Oracle® Payment Interface

Oracle Hospitality OPERA Property Management System Installation Guide

Release 6.1.1

E85868-01

April 2017

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
- Screen shots of each step you take

Documentation

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

Revision History

Date	Description of Change
April 2017	• Initial publication

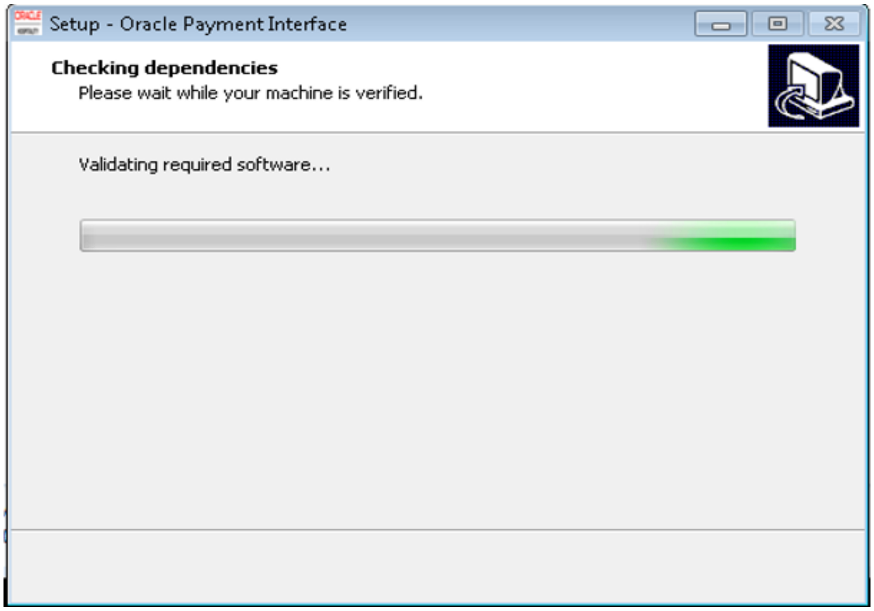
1 Pre-Installation

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

- OPERA Property Management System release 5.0.05.11 is the minimum release you can use to integrate with OPI.
- Upgrading to OPI 6.1.1.9 from any previous OPI is supported but MPG versions are not supported.
- Any previous version of MPG should be uninstalled prior to installing OPI 6.1.1.9.
- 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

2 Install OPI 6.1.1.9

- Download 6.1.1.9 OPI installer from My Oracle Support (MOS) website and then complete the following steps to install OPI.
- Double-click the OPI installer.
- The installer validates the required software.



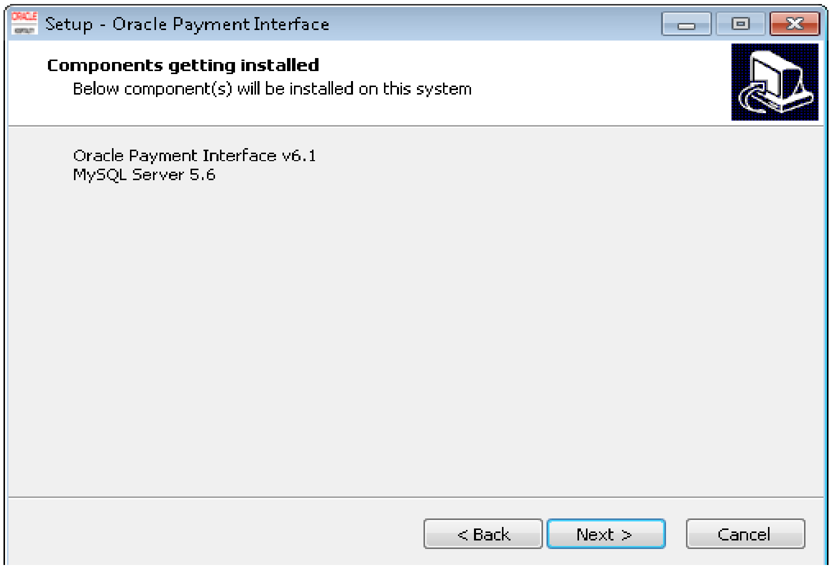
Setup - Oracle Payment Interface

Checking dependencies

Please wait while your machine is verified.

Validating required software...

1 Next, the Oracle Payment Interface release 6.1 and the MySQL release 5.6 applications install.



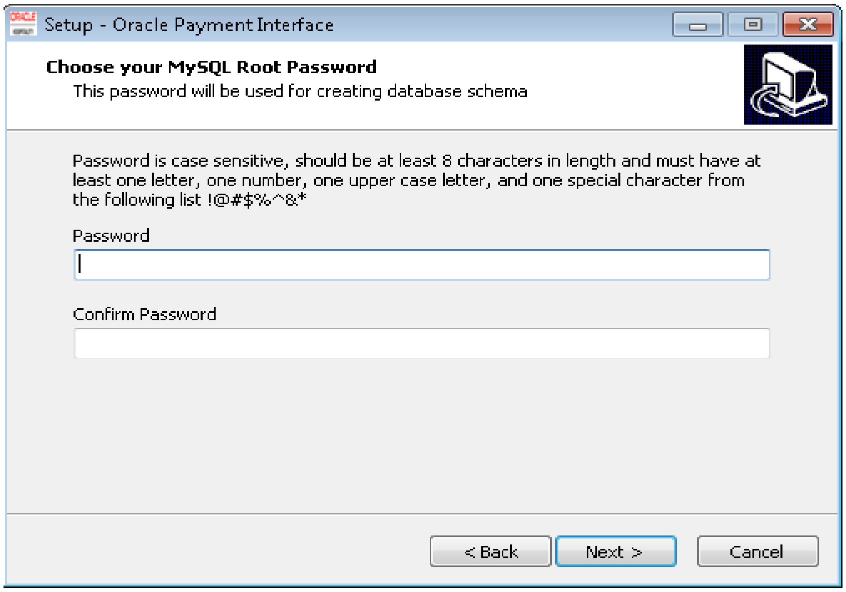
Setup - Oracle Payment Interface

Components getting installed

Below component(s) will be installed on this system

Oracle Payment Interface v6.1
MySQL Server 5.6

2 Create a MySQL root password.



Choose your MySQL Root Password

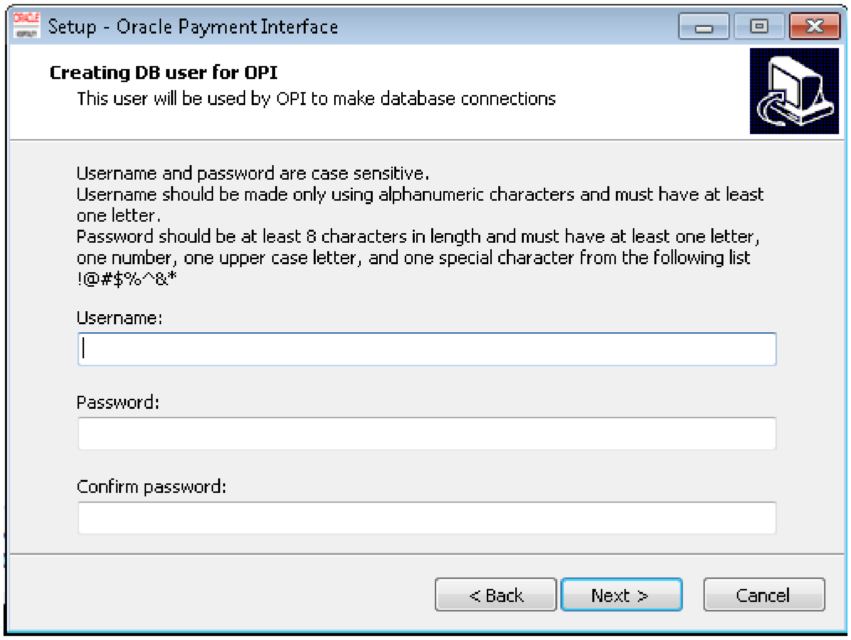
This password will be used for creating database schema

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

Password

Confirm Password

3 Create the MySQL database user and password for OPI. OPI uses this account to connect to MySQL.



Creating DB user for OPI

This user will be used by OPI to make database connections

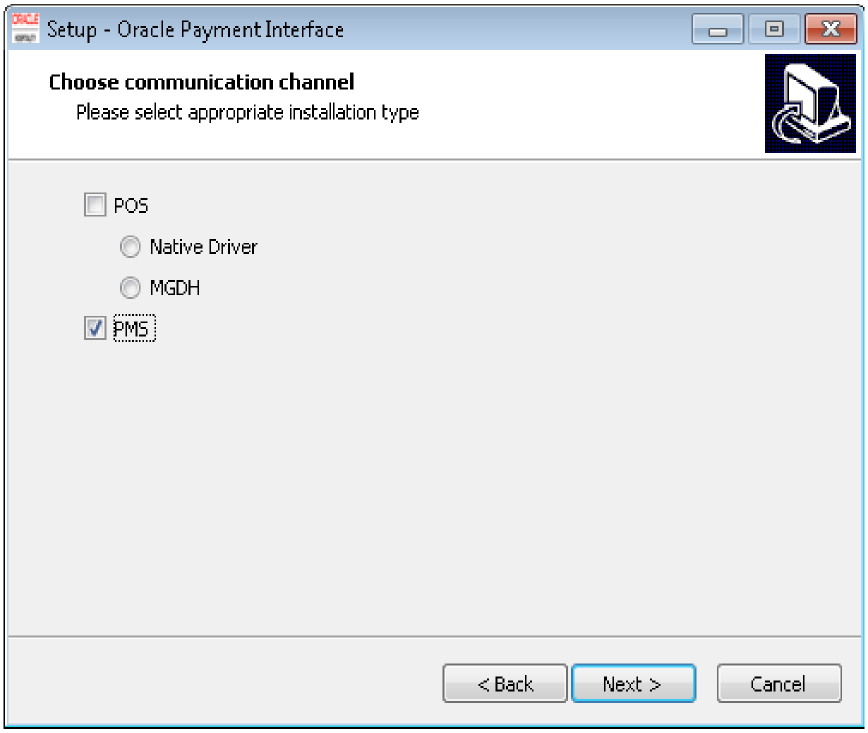
Username and password are case sensitive.
Username should be made only using alphanumeric characters and must have at least one letter.
Password should be at least 8 characters in length and must have at least one letter, one number, one upper case letter, and one special character from the following list !@#$%^&*

Username:

Password:

Confirm password:

4 Select the Oracle Hospitality product integrating with this OPI installation.



Setup - Oracle Payment Interface

Choose communication channel

Please select appropriate installation type

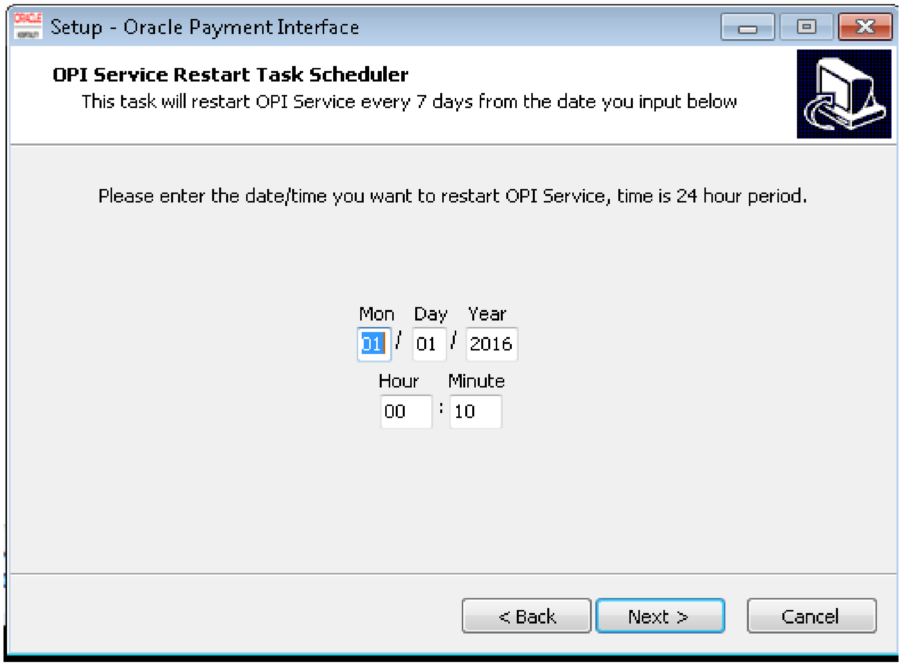
□ POS

○ Native Driver

○ MGDH

☑ PMS

5 Setup the Microsoft Windows task scheduler to restart OPI service weekly.



Setup - Oracle Payment Interface

OPI Service Restart Task Scheduler

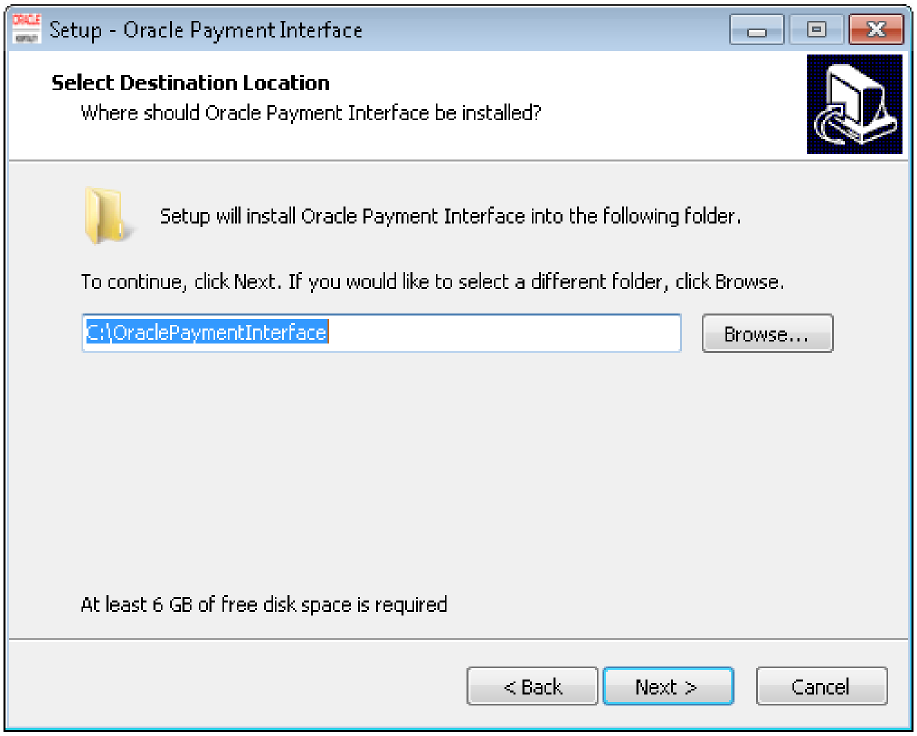
This task will restart OPI Service every 7 days from the date you input below

Please enter the date/time you want to restart OPI Service, time is 24 hour period.

Mon / Day / Year: 01 / 01 / 2016

Hour : Minute: 00 : 10

6 Select the location to install OPI. You can change the folder name or you can keep the default folder name.



Setup - Oracle Payment Interface

Select Destination Location

Where should Oracle Payment Interface be installed?

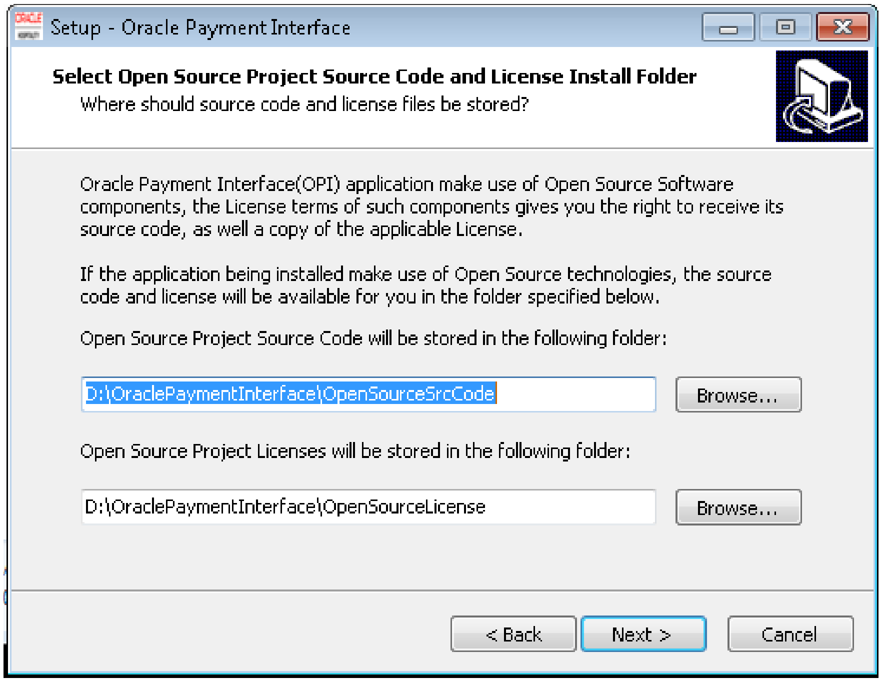
Setup will install Oracle Payment Interface into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\OraclePaymentInterface

At least 6 GB of free disk space is required

7 Select the open source project source code and license installation folder. You can keep the default location inside the OPI folder.



Setup - Oracle Payment Interface

Select Open Source Project Source Code and License Install Folder

Where should source code and license files be stored?

Oracle Payment Interface(OPI) application make use of Open Source Software components, the License terms of such components gives you the right to receive its source code, as well a copy of the applicable License.

If the application being installed make use of Open Source technologies, the source code and license will be available for you in the folder specified below.

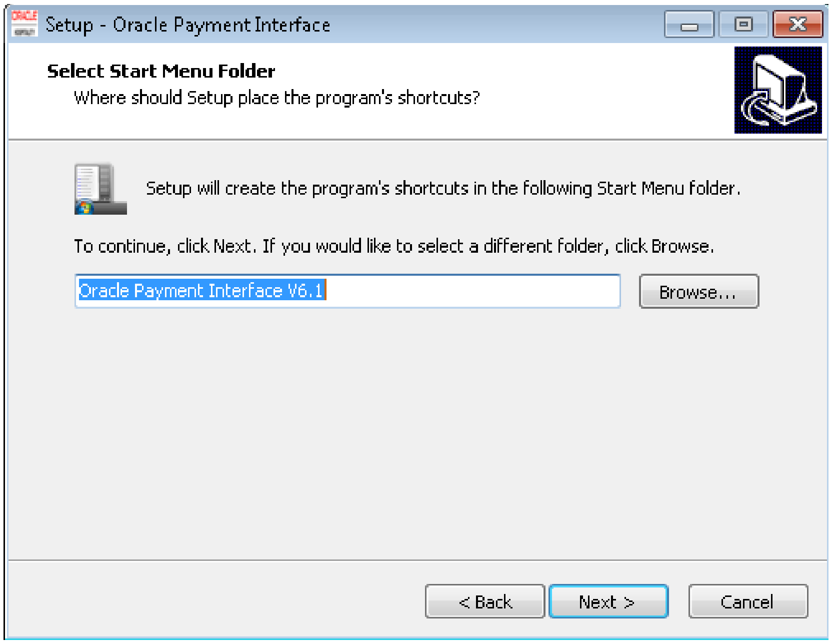
Open Source Project Source Code will be stored in the following folder:

D:\OraclePaymentInterface\OpenSourceSrcCode

Open Source Project Licenses will be stored in the following folder:

D:\OraclePaymentInterface\OpenSourceLicense

8 Select the Start Menu folder for OPI, you can keep the default location.



Select Start Menu Folder

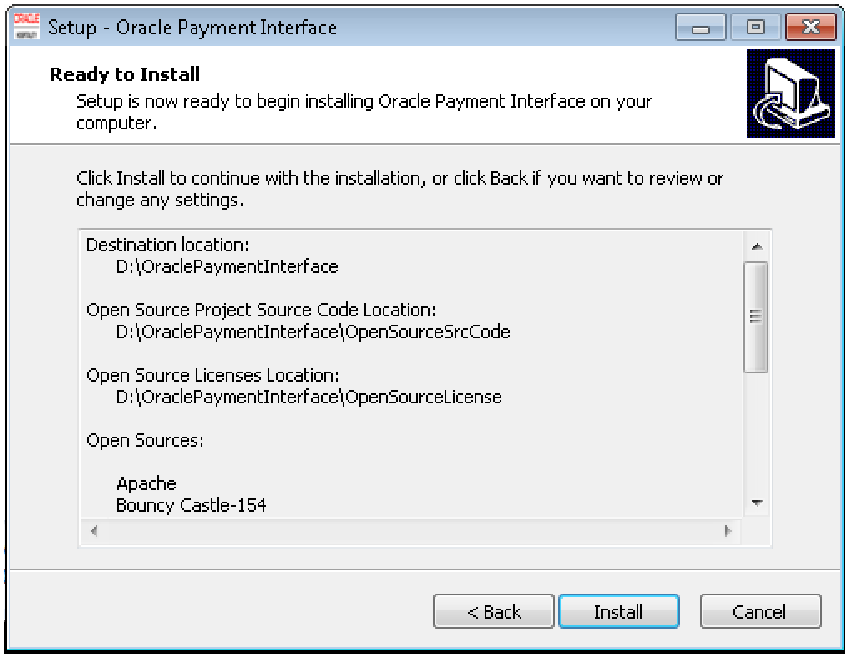
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

Oracle Payment Interface V6.1

9 **Install** will begin installing OPI.



Ready to Install

Setup is now ready to begin installing Oracle Payment Interface on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

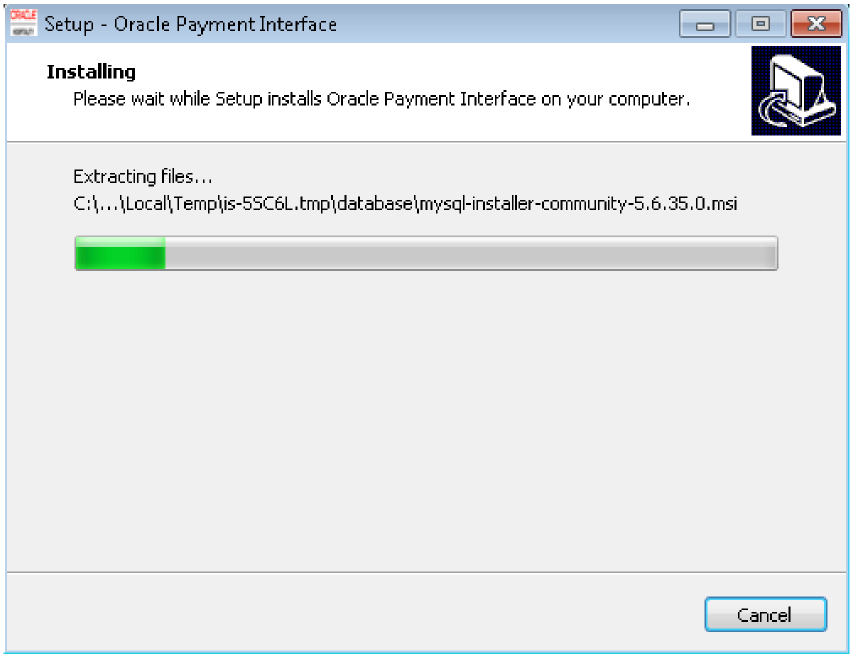
Destination location:
D:\OraclePaymentInterface

Open Source Project Source Code Location:
D:\OraclePaymentInterface\OpenSourceSrcCode

Open Source Licenses Location:
D:\OraclePaymentInterface\OpenSourceLicense

Open Sources:

Apache
Bouncy Castle-154



Installing

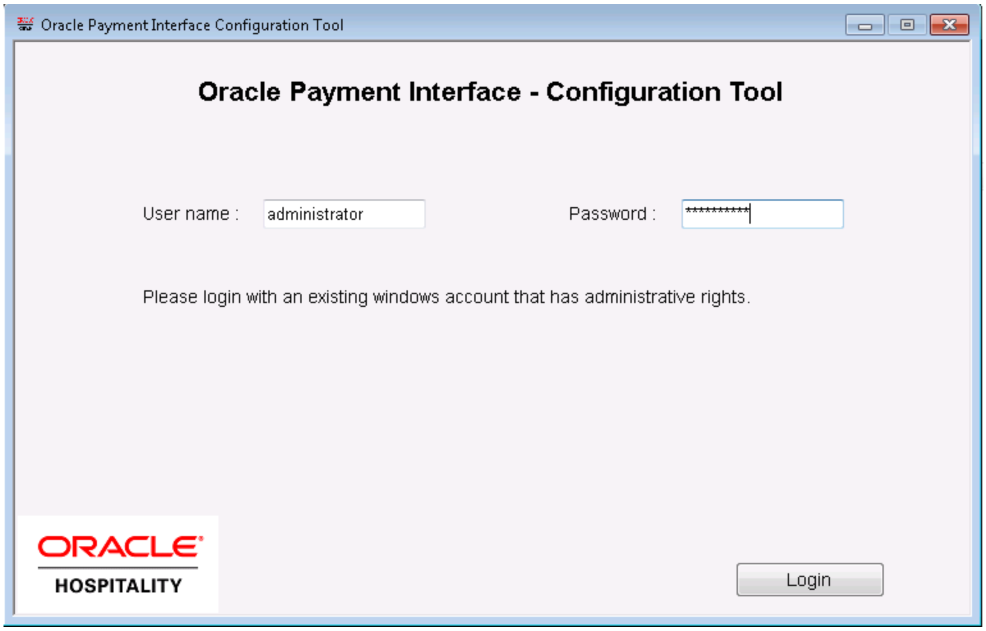
Please wait while Setup installs Oracle Payment Interface on your computer.

Extracting files...

C:\...\Local\Temp\is-5SC6L.tmp\database\mysql-installer-community-5.6.35.0.msi

3 Configuring OPI

1 Run *:\OraclePaymentInterface\bin\OPIConfigurationWizard.exe*
Login as local or domain administrator.



Oracle Payment Interface - Configuration Tool

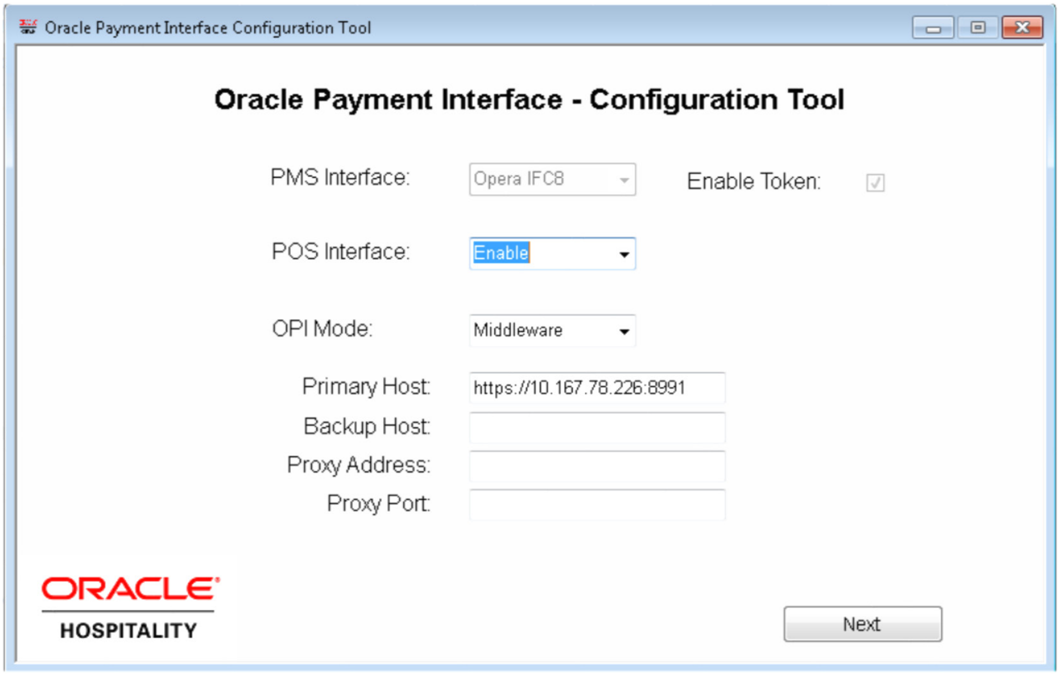
User name : administrator

Password : ***********

Please login with an existing windows account that has administrative rights.

Select the ***Enable Token*** box. The Token Exchange service effectively runs via a second merchant configuration within OPI. The Token Exchange functionality is separate to the IFC8 merchant functionality.

- From the **OPI Mode** drop-down list, select the **Terminal** for the PED direct connection or select **Middleware** for middleware connection.
- Enter the third-party payment service provider middleware Host IP address if Middleware mode selected. If Terminal mode selected OPI configuration will populate another window in further steps to input Workstation ID and IP address.



Oracle Payment Interface Configuration Tool

Oracle Payment Interface - Configuration Tool

PMS Interface: Opera IFC8

Enable Token: ☑

POS Interface: Enable

OPI Mode: Middleware

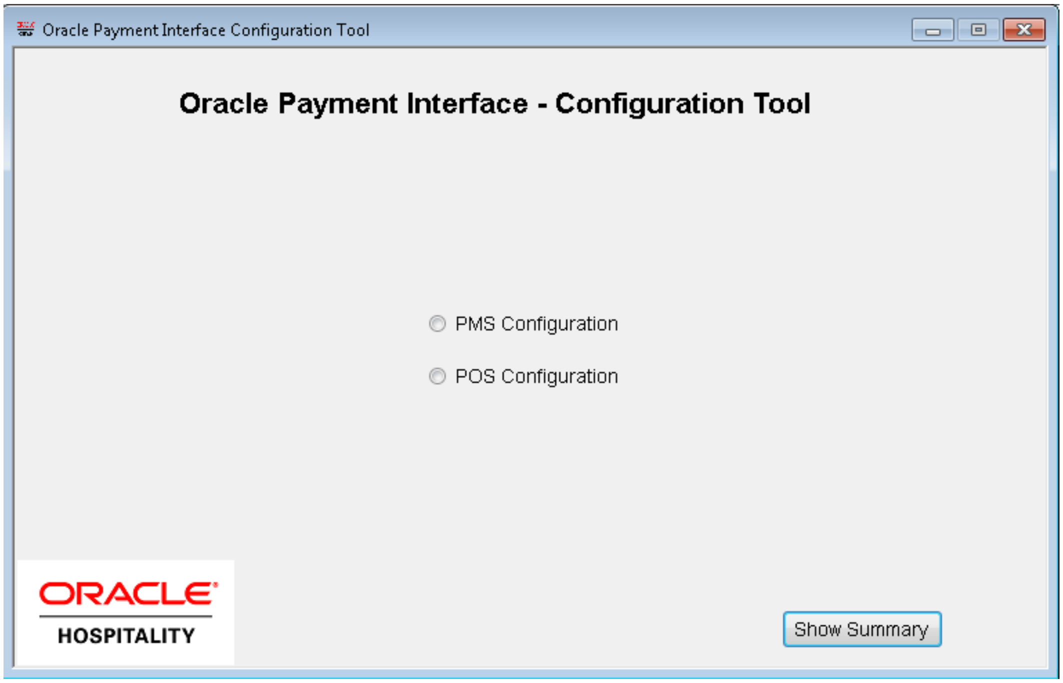
Primary Host: https://10.167.78.226:8991

Backup Host:

Proxy Address:

Proxy Port:

2 Select PMS Configuration.



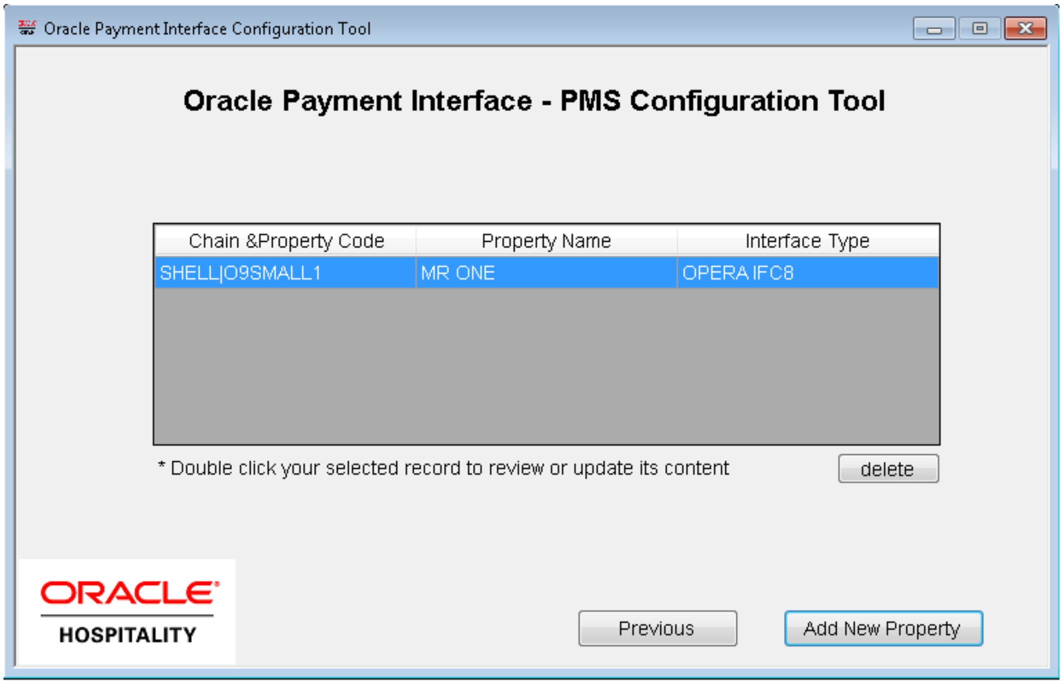
Oracle Payment Interface Configuration Tool

Oracle Payment Interface - Configuration Tool

○ PMS Configuration

○ POS Configuration

3 Click on add Property to add a new merchant configuration for OPERA



Oracle Payment Interface - PMS Configuration Tool

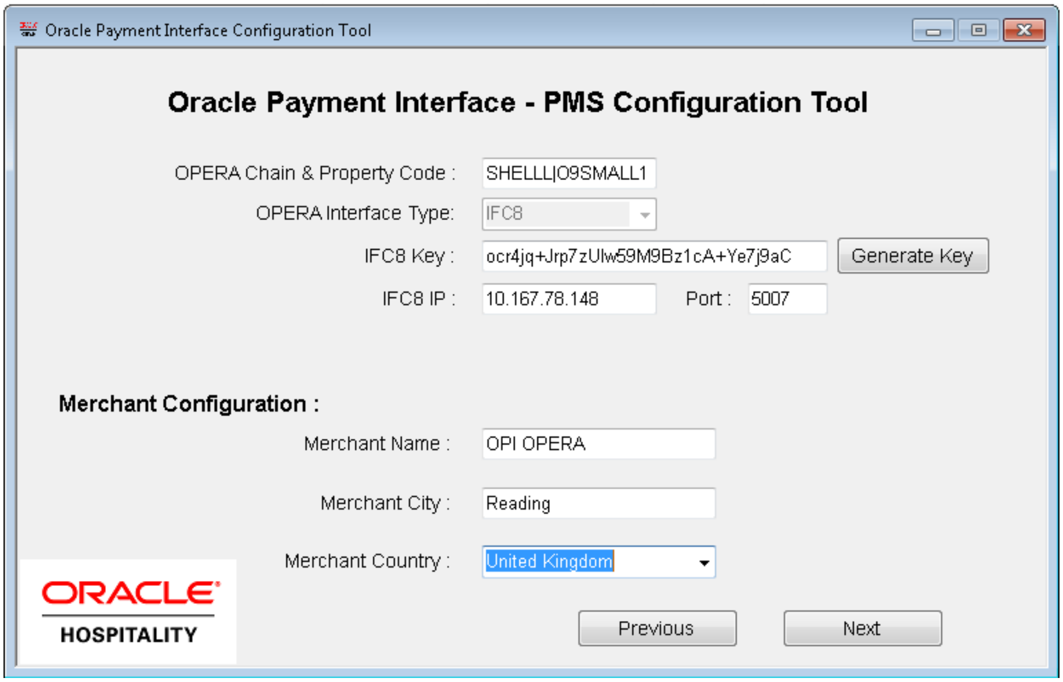
Chain &Property Code	Property Name	Interface Type
SHELL|O9SMALL1	MR ONE	OPERA IFC8

* Double click your selected record to review or update its content

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.
- The format of the ***SiteId*** field includes a pipe character to separate the two *OPERA Vault Chain Code & Property Code* values.
- See the screenshot below where OPERA Vault chain code is “**SHELL**” and Property code is “**O9SMALL1**” so value in field will be “**SHELL|O9SMALL1**”
- Select **Generate Key**. You must use this key to configure the Hotel Property Interface (IFC8).
- Enter the **IFC8 IP address** and **port** number for the Hotel Property Interface (IFC8) server.
- Enter the **Merchant name**, **city**, and **country** information.
- Select **Next.**

Whilst 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 - PMS Configuration Tool

OPERA Chain & Property Code : SHELLL|O9SMALL1

OPERA Interface Type: IFC8

IFC8 Key : ocr4jq+Jrp7zUlw59M9Bz1cA+Ye7j9aC

IFC8 IP : 10.167.78.148 Port : 5007

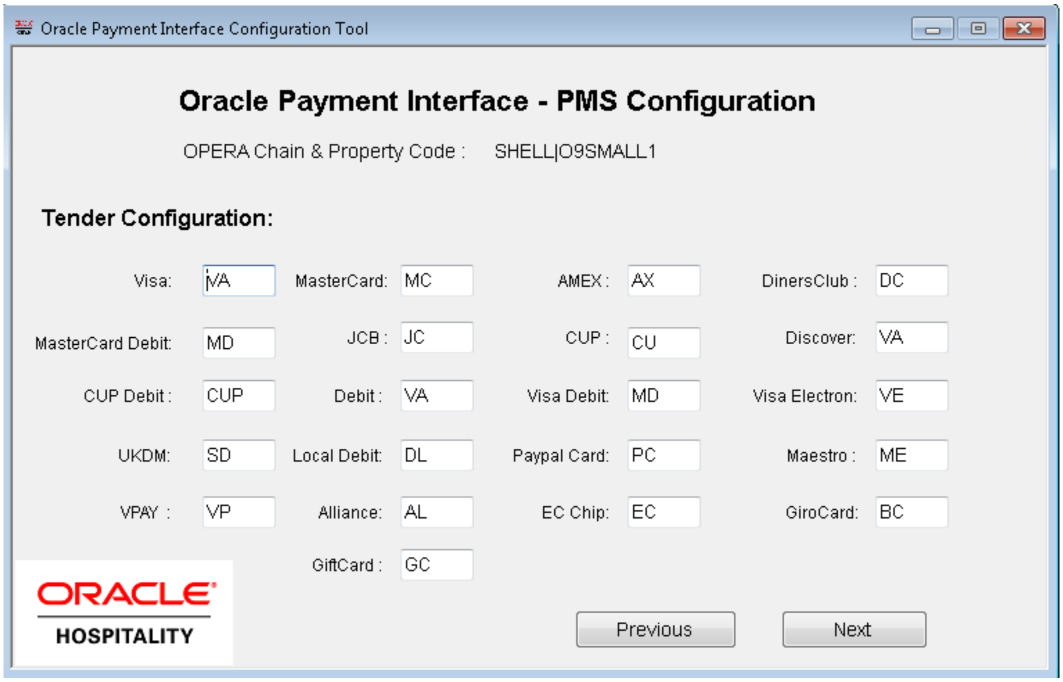
Merchant Configuration :

Merchant Name : OPI OPERA

Merchant City : Reading

Merchant Country : United Kingdom

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



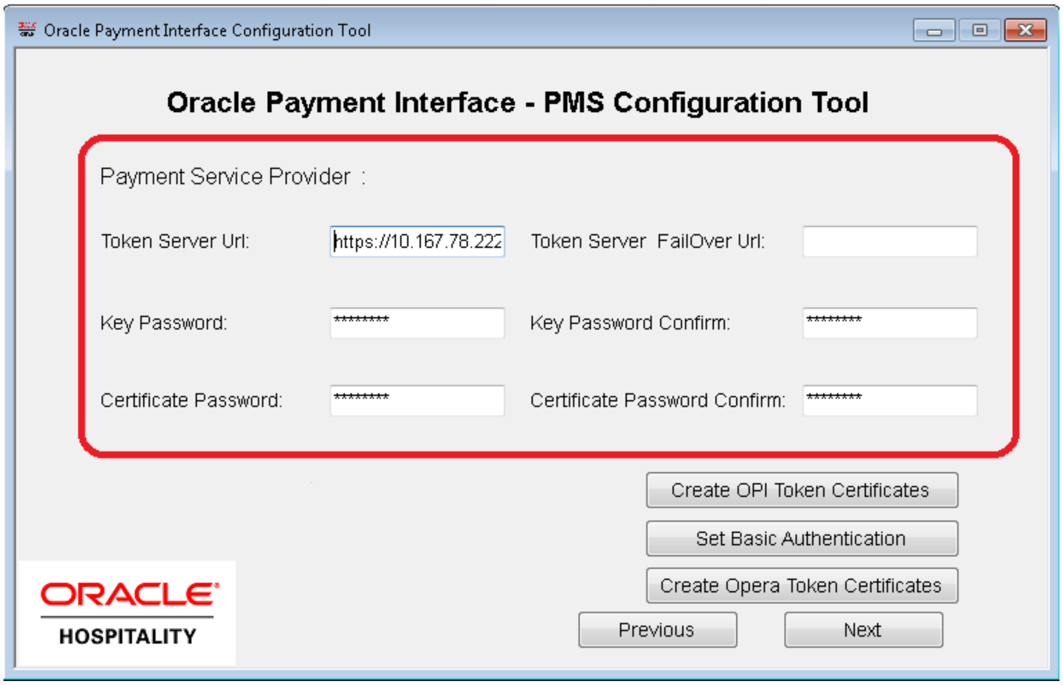
Oracle Payment Interface - PMS Configuration

OPERA Chain & Property Code : SHELLL|O9SMALL1

Tender Configuration:

Visa:	VA	MasterCard:	MC	AMEX :	AX	DinersClub :	DC
MasterCard Debit:	MD	JCB :	JC	CUP :	CU	Discover:	VA
CUP Debit :	CUP	Debit :	VA	Visa Debit:	MD	Visa Electron:	VE
UKDM:	SD	Local Debit:	DL	Paypal Card:	PC	Maestro :	ME
VPAY :	VP	Alliance:	AL	EC Chip:	EC	GiroCard:	BC
		GiftCard :	GC				

6 The top half of the next page relates to communication from OPI to the PSP host, and the PSP Client certificate credentials.


Oracle Payment Interface Configuration Tool

Oracle Payment Interface - PMS Configuration Tool

Payment Service Provider :

Token Server Url: https://10.167.78.222

Token Server FailOver Url:

Key Password: *********

Key Password Confirm: *********

Certificate Password: *********

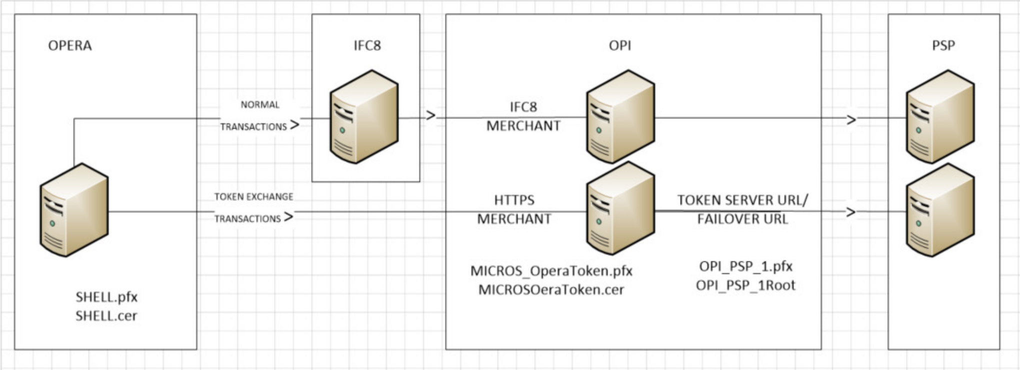
Certificate Password Confirm: *********

Create OPI Token Certificates
Set Basic Authentication
Create Opera Token Certificates
Previous
Next
ORACLE
HOSPITALITY

Key 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.

Certificates



OPI on Premise Token Exchange requires three sets of certificates:

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

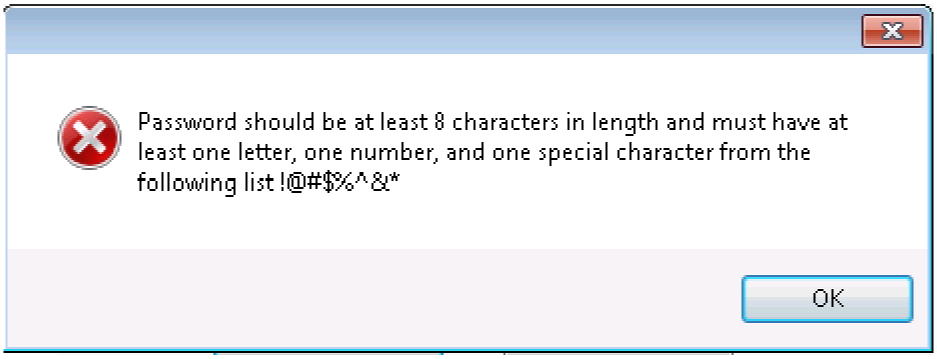
- A client side certificate file in the name of "OPI_PSP_1.pfx", this is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password. If the file provided by PSP has a different name, rename to "OPI_PSP_1.pfx" before deploying it to OPI.
- The root certificate 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

Deploying the client certificate at OPI side is straightforward - you just need to place the file in folder "*:\OraclePaymentInterface\key\*".

The passwords set by the PSP should meet the minimum complexity requirements discussed below; otherwise, it will not be possible to enter the details to the OPI configuration.

Note: The PSP Client Side Certificates expiry date will vary depending on what the PSP set during creation of the certificate. Check the expiry date in the properties of the certificate files.
Be aware the PSP certificates will need to updating, prior to the expiry date to avoid downtime to the interface.

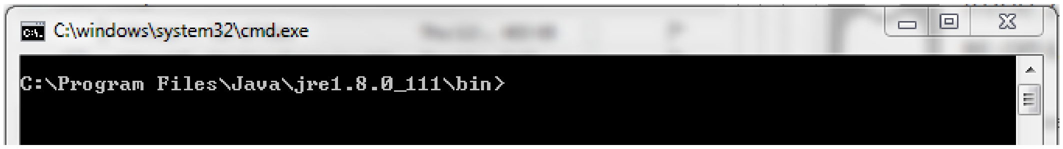

Password should be at least 8 characters in length and must have at least one letter, one number, and one special character from the following list !@#$%^&*

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>
```

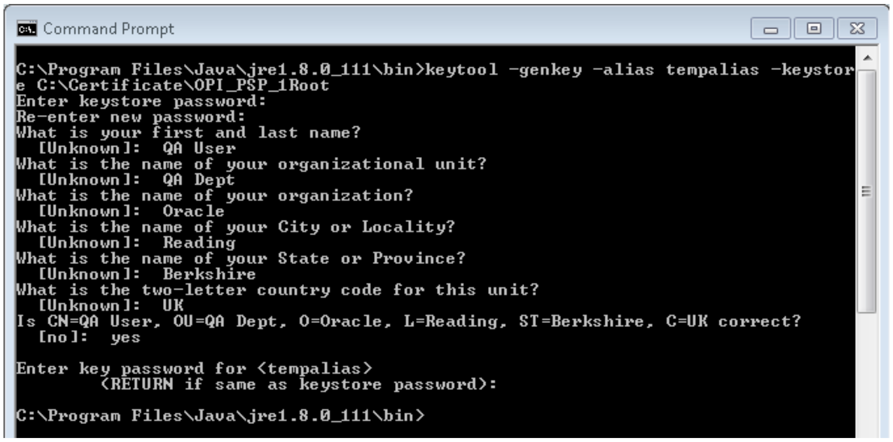
The three commands below, when run in sequence;

- 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.

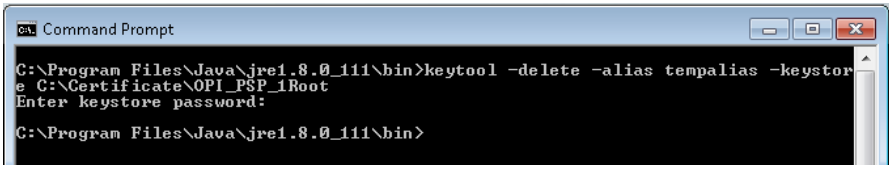


```
C:\Program Files\Java\jre1.8.0_111\bin>keytool -genkey -alias tempalias -keystor
e C:\Certificate\OPI_PSP_1Root
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  QA User
What is the name of your organizational unit?
  [Unknown]:  QA Dept
What is the name 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.

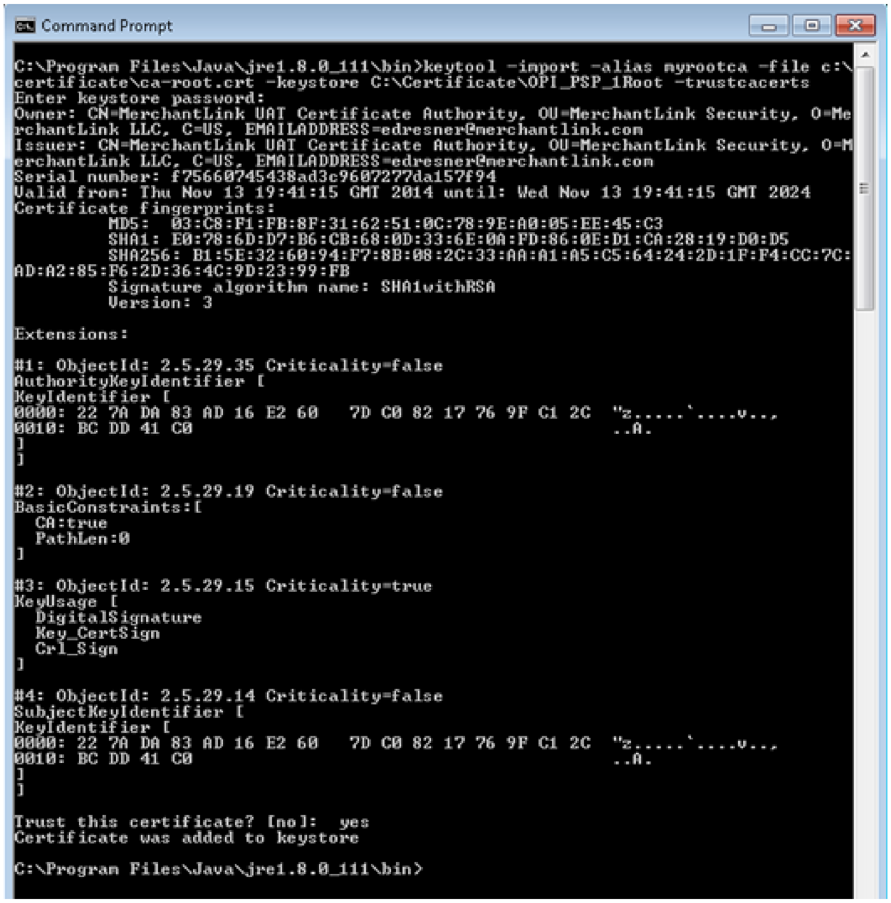
(i.e. RETURN if same as keystore password – Press Enter)

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>
```

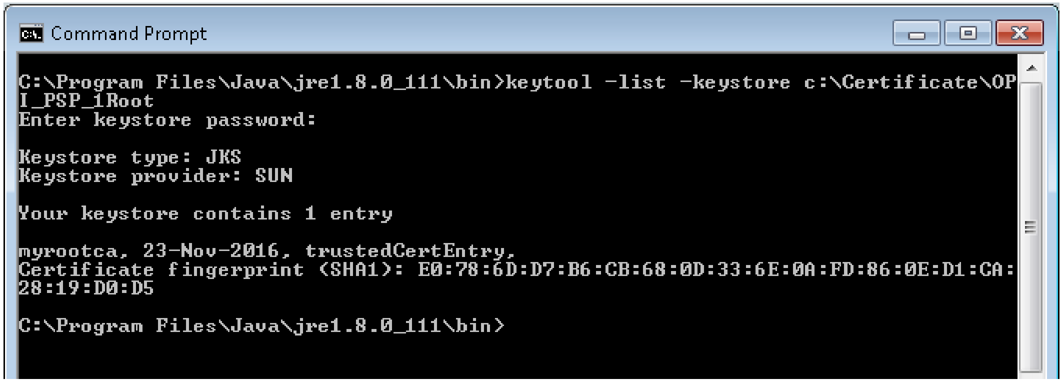
keytool -import -alias myrootca -file C:\Certificates\ca-cert.crt -keystore C:\Certificates\OPI_PSP_1Root -trustcacerts



```
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>
```

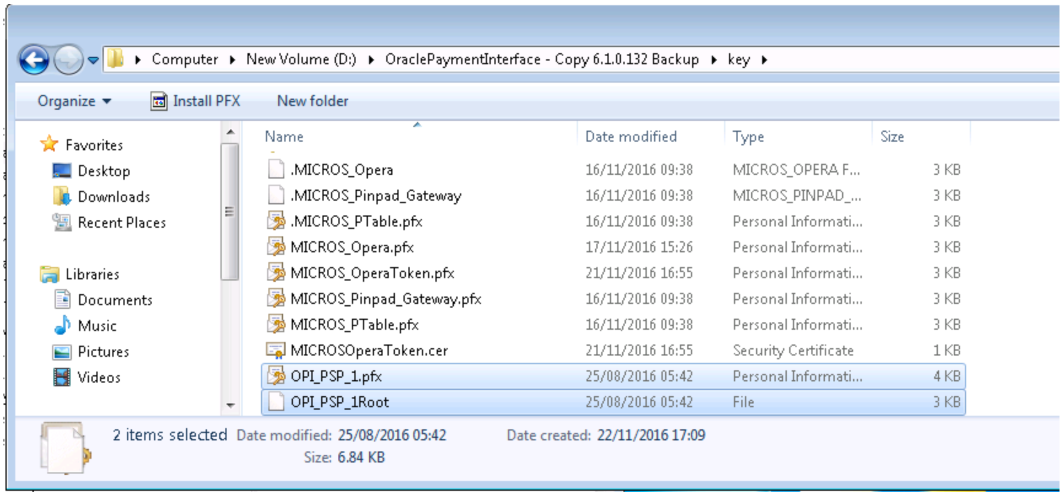
Verify the new Java keystore's details by running the following command if required;

```
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 once ready, will need to be located in the folder; *:\OraclePaymentInterface\key\*



Name	Date modified	Type	Size
.MICROS_Opera	16/11/2016 09:38	MICROS_OPERA F...	3 KB
.MICROS_Pinpad_Gateway	16/11/2016 09:38	MICROS_PINPAD_...	3 KB
.MICROS_PTable.pfx	16/11/2016 09:38	Personal Informati...	3 KB
MICROS_Opera.pfx	17/11/2016 15:26	Personal Informati...	3 KB
MICROS_OperaToken.pfx	21/11/2016 16:55	Personal Informati...	3 KB
MICROS_Pinpad_Gateway.pfx	16/11/2016 09:38	Personal Informati...	3 KB
MICROS_PTable.pfx	16/11/2016 09:38	Personal Informati...	3 KB
MICROSOperaToken.cer	21/11/2016 16:55	Security Certificate	1 KB
OPI_PSP_1.pfx	25/08/2016 05:42	Personal Informati...	4 KB
OPI_PSP_1Root	25/08/2016 05:42	File	3 KB

2 items selected Date modified: 25/08/2016 05:42 Date created: 22/11/2016 17:09
Size: 6.84 KB

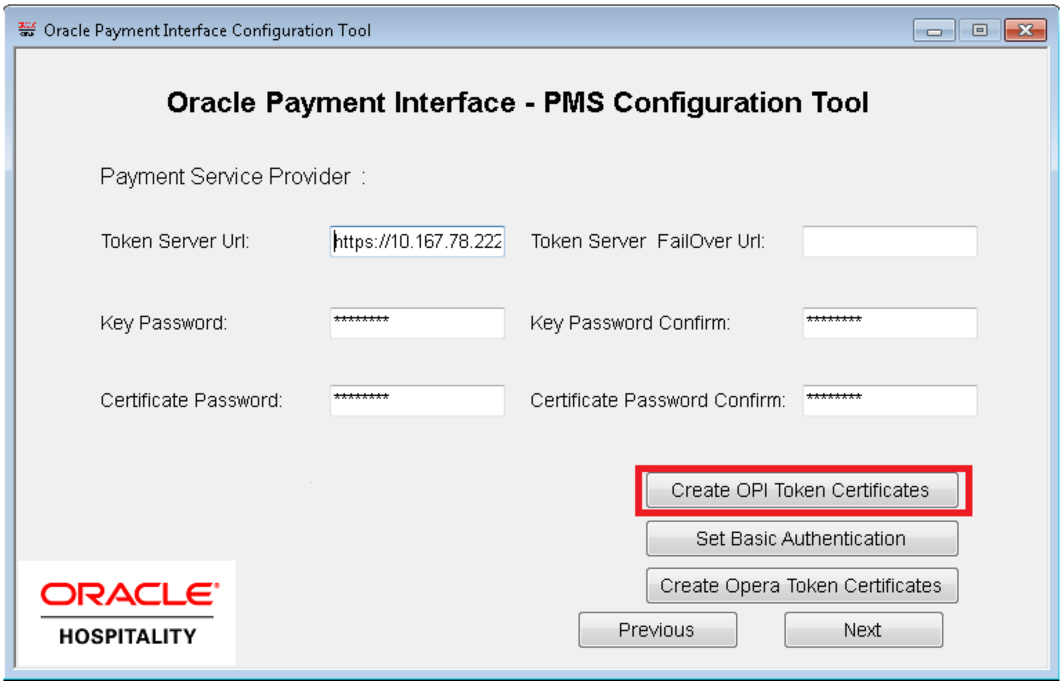
Updating a JKS with a new PSP certificate

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\key\* folder prior to following the steps above to import new certificate file.

OPI - Server Side Certificates

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

- Click the ***Create OPI Token Certificates*** button to proceed.



Oracle Payment Interface Configuration Tool

Oracle Payment Interface - PMS Configuration Tool

Payment Service Provider :

Token Server Url: https://10.167.78.222

Token Server FailOver Url:

Key Password: *********

Key Password Confirm: *********

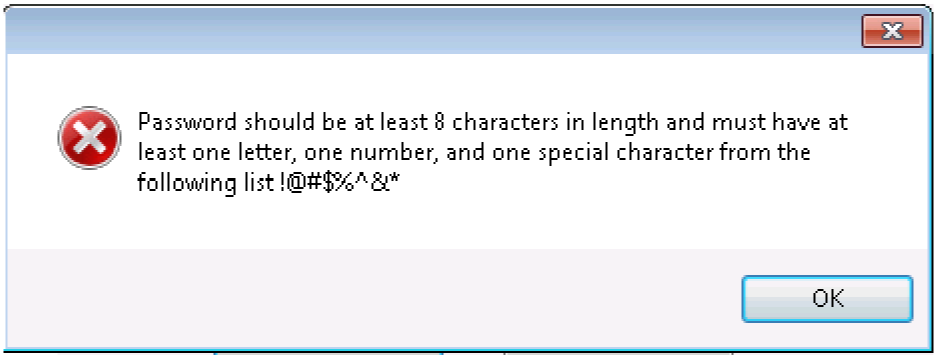
Certificate Password: *********

Certificate Password Confirm: *********

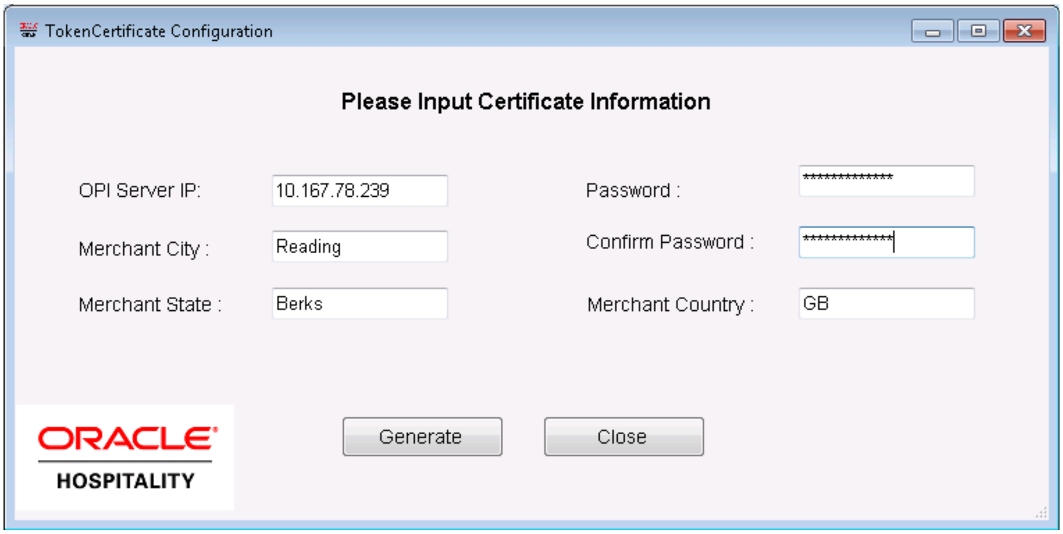
Create OPI Token Certificates
Set Basic Authentication
Create Opera Token Certificates
Previous
Next
ORACLE
HOSPITALITY

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 !@#$%^&*

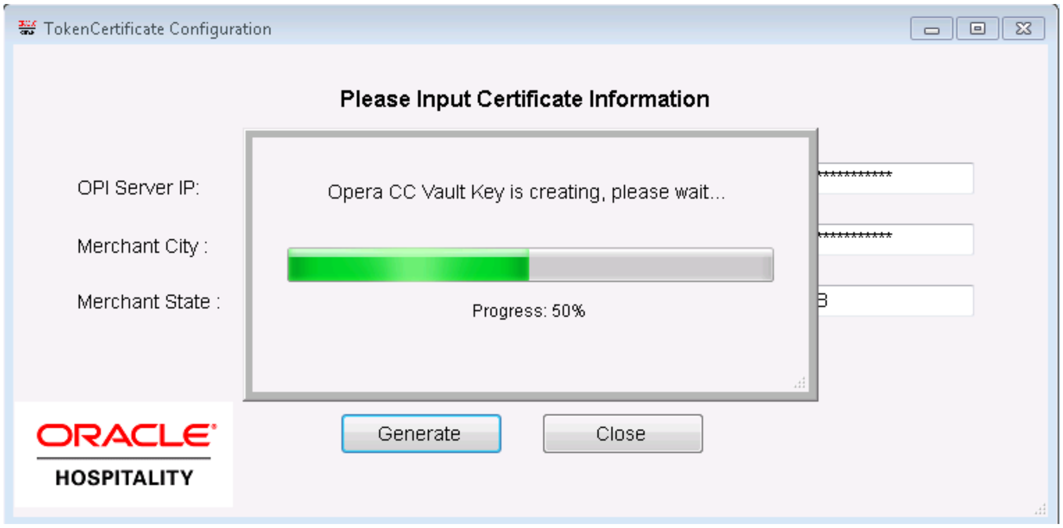


TokenCertificate Configuration

Please Input Certificate Information

OPI Server IP:	10.167.78.239	Password :	**************
Merchant City :	Reading	Confirm Password :	**************
Merchant State :	Berks	Merchant Country :	GB

Once ready select ***Generate***

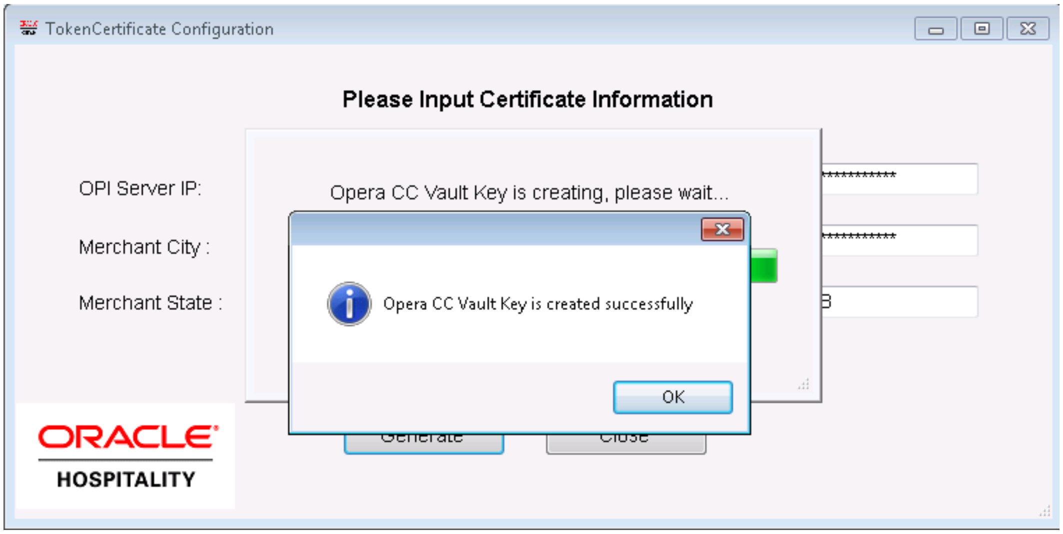


TokenCertificate Configuration

Please Input Certificate Information

Opera CC Vault Key is creating, please wait...

Progress: 50%



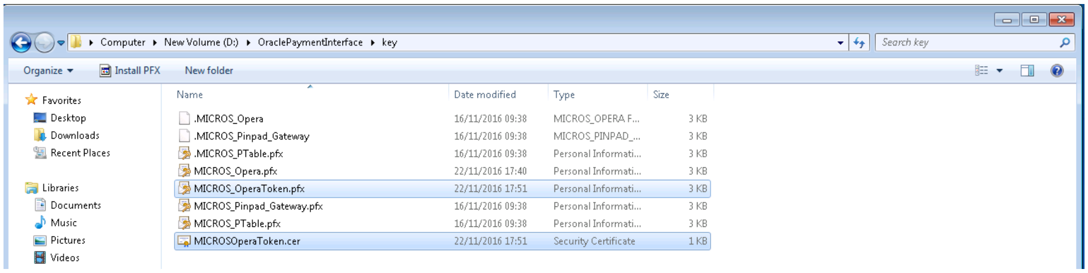
TokenCertificate Configuration

Please Input Certificate Information

Opera CC Vault Key is creating, please wait...

Opera CC Vault Key is created successfully

This process will generate the MICROS_OperaToken.pfx & MICROSOperaToken.cer files in the folder;
:*OraclePaymentInterface**key*\



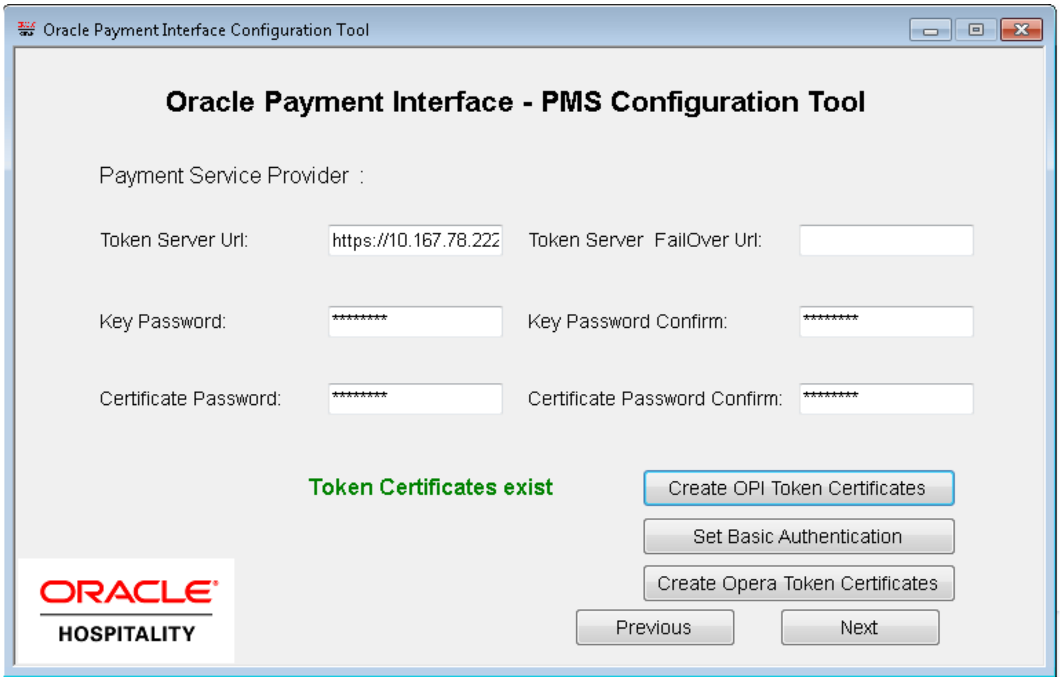
Computer ▸ New Volume (D:) ▸ OraclePaymentInterface ▸ key

Name	Date modified	Type	Size
.MICROS_Opera	16/11/2016 09:38	MICROS_OPERA F...	3 KB
.MICROS_Pinpad_Gateway	16/11/2016 09:38	MICROS_PINPAD_...	3 KB
.MICROS_PTable.pfx	16/11/2016 09:38	Personal Informati...	3 KB
MICROS_Opera.pfx	22/11/2016 17:40	Personal Informati...	3 KB
MICROS_OperaToken.pfx	22/11/2016 17:51	Personal Informati...	3 KB
MICROS_Pinpad_Gateway.pfx	16/11/2016 09:38	Personal Informati...	3 KB
MICROS_PTable.pfx	16/11/2016 09:38	Personal Informati...	3 KB
MICROSOperaToken.cer	22/11/2016 17:51	Security Certificate	1 KB

<u>Note: The OPI Server 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.</u>
<u>The OPI Server Side Certificates will need updating prior to the expiry date to avoid downtime to the interface.</u>

Copy the ***MICROSOperaToken.cer*** files to <u>*all*</u> of the Opera registered terminal 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*)

8 Close the Certificate generation screen, you should now see the green message *Token Certificate exists*.



Oracle Payment Interface Configuration Tool

Oracle Payment Interface - PMS Configuration Tool

Payment Service Provider :

Token Server Url: https://10.167.78.222
Token Server FailOver Url:

Key Password: *********
Key Password Confirm: *********

Certificate Password: *********
Certificate Password Confirm: *********

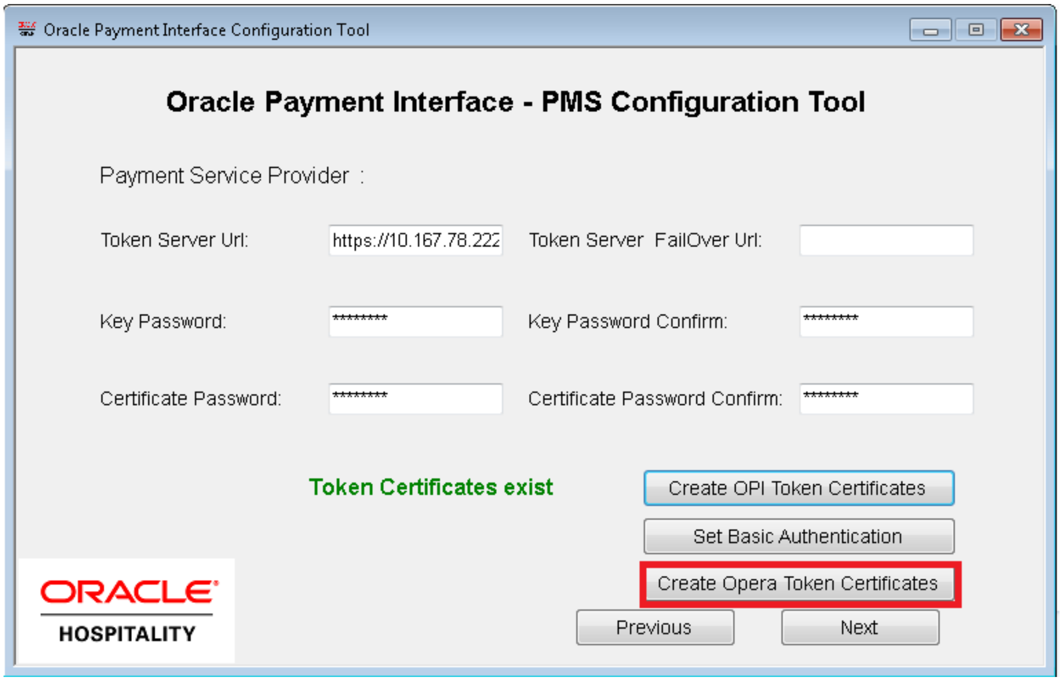
Token Certificates exist

Create OPI Token Certificates
Set Basic Authentication
Create Opera Token Certificates
Previous
Next
ORACLE
HOSPITALITY

OPI - Client Side Certificates

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

- Click the ***Create Opera Token Certificates*** button to proceed.



Oracle Payment Interface Configuration Tool

Oracle Payment Interface - PMS Configuration Tool

Payment Service Provider :

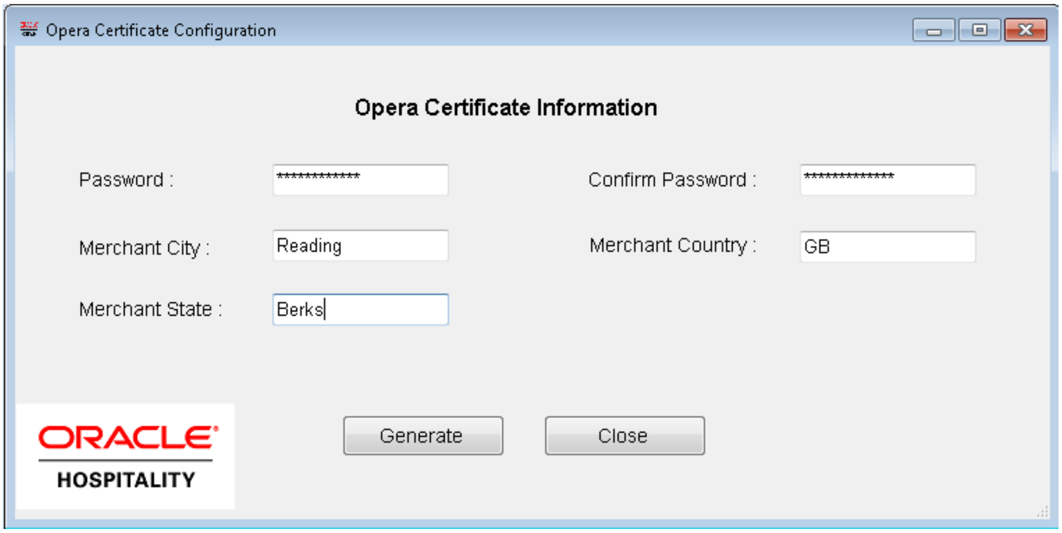
Token Server Url: https://10.167.78.222
Token Server FailOver Url:

Key Password: *********
Key Password Confirm: *********

Certificate Password: *********
Certificate Password Confirm: *********

Token Certificates exist

Create OPI Token Certificates
Set Basic Authentication
Create Opera Token Certificates
Previous
Next
ORACLE
HOSPITALITY



Opera Certificate Configuration

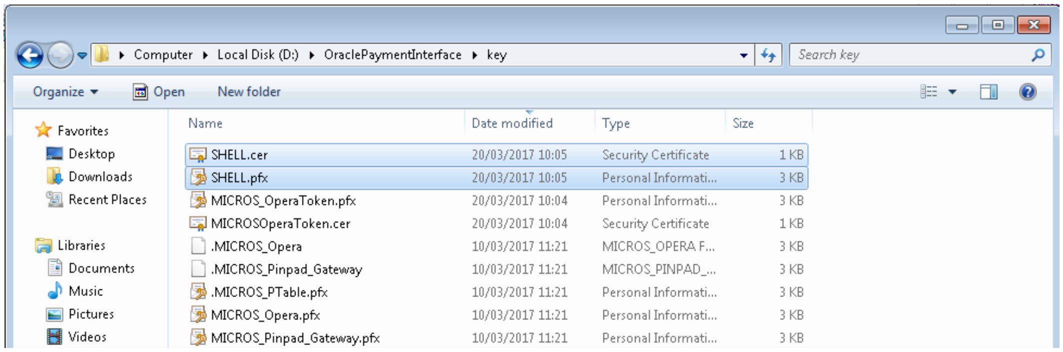
Opera Certificate Information

Password : *************
Confirm Password : **************

Merchant City : Reading
Merchant Country : GB

Merchant State : Berks

- Once values entered and ready click generate.



Name	Date modified	Type	Size
SHELL.cer	20/03/2017 10:05	Security Certificate	1 KB
SHELL.pfx	20/03/2017 10:05	Personal Informati...	3 KB
MICROS_OperaToken.pfx	20/03/2017 10:04	Personal Informati...	3 KB
MICROSOperaToken.cer	20/03/2017 10:04	Security Certificate	1 KB
.MICROS_Opera	10/03/2017 11:21	MICROS_OPERA F...	3 KB
.MICROS_Pinpad_Gateway	10/03/2017 11:21	MICROS_PINPAD_...	3 KB
.MICROS_PTable.pfx	10/03/2017 11:21	Personal Informati...	3 KB
MICROS_Opera.pfx	10/03/2017 11:21	Personal Informati...	3 KB
MICROS_Pinpad_Gateway.pfx	10/03/2017 11:21	Personal Informati...	3 KB

In the example above the certificates are named SHELL, 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.

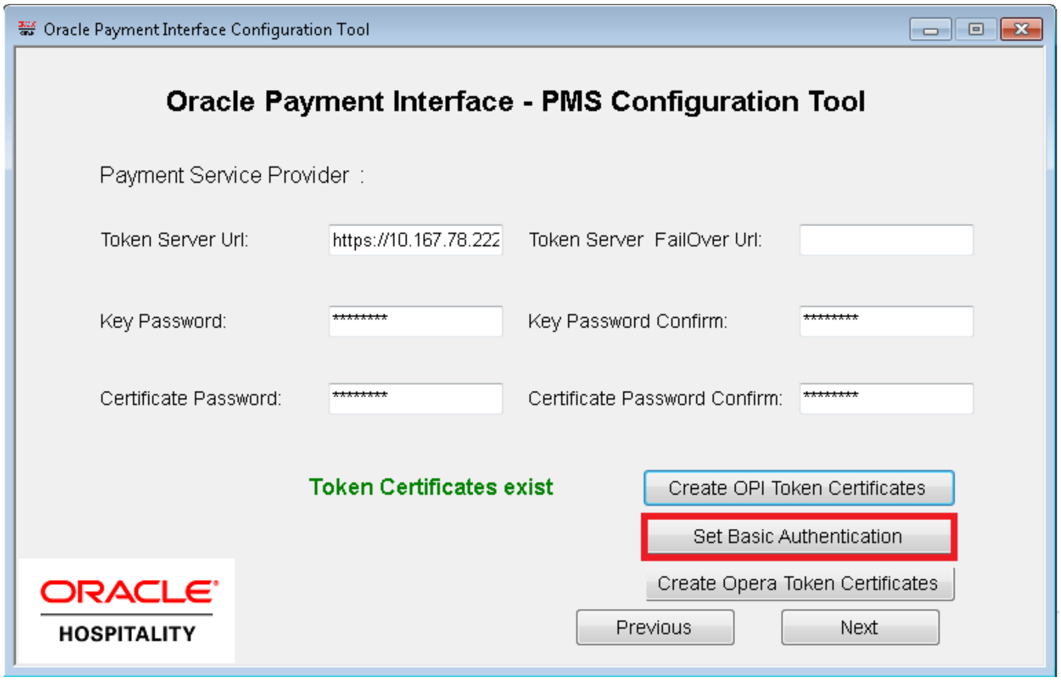
Copy the *SHELL.pfx* & *SHELL.crt* files created, to *all* of the Opera registered terminals that you will run the Token Exchange transactions from. Import the certificates using *mmc.exe* (*see below for more info*)

- SHELL.pfx import to Personal – you will need the password used during the creation in the previous steps.

- SHELL.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.

10 Select ***Set Basic Authentication*** to configure the Header Authentication credentials used in communications from Opera > OPI.



Oracle Payment Interface Configuration Tool

Oracle Payment Interface - PMS Configuration Tool

Payment Service Provider :

Token Server Url: https://10.167.78.222

Token Server FailOver Url:

Key Password: *********

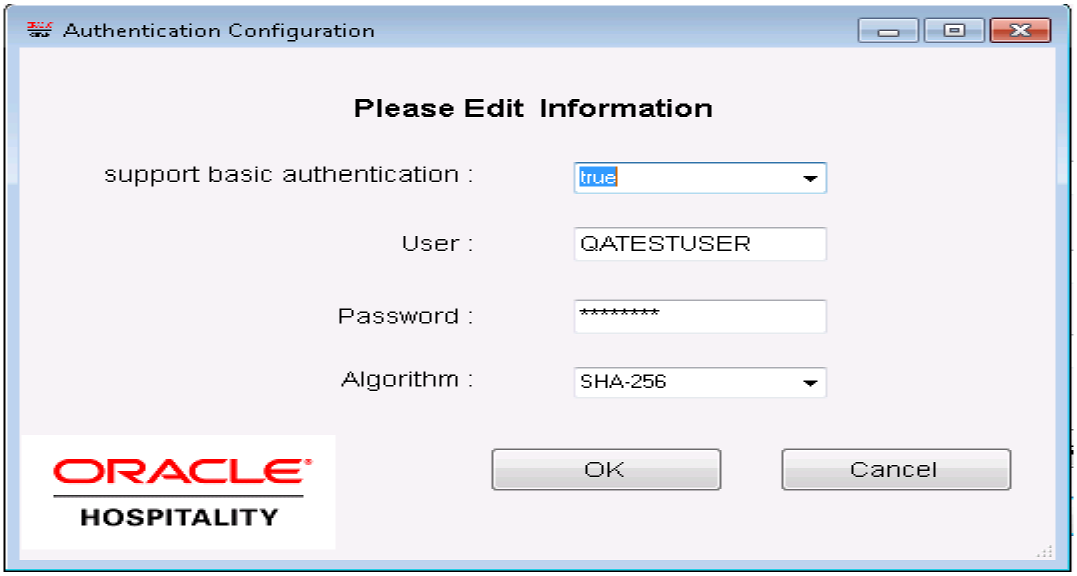
Key Password Confirm: *********

Certificate Password: *********

Certificate Password Confirm: *********

Token Certificates exist

Create OPI Token Certificates
Set Basic Authentication
Create Opera Token Certificates
Previous
Next
ORACLE
HOSPITALITY



Authentication Configuration

Please Edit Information

support basic authentication : true

User : QATESTUSER

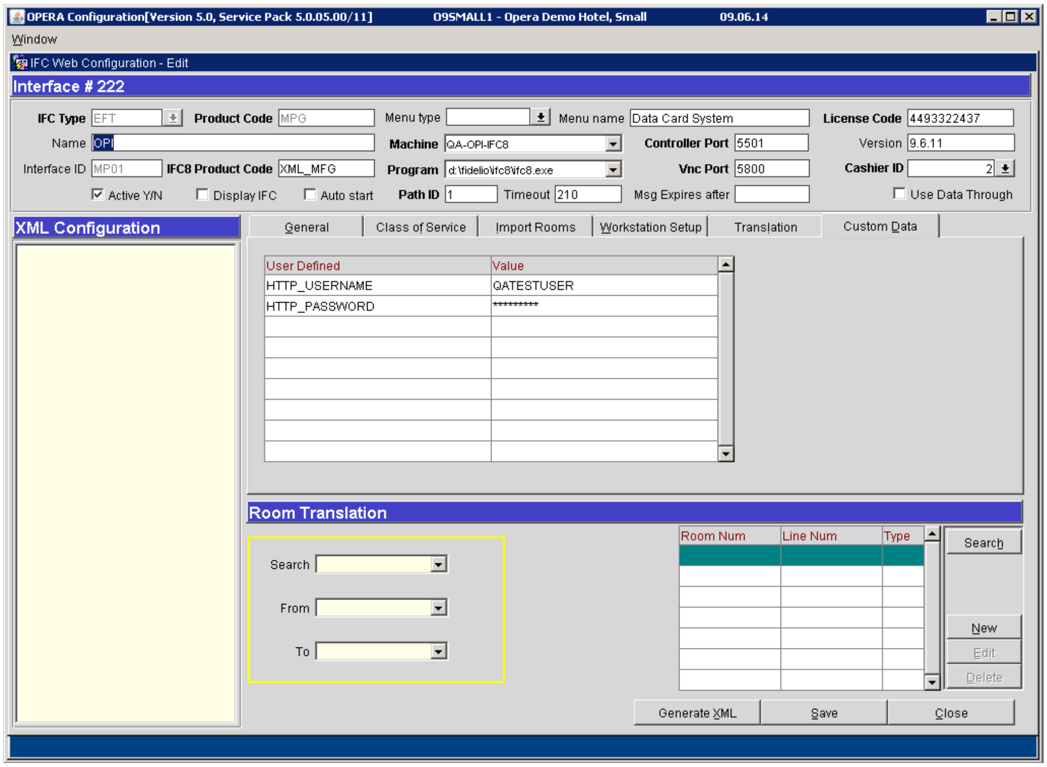
Password : *********

Algorithm : SHA-256

11 Select OK to confirm the Authentication details and return to the PSP/Certificate Page.

- The Algorithm setting is the hashing method used to store the password at the OPI host machine; it is not set at the Opera side. The minimum supported method is ***SHA-256***.

- The details entered will need to match the details entered in the OPERA Interface Custom Data page, see below;
  OPERA PMS Configuration > Setup > Property Interfaces > Interface Configuration > edit EFT IFC OPI > Custom Data tab



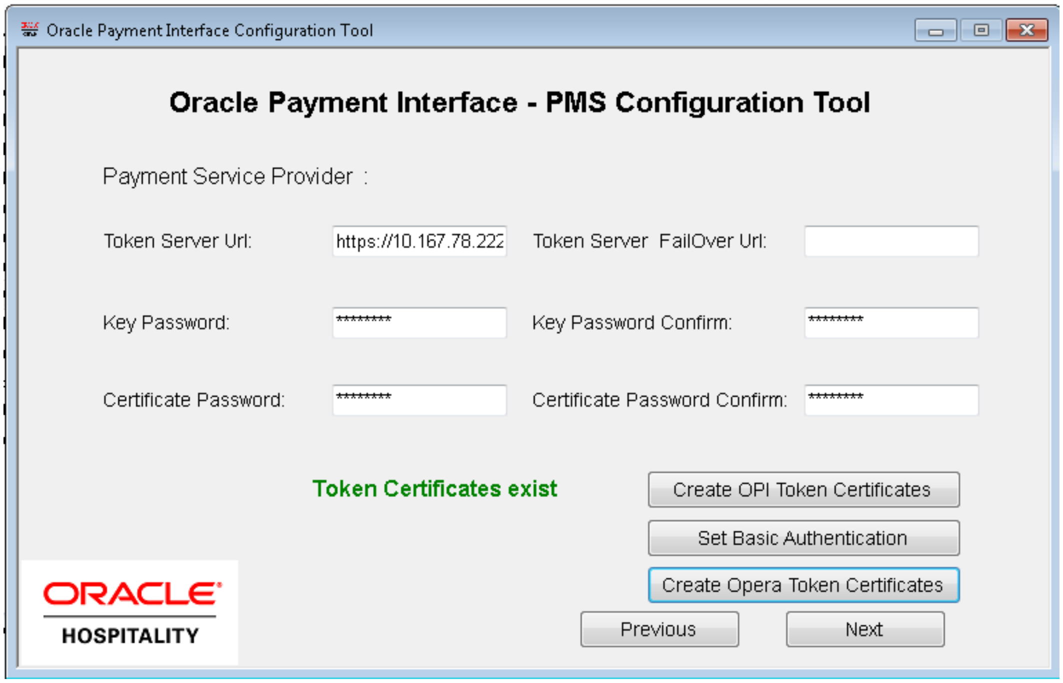
IFC Type EFT
Product Code MPG
Menu type
Menu name Data Card System
License Code 4493322437
Name OPI
Machine QA-OPI-IFC8
Controller Port 5501
Version 9.6.11
Interface ID MP01
IFC8 Product Code XML_MFG
Program d:\fidelio\ifc8\ifc8.exe
Vnc Port 5800
Cashier ID 2
☑ Active Y/N ☐ Display IFC ☐ Auto start
Path ID 1
Timeout 210
Msg Expires after
☐ Use Data Through

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

Search
From
To

Room Num	Line Num	Type

12 Select ***Next*** to continue.


Oracle Payment Interface Configuration Tool
Create OPI Token Certificates
Set Basic Authentication
Create Opera Token Certificates
Previous
Next
ORACLE
HOSPITALITY

Oracle Payment Interface - PMS Configuration Tool

Payment Service Provider :

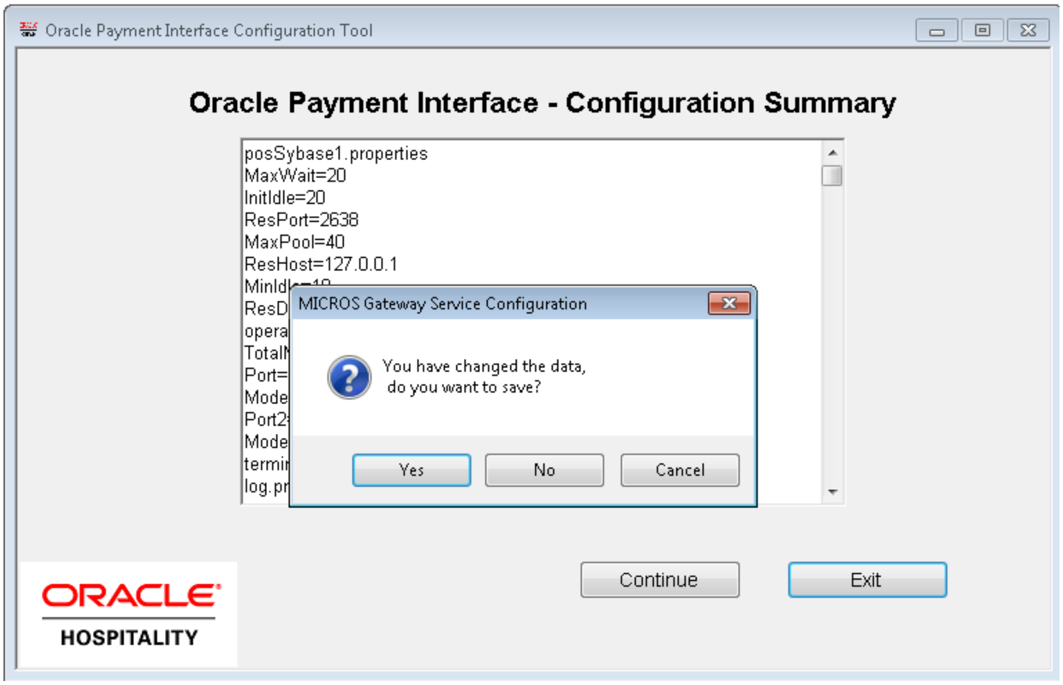
Token Server Url: https://10.167.78.222 Token Server FailOver Url:

Key Password: ********* Key Password Confirm: *********

Certificate Password: ********* Certificate Password Confirm: *********

Token Certificates exist

13 Select *Exit*, and save the changes when prompted.



Oracle Payment Interface - Configuration Summary

```
posSybase1.properties
MaxWait=20
InitIdle=20
ResPort=2638
MaxPool=40
ResHost=127.0.0.1
MinIdl
ResD
opera
TotalI
Port=
Mode
Port2
Mode
termi
log.pr
```

MICROS Gateway Service Configuration

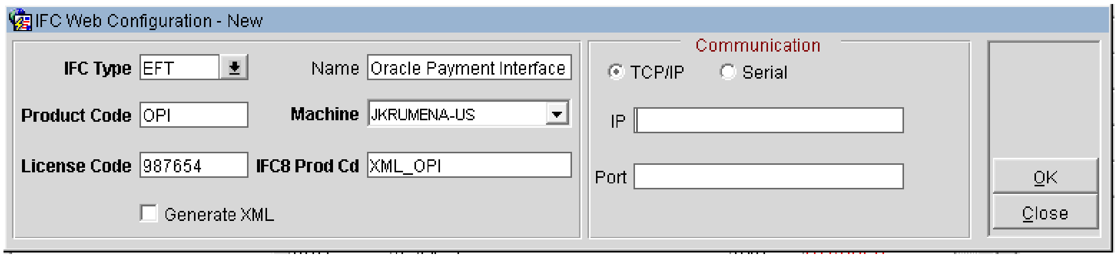
You have changed the data, do you want to save?

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

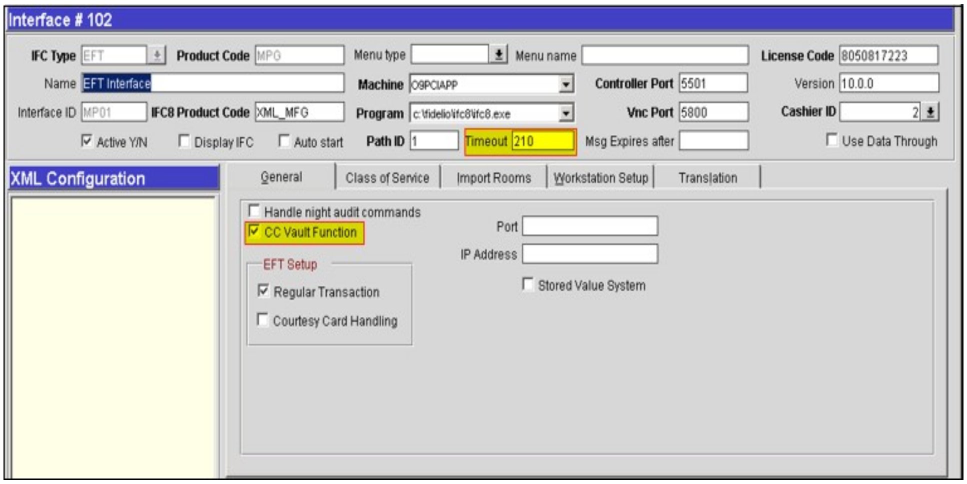


IFC Web Configuration - New

IFC Type: EFT
Name: Oracle Payment Interface
Product Code: OPI
Machine: JKRUMENA-US
License Code: 987654
IFC8 Prod Cd: XML_OPI
□ Generate XML

Communication
● TCP/IP ○ Serial
IP:
Port:

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

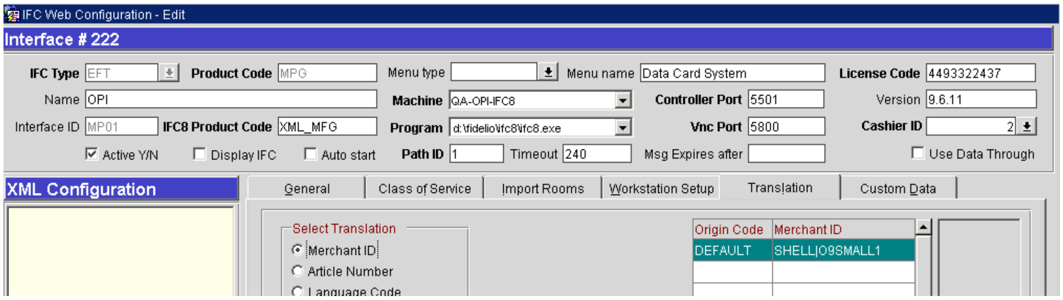


Interface # 102

IFC Type EFT
Product Code MPG
Menu type
Menu name
License Code 8050817223
Name EFT Interface
Machine O9PCIAPP
Controller Port 5501
Version 10.0.0
Interface ID MP01
IFC8 Product Code XML_MFG
Program c:\fidelio\ifc8\ifc8.exe
Vnc Port 5800
Cashier ID 2
☑ Active Y/N
☐ Display IFC
☐ Auto start
Path ID 1
Timeout 210
Msg Expires after
☐ Use Data Through

☐ Handle night audit commands
☑ CC Vault Function
Port
IP Address
EFT Setup
☑ Regular Transaction
☐ Courtesy Card Handling
☐ Stored Value System

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



IFC Web Configuration - Edit

Interface # 222

IFC Type EFT
Product Code MPG
Menu type
Menu name Data Card System
License Code 4493322437
Name OPI
Machine QA-OPI-IFC8
Controller Port 5501
Version 9.6.11
Interface ID MP01
IFC8 Product Code XML_MFG
Program d:\fidelio\ifc8\ifc8.exe
Vnc Port 5800
Cashier ID 2
☑ Active Y/N
☐ Display IFC
☐ Auto start
Path ID 1
Timeout 240
Msg Expires after
☐ Use Data Through

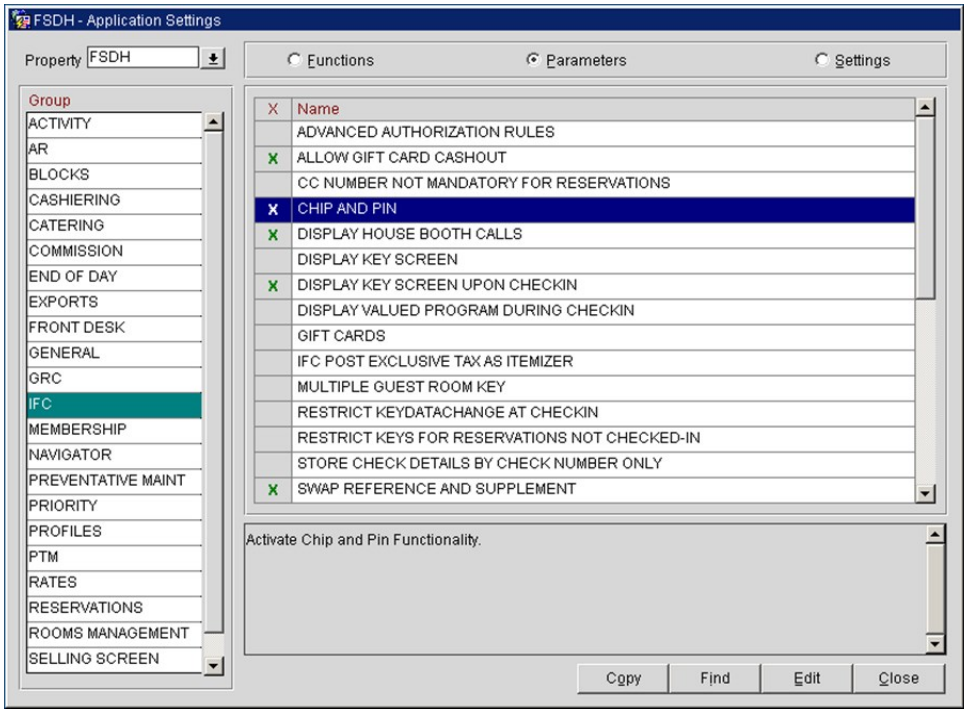
Select Translation
● Merchant ID
○ Article Number
○ Language Code

Origin Code	Merchant ID
DEFAULT	SHELL|O9SMALL1

Configuring CHIP AND PIN (EMV)

To configure the Functionality Setup:

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



Property FSDH

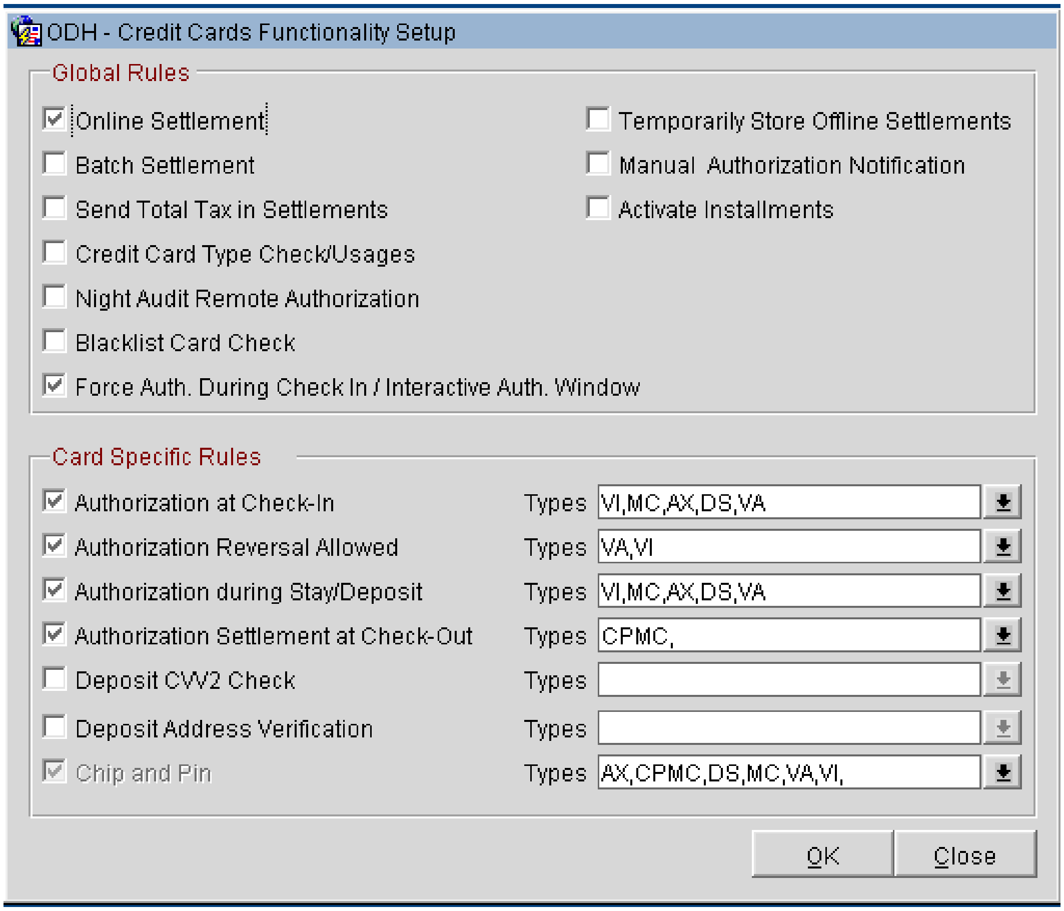
Group

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.

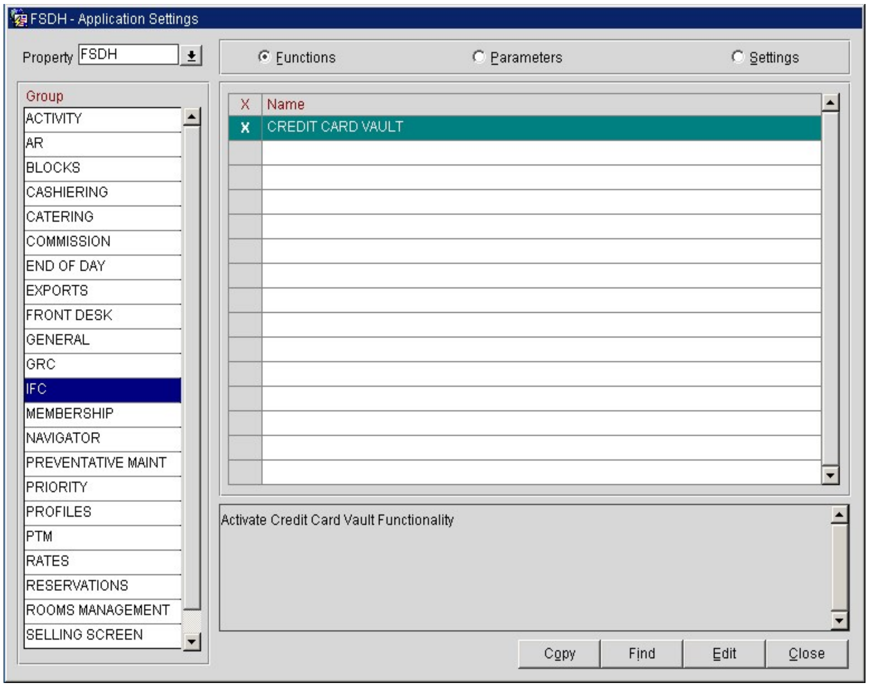
- **Authorization During Stay/Deposit.** Select the payment methods that allow manual and automatic authorizations following check-in and prior to check-out and settlement. This option must be enabled in order to allow authorizations by the end-of-day routine.

- **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

X	Name
X	CREDIT CARD VAULT

Activate Credit Card Vault Functionality

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

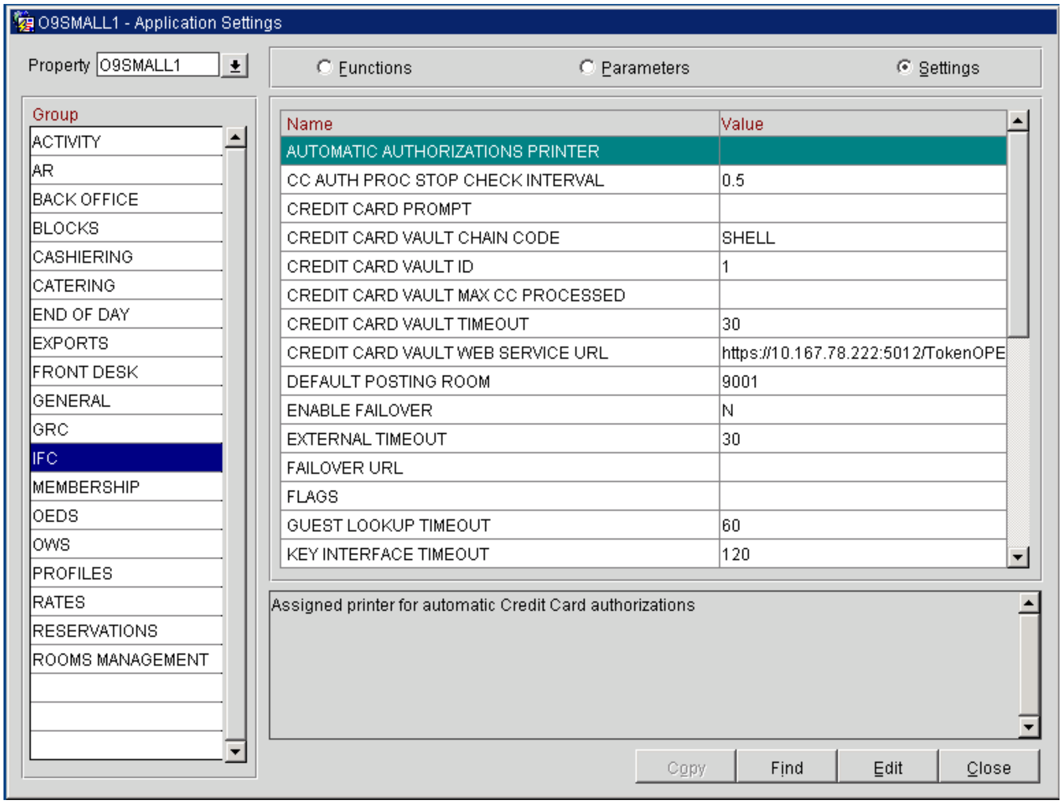
OPERA uses the CREDIT CARD VAULT CHAIN CODE for the certificate lookup and should be populated with what was entered during the OPI configuration for PMS. The CREDIT CARD VAULT WEB SERVICE URL should be in the format:

https://<ipaddress_opi_host>:5012/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 O9SMALL1

○ Functions ○ Parameters ● Settings

Group

- ACTIVITY
- AR
- BACK OFFICE
- BLOCKS
- CASHIERING
- CATERING
- END OF DAY
- EXPORTS
- FRONT DESK
- GENERAL
- GRC
- IFC
- MEMBERSHIP
- OEDS
- OWS
- PROFILES
- RATES
- RESERVATIONS
- ROOMS MANAGEMENT

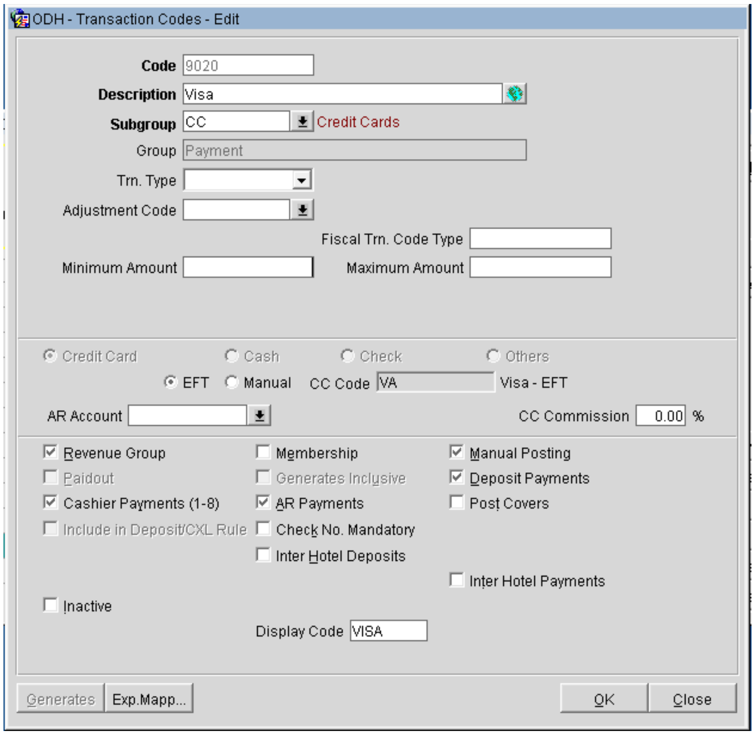
Name	Value
AUTOMATIC AUTHORIZATIONS PRINTER	
CC AUTH PROC STOP CHECK INTERVAL	0.5
CREDIT CARD PROMPT	
CREDIT CARD VAULT CHAIN CODE	SHELL
CREDIT CARD VAULT ID	1
CREDIT CARD VAULT MAX CC PROCESSED	
CREDIT CARD VAULT TIMEOUT	30
CREDIT CARD VAULT WEB SERVICE URL	https://10.167.78.222:5012/TokenOPE
DEFAULT POSTING ROOM	9001
ENABLE FAILOVER	N
EXTERNAL TIMEOUT	30
FAILOVER URL	
FLAGS	
GUEST LOOKUP TIMEOUT	60
KEY INTERFACE TIMEOUT	120

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

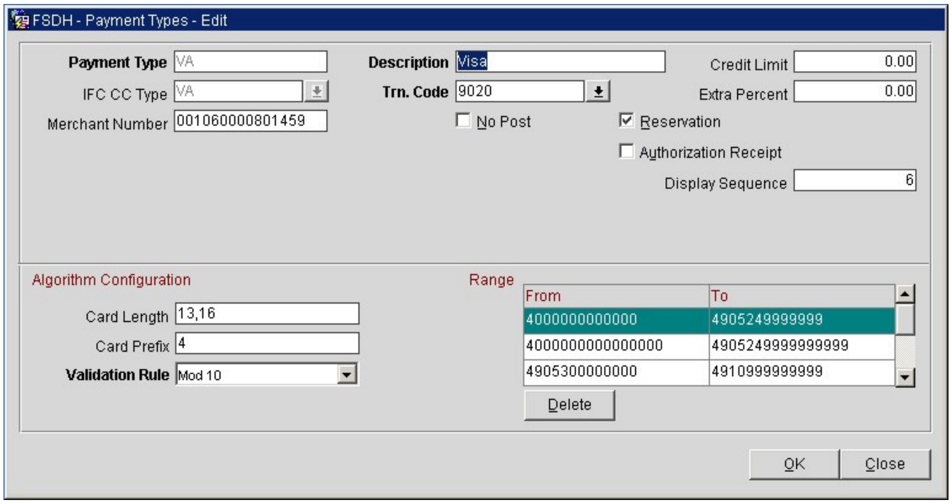
Display Code VISA

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 **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

IFC CC Type VA

Merchant Number 001060000801459

Description Visa

Trn. Code 9020

☐ No Post

Credit Limit 0.00

Extra Percent 0.00

☑ Reservation

☐ Authorization Receipt

Display Sequence 6

Algorithm Configuration

Card Length 13,16

Card Prefix 4

Validation Rule Mod 10

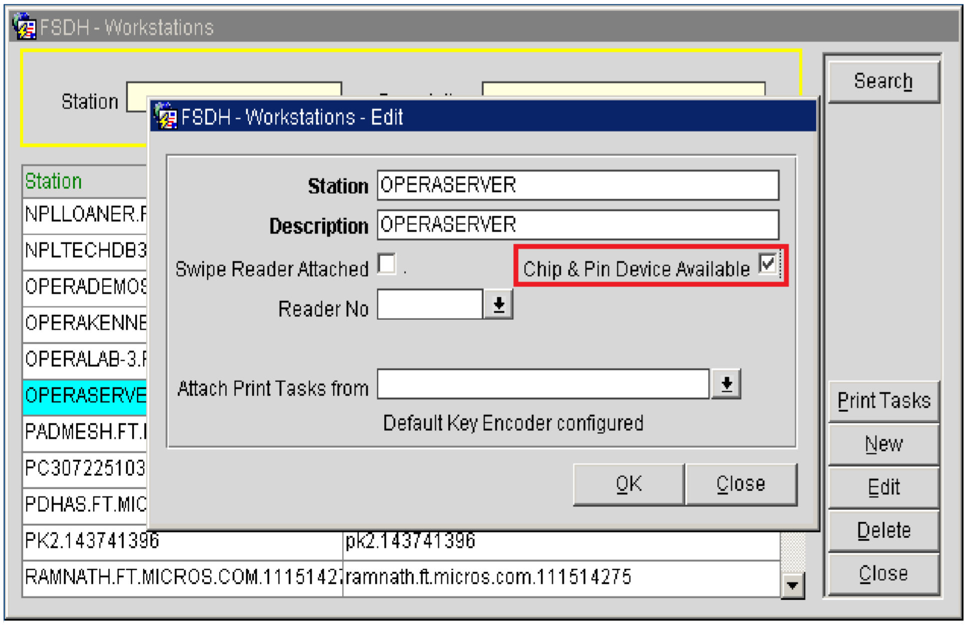
Range

From	To
4000000000000	4905249999999
4000000000000000	4905249999999999
4905300000000	4910999999999

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 selected.
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).



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

Station OPERASERVER

Description OPERASERVER

Swipe Reader Attached □

Chip & Pin Device Available ☑

Reader No

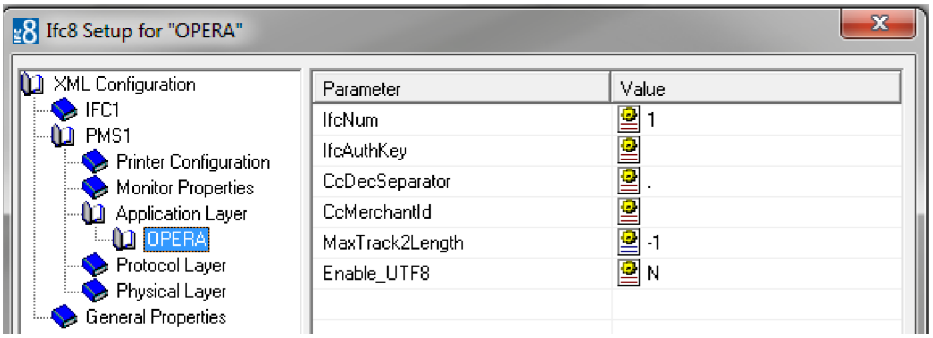
Attach Print Tasks from

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:

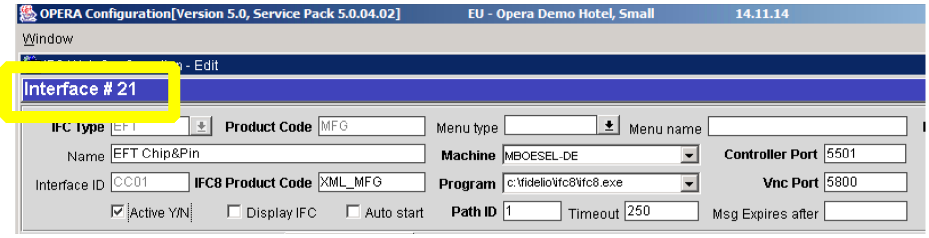
1. In the **Hotel Property Interface**, go to the **PMS1** tree and select **OPERA** in the application layer.
2. Enter the **OPERA IFC** number in the parameter **IfcNum** value.



Ifc8 Setup for "OPERA"

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

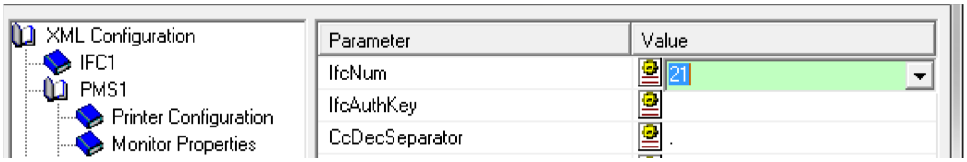
Interface # 21

IFC Type EFT | Product Code MFG | Menu type | Menu name

Name EFT Chip&Pin | Machine MBOESEL-DE | Controller Port 5501

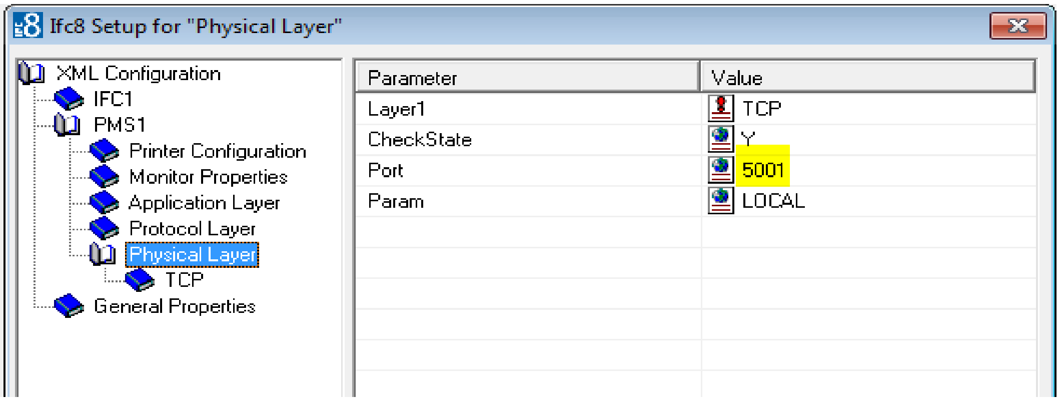
Interface ID CC01 | IFC8 Product Code XML_MFG | Program c:\fidelio\ifc8\ifc8.exe | Vnc Port 5800

☑ 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**.



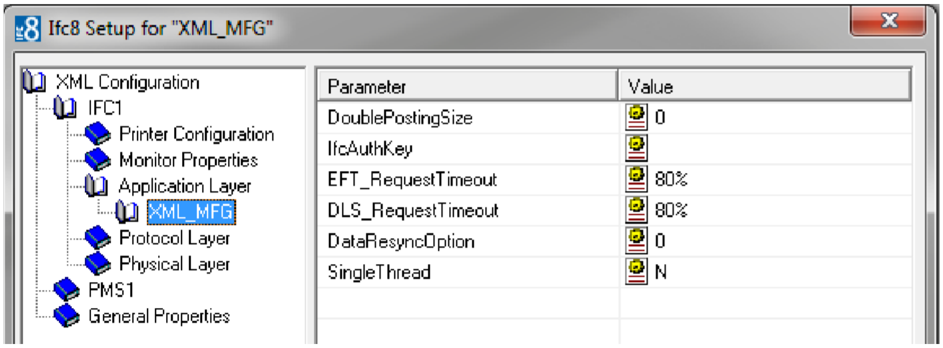
Parameter	Value
Layer1	TCP
CheckState	Y
Port	5001
Param	LOCAL

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.

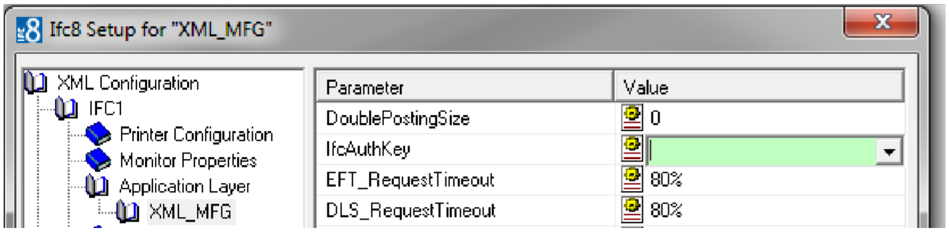
This authentication key must be defined by OPI. The corresponding key must be entered in the Hotel Property Interface (IFC8) configuration.

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

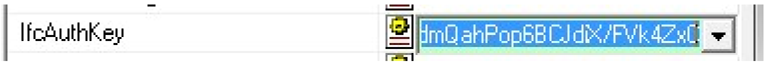


Parameter	Value
DoublePostingSize	0
IfcAuthKey	
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0
SingleThread	N

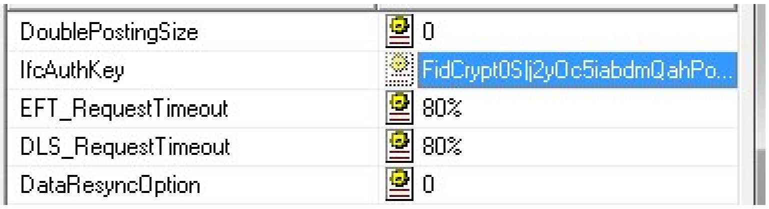
2. Copy the generated key from Configuring OPI - OPERA merchant step 5, and add "FidCrypt0S|" to the generated key as prefix.
   For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxxx
3. Copy this string into IFC8 Parameter **IfcAuthKey** value field.



Parameter	Value
DoublePostingSize	0
IfcAuthKey	
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%

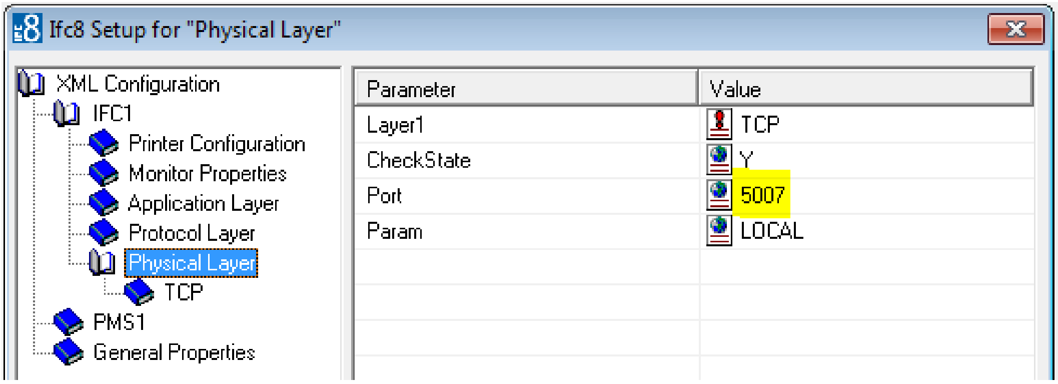


IfcAuthKey	dmQahPop6BCJdiX/FVk4ZxC



DoublePostingSize	0
IfcAuthKey	FidCrypt0S|j2yOc5iabdmQahPo...
EFT_RequestTimeout	80%
DLS_RequestTimeout	80%
DataResyncOption	0

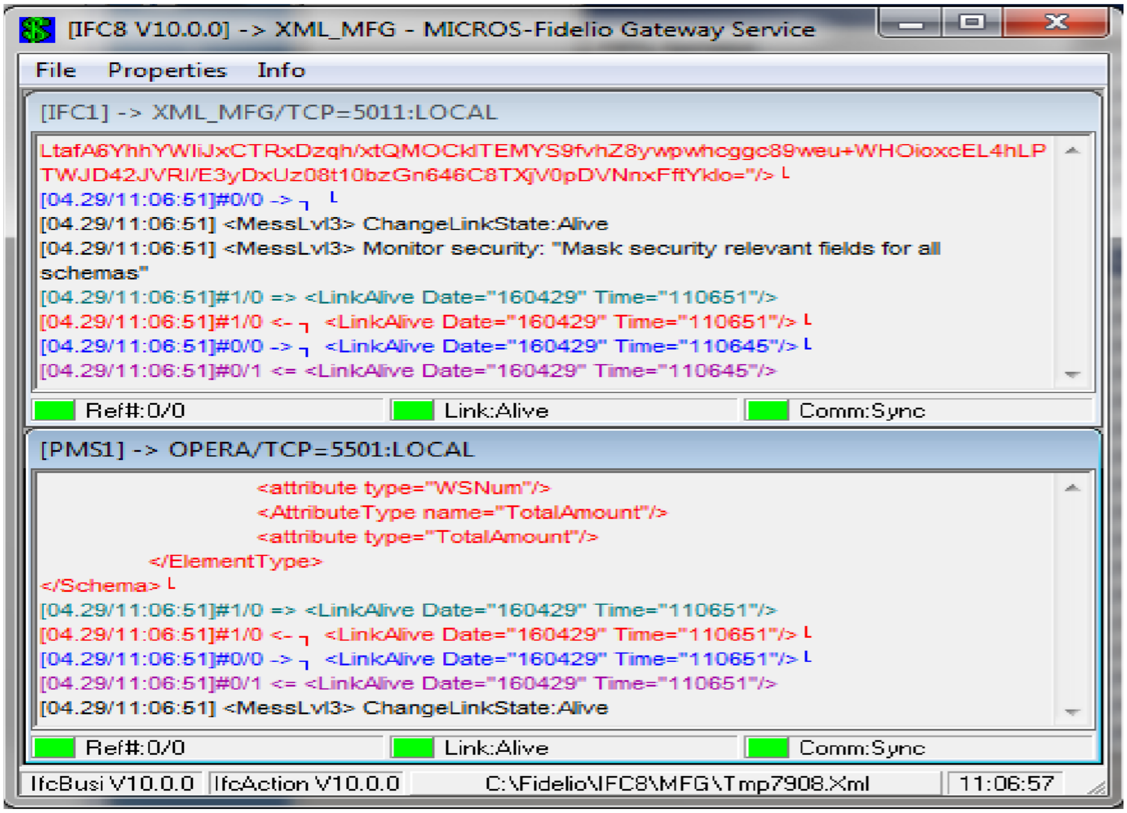
4. Go to **IFC1** tree and select the **Physical Layer**.
5. Enter the port number in port value. This is the same port that was configured in OPI.



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.

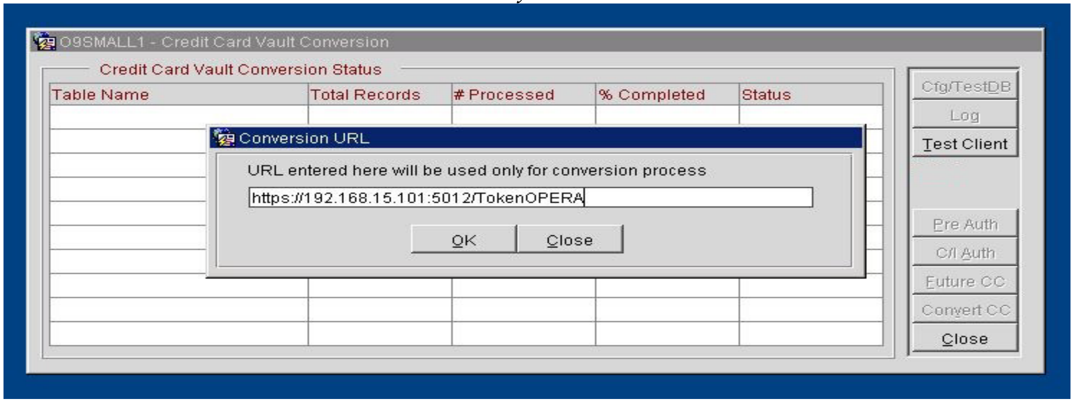
IFC8 now connects with OPI and OPERA IFC Controller.
To verify IFC8 successful status, confirm that all 6 status indicators are green.



```
[IFC1] -> XML_MFG/TCP=5011:LOCAL
LtafA6YhhYWliJxCTRxDzqh/xtQMOCklTEMYS9fvhZ8ywpwhcggc89weu+WHOioxcEL4hLP
TWJD42JVRI/E3yDxUz08t10bzGn646C8TXjV0pDVNnxFftYklo="/> ʟ
[04.29/11:06:51]#0/0 -> ┐ ʟ
[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"/> ʟ
[04.29/11:06:51]#0/0 -> ┐ <LinkAlive Date="160429" Time="110645"/> ʟ
[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> ʟ
[04.29/11:06:51]#1/0 => <LinkAlive Date="160429" Time="110651"/>
[04.29/11:06:51]#1/0 <- ┐ <LinkAlive Date="160429" Time="110651"/> ʟ
[04.29/11:06:51]#0/0 -> ┐ <LinkAlive Date="160429" Time="110651"/> ʟ
[04.29/11:06:51]#0/1 <= <LinkAlive Date="160429" Time="110651"/>
[04.29/11:06:51] <MessLvl3> ChangeLinkState:Alive
Ref#:0/0    Link:Alive    Comm:Sync

IfcBusi V10.0.0 | IfcAction V10.0.0 | C:\Fidelio\IFC8\MFG\Tmp7908.Xml | 11:06:57
```

Perform a Tokenization

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



Credit Card Vault Conversion Status

Table Name	Total Records	# Processed	% Completed	Status

Conversion URL

URL entered here will be used only for conversion process

https://192.168.15.101:5012/TokenOPERA

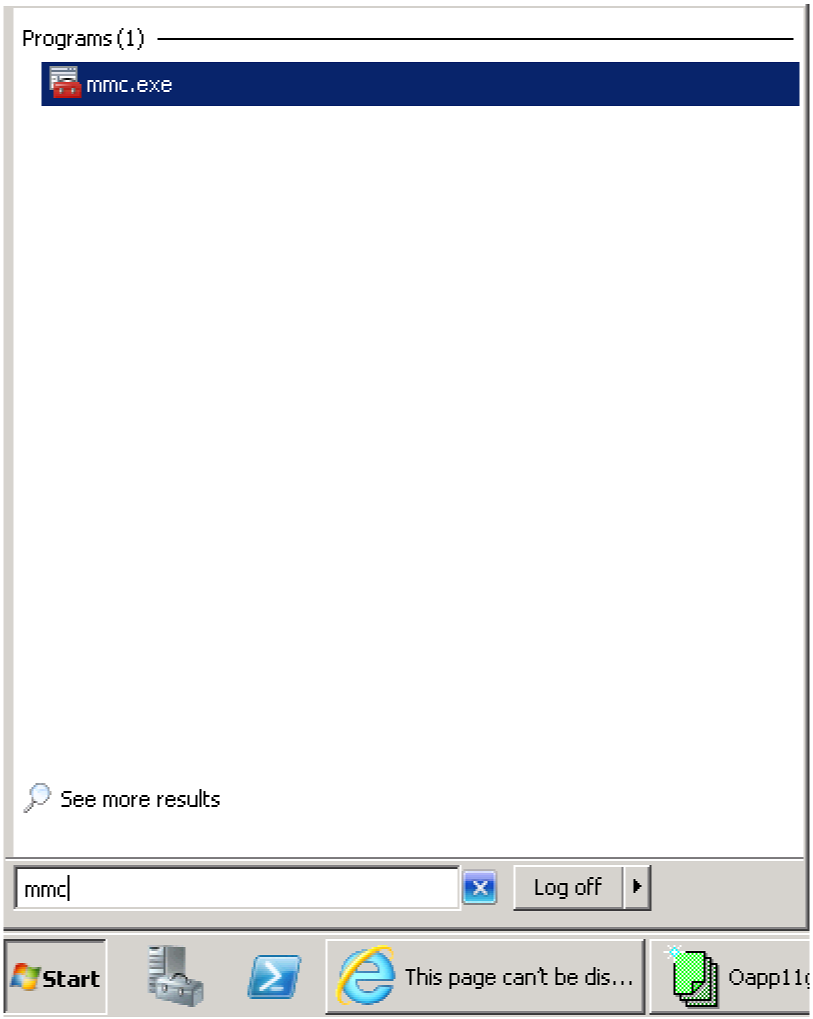
OK | Close

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

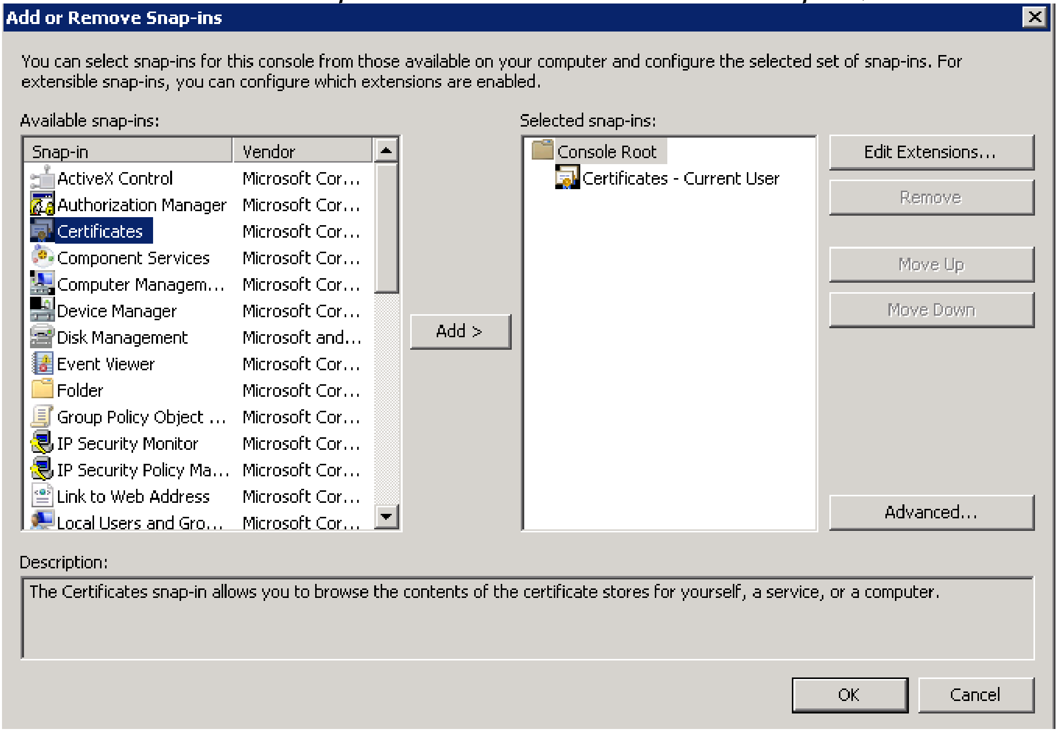
OPI only supports the **Convert CC** function; the other conversion options are not currently supported.

Certificate Import using Microsoft Management Console

1 Find and open mmc.exe from start menu



2 Select *File* > *Add/remove snap in* and add certificates to *Selected snap-ins,* select *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...

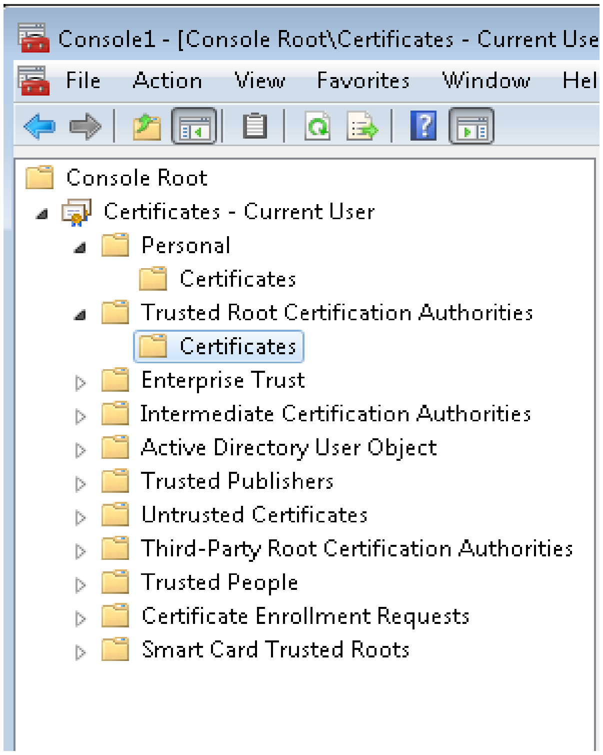
Selected snap-ins:

- 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.

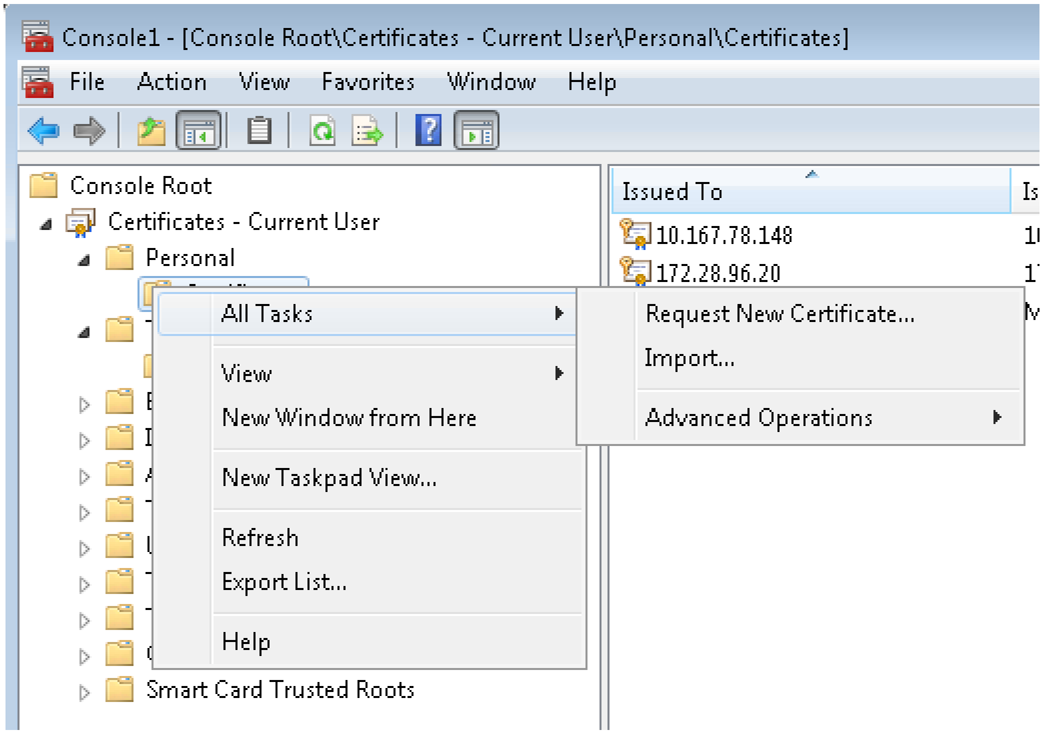
3 Expand *Certificates*, expand *Personal* or *Trusted Root* as required, and select *Certificates*.



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*, select *Import*.



- On the ***Certificate Import Wizard Welcome** page*, click ***Next***.

- Browse to the location of the certificate file, and then click ***Next***.

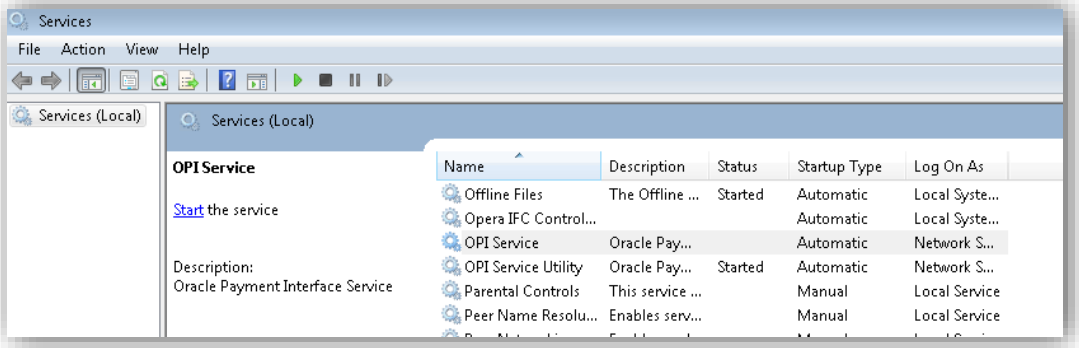
- If required enter the password relevant to the certificate you are importing, and then click ***Next***.

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

5 OPI Maintenance & FAQ

OPI Services

Once installation is complete, there will be 2 OPI Services present.



OPI Service

Start the service

Description:
Oracle Payment Interface Service

Name	Description	Status	Startup Type	Log On As
Offline Files	The Offline ...	Started	Automatic	Local Syste...
Opera IFC Control...			Automatic	Local Syste...
OPI Service	Oracle Pay...		Automatic	Network S...
OPI Service Utility	Oracle Pay...	Started	Automatic	Network S...
Parental Controls	This service ...		Manual	Local Service
Peer Name Resolu...	Enables serv...		Manual	Local Service

OPI Service

The OPI Service deals with communication between the PSP and Opera.
The OPI Service will need to be restarted each time any configuration changes are made to the Oracle Payment Interface.

OPI Service Utility

The OPI Service Utility handles communication between the OPI configuration tools and the MySQL database.
If you are having trouble logging into the configuration wizards, make sure this is running.

OPI Uninstallation / Re-installation

If you are uninstalling OPI with the intention of reinstalling it again, be sure to remove the :\ProgramData\MySQL\ folder manually, as the uninstall of MySQL does not remove this automatically. If the folder is left the old schema information will cause challenges during the re-install.
NOTE: The :\ProgramData\ folder is usually a hidden folder by default.

OPI Additional Configuration

The majority of configuration can now be completed using the configuration wizard. The configuration wizard should be used wherever possible to ensure configuration is completed to the same standard.
There will however be instances, where certain configurations are not dealt with yet by the configuration wizard, and the Config.exe must be used as it has been in the past.

OPI Log Files

OPI Logs are found at the following path :\OraclePaymentInterface\Log\

- Debug log

Is rotated by file size, the maximum size is 20MB.

Current debug log file name is “debug.log”, previous debug log file name is “debug.log.1”, “debug.log.X”, sort by date.

- Gateway.log

Is rotated by file size, the maximum size is 20MB

- System.log

Check the Oracle Payment Interface build number.

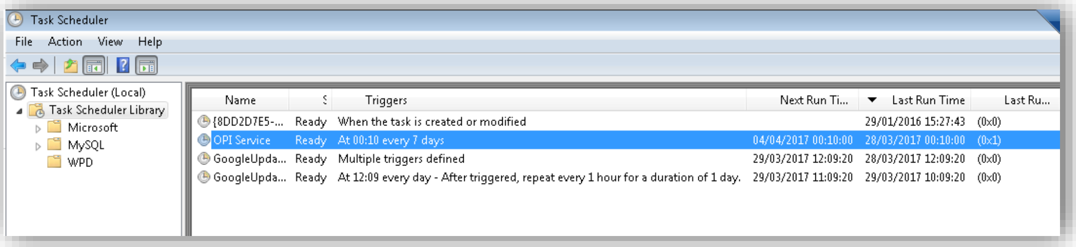
Is rotated by file size, the maximum size is 20MB

- Transaction log

Is rotated daily, the current transaction log file name is “transaction.log”, and previous day transaction log file name is “transaction.log.YYYY-MM-DD”.

OPI Service Restart Task

If the details of service restart need to be amended once OPI is installed, these can be changed using Windows Task Scheduler.
The OPI installer creates an ***OPI Service*** task.



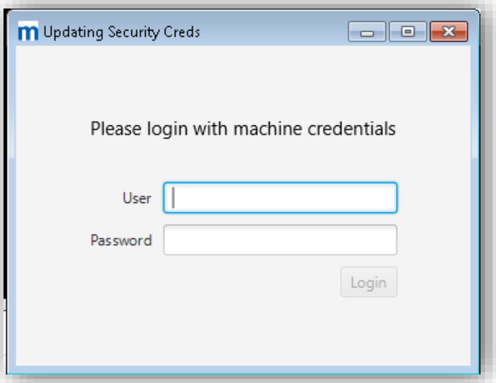
Name	S	Triggers	Next Run Ti...	Last Run Time	Last Ru...
{8DD2D7E5-...	Ready	When the task is created or modified		29/01/2016 15:27:43	(0x0)
OPI Service	Ready	At 00:10 every 7 days	04/04/2017 00:10:00	28/03/2017 00:10:00	(0x1)
GoogleUpda...	Ready	Multiple triggers defined	29/03/2017 12:09:20	28/03/2017 12:09:20	(0x0)
GoogleUpda...	Ready	At 12:09 every day - After triggered, repeat every 1 hour for a duration of 1 day.	29/03/2017 11:09:20	29/03/2017 10:09:20	(0x0)

OPI Password Maintenance

The passwords for the OPI database and the Native Driver Pass Phrase are set during installation.

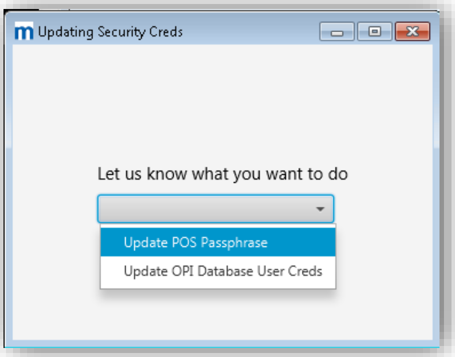
If the passwords for the OPI database, or the Native Driver Pass Phrase, need to be updated once OPI is already installed the :\OraclePaymentInterface\Bin\rwregistry.exe utility can be used to update these within the OPI configuration.
Note: The rwregistry utility does not change the MySQL password within MySQL, this would normally be done by the System Administrator on site.

- Run :\OraclePaymentInterface\bin\rwregistry.exe as Administrator, and Login with local Administrator user credentials.

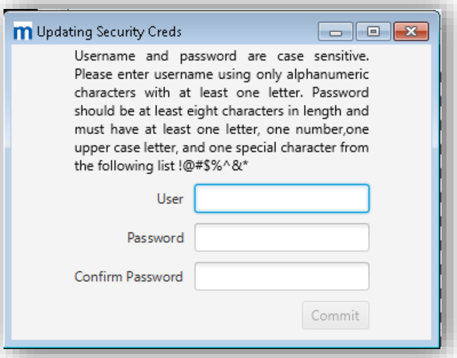


Please login with machine credentials

- Select the required function. Enter the updated credentials you want to set in the OPI configuration. Commit



Let us know what you want to do

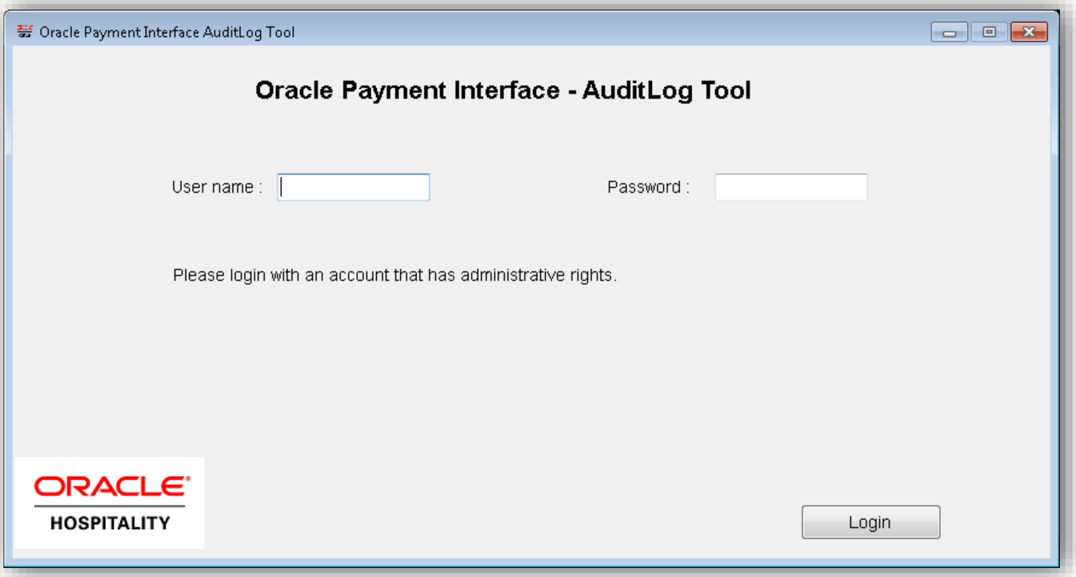


Username and password are case sensitive. Please enter username using only alphanumeric characters with at least one letter. Password should be at least eight characters in length and must have at least one letter, one number,one upper case letter, and one special character from the following list !@#$%^&*

OPI Configuration Logs

Logs of any configuration changes are no longer written to the log files at :\OraclePaymentInterface\log\configAudit\
Instead this data is now stored in the OPI MySQL database. A utility now exists to access these logs, and administrator login is now required to view them.

- Run :\OraclePaymentInterface\bin\AuditLogTool.exe



Oracle Payment Interface AuditLog Tool

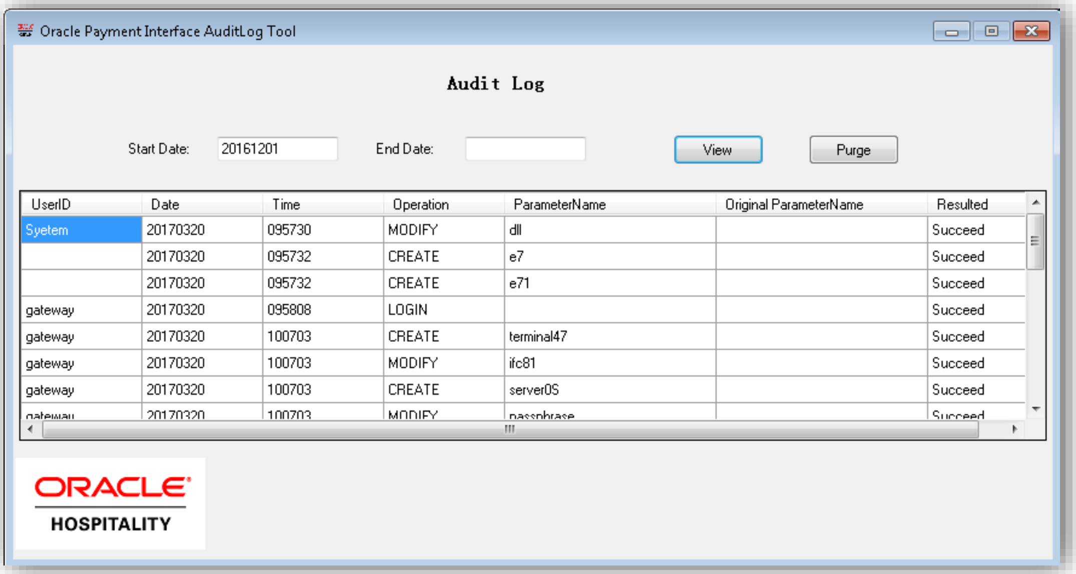
Oracle Payment Interface - AuditLog Tool

User name :

Password :

Please login with an account that has administrative rights.

- Select the date range required, and select View to see the required logs;



Oracle Payment Interface AuditLog Tool

Audit Log

Start Date: 20161201

End Date:

UserID	Date	Time	Operation	ParameterName	Original ParameterName	Resulted
Syetem	20170320	095730	MODIFY	dll		Succeed
	20170320	095732	CREATE	e7		Succeed
	20170320	095732	CREATE	e71		Succeed
gateway	20170320	095808	LOGIN			Succeed
gateway	20170320	100703	CREATE	terminal47		Succeed
gateway	20170320	100703	MODIFY	ifc81		Succeed
gateway	20170320	100703	CREATE	server0S		Succeed
gateway	20170320	100703	MODIFY	passphrase		Succeed