Oracle® Payment Interface

Oracle Hospitality OPERA Property Management System Installation Guide
Release 6.2
E92110-02

January 2020

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.

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

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
December 2017	• Initial publication
March 2019	• Documentation Updates
December 2019	• Updated OPERA client side certificates section and added content for Credit Card Payment Types.

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.

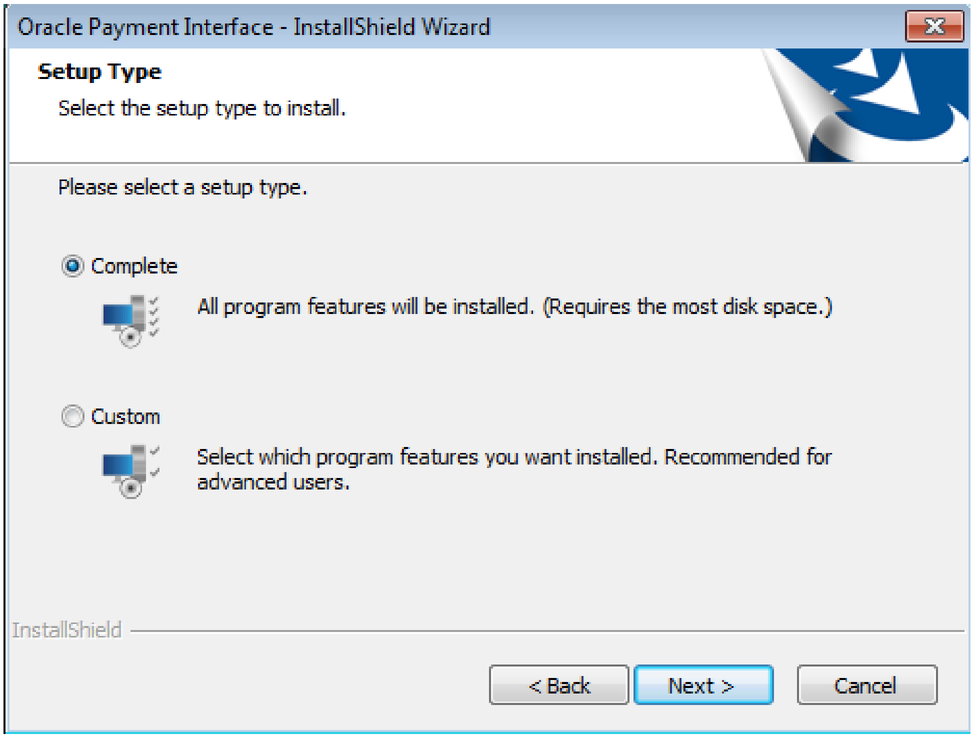
- OPERA Property Management System release 5.0.05.11 is the minimum release you can use to integrate with OPI.
- OPI 6.2 does not install a database. If doing a clean install of OPI, a database must be installed first.
- Upgrading to OPI 6.2 from OPI 6.1 and higher is supported but MPG versions are not 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.
- You cannot upgrade from MGDH 6.1.1.X to Native Driver 6.2 (must upgrade then switch to Native configuration).
- You cannot run upgrade from 6.1.1.X to 6.2 as unattended/silent (due to 6.1.1.X installation program differences between 6.2)
- The application requires Microsoft.NET Framework version 4.0 or higher.
- OPI requires at least 6 GB of free disk space and 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 appears.



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.)

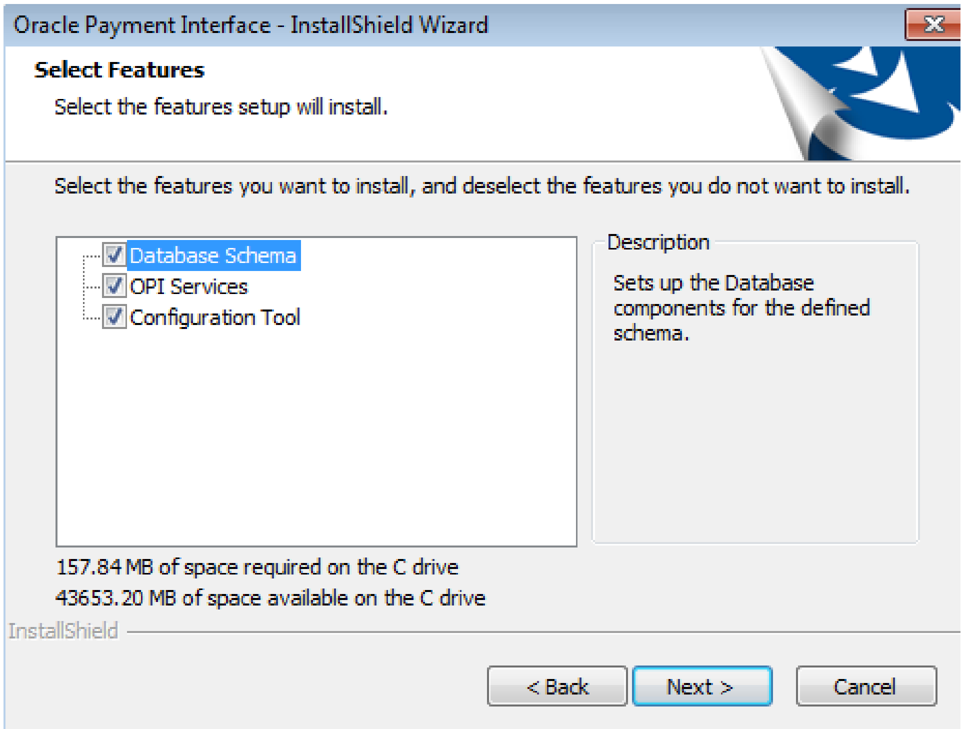
○ Custom

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, and then click **Next**.



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**.

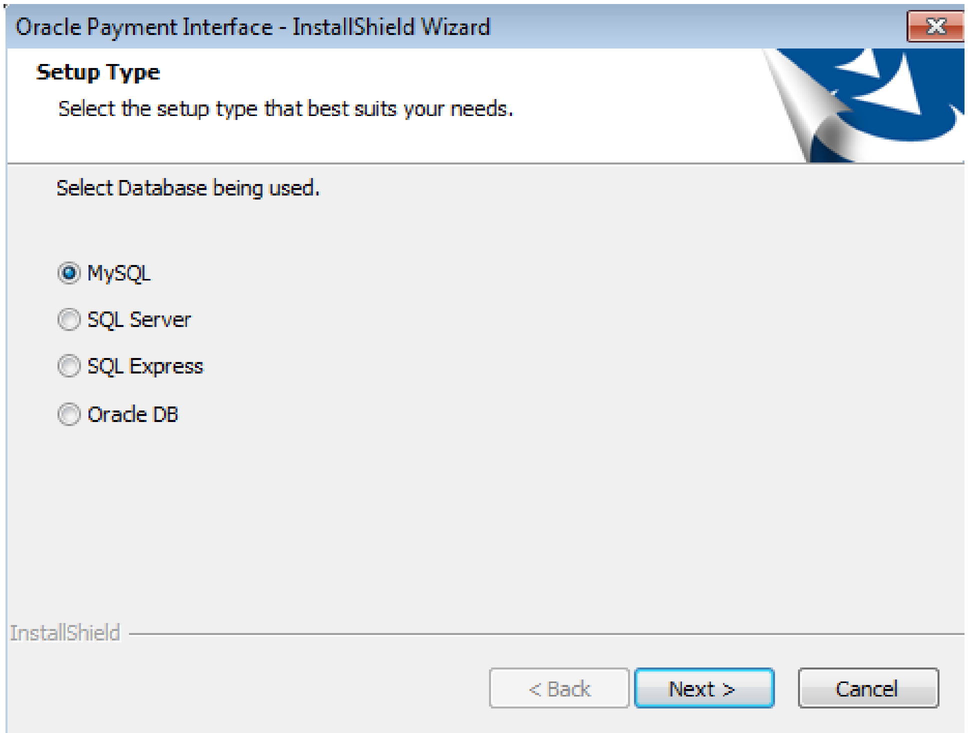
   The *Choose Destination Location* screen appears.

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

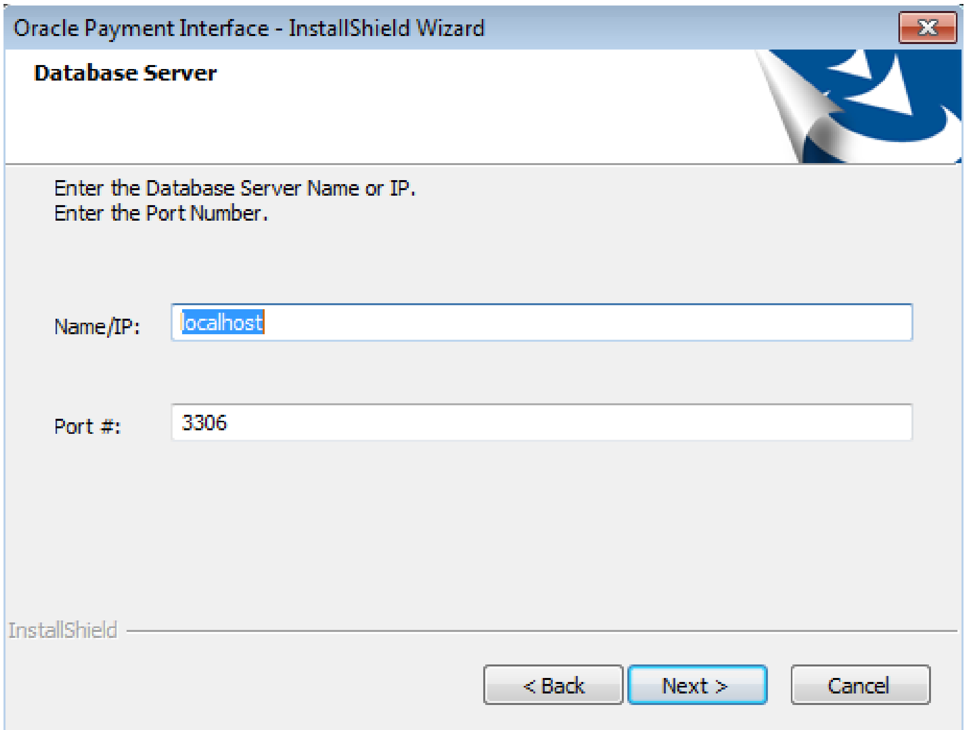
○ SQL Server

○ 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

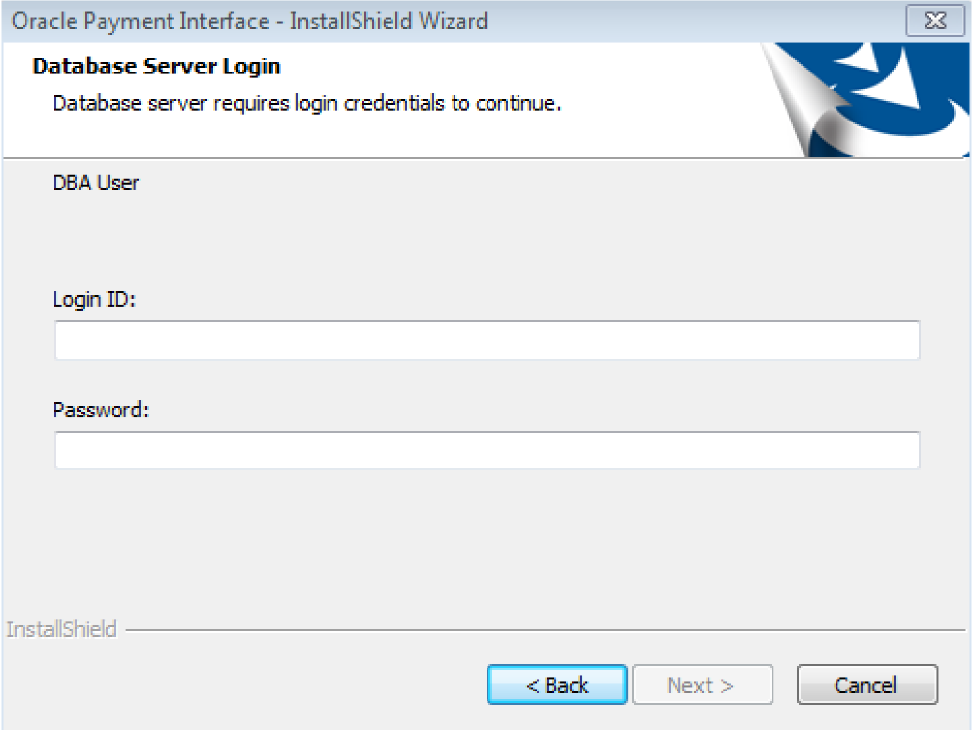
The *Database Server* screen appears.

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 **MySQL command link** in the **OPI Basic Install** doc for instructions. Setup will not complete if this is not done.

11. 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

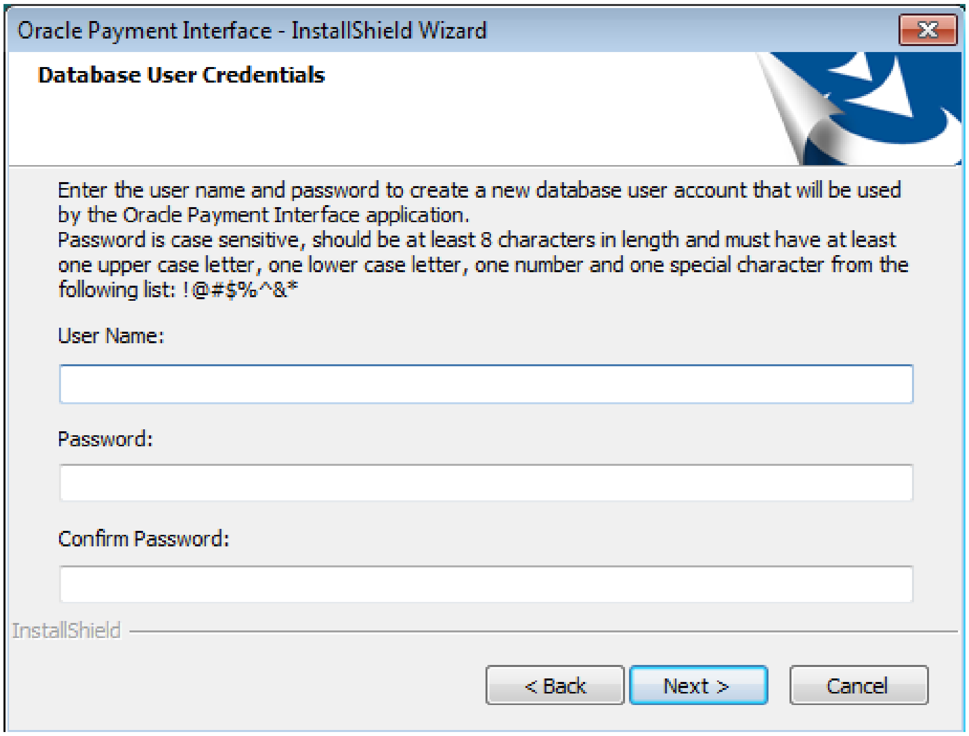
Login ID:

Password:

12. 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.



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:

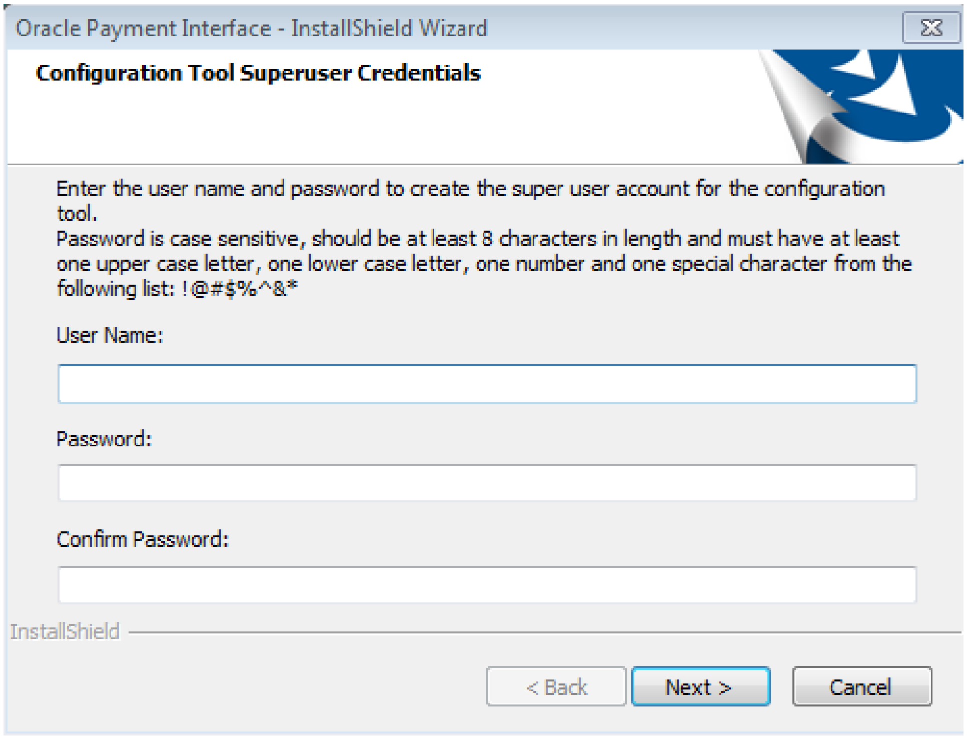
Password:

Confirm Password:

- **User Name**: Create a new user.
- **Password**: Create a password.
  - Password is case sensitive
  - Should be at least 8 characters in length
  - Must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*

13. Confirm the password, and then click **Next**.
14. Click **OK** on the *Database connection successful* dialog.
15. 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:

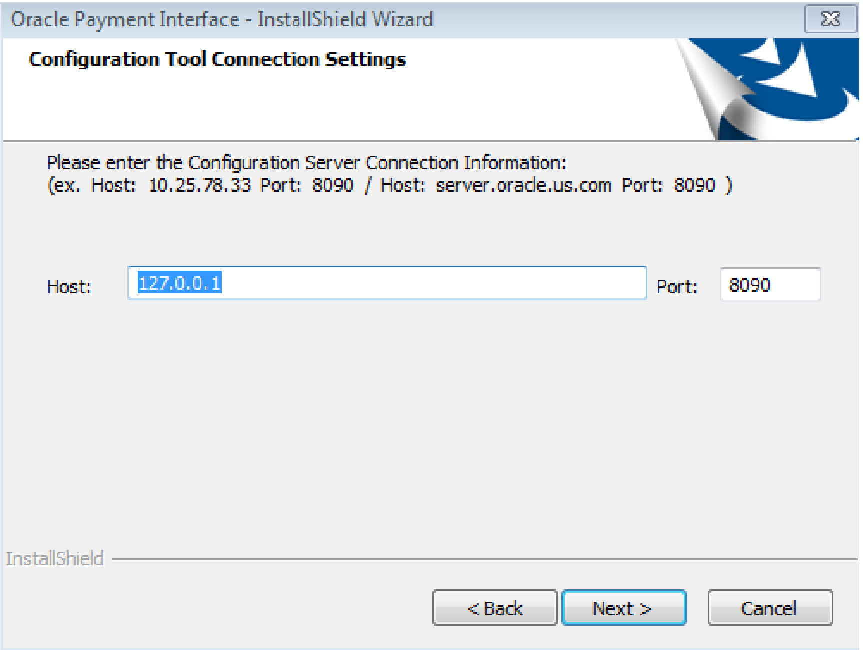
Password:

Confirm Password:

- **User Name**: This can be any user name. It does not have to be a Windows account user.
- **Password**: Create a password.
  - Password is case sensitive
  - Should be at least 8 characters in length
  - 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 *Create SuperUser operation successful* dialog.

    The *Configuration Tool Connection Settings* screen appears.


Oracle Payment Interface - InstallShield Wizard

Configuration Tool Connection Settings

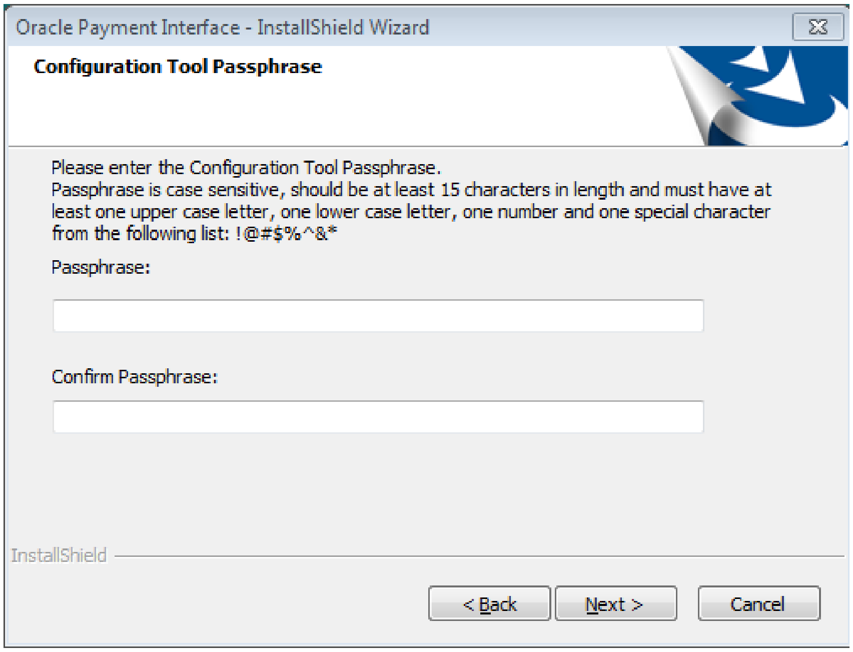
Please enter the Configuration Server Connection Information:
(ex. Host: 10.25.78.33 Port: 8090 / Host: server.oracle.us.com Port: 8090)

Host: 127.0.0.1 Port: 8090

- **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.
- Leave the default **Port** of 8090**.**

18. 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: !@#$%^&*

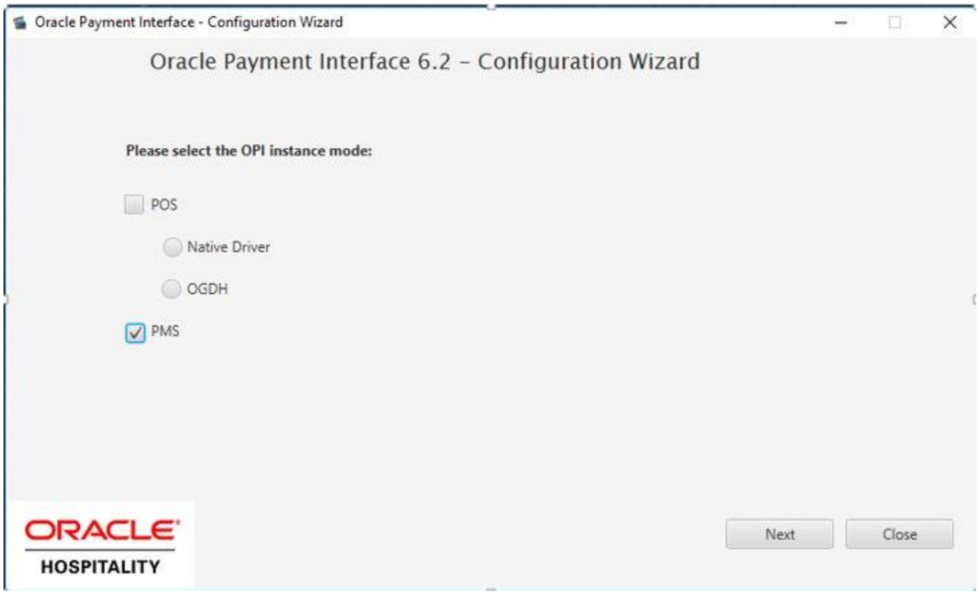
Passphrase:

Confirm Passphrase:

19. **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: !@#$%^&*

20. 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 6.2 – Configuration Wizard

Please select the OPI instance mode:

□ POS

○ Native Driver

○ OGDH

☑ PMS

21. Select **PMS**, Click **Next**.

3 Upgrading the OPI

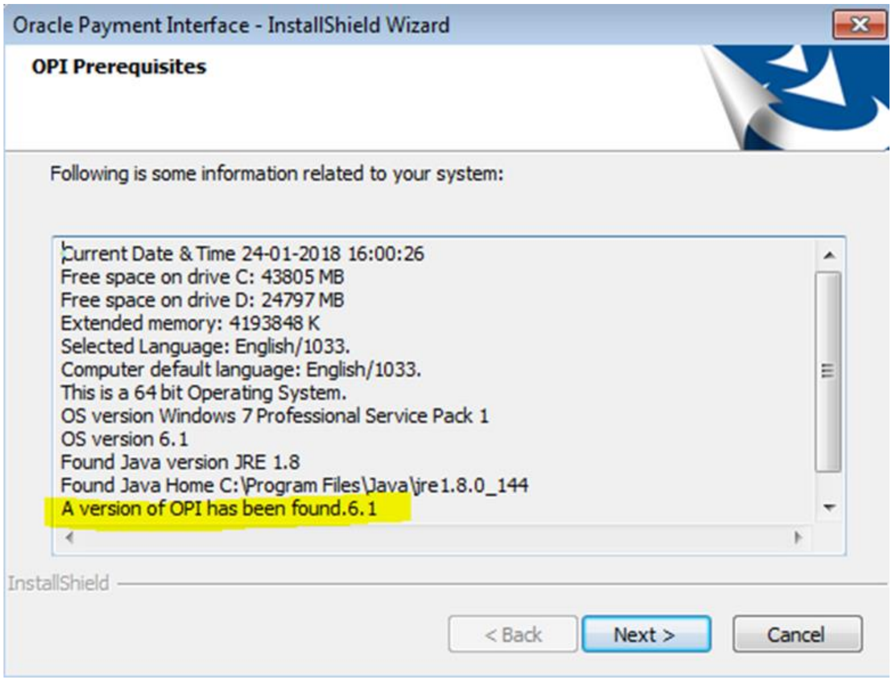
VERY IMPORTANT: Read and follow the upgrade directions.

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.



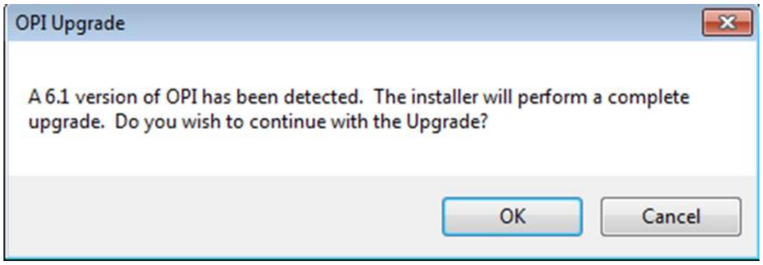
Oracle Payment Interface - InstallShield Wizard

OPI Prerequisites

Following is some information related to your system:

```
Current Date & Time 24-01-2018 16:00:26
Free space on drive C: 43805 MB
Free space on drive D: 24797 MB
Extended memory: 4193848 K
Selected Language: English/1033.
Computer default language: English/1033.
This is a 64 bit Operating System.
OS version Windows 7 Professional Service Pack 1
OS version 6.1
Found Java version JRE 1.8
Found Java Home C:\Program Files\Java\jre1.8.0_144
A version of OPI has been found.6.1
```

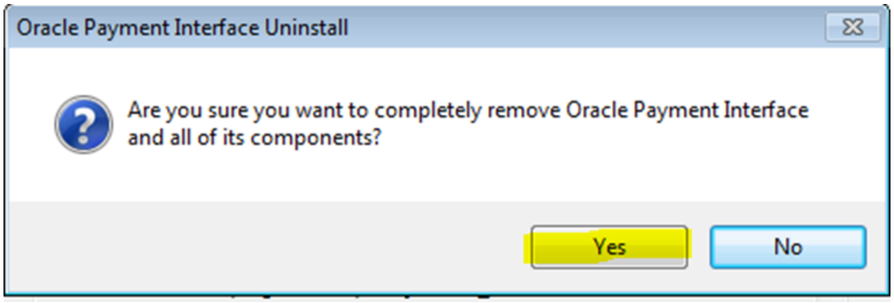
4. Click **Next** on the *OPI Prerequisites* screen.



OPI Upgrade

A 6.1 version of OPI has been detected. The installer will perform a complete upgrade. Do you wish to continue with the Upgrade?

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



Oracle Payment Interface Uninstall

Are you sure you want to completely remove Oracle Payment Interface and all of its components?

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.

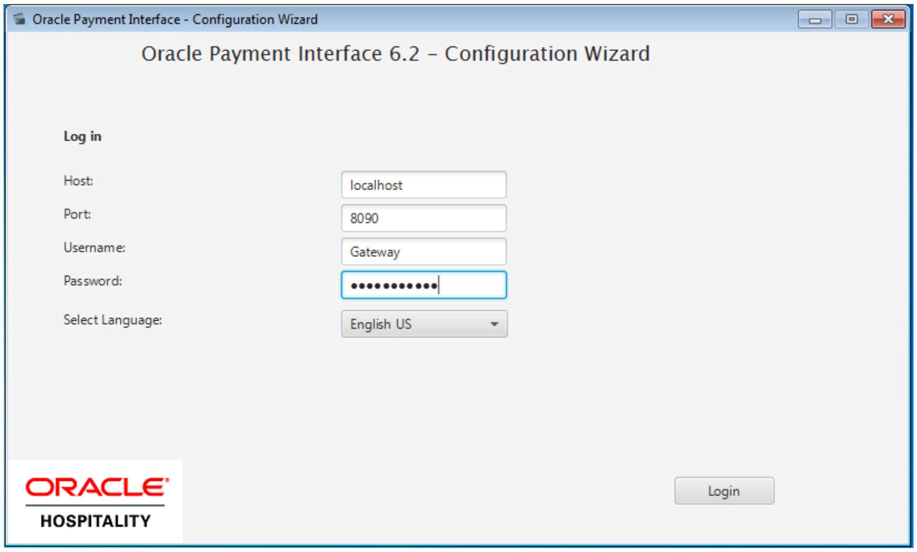
Continue to follow the on-screen directions.

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**.
2. Login as the Super user you created during OPI installation.


Oracle Payment Interface - Configuration Wizard
Oracle Payment Interface 6.2 – Configuration Wizard
ORACLE
HOSPITALITY
Login

Log in

Host: localhost

Port: 8090

Username: Gateway

Password: ●●●●●●●●●●●

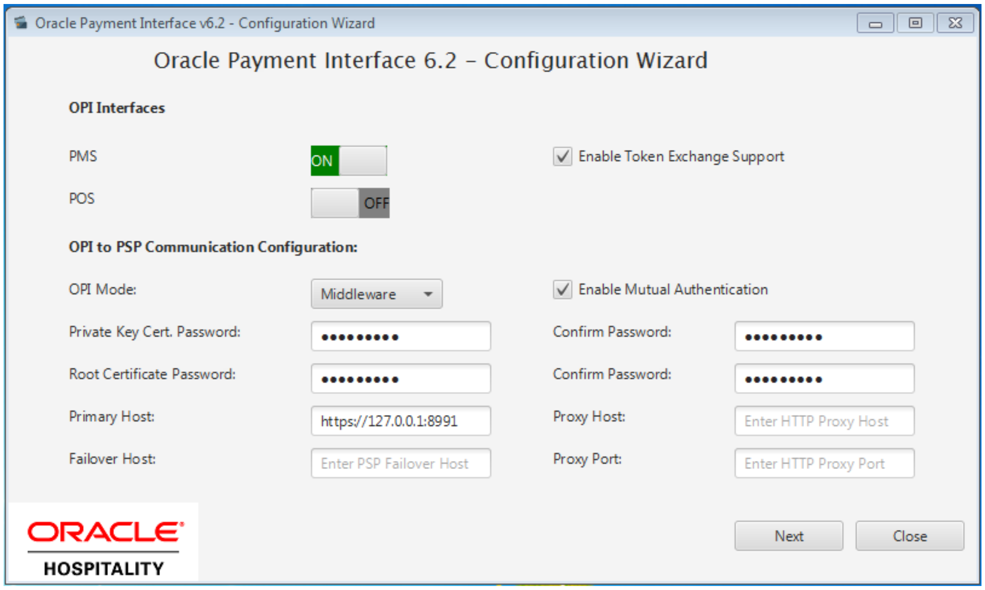
Select Language: English US

OPI Interface

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 OPI configuration will populate another window in further steps to input Workstation ID and IP address.



Oracle Payment Interface 6.2 – 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: ●●●●●●●●●

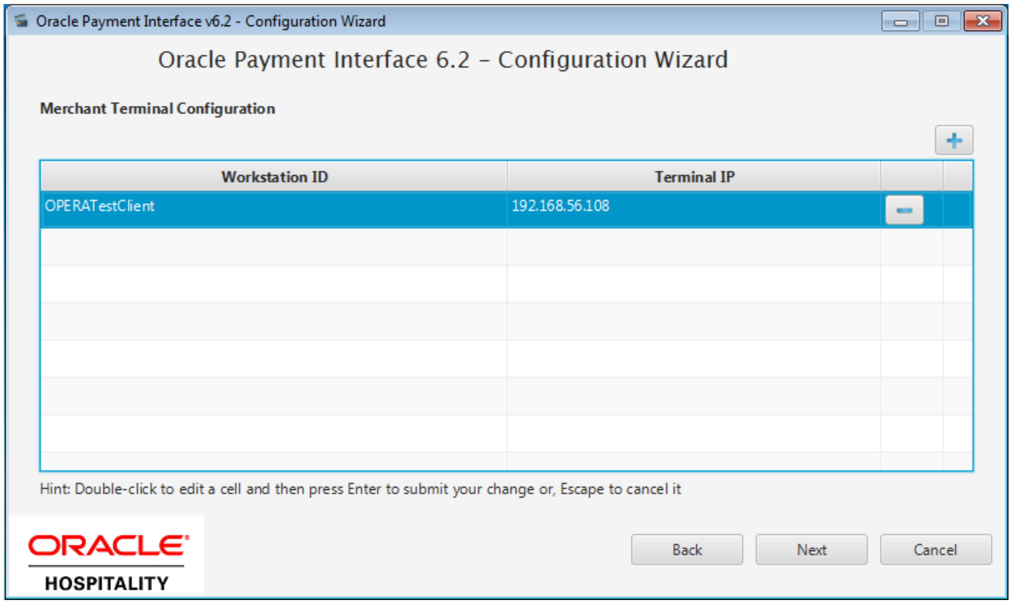
Primary Host: https://127.0.0.1:8991

Proxy Host: Enter HTTP Proxy Host

Failover Host: Enter PSP Failover Host

Proxy Port: Enter HTTP Proxy Port

Below is terminal mapping if you select terminal mode.



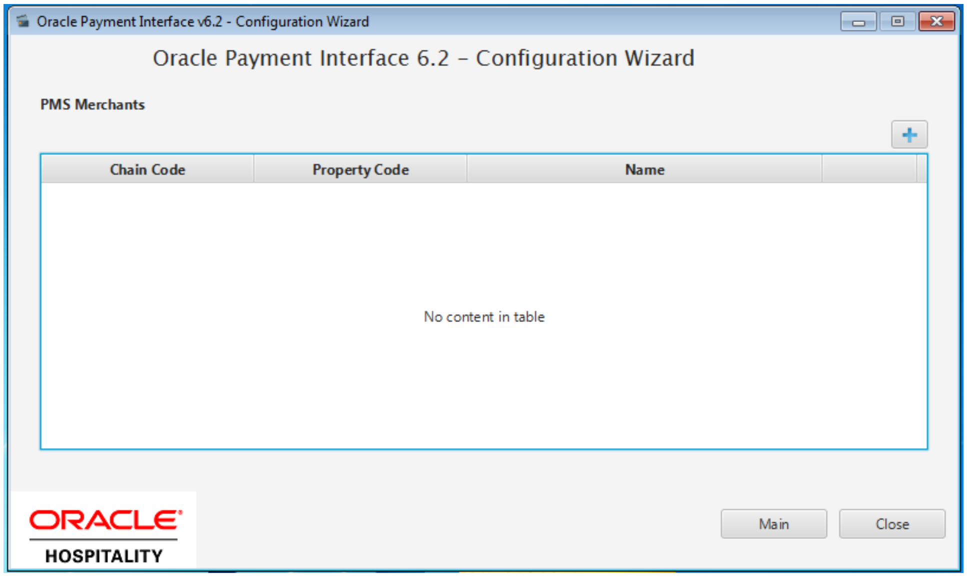
Oracle Payment Interface 6.2 – Configuration Wizard

Merchant Terminal Configuration

Workstation ID	Terminal IP
OPERATestClient	192.168.56.108

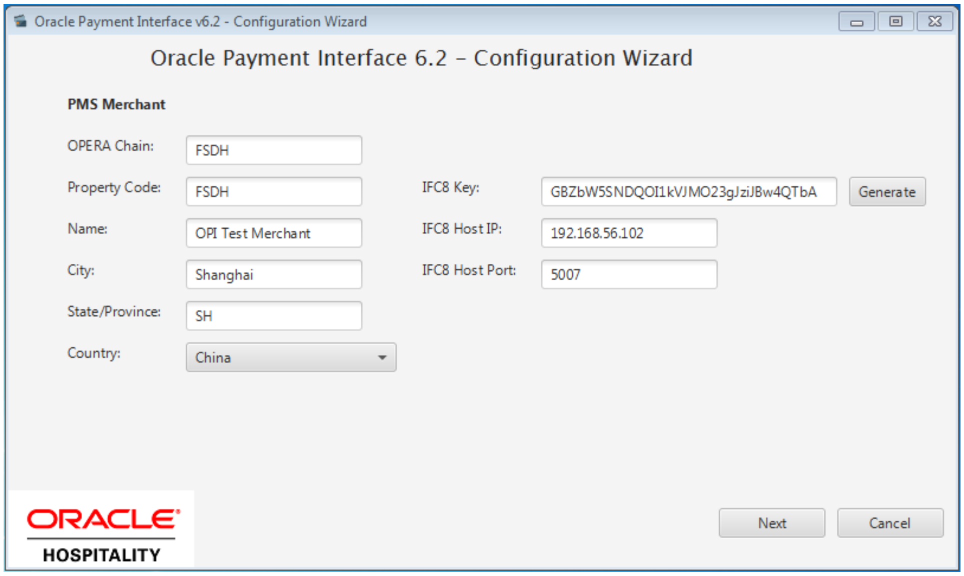
Hint: Double-click to edit a cell and then press Enter to submit your change or, Escape to cancel it

3. Click the blue + icon to add a new merchant configuration for OPERA.


Oracle Payment Interface v6.2 - Configuration Wizard
Oracle Payment Interface 6.2 – Configuration Wizard
PMS Merchants
+
Chain Code
Property Code
Name
No content in table
ORACLE
HOSPITALITY
Main
Close

4. To configure the OPERA merchant, enter the following information:
   - The *OPERA 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|xxxxxxxxxxxxxxxxxxxxxxxx
   - 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: FSDH

Property Code: FSDH

Name: OPI Test Merchant

City: Shanghai

State/Province: SH

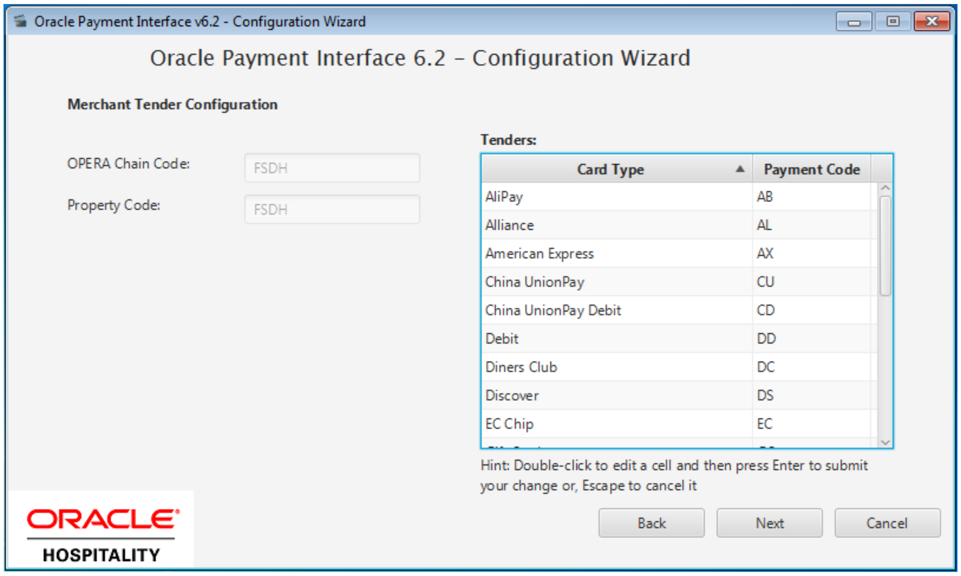
Country: China

IFC8 Key: GBZbW5SNDQOI1kVJMO23gJziJBw4QTbA

IFC8 Host IP: 192.168.56.102

IFC8 Host Port: 5007

5. Enter the OPERA payment code for each card type & next.



Oracle Payment Interface 6.2 – Configuration Wizard

Merchant Tender Configuration

OPERA Chain Code: FSDH

Property Code: FSDH

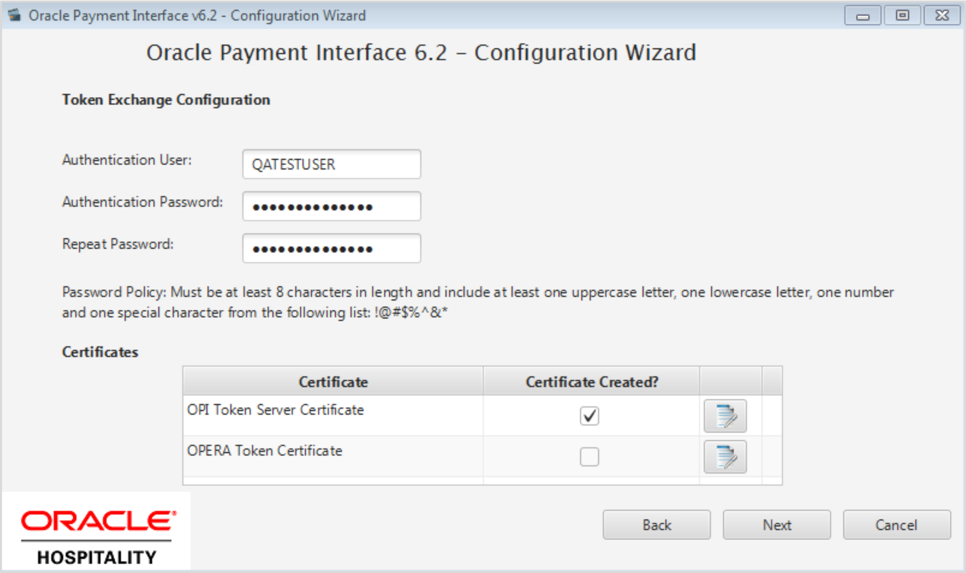
Tenders:

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

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

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

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



Oracle Payment Interface 6.2 – Configuration Wizard

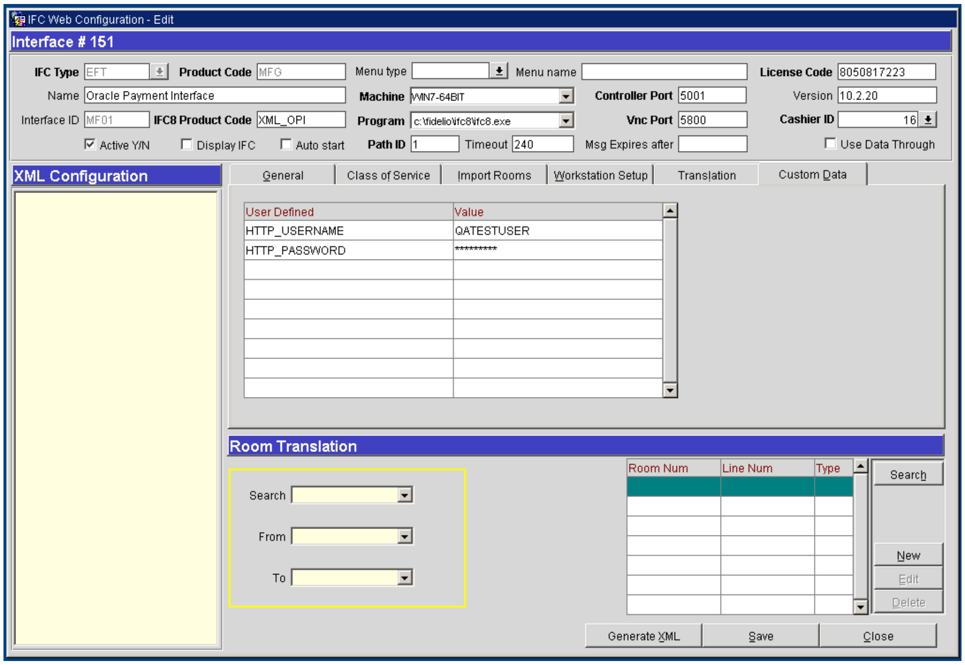
Token Exchange Configuration

Authentication User:	QATESTUSER
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	☐



Interface # 151

IFC Type	EFT	Product Code	MFG	Menu type		Menu name		License Code	8050817223
Name	Oracle Payment Interface			Machine	WIN7-64BIT	Controller Port	5001	Version	10.2.20
Interface ID	MF01	IFC8 Product Code	XML_OPI	Program	c:\fidelio\ifc8\ifc8.exe	Vnc Port	5800	Cashier ID	16
☑ Active Y/N		☐ Display IFC	☐ Auto start	Path ID	1	Timeout	240	Msg Expires after	☐ Use Data Through

User Defined	Value
HTTP_USERNAME	QATESTUSER
HTTP_PASSWORD	*********

Room Translation

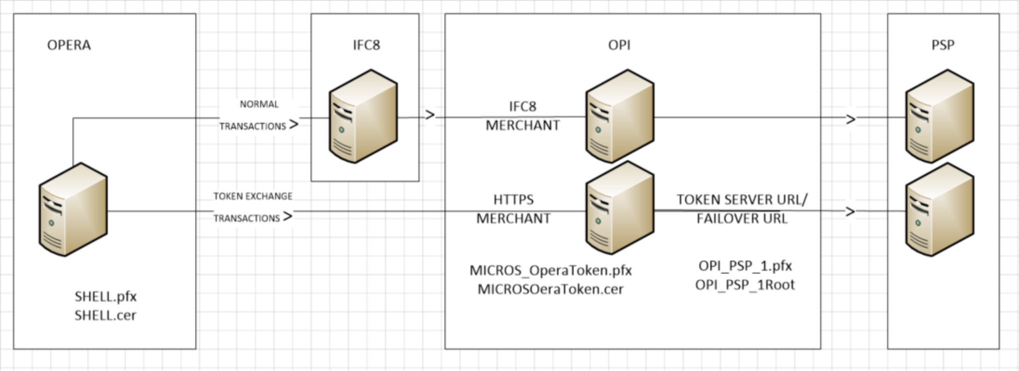
Search

From

To

Room Num	Line Num	Type

Certificates



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

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

Refer to the sections below for further details.

PSP - Client Side Certificates

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

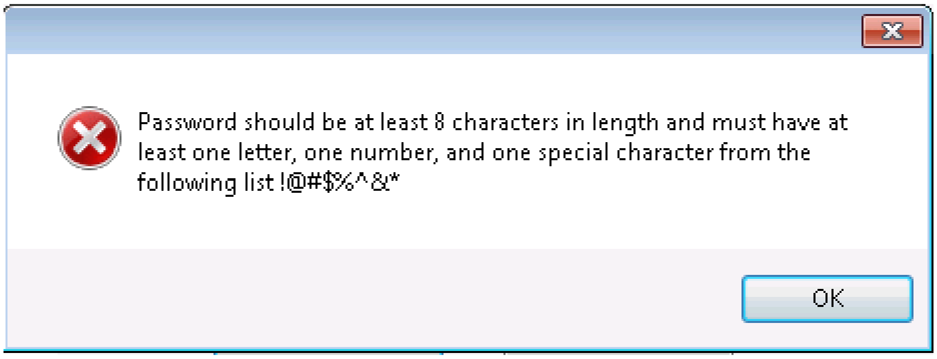
In order to achieve this, PSP is required to provide two files:

- 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.

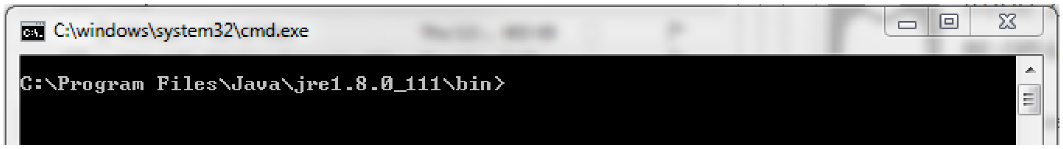

Password should be at least 8 characters in length and must have at least one letter, one number, and one special character from the following list !@#$%^&*

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;



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

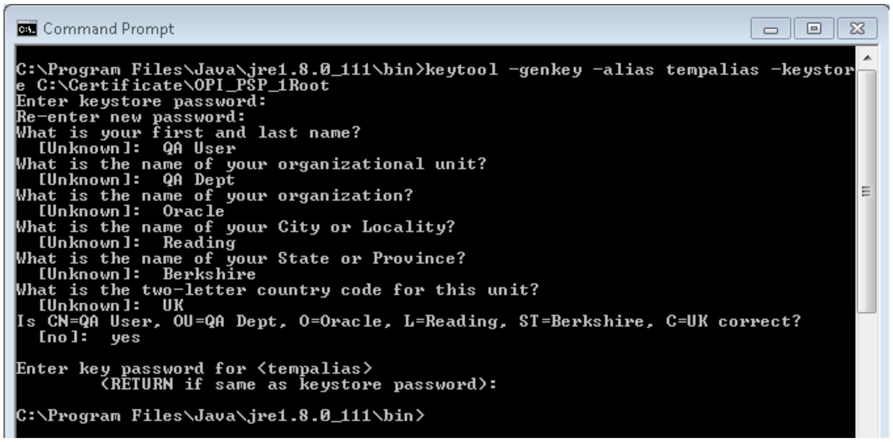
The three commands below, when run in sequence;

- 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
```

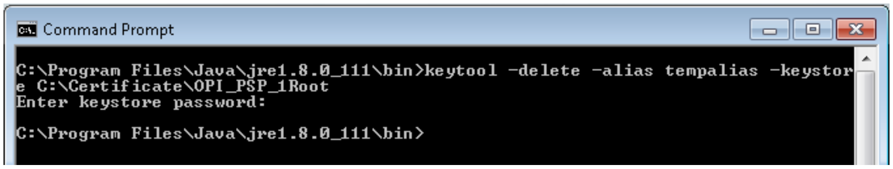
You must supply some basic information during the creation of the Java keystore, including a password.



```
C:\Program Files\Java\jre1.8.0_111\bin>keytool -genkey -alias tempalias -keystor
e C:\Certificate\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>
```

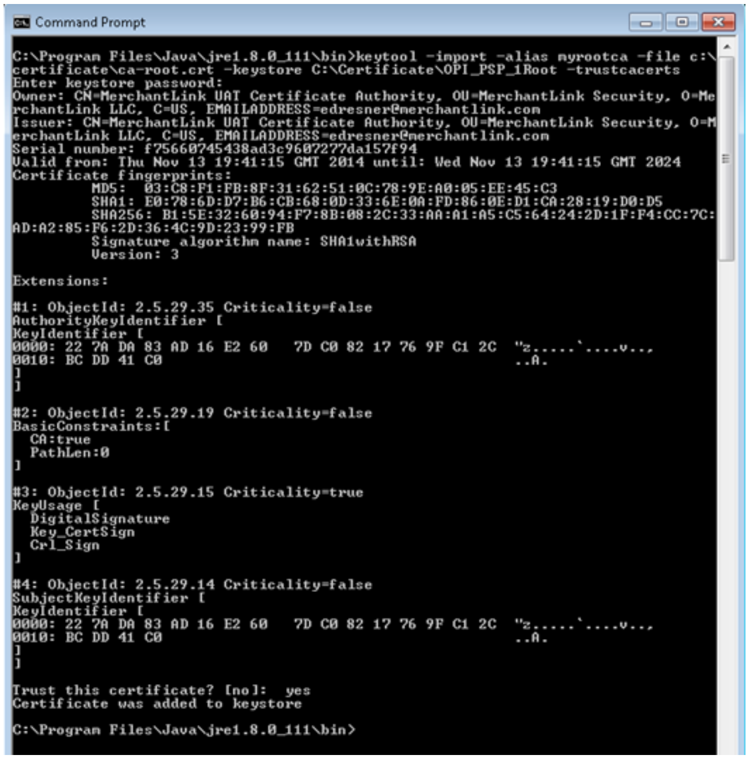
You should use the same key password as for the keystore password when prompted. (i.e. RETURN if same as keystore password – Press Enter)

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



```
C:\Program Files\Java\jre1.8.0_111\bin>keytool -delete -alias tempalias -keystor
e C:\Certificate\OPI_PSP_1Root
Enter keystore password:

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

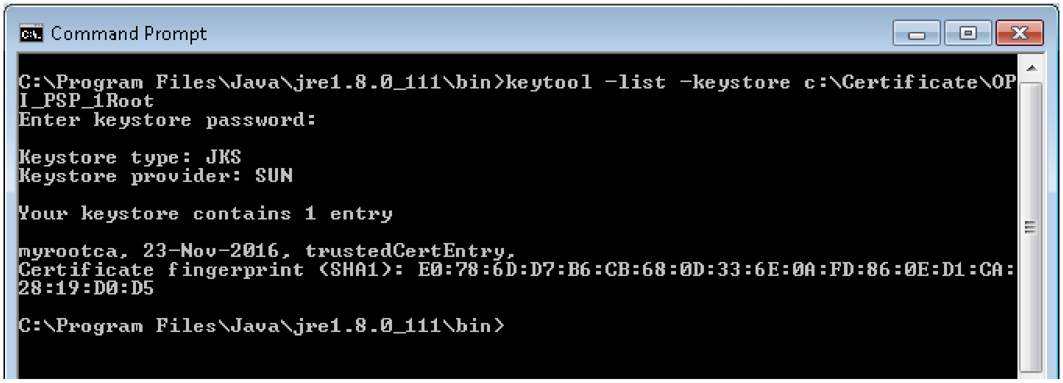
```
keytool -import -alias myrootca -file C:\Certificates\ca-cert.crt -keystore
C:\Certificates\OPI_PSP_1Root -trustcacerts
```



```
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=edresner@merchantlink.com
Issuer: CN=MerchantLink UAT Certificate Authority, OU=MerchantLink Security, O=M
erchantLink LLC, C=US, EMAILADDRESS=edresner@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>
```

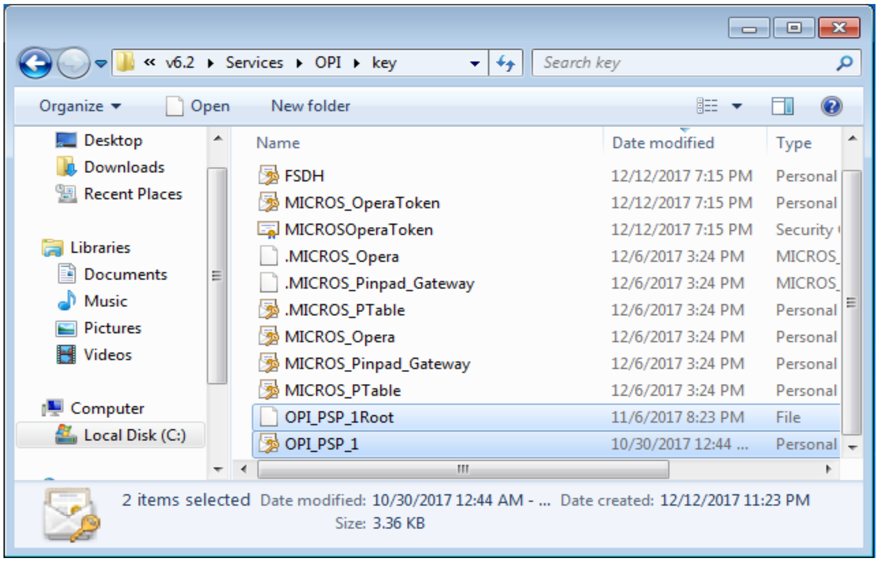
Verify the new Java keystore's details by running the following command if required;

```
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\`



Name	Date modified	Type
FSDH	12/12/2017 7:15 PM	Personal
MICROS_OperaToken	12/12/2017 7:15 PM	Personal
MICROSOperaToken	12/12/2017 7:15 PM	Security
.MICROS_Opera	12/6/2017 3:24 PM	MICROS_
.MICROS_Pinpad_Gateway	12/6/2017 3:24 PM	MICROS_
.MICROS_PTable	12/6/2017 3:24 PM	Personal
MICROS_Opera	12/6/2017 3:24 PM	Personal
MICROS_Pinpad_Gateway	12/6/2017 3:24 PM	Personal
MICROS_PTable	12/6/2017 3:24 PM	Personal
OPI_PSP_1Root	11/6/2017 8:23 PM	File
OPI_PSP_1	10/30/2017 12:44 ...	Personal

2 items selected Date modified: 10/30/2017 12:44 AM - ... Date created: 12/12/2017 11:23 PM
Size: 3.36 KB

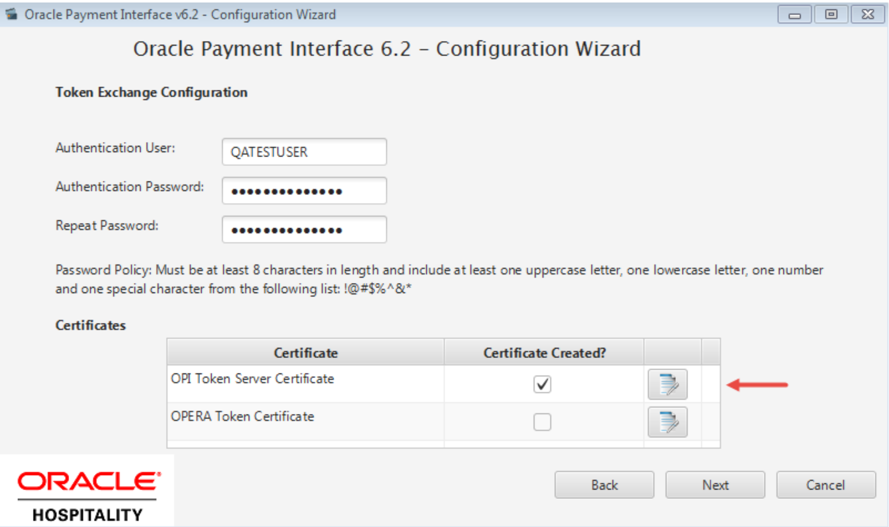
Updating a JKS with a new PSP certificate

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 certificate used in communication from Opera to OPI.

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



Oracle Payment Interface v6.2 - Configuration Wizard

Oracle Payment Interface 6.2 – Configuration Wizard

Token Exchange Configuration

Authentication User: QATESTUSER

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

Repeat Password: ••••••••••••••

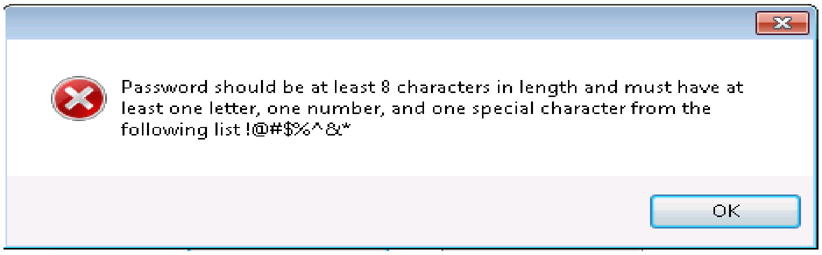
Password Policy: Must be at least 8 characters in length and include at least one uppercase letter, one lowercase letter, one number and one special character from the following list: !@#$%^&*

Certificates

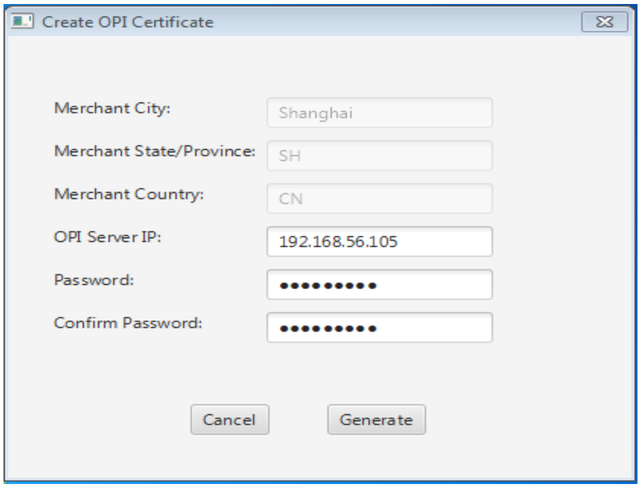
Certificate	Certificate Created?
OPI Token Server Certificate	☑
OPERA Token Certificate	□

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 !@#$%^&*



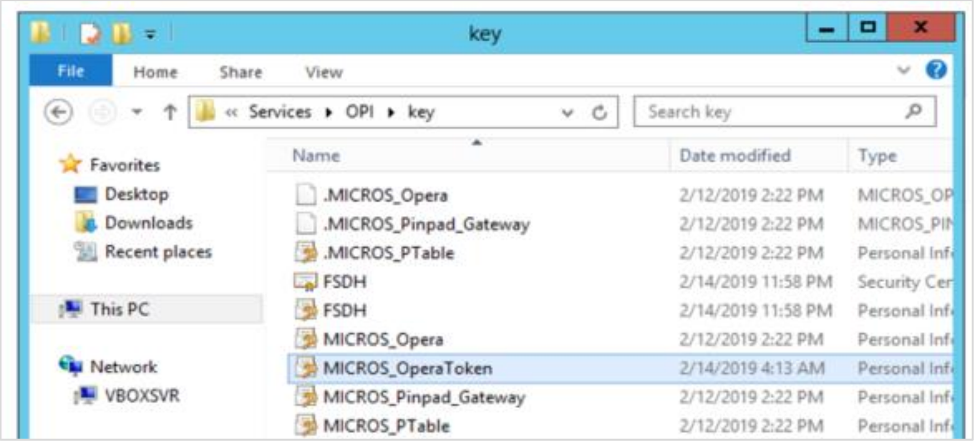
Password should be at least 8 characters in length and must have at least one letter, one number, and one special character from the following list !@#$%^&*



Merchant City: Shanghai
Merchant State/Province: SH
Merchant Country: CN
OPI Server IP: 192.168.56.105
Password: •••••••••
Confirm Password: •••••••••

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\`



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

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

Copy the ***MICROSOperaToken.cer*** 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* (Refer to section Certificate Import using Microsoft Management Console for more details)

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

OPI - Client Side Certificates

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

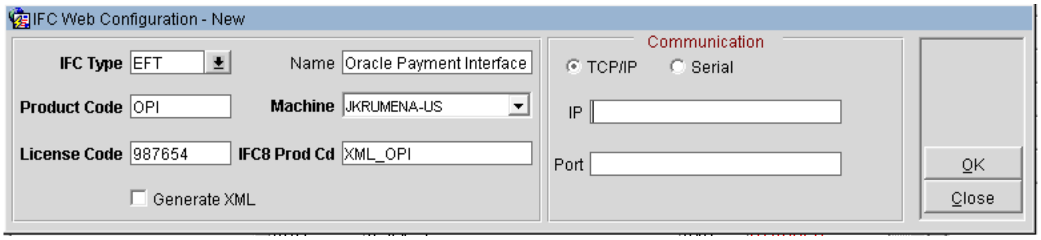
- OPERA V5.5.0.23 and V5.6.4.0.
- OPERA Cloud 19.2.0.0 and 1.20.16.0.

5 Opera Configuration

Creating an EFT Interface

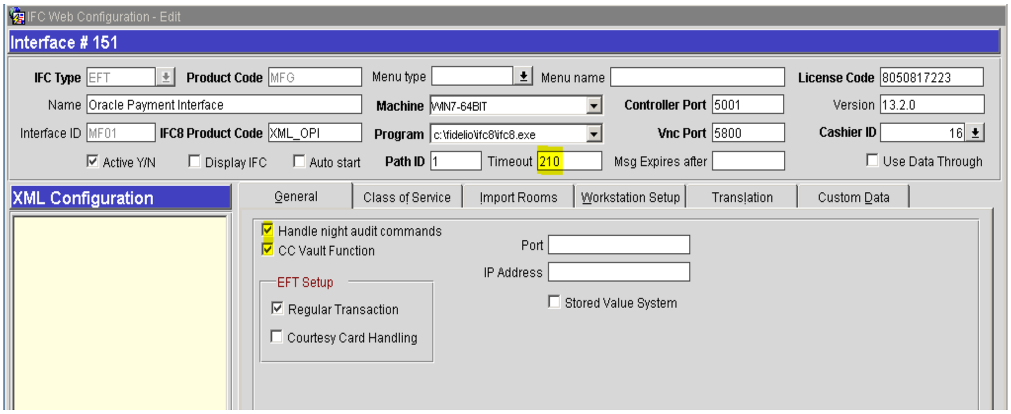
Log in to OPERA and go to Configuration. Select the menu option **Setup** | **Property Interfaces** | **Interface Configuration**. If there is no active EFT or CCW IFC Type, select **New** to add configuration for a new EFT interface.

1. Enter the following options, and then click **OK**:
    - **IFC Type:** EFT
    - **Name:** Oracle Payment Interface
    - **Product Code:** OPI
    - **Machine:** Select the machine
    - **License Code:** License code for interface
    - **IFC8 Prod Cd:** XML_OPI



IFC Type: EFT
Name: Oracle Payment Interface
Product Code: OPI
Machine: JKRUMENA-US
License Code: 987654
IFC8 Prod Cd: XML_OPI
□ Generate XML
● TCP/IP ○ Serial
IP:
Port:

2. Select the check box to enable the **CC Vault Function**.
3. Define the **Timeout** value as 210.



IFC Web Configuration - Edit

Interface # 151

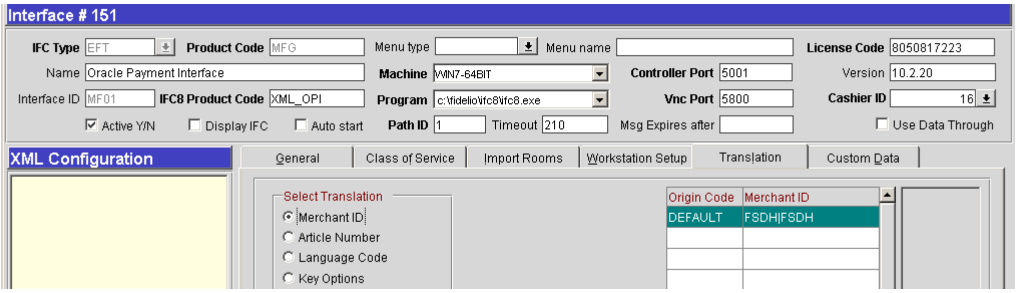
IFC Type EFT | Product Code MFG | Menu type | Menu name | License Code 8050817223
Name Oracle Payment Interface | Machine WIN7-64BIT | Controller Port 5001 | Version 13.2.0
Interface ID MF01 | IFC8 Product Code XML_OPI | Program c:\fidelio\ifc8\ifc8.exe | Vnc Port 5800 | Cashier ID 16
☑ Active Y/N ☐ Display IFC ☐ Auto start | Path ID 1 | Timeout 210 | Msg Expires after | ☐ Use Data Through

XML Configuration

☑ Handle night audit commands
☑ CC Vault Function
Port
IP Address
☐ Stored Value System

EFT Setup
☑ Regular Transaction
☐ Courtesy Card Handling

4. Select the **Translation** tab and then click **Merchant ID**.
5. Select **New** to add the Merchant ID. This must be the same as previously configured in OPI (MPG) Configuration.



Interface # 151

IFC Type EFT | Product Code MFG | Menu type | Menu name | License Code 8050817223
Name Oracle Payment Interface | Machine WIN7-64BIT | Controller Port 5001 | Version 10.2.20
Interface ID MF01 | IFC8 Product Code XML_OPI | Program c:\fidelio\ifc8\ifc8.exe | Vnc Port 5800 | Cashier ID 16
☑ Active Y/N ☐ Display IFC ☐ Auto start | Path ID 1 | Timeout 210 | Msg Expires after | ☐ Use Data Through

XML Configuration

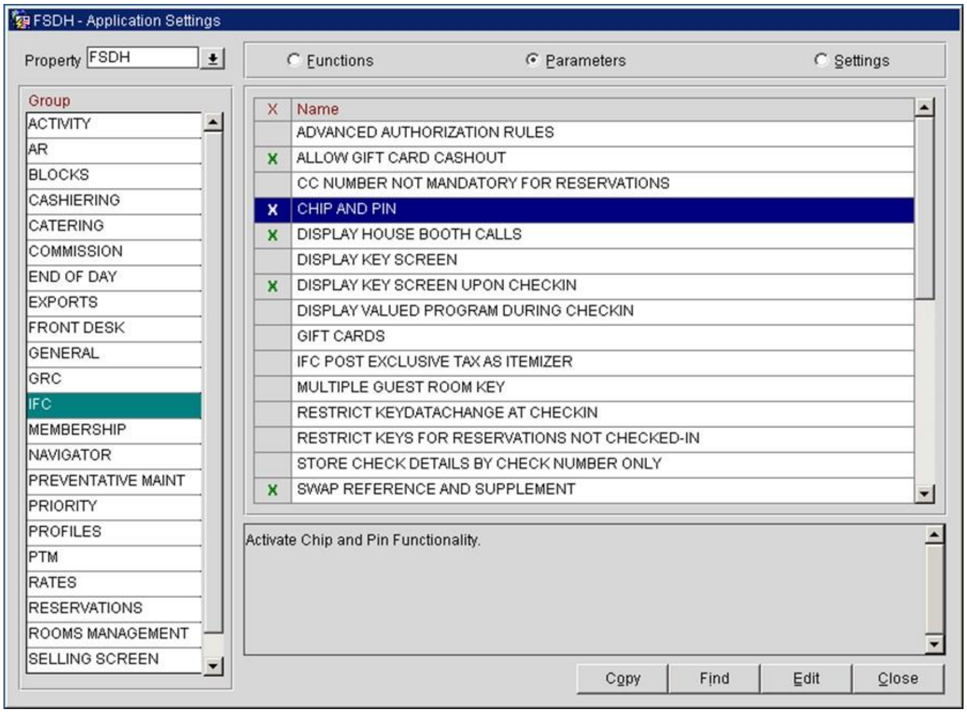
Select Translation
● Merchant ID
○ Article Number
○ Language Code
○ Key Options

Origin Code	Merchant ID
DEFAULT	FSDH|FSDH

Configuring CHIP AND PIN (EMV)

To configure the Functionality Setup:

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



FSDH - Application Settings

Property FSDH

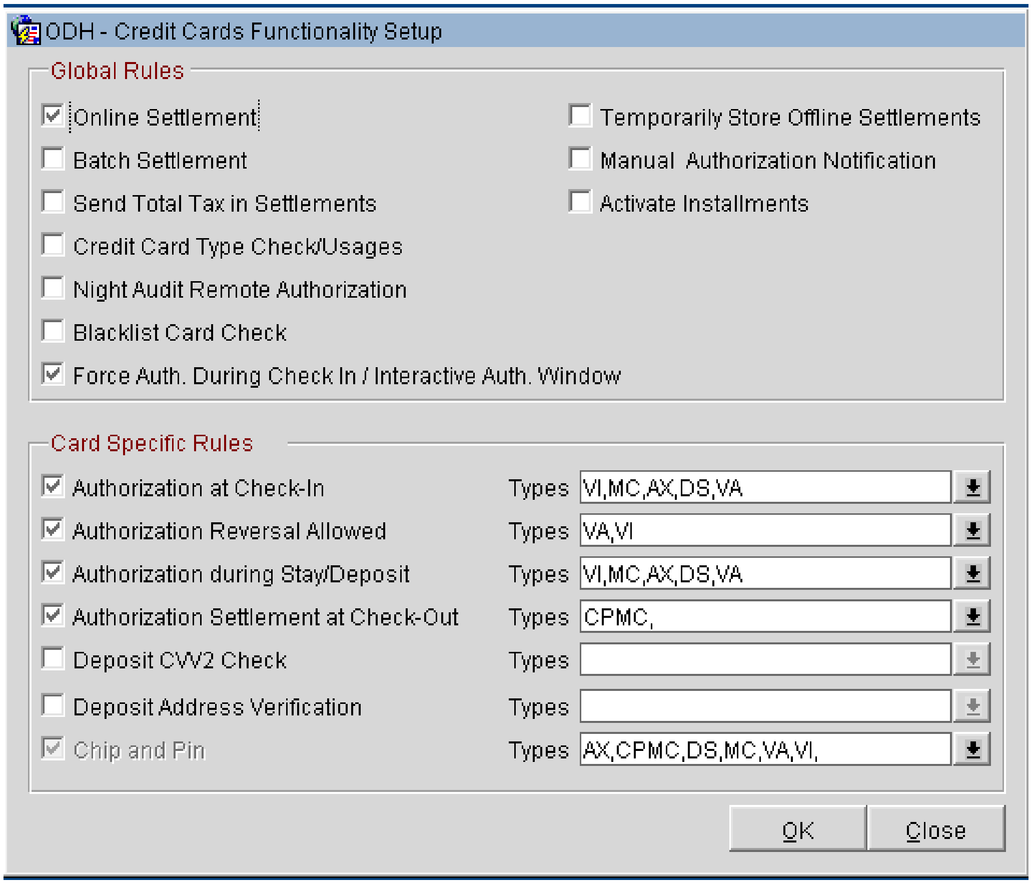
○ Functions ● Parameters ○ Settings

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

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

Activate Chip and Pin Functionality.

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



ODH - Credit Cards Functionality Setup

Global Rules

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

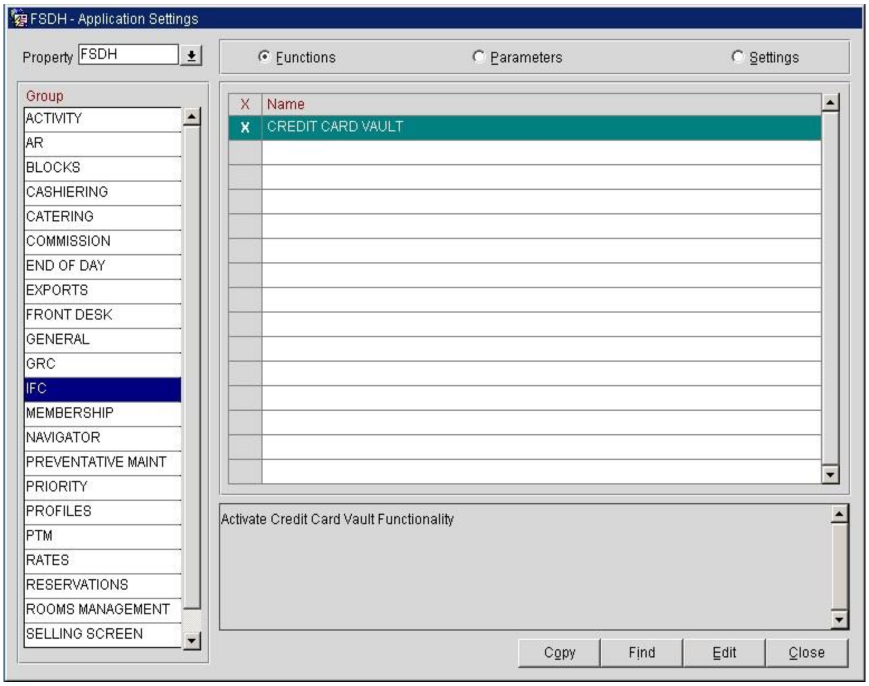
Card Specific Rules

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

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

Configuring the CC Vault

Go to **Setup | Application Settings | IFC Group | Functions**, and enable **CREDIT CARD VAULT.**



FSDH - Application Settings

Property FSDH

● Functions ○ Parameters ○ Settings

Group

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

X	Name
X	CREDIT CARD VAULT

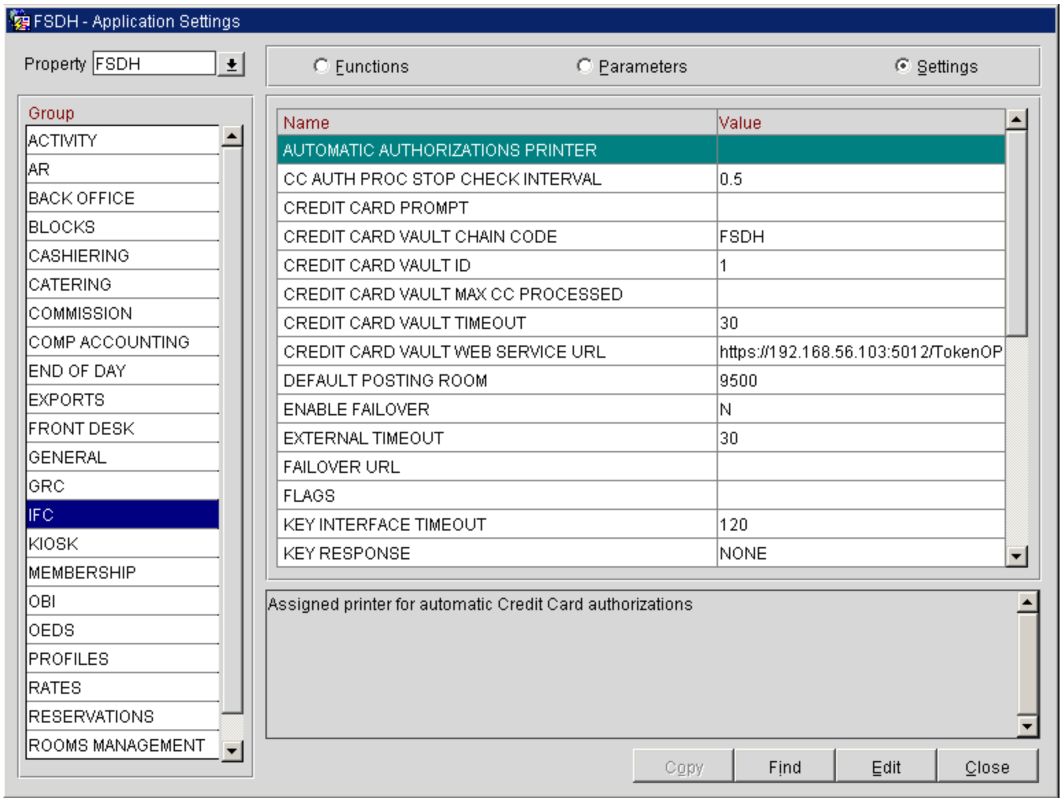
Activate Credit Card Vault Functionality

Configuration -> Setup -> Application Settings -> IFC -> Settings

OPERA uses the CREDIT CARD VAULT CHAIN CODE for the certificate lookup and should be populated with what was entered during the OPI configuration for PMS.
The CREDIT CARD VAULT WEB SERVICE URL should be in the format:
https://OPIHostIP:OPITokenPortNumber/TokenOPERA
The CREDIT CARD VAULT ID is currently not used.

The CREDIT CARD MAX CC PROCESSED is set to what the Payment Partner can support for the number of rows sent in one Token (GetID/GetCC) request. This is used during the bulk tokenization process and when multiple folio windows exist on OPERA Reservations. 50 is the default used when nothing is set here.

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



Property FSDH

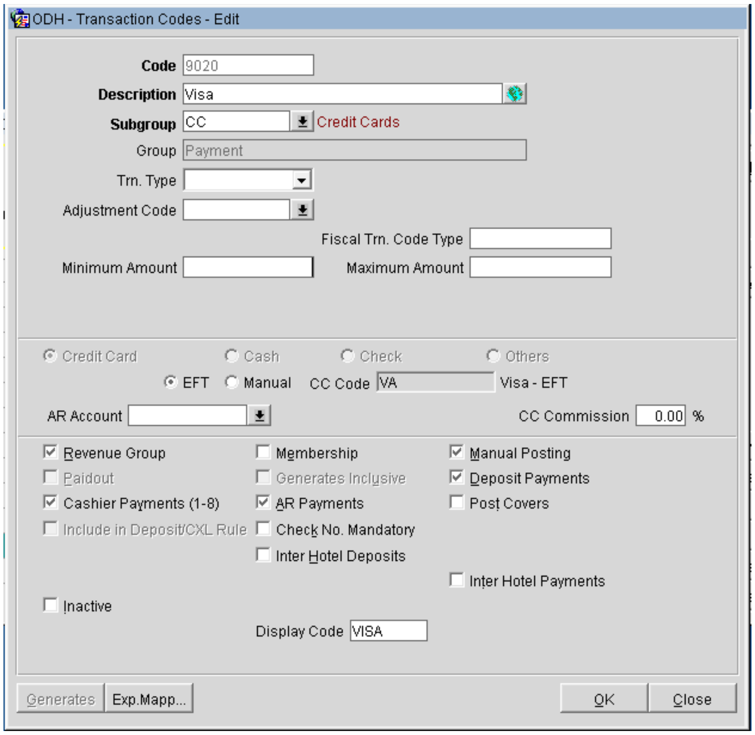
Name	Value
AUTOMATIC AUTHORIZATIONS PRINTER	
CC AUTH PROC STOP CHECK INTERVAL	0.5
CREDIT CARD PROMPT	
CREDIT CARD VAULT CHAIN CODE	FSDH
CREDIT CARD VAULT ID	1
CREDIT CARD VAULT MAX CC PROCESSED	
CREDIT CARD VAULT TIMEOUT	30
CREDIT CARD VAULT WEB SERVICE URL	https://192.168.56.103:5012/TokenOP
DEFAULT POSTING ROOM	9500
ENABLE FAILOVER	N
EXTERNAL TIMEOUT	30
FAILOVER URL	
FLAGS	
KEY INTERFACE TIMEOUT	120
KEY RESPONSE	NONE

Assigned printer for automatic Credit Card authorizations

Cashiering Overview

Credit Card Payment Transaction Codes

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



ODH - Transaction Codes - Edit

Code 9020

Description Visa

Subgroup CC Credit Cards

Group Payment

Trn. Type

Adjustment Code

Fiscal Trn. Code Type

Minimum Amount

Maximum Amount

● Credit Card ○ Cash ○ Check ○ Others

● EFT ○ Manual CC Code VA Visa - EFT

AR Account

CC Commission 0.00 %

☑ Revenue Group ☐ Membership ☑ Manual Posting

☐ Paidout ☐ Generates Inclusive ☑ Deposit Payments

☑ Cashier Payments (1-8) ☑ AR Payments ☐ Post Covers

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

☐ Inter Hotel Deposits

☐ Inter Hotel Payments

☐ Inactive

Display Code VISA

2. Information for credit card payment transaction codes:

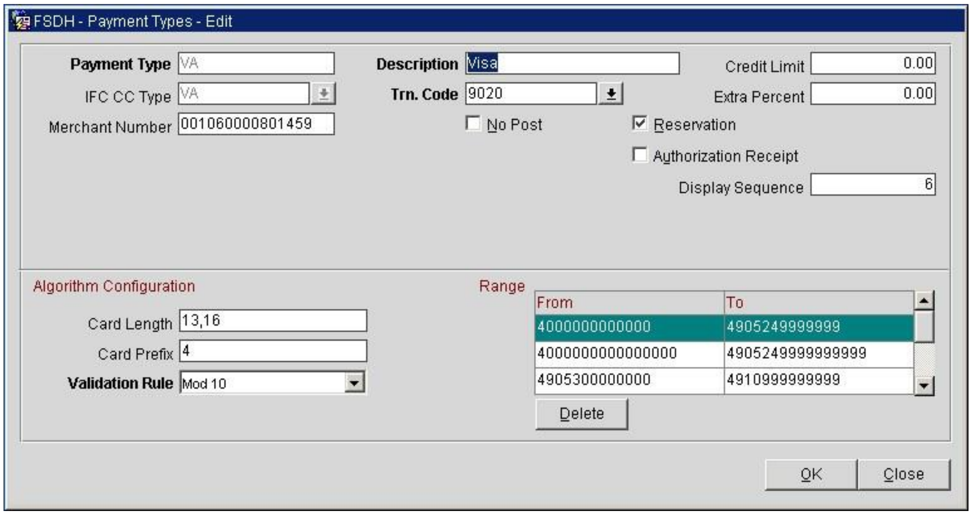
   - **EFT** selection is necessary to send credit card transactions out to the integrated payment partner for the specific Payment type.
   - **Manual** selection will not send out any transactions to the integrated payment partner.
   - **CC Code** will auto-populate once the transaction code is associated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

Overview of Credit Card Payment Types

The credit card payment types link with the transaction code:

1. In OPERA, go to **Configuration | Cashiering | Payment Types**.

- The **IFC CC Type** field has the credit card code used such as MC, VA, AX.
- The **Trn Code** field has the credit card transaction code.



FSDH - Payment Types - Edit

Payment Type: VA

Description: Visa

Credit Limit: 0.00

IFC CC Type: VA

Trn. Code: 9020

Extra Percent: 0.00

Merchant Number: 001060000801459

□ No Post

☑ Reservation

□ Authorization Receipt

Display Sequence: 6

Algorithm Configuration

Card Length: 13,16

Card Prefix: 4

Validation Rule: Mod 10

Range

From	To
4000000000000	4905249999999
4000000000000000	4905249999999999
4905300000000	4910999999999

Credit Card Type Payment Setup Information

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

Sample List of Card Types

Payment Types - Customer Present (Chip & PIN)	**Description**	**Capture Method**
VA	Visa	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
MC	Mastercard	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
AX	American Express	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
DC	Diners Club	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
JC	JCB	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
CU	China Union Pay	CP can be used. Transaction will go to the EMV (Chip & PIN) device.
VD	Visa Debit	CP cannot be used, manual card type selection is required. If CP is used, OPERA will default to Visa. Transaction will go to the EMV (Chip & PIN) device.
MD	Mastercard Debit	CP cannot be used, manual card type selection is required. If CP is used, OPERA will default to Mastercard. Transaction will go to the EMV (Chip & PIN) device.

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

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

Payment Types - Customer NOT Present (Keyed)	Description	Capture Method
KCD	China Union Pay Debit	Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)

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

Individual Card Functions

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

Payment Types - Customer Present (Chip & PIN)	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
AB	N	Y	N	Y	N

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

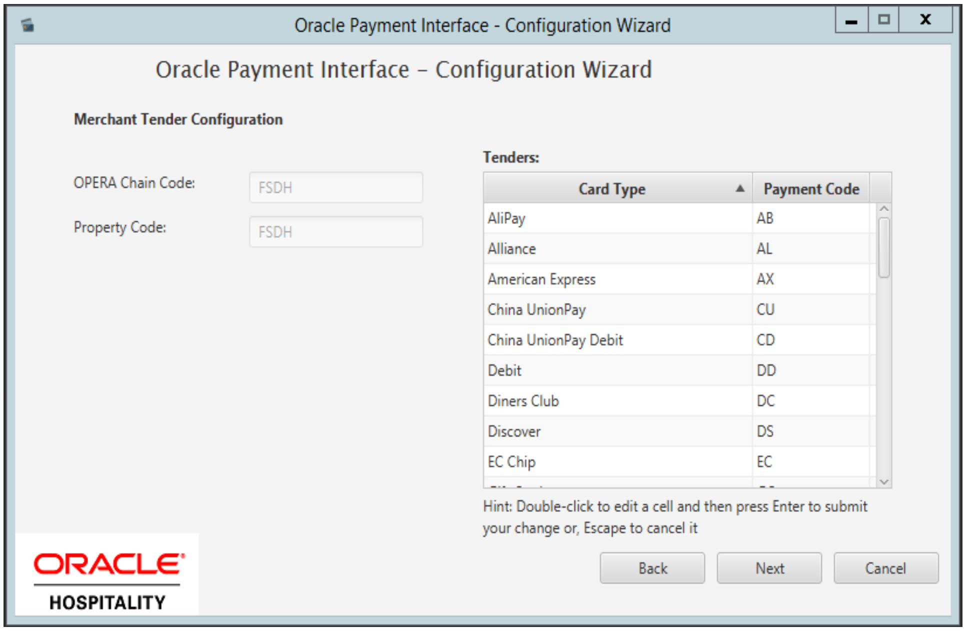
Payment Types – One Shot Cards (Keyed) OPTIONAL!!!	Authorization at Check-in	Pay Only (no Authorization)	Deposit Y/N	Cashier Payment Y/N	A/R Payment Y/N
VVA	N	Y	N	Y	N
VMC	N	Y	N	Y	N
VAX	N	Y	N	Y	N

Important Considerations

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

Update OPI Configuration Merchant Tenders

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



Oracle Payment Interface - Configuration Wizard

Oracle Payment Interface – Configuration Wizard

Merchant Tender Configuration

OPERA Chain Code: FSDH

Property Code: FSDH

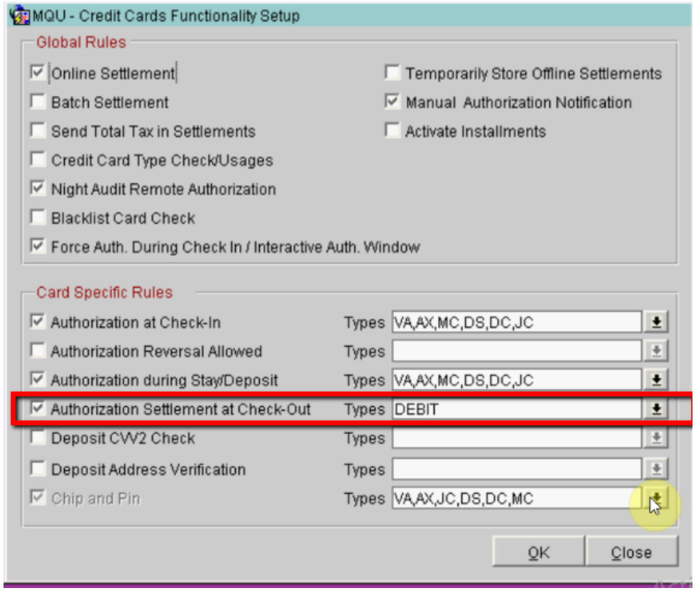
Tenders:

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

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

Update Functionality settings for Chip & Pin and PayOnly

- Selection for Chip & Pin and PayOnly cards



MQU - Credit Cards Functionality Setup

Global Rules

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

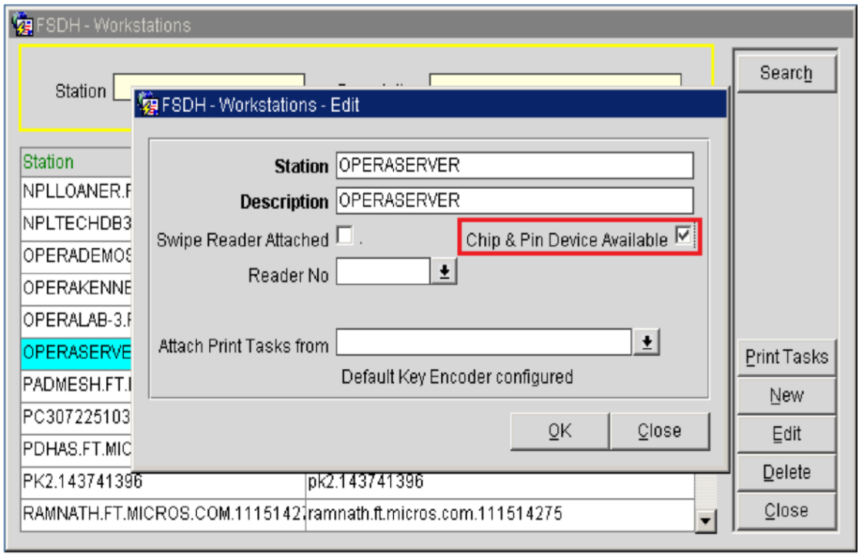
Card Specific Rules

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

Configuring the Workstation

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

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



FSDH - Workstations

Station

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

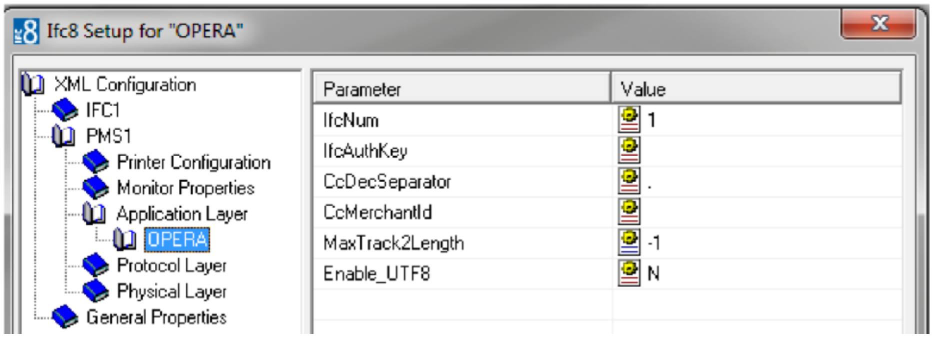
FSDH - Workstations - Edit

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

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

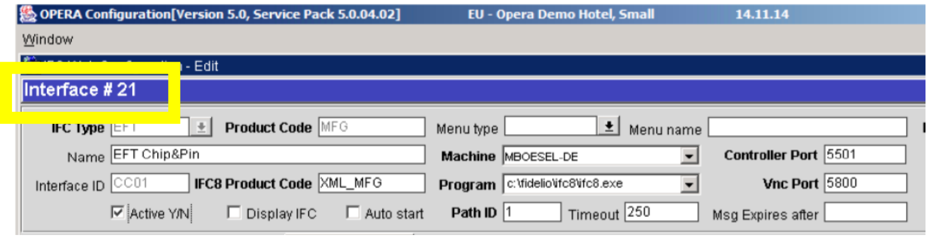
To configure the link between the interfaces:

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

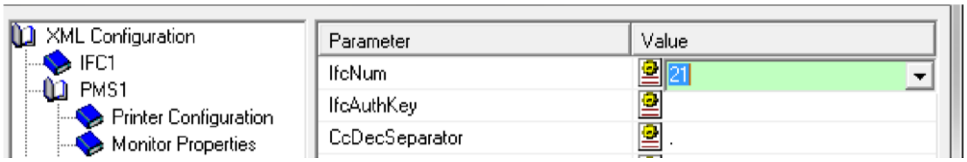


Parameter	Value
IfcNum	1
IfcAuthKey	
CcDecSeparator	.
CcMerchantId	
MaxTrack2Length	-1
Enable_UTF8	N

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

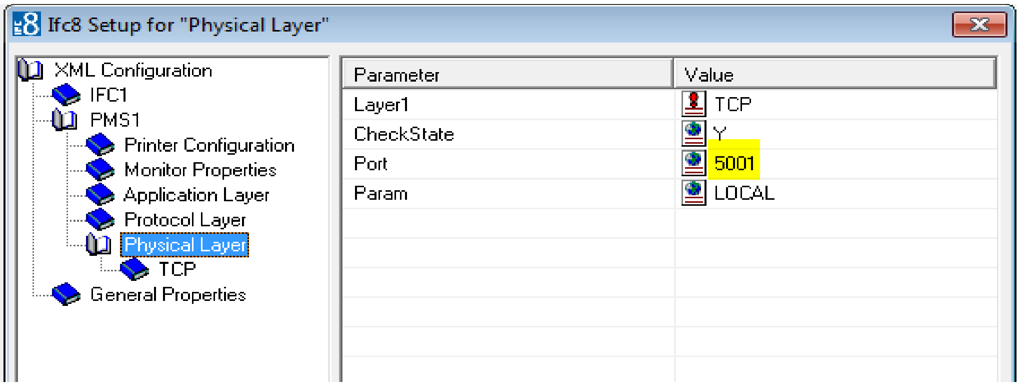

OPERA Configuration[Version 5.0, Service Pack 5.0.04.02]
EU - Opera Demo Hotel, Small
14.11.14
Window
- Edit
Interface # 21

IFC Type EFT
Product Code MFG
Menu type
Menu name
Name EFT Chip&Pin
Machine MBOESEL-DE
Controller Port 5501
Interface ID CC01
IFC8 Product Code XML_MFG
Program c:\fidelio\ifc8\ifc8.exe
Vnc Port 5800
☑ Active Y/N ☐ Display IFC ☐ Auto start
Path ID 1
Timeout 250
Msg Expires after



Parameter	Value
IfcNum	21
IfcAuthKey	
CcDecSeparator	.

3. Go to the **PMS1** tree in the **Physical Layer**.
4. Enter the port number into Parameter value **Port**. This is the port IFC8 uses to communicate with the opera IFC controller.
5. Select **Enter** and **Apply** to re-initiate IFC8, and then click **Save**.

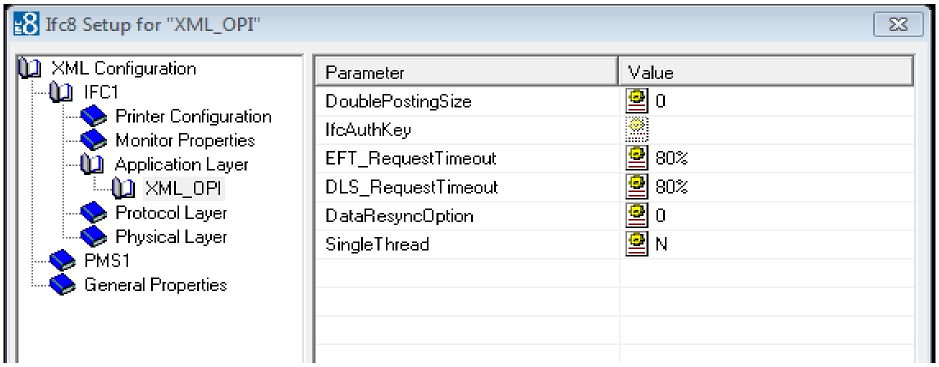


Parameter	Value
Layer1	TCP
CheckState	Y
Port	5001
Param	LOCAL

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

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

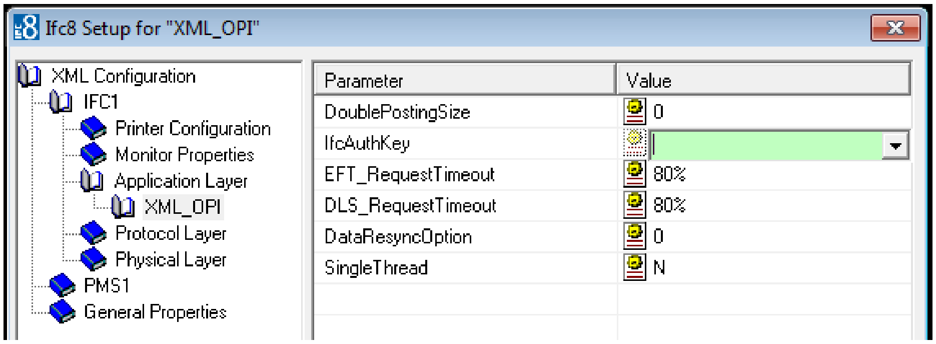
1. In the Hotel Property Interface (IFC8) configuration, go to the **IFC1** tree, and then in the **Application Layer,** select the **XML_OPI** option.



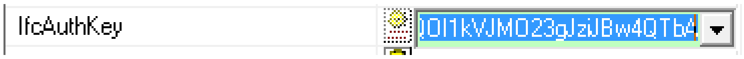
Parameter	Value
DoublePostingSize	0
IfcAuthKey	
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0
SingleThread	N

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

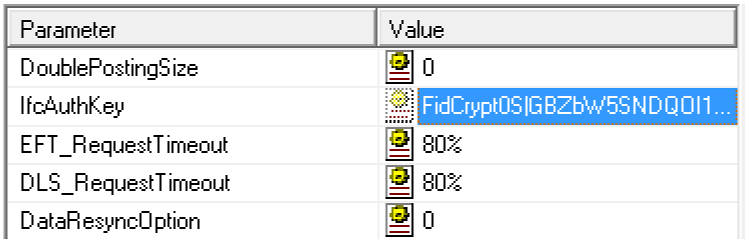
3. Copy this string into IFC8 Parameter **IfcAuthKey** value field.



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

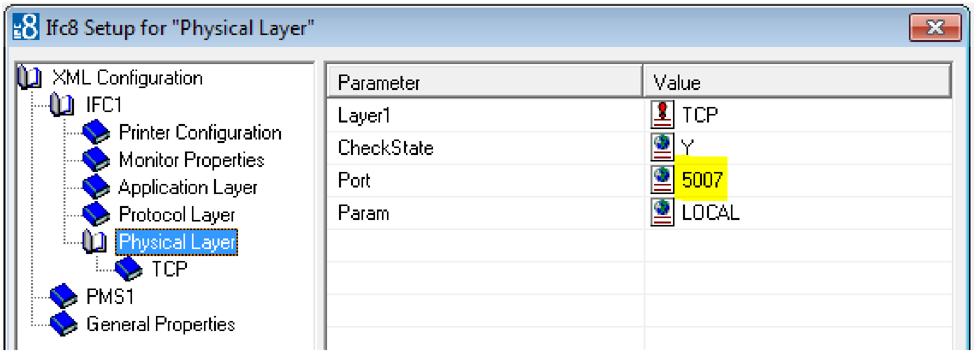


IfcAuthKey	QOI1kVJMO23gJziJBw4QTb4



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

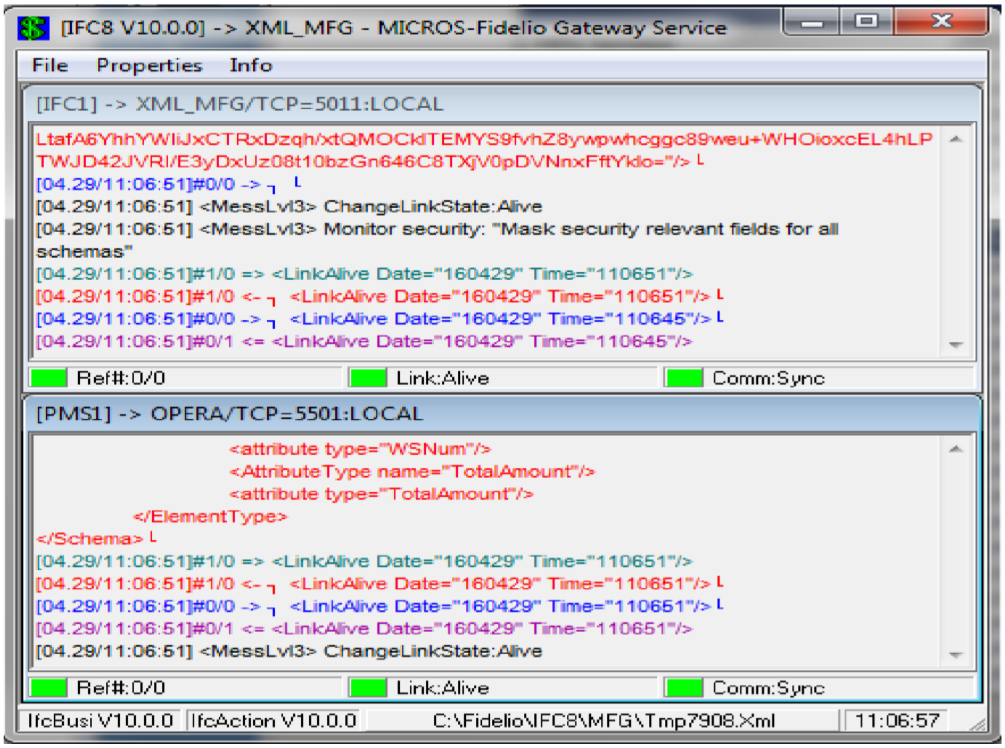
4. Go to **IFC1** tree and select the **Physical Layer**.
5. Enter the port number in port value. This is the same port that was configured in OPI.



Parameter	Value
Layer1	TCP
CheckState	Y
Port	5007
Param	LOCAL

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

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



[IFC8 V10.0.0] -> XML_MFG - MICROS-Fidelio Gateway Service
File
Properties
Info
[IFC1] -> XML_MFG/TCP=5011:LOCAL

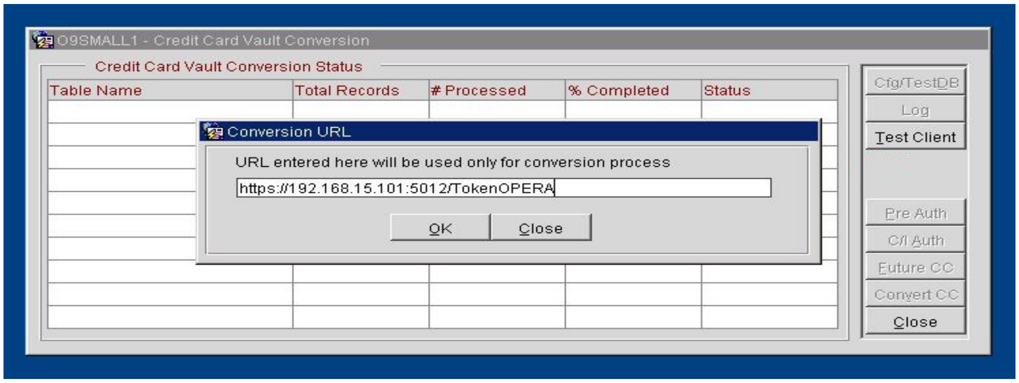
```
LtafA6YhhYWIiJxCTRxDzqh/xtQMOCklTEMYS9fvhZ8ywpwhcggc89weu+WHOioxcEL4hLP
TWJD42JVRI/E3yDxUz08t10bzGn646C8TXjV0pDVNnxFftYklo="/> └
[04.29/11:06:51]#0/0 -> ┐  └
[04.29/11:06:51] <MessLvl3> ChangeLinkState:Alive
[04.29/11:06:51] <MessLvl3> Monitor security: "Mask security relevant fields for all
schemas"
[04.29/11:06:51]#1/0 => <LinkAlive Date="160429" Time="110651"/>
[04.29/11:06:51]#1/0 <- ┐  <LinkAlive Date="160429" Time="110651"/> └
[04.29/11:06:51]#0/0 -> ┐  <LinkAlive Date="160429" Time="110645"/> └
[04.29/11:06:51]#0/1 <= <LinkAlive Date="160429" Time="110645"/>
```

🟩 Ref#:0/0
🟩 Link:Alive
🟩 Comm:Sync
[PMS1] -> OPERA/TCP=5501:LOCAL

```
                    <attribute type="WSNum"/>
                    <AttributeType name="TotalAmount"/>
                    <attribute type="TotalAmount"/>
          </ElementType>
</Schema> └
[04.29/11:06:51]#1/0 => <LinkAlive Date="160429" Time="110651"/>
[04.29/11:06:51]#1/0 <- ┐  <LinkAlive Date="160429" Time="110651"/> └
[04.29/11:06:51]#0/0 -> ┐  <LinkAlive Date="160429" Time="110651"/> └
[04.29/11:06:51]#0/1 <= <LinkAlive Date="160429" Time="110651"/>
[04.29/11:06:51] <MessLvl3> ChangeLinkState:Alive
```

Perform a Tokenization

Utilities -> Convert CC -> Convert Vault CC Information -> Test Client



O9SMALL1 - Credit Card Vault Conversion
Credit Card Vault Conversion Status
Cfg/TestDB
Log
Test Client
Pre Auth
C/I Auth
Future CC
Convert CC
Close

Table Name	Total Records	# Processed	% Completed	Status

URL entered here will be used only for conversion process

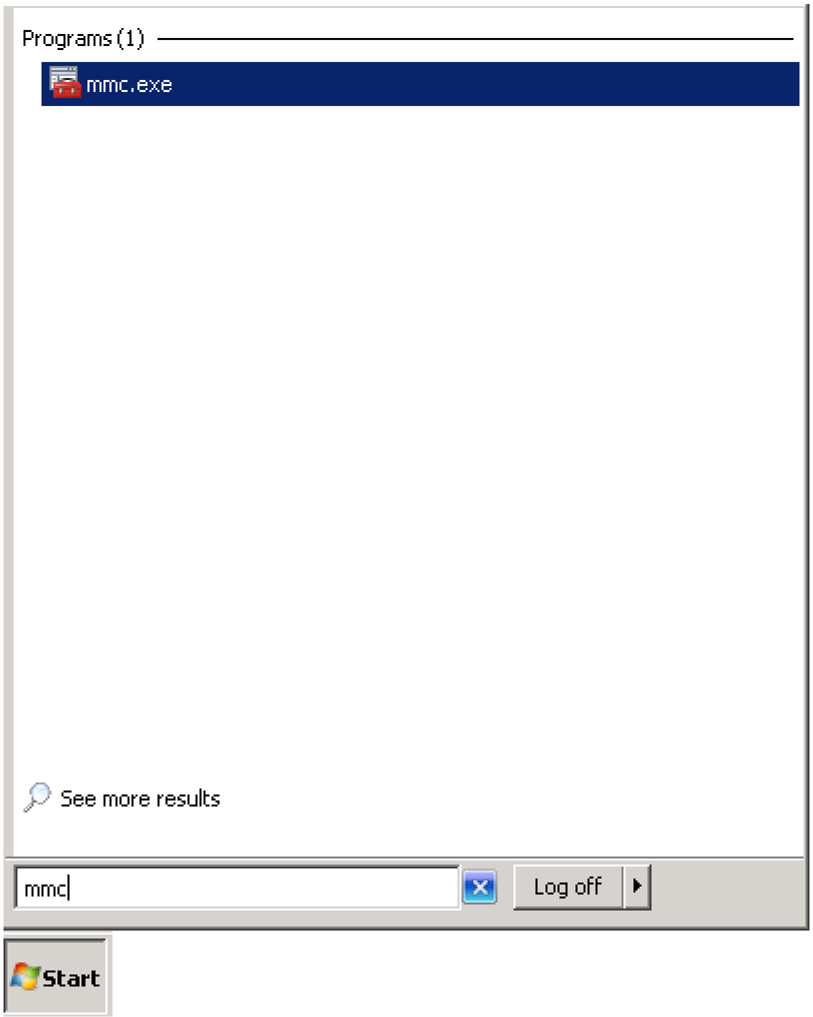
https://192.168.15.101:5012/TokenOPERA

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

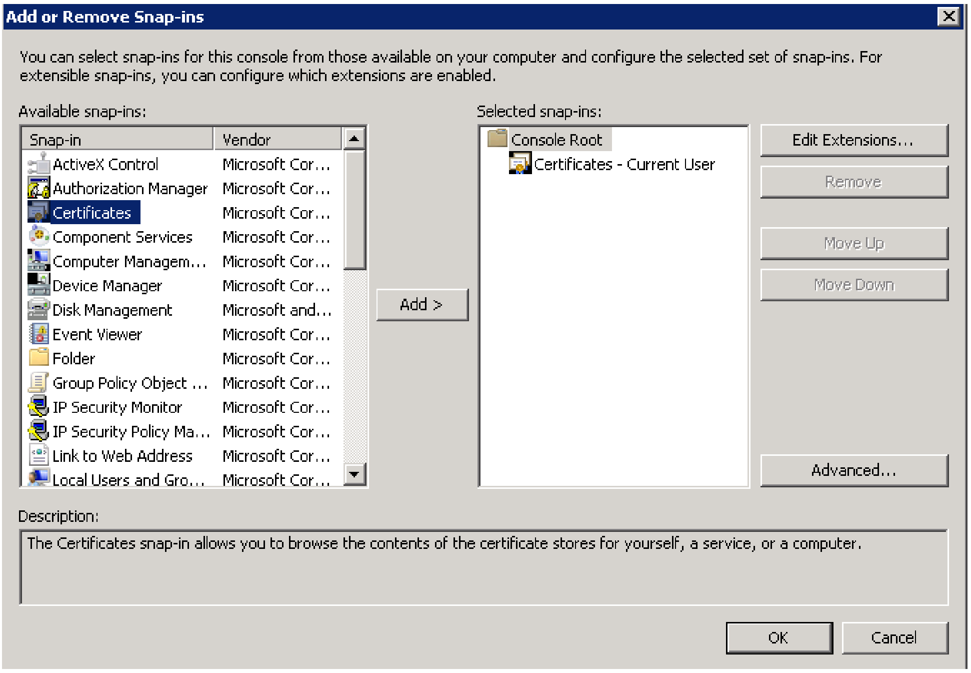
OPI only supports the **Convert CC** function; the other conversion options are not currently supported.

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**.



Add or Remove Snap-ins

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

Available snap-ins:

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

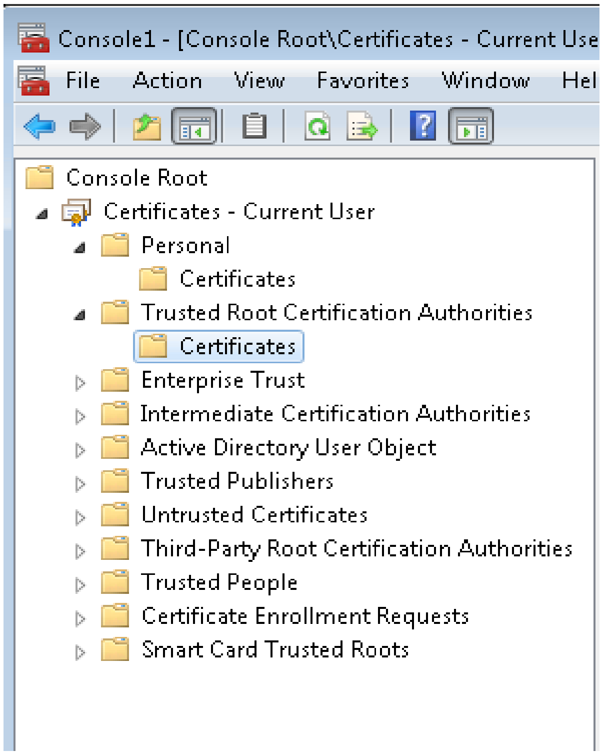
Selected snap-ins:

Console Root
 Certificates - Current User

Description:

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

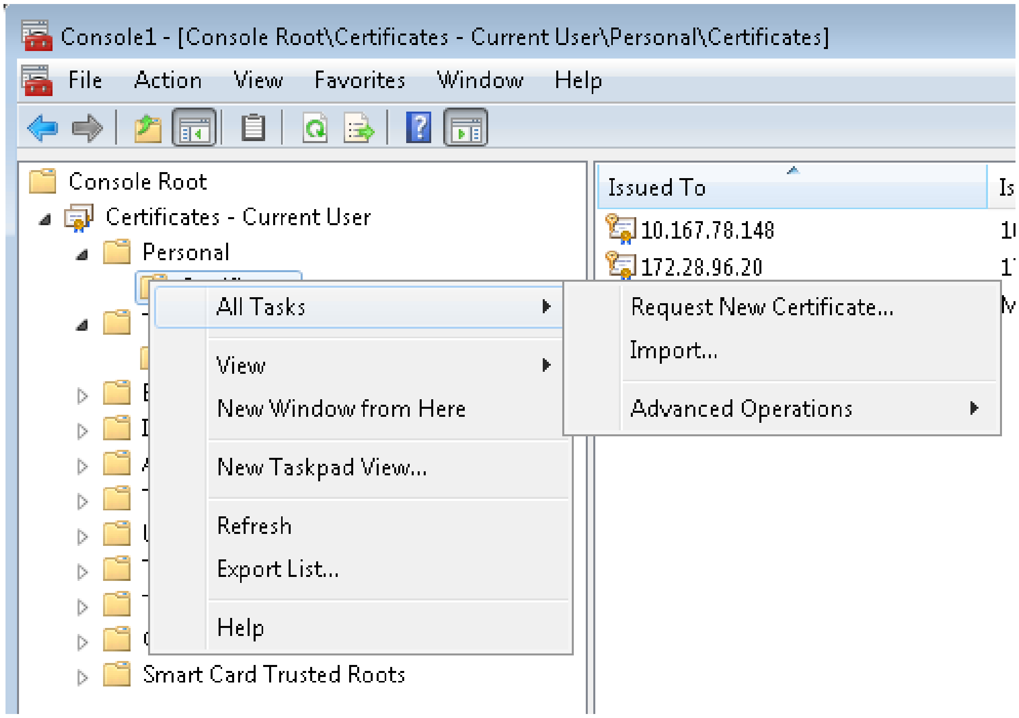
3. Expand Certificates, expand Personal or Trusted Root as required, and then select **Certificates**.



Console1 - [Console Root\Certificates - Current Use

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