

## **Oracle® Payment Interface**

Oracle Hospitality Suite8 Property Management  
System Installation Guide

Release 6.2

**F18591-01**

March 2019

---

Copyright © 2010, 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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

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

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

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

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

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

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

---

---

# Contents

<b>Preface</b> .....	<b>vii</b>
Audience .....	vii
Customer Support.....	vii
Documentation.....	vii
Revision History.....	vii
<b>1 Pre-Installation</b> .....	<b>1-1</b>
<b>2 Installing the OPI</b> .....	<b>2-2</b>
<b>3 Upgrading the OPI</b> .....	<b>3-1</b>
OPI Upgrade Steps .....	3-1
<b>4 Configuring OPI</b> .....	<b>4-4</b>
Certificates .....	4-9
PSP - Client Side Certificates.....	4-9
OPI - Server Side Certificates .....	4-13
OPI - Client Side Certificates.....	4-15
<b>5 Suite8 Credit Card Configuration</b> .....	<b>5-18</b>
General Credit Card Interface Setup .....	5-18
Payment Type Configuration.....	5-20
Tokenization Setup .....	5-23
Configuring the Hotel Property Interface (IFC8) Instance to the Suite8 Hotel Property Interface (IFC).....	5-24
Configuring encryption for the Hotel Property Interface (IFC8) with OPI .....	5-25
Perform a Tokenization.....	5-27
Certificate Import using Microsoft Management Console.....	5-28

---

---

# Preface

This document is to guide users attempting to configure Oracle Payment Interfaces 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

Oracle Hospitality 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	<ul style="list-style-type: none"><li>• Initial publication</li></ul>

---

---

# 1 Pre-Installation

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 6.2 does not install a database. If doing a clean install of OPI, a database must be installed first.
- Upgrading to OPI 6.2 from OPI 6.1 and higher is supported but MPG versions are not supported. Prior to upgrading from OPI 6.1 to OPI 6.2 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 6.2.
- 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:

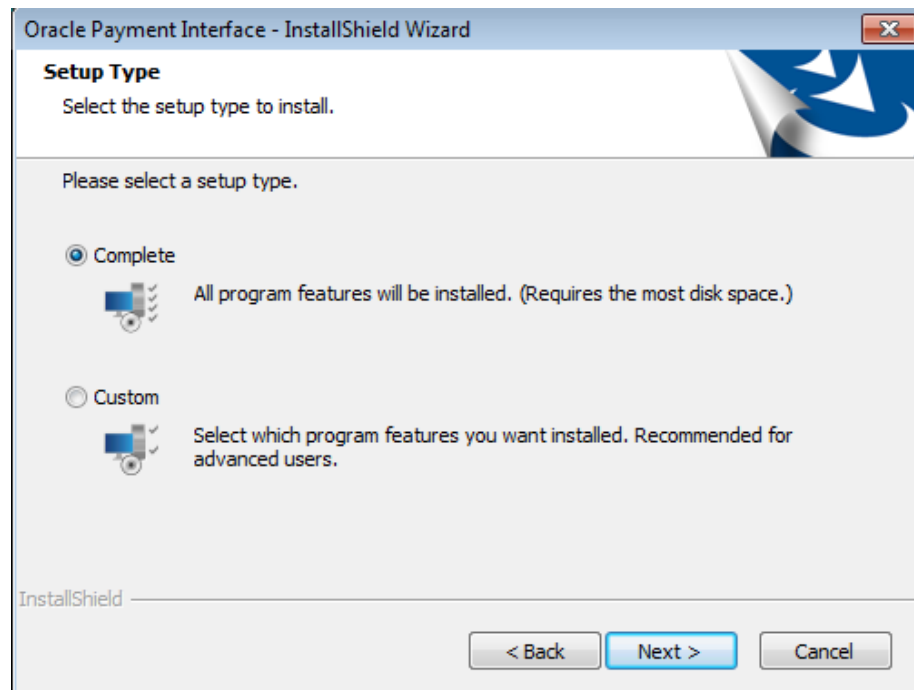
- Merchant IDs
- IP address of the OPI Server
- If there is an existing MySQL database installed, then the SQL root password is required.
- Workstation IDs and IPs that integrate with the PIN pad.

---

---

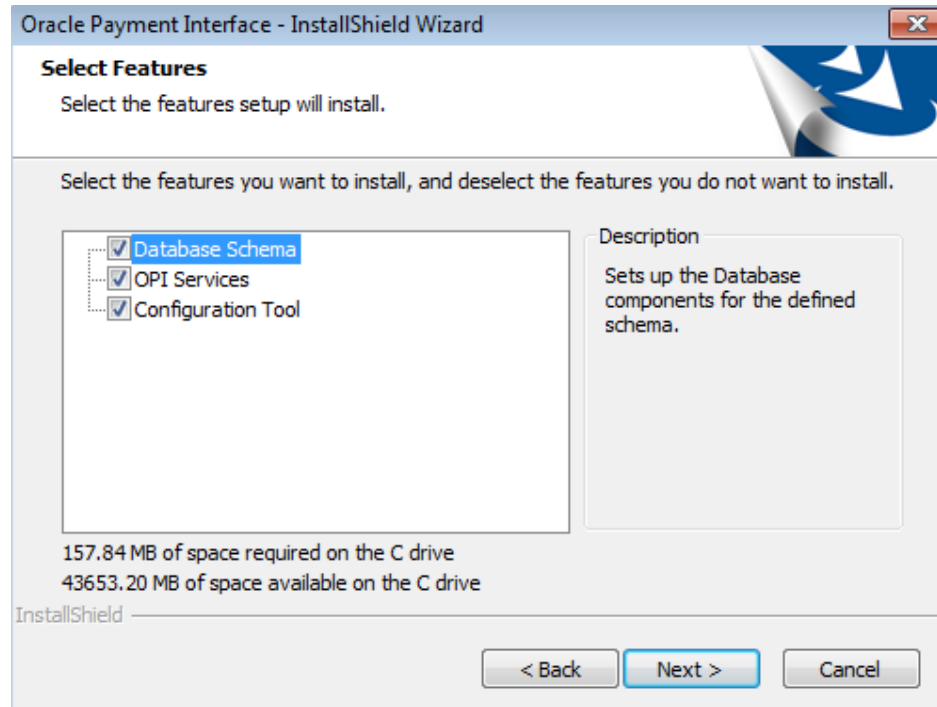
## 2 Installing the OPI

1. Copy OraclePaymentInterfaceInstaller-6.2.0.0.exe, double click it to launch the install.
2. Select your 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.



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, and then click **Next**.



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

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

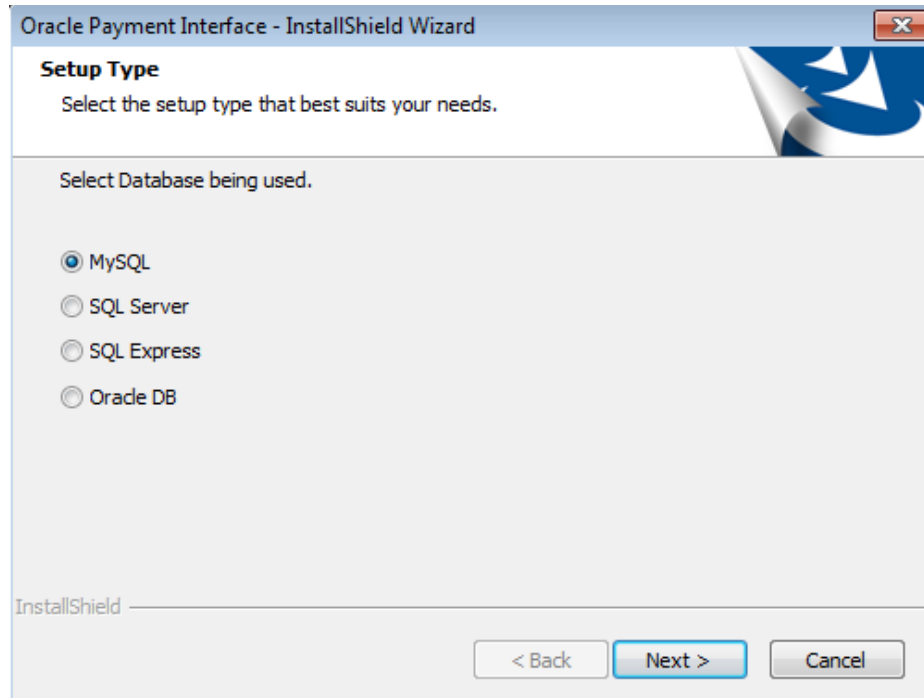
The *Choose Destination Location* screen appears.

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.

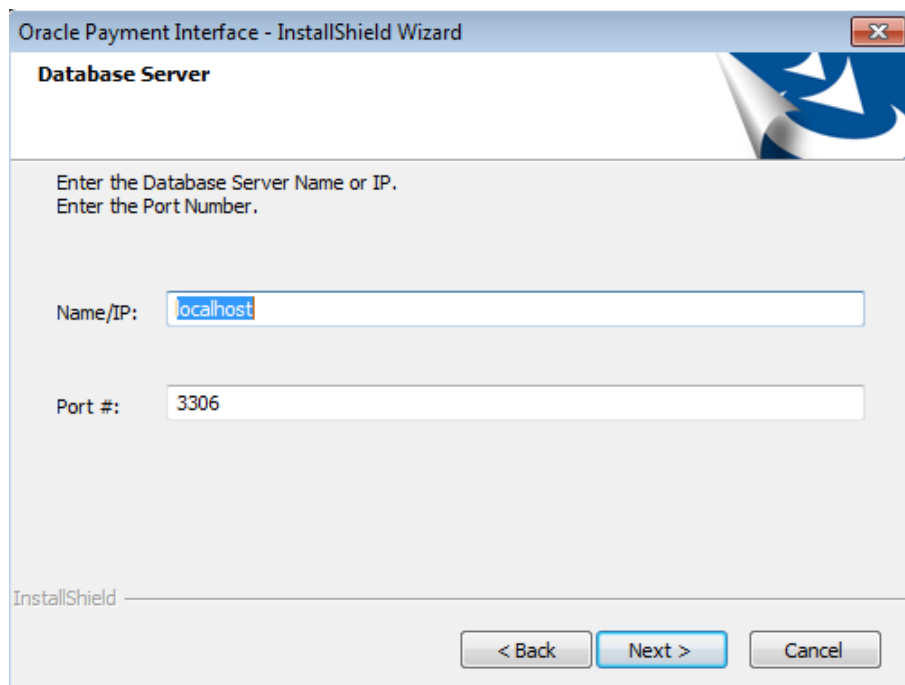
The *Setup Status* screen displays for a few minutes.

9. The *Setup Type* screen appears.



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.



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.

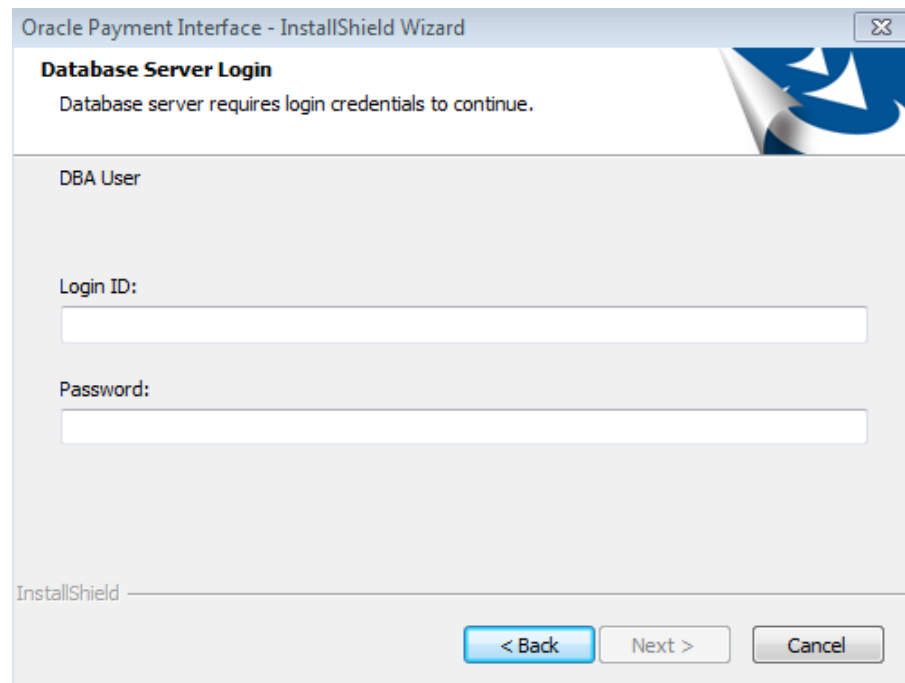


---

**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 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.



The screenshot shows a window titled "Oracle Payment Interface - InstallShield Wizard". The main heading is "Database Server Login" with a sub-message: "Database server requires login credentials to continue." Below this, the text "DBA User" is displayed. There are two input fields: "Login ID:" and "Password:". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

13. Enter the server login credentials of DBA user for 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:

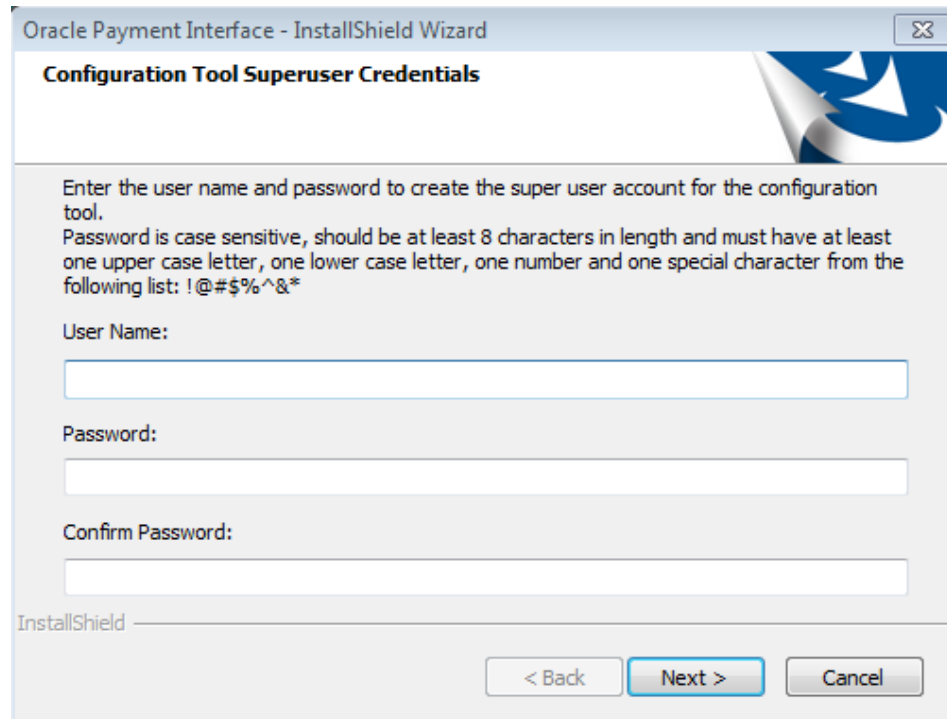
Password:

Confirm Password:

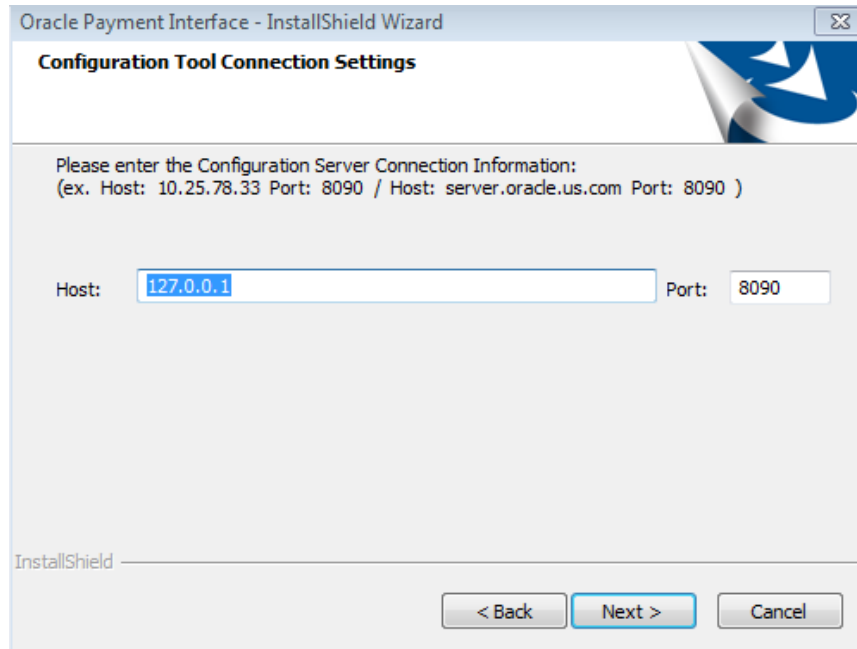
InstallShield

< Back   Next >   Cancel

14. **User Name:** Enter the user name to create a new database user account.
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 Password:** 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.

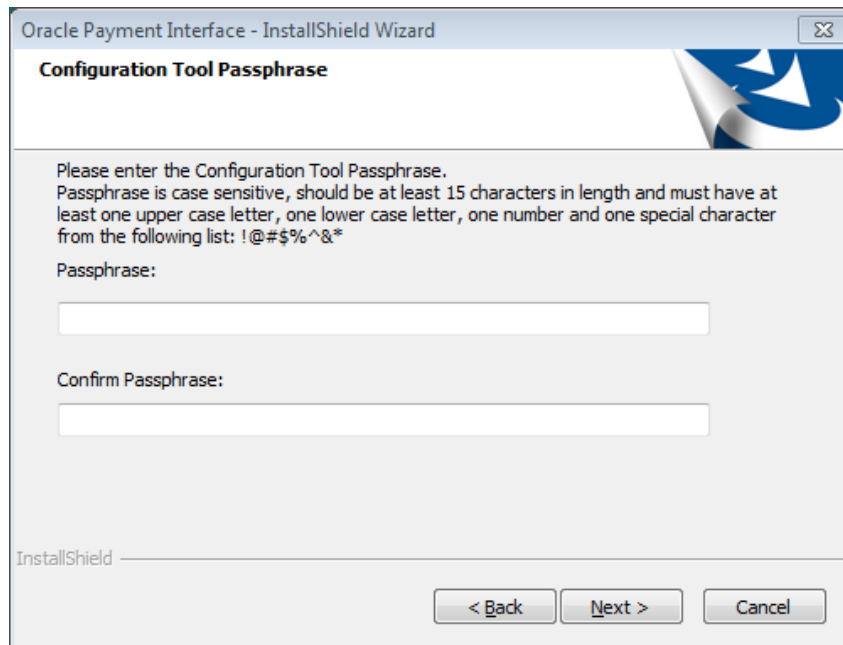


19. **User Name:** Enter the user name to create the Super user account. This can be any user name. It does not have to be a Windows account user.
20. **Password:** Create a password. Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one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



23. **Host:** May be left at 127.0.0.1 if the OPI configuration server is installed on this PC. Otherwise, specify the name or IP address of the PC where the OPI configuration server will be installed.
24. Leave the default **Port** of 8090.
25. Click **Next**.

The *Configuration Tool Passphrase* screen appears.

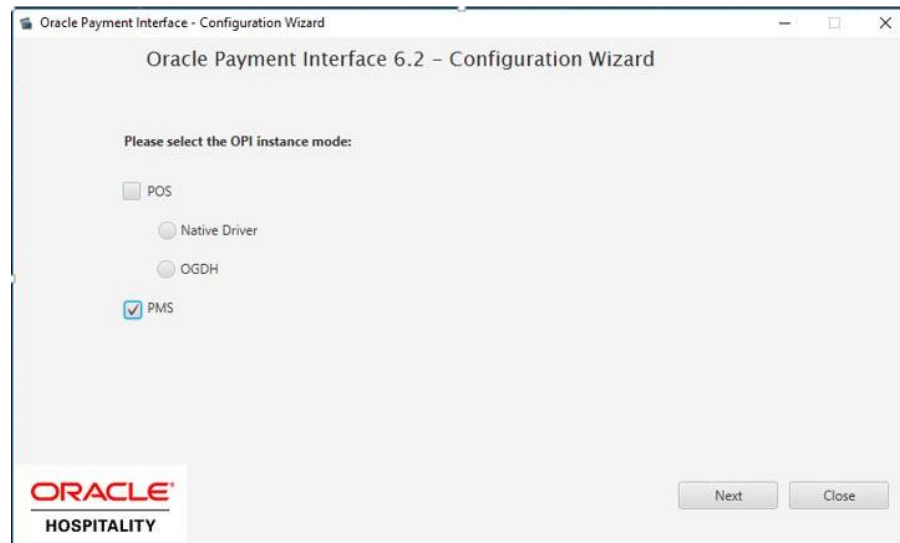


26. **Passphrase:** The passphrase is case sensitive, should be at least 15 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#\$\$%^&\*.

---

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

After a brief pause, the *Configuration Wizard* launches.



28. Select **PMS**, Click **Next**.

---

---

## 3 Upgrading the OPI

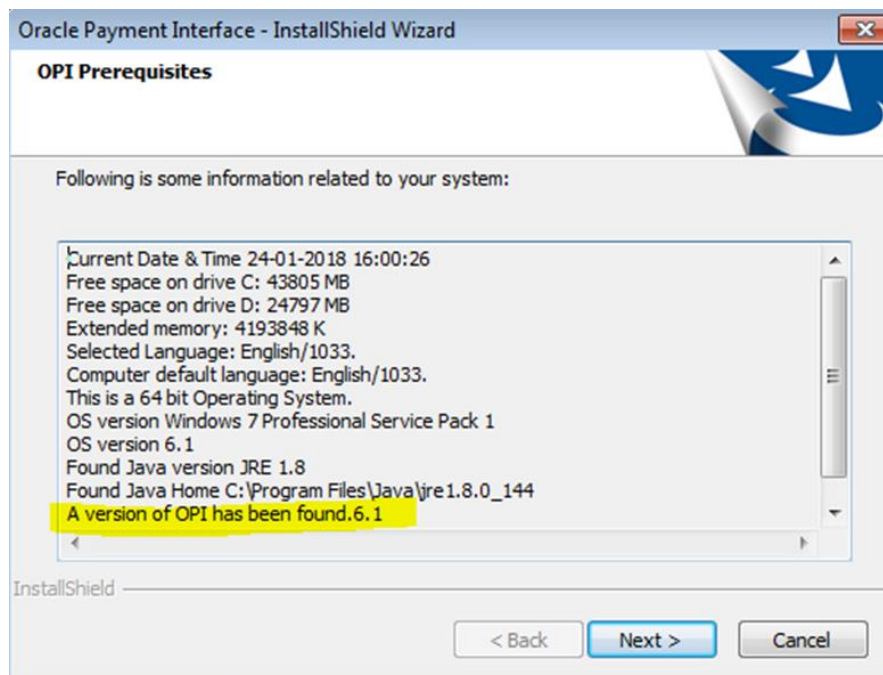
**VERY IMPORTANT:** Read and follow the upgrade directions.

**Note:** OPI 6.1 and higher can be upgraded to OPI 6.2.

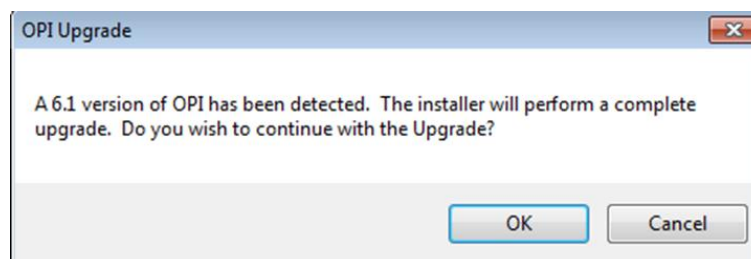
### OPI Upgrade Steps

1. Right-click and Run as Administrator the OraclePaymentInterfaceInstaller\_6.2.0.0.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.

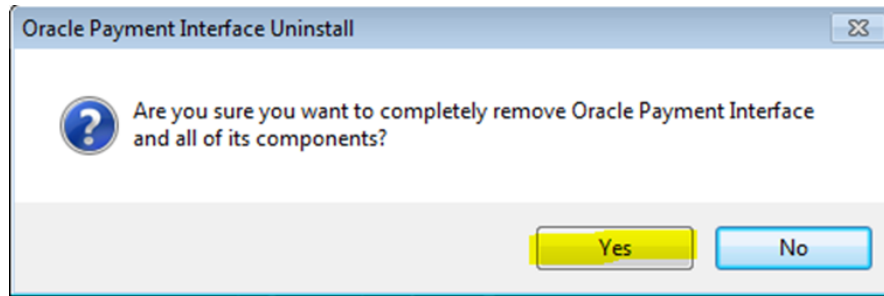
Prerequisites for the installation will be checked, including the required free drive space, details of the host environment, and the Java version that is present.



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



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



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

IF YOU CLICK **NO**, YOU WILL HAVE BOTH OPI 6.1 AND OPI 6.2 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: May be left at 127.0.0.1 if the OPI configuration server is installed on this PC. Otherwise, specify the name or IP address of the PC where the OPI configuration server will 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.

### **POS Merchants**

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

Verify the merchant settings are correct.

### **Merchant Pay At Table Configuration**

If using Pay@Table, review the tender settings carefully as there are new fields that will not be pre-populated from the previous OPI install.

Continue to follow the on-screen directions.

### **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.

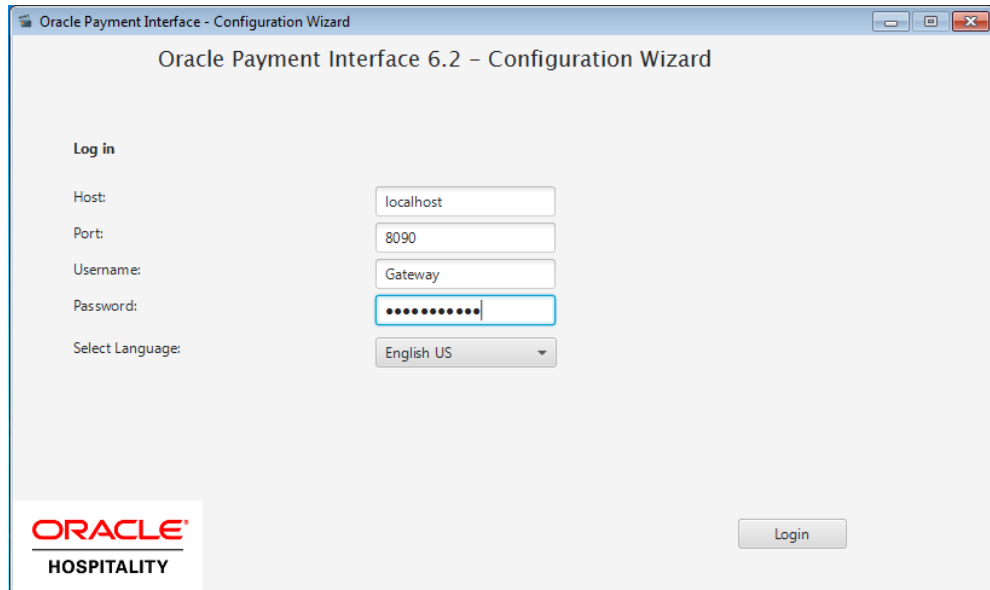


---

---

## 4 Configuring OPI

1. If manual start is required, run  
:`OraclePaymentInterface\V6.2\Config\LaunchWizard.exe`. Login as the Super user you created during OPI installation.

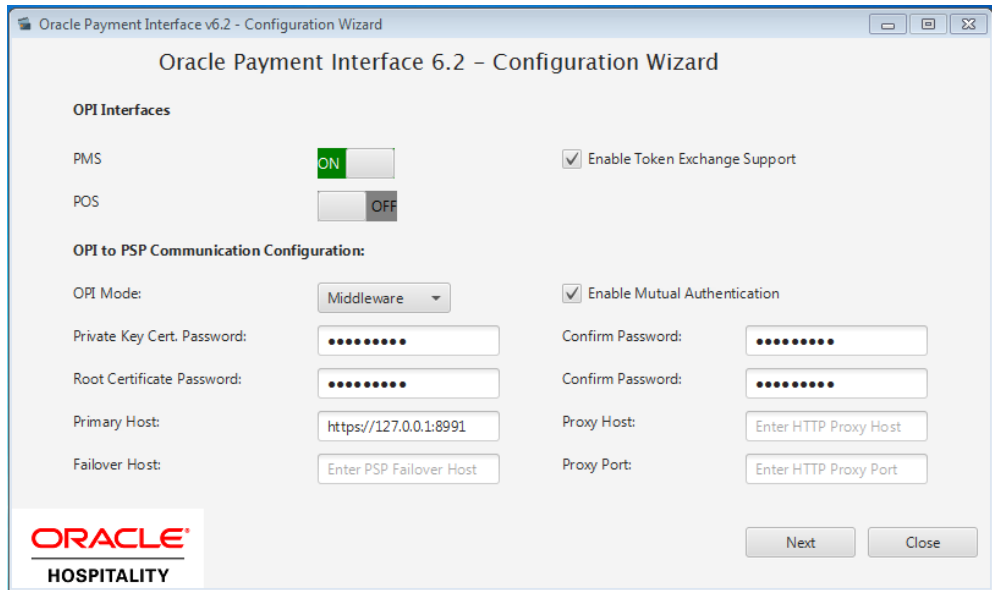


### OPI Interface

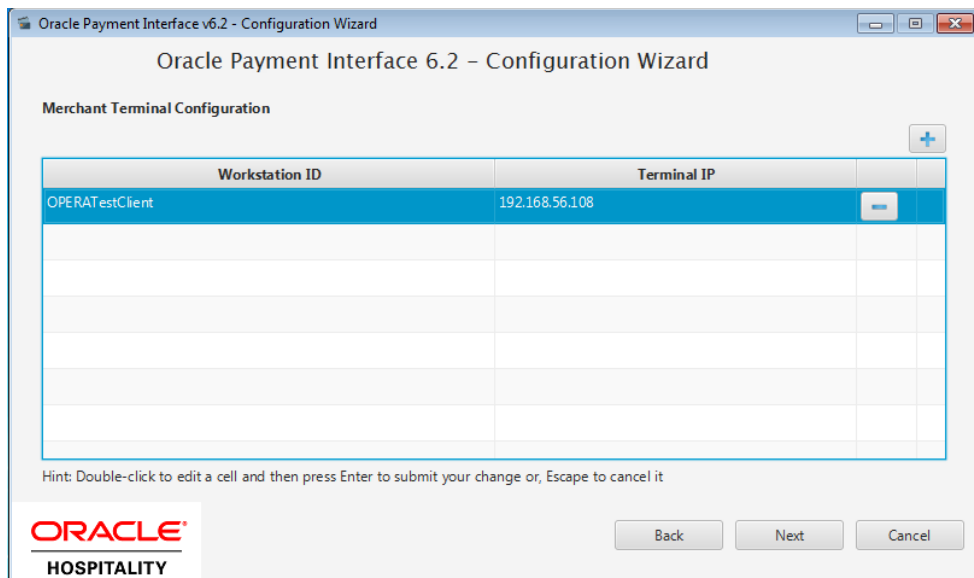
Turn PMS on, and select the *Enable Token Exchange Support* box. The Token Exchange functionality is separate for IFC8 merchant functionality.

### OPI to PSP Communication Configuration

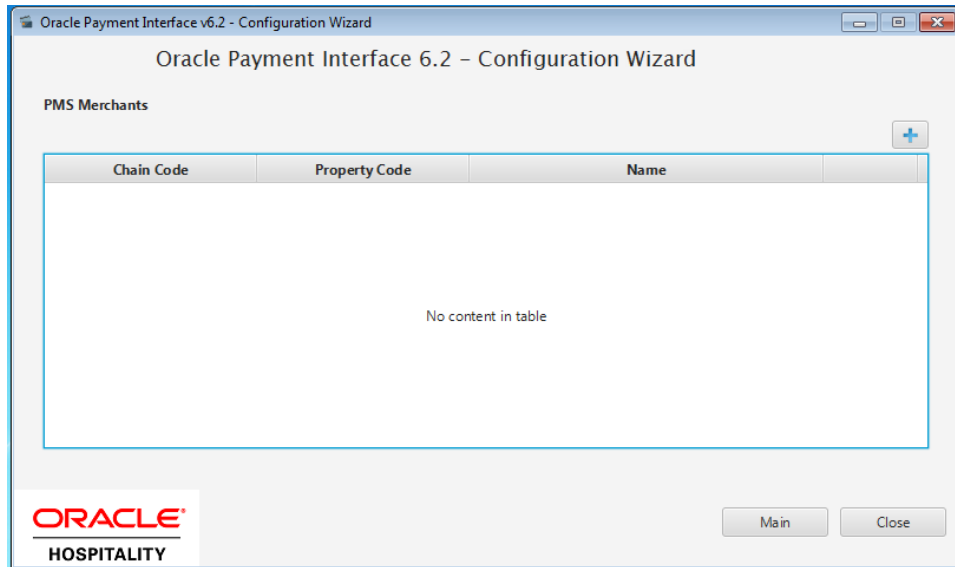
- From the **OPI Mode** drop-down list, select the **Terminal** for the PED direct connection or select **Middleware** for middleware connection.
- Enable Mutual Authentication, this supports two-way authentication. The PSP partner needs to provide a set of .cer and .pfx files. Load the .cer file into 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.



Below is terminal mapping if you select terminal mode.



2. Click the blue + icon to add a new merchant configuration for Suite8.



3. 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|xxxxxxxxxxxxxxxxxxxxxxxxxxxx
  - Enter the **IFC8 IP address** and **port** number for the Hotel Property Interface (IFC8) server.
  - Enter the **Merchant name**, **city**, and **country** information.
  - 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 6.2 - Configuration Wizard

**PMS Merchant**

OPERA Chain: SUITE8

Property Code: HOTEL

Name: Suite8 Test Hotel

City: Dusseldorf

State/Province: NRW

Country: Germany

IFC8 Key: TXoX18JHRZ3cUsmfOeXShJm52U48wo0

IFC8 Host IP: 127.0.0.1

IFC8 Host Port: 5041

Only Do Refund

**ORACLE**  
HOSPITALITY

4. Enter the Suite8 payment code for each card type & next.

Oracle Payment Interface 6.2 - Configuration Wizard

**Merchant Tender Configuration**

OPERA Chain Code: SUITE8

Property Code: HOTEL

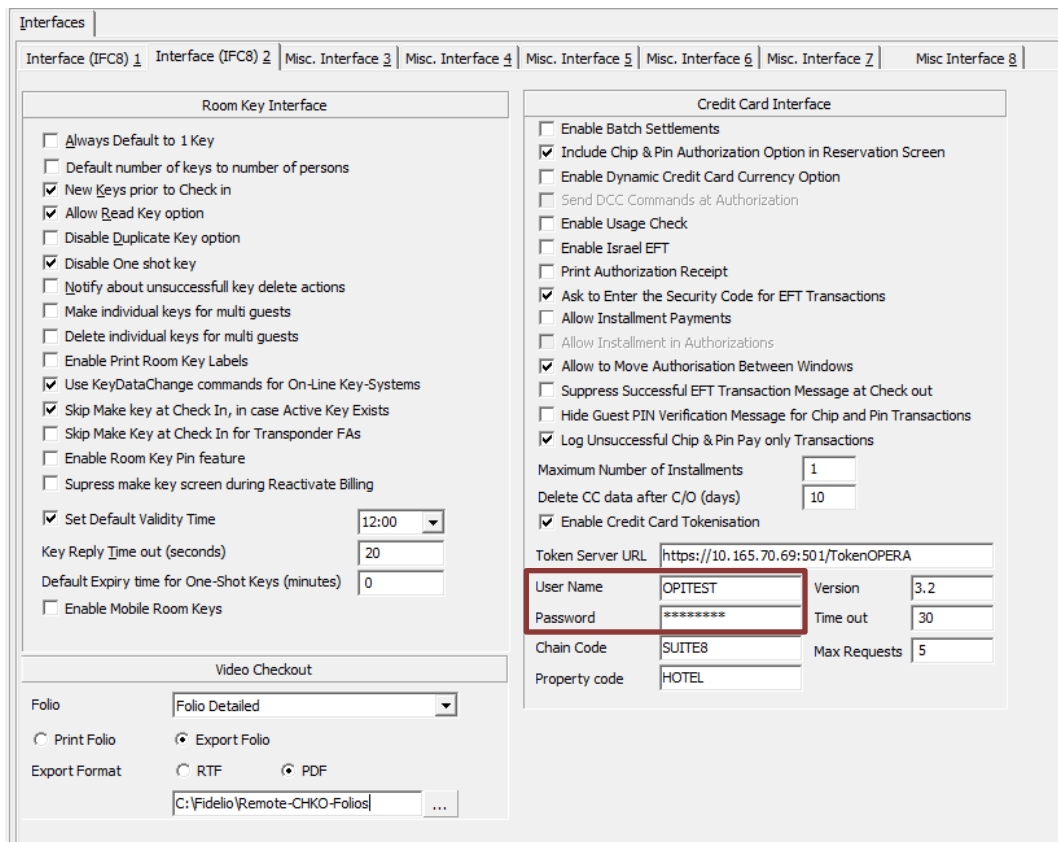
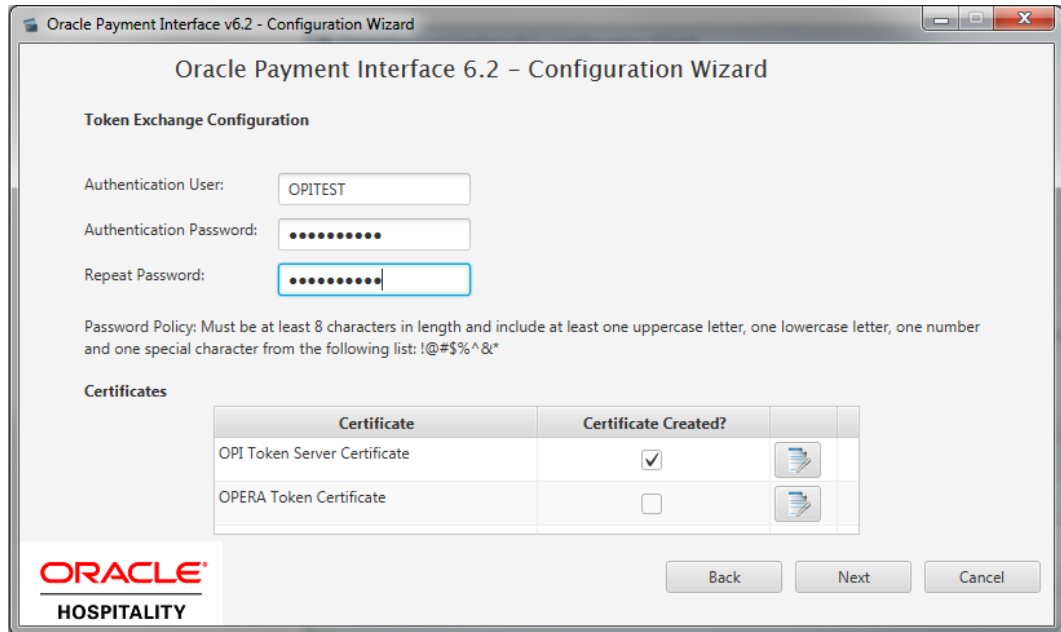
**Tenders:**

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

**ORACLE**  
HOSPITALITY

5. 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.**)



---

## 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:

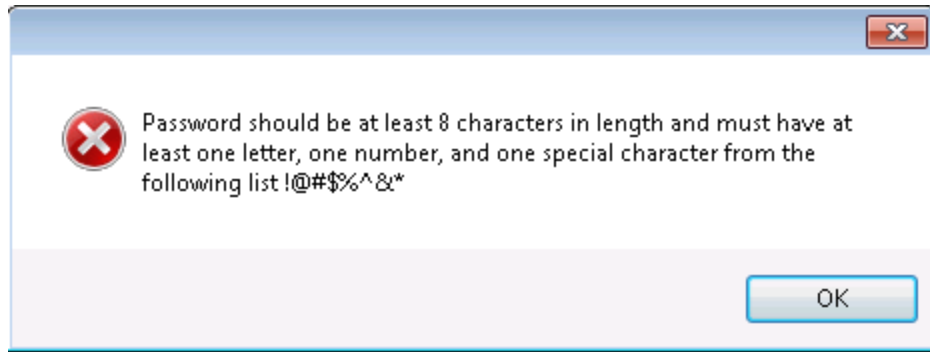
- A client side certificate file in the name of “OPI\_PSP\_1.pfx”, this is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password. If the file provided by PSP has a different name, rename to “OPI\_PSP\_1.pfx” before deploying it to OPI.
- The root 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. We expect the root certificate file provided by PSP to be in the format of .cer or .crt. For the demo purpose in this document, we assume the file has the name “ca-cert.crt”.

### Handling the Client Side Certificate

To deploy the client certificate on the OPI side, place the file in folder  
`\OraclePaymentInterface\v6.2\Services\OPI\key\`

The passwords set by the PSP 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.



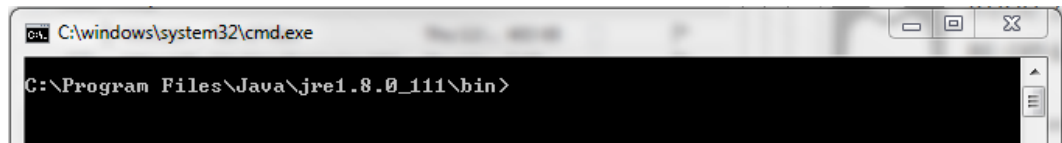
## Handling the Root Certificate File

In order to load the root certificate file for the PSP server certificate into the Java key store, perform the following steps:

### Creating a JKS

From a command prompt change to the JRE bin folder, in order for the *keytool* command to be recognized.

The exact path of your JRE bin folder will depend on the environment on which you are running the commands, and the JRE version you have installed, but may be similar to the example path shown below;



The three commands below, when run in sequence;

- Create a new Java keystore,
- Delete the default key created inside the Java Key Store
- Import the supplied root certificate in its place:

In the following example, the root .cer / .crt file is named ca-cert.crt, and is located in the folder *C:\Certificates*. Adjust file names and paths to be relevant to your details. OPI expects that the Java key store file that contains the root certificate for PSP server certificate to be in the name of "OPI\_PSP\_1Root".

```
keytool -genkey -alias tempalias -keystore C:\Certificates\OPI_PSP_1Root
```

You must supply some basic information during the creation of the Java keystore, including a password.

```
Command Prompt
C:\Program Files\Java\jre1.8.0_111\bin>keytool -genkey -alias tempalias -keystore C:\Certificates\OPI_PSP_1Root
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: QA User
What is the name of your organizational unit?
[Unknown]: QA Dept
What is the name of your organization?
[Unknown]: Oracle
What is the name of your City or Locality?
[Unknown]: Reading
What is the name of your State or Province?
[Unknown]: Berkshire
What is the two-letter country code for this unit?
[Unknown]: UK
Is CN=QA User, OU=QA Dept, O=Oracle, L=Reading, ST=Berkshire, C=UK correct?
[no]: yes

Enter key password for <tempalias>
<RETURN if same as keystore password>:

C:\Program Files\Java\jre1.8.0_111\bin>
```

You should use the same key password as for the keystore password when prompted. (i.e. RETURN if same as keystore password – Press Enter)

```
keytool -delete -alias tempalias -keystore C:\Certificates\OPI_PSP_1Root
```

```
Command Prompt
C:\Program Files\Java\jre1.8.0_111\bin>keytool -delete -alias tempalias -keystore C:\Certificates\OPI_PSP_1Root
Enter keystore password:

C:\Program Files\Java\jre1.8.0_111\bin>
```

```
keytool -import -alias myrootca -file C:\Certificates\ca-cert.crt -keystore C:\Certificates\OPI_PSP_1Root -trustcacerts
```



```

C:\Program Files\Java\jre1.8.0_111\bin>keytool -import -alias myrootca -file c:\
certificate\ca-root.crt -keystore C:\Certificate\OPI_PSP_1Root -trustcacerts
Enter keystore password:
Owner: CN=MerchantLink UAT Certificate Authority, OU=MerchantLink Security, O=Me
rchantLink LLC, C=US, EMAILADDRESS=adresner@merchantlink.com
Issuer: CN=MerchantLink UAT Certificate Authority, OU=MerchantLink Security, O=Me
rchantLink LLC, C=US, EMAILADDRESS=adresner@merchantlink.com
Serial number: f75660745438ad3c9607277da157f94
Valid from: Thu Nov 13 19:41:15 GMT 2014 until: Wed Nov 13 19:41:15 GMT 2024
Certificate fingerprints:
    MD5:  03:C8:F1:FB:8F:31:62:51:0C:78:9E:A0:05:EE:45:C3
    SHA1: E0:78:6D:D7:B6:CB:68:0D:33:6E:0A:FD:86:0E:D1:CA:28:19:D0:D5
    SHA256: B1:5E:32:60:94:F7:8B:08:2C:33:AA:A1:A5:C5:64:24:2D:1F:F4:CC:7C:
AD:A2:85:F6:2D:36:4C:9D:23:99:FB
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:
#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 22 7A DA 83 AD 16 E2 60  7D C0 82 17 76 9F C1 2C  "z.....".....v...
0010: BC DD 41 C0                ..A.
]
]
#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:0
]
#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
DigitalSignature
Key_CertSign
Crl_Sign
]
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 22 7A DA 83 AD 16 E2 60  7D C0 82 17 76 9F C1 2C  "z.....".....v...
0010: BC DD 41 C0                ..A.
]
]
Trust this certificate? [no]: yes
Certificate was added to keystore

C:\Program Files\Java\jre1.8.0_111\bin>

```

Verify the new Java keystore's details by running the following command if required;

```
keytool -list -keystore c:\Certificates\OPI_PSP_1Root
```

```

C:\Program Files\Java\jre1.8.0_111\bin>keytool -list -keystore c:\Certificate\OP
I_PSP_1Root
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

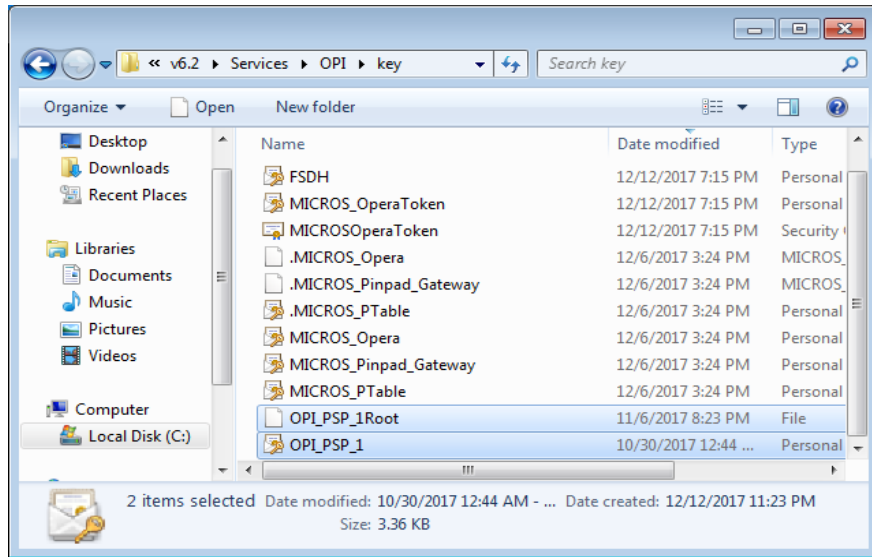
Your keystore contains 1 entry

myrootca, 23-Nov-2016, trustedCertEntry,
Certificate fingerprint (SHA1): E0:78:6D:D7:B6:CB:68:0D:33:6E:0A:FD:86:0E:D1:CA:
28:19:D0:D5

C:\Program Files\Java\jre1.8.0_111\bin>

```

OPI\_PSP\_1.pfx & OPI\_PSP\_1Root must be located in the following folder:  
 \OraclePaymentInterface\v6.2\Services\OPI\key\



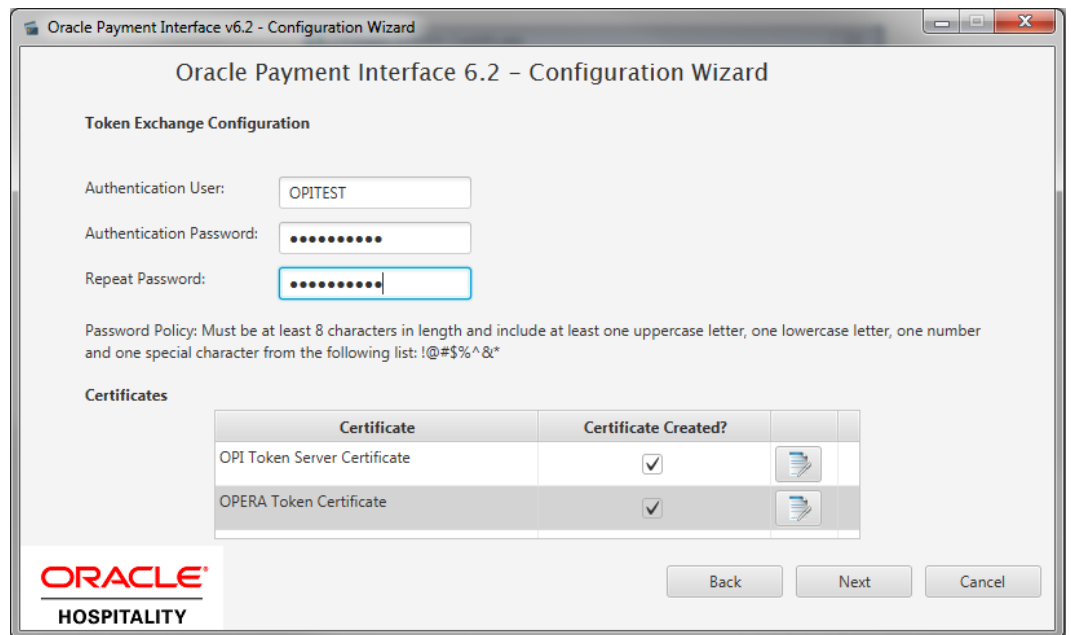
### Updating a JKS with a new PSP certificate

If this is an existing OPI On Premise Token Exchange installation, and you are importing a new PSP certificate prior to an existing key expiring, the current OPI\_PSP\_1.pfx & OPI\_PSP\_1Root, should be deleted from the `\OraclePaymentInterface\v6.2\Services\OPI\key\` folder prior to following the steps above to import new certificate file.

### OPI - Server Side Certificates

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

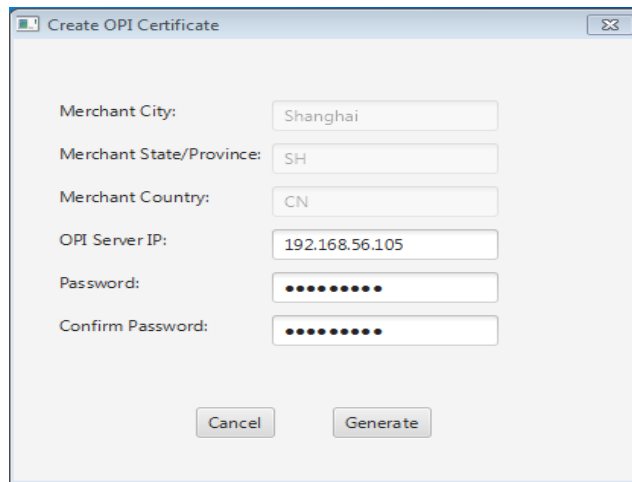
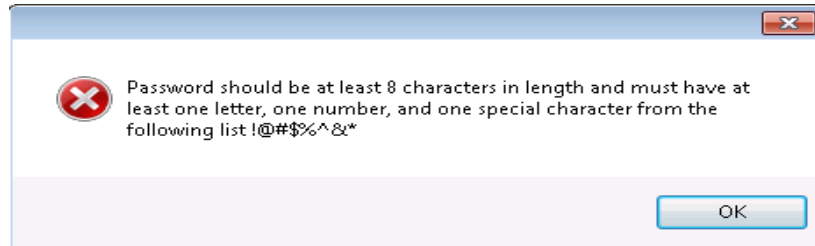
1. Click **Create OPI Token Certificates** to proceed.



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;

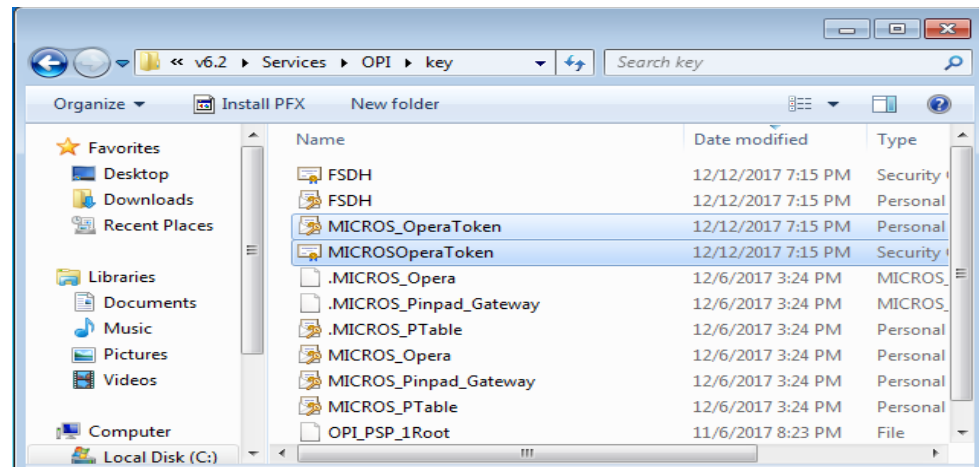
- Min 8 characters in length
- Min 1 Alpha Character
- Min 1 Numeric Character
- Min 1 Special Character from the following list !@#\$\$%^&\*



3. Click **Generate** to continue.

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

`\OraclePaymentInterface\v6.2\Services\OPI\key\`



**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.

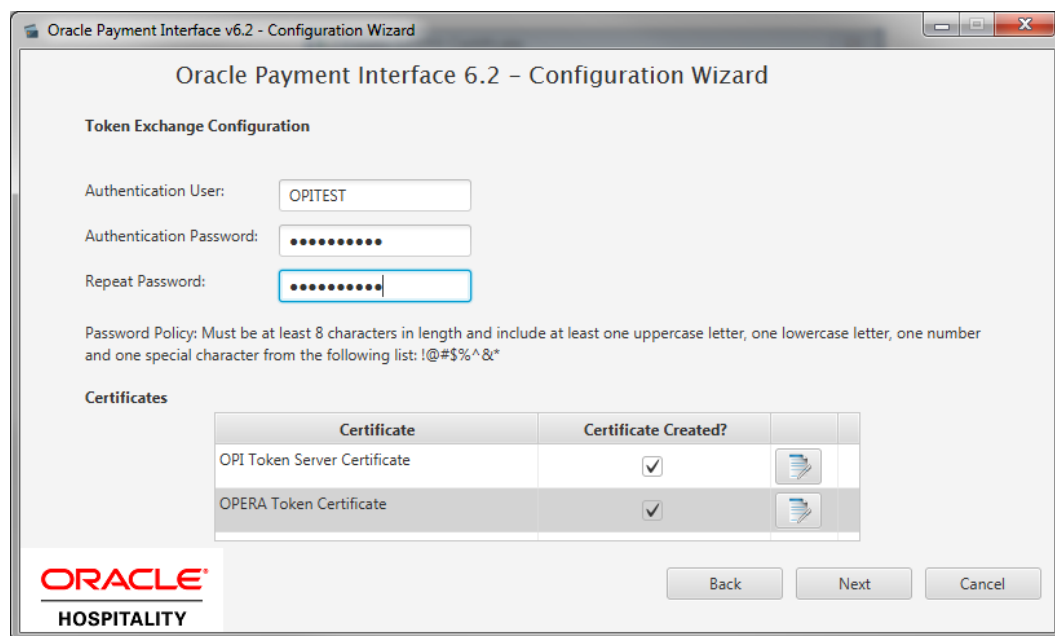
Copy the *MICROSOperaToken.cer* files to all of the Opera registered terminals that you will run the Token Exchange process from, and then import to Trusted Root Certification Authorities, using *mmc.exe* ([see below for more info](#))

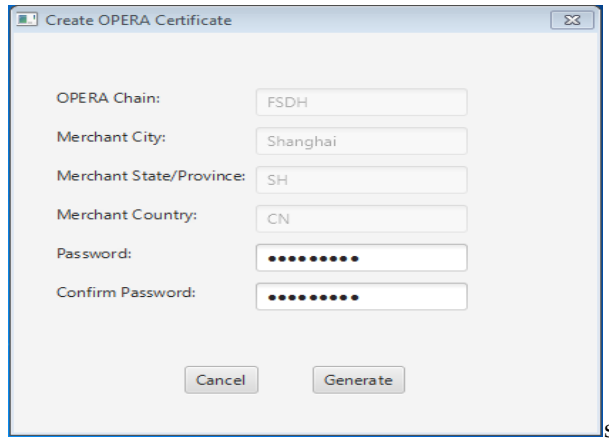
Close the Certificate generation screen. You should now see  under Certificate Created.

## OPI - Client Side Certificates

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

- 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.





- Once values entered and ready click **Generate**.  
This process will generate the SUITE8.pfx & SUITE8.cer files in the folder;  
`\OraclePaymentInterface\v6.2\Services\OPI\key\`

Name	Date modified	Type	Size
SUITE8.cer	26.02.2019 12:43	Security Certificate	1 KB
SUITE8.pfx	26.02.2019 12:43	Personal Informati...	3 KB
MICROS_OperaToken.pfx	07.11.2018 09:32	Personal Informati...	3 KB
MICROSOperaToken.cer	07.11.2018 09:32	Security Certificate	1 KB

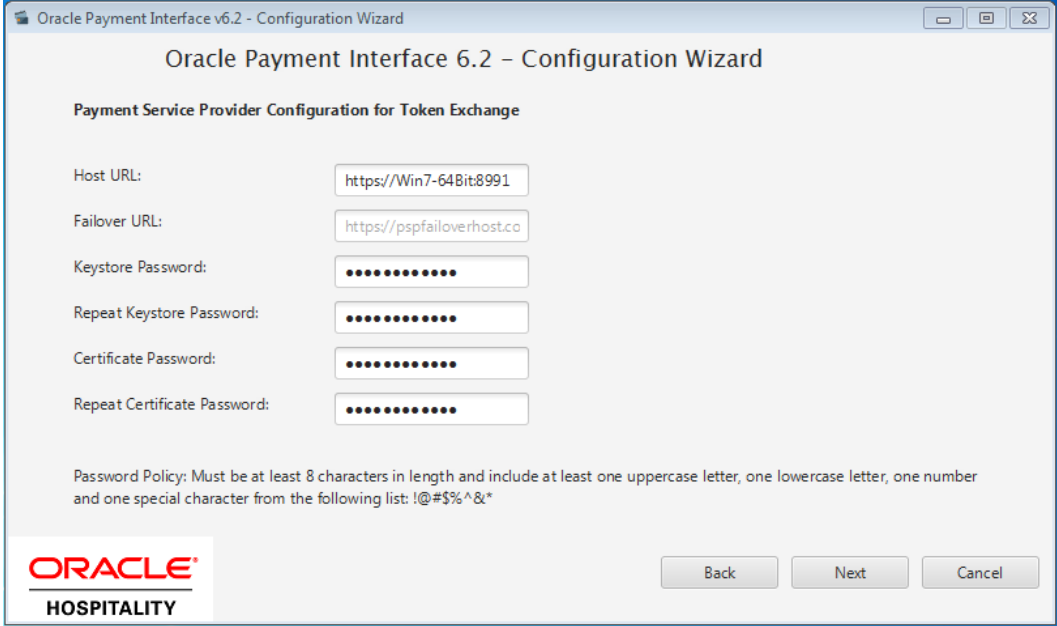
In the example above the certificates are named SUITE8 which is picked up from the **Chain Code** entered in previous steps. The certificates you create may be named differently relative to the environment in which they are being installed.

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.

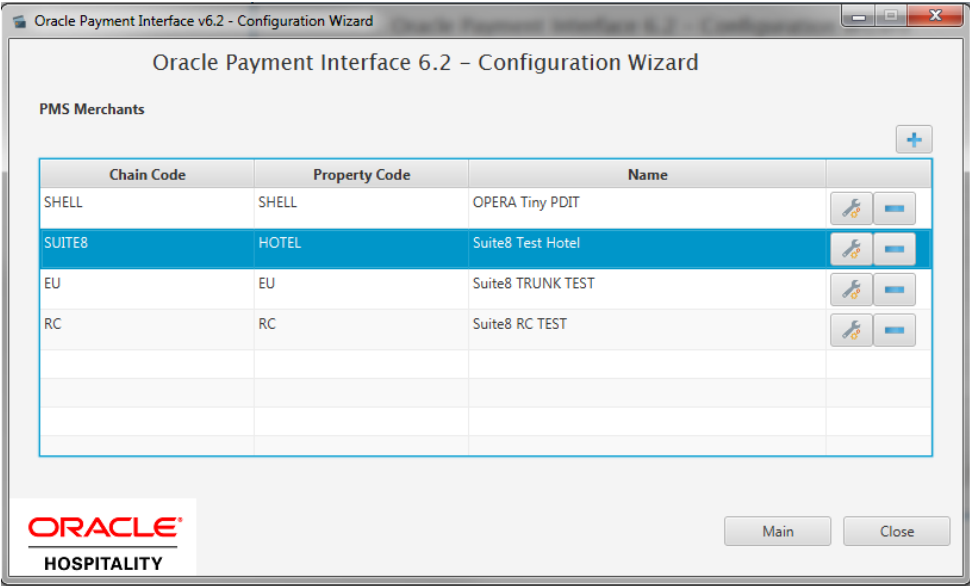
The next configuration relates to communication from OPI to the PSP host, and the PSP Client certificate credentials.



**Keystore Password:** The password provided with the client .pfx file by the PSP.

**Certificate Password:** Is the password that when creating the Java Key Store (JKS) in the steps below.

1. Click **Close**, and then restart the OPI service for the update to take effect.



---

---

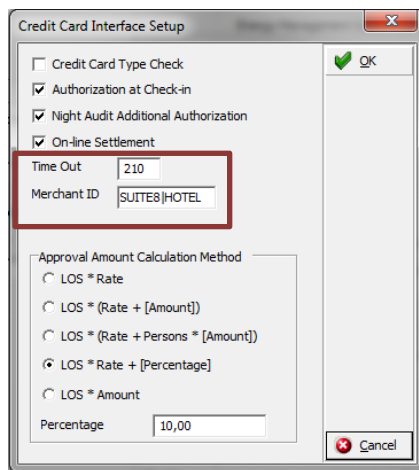
# 5 Suite8 Credit Card Configuration

## General Credit Card Interface Setup

### Global Settings

Log in to Suite8 and go to Configuration. Select the menu option **Global Settings | Interface | 1Interfaces (IFC8) | Credit Card Interface**.

- Ensure that 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]

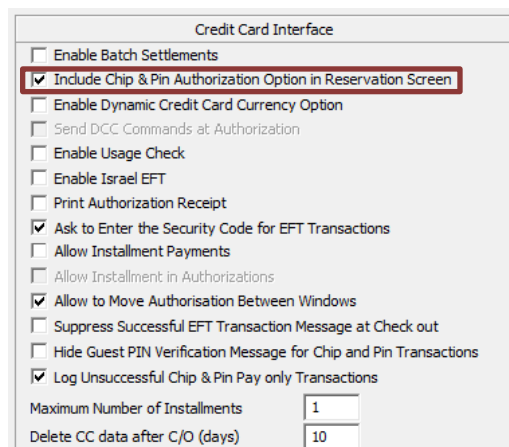
LOS \* Amount

Percentage: 10,00

OK

Cancel

- **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.
- **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.
- 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

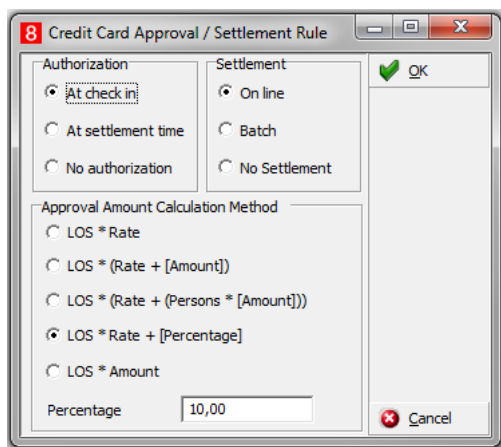
Delete CC data after C/O (days): 10

---

## Card Type Functionality Setup

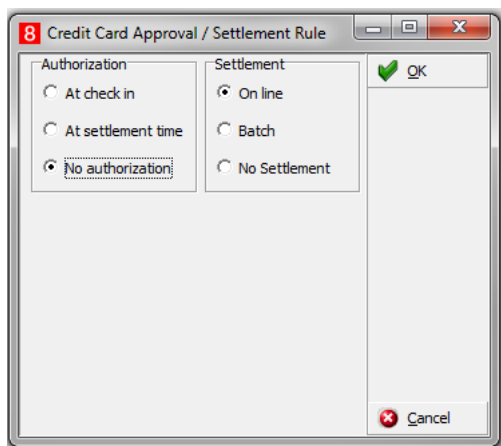
Define Credit card type functionality to handle authorization requests and settlement requests as per card type. EFT functionality with OPI requires following settings for all common **Credit Card types** (MasterCard, Visa, Amex, Diners/those card types who support amount authorization).

- 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.



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

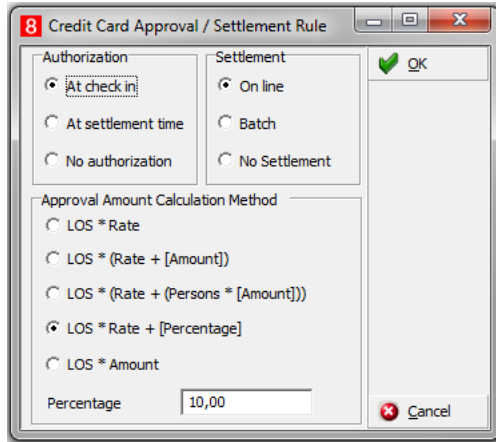
- Set **Authorization = No Authorization**. No authorization amount will be possible for this Card type.
- Set **Settlement = On Line** to enable functionality to send Payment request at the time of checkout/at the time when a payment shall be performed. Authorization of the payment amount will be done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





## Authorization Amount Calculation Method

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



The screenshot shows a dialog box titled "8 Credit Card Approval / Settlement Rule". It is divided into three main sections: "Authorization", "Settlement", and "Approval Amount Calculation Method".

- Authorization:** Radio buttons for "At check in" (selected), "At settlement time", and "No authorization".
- Settlement:** Radio buttons for "On line" (selected), "Batch", and "No Settlement".
- Approval Amount Calculation Method:** Radio buttons for "LOS \* Rate", "LOS \* (Rate + [Amount])", "LOS \* (Rate + (Persons \* [Amount]))", "LOS \* Rate + [Percentage]" (selected), and "LOS \* Amount". Below this is a text field for "Percentage" containing "10,00".

Buttons for "OK" and "Cancel" are located on the right side of the dialog.

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

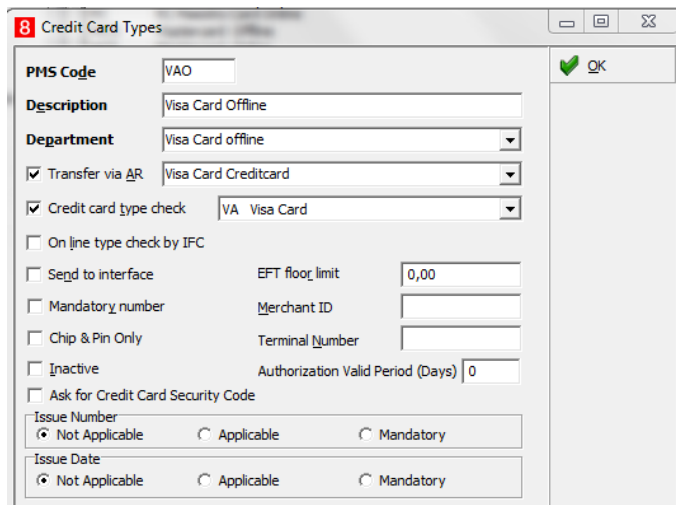
## Payment Type Configuration

### 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.



The screenshot shows a dialog box titled "8 Credit Card Types". It contains various configuration options for a credit card type.

- PMS Code:** VAO
- Description:** Visa Card Offline
- Department:** Visa Card offline
- Transfer via AR:** Checked, Visa Card Creditcard
- Credit card type check:** Checked, VA Visa Card
- On line type check by IFC:** Unticked
- Send to interface:** Unticked, EFT floor limit: 0,00
- Mandatory number:** Unticked, Merchant ID: [empty]
- Chip & Pin Only:** Unticked, Terminal Number: [empty]
- Inactive:** Unticked, Authorization Valid Period (Days): 0
- Ask for Credit Card Security Code:** Unticked
- Issue Number:** Radio buttons for "Not Applicable" (selected), "Applicable", and "Mandatory".
- Issue Date:** Radio buttons for "Not Applicable" (selected), "Applicable", and "Mandatory".

Buttons for "OK" and "Cancel" are located on the right side of the dialog.

## 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

The screenshot shows the 'Credit Card Types' configuration window in Suite8. The window title is '8 Credit Card Types'. It contains several fields and checkboxes for configuring a credit card type. The 'PMS Code' is 'VAP'. The 'Description' is 'Visa Card Online'. The 'Department' is 'Visa Card online'. The 'Transfer via AR' checkbox is checked, and the dropdown is 'Visa Card Creditcard'. The 'Credit card type check' checkbox is checked, and the dropdown is 'VA Visa Card'. The 'On line type check by IFC' checkbox is checked, and the 'IFC credit card type' is 'VA'. The 'Send to interface' checkbox is checked, and the 'EFT floor limit' is '0,00'. The 'Mandatory number' checkbox is unchecked. The 'Chip & Pin Only' checkbox is checked. The 'Terminal Number' field is empty. The 'Inactive' checkbox is unchecked, and the 'Authorization Valid Period (Days)' is '0'. The 'Ask for Credit Card Security Code' checkbox is unchecked. The 'Issue Number' section has 'Not Applicable' selected. The 'Issue Date' section has 'Not Applicable' selected. The 'Authorization rule' section shows 'Authorization amount' as 'LOS \* Rate + [ 10 % ]', 'Authorization type' as 'At Check In', and 'Settlement type' as 'On line'. There is a 'Change' button next to the settlement type.

## 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

**8 Credit Card Types**

**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

Change

## 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) etc...

**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 = Onlin - will use CpPayOnly messages to IFC8

**8 Credit Card Types**

**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

Change

# Tokenization Setup

## User Right to Enable the Tokenization Feature

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

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

## Tokenization Functionality Settings

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

Credit Card Interface

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

Maximum Number of Installments:

Delete CC data after C/O (days):

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.

Parameter Name	Value	Description
Token Server URL	https:// <i>IP Address of PC OPI is installed on</i> :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.

Parameter Name	Value	Description
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://10.165.70.69:501/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)

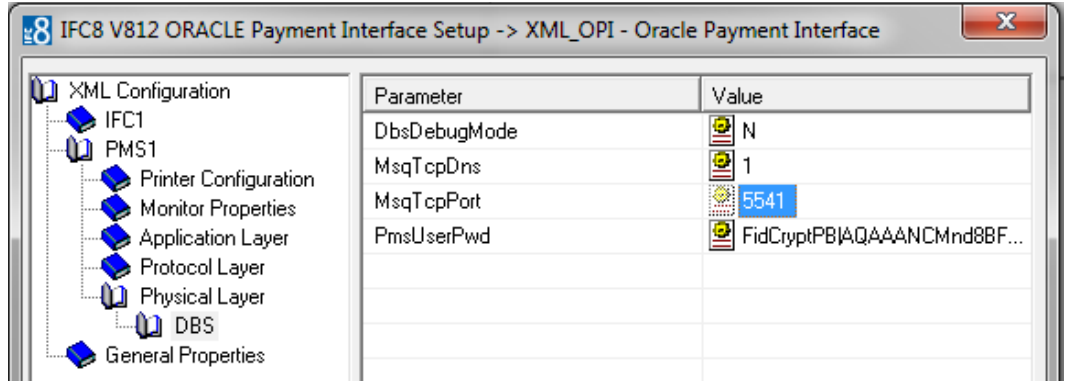
To configure the link between the interfaces:

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 in the IFC8 Database Configuration (ICFG\_ID).

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

Parameter	Value
IfcNum	18

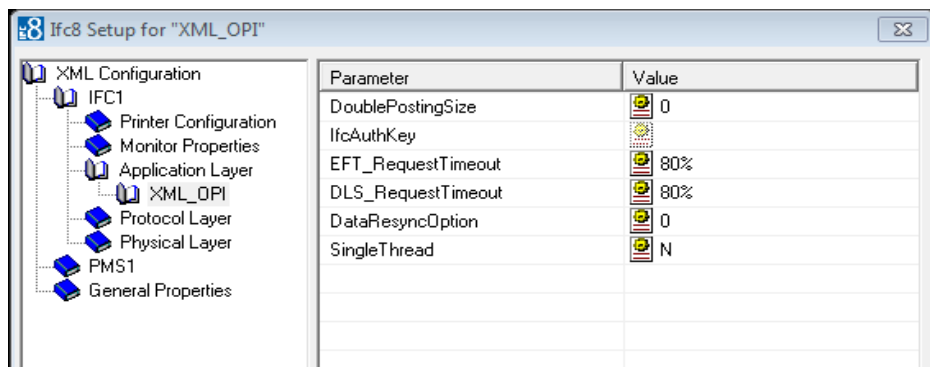
3. Go to the **PMS1 | Physical Layer | DBS**
4. Enter the port number into Parameter value **MsqTcpPort**. This is the port IFC8 uses to communicate with Suite8 PMS.
5. Select **Enter** and **Apply** to re-initiate IFC8, and then click **Save**.



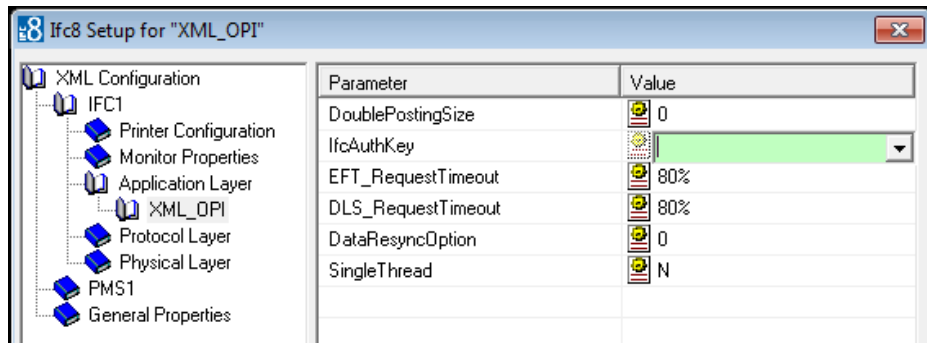
## Configuring encryption for the Hotel Property Interface (IFC8) with OPI

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

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

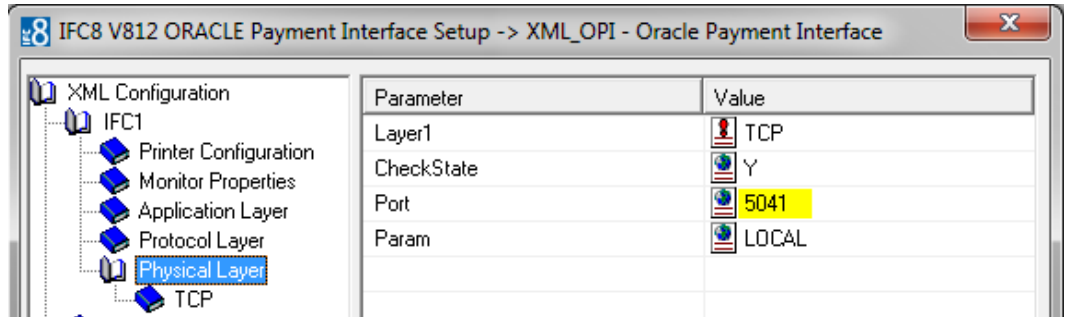


2. Copy the [generated key](#) from Configuring OPI - OPERA merchant step 3, and add "FidCrypt0S|" to the generated key as prefix.  
For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxxxx
3. Copy this string into IFC8 Parameter **IfcAuthKey** value field.



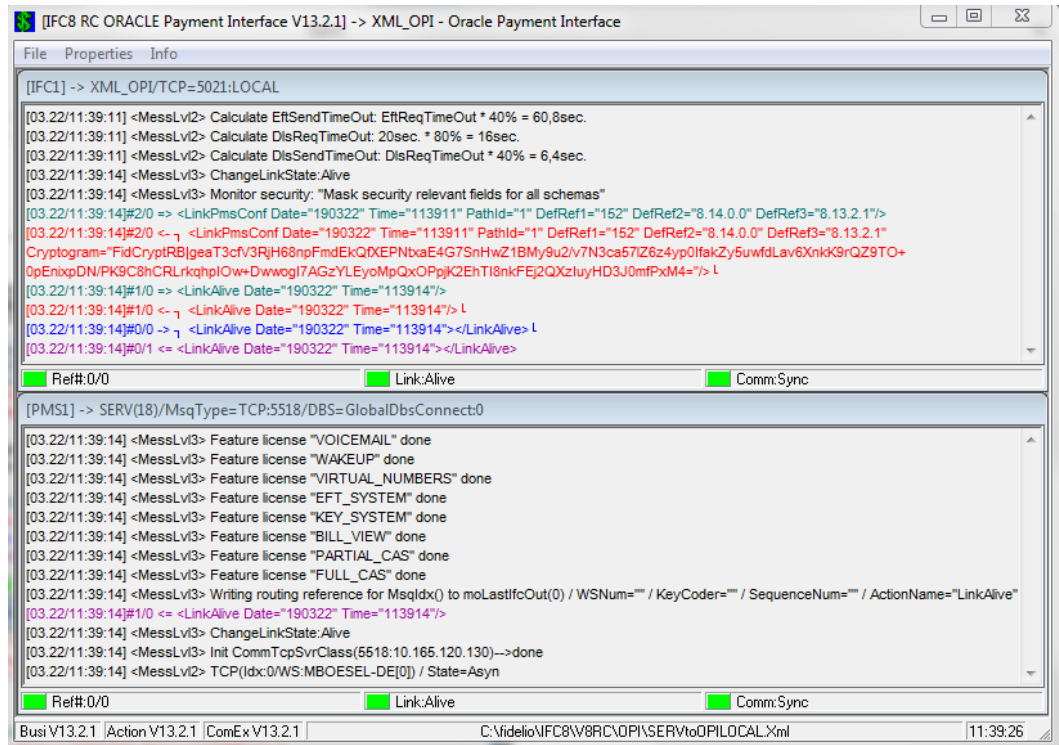
Parameter	Value
DoublePostingSize	0
IfcAuthKey	FidCrypt0SjGBZbw5SNDQ0I1...
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0

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.



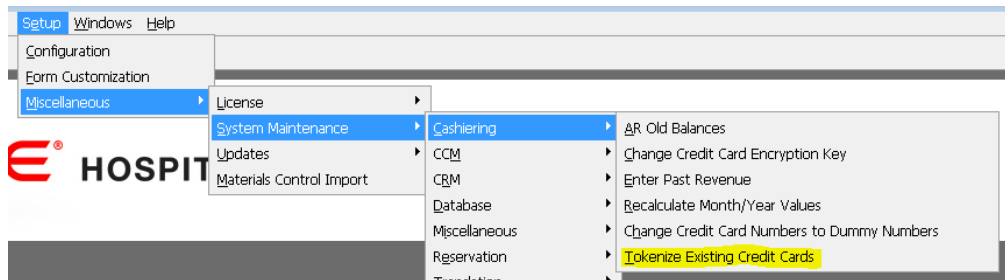
6. Click **Apply**, IFC8 reinitiates.
7. The **IfcAuthKey** value now shows an encrypted key and the entered string is now encrypted by IFC8.
8. Click **Save**, and then click **OK** to close the IFC8 Configuration form.

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

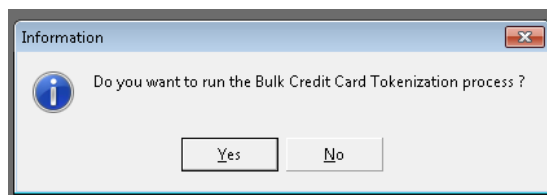


## Perform a Tokenization

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



A new window will open:



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.

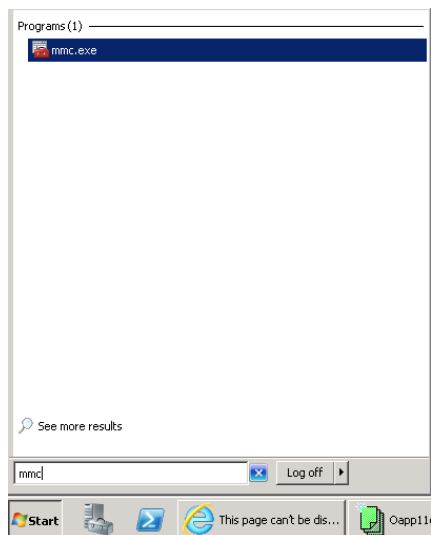
**Note:** After the successful replacement of credit card numbers with token ID's the process should **NOT** be executed again.

2. 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.

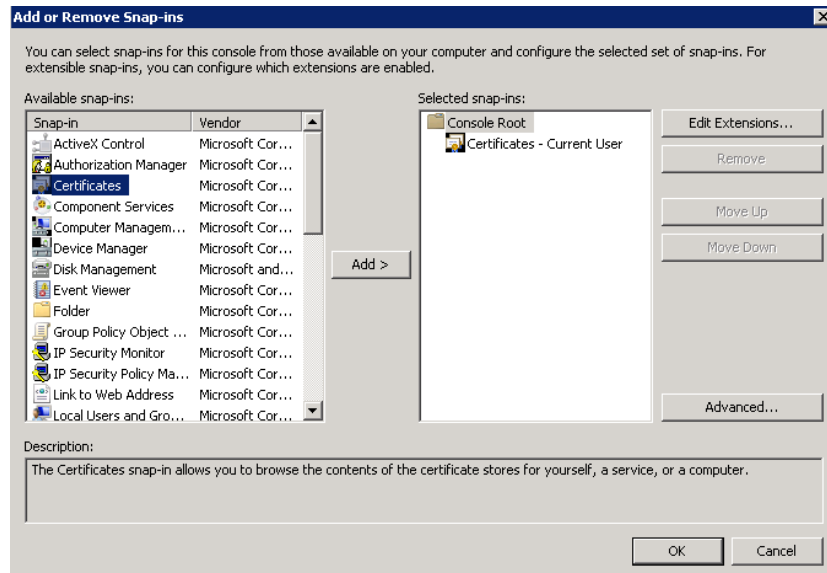
OPI only supports the **Convert CC** function; the other conversion options are not currently supported.

## Certificate Import using Microsoft Management Console

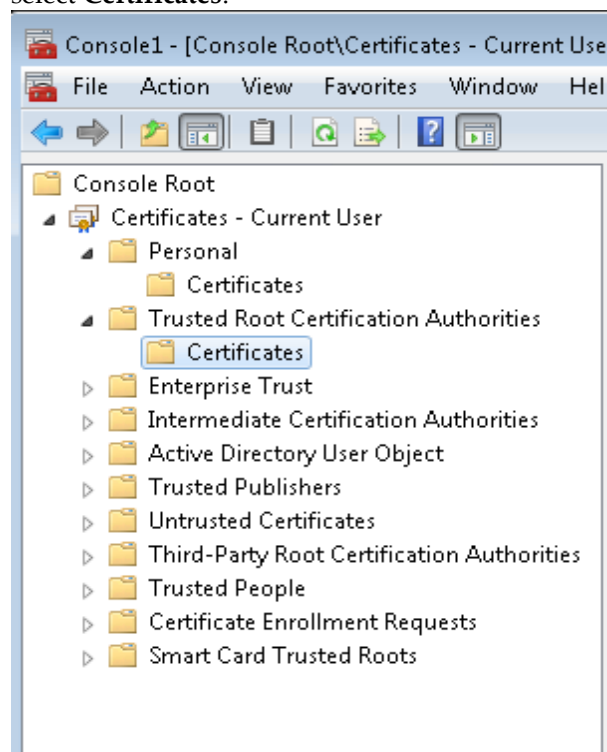
1. Find and open mmc.exe from the start menu.



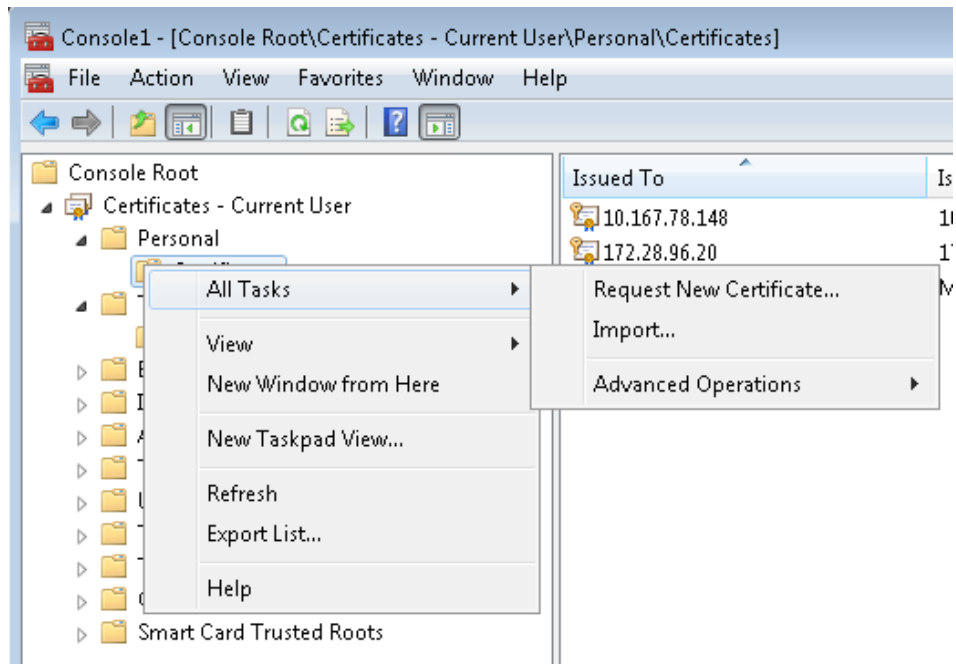
2. Go to **File | Add or Remove Snap-ins**, add certificates to **Selected snap-ins**, and then click **OK**



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



- 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 import is successful, then the certificates Common Name will be listed under the folder that was selected during import.