Oracle® Payment Interface

Oracle Hospitality Suite8 Property Management System Installation Guide

Release 19.1
F19823-01
July 2019

Oracle Payment Interface Oracle Hospitality Suite8 Property Management System Installation Guide, Release 19.1

F19823-01

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Purpose

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

Audience

This document is intended to cover the additional steps required to setup OPI to handle the On Premise Token Exchange functionality.

This document covers only the configuration of the additional On Premise Token Exchange functionality, it does not cover in detail, installation of the OPI software and IFC8 merchant configuration, separate documentation already exists to cover this.

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 and any associated log files
- Screenshots of each step you take

Documentation

Product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/

Revision History

Date	Description of Change
March 2019	Initial publication.
June 2019	• Updated formatting and cover page with new template. • Updated content and screenshots for OPI 19.1 release.
July 2019	Updated security bugs in few chapters.

1

Pre-Installation Steps

Consider the following guidelines before installing Oracle Payment Interface (OPI):

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

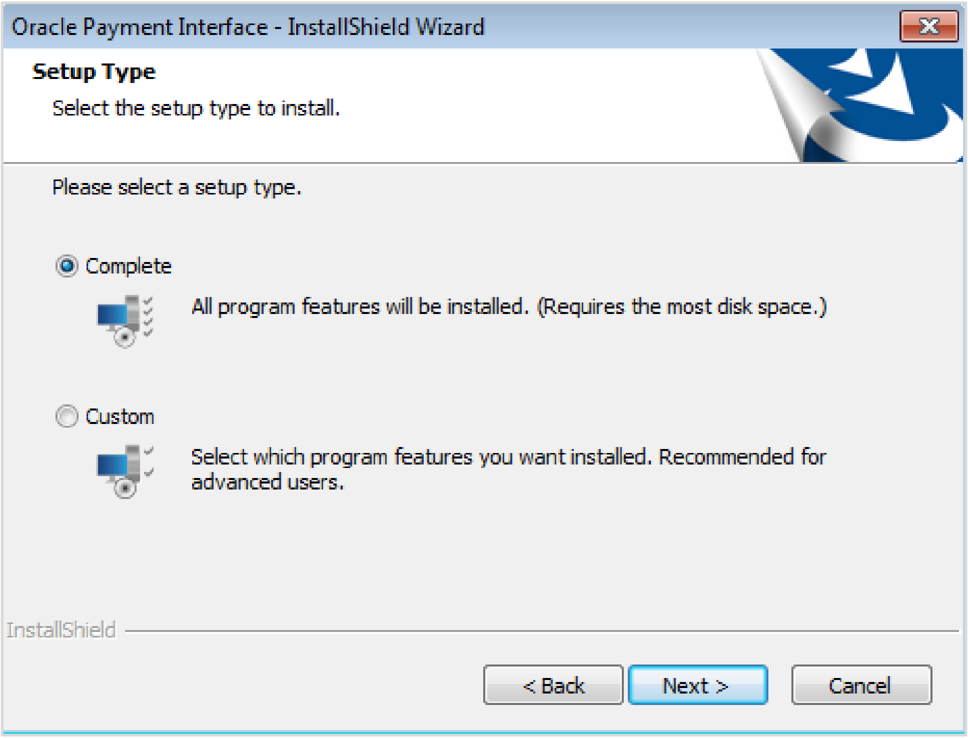
- Suite8 Property Management System release 8.12.0.0 is the minimum release you can use to integrate with OPI.
- OPI 19.1 does not install a database. If doing a clean install of OPI, a database must be installed first.
- Upgrading to OPI 19.1 from OPI 6.1 and higher is supported but MPG versions are not supported. Prior to upgrading from OPI 6.1 to OPI 19.1 all credit card transactions must be finalized and closed as the schema upgrade will not include the migration of old transaction data to OPI side.
- Any previous version of MPG should be uninstalled prior to installing OPI 19.1.
- The application requires Microsoft.NET Framework version 4.0 or higher.
- OPI requires at least 6 GB of free disk space & you must install OPI as a System Administrator.

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. Copy **OraclePaymentInterfaceInstaller_19.1.0.0.exe** to the Server and double-click it to launch the install.
2. Select a language, and then click **OK**.
3. Click **Next** on the Welcome to the InstallShield Wizard for Oracle Payment Interface screen.
4. Click **Next** on the OPI Prerequisites screen.



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.)

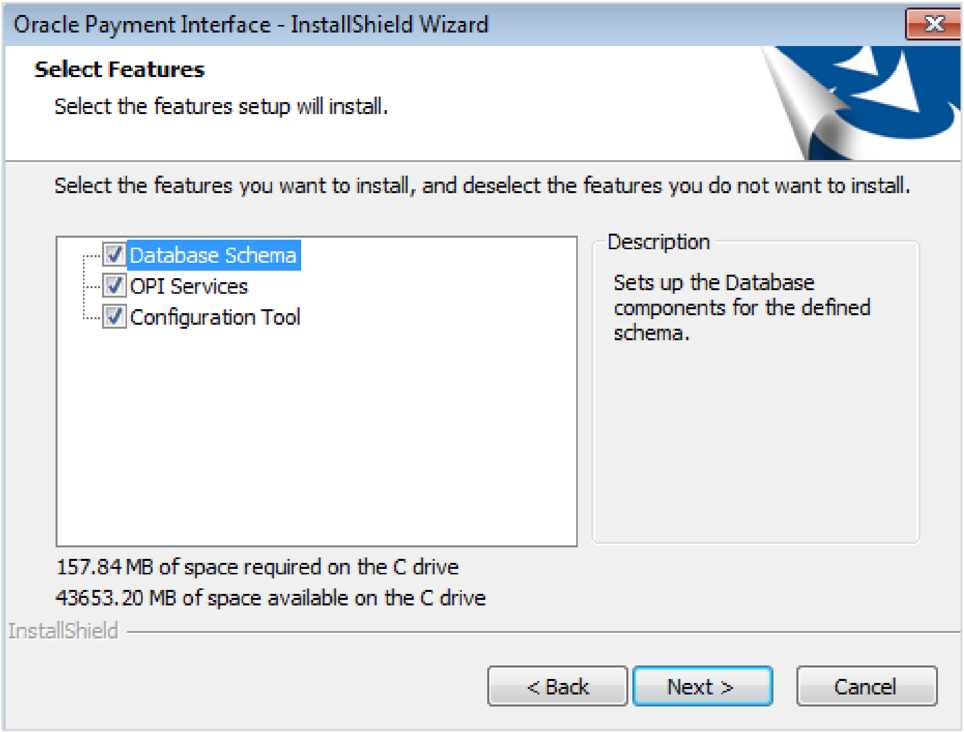
○ Custom

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

The Setup Type screen appears.

- **Complete**: All program features will be installed.
- **Custom**: Select which program features you want installed. Recommended for advanced users only.

5. Make a selection (only for Custom install), and then click **Next**. If you select Complete Install, it will go to the Step 7 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.

- ☑ Database Schema
- ☑ OPI Services
- ☑ Configuration Tool

Description

Sets up the Database components for the defined schema.

157.84 MB of space required on the C drive
43653.20 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 three of these features must be installed. It is just a matter of whether they are all installed on the same computer or on separate computers.

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

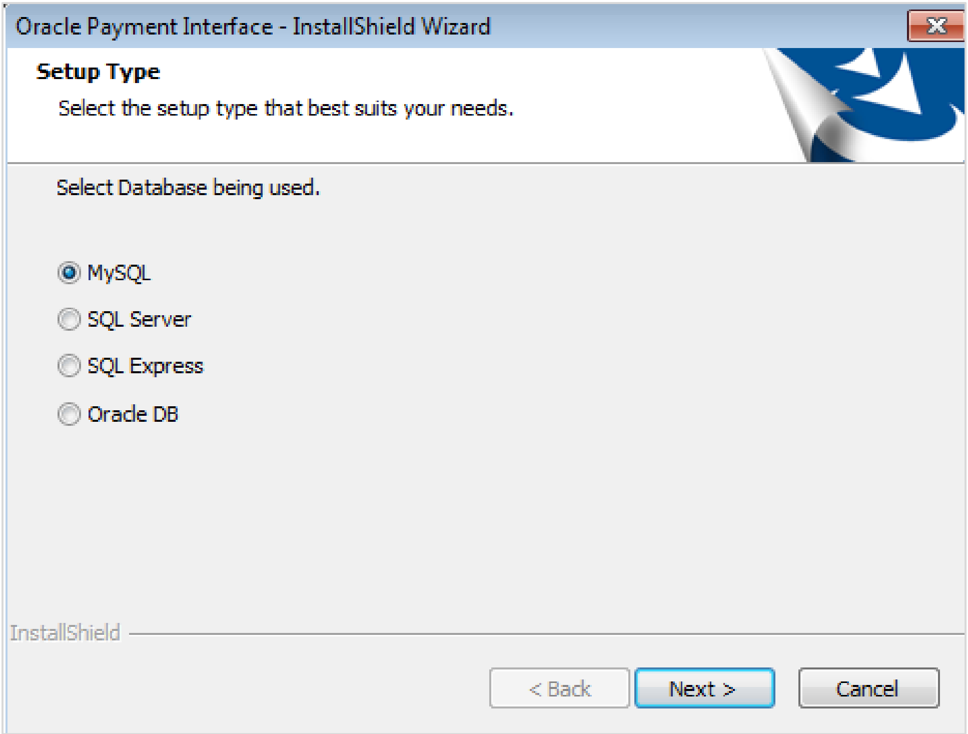
   The Choose Destination Location screen appears.

7. Accept the default installation location or click **Change**… to choose a different location, and then click **Next**.

8. Click **Install** on the Ready to Install the Program screen.

   The Setup Status screen displays for a few minutes.

9. The Setup Type screen appears.



Oracle Payment Interface - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Select Database being used.

● MySQL

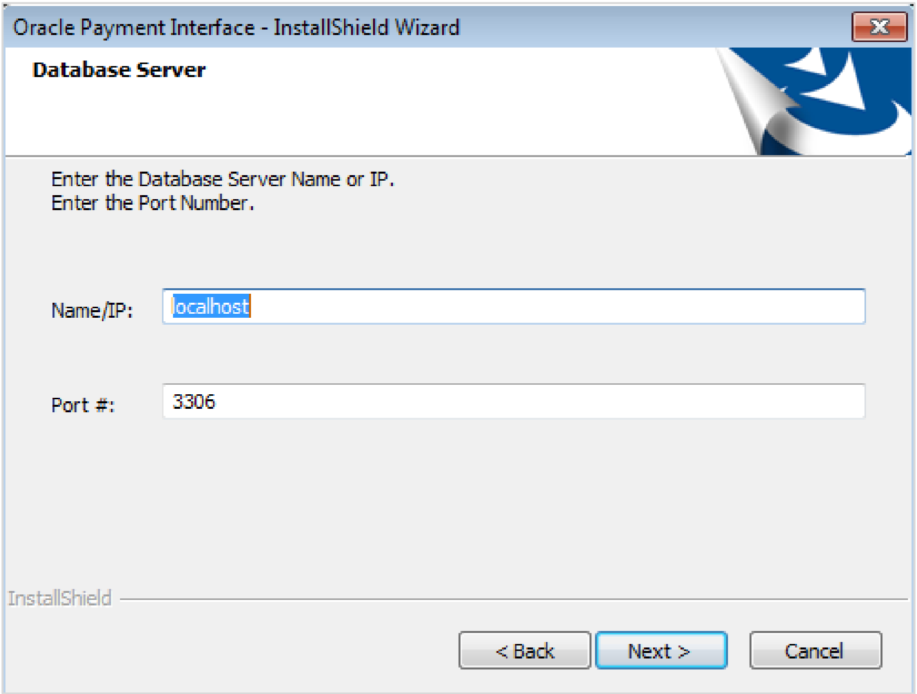
○ SQL Server

○ SQL Express

○ Oracle DB

10. Select the database type being used, and then click **Next**.

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



Oracle Payment Interface - InstallShield Wizard

Database Server

Enter the Database Server Name or IP.
Enter the Port Number.

Name/IP: localhost

Port #: 3306

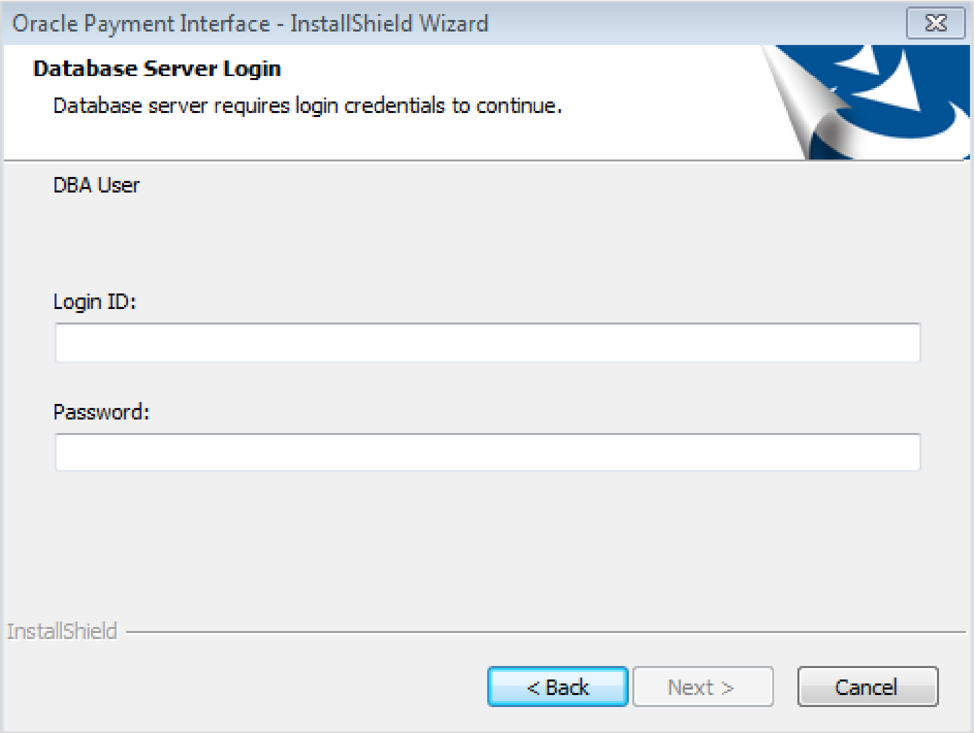
The Database Server screen appears.

11. **The Name/IP**: field defaults to localhost. This should be left as localhost if the OPI database is installed on the same computer. If the database is installed on another computer, the Name or IP address of that machine should be entered here.

> **NOTE:**
>
> If the database type is MySQL, and you cannot use localhost for the Name/IP field, then some commands must be run manually on that MySQL database before proceeding. See **Granting Permission in MySQL** section in the Oracle Payment Interface Installation and Reference Guide for instructions. Setup will not complete if this is not done.

12. Accept the default **Port #** of 3306 (for MySQL), and then click **Next**.

    The Database Server Login screen appears.



Oracle Payment Interface - InstallShield Wizard

Database Server Login

Database server requires login credentials to continue.

DBA User

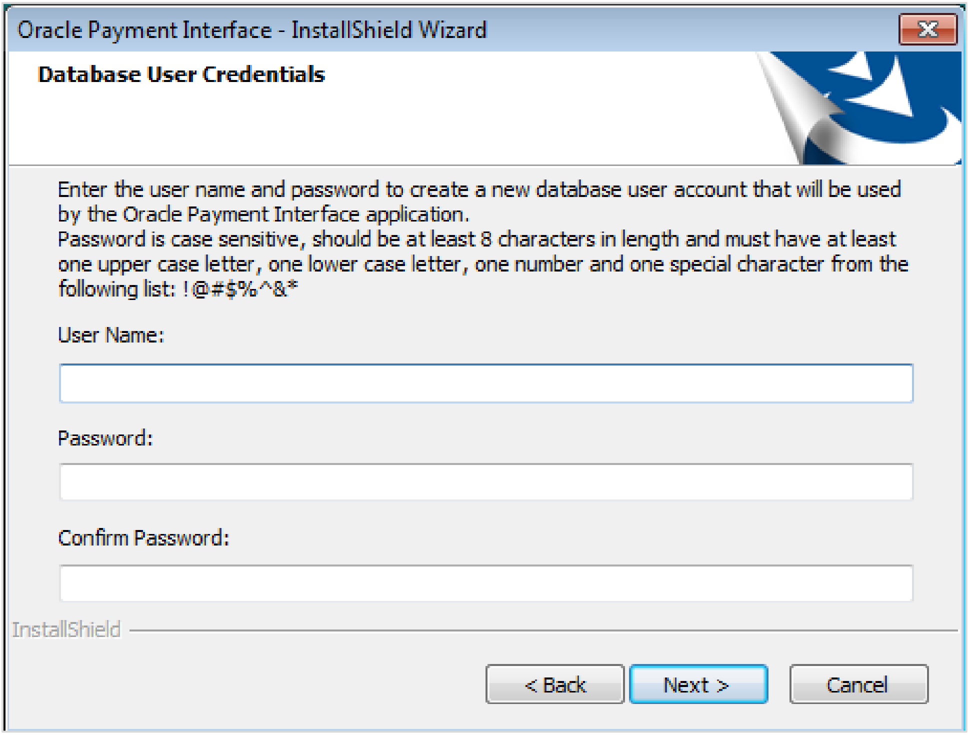
Login ID:

Password:

13. Enter the credentials for the DBA user of the database type selected, and then click **Next**.

- For MySQL the Login ID: = root
- For other database types the DBA user name/Login ID may be different.
- Enter the correct password for the DBA user.

The Database User Credentials screen appears.



Oracle Payment Interface - InstallShield Wizard

Database User Credentials

Enter the user name and password to create a new database user account that will be used by the Oracle Payment Interface application.
Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*

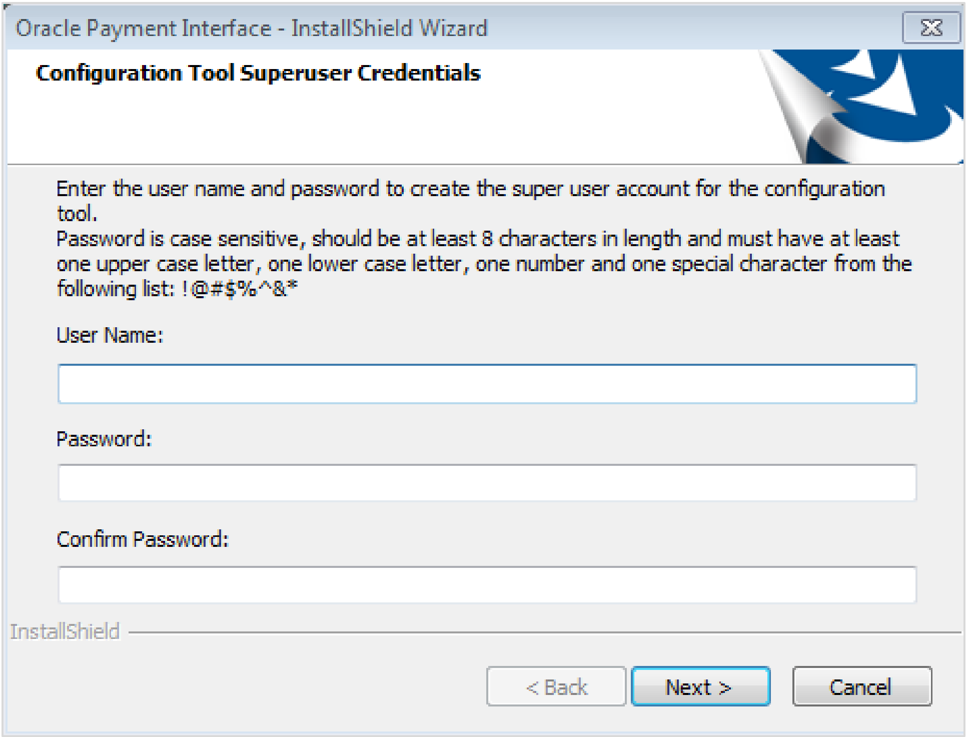
User Name:

Password:

Confirm Password:

14. **User Name**: Create a new user.
15. **Password**: Create a password. Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list:!@#$%^&*.
16. Confirm the password, and then click **Next**.
17. Click **OK** on the Database connection successful dialog.
18. Click **OK** on the Database Configuration operation successful dialog.

    The Configuration Tool Superuser Credentials screen appears.



Oracle Payment Interface - InstallShield Wizard

Configuration Tool Superuser Credentials

Enter the user name and password to create the super user account for the configuration tool.
Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*

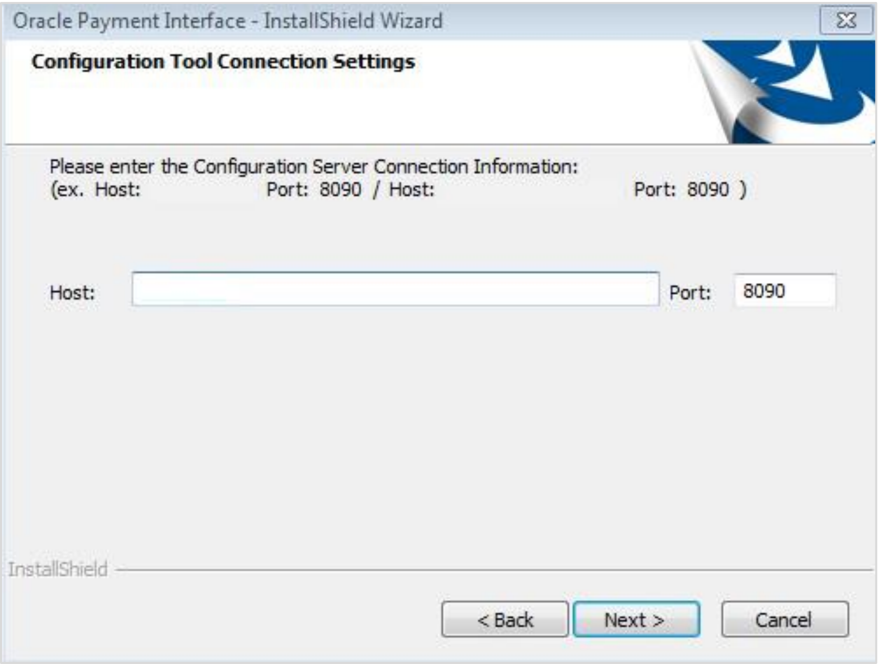
User Name:

Password:

Confirm Password:

19. **User Name**: This can be any user name. It does not have to be a Windows account user.
20. **Password**: Create a password. Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list:!@#$%^&*
21. Confirm the password, and then click **Next**.
22. Click **OK** on the Create SuperUser operation successful dialog.

    The Configuration Tool Connection Settings screen appears.



Oracle Payment Interface - InstallShield Wizard

Configuration Tool Connection Settings

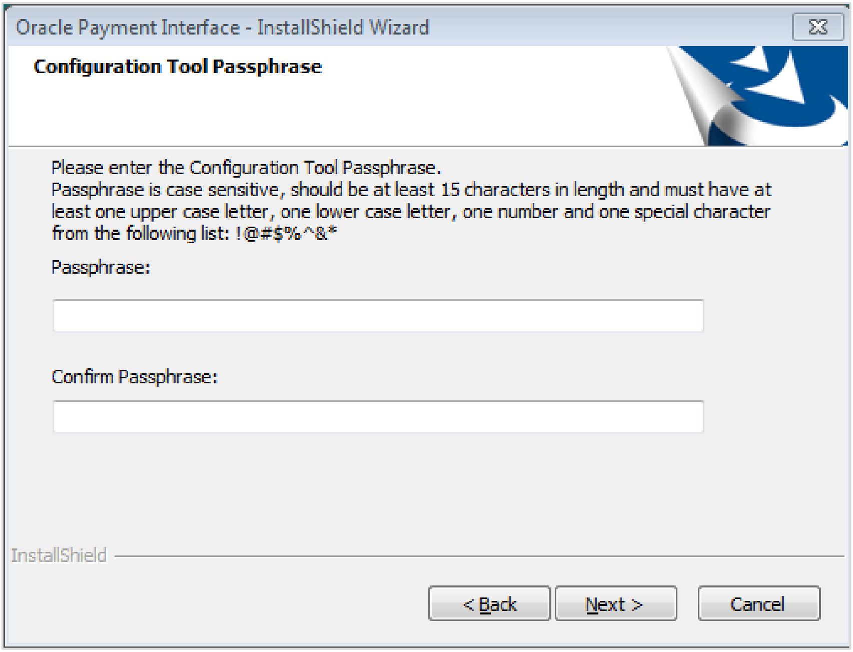
Please enter the Configuration Server Connection Information:
(ex. Host: Port: 8090 / Host: Port: 8090)

Host:
Port: 8090

- **Host**: Enter the IP address or server name of the PC where the OPI Config Service is installed. This will be the PC where you selected “OPI Services” to be installed.
- Leave the default Port of 8090.

23. Click **Next**.

    The Configuration Tool Passphrase screen appears.



Oracle Payment Interface - InstallShield Wizard

Configuration Tool Passphrase

Please enter the Configuration Tool Passphrase.
Passphrase is case sensitive, should be at least 15 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*

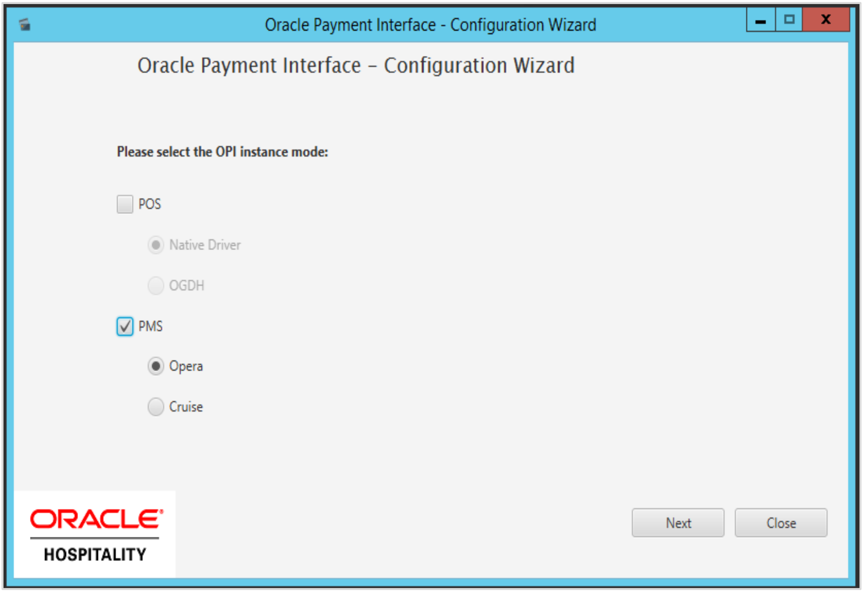
Passphrase:

Confirm Passphrase:

24. **Passphrase**: The passphrase is case sensitive, should be at least 15 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*.

25. Enter a passphrase, confirm it, and then click **Next**.

    After a brief pause, the Configuration Wizard launches.



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

Please select the OPI instance mode:

□ POS

○ Native Driver

○ OGDH

☑ PMS

● Opera

○ Cruise

26. Select **PMS**, select **Opera**, and then click **Next**.

    The OPI Interface screen appears.

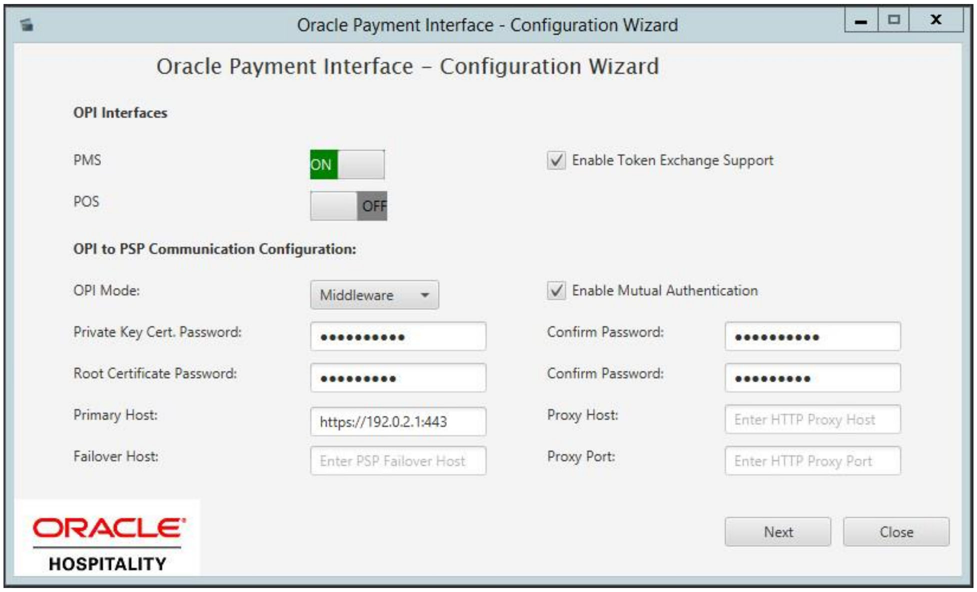
27. Turn **PMS** on, and select the **Enable Token Exchange Support** box. The Token Exchange functionality is separate to the IFC8 merchant functionality.

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.

- 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 IP address if Middleware mode is selected. If Terminal mode is selected, then OPI configuration will populate another window in further steps to input Workstation ID and IP address.



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

OPI Interfaces

PMS: ON

POS: OFF

☑ Enable Token Exchange Support

OPI to PSP Communication Configuration:

OPI Mode: Middleware

☑ Enable Mutual Authentication

Private Key Cert. Password: ●●●●●●●●●●

Confirm Password: ●●●●●●●●●●

Root Certificate Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

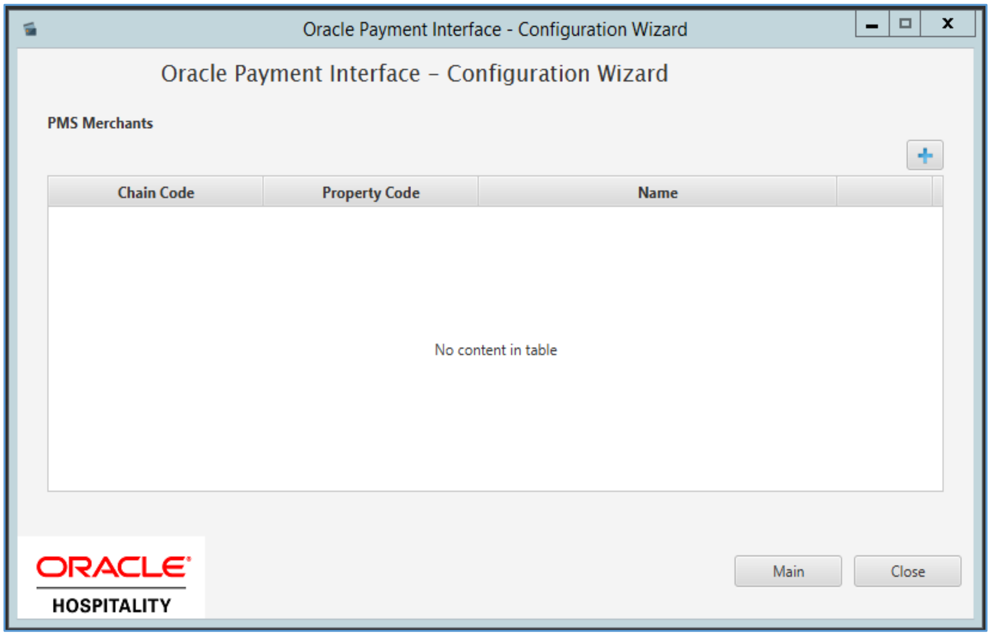
Primary Host: https://192.0.2.1:443

Proxy Host: Enter HTTP Proxy Host

Failover Host: Enter PSP Failover Host

Proxy Port: Enter HTTP Proxy Port

28. Click the blue + 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

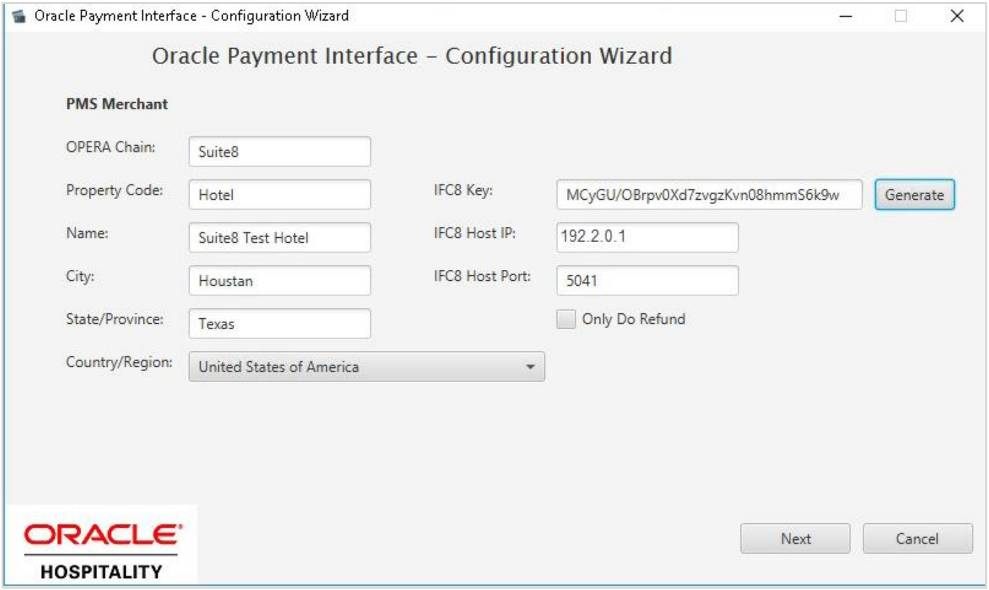
No content in table

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

- The *Suite8 Vault Chain Code & Property Code*; will form the **SiteId** value in the Token request messages.
- 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|xxxxxxxxxxxxxxxxxxxxxxxxx
- Enter the **IFC8 IP address** and **port** number for the Hotel Property Interface (IFC8) server.
- Enter the **Merchant name**, **city**, and **country** information.

- Select the option of **Only Do Refund** if you want to disable differentiating between void and refund from Opera.
- Click **Next**.

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

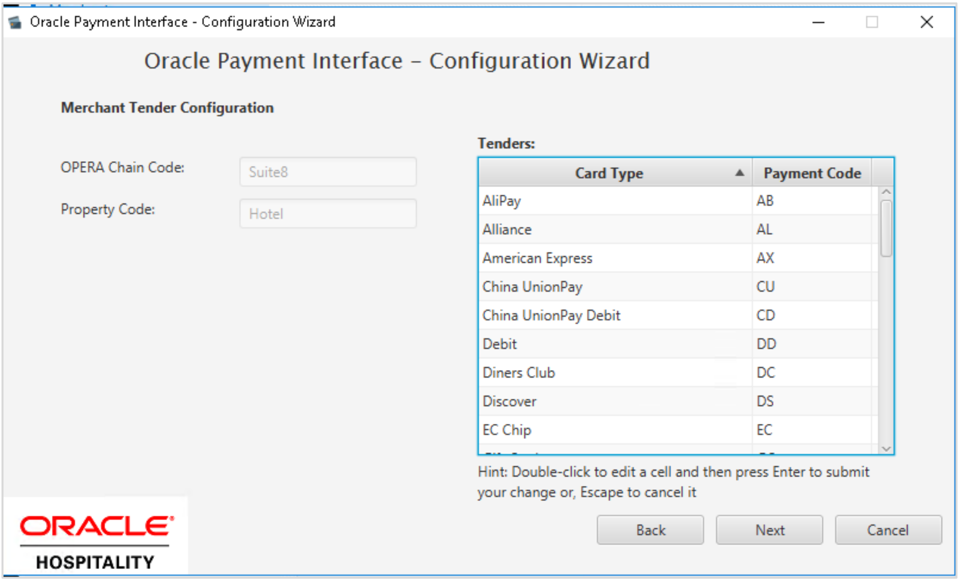


Oracle Payment Interface – Configuration Wizard

PMS Merchant

OPERA Chain:	Suite8		
Property Code:	Hotel	IFC8 Key:	MCyGU/OBrpv0Xd7zvgzKvn08hmmS6k9w
Name:	Suite8 Test Hotel	IFC8 Host IP:	192.2.0.1
City:	Houstan	IFC8 Host Port:	5041
State/Province:	Texas		□ Only Do Refund
Country/Region:	United States of America		

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



Oracle Payment Interface – Configuration Wizard

Merchant Tender Configuration

OPERA Chain Code: Suite8

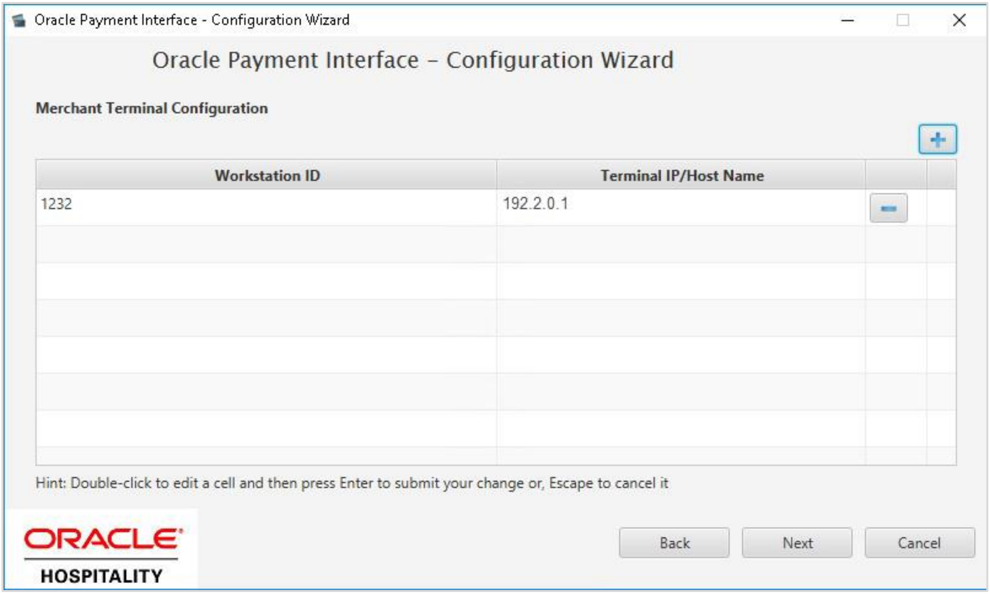
Property Code: Hotel

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

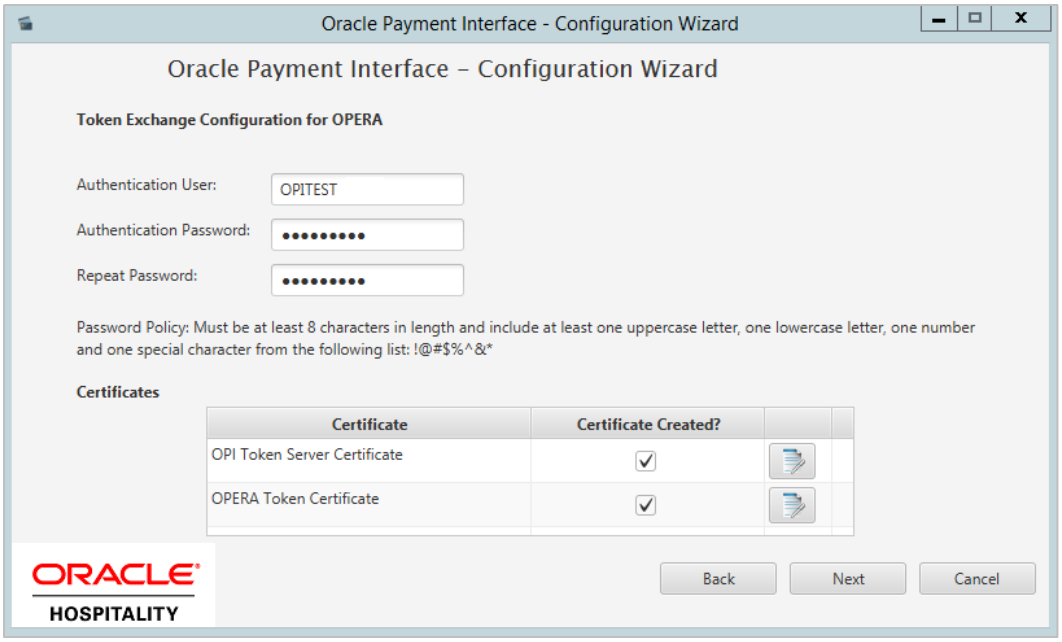
Merchant Terminal Configuration

Workstation ID	Terminal IP/Host Name
1232	192.2.0.1

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

31. The top half of the Token Exchange Configuration screen allows you to configure the Header Authentication credentials used in communications from Suite8→OPI.

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



Oracle Payment Interface - Configuration Wizard

Token Exchange Configuration for OPERA

Authentication User: OPITEST

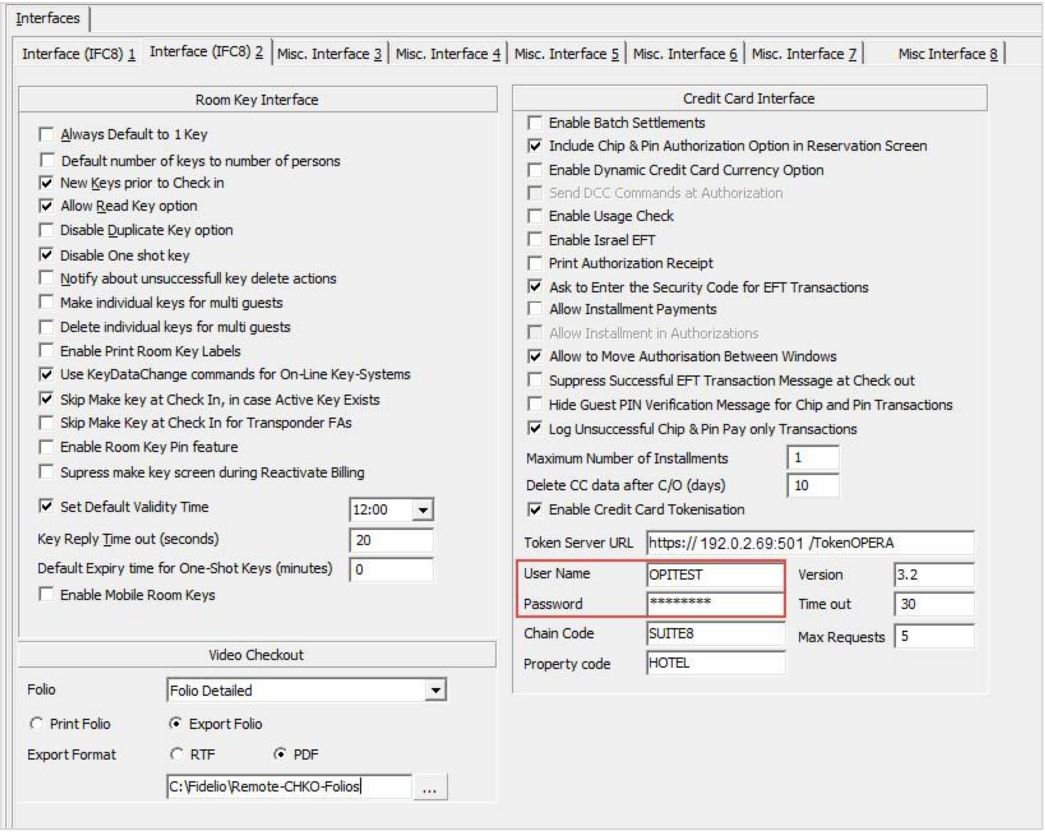
Authentication Password: ••••••••••

Repeat 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: !@#$%^&*

Certificates

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



Interfaces

Interface (IFC8) 1 | Interface (IFC8) 2 | Misc. Interface 3 | Misc. Interface 4 | Misc. Interface 5 | Misc. Interface 6 | Misc. Interface 7 | Misc Interface 8

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

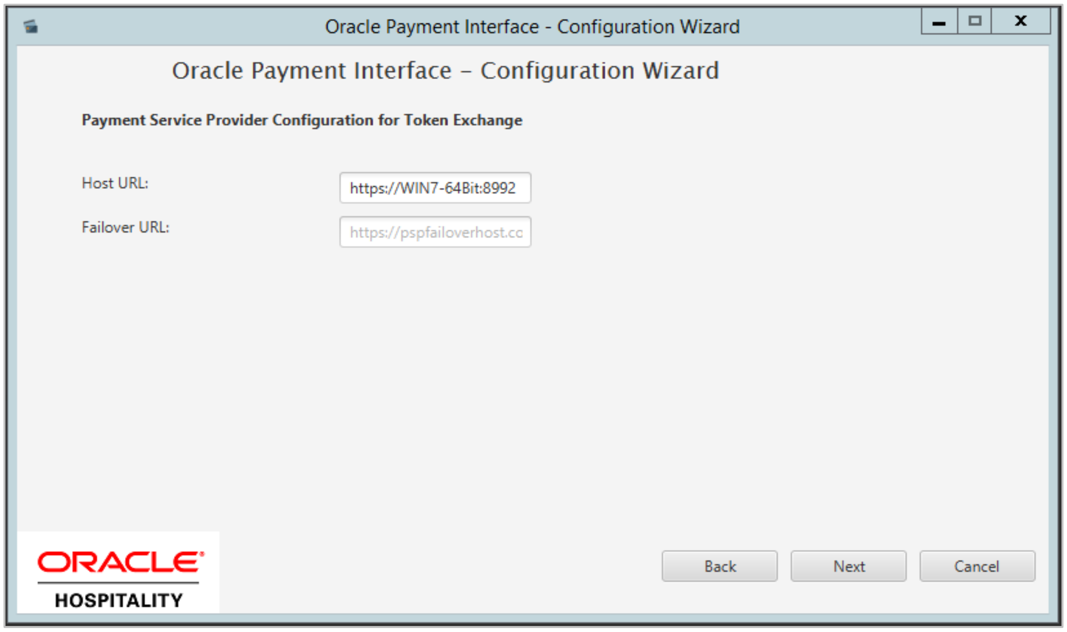
- Folio: Folio Detailed
- ○ Print Folio ● Export Folio
- Export Format: ○ RTF ● PDF
- C:\Fidelio\Remote-CHKO-Folios ...

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: OPITEST
- Password: ********
- Version: 3.2
- Time out: 30
- Chain Code: SUITE8
- Max Requests: 5
- Property code: HOTEL

- Certificates are explained in the Certificates section.

32. 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: https://WIN7-64Bit:8992

Failover URL: https://pspfailoverhost.cc

33. Click **Finish** to restart.

Certificates

OPI on Premise Token Exchange requires three 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

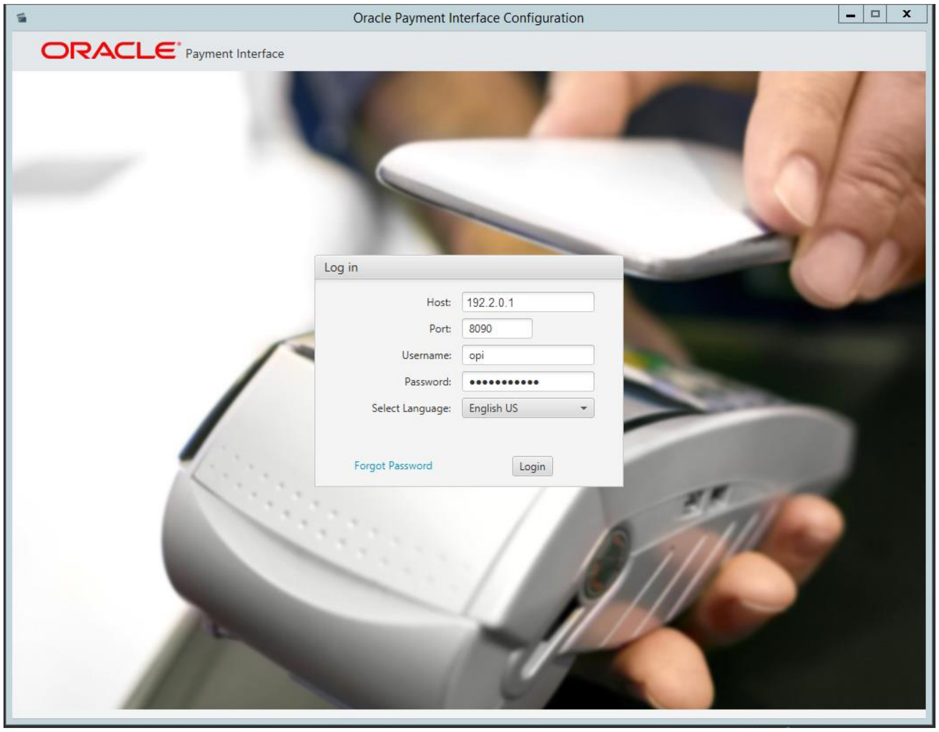
The communication from OPI to the PSP for token exchange uses HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed at PSP (server side) for HTTPS communication, PSP is also expected to provide a client side certificate to be deployed at OPI side. OPI will present this 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 at 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 at 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\v19.1\Config\LaunchConfiguration.bat**
2. Log in as the Super user you created during OPI installation.



Host: 192.2.0.1

Port: 8090

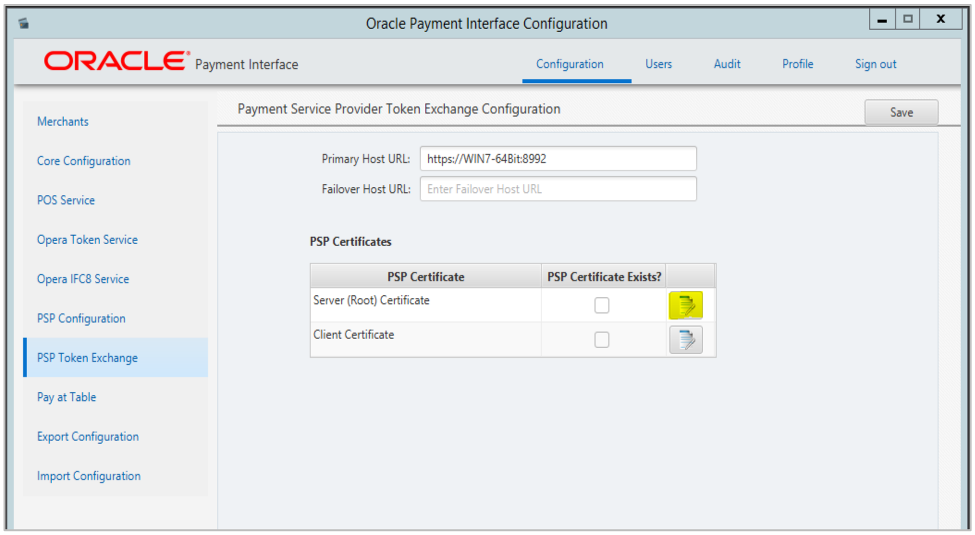
Username: opi

Password: •••••••••••

Select Language: English US

Handling the Root Certificate File by OPI Configuration Tool.

1. Select **PSP Token Exchange**, and then edit the **Server (Root) Certificate**.



Payment Service Provider Token Exchange Configuration

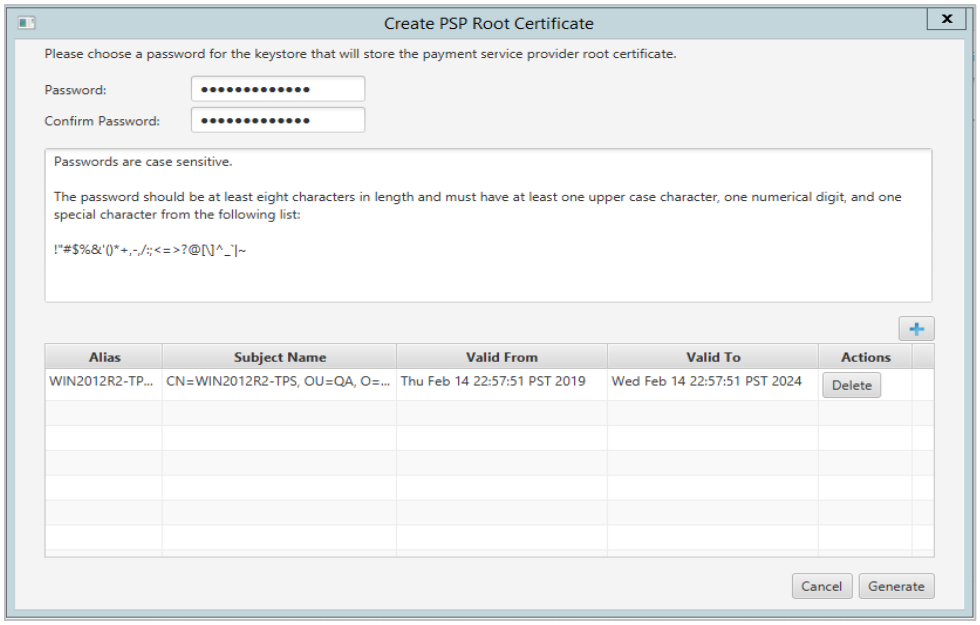
Primary Host URL: https://WIN7-64Bit:8992

Failover Host URL: Enter Failover Host URL

PSP Certificates

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

2. Enter the password for the keystore, and then browse to the location of the certificate you wish to import from add icon available or drag and drop the .cer or.crt.



Create PSP Root Certificate

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

Password: ••••••••••••••

Confirm Password: ••••••••••••••

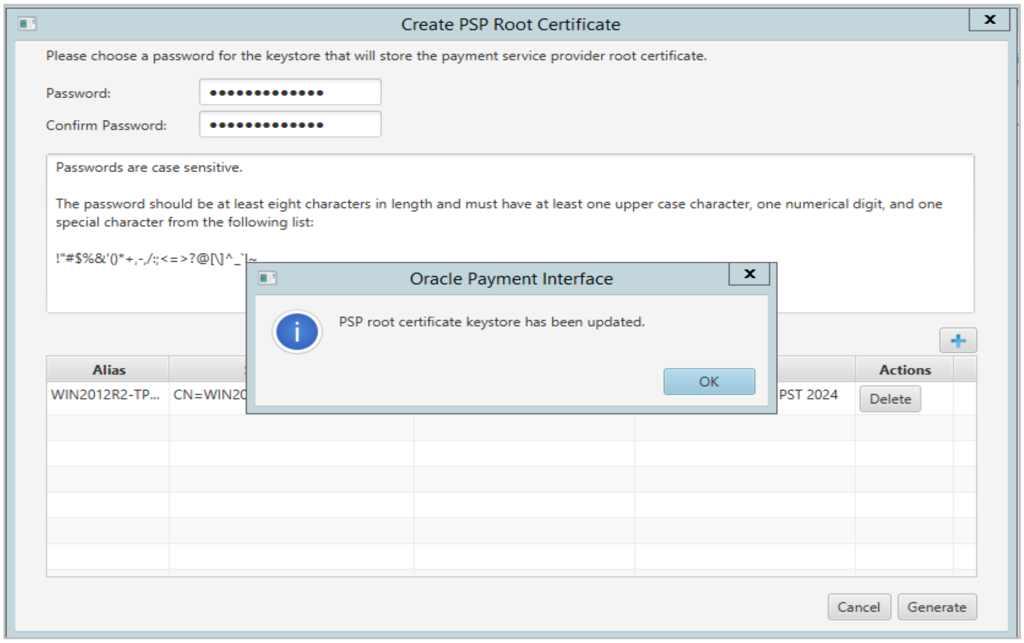
Passwords are case sensitive.

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:

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

Alias	Subject Name	Valid From	Valid To	Actions
WIN2012R2-TP...	CN=WIN2012R2-TPS, OU=QA, O=...	Thu Feb 14 22:57:51 PST 2019	Wed Feb 14 22:57:51 PST 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:

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

Oracle Payment Interface

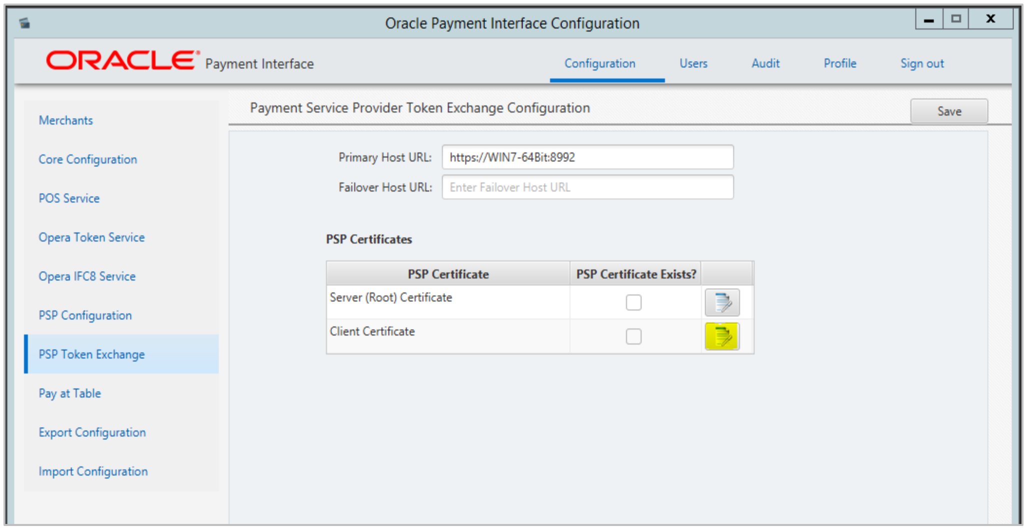
PSP root certificate keystore has been updated.

Alias				Actions
WIN2012R2-TP...	CN=WIN2C		PST 2024	Delete

OPI_PSP_1Root is created under \OraclePaymentInterface\v19.1\Services\OPI\key

Handling the Client Side Certificate

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



Payment Service Provider Token Exchange Configuration

Primary Host URL: https://WIN7-64Bit:8992

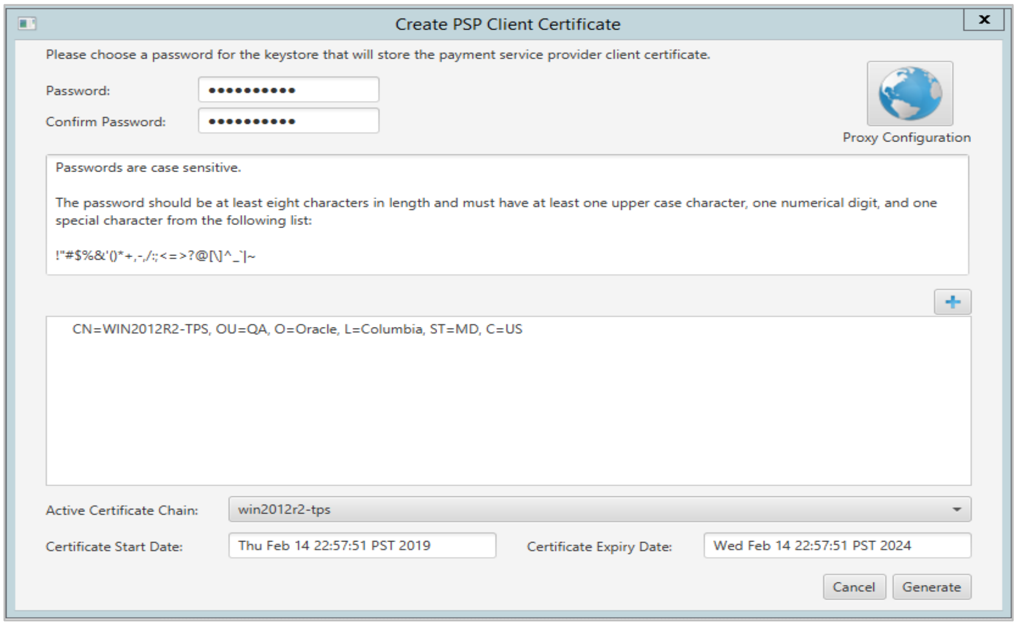
Failover Host URL: Enter Failover Host URL

PSP Certificates

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

2. Enter the password for the keystore then browse to the location of the certificate you wish to import from add icon available or 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 will vary depending on what the PSP 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:

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

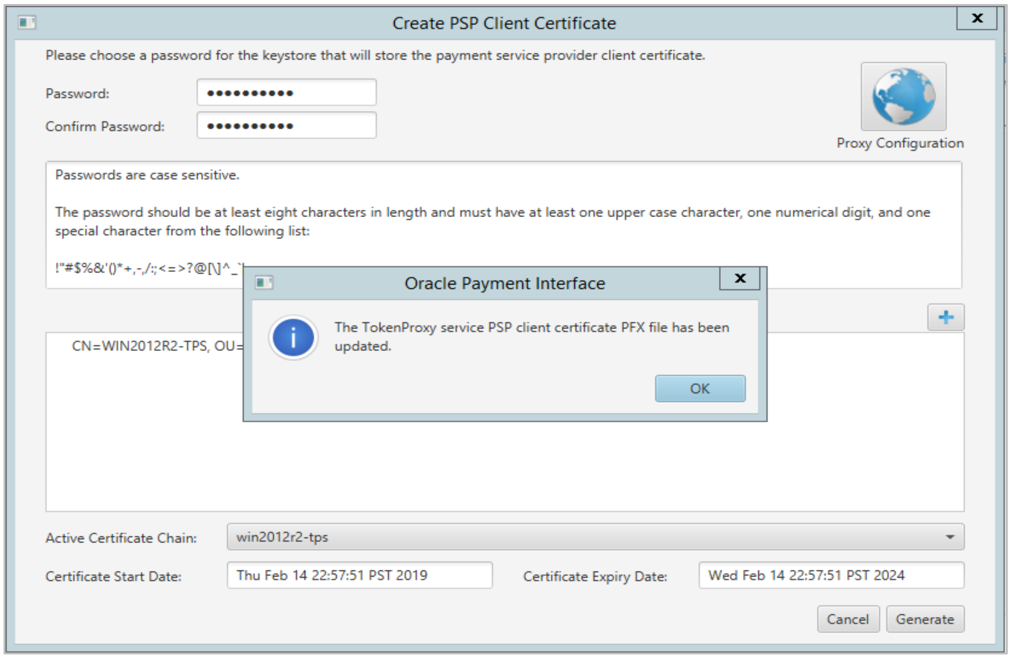
CN=WIN2012R2-TPS, OU=QA, O=Oracle, L=Columbia, ST=MD, C=US

Active Certificate Chain: win2012r2-tps

Certificate Start Date: Thu Feb 14 22:57:51 PST 2019

Certificate Expiry Date: Wed Feb 14 22:57:51 PST 2024

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:

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

CN=WIN2012R2-TPS, OU=

Oracle Payment Interface

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

Active Certificate Chain: win2012r2-tps

Certificate Start Date: Thu Feb 14 22:57:51 PST 2019

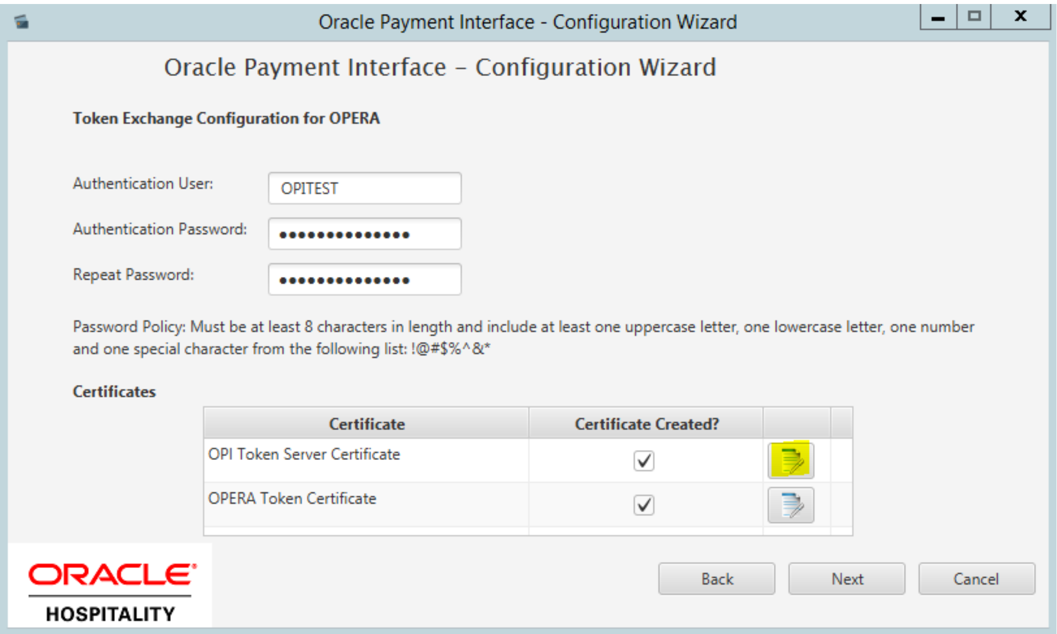
Certificate Expiry Date: Wed Feb 14 22:57:51 PST 2024

OPI_PSP_1.pfx is created under \OraclePaymentInterface\v19.1\Services\OPI\key folder.

OPI - Server Side Certificates

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

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

Token Exchange Configuration for OPERA

Authentication User: OPITEST

Authentication Password: ••••••••••••••

Repeat Password: ••••••••••••••

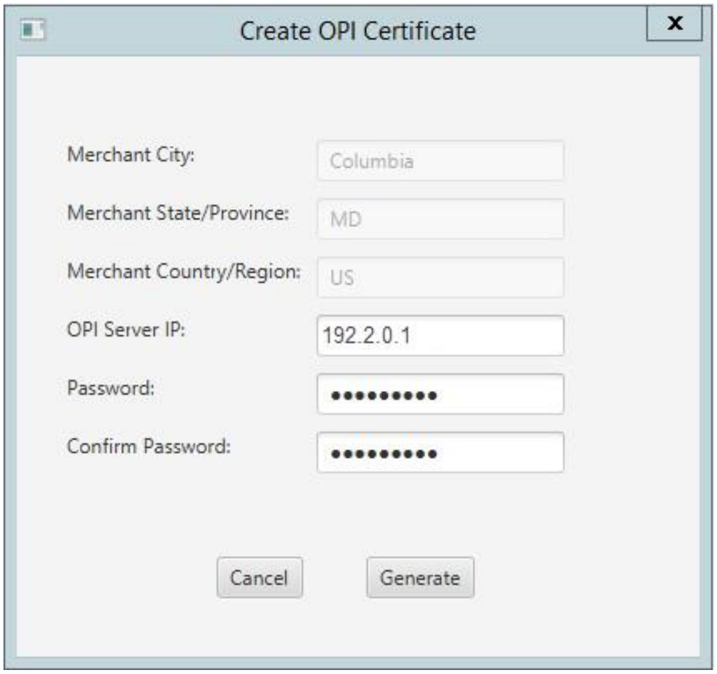
Password Policy: Must be at least 8 characters in length and include at least one uppercase letter, one lowercase letter, one number and one special character from the following list: !@#$%^&*

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 !@#$%^&*

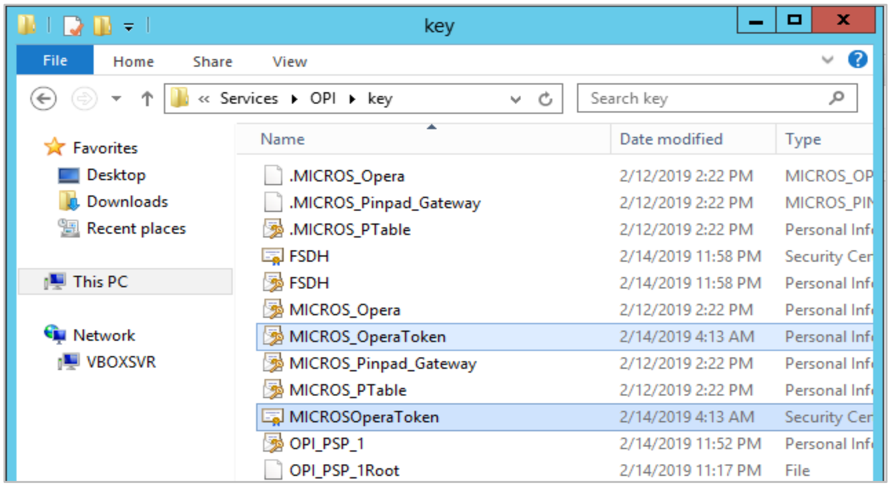


Merchant City:	Columbia
Merchant State/Province:	MD
Merchant Country/Region:	US
OPI Server IP:	192.2.0.1
Password:	••••••••••
Confirm Password:	••••••••••

3. Click **Generate** to continue.

This process will generate the **MICROS_OperaToken.pfx** & **MICROSOperaToken.cer** files in the following folder:

\OraclePaymentInterface\v19.1\Services\OPI\key\



Name	Date modified	Type
.MICROS_Opera	2/12/2019 2:22 PM	MICROS_OP
.MICROS_Pinpad_Gateway	2/12/2019 2:22 PM	MICROS_PIN
.MICROS_PTable	2/12/2019 2:22 PM	Personal Inf
FSDH	2/14/2019 11:58 PM	Security Cer
FSDH	2/14/2019 11:58 PM	Personal Inf
MICROS_Opera	2/12/2019 2:22 PM	Personal Inf
MICROS_OperaToken	2/14/2019 4:13 AM	Personal Inf
MICROS_Pinpad_Gateway	2/12/2019 2:22 PM	Personal Inf
MICROS_PTable	2/12/2019 2:22 PM	Personal Inf
MICROSOperaToken	2/14/2019 4:13 AM	Security Cer
OPI_PSP_1	2/14/2019 11:52 PM	Personal Inf
OPI_PSP_1Root	2/14/2019 11:17 PM	File

> **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.

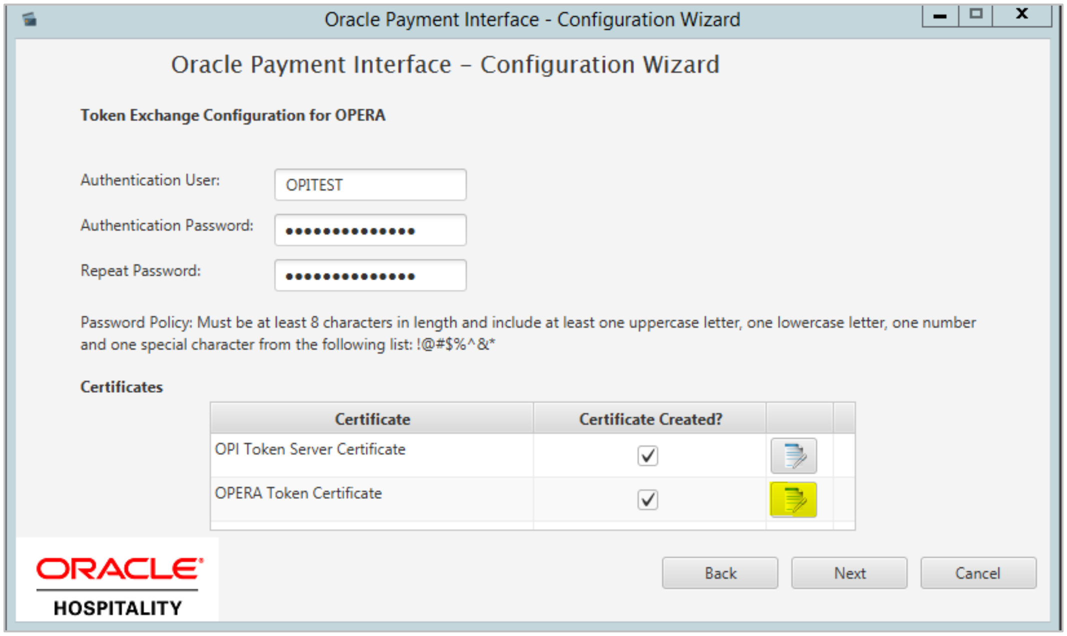
Copy the **MICROSOperaToken.cer** files to all of the Opera registered terminals that you will run the Token Exchange process from, and then import to Trusted Root Certification Authorities, using **mmc.exe** (see below for more info)

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

OPI - Client Side Certificates

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

1. Click the **Opera Token Certificates** button to proceed. There is no specific name for Suite8 thus the names in the forms always refer to OPERA.



Oracle Payment Interface – Configuration Wizard

Token Exchange Configuration for OPERA

Authentication User: OPITEST

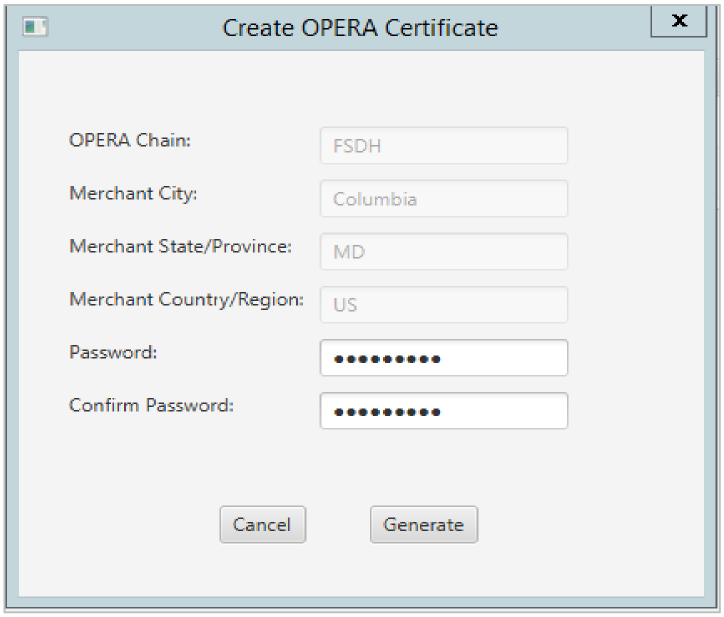
Authentication Password: •••••••••••••••

Repeat 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: !@#$%^&*

Certificates

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



OPERA Chain: FSDH

Merchant City: Columbia

Merchant State/Province: MD

Merchant Country/Region: US

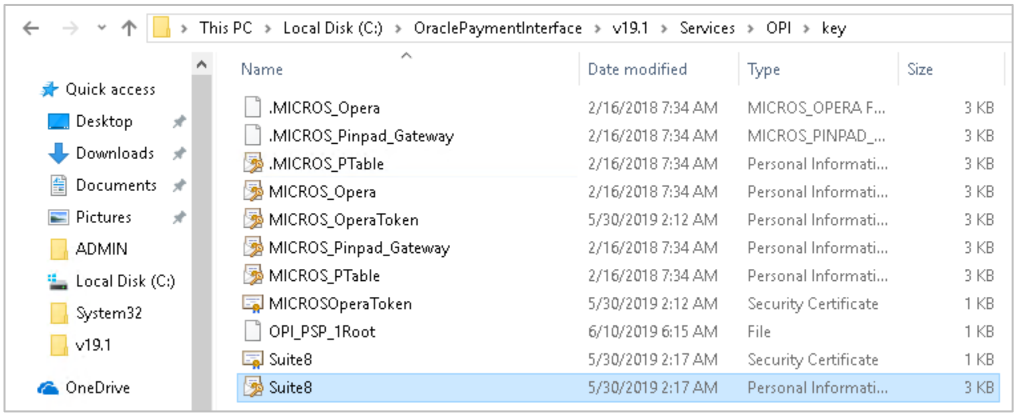
Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

2. After entering the required values, click **Generate**.

This process will generate the **Suite8.pfx** & **Suite8.cer** files in the following folder:

\OraclePaymentInterface\v19.1\Services\OPI\key\



Name	Date modified	Type	Size
.MICROS_Opera	2/16/2018 7:34 AM	MICROS_OPERA F...	3 KB
.MICROS_Pinpad_Gateway	2/16/2018 7:34 AM	MICROS_PINPAD_...	3 KB
.MICROS_PTable	2/16/2018 7:34 AM	Personal Informati...	3 KB
MICROS_Opera	2/16/2018 7:34 AM	Personal Informati...	3 KB
MICROS_OperaToken	5/30/2019 2:12 AM	Personal Informati...	3 KB
MICROS_Pinpad_Gateway	2/16/2018 7:34 AM	Personal Informati...	3 KB
MICROS_PTable	2/16/2018 7:34 AM	Personal Informati...	3 KB
MICROSOperaToken	5/30/2019 2:12 AM	Security Certificate	1 KB
OPI_PSP_1Root	6/10/2019 6:15 AM	File	1 KB
Suite8	5/30/2019 2:17 AM	Security Certificate	1 KB
Suite8	5/30/2019 2:17 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 relative to the environment in which they are being installed.

Copy the **Suite8.pfx** & **Suite8.crt** files created, to all of the Suite8 terminals that you will run the Token Exchange transactions from. Import the certificates using mmc.exe (see below for more info)

- **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.
>
> Be aware the OPI Server Side Certificates will need updating prior to the expiry date to avoid downtime to the interface.

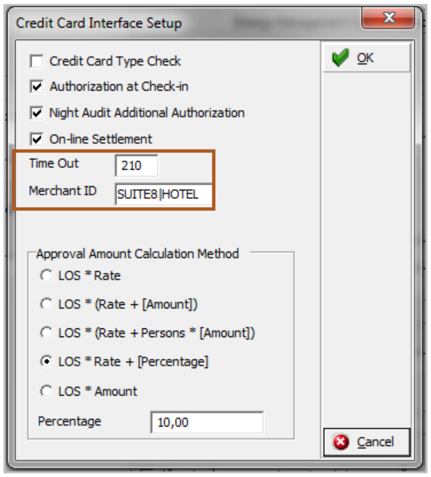
3. You must restart the OPI service for the update to take effect.

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

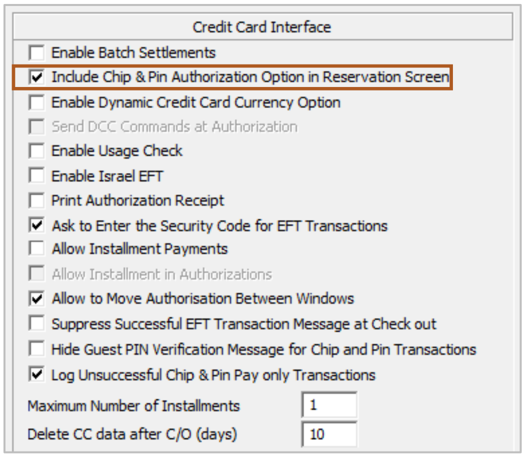
☐ Credit Card Type Check
☑ Authorization at Check-in
☑ Night Audit Additional Authorization
☑ On-line Settlement

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

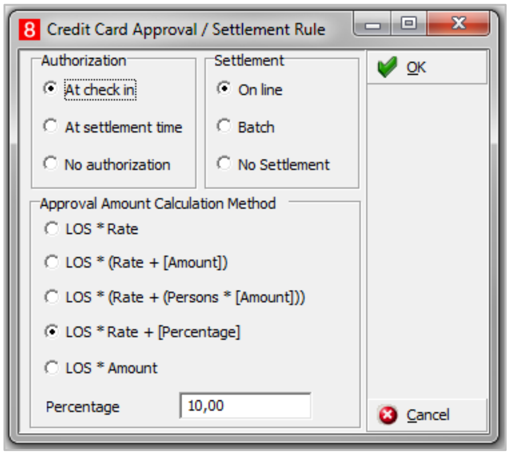
- ☐ Enable Batch Settlements
- ☑ Include Chip & Pin Authorization Option in Reservation Screen
- ☐ Enable Dynamic Credit Card Currency Option
- ☐ Send DCC Commands at Authorization
- ☐ Enable Usage Check
- ☐ Enable Israel EFT
- ☐ Print Authorization Receipt
- ☑ Ask to Enter the Security Code for EFT 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

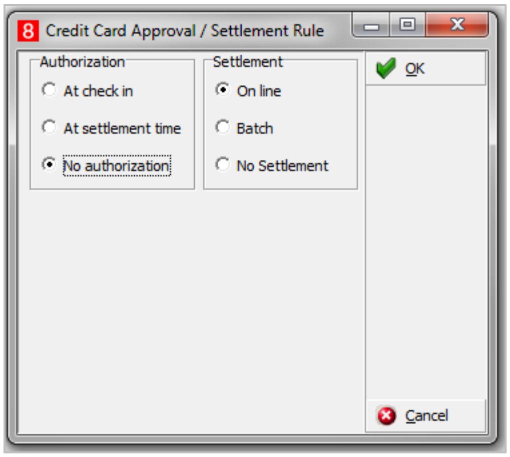
Settlement
- ● On line
- ○ Batch
- ○ No Settlement

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.



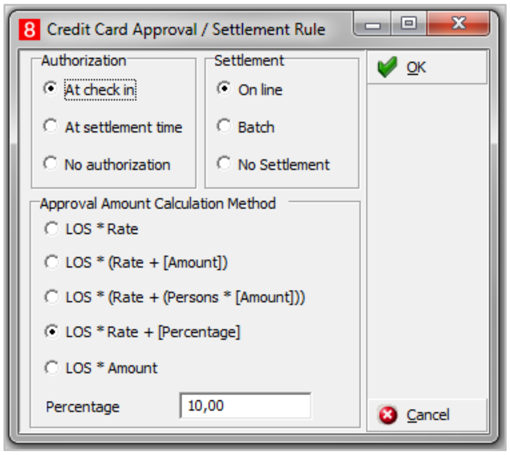
Credit Card Approval / Settlement Rule

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.

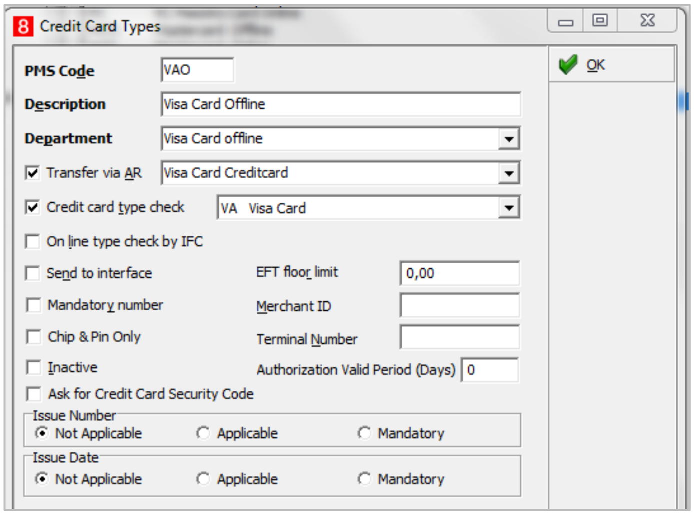
Payment Type Configuration

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

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.

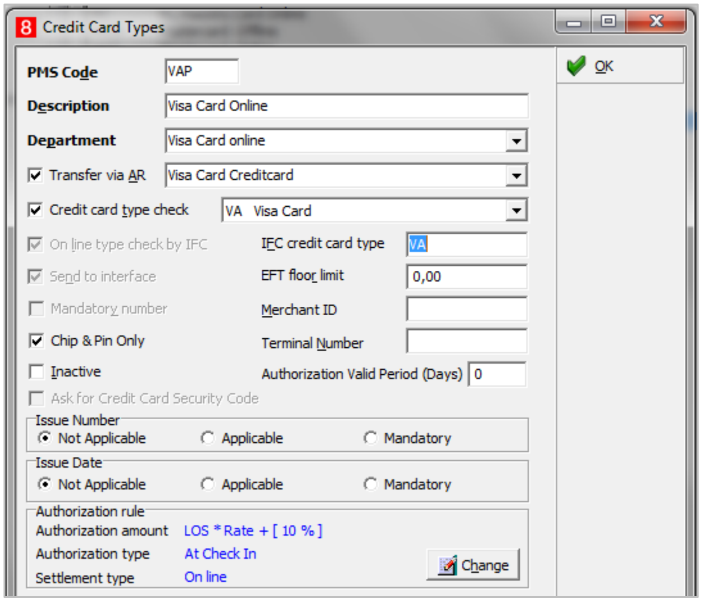
PMS Code = free definable 3-letter code

IFC Credit card type = 2-letter code as setup in OPI (e.g. 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

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

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 related field in Suite8.

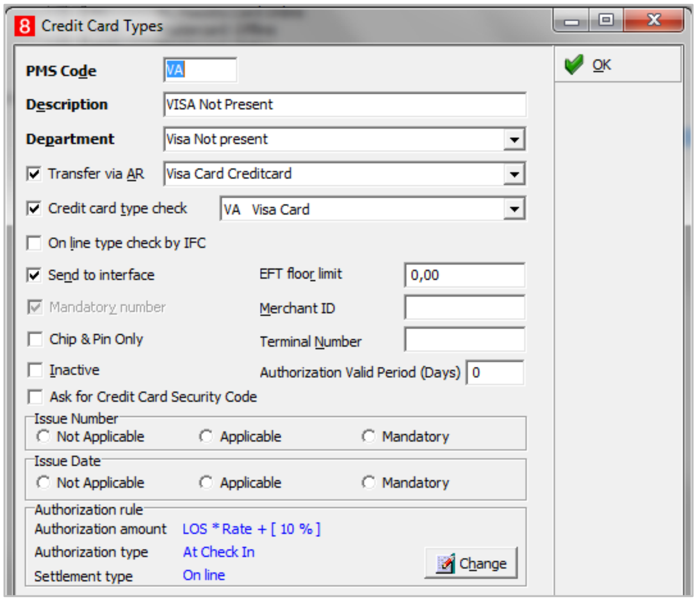
PMS Code = 2-letter code as setup in OPI (e.g. VA for VISA)

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.

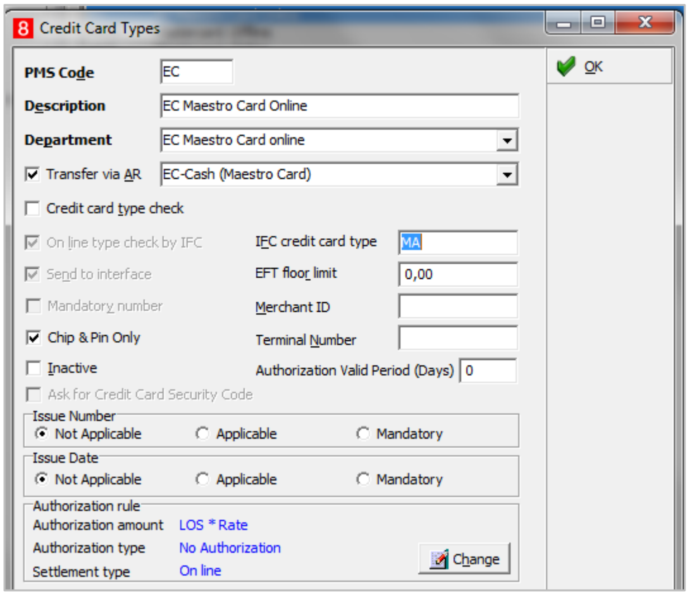
PMS Code = 2-letter code – freely definable

IFC Credit card type = 2-letter code as setup in OPI (e.g. 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

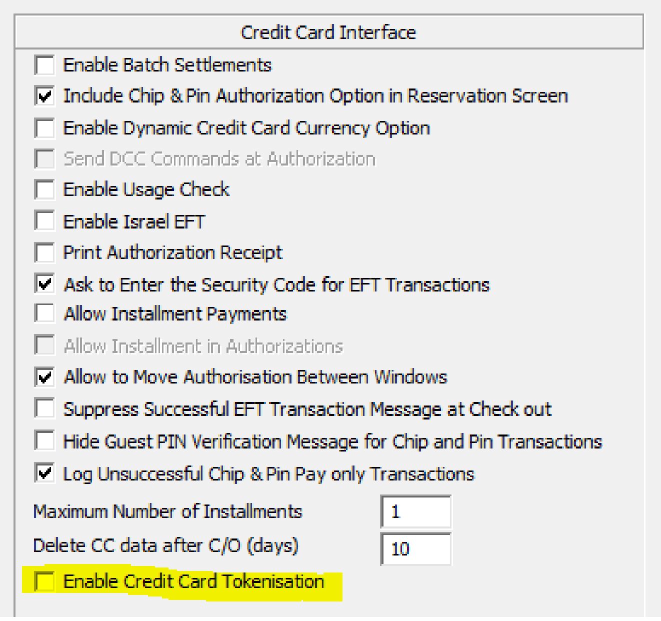
User Right to Enable the Tokenization Feature

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 Tokenisation** 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

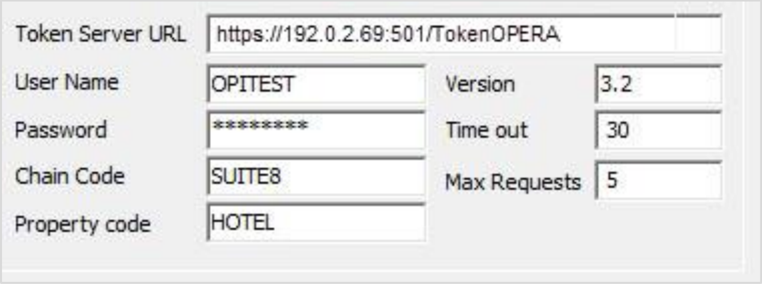
- □ Enable Credit Card Tokenisation

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 PC 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 will be 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:

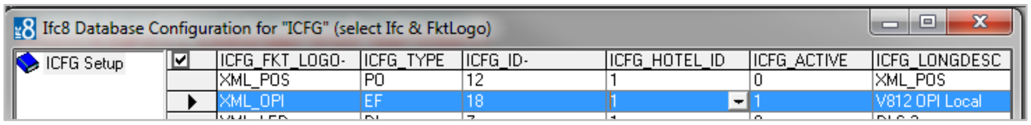


Token Server URL	https://192.0.2.69:501/TokenOPERA		
User Name	OPITEST	Version	3.2
Password	*********	Time out	30
Chain Code	SUITE8	Max Requests	5
Property code	HOTEL		

Configuring the Hotel Property Interface (IFC8) Instance to the Suite8 Hotel Property Interface (IFC)

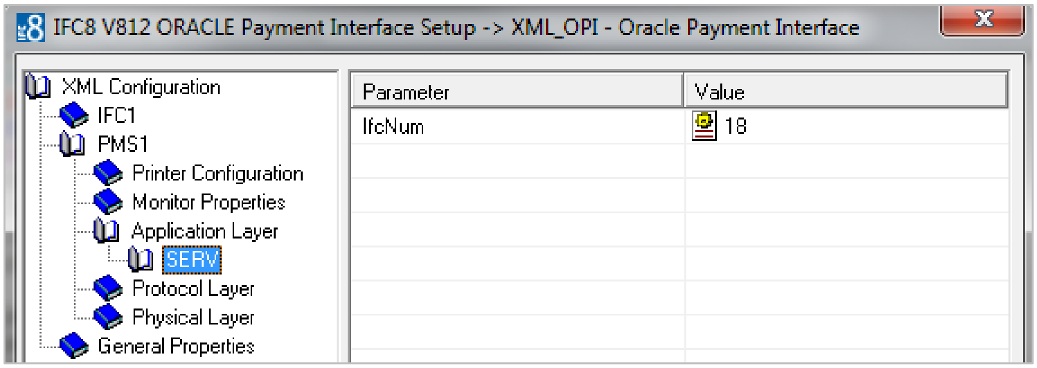
To configure the link between the interfaces:

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).



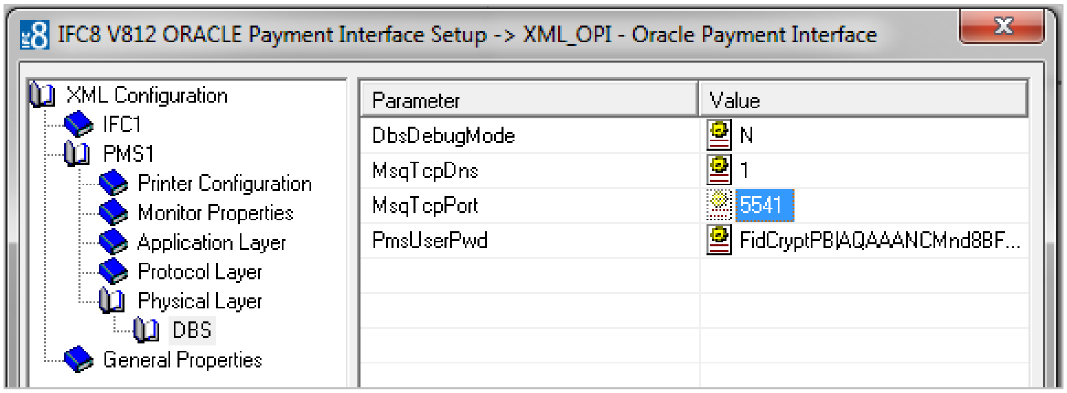
Ifc8 Database Configuration for "ICFG" (select Ifc & FktLogo)
ICFG Setup

☑	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



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**.

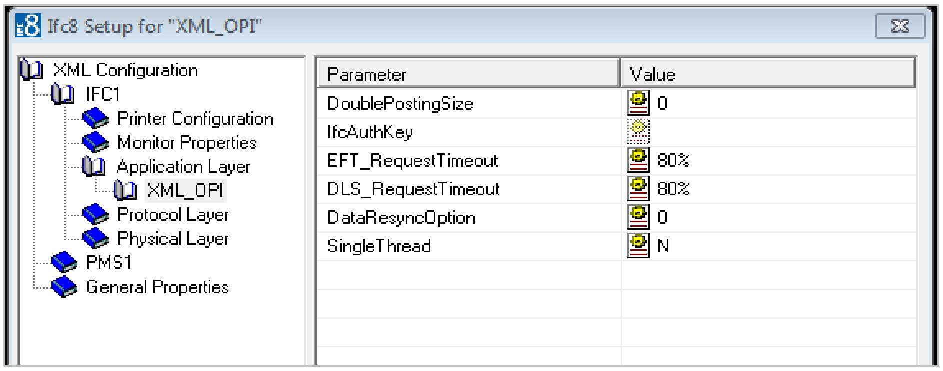


Parameter	Value
DbsDebugMode	N
MsqTcpDns	1
MsqTcpPort	5541
PmsUserPwd	FidCryptPB|AQAAANCMnd8BF...

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.

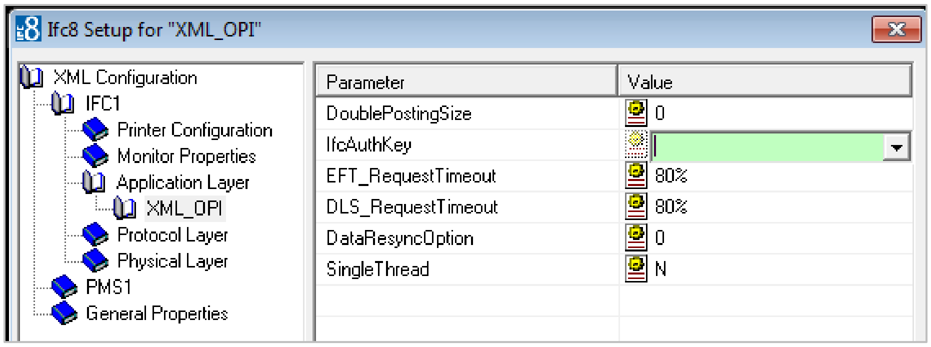


Parameter	Value
DoublePostingSize	0
IfcAuthKey	
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0
SingleThread	N

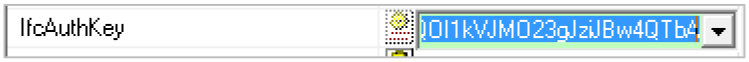
2. Copy the generated key from Configuring OPI - OPERA merchant step 3, and add “FidCrypt0S|” to the generated key as prefix.

   For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxxxx

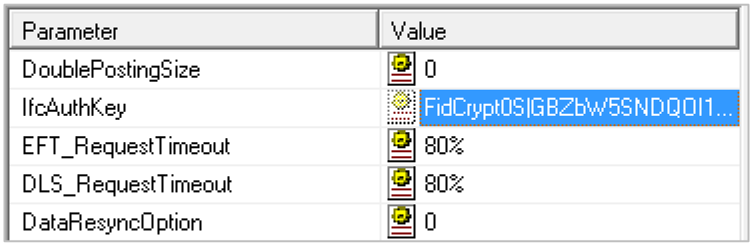
3. Copy this string into IFC8 Parameter **IfcAuthKey** value field.



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

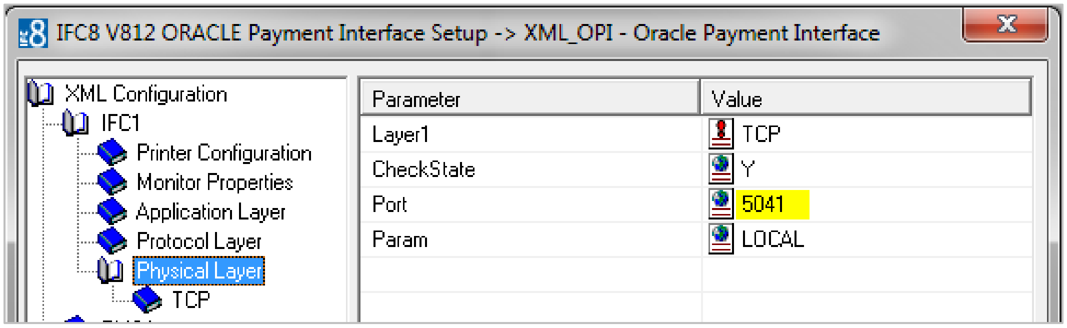


IfcAuthKey	)OI1kVJMO23gJziJBw4QTbA



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

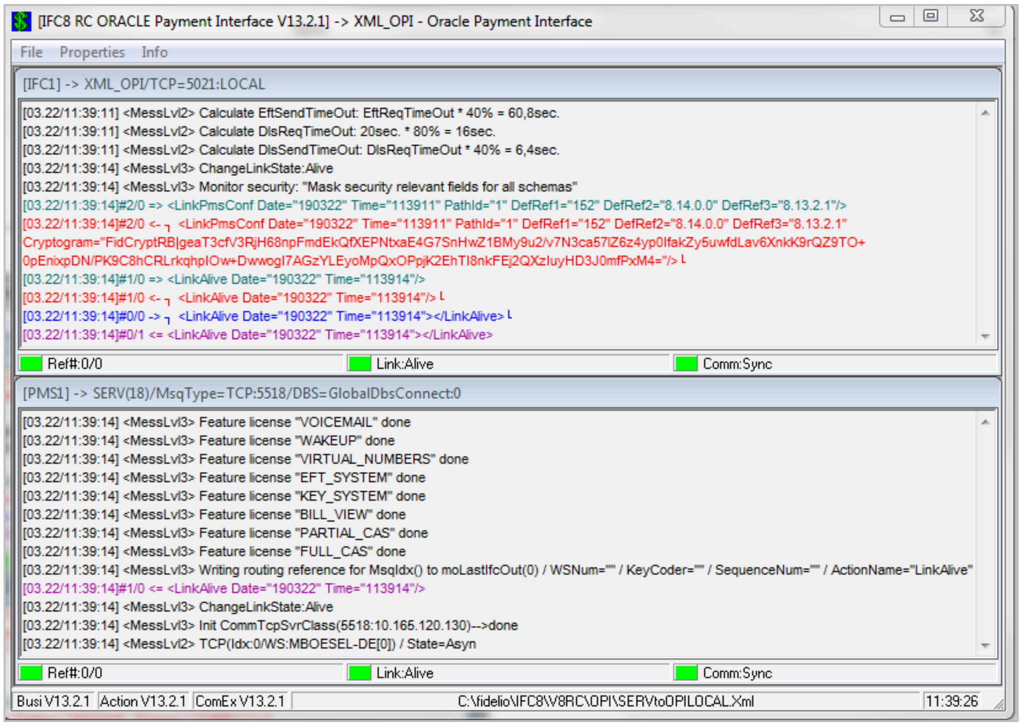
4. Go to **IFC1** tree and select the **Physical Layer**.
5. Enter the port number in port value. This is the same port that was configured in OPI.



Parameter	Value
Layer1	TCP
CheckState	Y
Port	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.

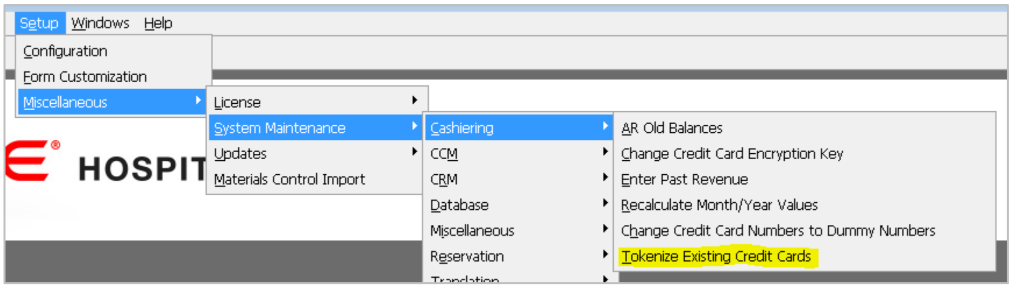

[IFC8 RC ORACLE Payment Interface V13.2.1] -> XML_OPI - Oracle Payment Interface
File
Properties
Info
[IFC1] -> XML_OPI/TCP=5021:LOCAL

```
[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>
```

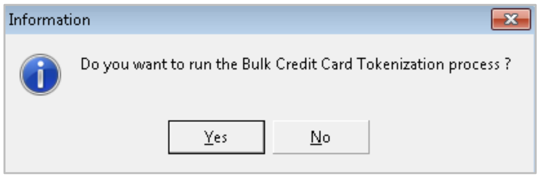
```
[03.22/11:39:14] <MessLvl3> Feature license "VOICEMAIL" done
[03.22/11:39:14] <MessLvl3> Feature license "WAKEUP" done
[03.22/11:39:14] <MessLvl3> Feature license "VIRTUAL_NUMBERS" done
[03.22/11:39:14] <MessLvl3> Feature license "EFT_SYSTEM" done
[03.22/11:39:14] <MessLvl3> Feature license "KEY_SYSTEM" 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.

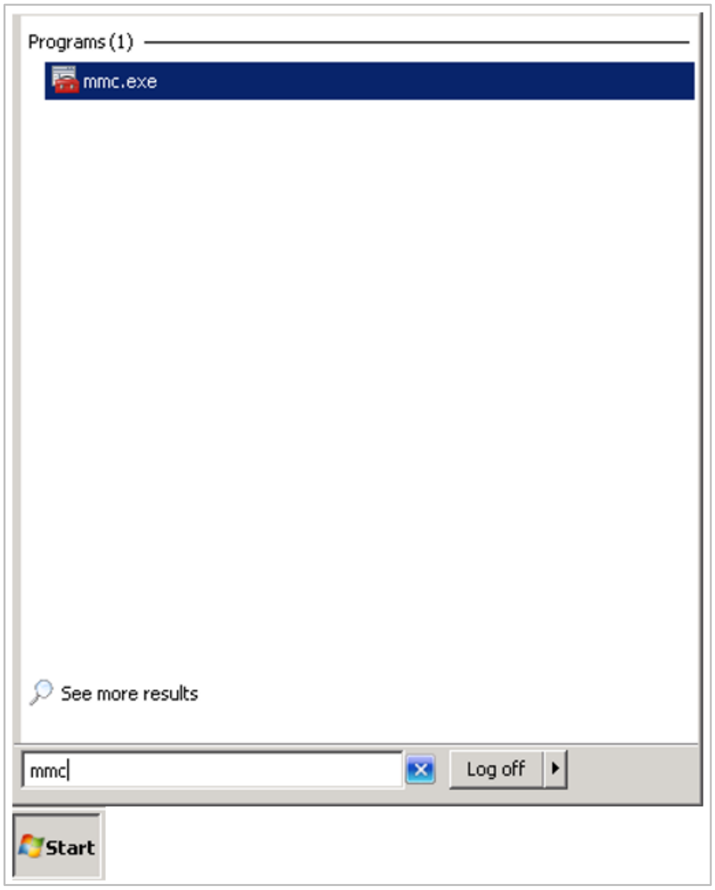
> **NOTE:**
>
> After the successful replacement of credit card numbers with token ID's the process should NOT be executed again.

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.

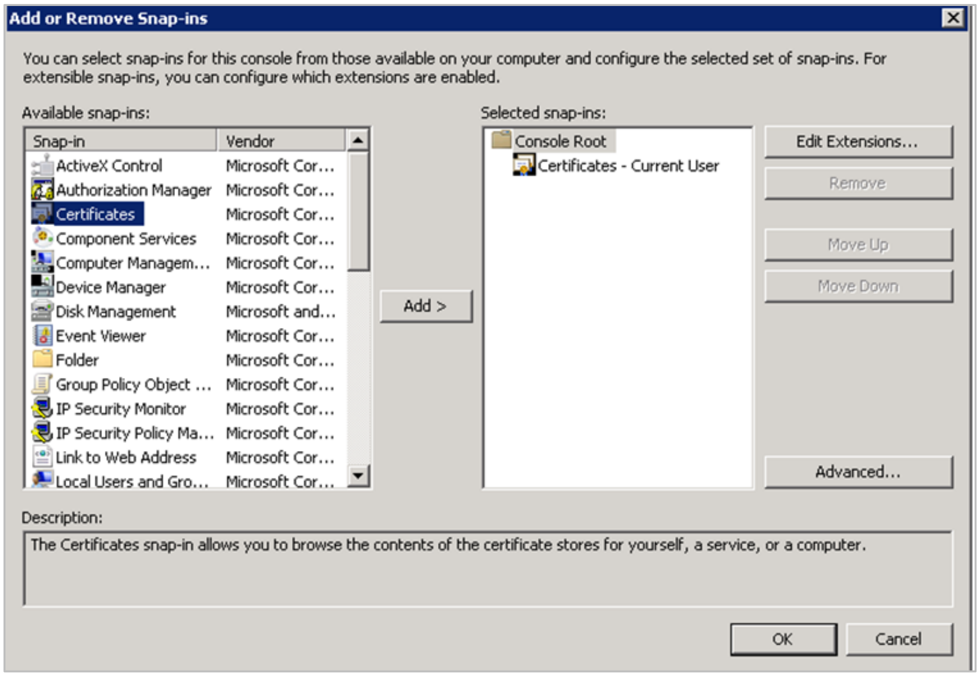
OPI only supports the **Convert CC** function; the other conversion options are not currently supported.

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**.

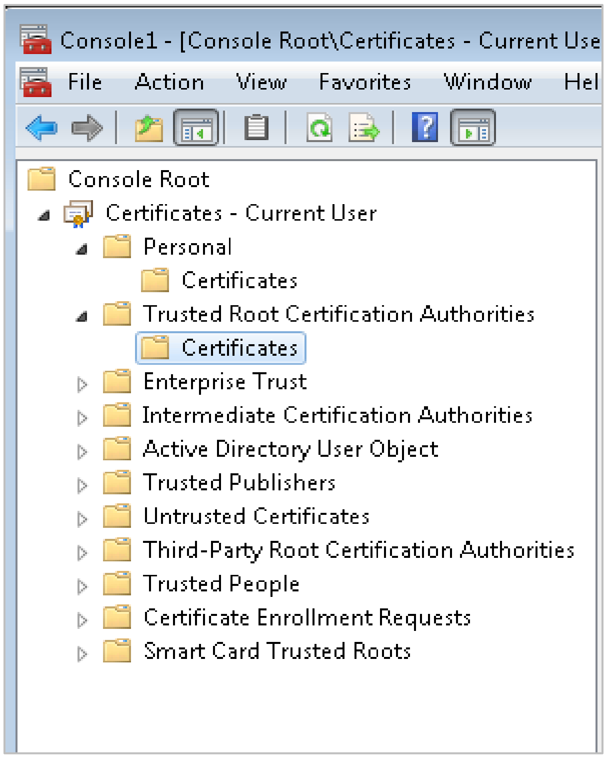


You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

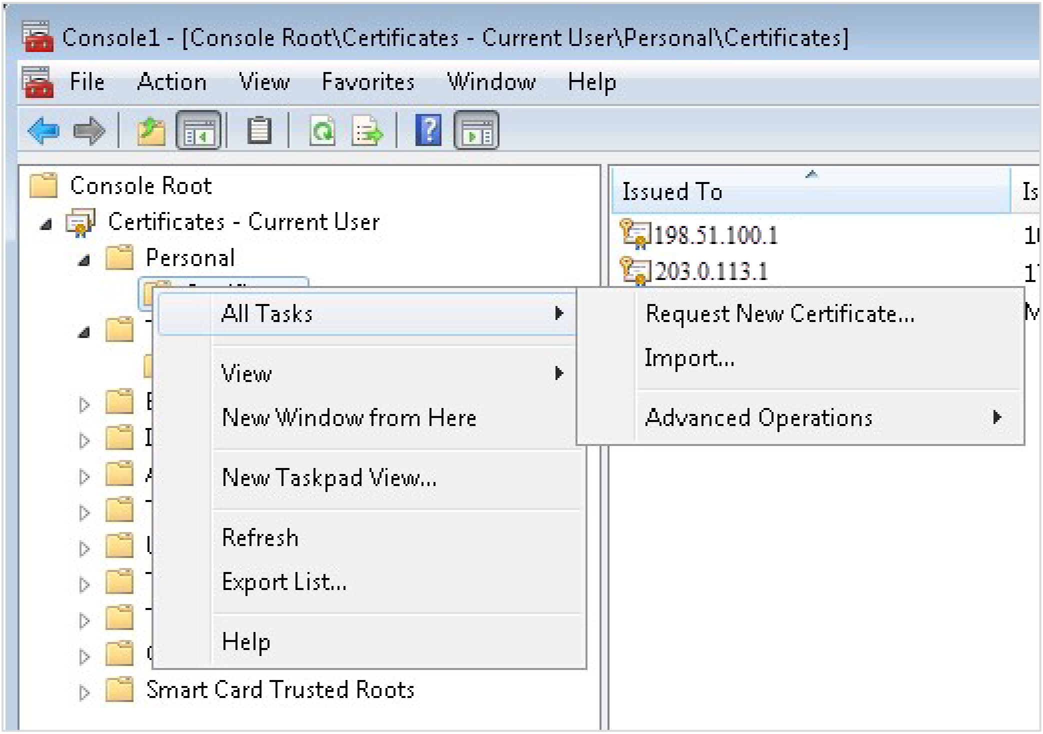
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft 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 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

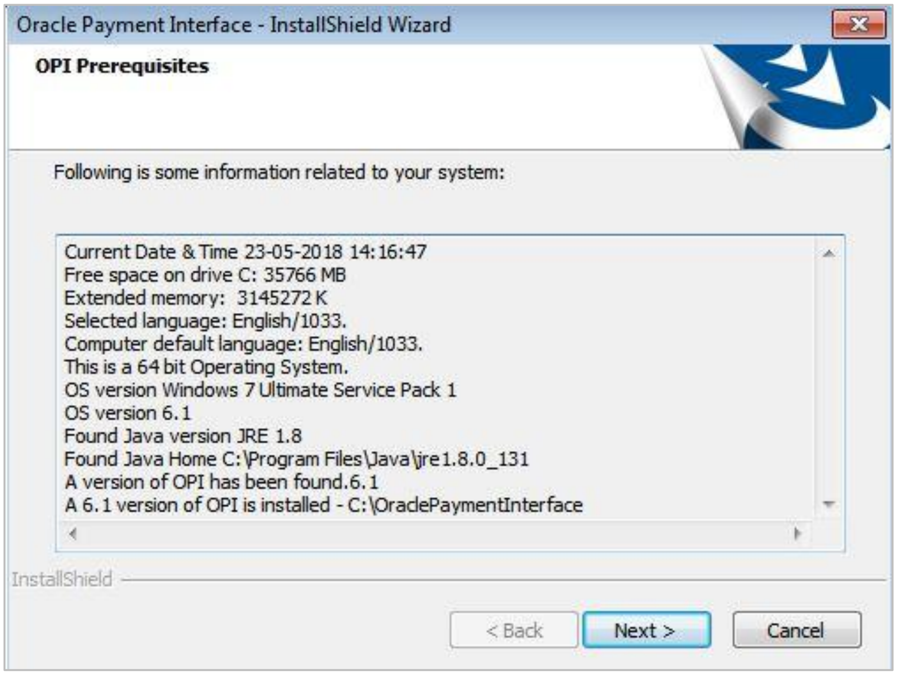
VERY IMPORTANT: Read and follow the upgrade directions.

> **NOTE:**
>
> OPI 6.1 and higher can be upgraded to OPI 19.1.

OPI 6.1 to 19.1.0.0 Upgrade Steps

1. Right-click and Run as Administrator the **OraclePaymentInterfaceInstaller_19.1.0.0.exe** file to perform an upgrade.
2. Select a language from the drop-down list, and then click **OK**.
3. Click **Next** on the Welcome screen to proceed with the installation.

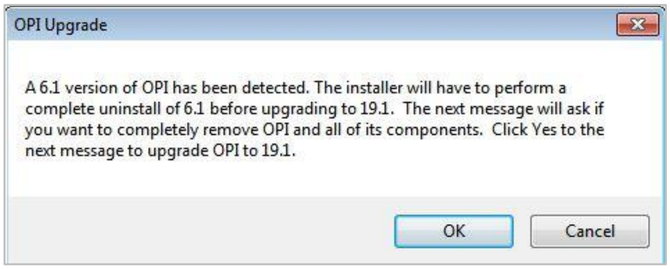
   Prerequisites for the installation will be checked, including the required free drive space, details of the host environment, and the Java version that is present.
4. Click **Next** on the OPI Prerequisites screen.



Following is some information related to your system:

```
Current Date & Time 23-05-2018 14:16:47
Free space on drive C: 35766 MB
Extended memory:  3145272 K
Selected language: English/1033.
Computer default language: English/1033.
This is a 64 bit Operating System.
OS version Windows 7 Ultimate Service Pack 1
OS version 6.1
Found Java version JRE 1.8
Found Java Home C:\Program Files\Java\jre1.8.0_131
A version of OPI has been found.6.1
A 6.1 version of OPI is installed - C:\OraclePaymentInterface
```

5. Click **OK** on the OPI Upgrade screen.



OPI Upgrade

A 6.1 version of OPI has been detected. The installer will have to perform a complete uninstall of 6.1 before upgrading to 19.1. The next message will ask if you want to completely remove OPI and all of its components. Click Yes to the next message to upgrade OPI to 19.1.

6. **WARNING!** You must click **Yes**.

   IF YOU CLICK NO, YOU WILL HAVE BOTH OPI 6.1 AND OPI 19.1 INSTALLED AND NEITHER WILL WORK.

   Explanation: OPI will migrate the existing MySQL configuration information, but all previous OPI applications will be removed before the new files are installed.

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

8. Click **Next**.

   The Ready to Install the Program screen displays.

9. Click **Install**.

   The Setup Status screen displays for a few minutes.

Setup Type

For database type, select MySQL. No other database type is supported for upgrades.

Database Server

Name/IP: The Hostname or IP Address used for communication to the MySQL database. This must be left at the default of localhost.

Port #: The Port number used for communication to the database

Database Server Login

DBA user

Login ID: root

Password: root user password for MySQL database.

Database User Credentials

User Name: This must be a new user name. It cannot be the same user from the 6.1 install.

Password: Password for the new database user.

Configuration Tool Superuser Credentials

User Name: This can be any user name. It does not have to be a Windows account user.

Password: Create a password, and then confirm it.

Configuration Tool Connection Settings

Host: Enter the IP address or server name of the PC where the OPI Config Service is installed. This will be the PC where you selected "OPI Services" to be installed.

Port: Leave at 8090.

Configuration Tool Passphrase

Enter and confirm a passphrase.

Click **Next**.

The Configuration Wizard launches.

Continue to follow on-screen directions, verifying settings as you go.

PMS Merchants

On the Merchants screen, click the wrench icon to the right of the existing merchant.

Verify the merchant settings are correct.

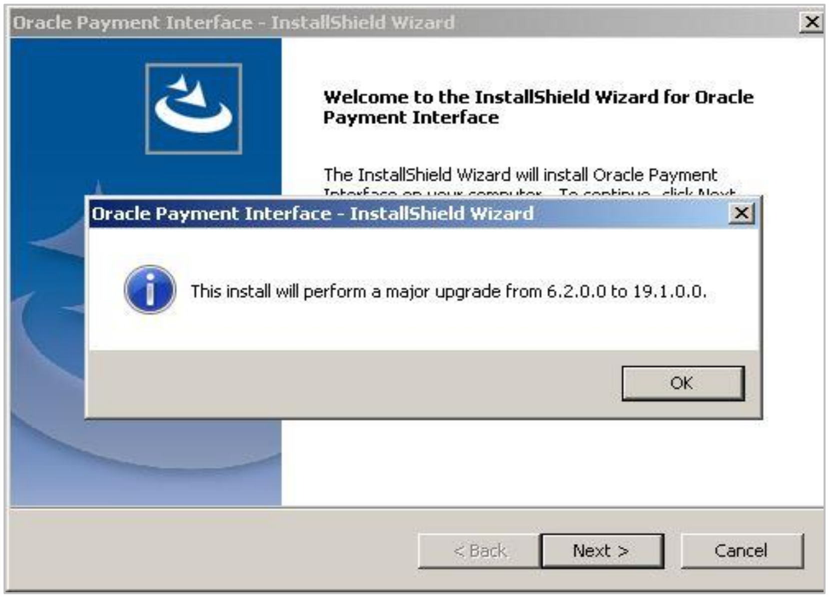
InstallShield Wizard Complete

Click **Finish** to allow a reboot.

If you cannot immediately reboot, you must stop and then start the OPI Service for the current settings to take effect.

OPI 6.2 to 19.1.0.0 Upgrade Steps

1. Right-click and Run as Administrator the **OraclePaymentInterfaceInstaller_19.1.0.0.exe** file to perform an upgrade.
2. Select a language from the drop-down list, and then click **OK**.
3. Click **Next** on the Welcome screen to proceed with the installation.



Oracle Payment Interface - InstallShield Wizard

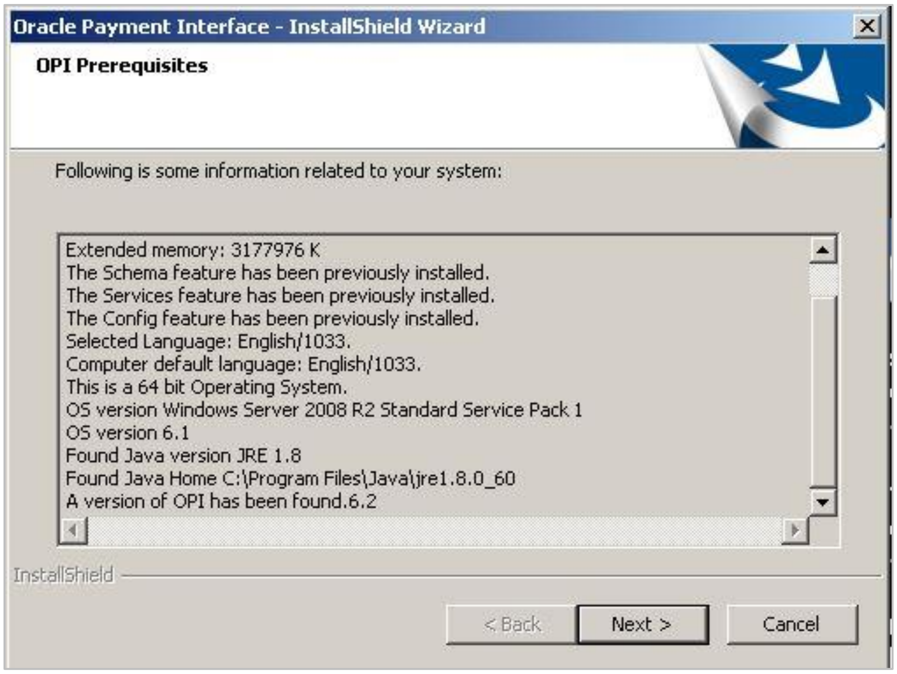
Welcome to the InstallShield Wizard for Oracle Payment Interface

The InstallShield Wizard will install Oracle Payment Interface on your computer. To continue, click Next.

Oracle Payment Interface - InstallShield Wizard

This install will perform a major upgrade from 6.2.0.0 to 19.1.0.0.

4. Click **Next** on the OPI Prerequisites screen.



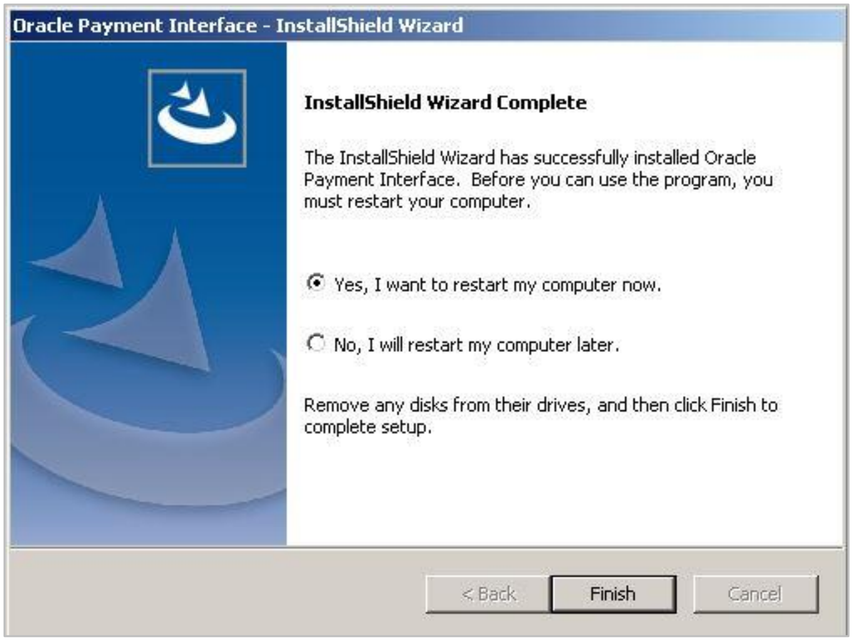
Oracle Payment Interface - InstallShield Wizard

OPI Prerequisites

Following is some information related to your system:

```
Extended memory: 3177976 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 2008 R2 Standard Service Pack 1
OS version 6.1
Found Java version JRE 1.8
Found Java Home C:\Program Files\Java\jre1.8.0_60
A version of OPI has been found.6.2
```

5. Choose a Destination Location. Accept the default installation location or click **Change…** to choose a different location and click **Next.**
6. Click **Install**. When The Ready to Install the Program screen displays.
7. Click **OK** when The Database upgrade operation was successful screen displays.
8. Enter the configuration Server connection information.
9. Click **Finish** to restart your computer.



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.