Oracle® Hospitality Payment Interface

OPERA V5 OPI Installation and Reference Guide

Release 20.1
F26820-01
July 2020

Oracle Hospitality Payment Interface OPERA V5 OPI Installation and Reference Guide Release 20.1

F26820-01

Contents

Preface

Purpose

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

Audience

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

Customer Support

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

https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Documentation

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

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

Table 1 Revision History

Date	Description
April 2020	• Initial publication.
July 2020	• Revised content across the entire document.

1 Pre-Installation Steps

IF UPGRADING OPI, YOU MUST READ THE UPGRADING THE OPI SECTION FIRST.

- Minimum OPERA Property Management Systems (for V5 Hosted) releases you can integrate with OPI:
  - OPERA V5 Hosted 5.5.25 or higher
  - OPERA V5.6.4 or higher
- OPI 20.1 does not install a database. If doing a clean install of OPI, a database must be installed first.
- You cannot upgrade directly from OPI 6.1 to OPI 20.1. Upgrading from OPI 6.2 and OPI 19.1 (including patch releases) to OPI 20.1 is supported.
- 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.

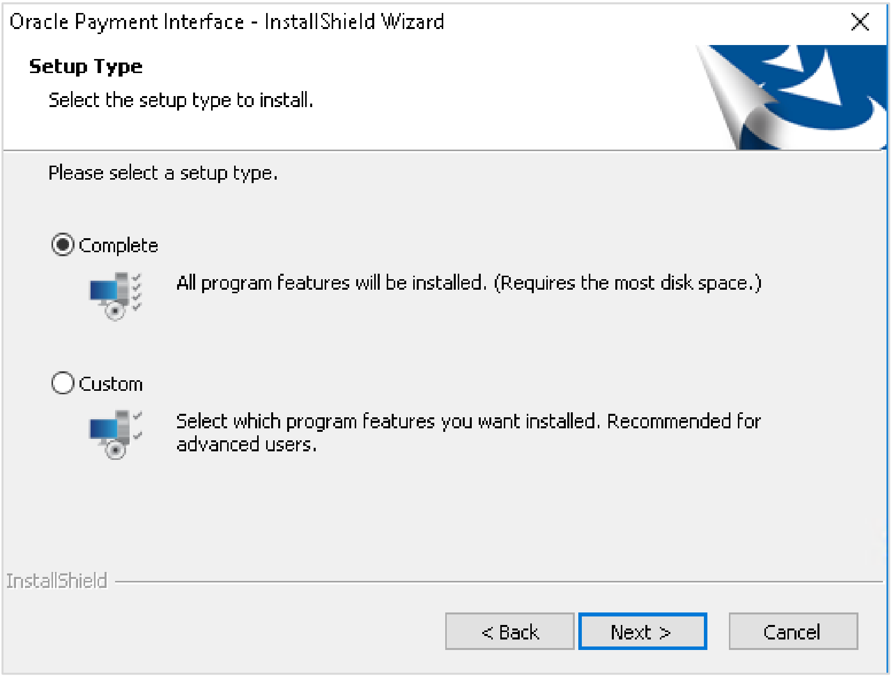
> **NOTE:**
>
> Stay current by upgrading your Java version as Oracle CPUs/Alerts are announced.

During the installation you must confirm the following:

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

2 Installing the OPI

1. Right-click **OraclePaymentInterfaceInstaller_20.1.0.0.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.

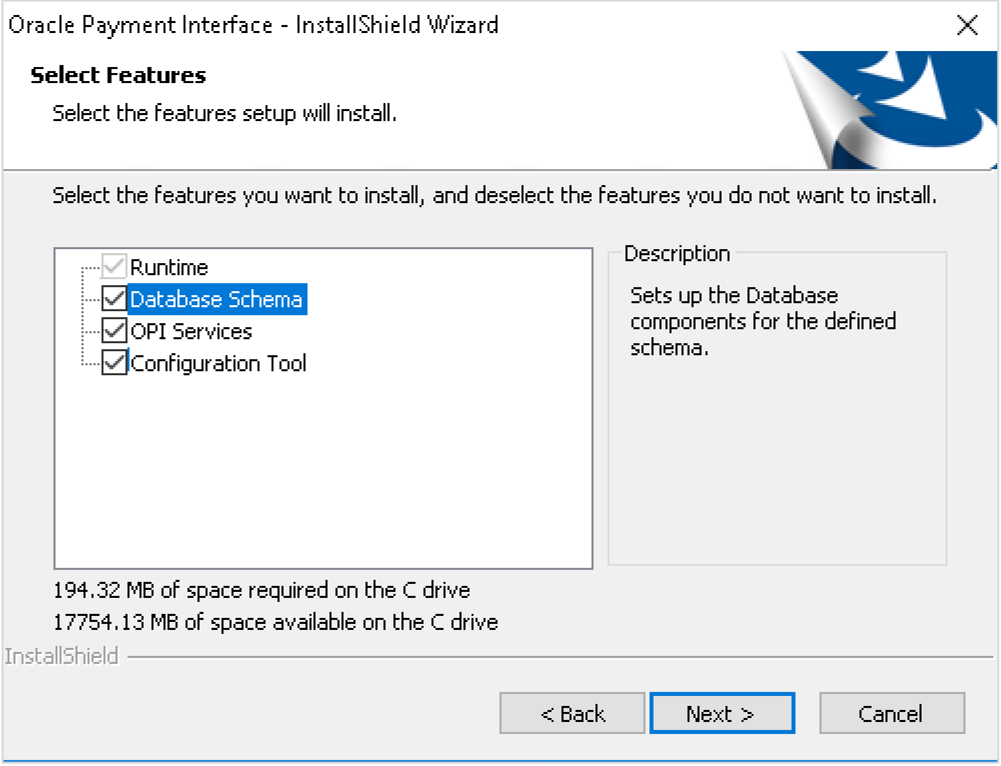
● Complete

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 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.

194.32 MB of space required on the C drive

17754.13 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.

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

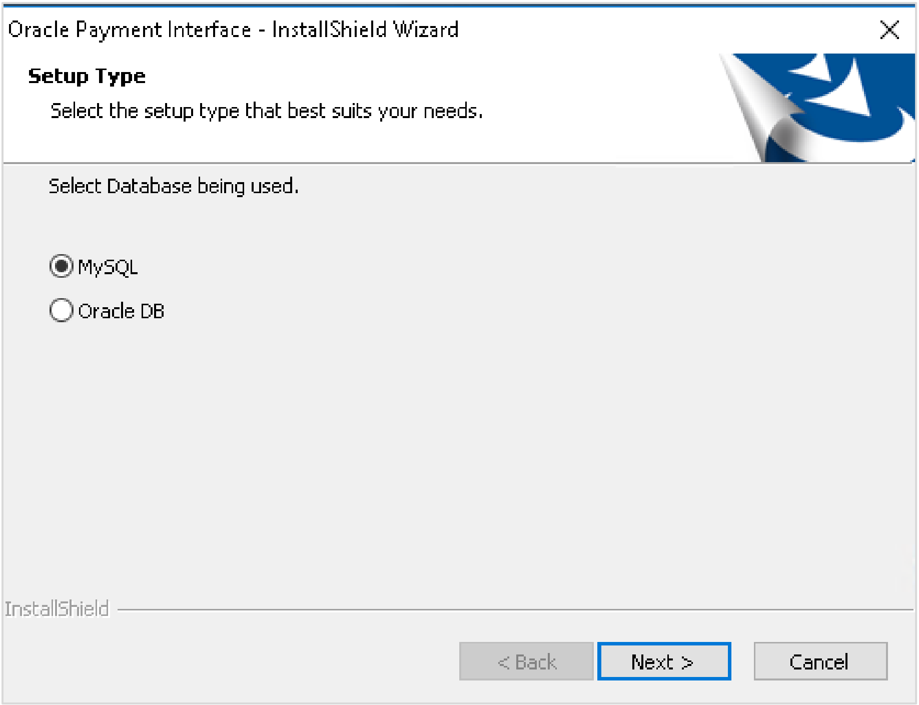
8. Click **Change** to amend the installation drive or path, if required and click **Next**.

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

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

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

11. Enter the relevant connection details for your database type. Details can be 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.

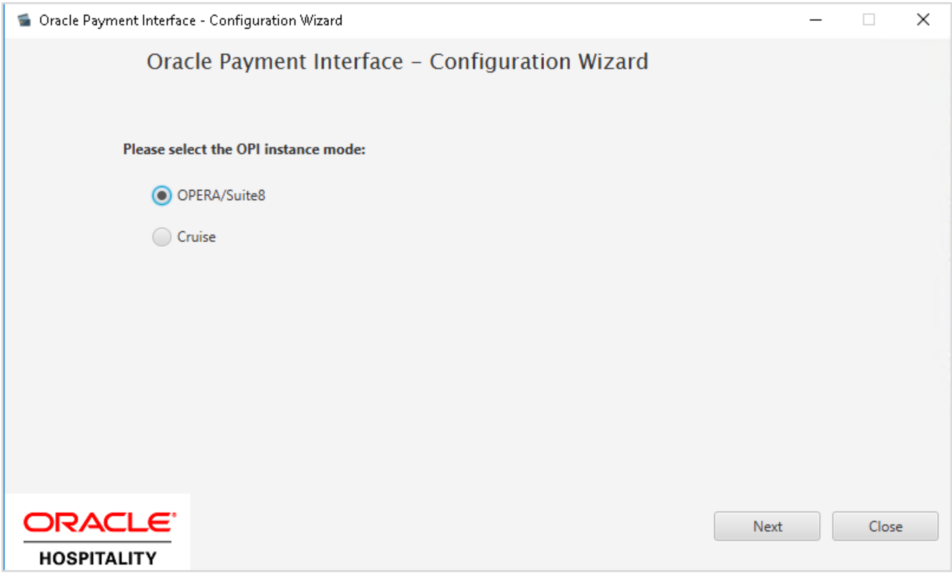
14. Enter the username and password to create a Super User System Admin level account that is used for configuring and maintaining the system.

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.



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**.

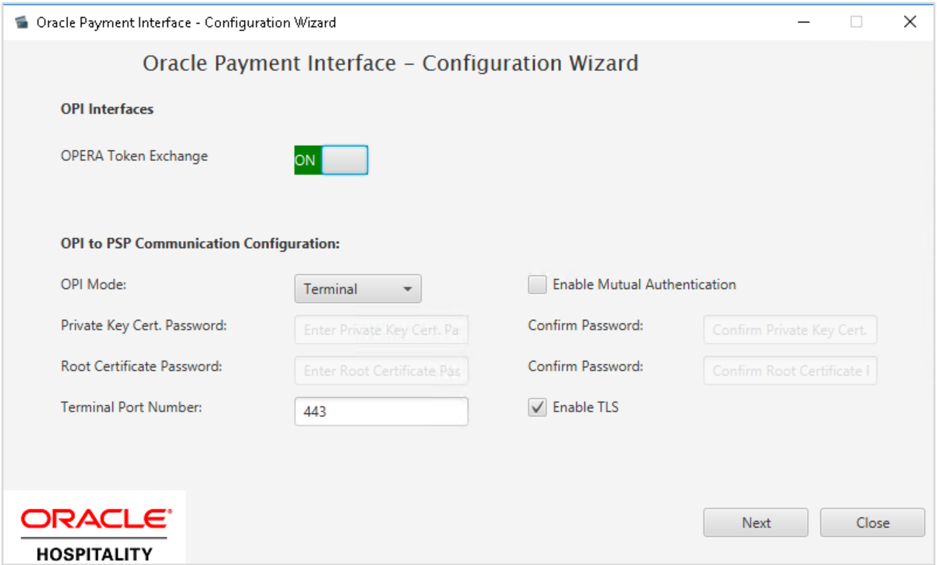
On the **OPI Interface** screen, the configuration screens displayed are same when the configuration wizard is launched manually. (**:\OraclePaymentInterface\v20.1\Config\LaunchWizard.bat**)

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

☐ Enable Mutual Authentication

Private Key Cert. Password: Enter Private Key Cert. Pa

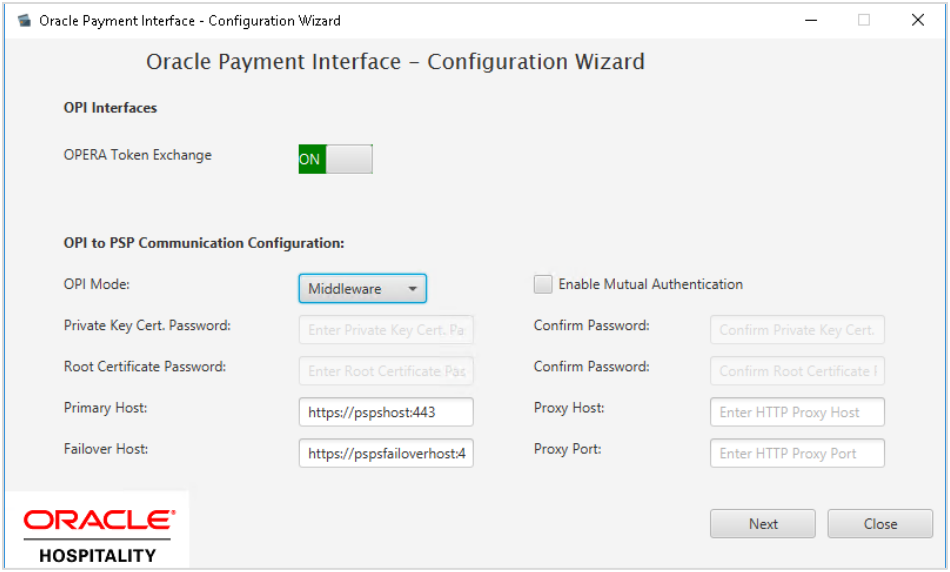
Confirm Password: Confirm Private Key Cert.

Root Certificate Password: Enter Root Certificate Pas

Confirm Password: Confirm Root Certificate I

Terminal Port Number: 443

☑ Enable TLS



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

OPI Interfaces

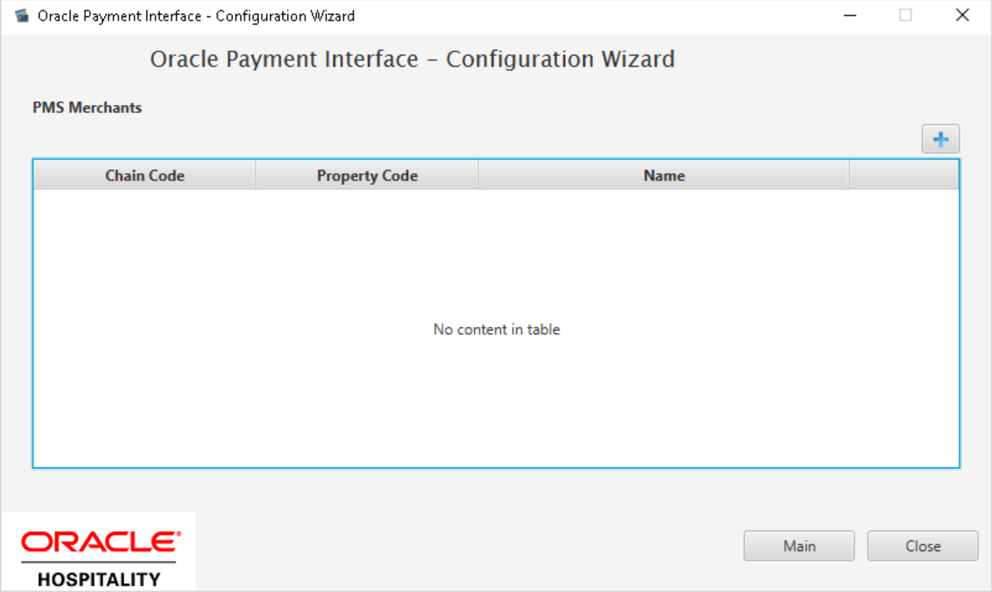
OPERA Token Exchange: ON

OPI to PSP Communication Configuration:

OPI Mode:	Middleware	□ Enable Mutual Authentication	
Private Key Cert. Password:	Enter Private Key Cert. Pa	Confirm Password:	Confirm Private Key Cert.
Root Certificate Password:	Enter Root Certificate Pas	Confirm Password:	Confirm Root Certificate I
Primary Host:	https://pspshost:443	Proxy Host:	Enter HTTP Proxy Host
Failover Host:	https://pspsfailoverhost:4	Proxy Port:	Enter HTTP Proxy Port

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

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

PMS Merchants

Chain Code	Property Code	Name	

No content in table

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

    a. The **OPERA 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**. You must use this key to configure the Hotel Property Interface (IFC8). Add “FidCrypt0S|” to the generated key as prefix. For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxx

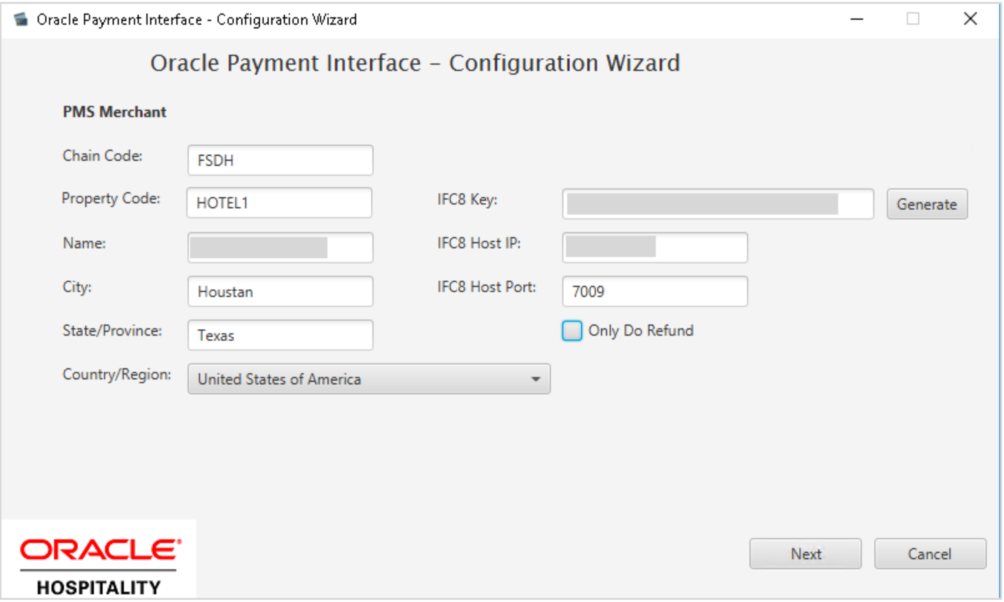
c. Enter the **IFC8 IP address** and **port** number for the Hotel Property Interface (IFC8) server.

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

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

f. 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
Generate
Next
Cancel
ORACLE
HOSPITALITY

PMS Merchant

Chain Code: FSDH

Property Code: HOTEL1

Name: [redacted]

City: Houstan

State/Province: Texas

Country/Region: United States of America

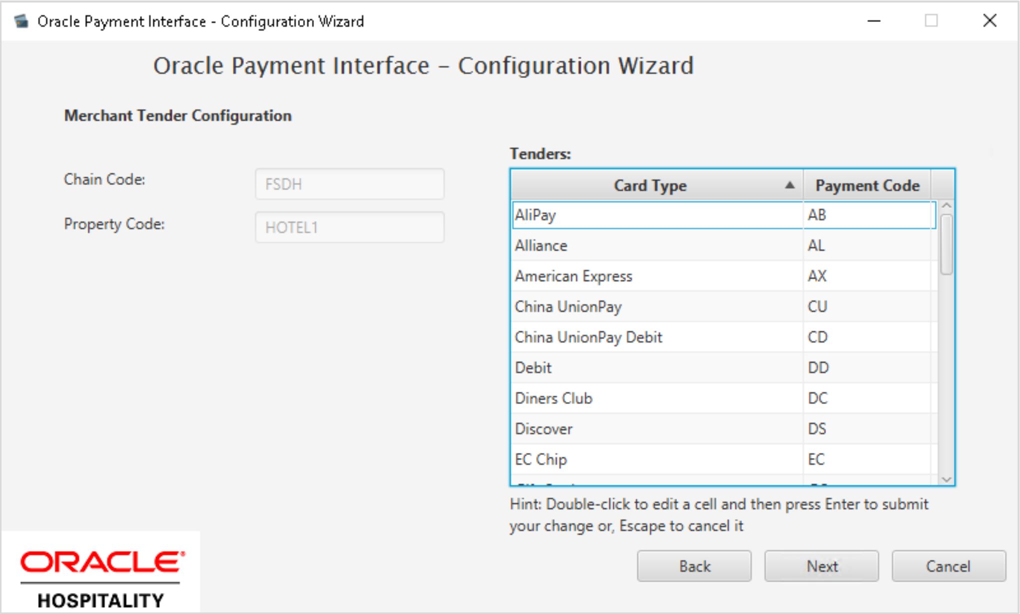
IFC8 Key: [redacted]

IFC8 Host IP: [redacted]

IFC8 Host Port: 7009

□ Only Do Refund

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

Merchant Tender Configuration

Chain Code: FSDH

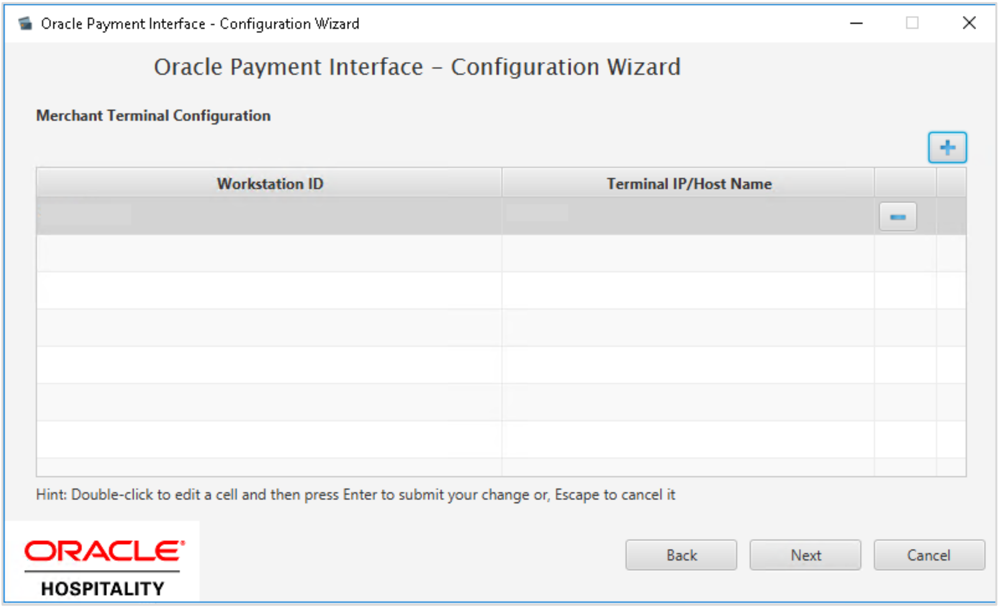
Property Code: HOTEL1

Tenders:

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

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

Below is terminal mapping if you select terminal mode.



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

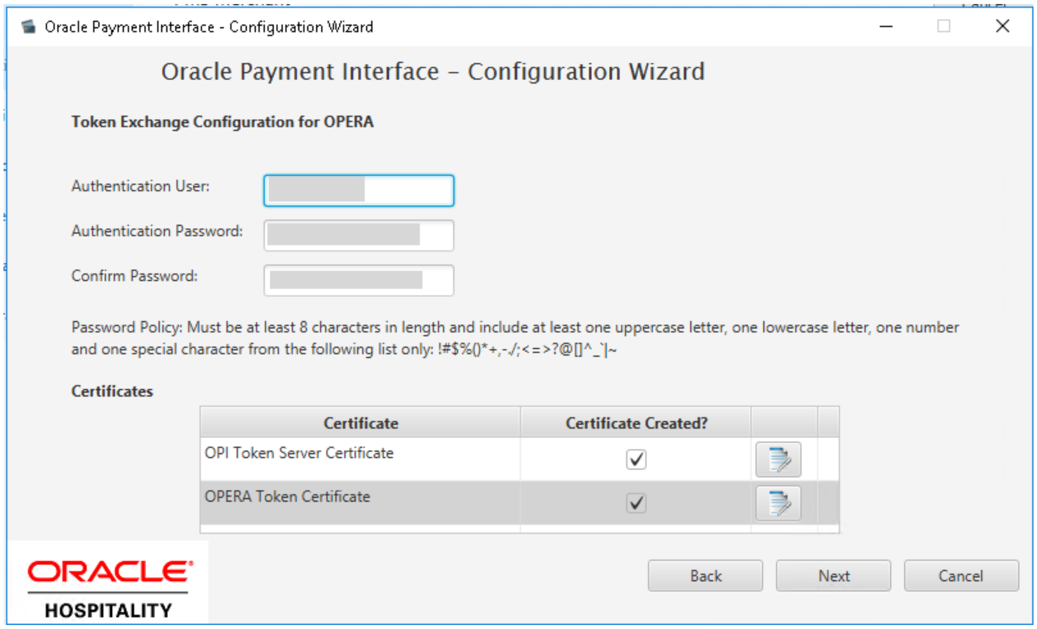
Merchant Terminal Configuration

Workstation ID	Terminal IP/Host Name

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

22. The top half of the Token Exchange Configuration screen allows you to configure the Header Authentication credentials used in communications from OPERA->OPI.

- The details entered must match the details entered in the OPERA Interface Custom Data page (**OPERA PMS Configuration | Setup | Property Interfaces | Interface Configuration** | edit **EFT IFC OPI | Custom Data** tab)



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

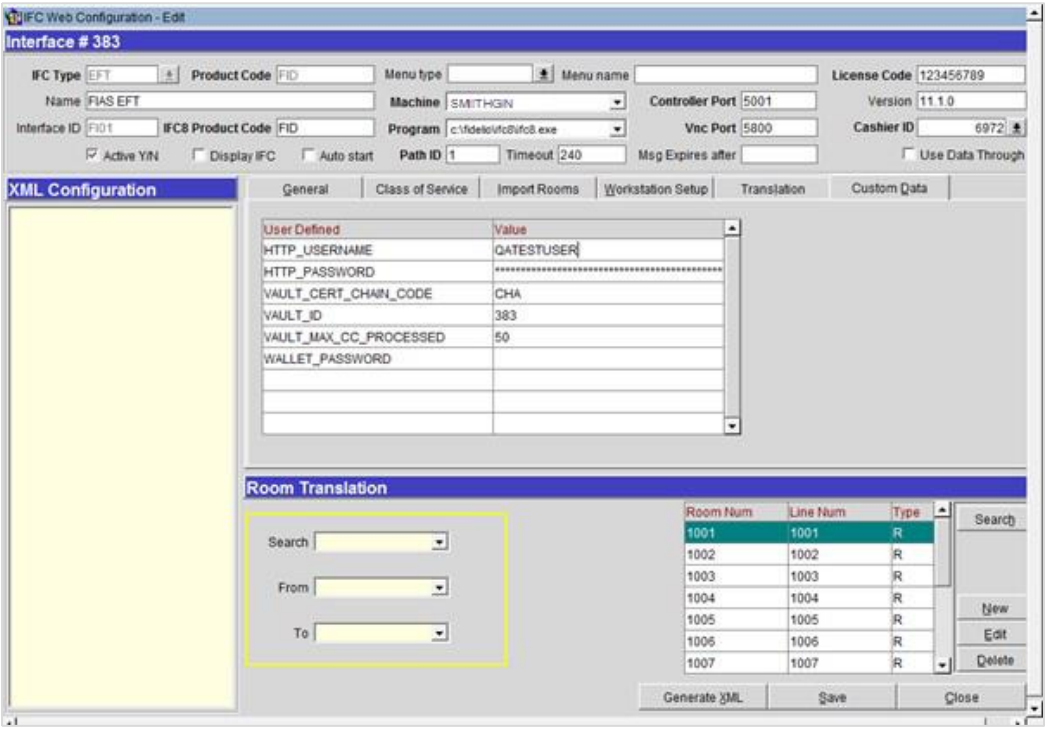
Token Exchange Configuration for OPERA

Authentication User:	[redacted]
Authentication Password:	[redacted]
Confirm Password:	[redacted]

Password Policy: Must be at least 8 characters in length and include at least one uppercase letter, one lowercase letter, one number and one special character from the following list only: !#$%()*+,-./;<=>?@[]^_`|~

Certificates

Certificate	Certificate Created?	
OPI Token Server Certificate	☑	
OPERA Token Certificate	☑	



IFC Web Configuration - Edit

Interface # 383

IFC Type	EFT	Product Code	FID	Menu type		Menu name		License Code	123456789
Name	FIAS EFT			Machine	SMITHGIN	Controller Port	5001	Version	11.1.0
Interface ID	FI01	IFC8 Product Code	FID	Program	c:\fidelio\ifc8\ifc8.exe	Vnc Port	5800	Cashier ID	6972

☑ Active Y/N ☐ Display IFC ☐ Auto start Path ID 1 Timeout 240 Msg Expires after ☐ Use Data Through

XML Configuration

User Defined	Value
HTTP_USERNAME	QATESTUSER
HTTP_PASSWORD	**
VAULT_CERT_CHAIN_CODE	CHA
VAULT_ID	383
VAULT_MAX_CC_PROCESSED	50
WALLET_PASSWORD	

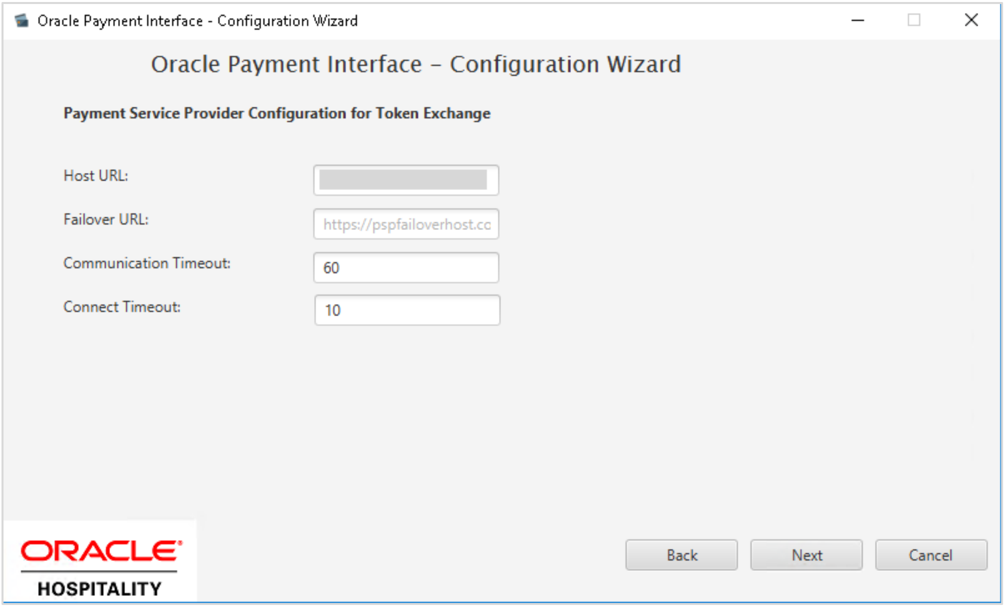
Room Translation

Search
From
To

Room Num	Line Num	Type
1001	1001	R
1002	1002	R
1003	1003	R
1004	1004	R
1005	1005	R
1006	1006	R
1007	1007	R

- Certificates are explained in the Certificates section.

23. 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

Oracle Payment Interface – Configuration Wizard

Payment Service Provider Configuration for Token Exchange

Host URL: [redacted]

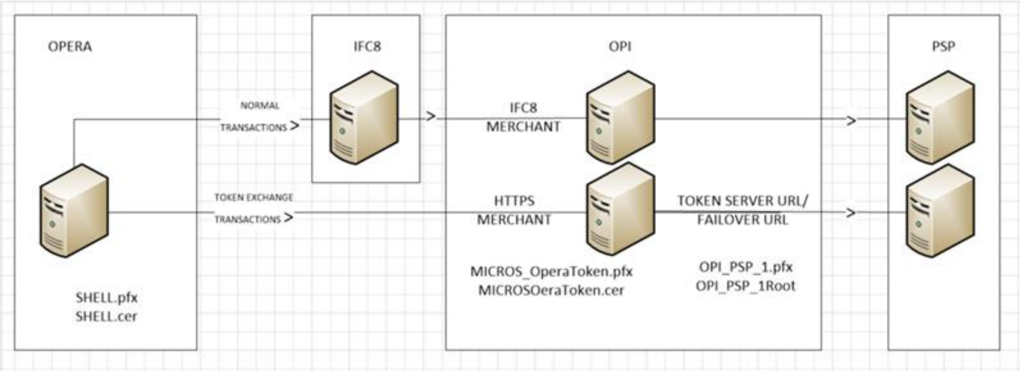
Failover URL: https://pspfailoverhost.cc

Communication Timeout: 60

Connect Timeout: 10

24. Click **Finish** to restart.

Certificates



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

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

Refer to the sections below for further details.

PSP - Client Side Certificates

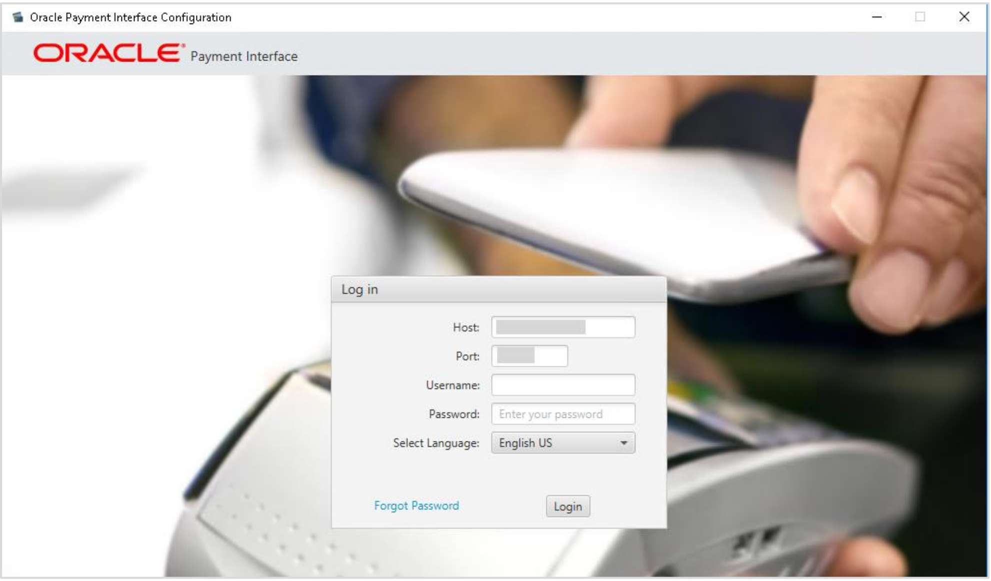
The communication from OPI to the PSP for token exchange uses HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed on PSP (server side) for HTTPS communication, the PSP is also expected to provide a client side certificate to be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

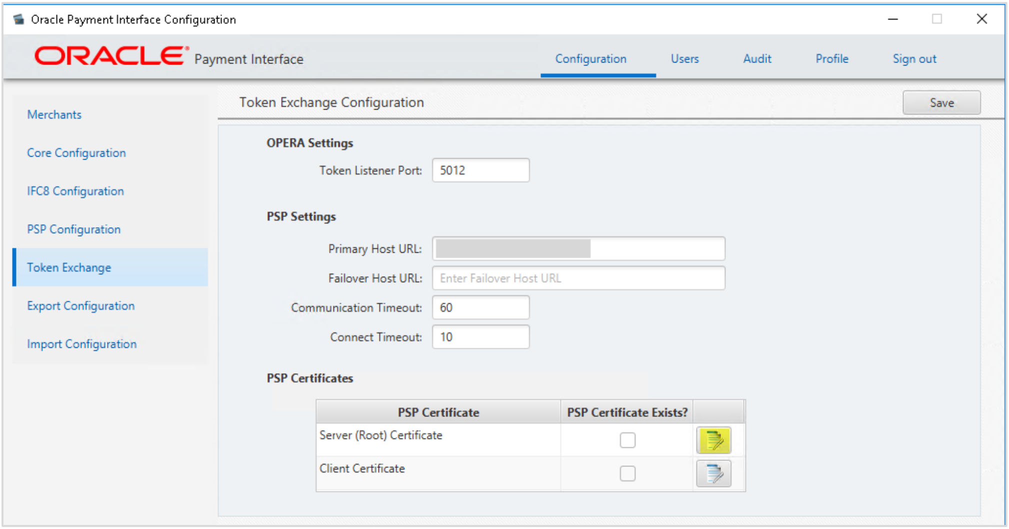
To deploy the client certificate on the OPI side:

1. Run **\OraclePaymentInterface\v20.1\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 **PSP Token Exchange**, and then edit the **Server (Root) Certificate**.



Token Exchange Configuration

OPERA Settings

Token Listener Port: 5012

PSP Settings

Primary Host URL: [redacted]

Failover Host URL: Enter Failover Host URL

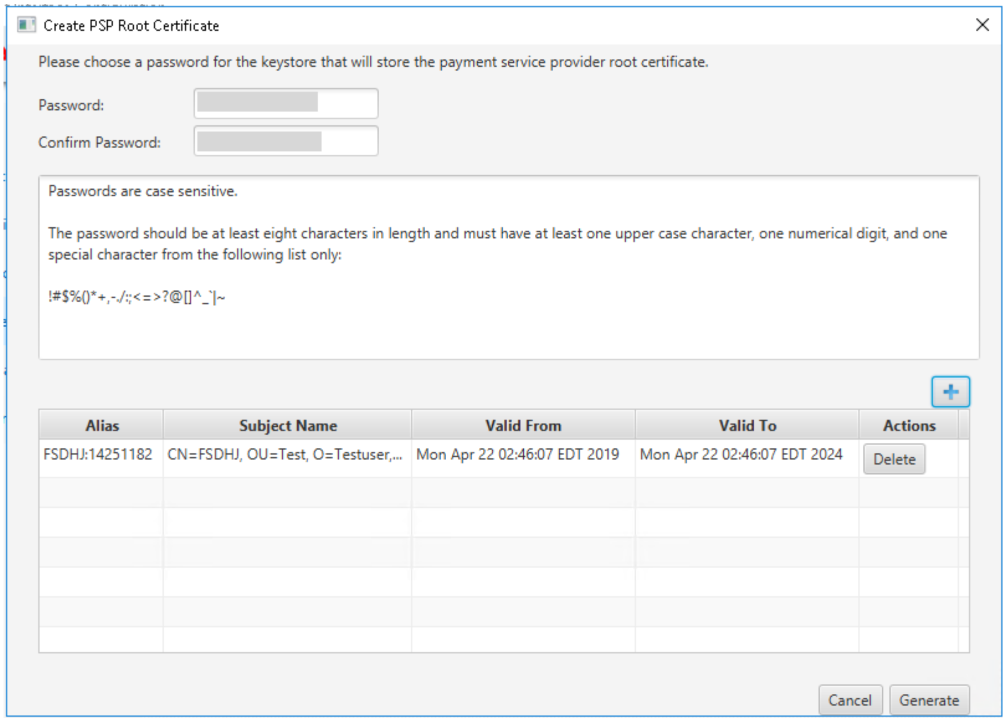
Communication Timeout: 60

Connect Timeout: 10

PSP Certificates

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

2. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** (+) icon or you can also drag and drop the .cer or.crt.



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

Password: [redacted]

Confirm Password: [redacted]

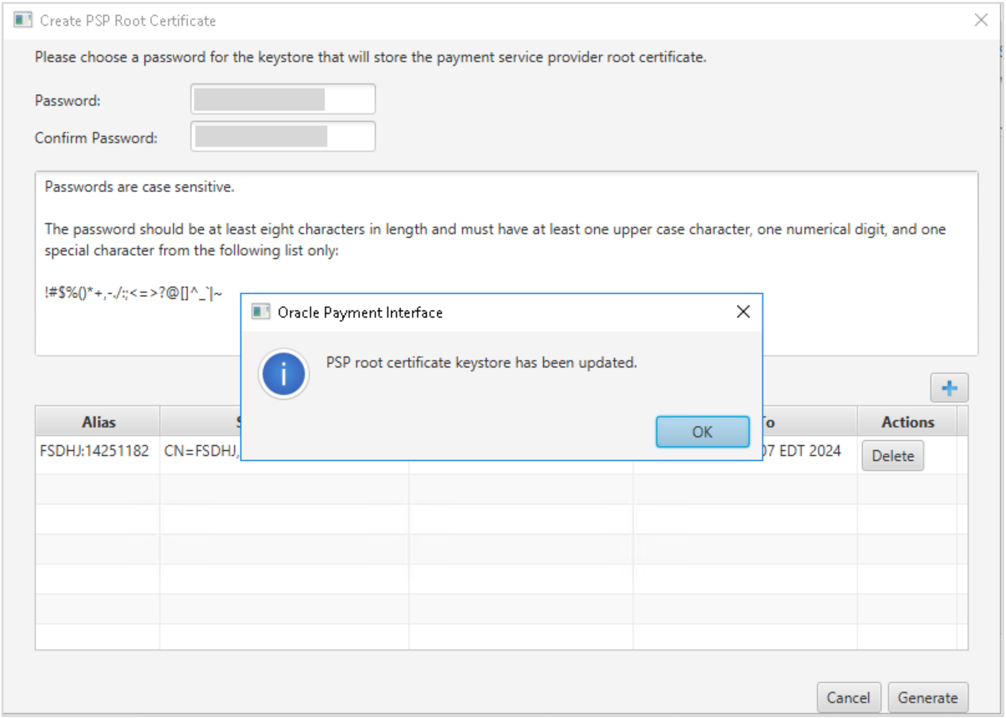
Passwords are case sensitive.

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	Actions
FSDHJ:14251182	CN=FSDHJ, OU=Test, O=Testuser,...	Mon Apr 22 02:46:07 EDT 2019	Mon Apr 22 02:46:07 EDT 2024	Delete

3. Click **Generate**.



Create PSP Root Certificate

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:

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

Oracle Payment Interface

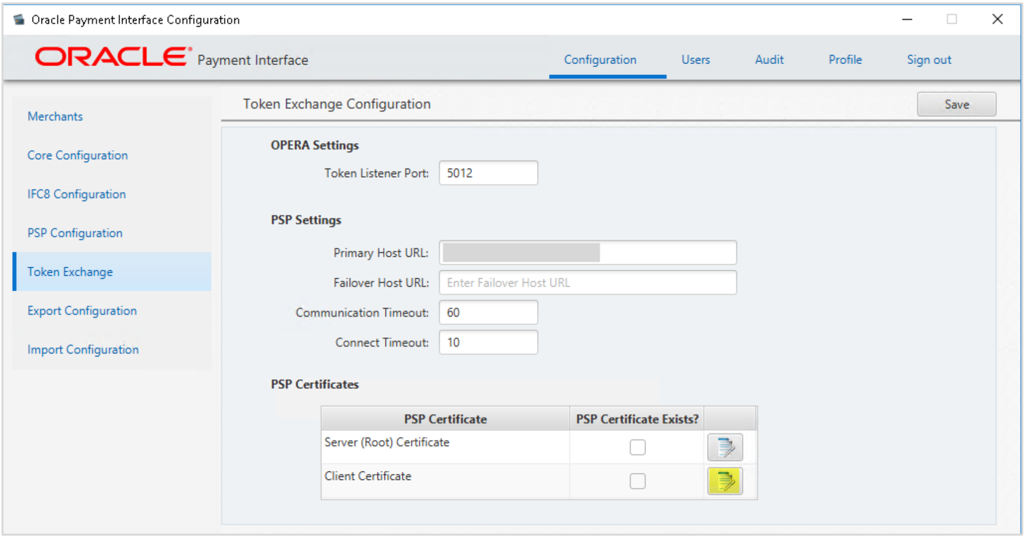
PSP root certificate keystore has been updated.

Alias	S		o	Actions
FSDHJ:14251182	CN=FSDHJ,		7 EDT 2024	Delete

OPI_PSP_1Root is created under \OraclePaymentInterface\v20.1\Services\OPI\key

Handling the Client Side Certificate

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



Token Exchange Configuration

OPERA Settings

Token Listener Port: 5012

PSP Settings

Primary Host URL:

Failover Host URL: Enter Failover Host URL

Communication Timeout: 60

Connect Timeout: 10

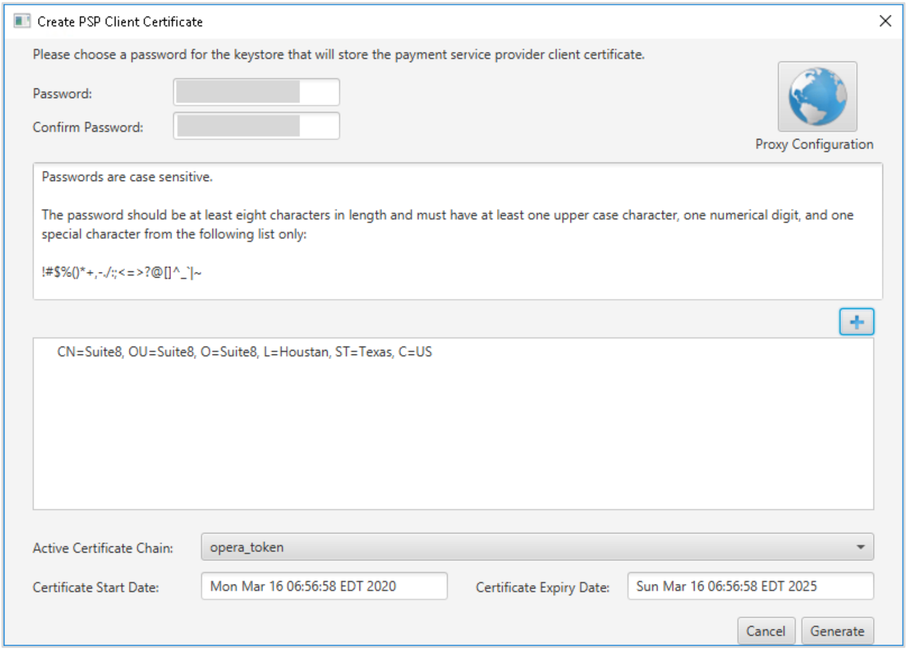
PSP Certificates

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

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



Create PSP Client Certificate

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:

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

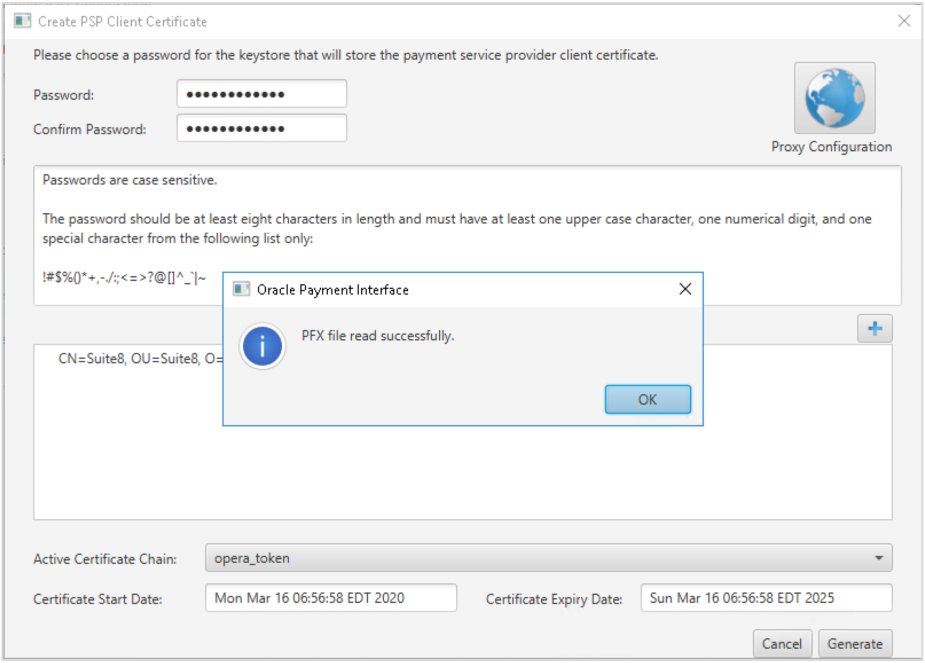
CN=Suite8, OU=Suite8, O=Suite8, L=Houstan, ST=Texas, C=US

Active Certificate Chain: opera_token

Certificate Start Date: Mon Mar 16 06:56:58 EDT 2020

Certificate Expiry Date: Sun Mar 16 06:56:58 EDT 2025

3. Click **Generate.**



Create PSP Client Certificate

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=Suite8, OU=Suite8, O=

Oracle Payment Interface

PFX file read successfully.

Active Certificate Chain: opera_token

Certificate Start Date: Mon Mar 16 06:56:58 EDT 2020

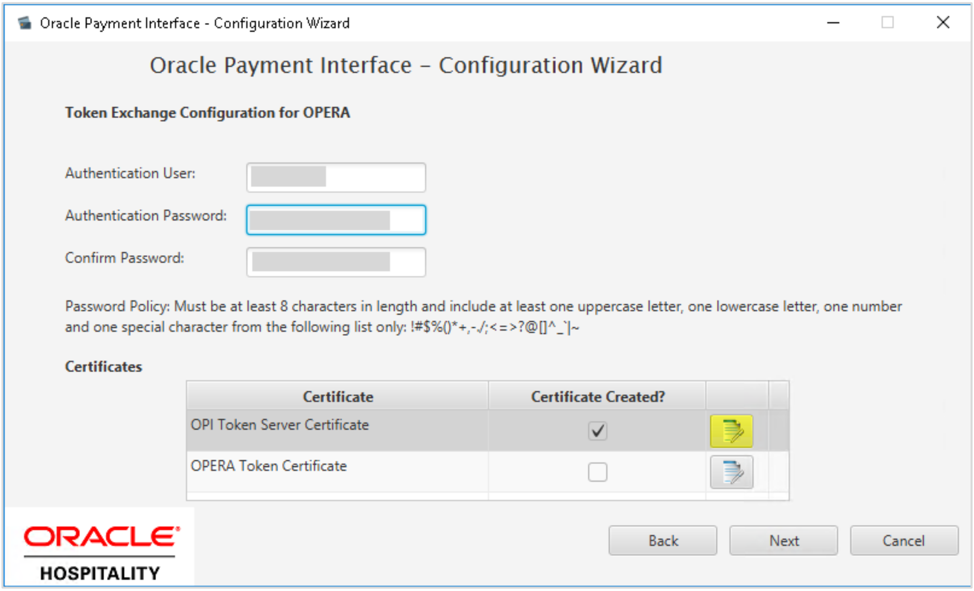
Certificate Expiry Date: Sun Mar 16 06:56:58 EDT 2025

OPI_PSP_1.pfx is created under **\OraclePaymentInterface\v20.1\Services\OPI\key** folder.

OPI - Server Side Certificates

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

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



Oracle Payment Interface – Configuration Wizard

Token Exchange Configuration for OPERA

Authentication User:

Authentication Password:

Confirm Password:

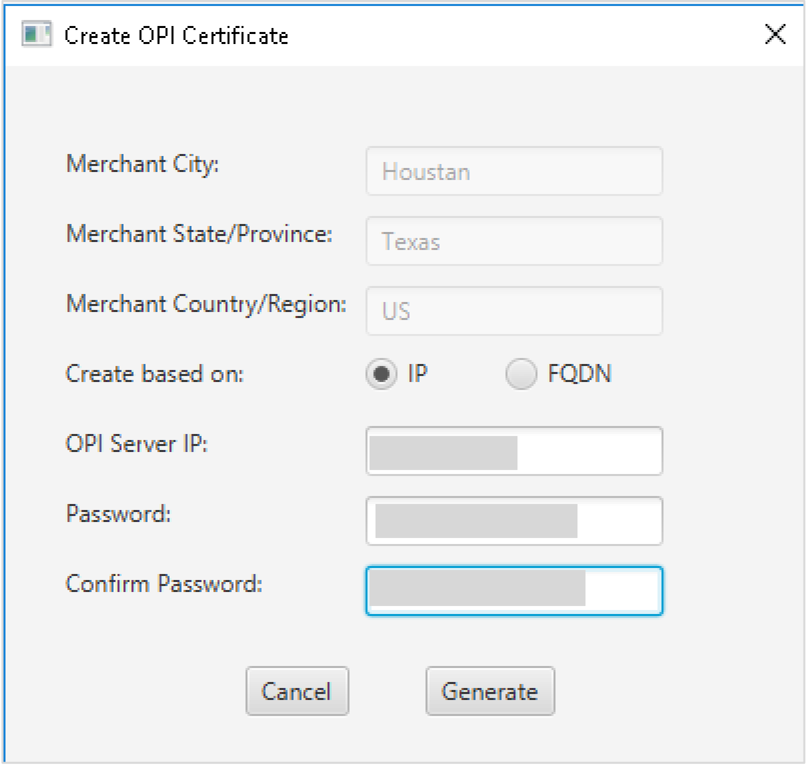
Password Policy: Must be at least 8 characters in length and include at least one uppercase letter, one lowercase letter, one number and one special character from the following list only: !#$%()*+,-./;<=>?@[]^_`|~

Certificates

Certificate	Certificate Created?
OPI Token Server Certificate	☑
OPERA Token Certificate	□

2. Populate the fields with the relevant information. The password fields validate the passwords are complex, so the passwords will need to meet these requirements;

- Min 8 characters in length
- Min 1 Alpha Character
- Min 1 Numeric Character
- Min 1 Special Character from the following list !@#$%^&*



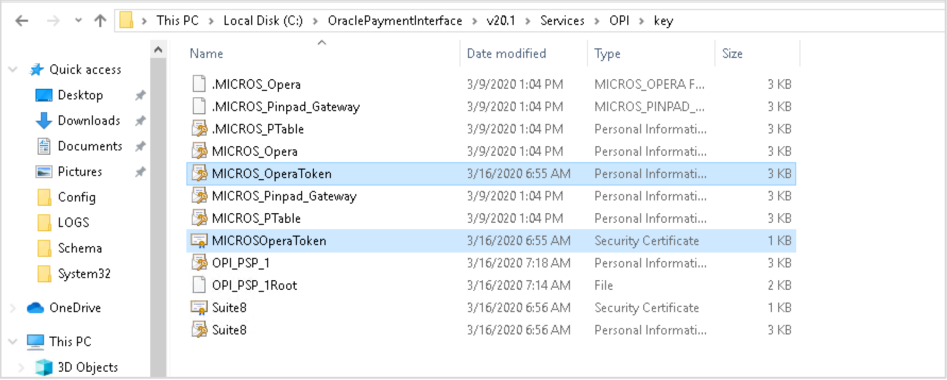
Create OPI Certificate

Merchant City:	Houstan
Merchant State/Province:	Texas
Merchant 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\v20.1\Services\OPI\key\



This PC › Local Disk (C:) › OraclePaymentInterface › v20.1 › Services › OPI › key

Name	Date modified	Type	Size
.MICROS_Opera	3/9/2020 1:04 PM	MICROS_OPERA F...	3 KB
.MICROS_Pinpad_Gateway	3/9/2020 1:04 PM	MICROS_PINPAD_...	3 KB
.MICROS_PTable	3/9/2020 1:04 PM	Personal Informati...	3 KB
MICROS_Opera	3/9/2020 1:04 PM	Personal Informati...	3 KB
MICROS_OperaToken	3/16/2020 6:55 AM	Personal Informati...	3 KB
MICROS_Pinpad_Gateway	3/9/2020 1:04 PM	Personal Informati...	3 KB
MICROS_PTable	3/9/2020 1:04 PM	Personal Informati...	3 KB
MICROSOperaToken	3/16/2020 6:55 AM	Security Certificate	1 KB
OPI_PSP_1	3/16/2020 7:18 AM	Personal Informati...	3 KB
OPI_PSP_1Root	3/16/2020 7:14 AM	File	2 KB
Suite8	3/16/2020 6:56 AM	Security Certificate	1 KB
Suite8	3/16/2020 6:56 AM	Personal Informati...	3 KB

NOTE:

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

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

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

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

OPI - Client Side Certificates

NOTE:

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

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

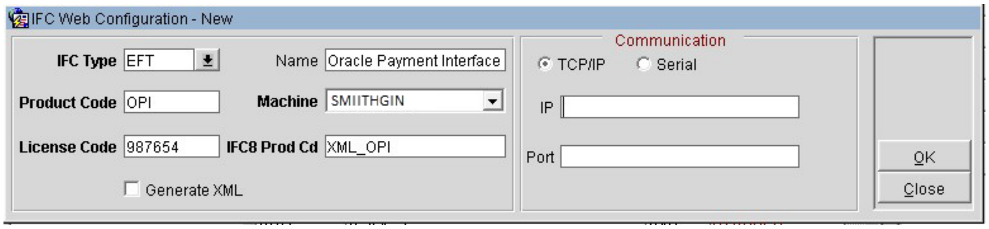
3

OPERA Configuration

Creating an EFT Interface

1. Log in to OPERA and go to **Configuration**.
2. Select the menu option **Setup | Property Interfaces | Interface Configuration**. If there is no active EFT or CCW IFC Type, select New to add configuration for a new EFT interface.
3. Enter the following options, and then click **OK**:

- **IFC Type**: EFT
- **Name**: Oracle Payment Interface
- **Product Code**: OPI
- **Machine**: Select the machine
- **License Code**: License code for interface
- **IFC8 Prod Cd**: XML_OPI



IFC Web Configuration - New

IFC Type	EFT	Name	Oracle Payment Interface
Product Code	OPI	Machine	SMIITHGIN
License Code	987654	IFC8 Prod Cd	XML_OPI

□ Generate XML

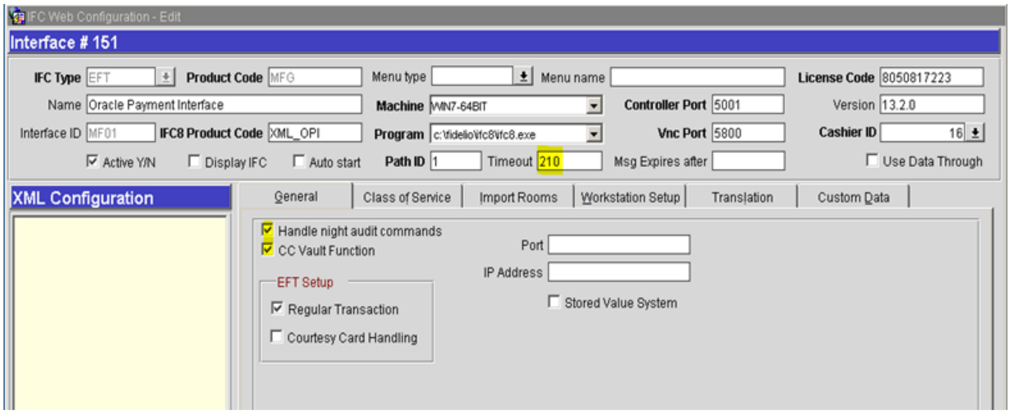
Communication

● TCP/IP ○ Serial

IP

Port

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



IFC Web Configuration - Edit

Interface # 151

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

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

Interface ID: MF01 | IFC8 Product Code: XML_OPI | Program: c:\fidelio\ifc8\ifc8.exe | Vnc Port: 5800 | Cashier ID: 16

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

XML Configuration

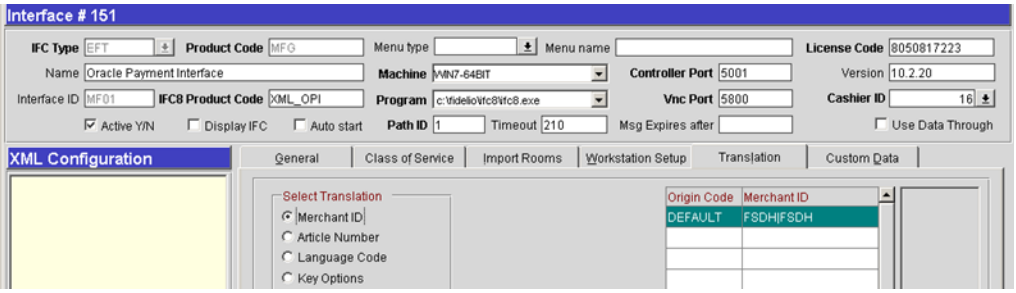
☑ Handle night audit commands
☑ CC Vault Function

Port:
IP Address:
□ Stored Value System

EFT Setup
☑ Regular Transaction
□ Courtesy Card Handling

7. Select the **Translation** tab, and then click **Merchant ID**.

8. Select **New** to add the Merchant ID. This must be the same as previously configured in OPI (MPG) Configuration.



Interface # 151

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

Name: Oracle Payment Interface | Machine: WIN7-64BIT | Controller Port: 5001 | Version: 10.2.20

Interface ID: MF01 | IFC8 Product Code: XML_OPI | Program: c:\fidelio\ifc8\ifc8.exe | Vnc Port: 5800 | Cashier ID: 16

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

XML Configuration

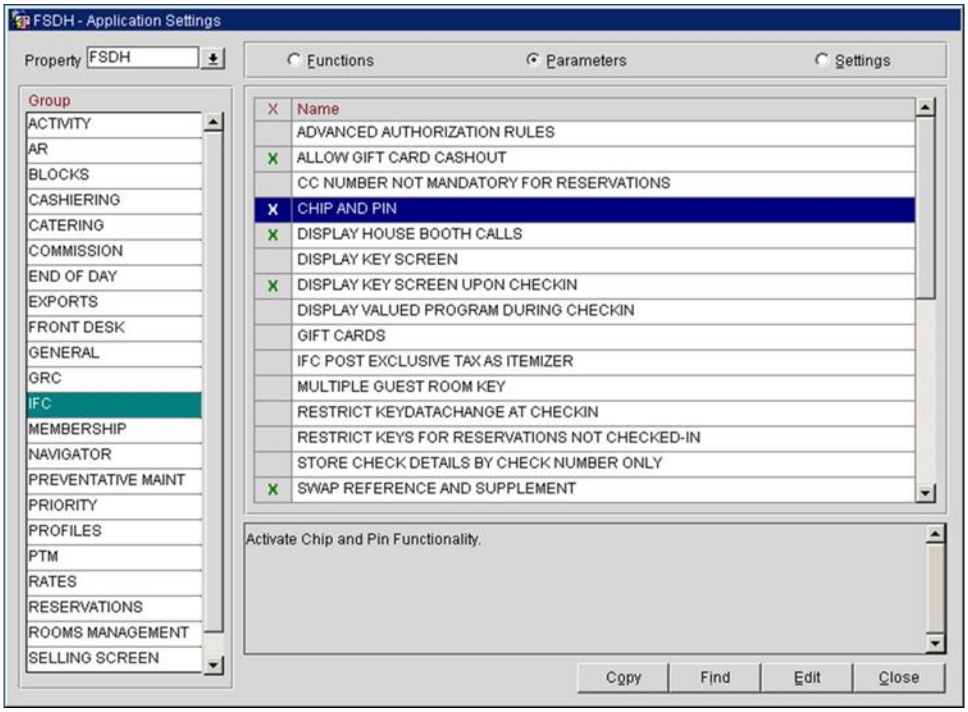
Select Translation
● Merchant ID
○ Article Number
○ Language Code
○ Key Options

Origin Code	Merchant ID
DEFAULT	FSDH|FSDH

Configuring CHIP AND PIN (EMV)

To configure the Functionality Setup:

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



FSDH - Application Settings

Property FSDH

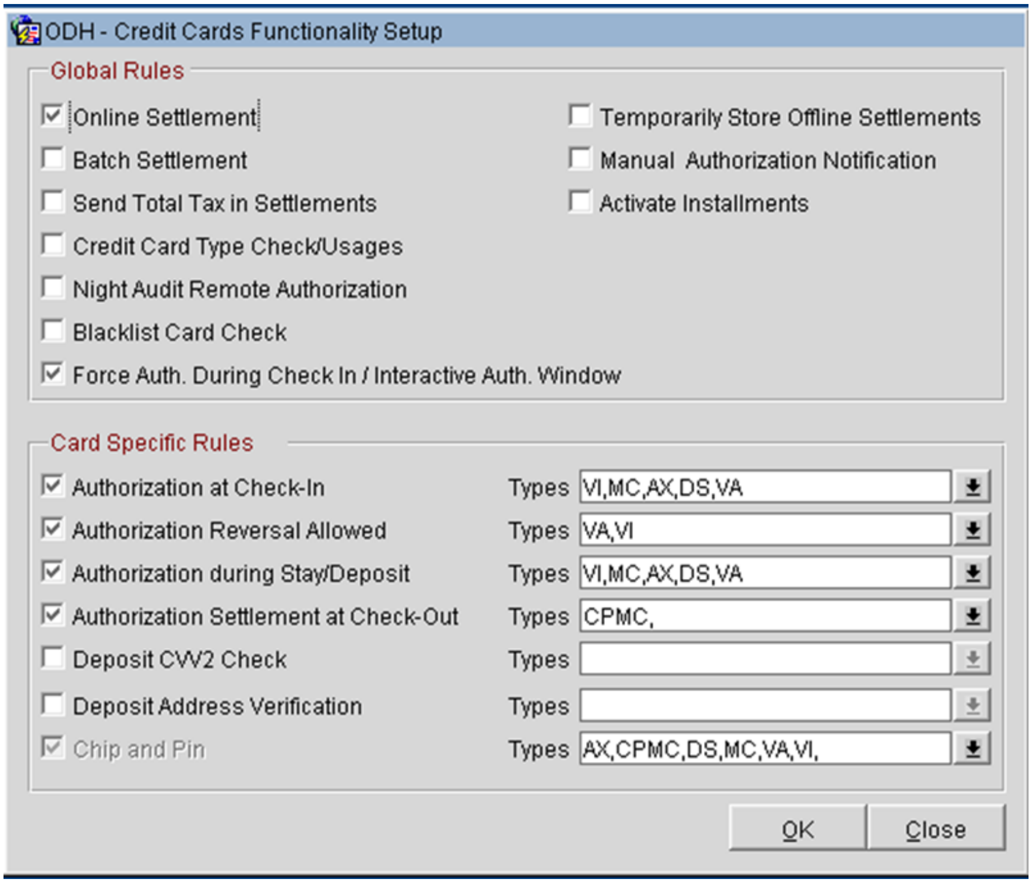
○ Functions ● Parameters ○ Settings

Group
ACTIVITY
AR
BLOCKS
CASHIERING
CATERING
COMMISSION
END OF DAY
EXPORTS
FRONT DESK
GENERAL
GRC
IFC
MEMBERSHIP
NAVIGATOR
PREVENTATIVE MAINT
PRIORITY
PROFILES
PTM
RATES
RESERVATIONS
ROOMS MANAGEMENT
SELLING SCREEN

X	Name
	ADVANCED AUTHORIZATION RULES
X	ALLOW GIFT CARD CASHOUT
	CC NUMBER NOT MANDATORY FOR RESERVATIONS
X	CHIP AND PIN
X	DISPLAY HOUSE BOOTH CALLS
	DISPLAY KEY SCREEN
X	DISPLAY KEY SCREEN UPON CHECKIN
	DISPLAY VALUED PROGRAM DURING CHECKIN
	GIFT CARDS
	IFC POST EXCLUSIVE TAX AS ITEMIZER
	MULTIPLE GUEST ROOM KEY
	RESTRICT KEYDATACHANGE AT CHECKIN
	RESTRICT KEYS FOR RESERVATIONS NOT CHECKED-IN
	STORE CHECK DETAILS BY CHECK NUMBER ONLY
X	SWAP REFERENCE AND SUPPLEMENT

Activate Chip and Pin Functionality.

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



ODH - Credit Cards Functionality Setup

Global Rules

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

Card Specific Rules

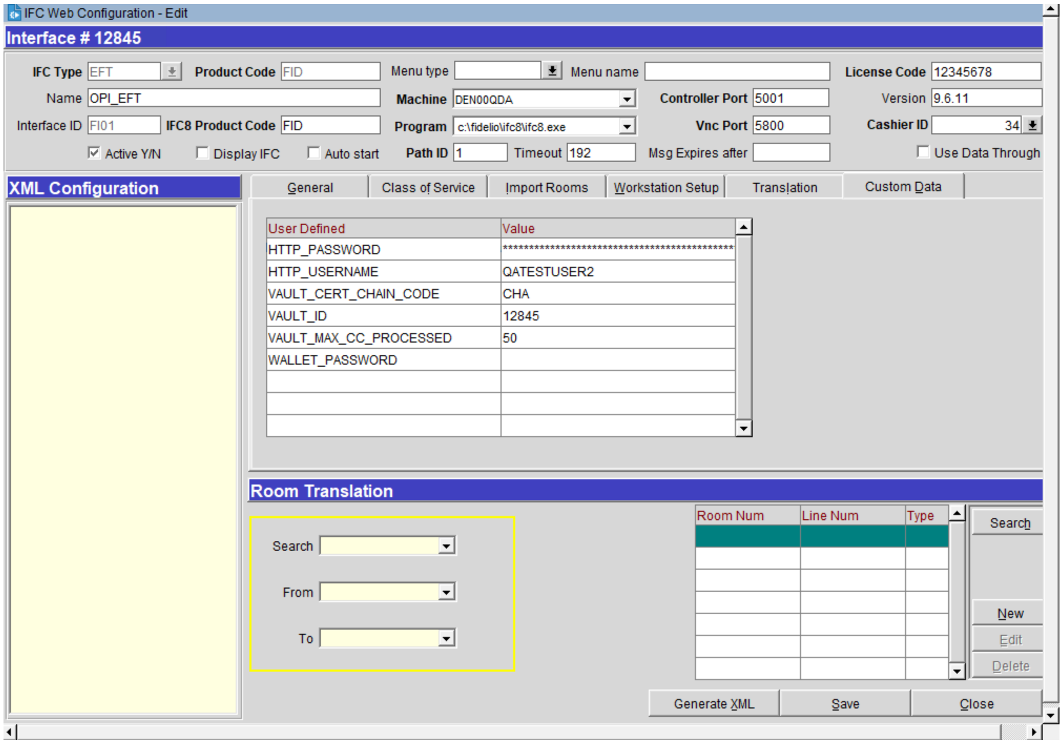
☑ Authorization at Check-In	Types	VI,MC,AX,DS,VA
☑ Authorization Reversal Allowed	Types	VA,VI
☑ Authorization during Stay/Deposit	Types	VI,MC,AX,DS,VA
☑ Authorization Settlement at Check-Out	Types	CPMC,
☐ Deposit CVV2 Check	Types	
☐ Deposit Address Verification	Types	
☑ Chip and Pin	Types	AX,CPMC,DS,MC,VA,VI,

- **Online Settlement**: Select this check box to allow online settlement. OPI is an online settlement. This must be checked to activate the Chip and PIN Application Setting.
- **Authorization at Check-In**: Select the payment methods that will trigger an automatic credit card authorization at check-in.
- **Authorization Reversal Allowed**: Select the payment methods that can process authorization reversals. This provides a request transaction to the Payment Partner to remove the existing authorization on a guest credit card or debit card if the folio payment type is changed or at check-out a different payment method is used. For example, a guest checks in on a reservation for a 5-night stay using a Visa credit card for payment type. At the time of authorization, a hold is put on the Visa credit card for the total cost of the stay. If the payment type is changed to another type on the reservation or the guest checks out using cash or a different brand of credit card, OPERA will send a reversal request for the originally selected Visa credit card authorization. A partial reverse authorization is not supported.
- **Authorization During Stay/Deposit**: Select the payment methods that allow manual and automatic authorizations following check-in and prior to check-out and settlement. This option must be enabled in order to allow authorizations by the end-of-day routine.
- **Authorization Settlement at Check-Out**: Select the payment types that use credit card authorization and settlement in one transaction request. These are payment types that do not allow an authorization separate from the settlement/sale.
  - The payment types that are available in the multi-select list of values are only payment types configured as EFT payment types. Any one payment type can be selected for credit card specific rules of Authorization at check-in, Authorization Reversal, and Authorization during Stay/Deposit. If they are selected for these card specific rules, then the payment types will not be available for Authorization During Stay/Deposit.
- **Chip and PIN Enabled Payment Types**: When the **IFC | Chip and PIN** application parameter is set to Y, this option is visible and selected by default. You may not unselect the check box. Select the LOV to choose the credit card payment types that will trigger a Chip and PIN message with or without credit card data to the EMV Device. Payment types that are configured here will not require that a credit card number or expiration date to be entered when selected as a payment method on the Reservation screen or on the Payment screen. This data can be provided in the response message from the Payment Partner.

Configuring the CC Vault

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

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



IFC Web Configuration - Edit

Interface # 12845

IFC Type	EFT	Product Code	FID	Menu type		Menu name		License Code	12345678
Name	OPI_EFT			Machine	DEN00QDA	Controller Port	5001	Version	9.6.11
Interface ID	FI01	IFC8 Product Code	FID	Program	c:\fidelio\ifc8\ifc8.exe	Vnc Port	5800	Cashier ID	34

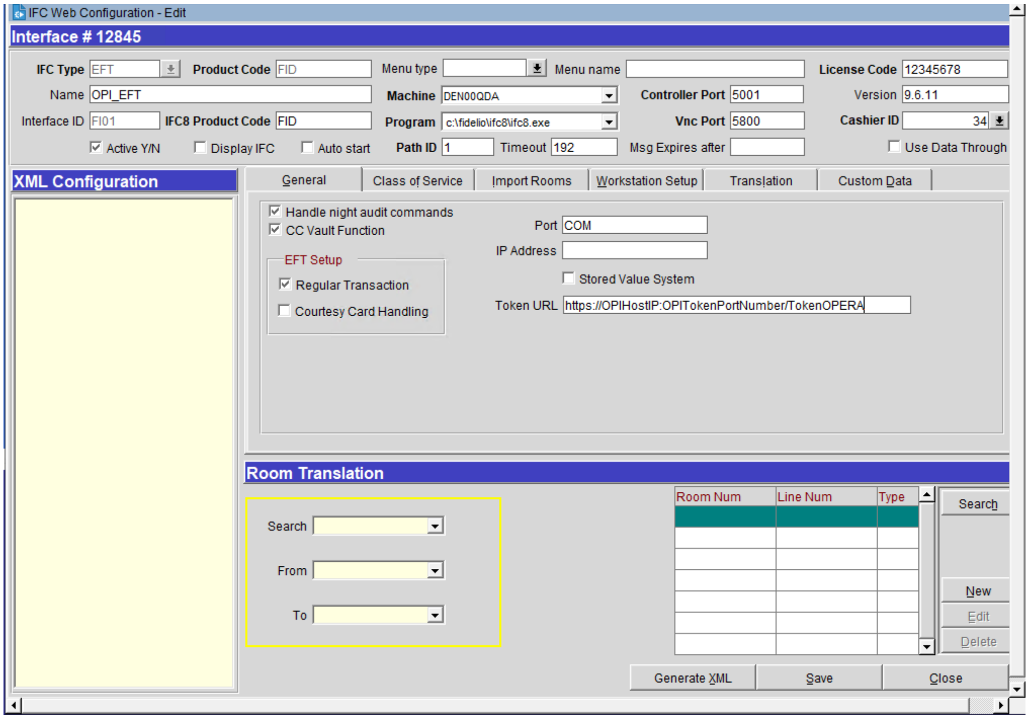
☑ Active Y/N ☐ Display IFC ☐ Auto start Path ID 1 Timeout 192 Msg Expires after ☐ Use Data Through

User Defined	Value
HTTP_PASSWORD	***
HTTP_USERNAME	QATESTUSER2
VAULT_CERT_CHAIN_CODE	CHA
VAULT_ID	12845
VAULT_MAX_CC_PROCESSED	50
WALLET_PASSWORD	

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

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

Example: https://OPIHost or address :OPITokenPortNumber/TokenOPERA



IFC Web Configuration - Edit

Interface # 12845

IFC Type EFT
Product Code FID
Menu type
Menu name
License Code 12345678
Name OPI_EFT
Machine DEN00QDA
Controller Port 5001
Version 9.6.11
Interface ID FI01
IFC8 Product Code FID
Program c:\fidelio\ifc8\ifc8.exe
Vnc Port 5800
Cashier ID 34
☑ Active Y/N
□ Display IFC
□ Auto start
Path ID 1
Timeout 192
Msg Expires after
□ Use Data Through

XML Configuration

☑ Handle night audit commands
☑ CC Vault Function
Port COM
IP Address
□ Stored Value System
Token URL https://OPIHostIP:OPITokenPortNumber/TokenOPERA

EFT Setup
☑ Regular Transaction
□ Courtesy Card Handling

Room Translation

The CREDIT CARD VAULT ID is currently not used.

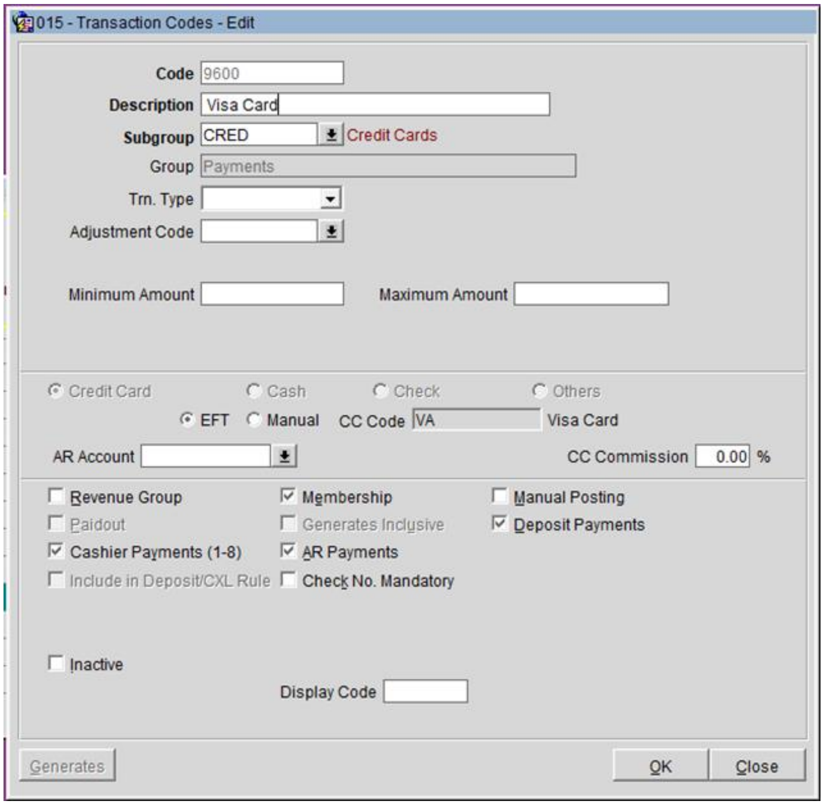
The CREDIT CARD MAX CC PROCESSED is set to what the Payment Partner can support for the number of rows sent in one Token (GetID/GetCC) request. This is used during the bulk tokenization process and when multiple folio windows exist on OPERA Reservations. 50 is the default used when nothing is set here (This is determined by Payment Partner/Vendor; please verify with Partner/Vendor, the number of credit cards that can be processed per batch).

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

Cashiering Overview

Credit Card Payment Transaction Codes

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



015 - Transaction Codes - Edit

Code 9600

Description Visa Card

Subgroup CRED Credit Cards

Group Payments

Trn. Type

Adjustment Code

Minimum Amount

Maximum Amount

● Credit Card ○ Cash ○ Check ○ Others

● EFT ○ Manual CC Code VA Visa Card

AR Account

CC Commission 0.00 %

□ Revenue Group ☑ Membership □ Manual Posting

□ Paidout □ Generates Inclusive ☑ Deposit Payments

☑ Cashier Payments (1-8) ☑ AR Payments

□ Include in Deposit/CXL Rule □ Check No. Mandatory

□ Inactive

Display Code

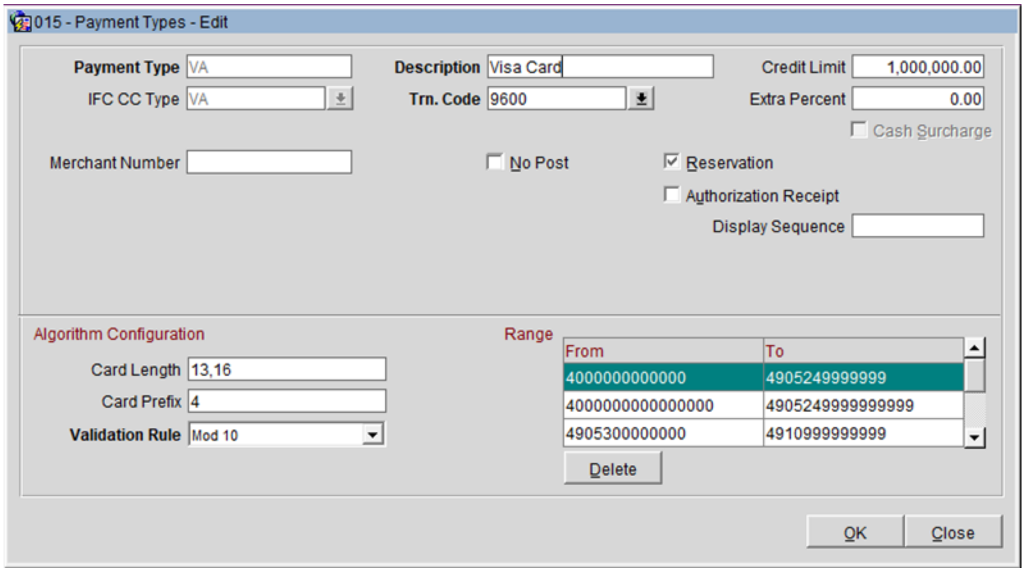
2. Information for credit card payment transaction codes:

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

Overview of Credit Card Payment Types

The credit card payment types link with the transaction code:

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


015 - Payment Types - Edit

Payment Type VA

IFC CC Type VA

Description Visa Card

Trn. Code 9600

Credit Limit 1,000,000.00

Extra Percent 0.00

□ Cash Surcharge

Merchant Number

□ No Post

☑ Reservation

□ Authorization Receipt

Display Sequence

Algorithm Configuration

Card Length 13,16

Card Prefix 4

Validation Rule Mod 10

Range

From	To
4000000000000	4905249999999
4000000000000000	4905249999999999
4905300000000	4910999999999

Credit Card Type Payment Setup Information

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

Sample List of Card Types

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

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

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

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

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

Individual Card Functions

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

Payment Types - Customer NOT Present (Keyed)	**Authorization at Check-in**	**Pay Only (no Authorization)**	**Deposit Y/N**	**Cashier Payment Y/N**	**A/R Payment Y/N**
KVA	Y	N	Y	Y	Y
KMC	Y	N	Y	Y	Y
KAX	Y	N	Y	Y	Y
KDC	Y	N	Y	Y	Y
KJC	Y	N	Y	Y	Y

Payment Types - Customer NOT Present (Keyed)	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
KCU	Y	N	Y	Y	Y
KVD	N	Y	Y	Y	Y
KMD	N	Y	Y	Y	Y
KCD	N	Y	Y	Y	Y

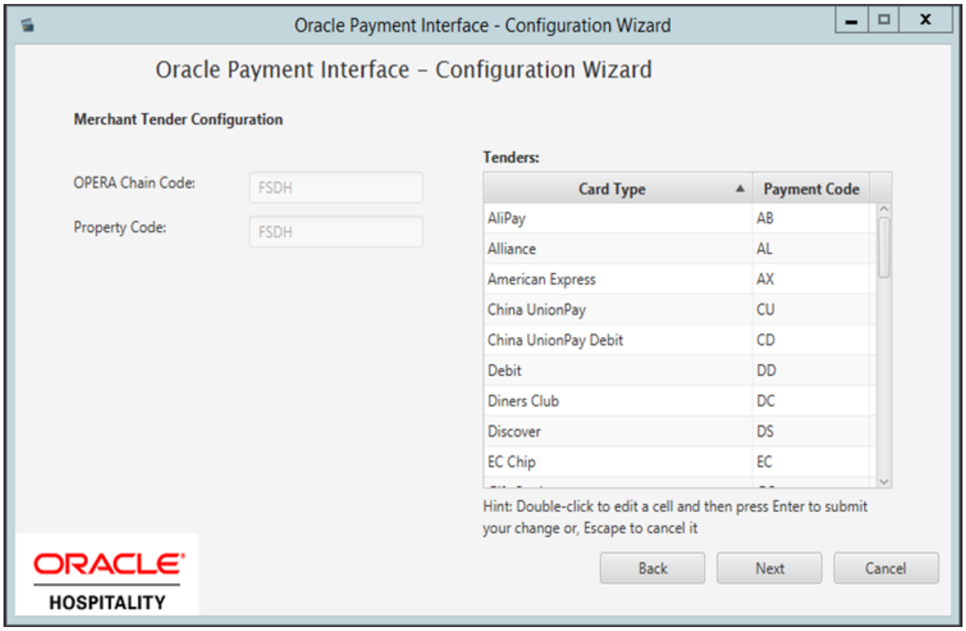
Payment Types – One Shot Cards (Keyed) OPTIONAL!!!	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
VVA	N	Y	N	Y	N
VMC	N	Y	N	Y	N
VAX	N	Y	N	Y	N

Important Considerations

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

Update OPI Configuration Merchant Tenders

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

Merchant Tender Configuration

OPERA Chain Code: FSDH

Property Code: FSDH

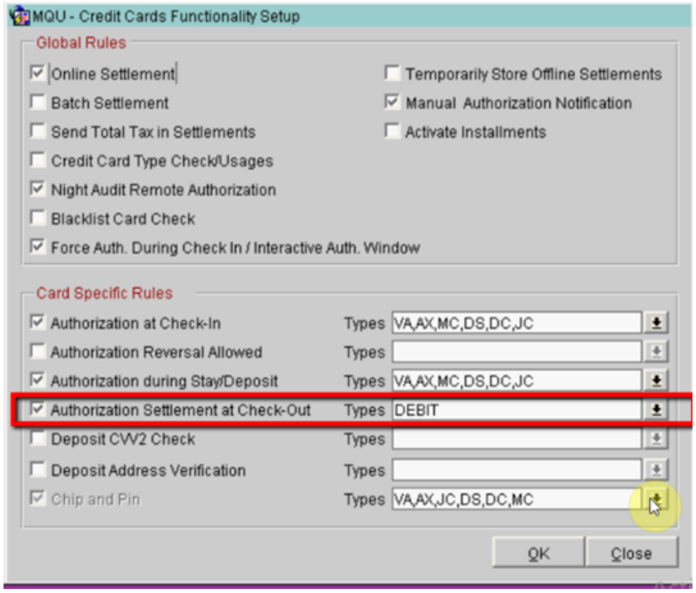
Tenders:

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

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

Update Functionality settings for Chip & Pin and PayOnly

- Selection for Chip and Pin and PayOnly cards.



MQU - Credit Cards Functionality Setup

Global Rules

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

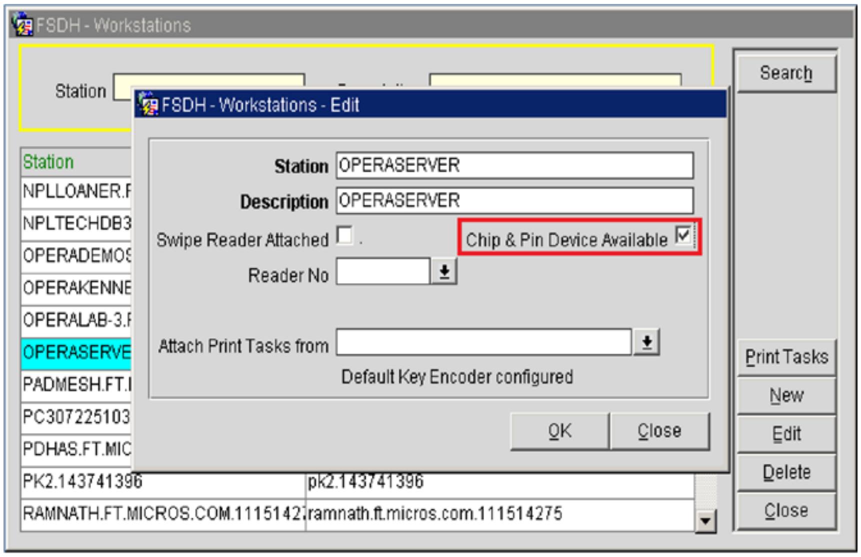
Card Specific Rules

☑ Authorization at Check-In — Types VA,AX,MC,DS,DC,JC
☐ Authorization Reversal Allowed — Types
☑ Authorization during Stay/Deposit — Types VA,AX,MC,DS,DC,JC
☑ Authorization Settlement at Check-Out — Types DEBIT
☐ Deposit CVV2 Check — Types
☐ Deposit Address Verification — Types
☑ Chip and Pin — Types VA,AX,JC,DS,DC,MC

Configuring the Workstation

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

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



FSDH - Workstations

FSDH - Workstations - Edit

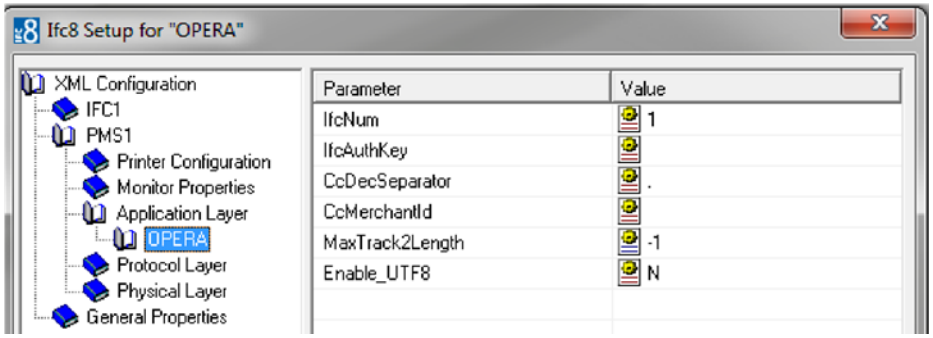
Station: OPERASERVER
Description: OPERASERVER
Swipe Reader Attached ☐
Chip & Pin Device Available ☑
Reader No
Attach Print Tasks from
Default Key Encoder configured

Station	
NPLLOANER.F	
NPLTECHDB3	
OPERADEMOS	
OPERAKENNE	
OPERALAB-3.F	
OPERASERVE	
PADMESH.FT.I	
PC307225103	
PDHAS.FT.MIC	
PK2.143741396	pk2.143741396
RAMNATH.FT.MICROS.COM.1115142	ramnath.ft.micros.com.111514275

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

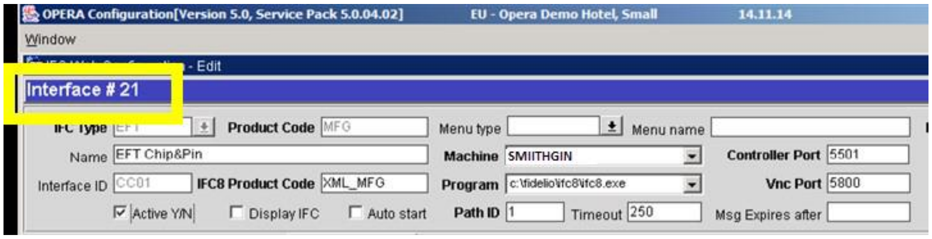
To configure the link between the interfaces:

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



Parameter	Value
IfcNum	1
IfcAuthKey	
CcDecSeparator	.
CcMerchantId	
MaxTrack2Length	-1
Enable_UTF8	N

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


OPERA Configuration[Version 5.0, Service Pack 5.0.04.02]
EU - Opera Demo Hotel, Small
14.11.14
Window
- Edit

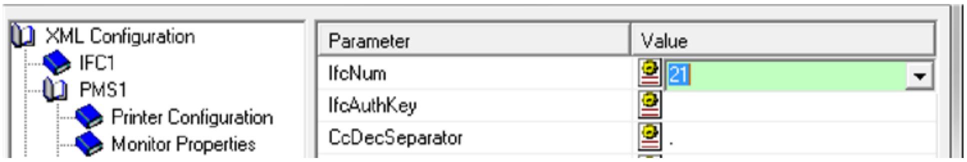
Interface # 21

IFC Type	EFT	Product Code	MFG	Menu type	
Name	EFT Chip&Pin	Machine	SMIITHGIN	Controller Port	5501
Interface ID	CC01	IFC8 Product Code	XML_MFG	Program	c:\fidelio\ifc8\ifc8.exe
Vnc Port	5800	Path ID	1	Timeout	250

Menu name:

☑ Active Y/N ☐ Display IFC ☐ Auto start

Msg Expires after:

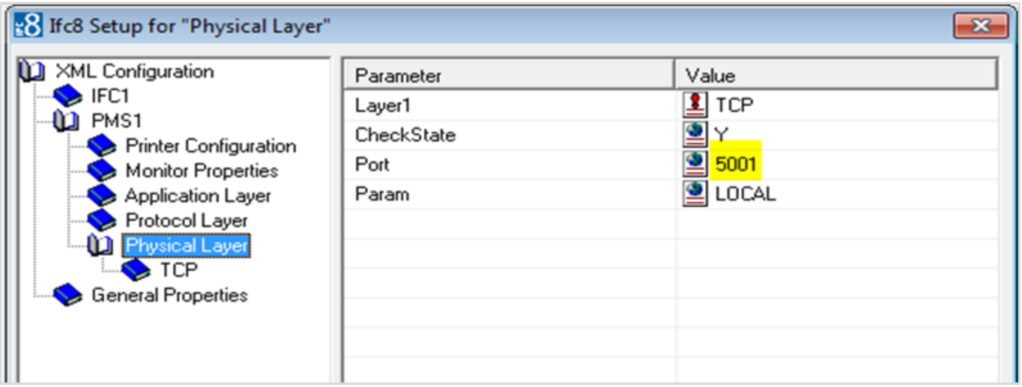


Parameter	Value
IfcNum	21
IfcAuthKey	
CcDecSeparator	.

3. Go to the **PMS1** tree in the **Physical Layer**.

4. Enter the port number into Parameter value Port. This is the port IFC8 uses to communicate with the OPERA IFC controller.

5. Select **Enter** and **Apply** to re-initiate IFC8, and then click **Save**.

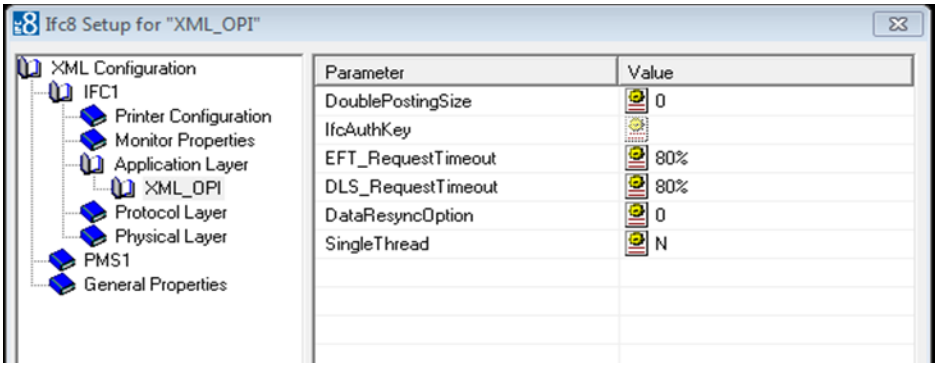


Parameter	Value
Layer1	TCP
CheckState	Y
Port	5001
Param	LOCAL

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

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

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

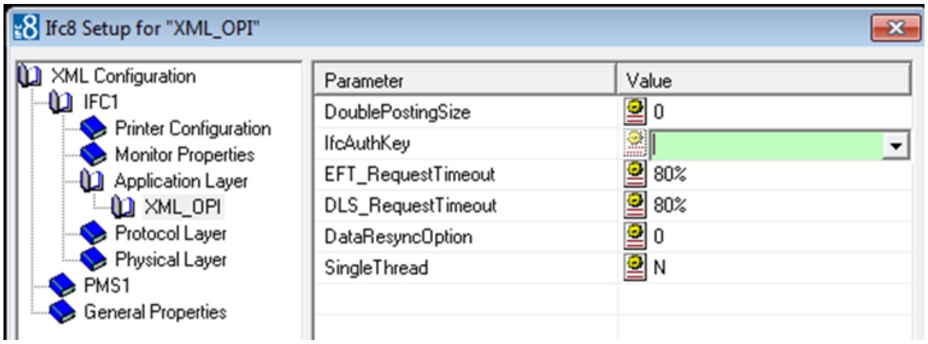


Parameter	Value
DoublePostingSize	0
IfcAuthKey	
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0
SingleThread	N

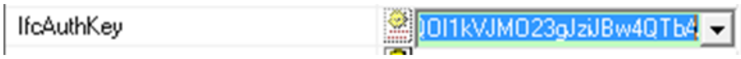
2. Copy the generated key from Configuring OPI - OPERA merchant step 3, and add “FidCrypt0S|” to the generated key as prefix.

   For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxxxx

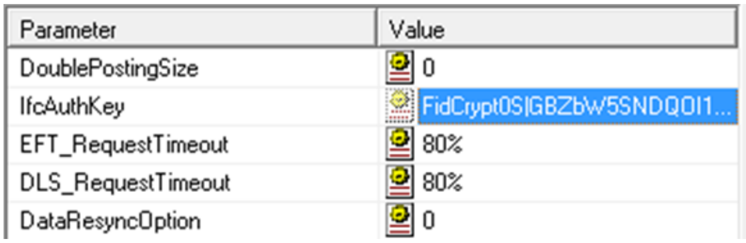
3. Copy this string into IFC8 Parameter **IfcAuthKey** value field.



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



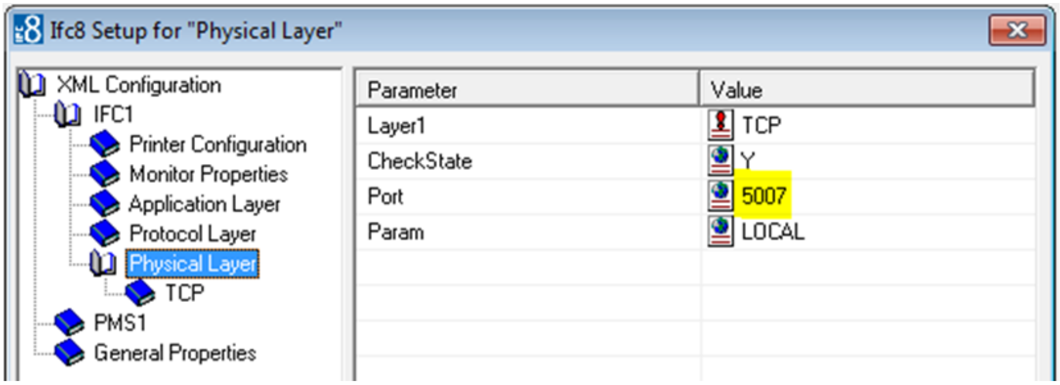
IfcAuthKey 	)OI1kVJMO23gJziJBw4QTb4



Parameter	Value
DoublePostingSize	0
IfcAuthKey	FidCrypt0S|GBZbW5SNDQOI1...
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0

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

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



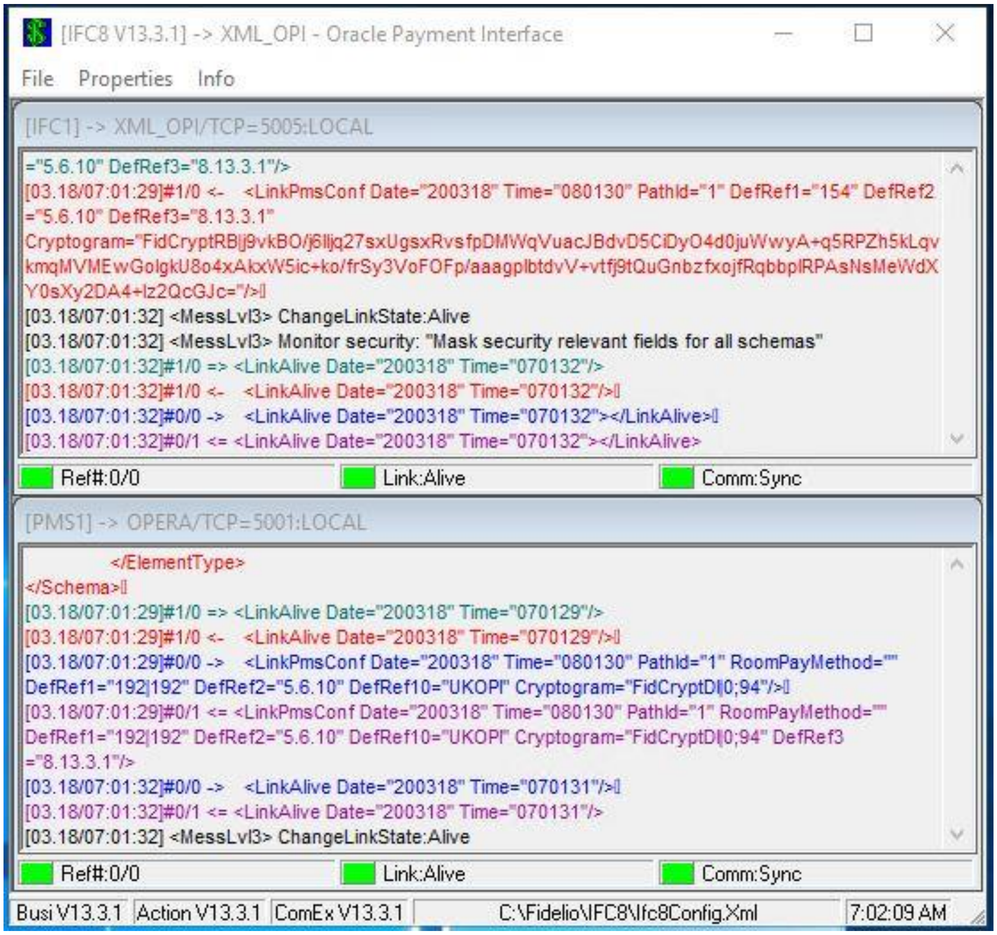
Parameter	Value
Layer1	TCP
CheckState	Y
Port	5007
Param	LOCAL

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

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

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

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


[IFC8 V13.3.1] -> XML_OPI - Oracle Payment Interface
File
Properties
Info
[IFC1] -> XML_OPI/TCP=5005:LOCAL

```
="5.6.10" DefRef3="8.13.3.1"/>
[03.18/07:01:29]#1/0 <-   <LinkPmsConf Date="200318" Time="080130" PathId="1" DefRef1="154" DefRef2
="5.6.10" DefRef3="8.13.3.1"
Cryptogram="FidCryptRBjj9vkBO/j6lljq27sxUgsxRvsfpDMWqVuacJBdvD5CiDyO4d0juWwyA+q5RPZh5kLqv
kmqMVMEwGolgkU8o4xAkxW5ic+ko/frSy3VoFOFp/aaagplbtdvV+vtfj9tQuGnbzfxojfRqbbplRPAsNsMeWdX
Y0sXy2DA4+Iz2QcGJc="/>▯
[03.18/07:01:32] <MessLvl3> ChangeLinkState:Alive
[03.18/07:01:32] <MessLvl3> Monitor security: "Mask security relevant fields for all schemas"
[03.18/07:01:32]#1/0 => <LinkAlive Date="200318" Time="070132"/>
[03.18/07:01:32]#1/0 <-   <LinkAlive Date="200318" Time="070132"/>▯
[03.18/07:01:32]#0/0 ->   <LinkAlive Date="200318" Time="070132"></LinkAlive>▯
[03.18/07:01:32]#0/1 <= <LinkAlive Date="200318" Time="070132"></LinkAlive>
```

🟩 Ref#:0/0 🟩 Link:Alive 🟩 Comm:Sync

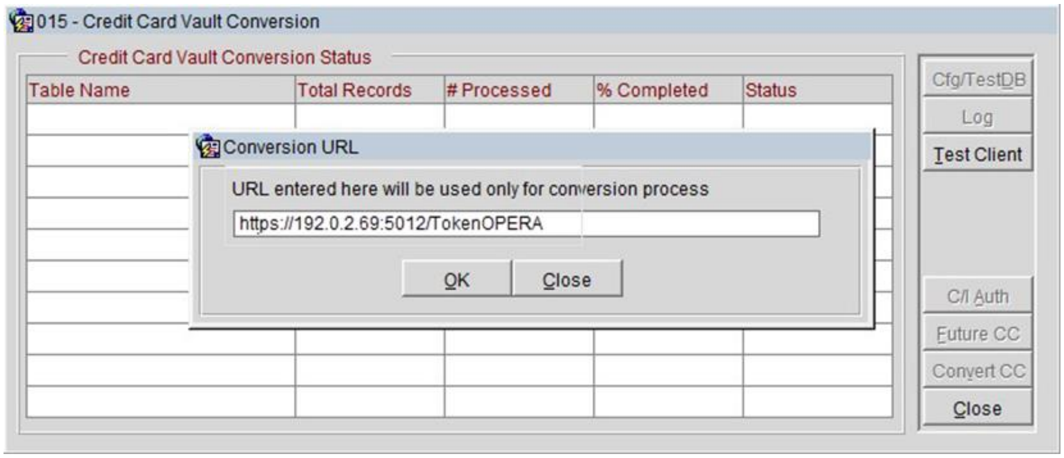
```
          </ElementType>
</Schema>▯
[03.18/07:01:29]#1/0 => <LinkAlive Date="200318" Time="070129"/>
[03.18/07:01:29]#1/0 <-   <LinkAlive Date="200318" Time="070129"/>▯
[03.18/07:01:29]#0/0 ->   <LinkPmsConf Date="200318" Time="080130" PathId="1" RoomPayMethod=""
DefRef1="192|192" DefRef2="5.6.10" DefRef10="UKOPI" Cryptogram="FidCryptDI|0;94"/>▯
[03.18/07:01:29]#0/1 <= <LinkPmsConf Date="200318" Time="080130" PathId="1" RoomPayMethod=""
DefRef1="192|192" DefRef2="5.6.10" DefRef10="UKOPI" Cryptogram="FidCryptDI|0;94" DefRef3
="8.13.3.1"/>
[03.18/07:01:32]#0/0 ->   <LinkAlive Date="200318" Time="070131"/>▯
[03.18/07:01:32]#0/1 <= <LinkAlive Date="200318" Time="070131"/>
[03.18/07:01:32] <MessLvl3> ChangeLinkState:Alive
```

🟩 Ref#:0/0 🟩 Link:Alive 🟩 Comm:Sync

Busi V13.3.1 | Action V13.3.1 | ComEx V13.3.1 | C:\Fidelio\IFC8\Ifc8Config.Xml | 7:02:09 AM

Perform a Tokenization

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



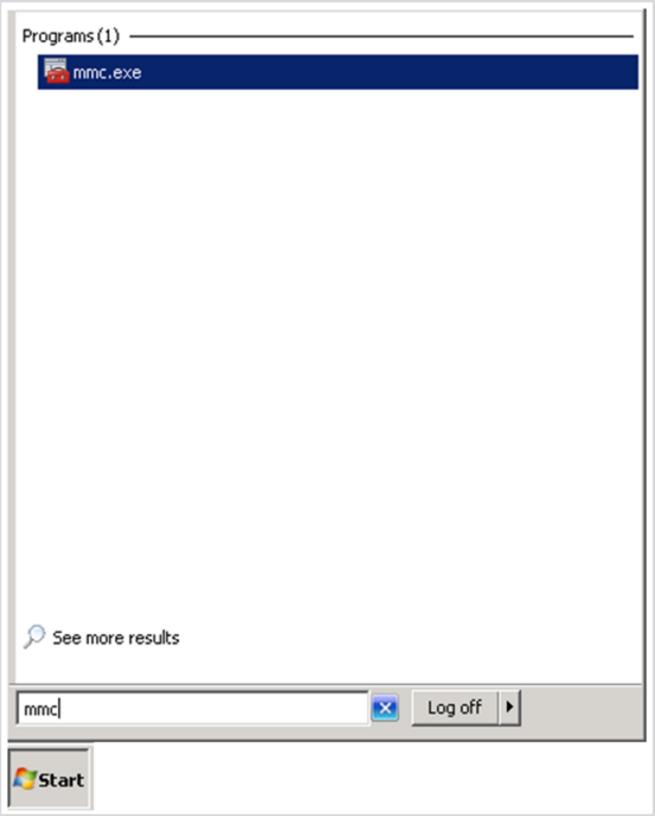
URL entered here will be used only for conversion process

https://192.0.2.69:5012/TokenOPERA

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

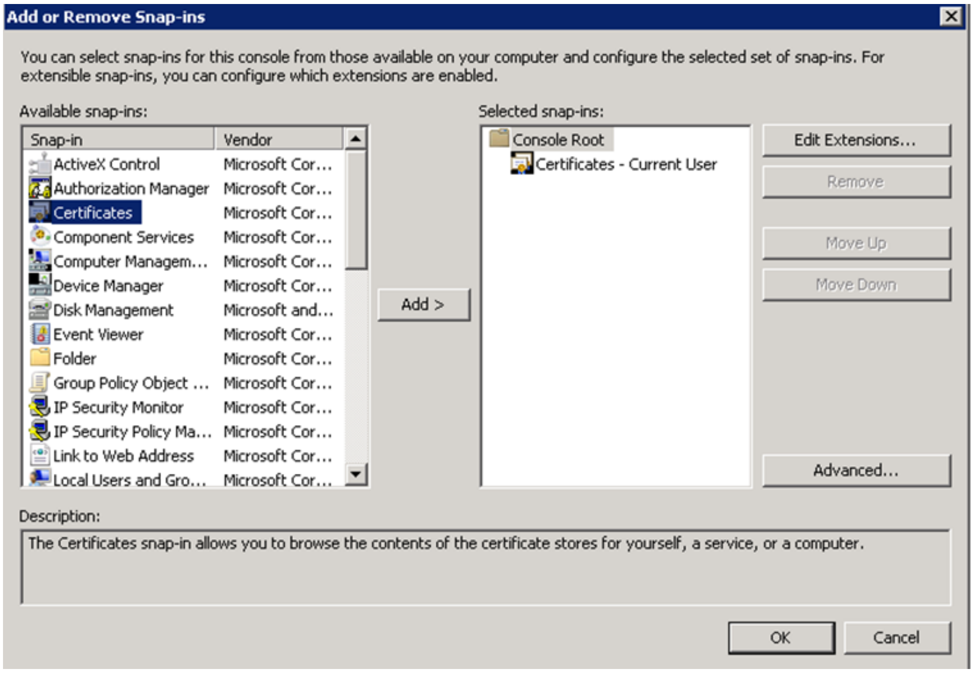
Certificate Import using Microsoft Management Console

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



mmc

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



Add or Remove Snap-ins

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.

Available snap-ins:

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...

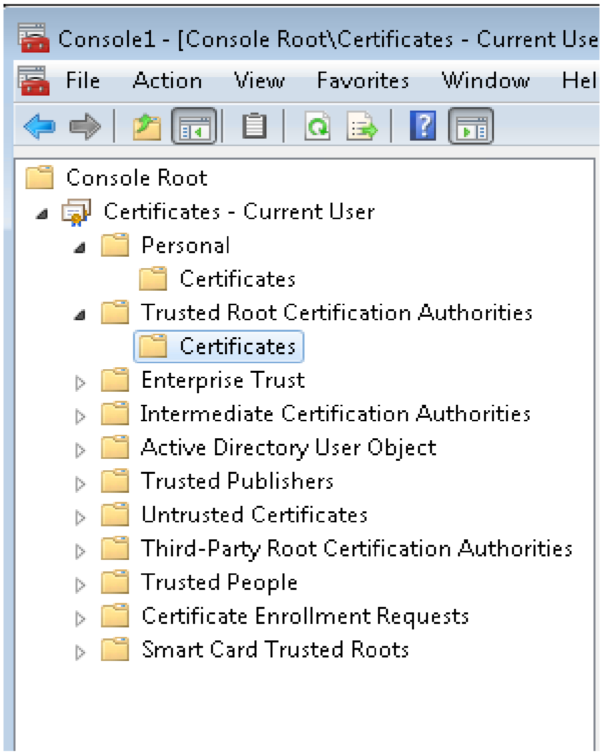
Selected snap-ins:

Console Root
Certificates - Current User

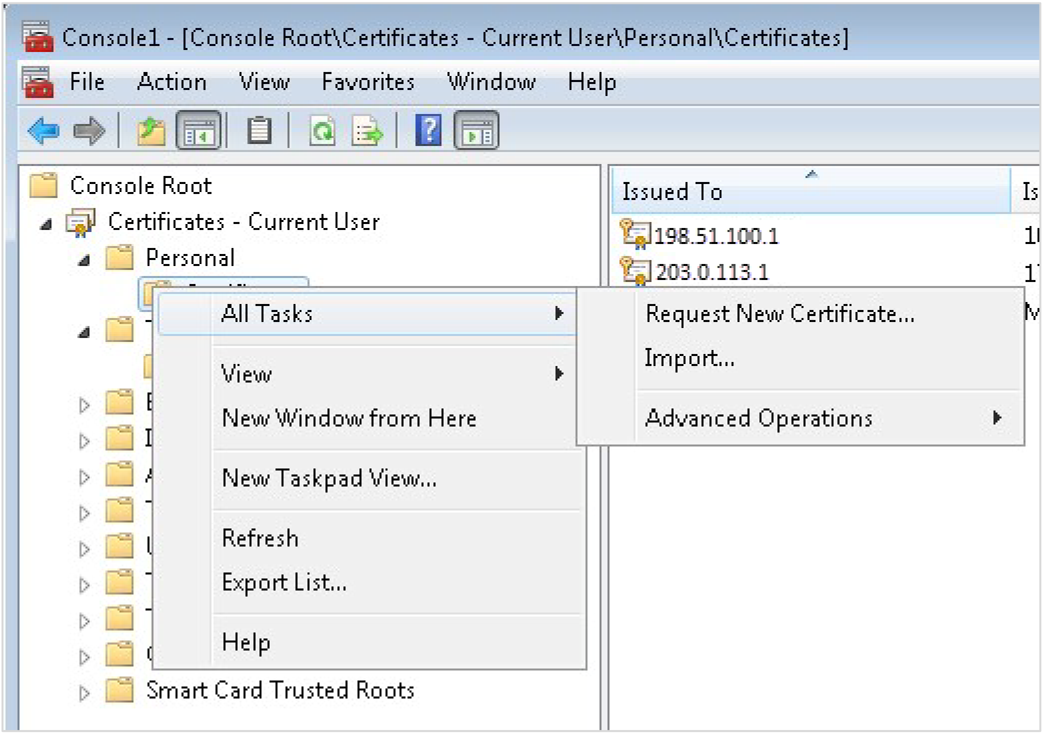
Description:

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 then click **Next**.

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

4

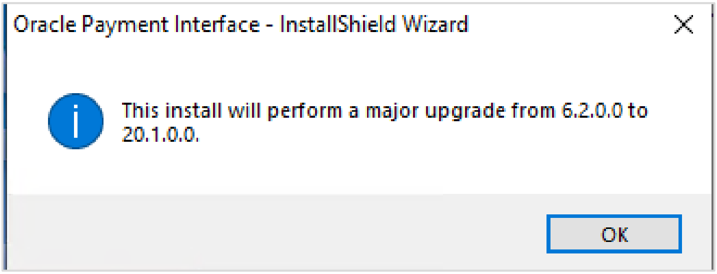
Upgrading the OPI

VERY IMPORTANT: Read and follow the upgrade directions.

> **NOTE:**
>
> OPI 6.1 cannot be upgraded to OPI 20.1. You will need to upgrade OPI 6.1 to either 6.2 or 19.1, before upgrading it to 20.1.

Upgrading OPI 6.2.0.0 to 20.1.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.1.0.0.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**.

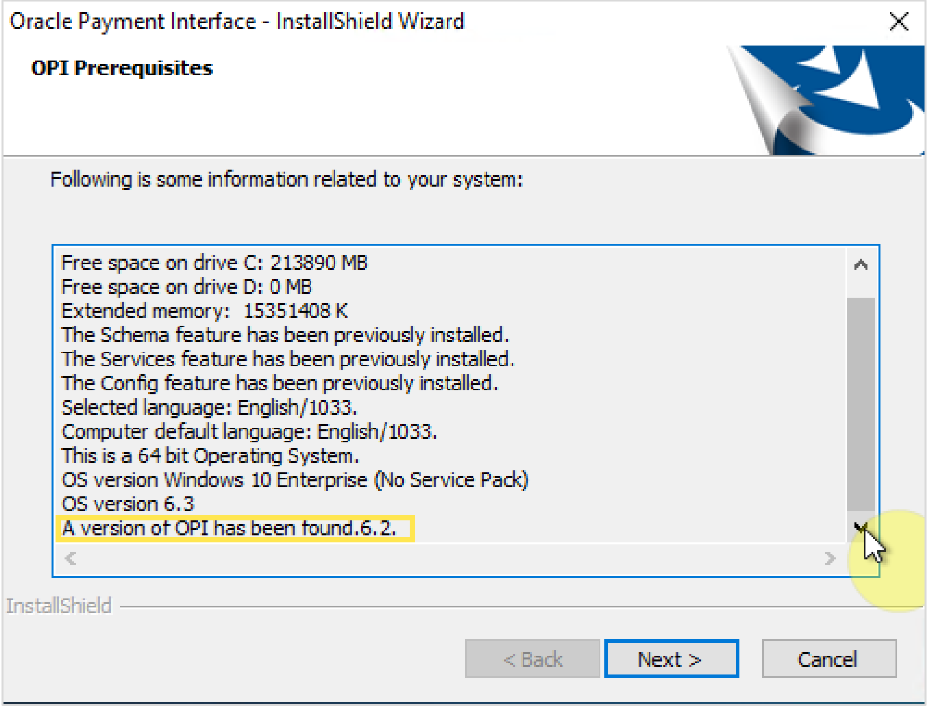


Oracle Payment Interface - InstallShield Wizard

This install will perform a major upgrade from 6.2.0.0 to 20.1.0.0.

5. Click **Next**.

   Ensure all the prerequisites for the OPI installation are met.



Oracle Payment Interface - InstallShield Wizard

OPI Prerequisites

Following is some information related to your system:

```
Free space on drive C: 213890 MB
Free space on drive D: 0 MB
Extended memory:  15351408 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 10 Enterprise (No Service Pack)
OS version 6.3
A version of OPI has been found.6.2.
```

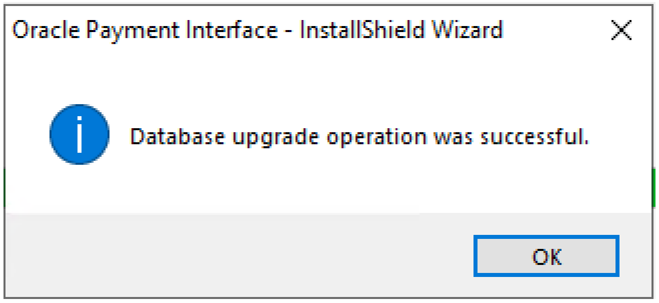
6. Choose a Destination Location. Accept the default installation location or click **Change**… to choose a different location.

7. Click **Next**.

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

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

9. Click **OK**.



Oracle Payment Interface - InstallShield Wizard

Database upgrade operation was successful.

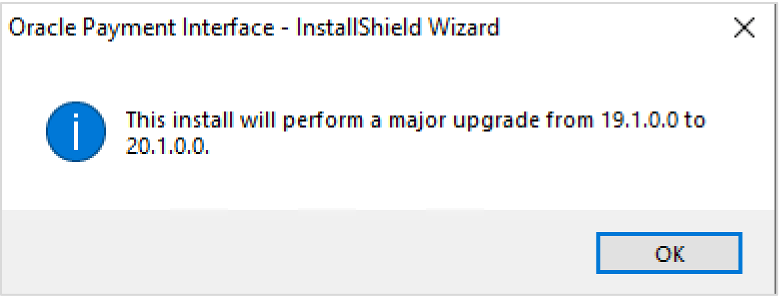
10. Enter the **Host** and **Port** that should be used to connect to the OPI Config Service for the Merchant Configuration.

11. Once 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 20.1.0.0

1. Right-click **OraclePaymentInterfaceInstaller_20.1.0.0.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**.

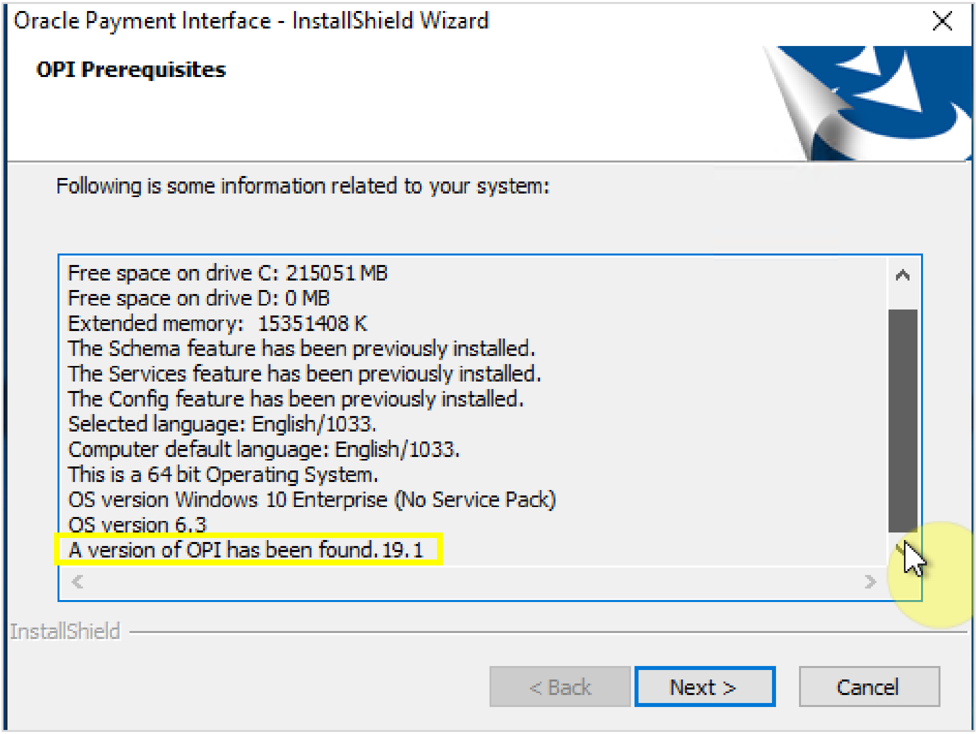


Oracle Payment Interface - InstallShield Wizard

This install will perform a major upgrade from 19.1.0.0 to 20.1.0.0.

5. Click **Next**.

   Ensure all the prerequisites for the OPI installation are met.



Oracle Payment Interface - InstallShield Wizard

OPI Prerequisites

Following is some information related to your system:

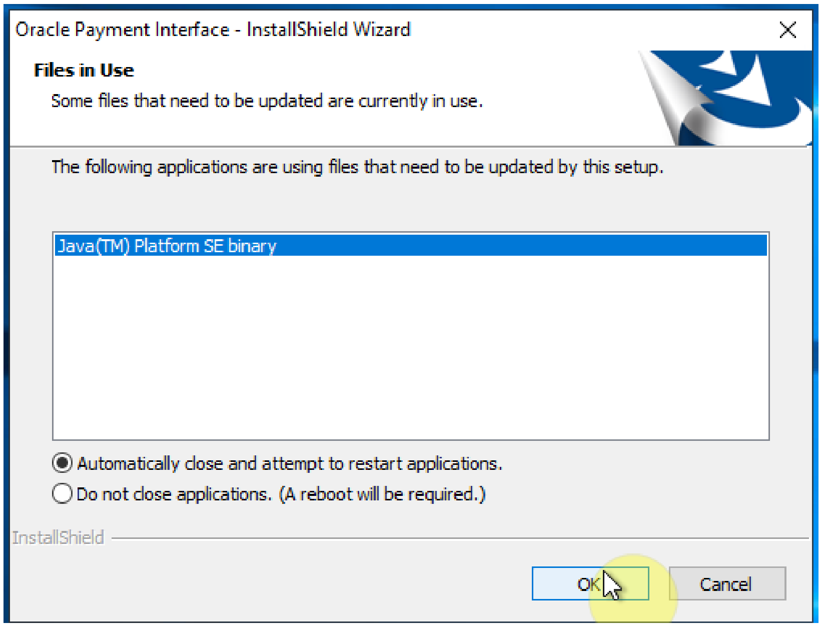
```
Free space on drive C: 215051 MB
Free space on drive D: 0 MB
Extended memory:  15351408 K
The Schema feature has been previously installed.
The Services feature has been previously installed.
The Config feature has been previously installed.
Selected language: English/1033.
Computer default language: English/1033.
This is a 64 bit Operating System.
OS version Windows 10 Enterprise (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 displays.

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

   The installer prompts some files need to be updated that are currently in use. Select **Automatically close and attempt to restart applications**.



Oracle Payment Interface - InstallShield Wizard

Files in Use

Some files that need to be updated are currently in use.

The following applications are using files that need to be updated by this setup.

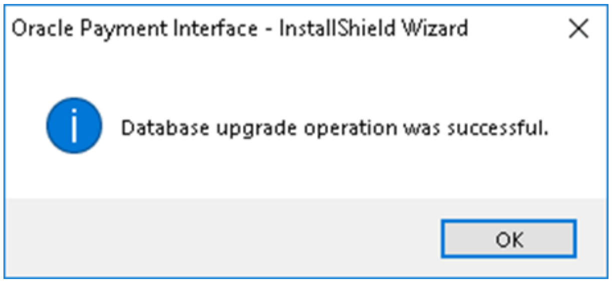
Java(TM) Platform SE binary

● Automatically close and attempt to restart applications.

○ Do not close applications. (A reboot will be required.)

9. Click **OK** to proceed with the installation.

10. Click **OK**.



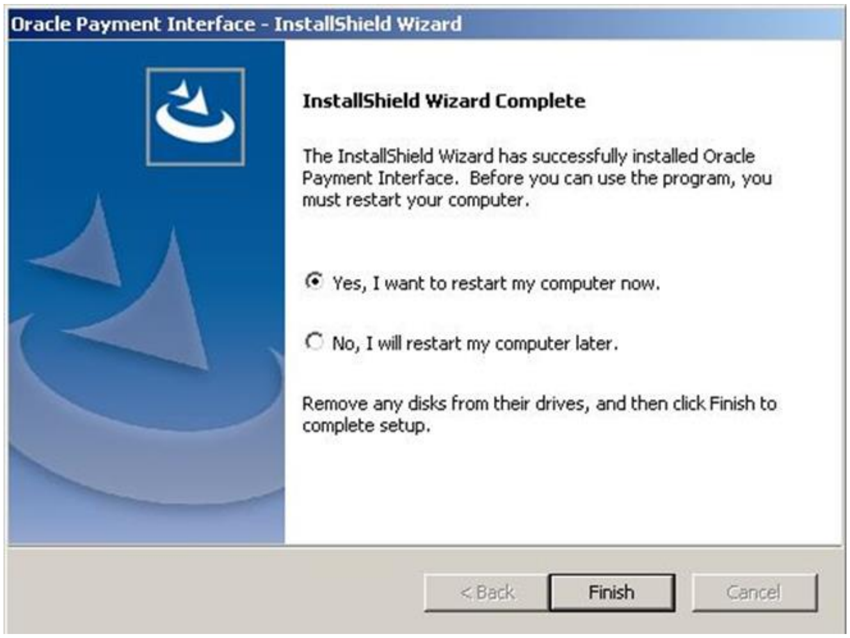
Oracle Payment Interface - InstallShield Wizard

Database upgrade operation was successful.

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

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

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



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.