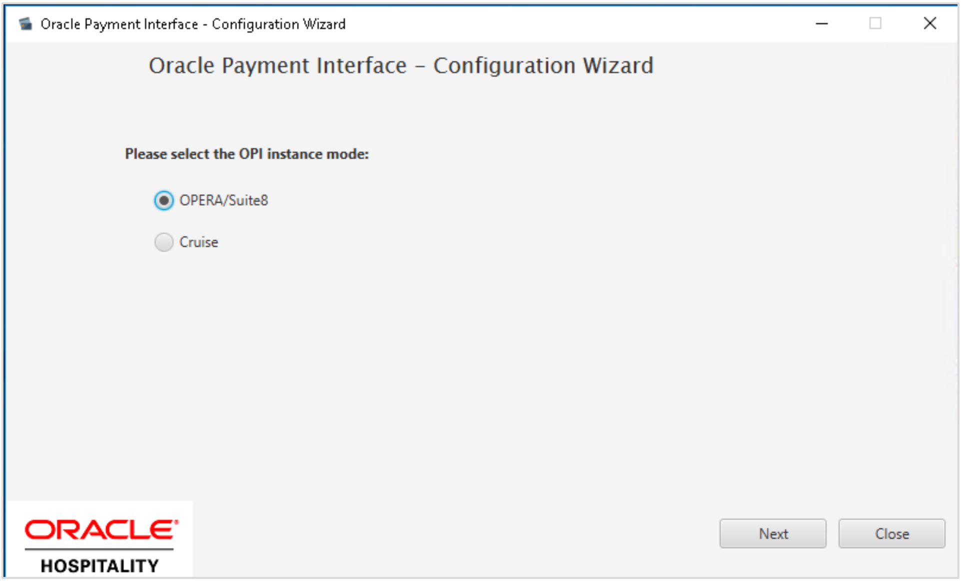
14. Enter the username and password to create a Super User System Admin level account that is used for configuring and maintaining the system.

15. Enter the **Host** and **Port**.

> **NOTE:**
>
> In the previous step you are not configuring the port the service will listen on. Instead, it is prompting for the details on how to connect.
>
> - The IP will depend on where the OPI Config Service is installed. If you are performing a complete installation, this can be left as the localhost address.
> - The default port is 8090.

16. Set and confirm the passphrase value.

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

Please select the OPI instance mode:

● OPERA/Suite8

○ Cruise

17. Select the OPI instance mode for PMS merchants as **OPERA/Suite8**.

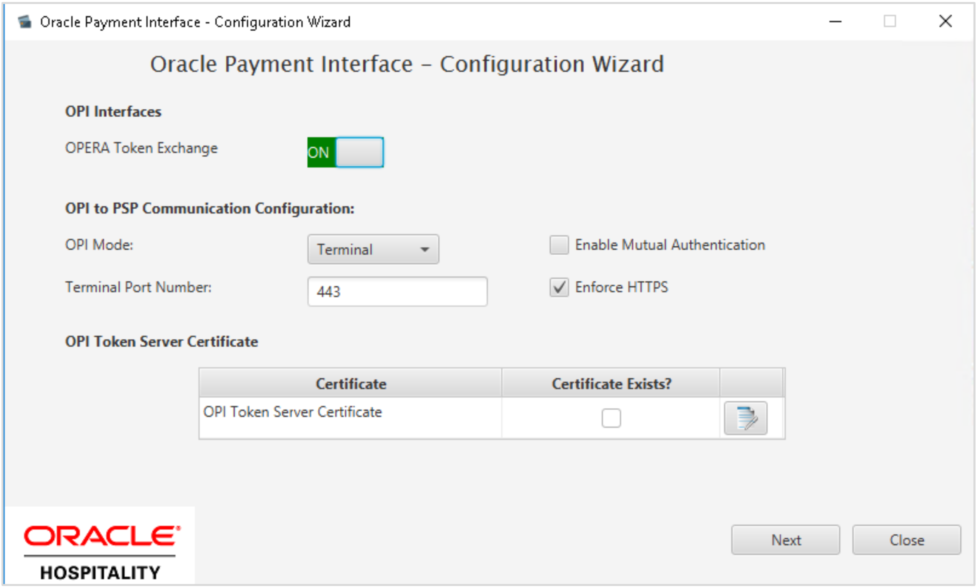
    On the **OPI Interface** screen, the configuration screens displayed are same as when the configuration wizard is launched manually. (**:\OraclePaymentInterface\v20.4\Config\LaunchWizard.bat**)

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.



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

OPI Interfaces

OPERA Token Exchange: ON

OPI to PSP Communication Configuration:

OPI Mode: Terminal

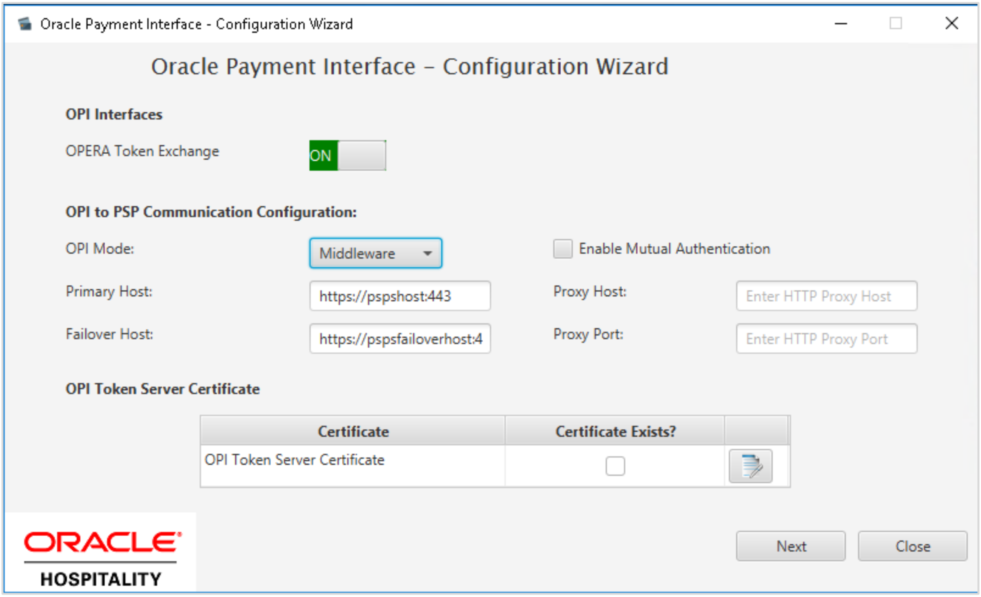
Terminal Port Number: 443

□ Enable Mutual Authentication

☑ Enforce HTTPS

OPI Token Server Certificate

Certificate	Certificate Exists?	
OPI Token Server Certificate	□	



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

OPI Interfaces

OPERA Token Exchange: ON

OPI to PSP Communication Configuration:

OPI Mode: Middleware

□ Enable Mutual Authentication

Primary Host: https://pspshost:443

Proxy Host: Enter HTTP Proxy Host

Failover Host: https://pspsfailoverhost:4

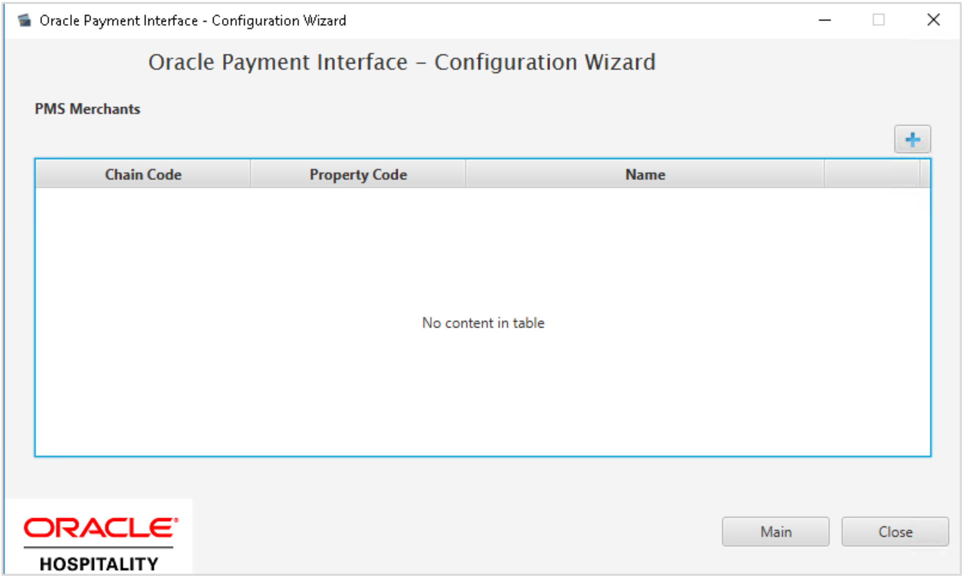
Proxy Port: Enter HTTP Proxy Port

OPI Token Server Certificate

Certificate	Certificate Exists?	
OPI Token Server Certificate	□	

- **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.


Oracle Payment Interface - Configuration Wizard
Oracle Payment Interface – Configuration Wizard
PMS Merchants
+
Chain Code
Property Code
Name
No content in table
ORACLE
HOSPITALITY
Main
Close

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

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

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

    b. Select **Generate Key**. Use to generate an IFC8 Communication key. The generated key will have the prefix **FidCrypt0S|** that is automatically added. Use this generated key when configuring the key in IFC8 software.

    c. Enter the **IFC8 IP address** and **port** number for the Hotel Property Interface (IFC8) server.

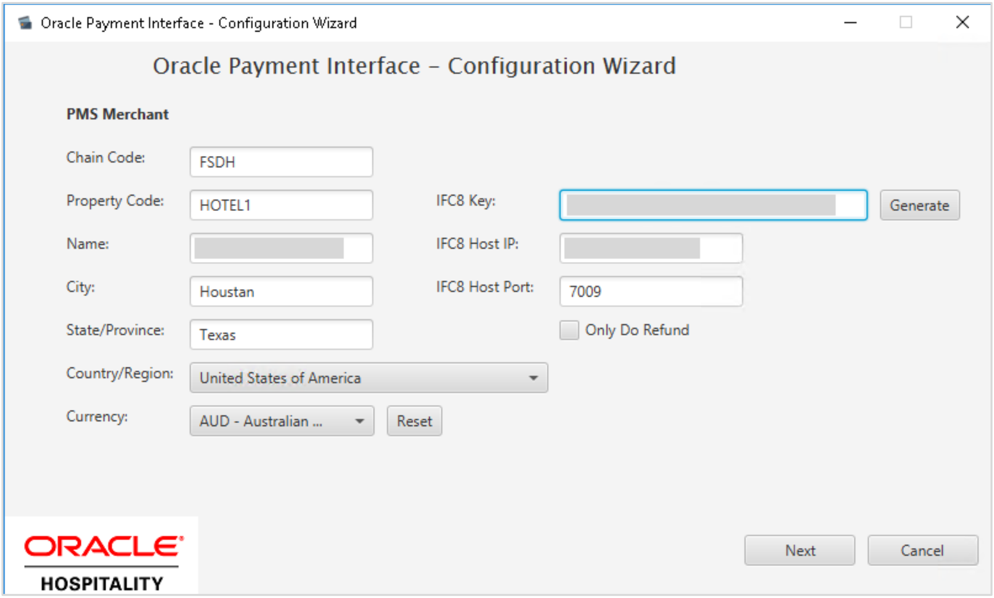
    d. Enter the Merchant **Name**, **City**, **State/Province** and **Country/Region** information.

    e. **Currency**: The currency selection by the merchant in which the transactions are to be processed. Merchants can override selected transaction currency irrespective of country/region selection. For example: If a merchant's selects country as 'United States of America', then they can select the currency from the list of all available currencies (AUD, AED, AFN and so on) and this currency is used for transaction currency. **Reset**: To reset the currency back to use country/region currency.

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

    g. Click **Next**.

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

PMS Merchant

Chain Code: FSDH

Property Code: HOTEL1

Name: [redacted]

City: Houstan

State/Province: Texas

Country/Region: United States of America

Currency: AUD - Australian ...

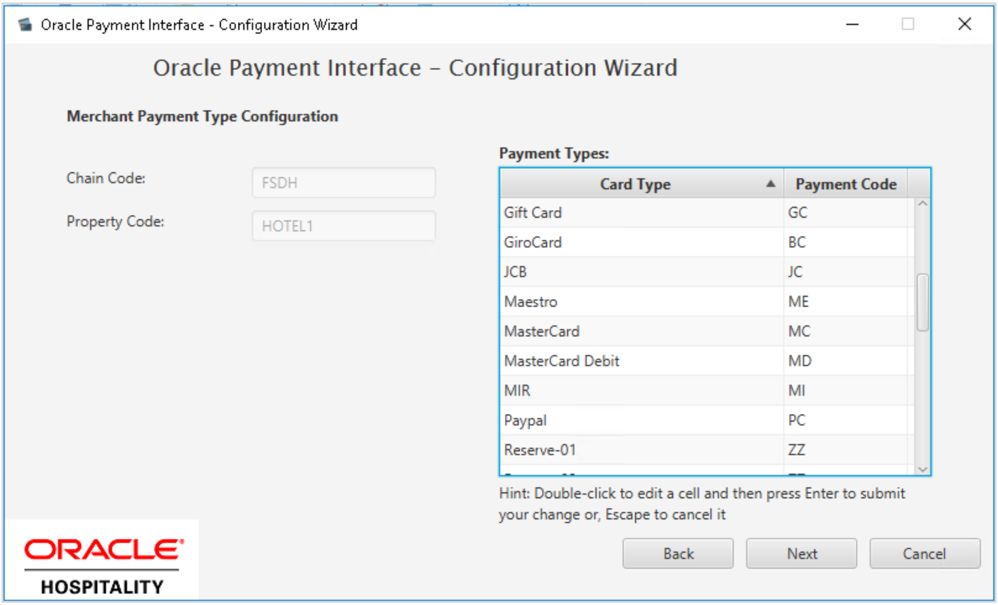
IFC8 Key: [redacted]

IFC8 Host IP: [redacted]

IFC8 Host Port: 7009

□ Only Do Refund

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

Merchant Payment Type Configuration

Chain Code: FSDH

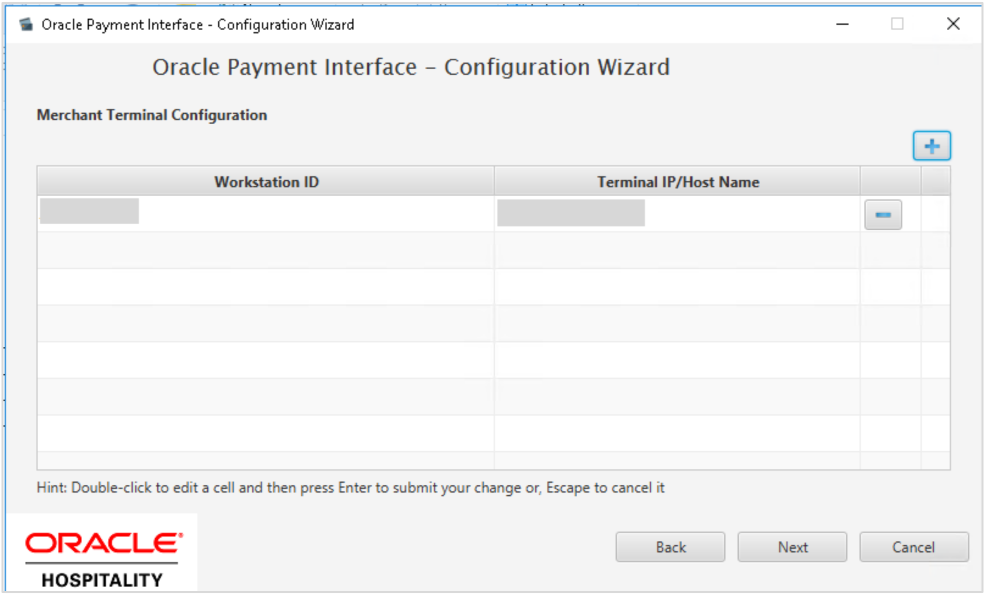
Property Code: HOTEL1

Payment Types:

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

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

Below is terminal mapping if you select Terminal mode.



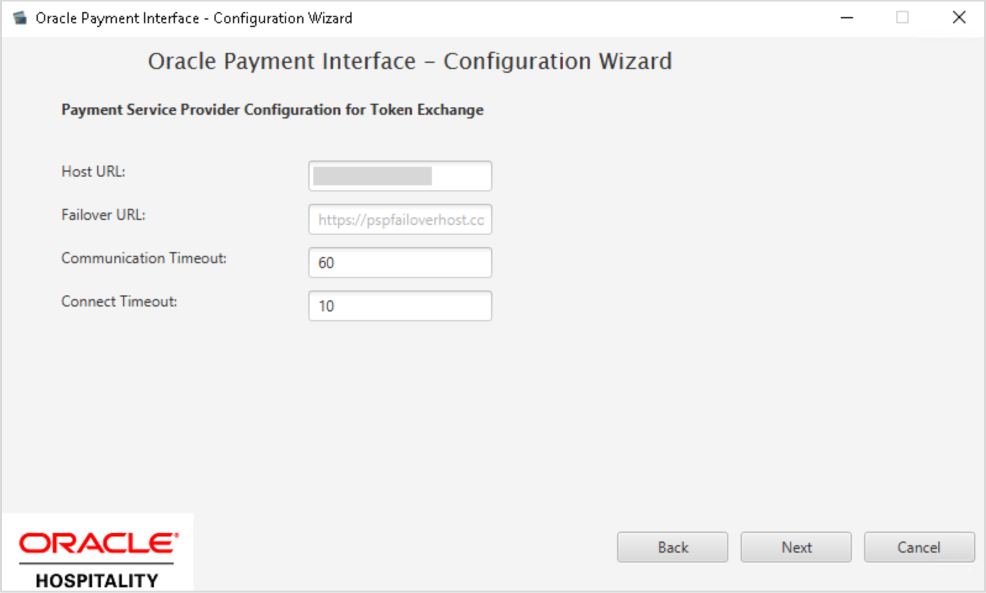
Oracle Payment Interface – Configuration Wizard

Merchant Terminal Configuration

Workstation ID	Terminal IP/Host Name
[redacted]	[redacted]

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

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.**



Oracle Payment Interface – Configuration Wizard

Payment Service Provider Configuration for Token Exchange

Host URL: [redacted]

Failover URL: https://pspfailoverhost.cc

Communication Timeout: 60

Connect Timeout: 10

23. Click **Finish** to restart.

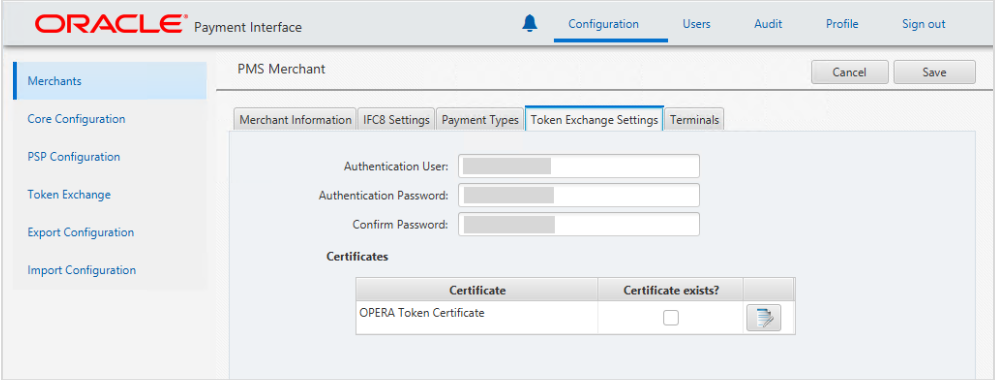
Token Exchange Settings

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\v20.4\Config\LaunchConfiguration.bat**
- Login with the Super user account created during OPI installation.

- Select **Merchants** tab, and click **Token Exchange Settings** subtab.



PMS Merchant

Authentication User: [redacted]

Authentication Password: [redacted]

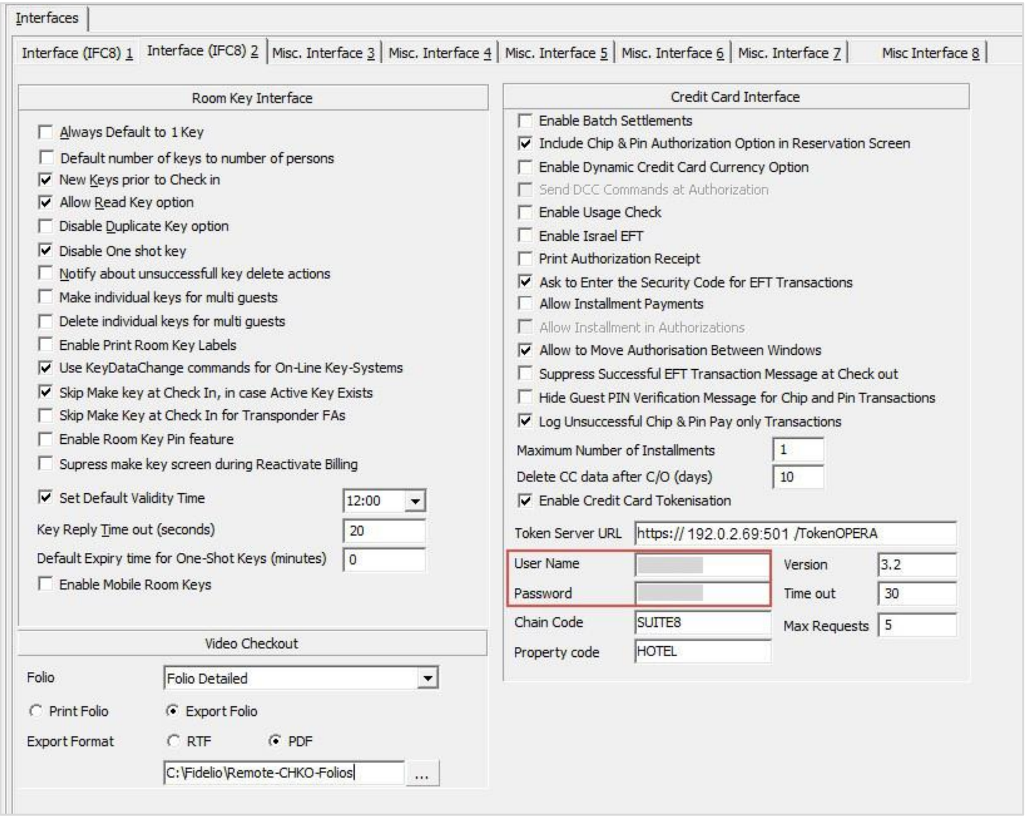
Confirm Password: [redacted]

Certificates

Certificate	Certificate exists?	
OPERA Token Certificate	□	

- **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.)**



Room Key Interface

- □ Always Default to 1 Key
- □ Default number of keys to number of persons
- ☑ New Keys prior to Check in
- ☑ Allow Read Key option
- □ Disable Duplicate Key option
- ☑ Disable One shot key
- □ Notify about unsuccessfull key delete actions
- □ Make individual keys for multi guests
- □ Delete individual keys for multi guests
- □ Enable Print Room Key Labels
- ☑ Use KeyDataChange commands for On-Line Key-Systems
- ☑ Skip Make key at Check In, in case Active Key Exists
- □ Skip Make Key at Check In for Transponder FAs
- □ Enable Room Key Pin feature
- □ Supress make key screen during Reactivate Billing
- ☑ Set Default Validity Time: 12:00

Key Reply Time out (seconds): 20

Default Expiry time for One-Shot Keys (minutes): 0

- □ Enable Mobile Room Keys

Video Checkout

Folio: Folio Detailed

○ Print Folio ● Export Folio

Export Format: ○ RTF ● PDF

C:\Fidelio\Remote-CHKO-Folios ...

Credit Card Interface

- □ Enable Batch Settlements
- ☑ Include Chip & Pin Authorization Option in Reservation Screen
- □ Enable Dynamic Credit Card Currency Option
- □ Send DCC Commands at Authorization
- □ Enable Usage Check
- □ Enable Israel EFT
- □ Print Authorization Receipt
- ☑ Ask to Enter the Security Code for EFT Transactions
- □ Allow Installment Payments
- □ Allow Installment in Authorizations
- ☑ Allow to Move Authorisation Between Windows
- □ Suppress Successful EFT Transaction Message at Check out
- □ Hide Guest PIN Verification Message for Chip and Pin Transactions
- ☑ Log Unsuccessful Chip & Pin Pay only Transactions

Maximum Number of Installments: 1

Delete CC data after C/O (days): 10

- ☑ Enable Credit Card Tokenisation

Token Server URL: https:// 192.0.2.69:501 /TokenOPERA

User Name	[redacted]	Version	3.2
Password	[redacted]	Time out	30
Chain Code	SUITE8	Max Requests	5
Property code	HOTEL		

- 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

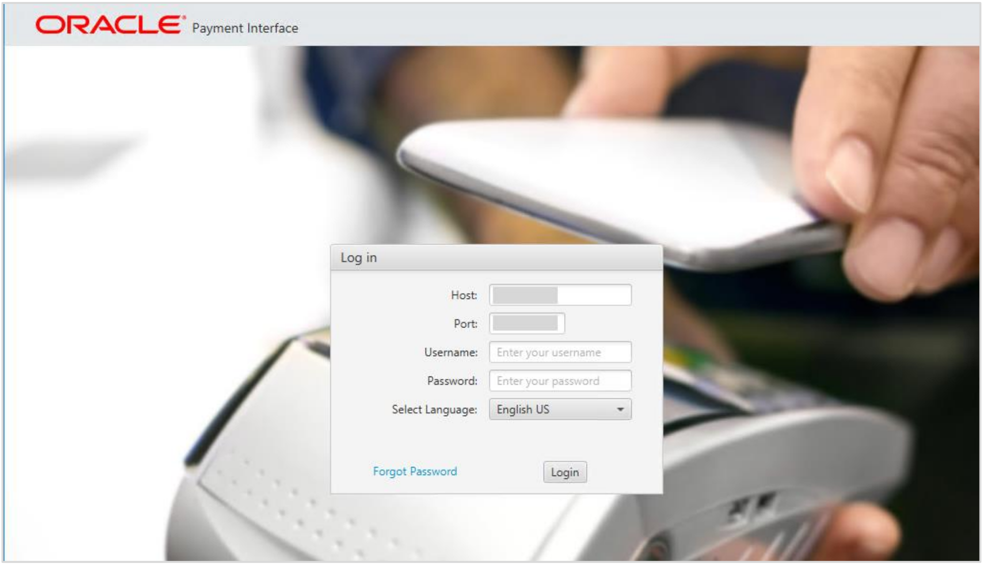
The communication from OPI to the PSP for the token exchange uses HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed on PSP (server side) for HTTPS communication, the PSP is also expected to provide a client side certificate 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\v20.4\Config\LaunchConfiguration.bat**
2. Login with the Super user account created during OPI installation.



Host:

Port:

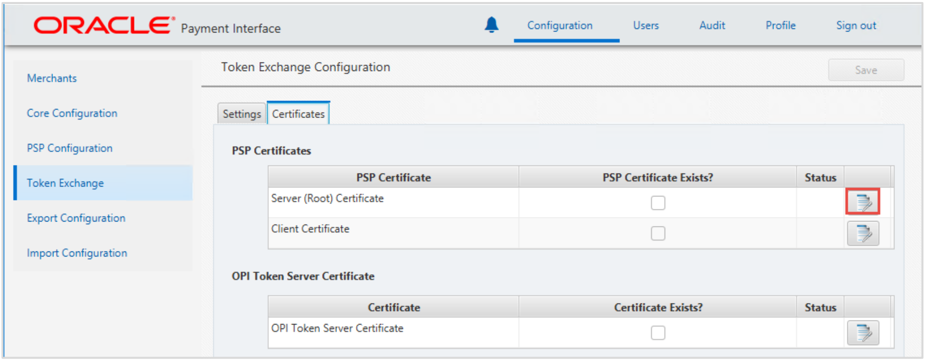
Username: Enter your username

Password: Enter your password

Select Language: English US

Handling the Root Certificate File by OPI Configuration Tool.

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



Token Exchange Configuration

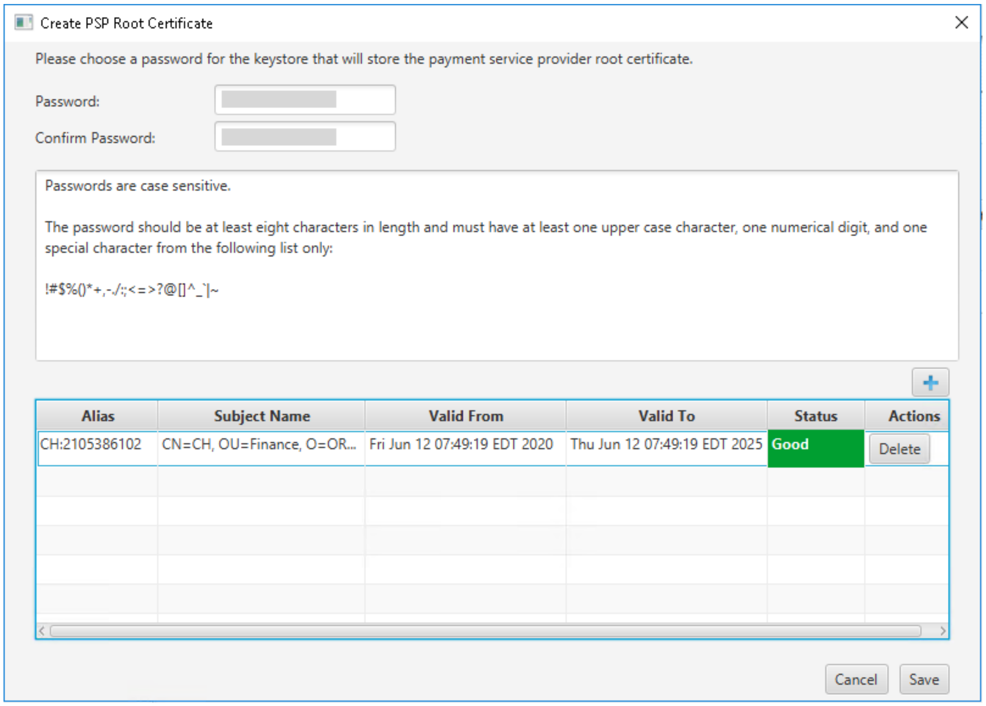
PSP Certificates

PSP Certificate	PSP Certificate Exists?	Status
Server (Root) Certificate	□	
Client Certificate	□	

OPI Token Server Certificate

Certificate	Certificate Exists?	Status
OPI Token Server 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.



Please choose a password for the keystore that will store the payment service provider root certificate.

Password:

Confirm Password:

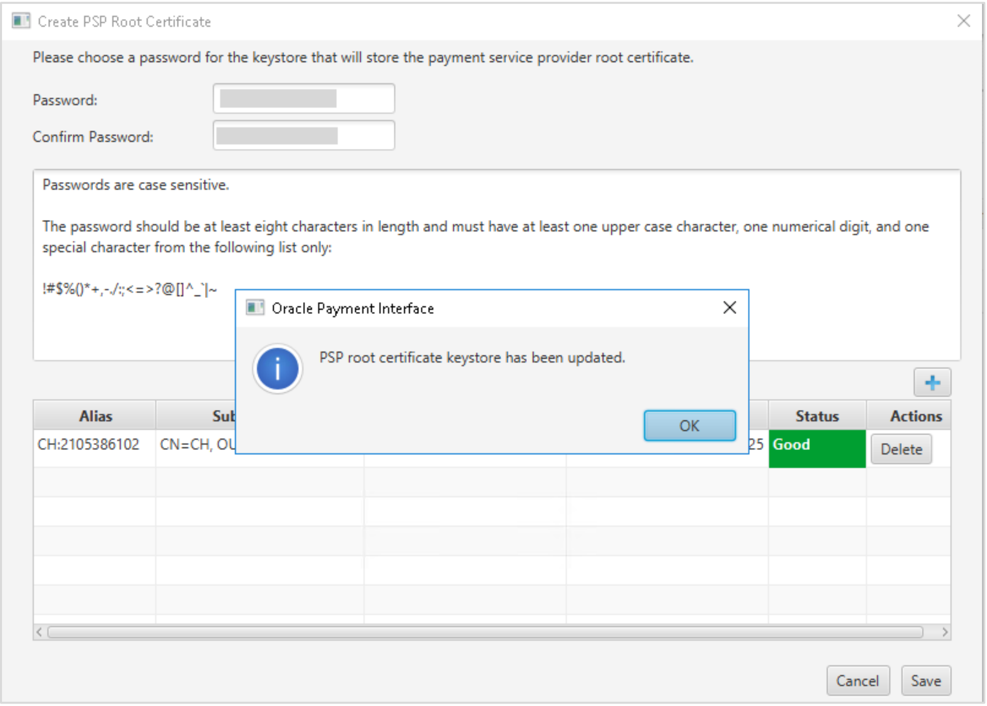
Passwords are case sensitive.

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

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

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**.



Please choose a password for the keystore that will store the payment service provider root certificate.

Password:

Confirm Password:

Passwords are case sensitive.

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

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

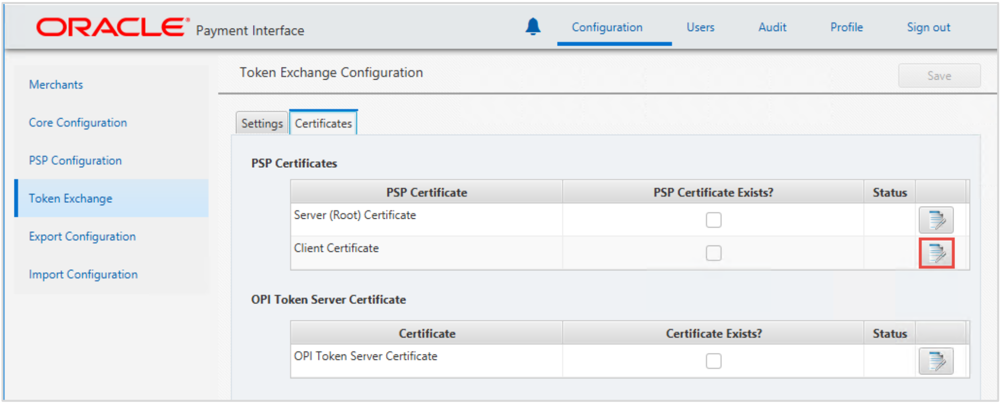
PSP root certificate keystore has been updated.

Alias	Sub	Status	Actions
CH:2105386102	CN=CH, OU	Good	Delete

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

Handling the Client Side Certificate

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



Token Exchange Configuration

PSP Certificates

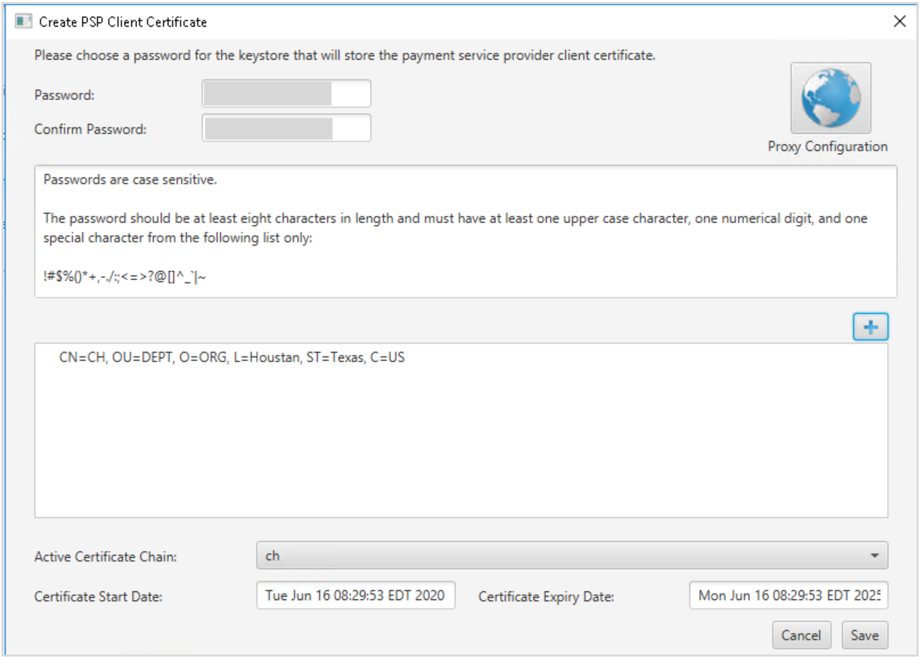
PSP Certificate	PSP Certificate Exists?	Status	
Server (Root) Certificate	□		
Client Certificate	□		

OPI Token Server Certificate

Certificate	Certificate Exists?	Status	
OPI Token Server 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 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.



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

Password:

Confirm Password:

Passwords are case sensitive.

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

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

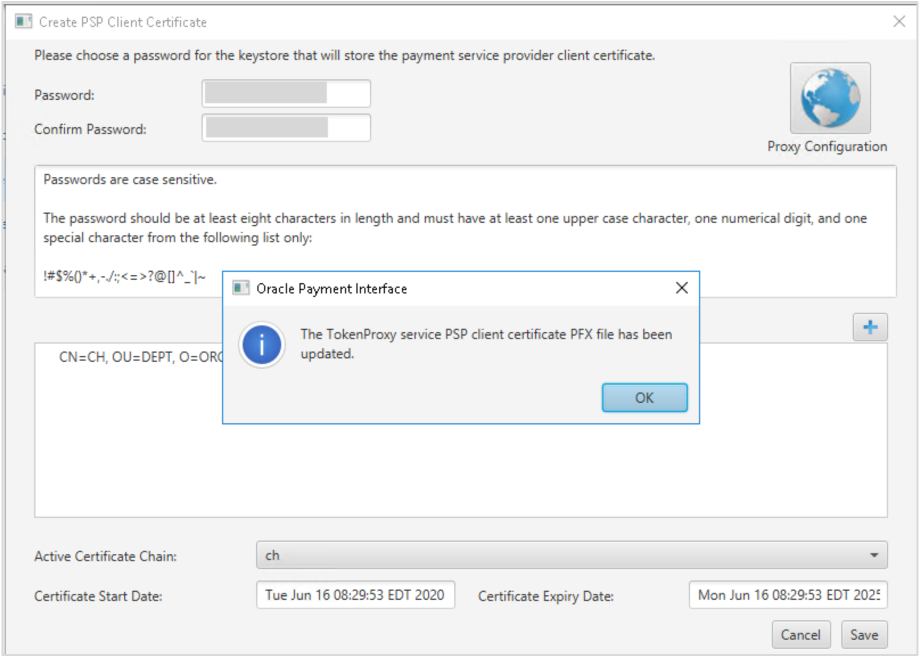
CN=CH, OU=DEPT, O=ORG, L=Houstan, ST=Texas, C=US

Active Certificate Chain: ch

Certificate Start Date: Tue Jun 16 08:29:53 EDT 2020

Certificate Expiry Date: Mon Jun 16 08:29:53 EDT 202

3. Click **Save**.



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

Password:

Confirm Password:

Passwords are case sensitive.

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

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

CN=CH, OU=DEPT, O=ORC

Oracle Payment Interface

The TokenProxy service PSP client certificate PFX file has been updated.

Active Certificate Chain: ch

Certificate Start Date: Tue Jun 16 08:29:53 EDT 2020

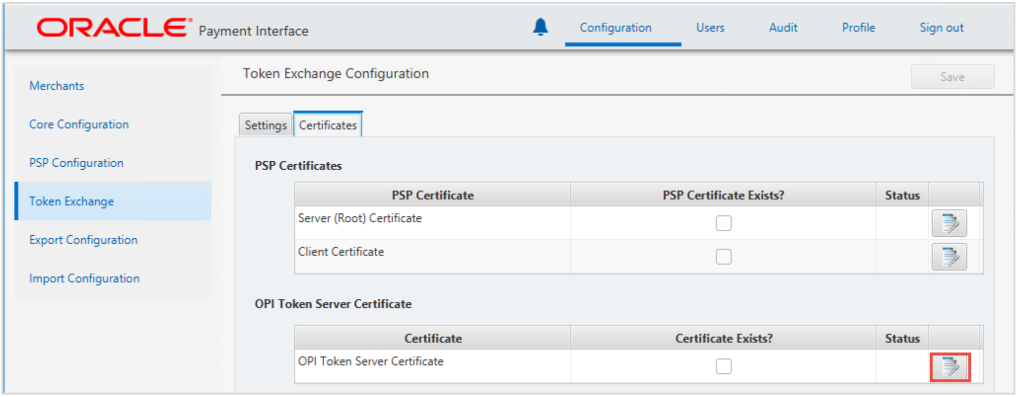
Certificate Expiry Date: Mon Jun 16 08:29:53 EDT 2025

OPI_PSP_1.pfx is created under **\OraclePaymentInterface\v20.4\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.



Token Exchange Configuration

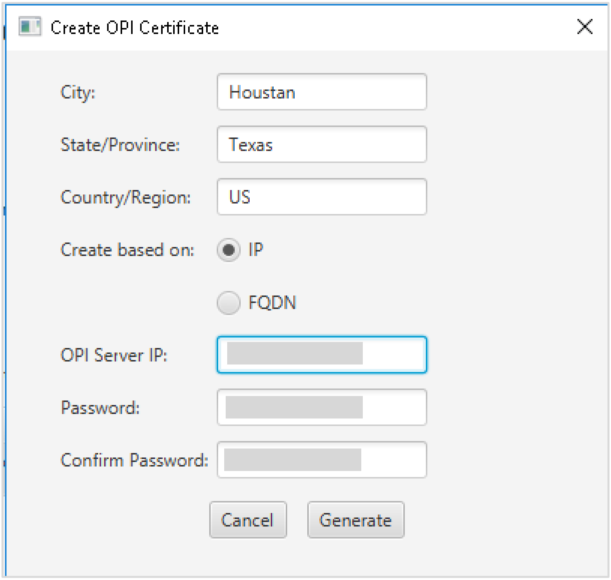
PSP Certificates

PSP Certificate	PSP Certificate Exists?	Status
Server (Root) Certificate	□	
Client Certificate	□	

OPI Token Server Certificate

Certificate	Certificate Exists?	Status
OPI Token Server Certificate	□	

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

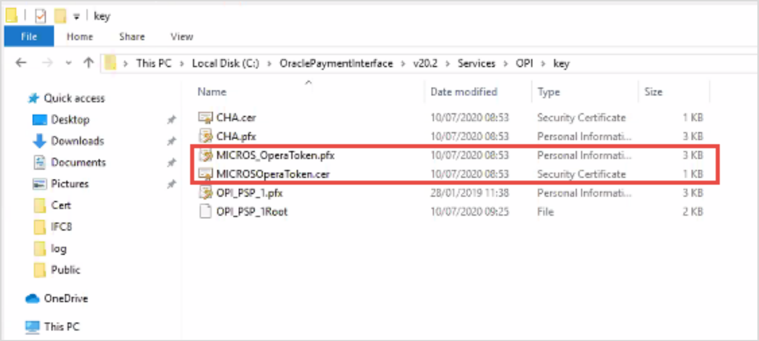


Create OPI Certificate

City:	Houstan
State/Province:	Texas
Country/Region:	US
Create based on:	● IP ○ FQDN
OPI Server IP:	[redacted]
Password:	[redacted]
Confirm Password:	[redacted]

3. Click **Generate** to continue.

   This process will generate the **MICROS_OPERAToken.pfx** and **MICROSOPERAToken.cer** files in the following folder: **\OraclePaymentInterface\v20.4\Services\OPI\key\**



Name	Date modified	Type	Size
CHA.cer	10/07/2020 08:53	Security Certificate	1 KB
CHA.pfx	10/07/2020 08:53	Personal Informati...	3 KB
MICROS_OperaToken.pfx	10/07/2020 08:53	Personal Informati...	3 KB
MICROSOperaToken.cer	10/07/2020 08:53	Security Certificate	1 KB
OPI_PSP_1.pfx	28/01/2019 11:38	Personal Informati...	3 KB
OPI_PSP_1Root	10/07/2020 09:25	File	2 KB

NOTE:

- OPI does not differentiate from OPERA PMS or Suite8 PMS. Therefore, the name of the certificate will always be MICROS_OperaToken.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 **MICROSOperaToken.cer** file to all the OPERA registered terminals that you want to run the Token Exchange process from and then Import to Trusted Root

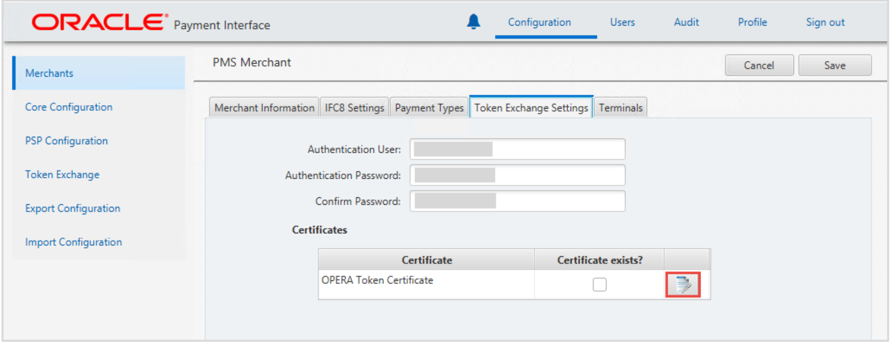
Certification Authorities, using **mmc.exe** (Refer to section Certificate Import using Microsoft Management Console for more details)

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

OPI - Client Side Certificates

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.



PMS Merchant

Authentication User:

Authentication Password:

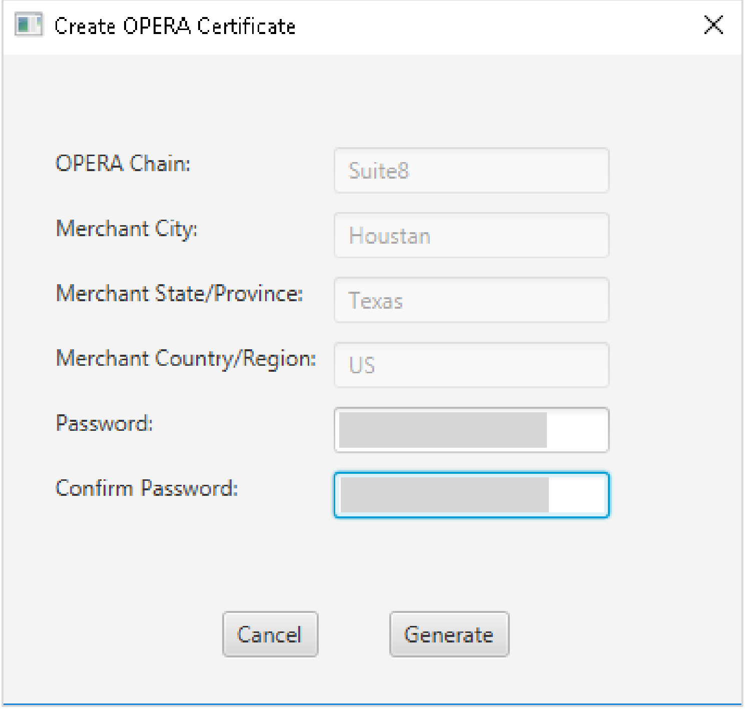
Confirm Password:

Certificates

Certificate	Certificate exists?	
OPERA Token Certificate	□	

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.

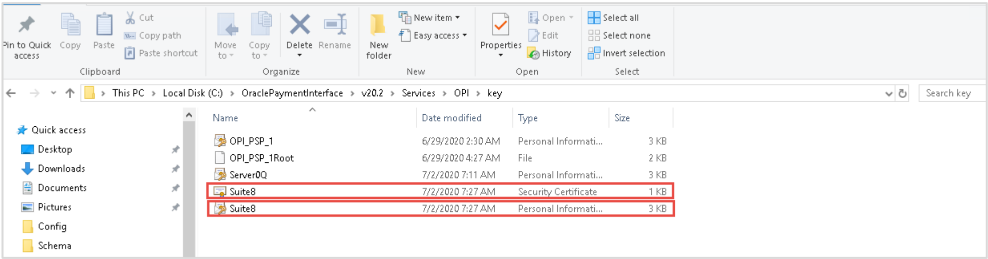


Create OPERA Certificate

OPERA Chain:	Suite8
Merchant City:	Houstan
Merchant State/Province:	Texas
Merchant Country/Region:	US
Password:	
Confirm Password:	

4. Click **Generate** to continue.

   This process will generate the **Suite8.pfx** and **Suite8.cer** files in the following folder: **\OraclePaymentInterface\v20.4\Services\OPI\key\**



Name	Date modified	Type	Size
OPI_PSP_1	6/29/2020 2:30 AM	Personal Informati...	3 KB
OPI_PSP_1Root	6/29/2020 4:27 AM	File	2 KB
Server0Q	7/2/2020 7:11 AM	Personal Informati...	3 KB
Suite8	7/2/2020 7:27 AM	Security Certificate	1 KB
Suite8	7/2/2020 7:27 AM	Personal Informati...	3 KB

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.

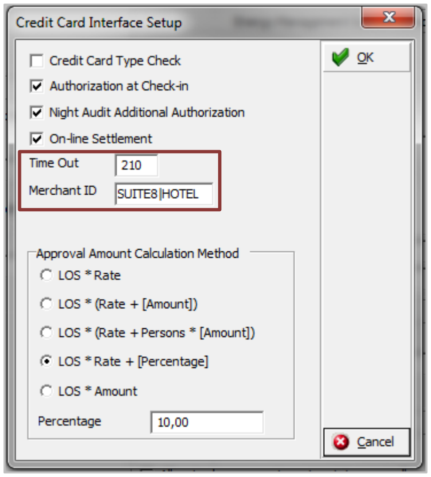
5. You must restart the OPI service for the update to take effect.

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.



Credit Card Interface Setup

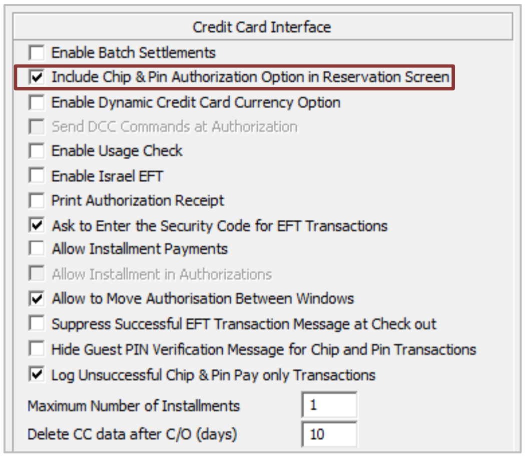
☐ Credit Card Type Check
☑ Authorization at Check-in
☑ Night Audit Additional Authorization
☑ On-line Settlement

Time Out 210
Merchant ID SUITE8|HOTEL

Approval Amount Calculation Method
○ LOS * Rate
○ LOS * (Rate + [Amount])
○ LOS * (Rate + Persons * [Amount])
● LOS * Rate + [Percentage]
○ LOS * Amount

Percentage 10,00

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.



Credit Card Interface

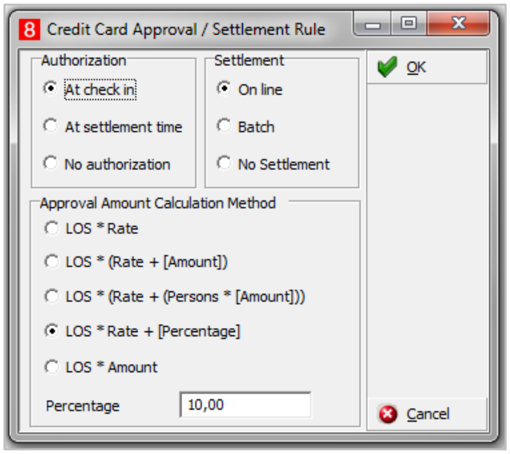
- ☐ Enable Batch Settlements
- ☑ Include Chip & Pin Authorization Option in Reservation Screen
- ☐ Enable Dynamic Credit Card Currency Option
- ☐ Send DCC Commands at Authorization
- ☐ Enable Usage Check
- ☐ Enable Israel EFT
- ☐ Print Authorization Receipt
- ☑ Ask to Enter the Security Code for EFT Transactions
- ☐ Allow Installment Payments
- ☐ Allow Installment in Authorizations
- ☑ Allow to Move Authorisation Between Windows
- ☐ Suppress Successful EFT Transaction Message at Check out
- ☐ Hide Guest PIN Verification Message for Chip and Pin Transactions
- ☑ Log Unsuccessful Chip & Pin Pay only Transactions

Maximum Number of Installments: 1
Delete CC data after C/O (days): 10

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.



Credit Card Approval / Settlement Rule

Authorization
- ● At check in
- ○ At settlement time
- ○ No authorization

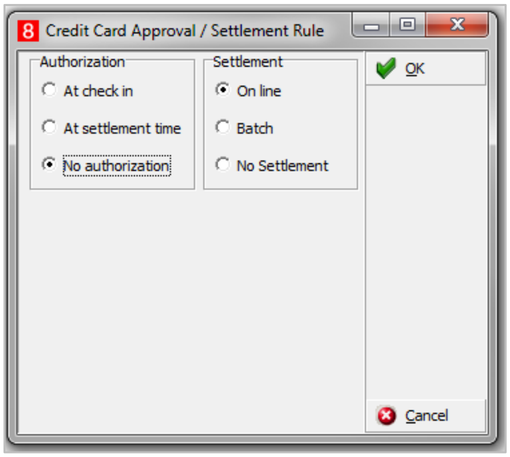
Settlement
- ● On line
- ○ Batch
- ○ No Settlement

Approval Amount Calculation Method
- ○ LOS * Rate
- ○ LOS * (Rate + [Amount])
- ○ LOS * (Rate + (Persons * [Amount]))
- ● LOS * Rate + [Percentage]
- ○ LOS * Amount

Percentage: 10,00

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.



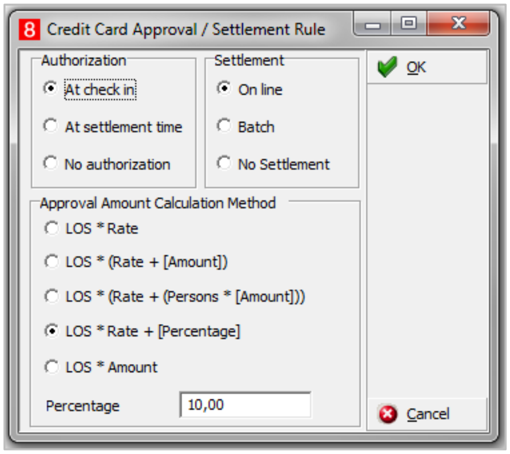
Credit Card Approval / Settlement Rule

Authorization
- ○ At check in
- ○ At settlement time
- ● No authorization

Settlement
- ● On line
- ○ Batch
- ○ No Settlement

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.



Credit Card Approval / Settlement Rule

Authorization
- ● At check in
- ○ At settlement time
- ○ No authorization

Settlement
- ● On line
- ○ Batch
- ○ No Settlement

Approval Amount Calculation Method
- ○ LOS * Rate
- ○ LOS * (Rate + [Amount])
- ○ LOS * (Rate + (Persons * [Amount]))
- ● LOS * Rate + [Percentage]
- ○ LOS * Amount

Percentage 10,00

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

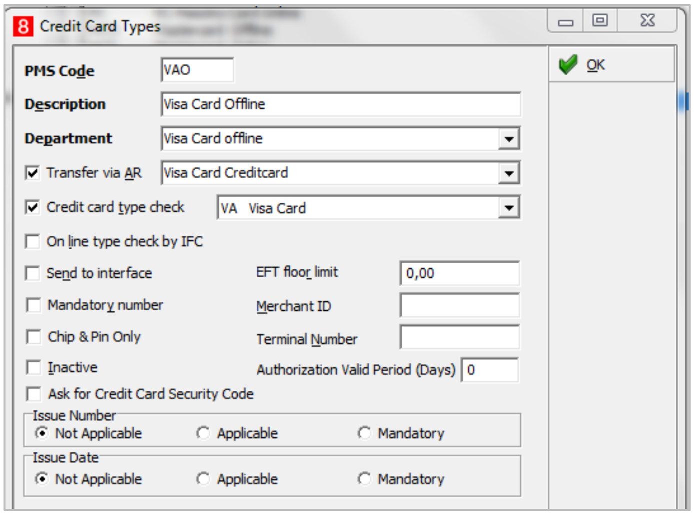
Payment Type Configuration

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.



Credit Card Types

✓ OK

PMS Code: VAO

Description: Visa Card Offline

Department: Visa Card offline

☑ Transfer via AR: Visa Card Creditcard

☑ Credit card type check: VA Visa Card

□ On line type check by IFC

□ Send to interface — EFT floor limit: 0,00

□ Mandatory number — Merchant ID:

□ Chip & Pin Only — Terminal Number:

□ Inactive — Authorization Valid Period (Days): 0

□ Ask for Credit Card Security Code

Issue Number: ● Not Applicable ○ Applicable ○ Mandatory

Issue Date: ● Not Applicable ○ Applicable ○ Mandatory

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.

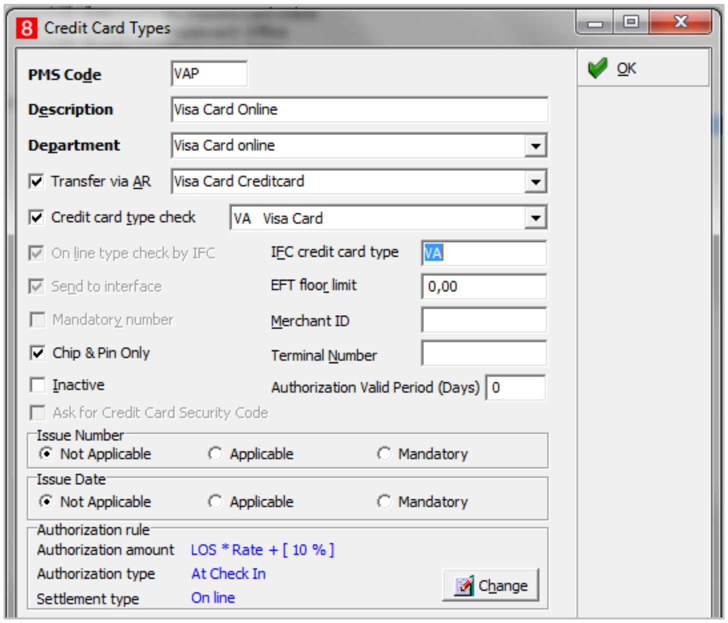
PMS Code = free definable 3-letter code

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



Credit Card Types

✓ OK

PMS Code: VAP

Description: Visa Card Online

Department: Visa Card online

☑ Transfer via AR: Visa Card Creditcard

☑ Credit card type check: VA Visa Card

☑ On line type check by IFC — IFC credit card type: VA

☑ Send to interface — EFT floor limit: 0,00

□ Mandatory number — Merchant ID:

☑ Chip & Pin Only — Terminal Number:

□ Inactive — Authorization Valid Period (Days): 0

□ Ask for Credit Card Security Code

Issue Number: ● Not Applicable ○ Applicable ○ Mandatory

Issue Date: ● Not Applicable ○ Applicable ○ Mandatory

Authorization rule

Authorization amount: LOS * Rate + [10 %]

Authorization type: At Check In

Settlement type: On line

Change

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.

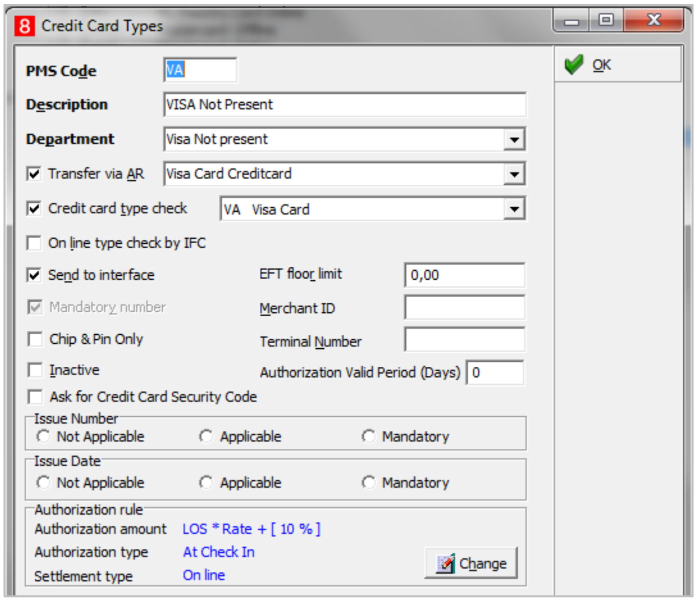
PMS Code = 2-letter code as setup in OPI (for example, VA for VISA)

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



PMS Code: VA
Description: VISA Not Present
Department: Visa Not present
☑ Transfer via AR: Visa Card Creditcard
☑ Credit card type check: VA Visa Card
☐ On line type check by IFC
☑ Send to interface — EFT floor limit: 0,00
☑ Mandatory number — Merchant ID:
☐ Chip & Pin Only — Terminal Number:
☐ Inactive — Authorization Valid Period (Days): 0
☐ Ask for Credit Card Security Code

Issue Number: ○ Not Applicable ○ Applicable ○ Mandatory

Issue Date: ○ Not Applicable ○ Applicable ○ Mandatory

Authorization rule
Authorization amount: LOS * Rate + [10 %]
Authorization type: At Check In
Settlement type: On line

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.

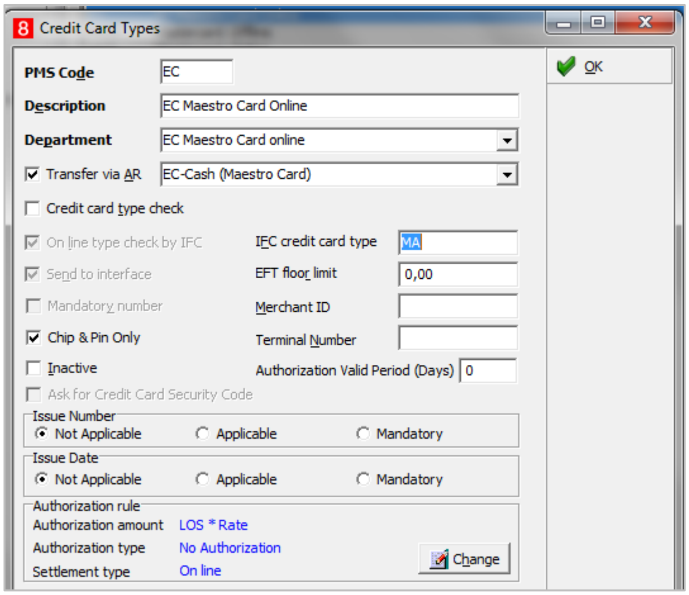
PMS Code = 2-letter code – freely definable

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



PMS Code: EC

Description: EC Maestro Card Online

Department: EC Maestro Card online

☑ Transfer via AR: EC-Cash (Maestro Card)

☐ Credit card type check

☑ On line type check by IFC — IFC credit card type: MA

☑ Send to interface — EFT floor limit: 0,00

☐ Mandatory number — Merchant ID:

☑ Chip & Pin Only — Terminal Number:

☐ Inactive — Authorization Valid Period (Days): 0

☐ Ask for Credit Card Security Code

Issue Number: ● Not Applicable ○ Applicable ○ Mandatory

Issue Date: ● Not Applicable ○ Applicable ○ Mandatory

Authorization rule
Authorization amount: LOS * Rate
Authorization type: No Authorization
Settlement type: On line

Tokenization Setup

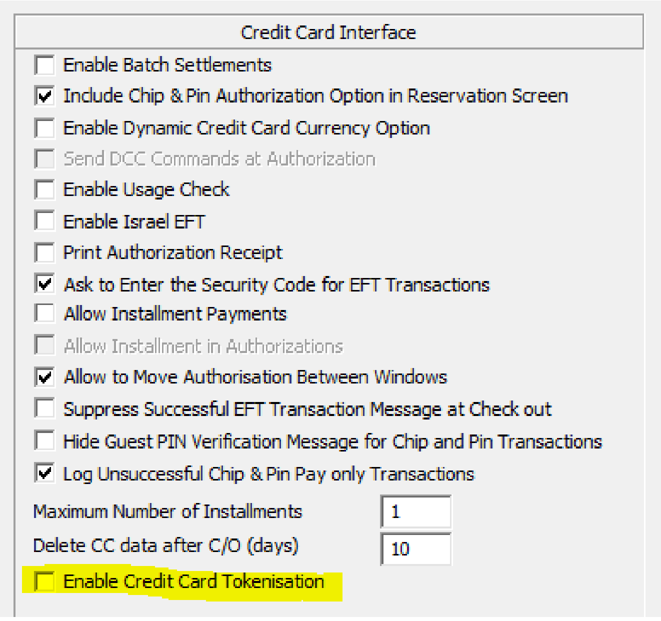
User Right to Enable the Tokenization Feature

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 Tokenization under Global Settings | Interface | 2 Interfaces (IFC8) | Credit Card Interface**.



Credit Card Interface

☐ Enable Batch Settlements

☑ Include Chip & Pin Authorization Option in Reservation Screen

☐ Enable Dynamic Credit Card Currency Option

☐ Send DCC Commands at Authorization

☐ Enable Usage Check

☐ Enable Israel EFT

☐ Print Authorization Receipt

☑ Ask to Enter the Security Code for EFT Transactions

☐ Allow Installment Payments

☐ Allow Installment in Authorizations

☑ Allow to Move Authorisation Between Windows

☐ Suppress Successful EFT Transaction Message at Check out

☐ Hide Guest PIN Verification Message for Chip and Pin Transactions

☑ Log Unsuccessful Chip & Pin Pay only Transactions

Maximum Number of Installments: 1

Delete CC data after C/O (days): 10

☐ Enable Credit Card Tokenisation

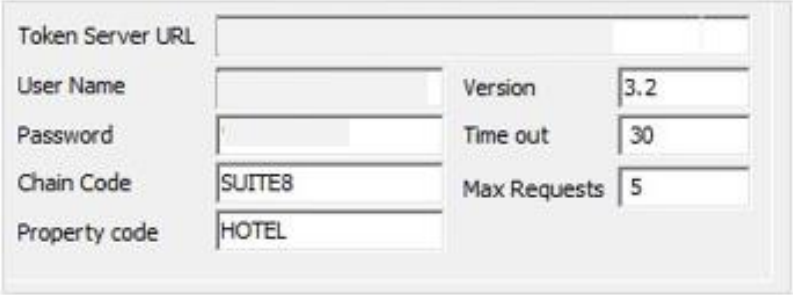
2. As soon as you have activated the setting additional fields will populate.

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	https://*IP Address of PC OPI is installed on*:5012 /TokenOPERA	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:

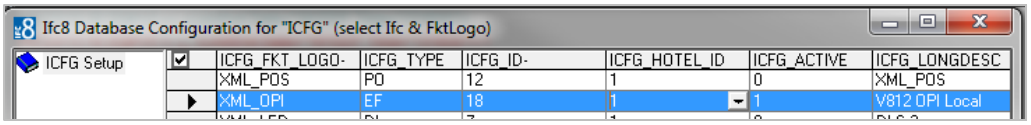


Token Server URL			
User Name		Version	3.2
Password		Time out	30
Chain Code	SUITE8	Max Requests	5
Property code	HOTEL		

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

To configure the link between the interfaces:

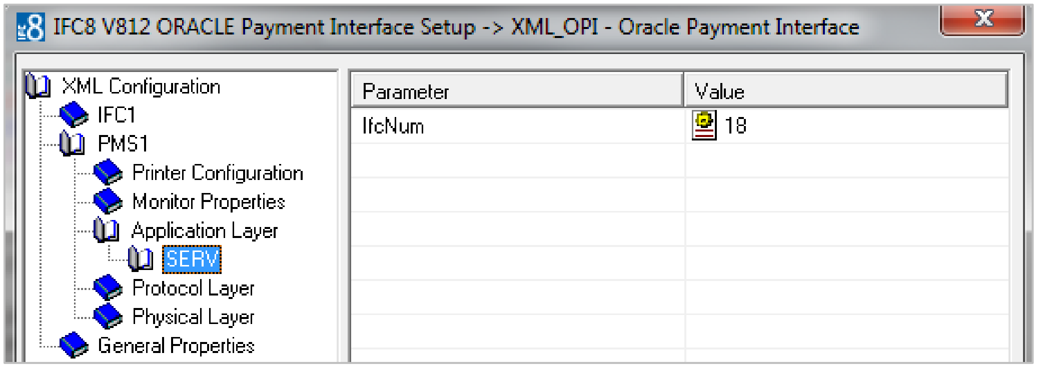
1. In the **Hotel Property Interface**, go to the **PMS1** tree and select **SERV** in the application layer.
2. Enter the **Suite8 IFC** number in the parameter **IfcNum** value. You can find the Suite8 IFC number in the IFC8 Database Configuration (ICFG_ID).



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

ICFG Setup

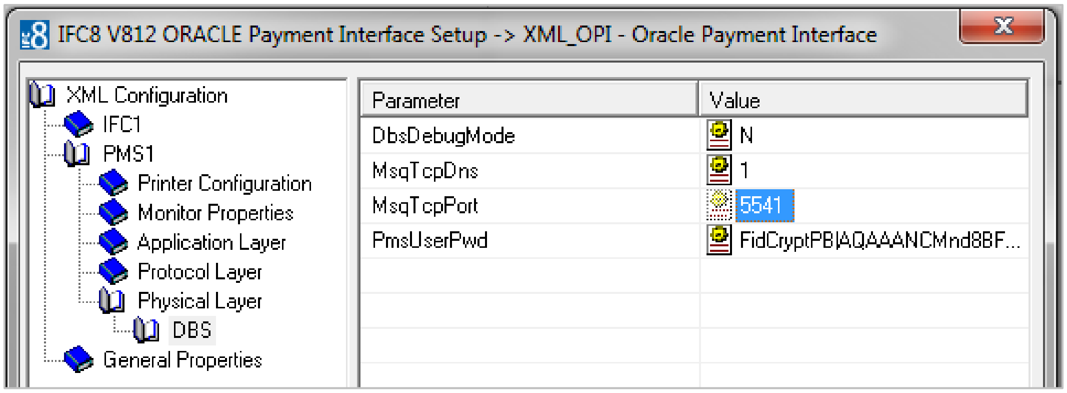
☑	ICFG_FKT_LOGO-	ICFG_TYPE	ICFG_ID-	ICFG_HOTEL_ID	ICFG_ACTIVE	ICFG_LONGDESC
	XML_POS	PO	12	1	0	XML_POS
▶	XML_OPI	EF	18	1	1	V812 OPI Local



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

Parameter	Value
IfcNum	18

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**.

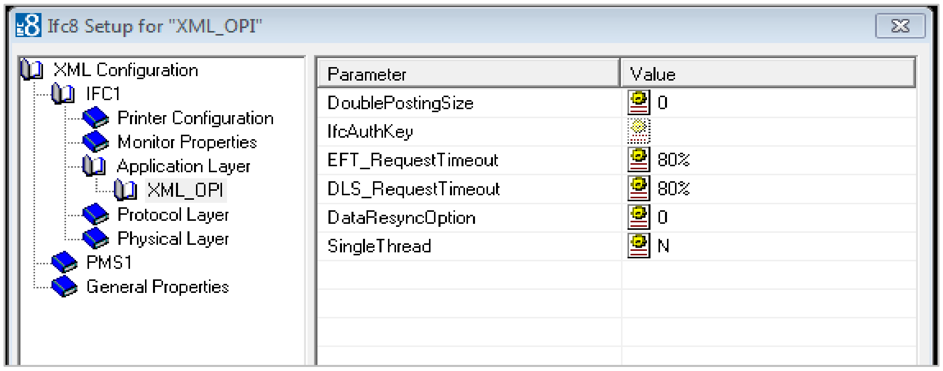


Parameter	Value
DbsDebugMode	N
MsqTcpDns	1
MsqTcpPort	5541
PmsUserPwd	FidCryptPB|AQAAANCMnd8BF...

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.

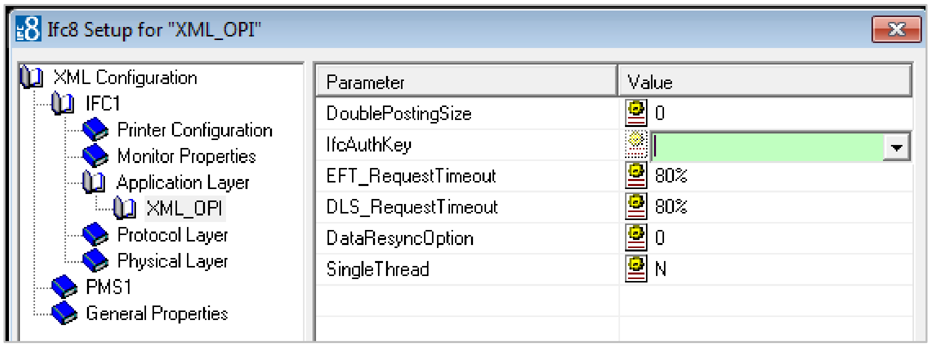


Parameter	Value
DoublePostingSize	0
IfcAuthKey	
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0
SingleThread	N

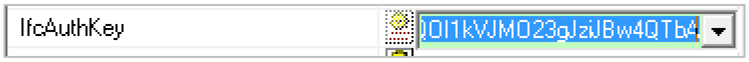
2. Copy the generated key from Configuring OPI - OPERA merchant step 3, and add “FidCrypt0S|” to the generated key as prefix.

   For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxx

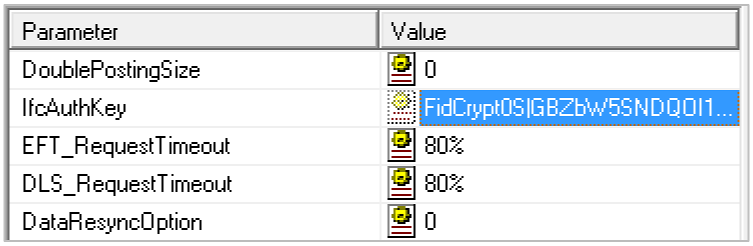
3. Copy this string into IFC8 Parameter **IfcAuthKey** value field.



Parameter	Value
DoublePostingSize	0
IfcAuthKey	
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0
SingleThread	N



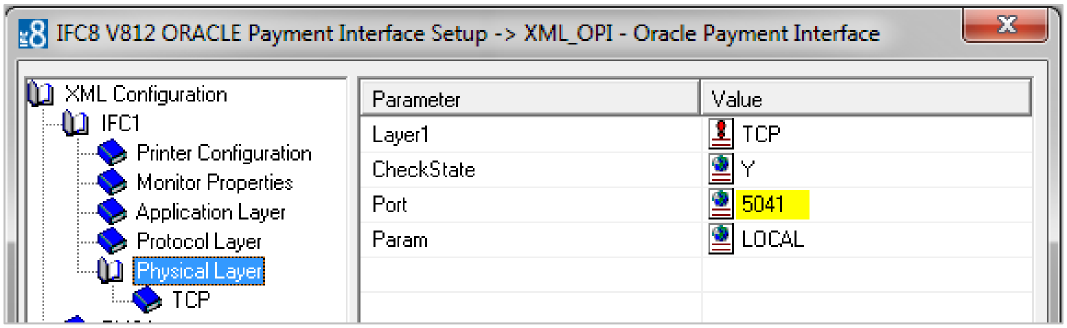
IfcAuthKey	0I1kVJMO23gJziJBw4QTb4



Parameter	Value
DoublePostingSize	0
IfcAuthKey	FidCrypt0S|GBZbW5SNDQ0I1...
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0

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

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



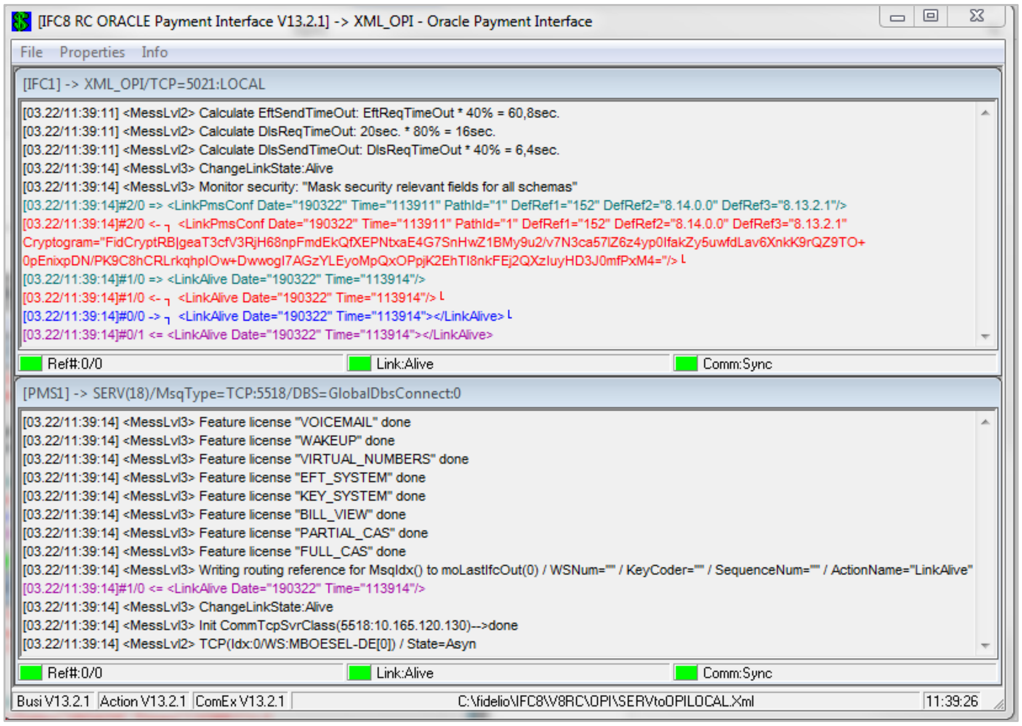
Parameter	Value
Layer1	TCP
CheckState	Y
Port	5041
Param	LOCAL

6. Click **Apply**, IFC8 reinitiates.

7. The **IfcAuthKey** value now shows an encrypted key and the entered string is now encrypted by IFC8.

8. Click **Save**, and then click **OK** to close the IFC8 Configuration form.

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

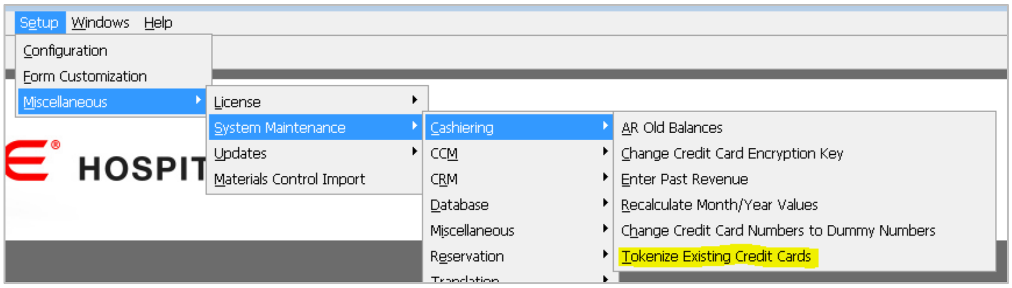

[IFC8 RC ORACLE Payment Interface V13.2.1] -> XML_OPI - Oracle Payment Interface
File Properties Info
[IFC1] -> XML_OPI/TCP=5021:LOCAL

```
[03.22/11:39:11] <MessLvl2> Calculate EftSendTimeOut: EftReqTimeOut * 40% = 60,8sec.
[03.22/11:39:11] <MessLvl2> Calculate DlsReqTimeOut: 20sec. * 80% = 16sec.
[03.22/11:39:11] <MessLvl2> Calculate DlsSendTimeOut: DlsReqTimeOut * 40% = 6,4sec.
[03.22/11:39:14] <MessLvl3> ChangeLinkState:Alive
[03.22/11:39:14] <MessLvl3> Monitor security: "Mask security relevant fields for all schemas"
[03.22/11:39:14]#2/0 => <LinkPmsConf Date="190322" Time="113911" PathId="1" DefRef1="152" DefRef2="8.14.0.0" DefRef3="8.13.2.1"/>
[03.22/11:39:14]#2/0 <- ┐ <LinkPmsConf Date="190322" Time="113911" PathId="1" DefRef1="152" DefRef2="8.14.0.0" DefRef3="8.13.2.1"
Cryptogram="FidCryptRB|geaT3cfV3RjH68npFmdEkQfXEPNtxaE4G7SnHwZ1BMy9u2/v7N3ca57lZ6z4yp0IfakZy5uwfdLav6XnkK9rQZ9TO+
0pEnixpDN/PK9C8hCRLrkqhplOw+DwwogI7AGzYLEyoMpQxOPpjK2EhTI8nkFEj2QXzluyHD3J0mfPxM4="/> └
[03.22/11:39:14]#1/0 => <LinkAlive Date="190322" Time="113914"/>
[03.22/11:39:14]#1/0 <- ┐ <LinkAlive Date="190322" Time="113914"/> └
[03.22/11:39:14]#0/0 -> ┐ <LinkAlive Date="190322" Time="113914"></LinkAlive> └
[03.22/11:39:14]#0/1 <= <LinkAlive Date="190322" Time="113914"></LinkAlive>
```

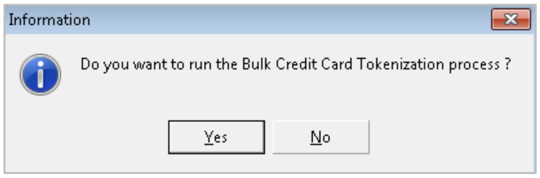
```
[03.22/11:39:14] <MessLvl3> Feature license "VOICEMAIL" done
[03.22/11:39:14] <MessLvl3> Feature license "WAKEUP" done
[03.22/11:39:14] <MessLvl3> Feature license "VIRTUAL_NUMBERS" done
[03.22/11:39:14] <MessLvl3> Feature license "EFT_SYSTEM" done
[03.22/11:39:14] <MessLvl3> Feature license "KEY_SYSTEM" done
[03.22/11:39:14] <MessLvl3> Feature license "BILL_VIEW" done
[03.22/11:39:14] <MessLvl3> Feature license "PARTIAL_CAS" done
[03.22/11:39:14] <MessLvl3> Feature license "FULL_CAS" done
[03.22/11:39:14] <MessLvl3> Writing routing reference for MsqIdx() to moLastIfcOut(0) / WSNum="" / KeyCoder="" / SequenceNum="" / ActionName="LinkAlive"
[03.22/11:39:14]#1/0 <= <LinkAlive Date="190322" Time="113914"/>
[03.22/11:39:14] <MessLvl3> ChangeLinkState:Alive
[03.22/11:39:14] <MessLvl3> Init CommTcpSvrClass(5518:10.165.120.130)-->done
[03.22/11:39:14] <MessLvl2> TCP(Idx:0/WS:MBOESEL-DE[0]) / State=Asyn
```

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.



Do you want to run the Bulk Credit Card Tokenization process ?

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.

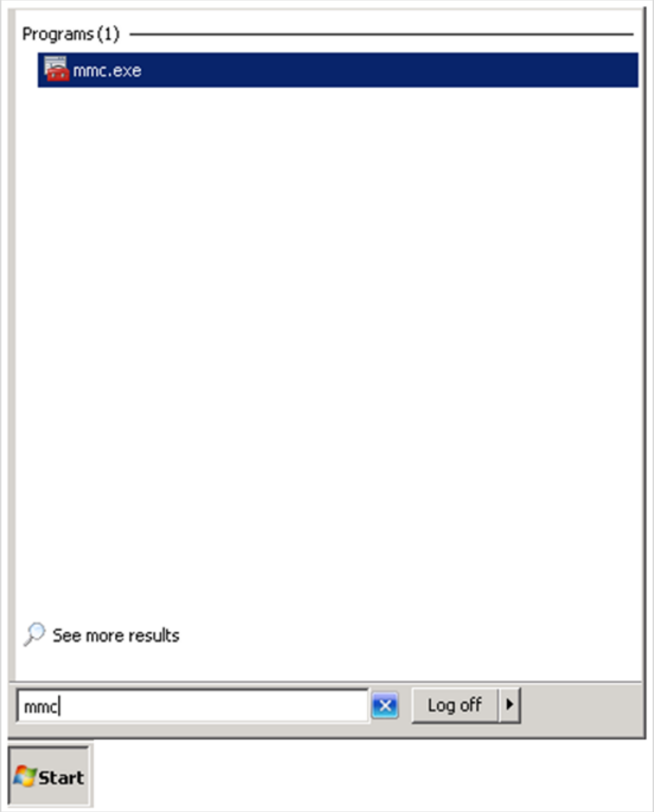
> **NOTE:**
>
> After the successful replacement of credit card numbers with token ID’s the process should NOT be executed again.

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.

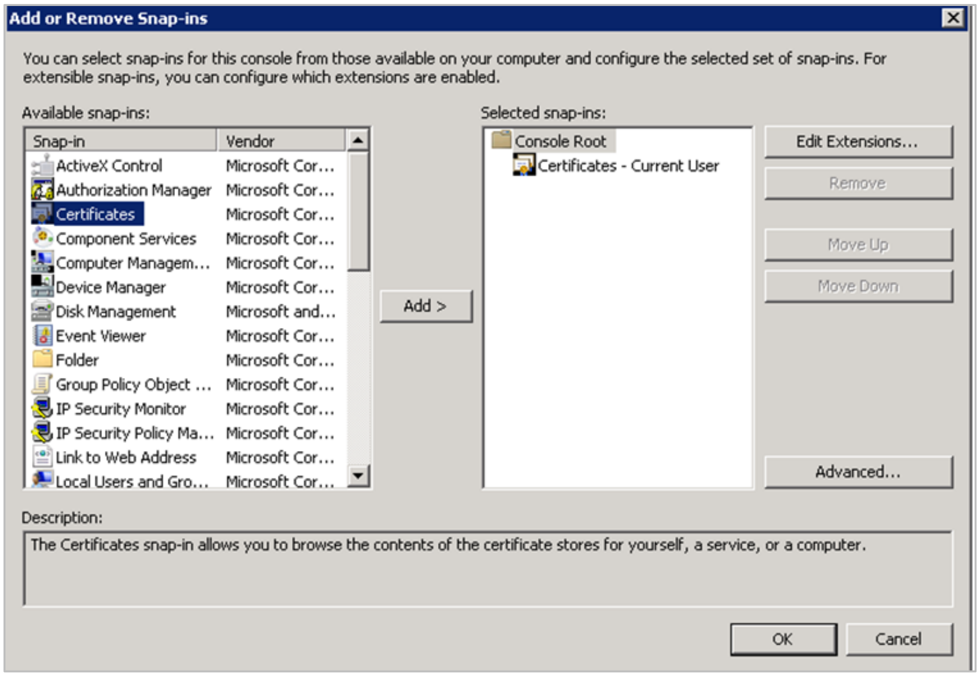
   OPI only supports the **Convert CC** function; the other conversion options are not currently supported.

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**.

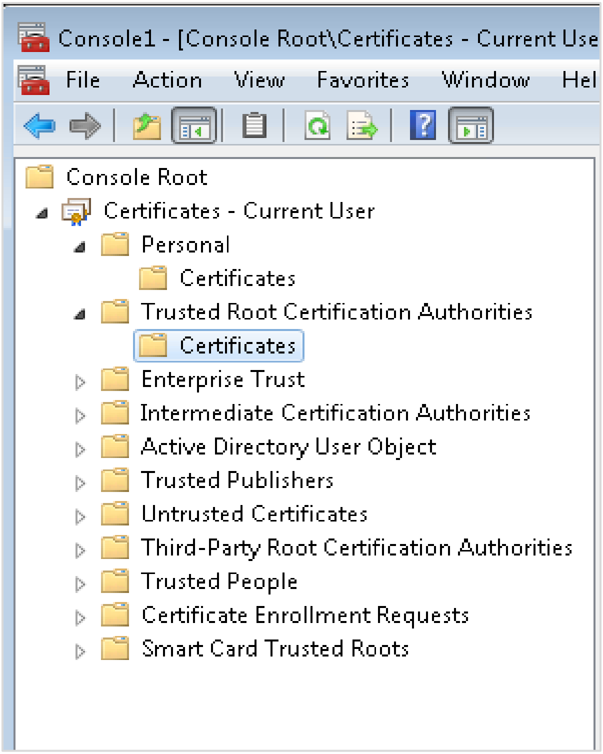


You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

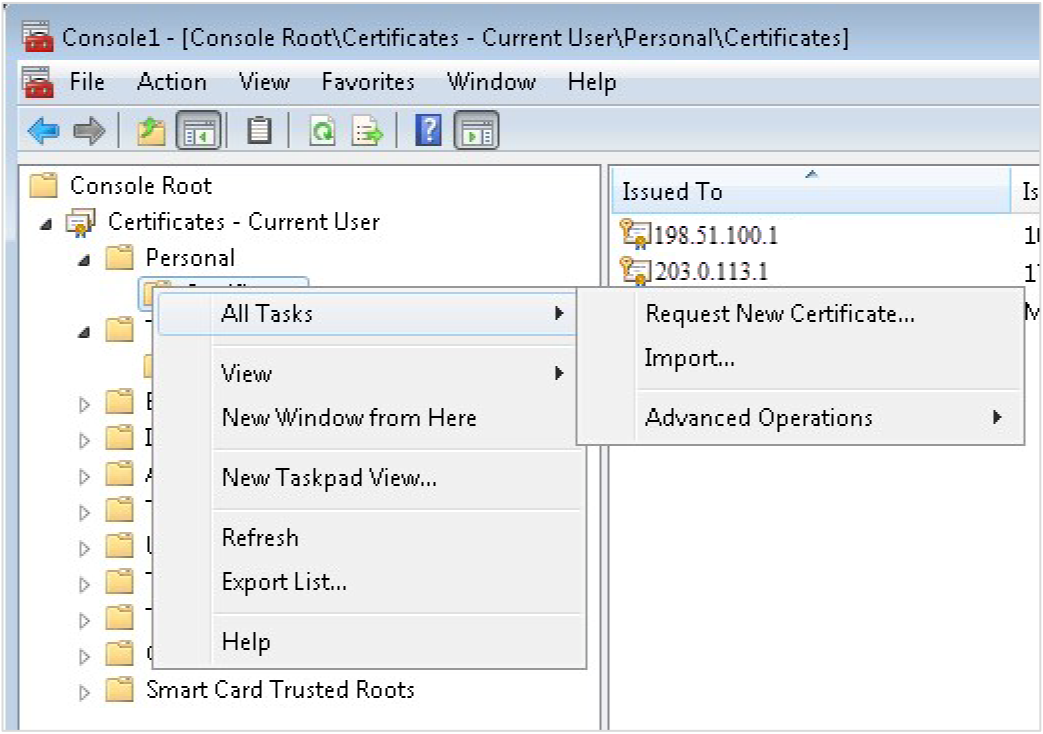
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

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


Console1 - [Console Root\Certificates - Current Use
File
Action
View
Favorites
Window
Hel
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots

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

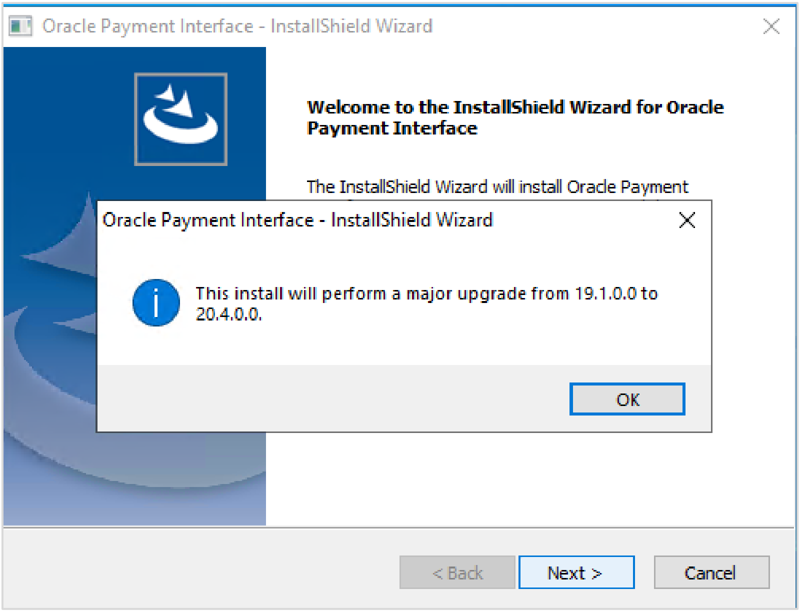
Upgrading the OPI

VERY IMPORTANT: Read and follow the upgrade directions.

> **NOTE:**
>
> - OPI upgrade functionality supports:
>   - Upgrading OPI 19.1 (include patch releases) to OPI 20.4
>   - Upgrading OPI 20.1 (include patch releases) to OPI 20.4
>   - Upgrading OPI 20.2 (include patch releases) to OPI 20.4
>   - Upgrading OPI 20.3 (include patch releases) to OPI 20.4

Upgrading OPI 19.1.0.0 to 20.4.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.4.0.0.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**.

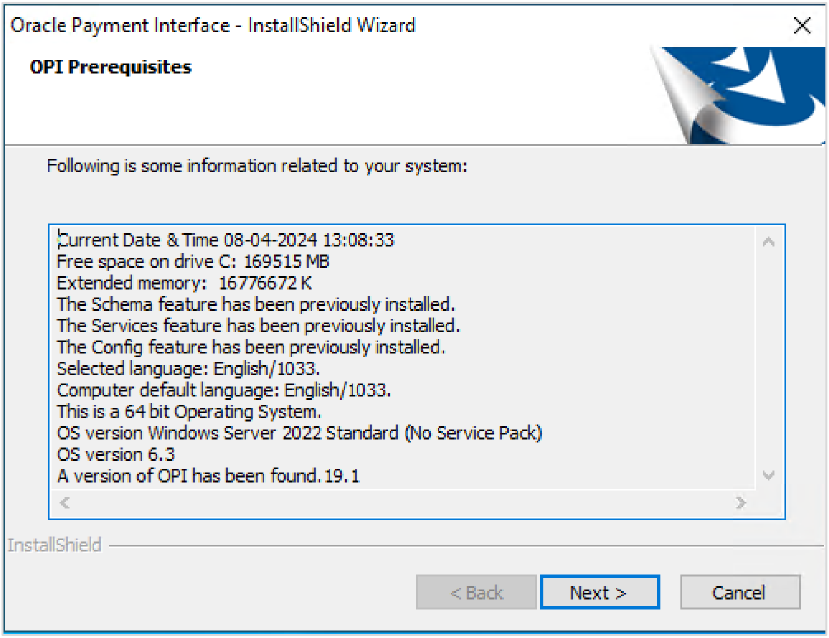

Oracle Payment Interface - InstallShield Wizard
Welcome to the InstallShield Wizard for Oracle Payment Interface
The InstallShield Wizard will install Oracle Payment
< Back
Next >
Cancel

Oracle Payment Interface - InstallShield Wizard

This install will perform a major upgrade from 19.1.0.0 to 20.4.0.0.

5. Click **Next**.

   Ensure all the prerequisites for the OPI installation are met.



OPI Prerequisites

Following is some information related to your system:

```
Current Date & Time 08-04-2024 13:08:33
Free space on drive C: 169515 MB
Extended memory:  16776672 K
The Schema feature has been previously installed.
The Services feature has been previously installed.
The Config feature has been previously installed.
Selected language: English/1033.
Computer default language: English/1033.
This is a 64 bit Operating System.
OS version Windows Server 2022 Standard (No Service Pack)
OS version 6.3
A version of OPI has been found. 19.1
```

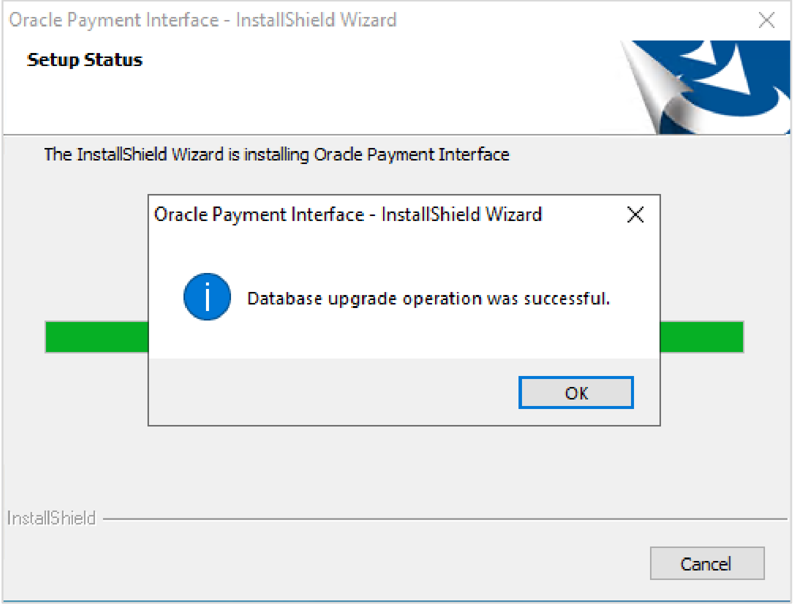
6. Choose a Destination Location. Accept the default installation location or click **Change**… to choose a different location.

7. Click **Next**.

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

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

9. Click **OK**.



Oracle Payment Interface - InstallShield Wizard

Setup Status

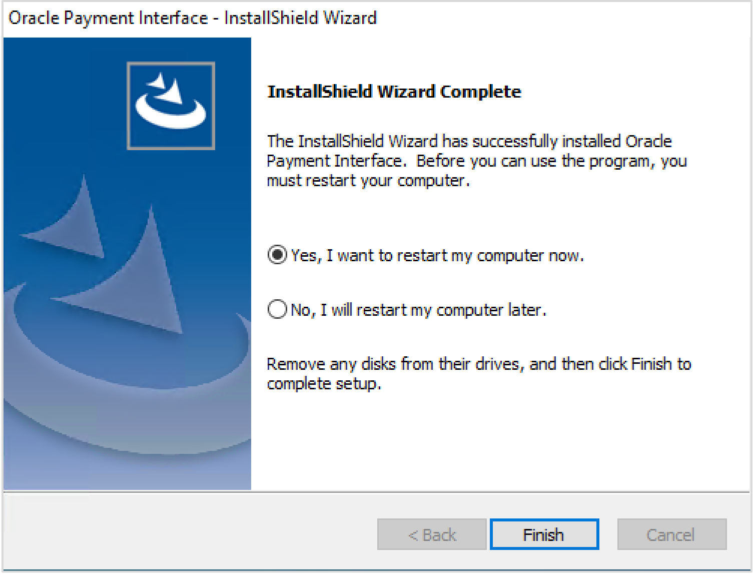
The InstallShield Wizard is installing Oracle Payment Interface

Oracle Payment Interface - InstallShield Wizard

Database upgrade operation was successful.

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.



Oracle Payment Interface - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Oracle Payment Interface. Before you can use the program, you must restart your computer.

● Yes, I want to restart my computer now.

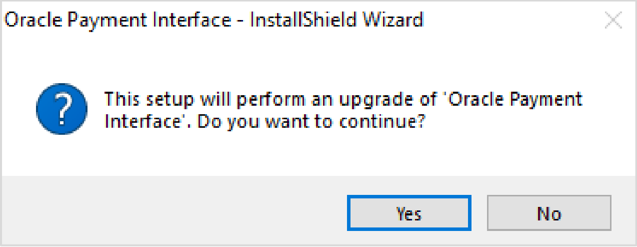
○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

12. Click **Finish**.

Upgrading OPI 20.1.0.0 to 20.4.0.0

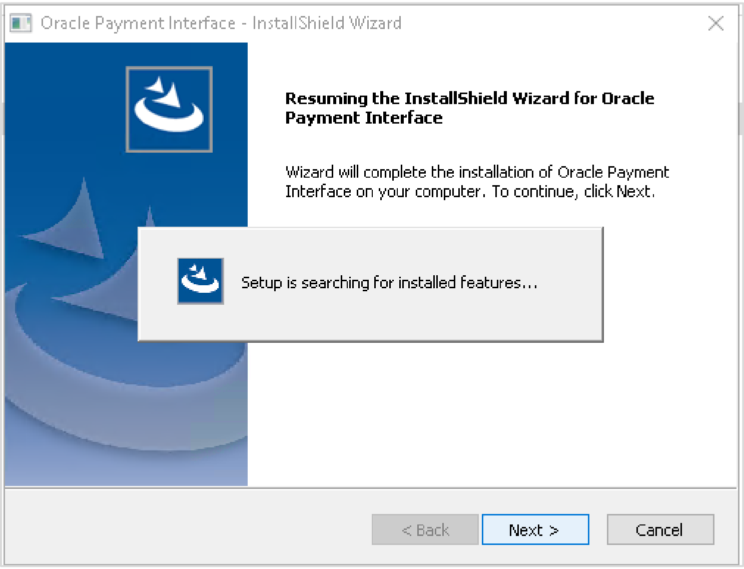
1. Right-click **OraclePaymentInterfaceInstaller_20.4.0.0.exe** file and select **Run as Administrator** to perform an upgrade.



Oracle Payment Interface - InstallShield Wizard

This setup will perform an upgrade of 'Oracle Payment Interface'. Do you want to continue?

2. Click **Yes**.



Oracle Payment Interface - InstallShield Wizard

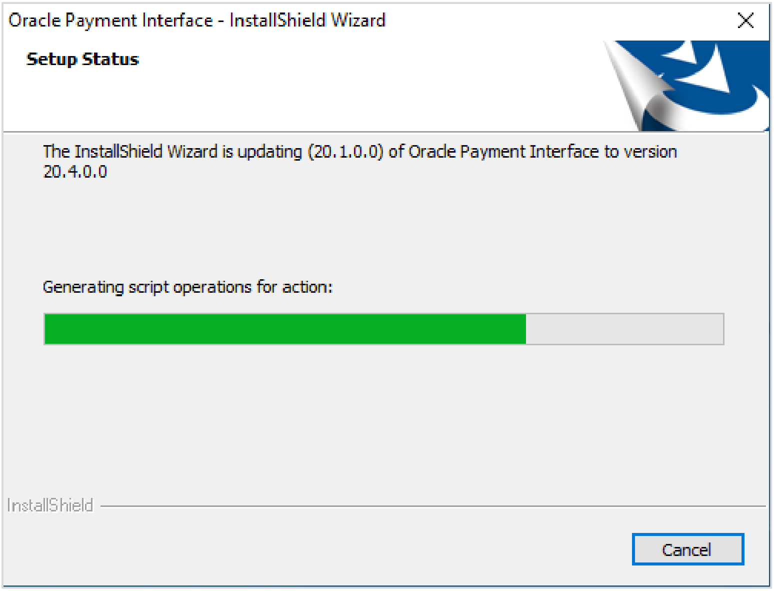
Resuming the InstallShield Wizard for Oracle Payment Interface

Wizard will complete the installation of Oracle Payment Interface on your computer. To continue, click Next.

Setup is searching for installed features...

3. Click **Next**.

   Setup is searching for installed features.



Oracle Payment Interface - InstallShield Wizard

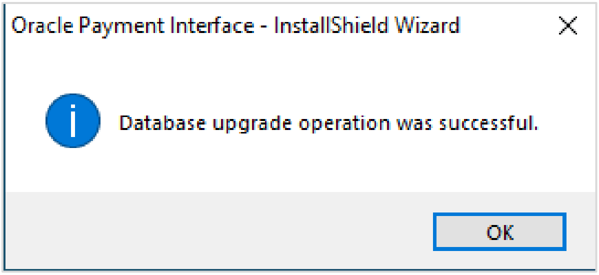
Setup Status

The InstallShield Wizard is updating (20.1.0.0) of Oracle Payment Interface to version 20.4.0.0

Generating script operations for action:

4. Click **Next**.

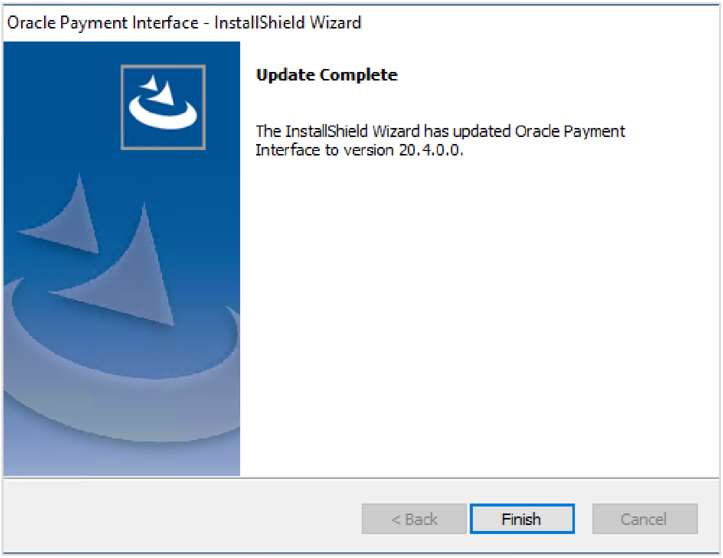
   The Install wizard is updating from **OPI 20.1** to version **20.4**.



Oracle Payment Interface - InstallShield Wizard

Database upgrade operation was successful.

5. Click **OK**.



Oracle Payment Interface - InstallShield Wizard

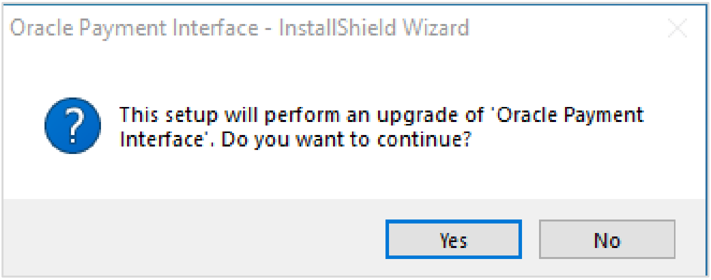
Update Complete

The InstallShield Wizard has updated Oracle Payment Interface to version 20.4.0.0.

6. Click **Finish**.

Upgrading OPI 20.2.0.0 to 20.4.0.0

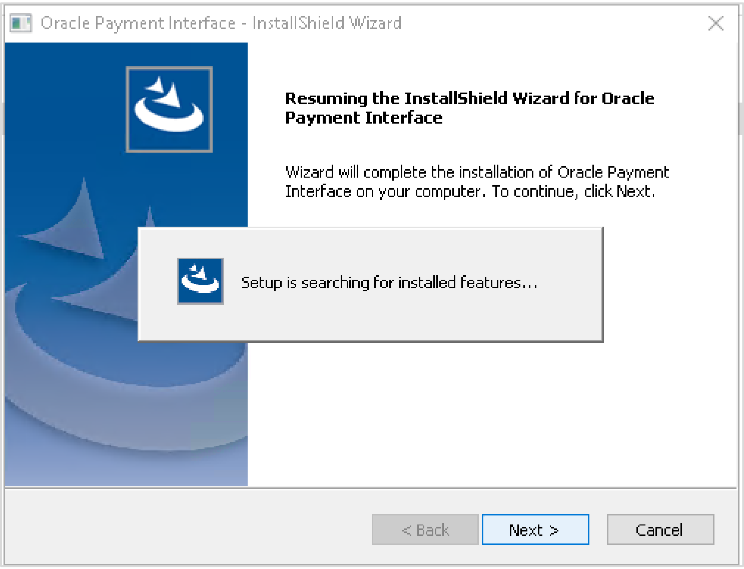
1. Right-click **OraclePaymentInterfaceInstaller_20.4.0.0.exe** file and select **Run as Administrator** to perform an upgrade.



Oracle Payment Interface - InstallShield Wizard

This setup will perform an upgrade of 'Oracle Payment Interface'. Do you want to continue?

2. Click **Yes**.



Oracle Payment Interface - InstallShield Wizard

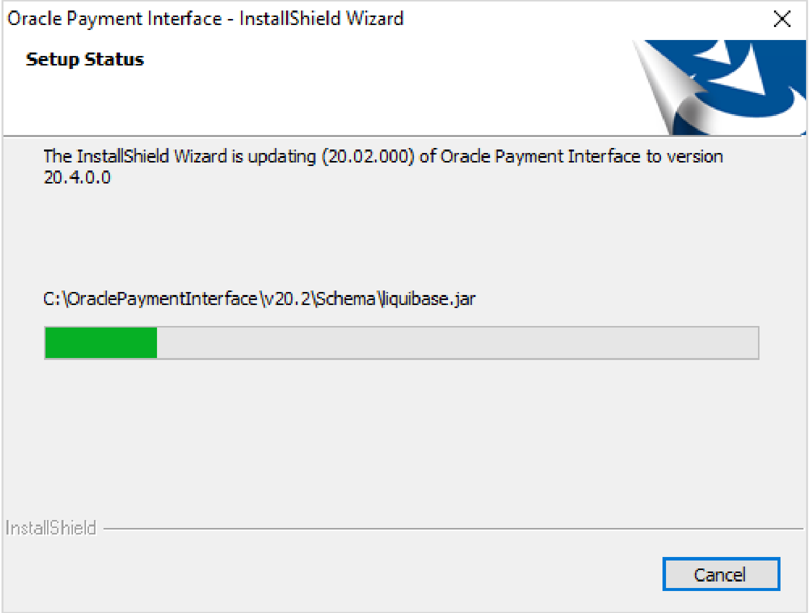
Resuming the InstallShield Wizard for Oracle Payment Interface

Wizard will complete the installation of Oracle Payment Interface on your computer. To continue, click Next.

Setup is searching for installed features...

3. Click **Next**.

   Setup is searching for installed features.



Oracle Payment Interface - InstallShield Wizard

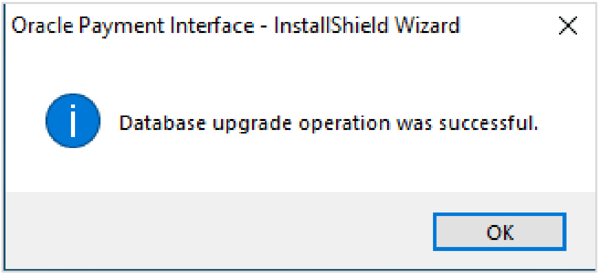
Setup Status

The InstallShield Wizard is updating (20.02.000) of Oracle Payment Interface to version 20.4.0.0

C:\OraclePaymentInterface\v20.2\Schema\liquibase.jar

4. Click **Next**.

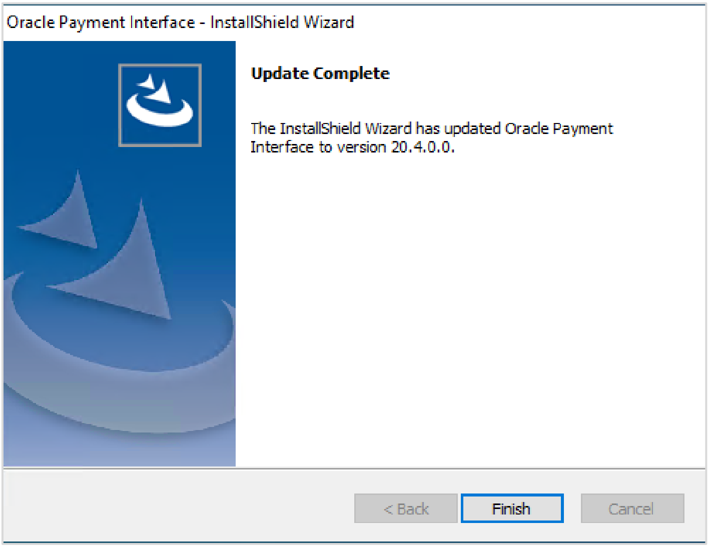
   The Install wizard is updating from **OPI 20.2** to version **20.4**.



Oracle Payment Interface - InstallShield Wizard

Database upgrade operation was successful.

5. Click **OK**.



Oracle Payment Interface - InstallShield Wizard

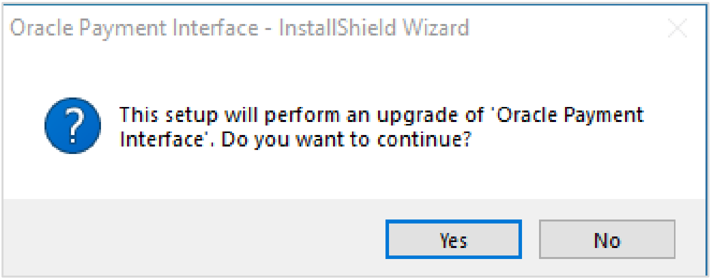
Update Complete

The InstallShield Wizard has updated Oracle Payment Interface to version 20.4.0.0.

6. Click **Finish**.

Upgrading OPI 20.3.0.0 to 20.4.0.0

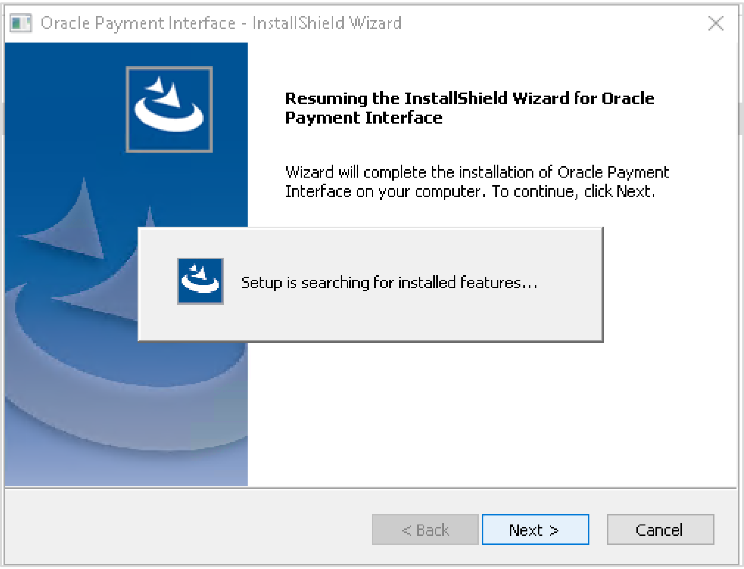
1. Right-click **OraclePaymentInterfaceInstaller_20.4.0.0.exe** file and select **Run as Administrator** to perform an upgrade.



Oracle Payment Interface - InstallShield Wizard

This setup will perform an upgrade of 'Oracle Payment Interface'. Do you want to continue?

2. Click **Yes**.



Oracle Payment Interface - InstallShield Wizard

Resuming the InstallShield Wizard for Oracle Payment Interface

Wizard will complete the installation of Oracle Payment Interface on your computer. To continue, click Next.

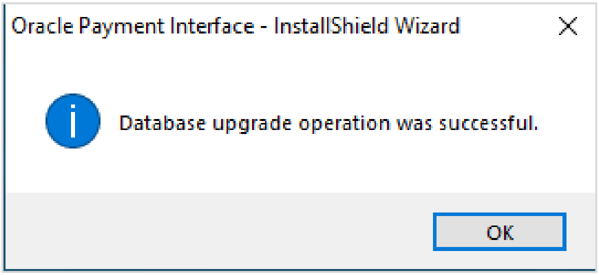
Setup is searching for installed features...

3. Click **Next**.

   Setup is searching for installed features.

4. Click **Next**.

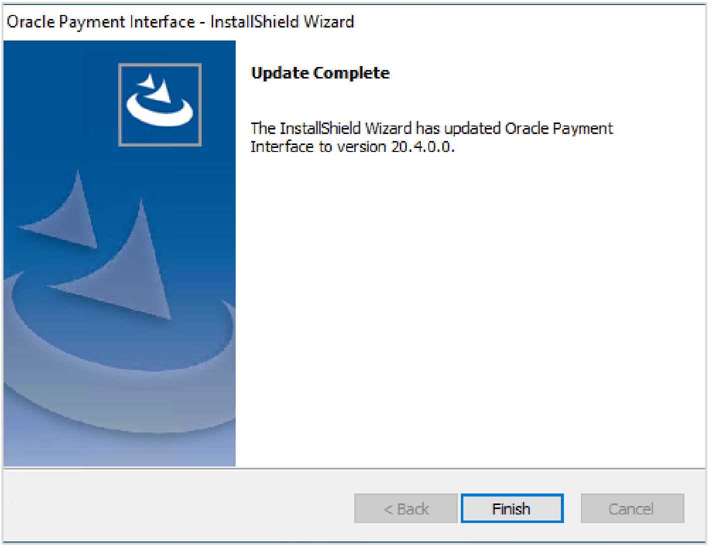
   The Install wizard is updating from **OPI 20.3** to version **20.4**.



Oracle Payment Interface - InstallShield Wizard

Database upgrade operation was successful.

5. Click **OK**.



Oracle Payment Interface - InstallShield Wizard

Update Complete

The InstallShield Wizard has updated Oracle Payment Interface to version 20.4.0.0.

6. Click **Finish**.