Oracle® Hospitality Product Name

OPERA Reservation System (ORS) OPI Installation Guide

Release 20.2
November 2020

Oracle Hospitality Product Name OPERA Reservation System (ORS) OPI Installation Guide Release 20.2

Contents

Contents 3

Preface 4

1 Pre-Installation Steps 1-1

2 ORS Assessment for OPI-OPERA 2-1

3 ORS-OPI Considerations 3-1

4 ORS-OPI Communication Flow Diagram**Error! Bookmark not defined.**

5 Installing the OPI 5-1

6 OPERA (ORS) Configuration 6-1

Creating an EFT Interface 6-1
Configuring CHIP AND PIN (EMV) 6-5
Configuring the CC Vault - Settings as per property 6-7
Cashiering Overview 6-8
Overview of Credit Card Payment Types 6-9
Credit Card Type Payment Setup Information 6-10
Configuring the Workstation 6-16
Configuring the Hotel Property Interface (IFC8) -Instance to the OPERA Hotel Property Interface (IFC) 6-16
Perform a Tokenization 6-16

7 Certificates 7-1

Preface

Purpose

This document describes how to organize environments for an installation of the Oracle Payment Interface (OPI) for ORS On Premise Token Exchange Service.

Audience

This document is intended to cover the additional steps required to setup OPI-ORS 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
- Screen shots of each step you take

Documentation

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

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

Table 1 Revision History

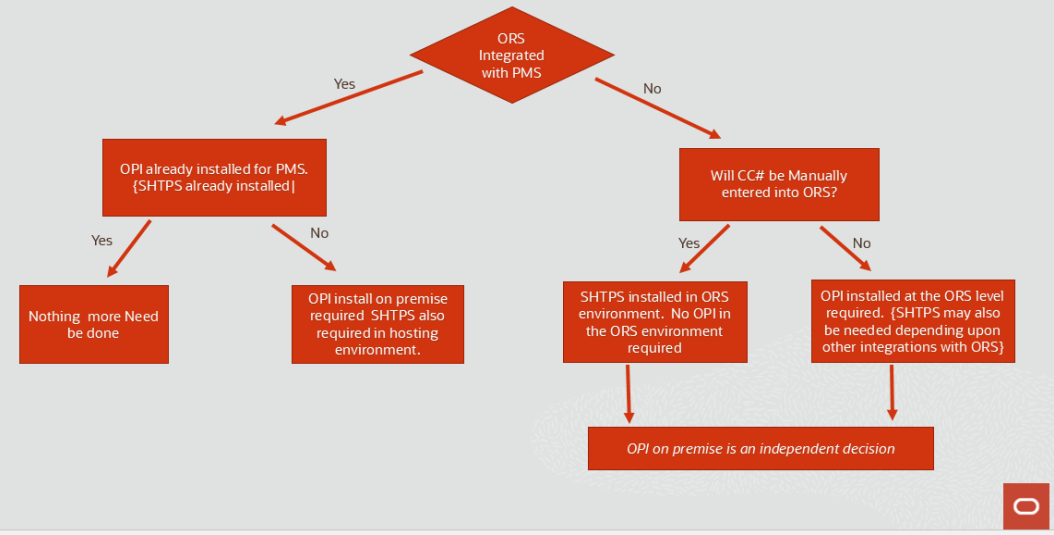
Date	Description
Aug 2020	• Initial Publication

1
Pre-Installation Steps

Follow this link for Minimum Opera Software & Hardware requirements for OPI and TPS
https://docs.oracle.com/en/industries/hospitality/integration_platforms.html

2
ORS Assessment for OPI-OPERA

Figure 2-1 - ORS OPI Flow Chart



3
ORS-OPI Considerations

Subject	Details
Installed Components	This depends on the data entry method chosen. If the customer will ONLY input credit card data into ORS to initiate the token request, then only the Token Proxy Server is required to be installed. However if the customer prefers to capture the data via an external payment terminal, a complete OPI installation is required in the ORS environment
OPI Server	OPI needs to be installed above property in the ORS environment (not on premise). Current OPI versions would require an OPI instance per resort (OPI can be supported in a virtual environment which would make it easier to deploy multiple instances). However with the next release of OPI (future version), support for multiple resorts within one OPI instance is targeted to become available at which point only one OPI instance at the ORS level should be required.
Tokenization	Since OPI is installed per resort, tokenization of the data at rest would be run one resort at a time. Multiple resorts can be also selected if desired tokenized at the same time.
Bulk tokenization	This function works the same as at the PMS level. Operationally there are a few things which do not apply. Since there are no financial transactions stored in ORS, there is nothing to settle at the ORS level. All the financial transactions for a reservation are processed at the PMS level.

Subject	Details
EMV vs. Encrypted Swipes	OPERA does not support the encrypted swipes with the OPI payment platform. If the goal is to collect credit card data via an external device, there will need to be an OPI environment installed at the ORS level. FP will need to configure their client software and payment terminals for the ORS clients. Operationally, when the agent opens the widget in ORS while taking the reservation, the agent will click ok without entering any data. This will trigger a token request through OPI to FP which lights up the pin pad for data entry. In order for one OPI instance to support the multiple resorts within ORS we would want to wait until OPI future versions are available so that we could support multiple resorts within one OPI installation

4

ORS-OPI Communication Flow Diagrams

Figure 4-1 ORS Multiple Property (ORS has Separate Database from PMS)

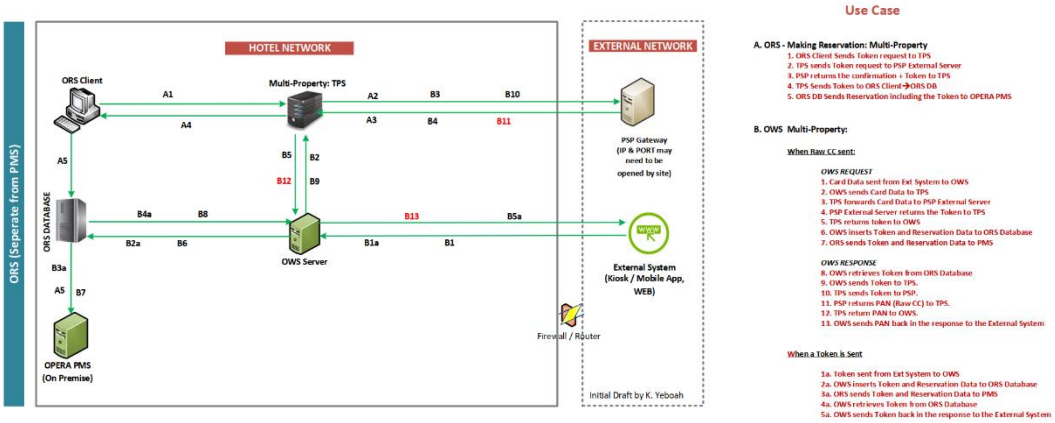


Figure 4-2 Single Property (ORS & PMS Share Database)

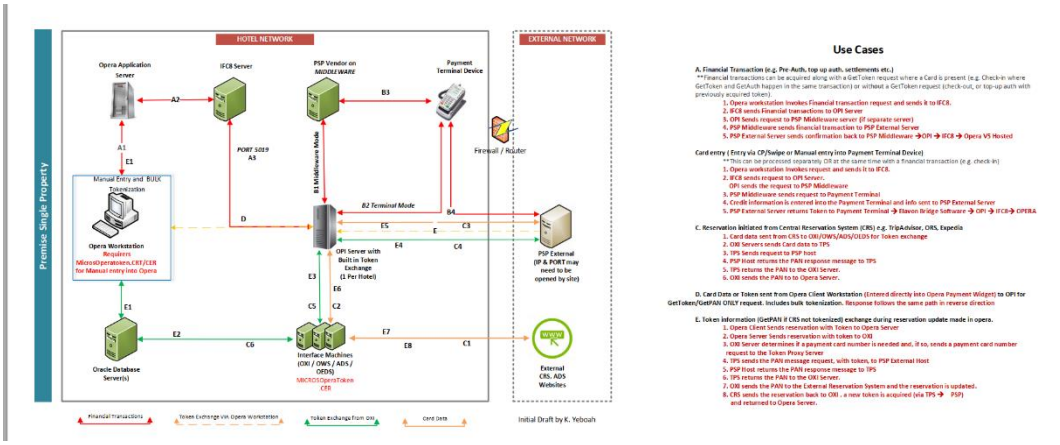
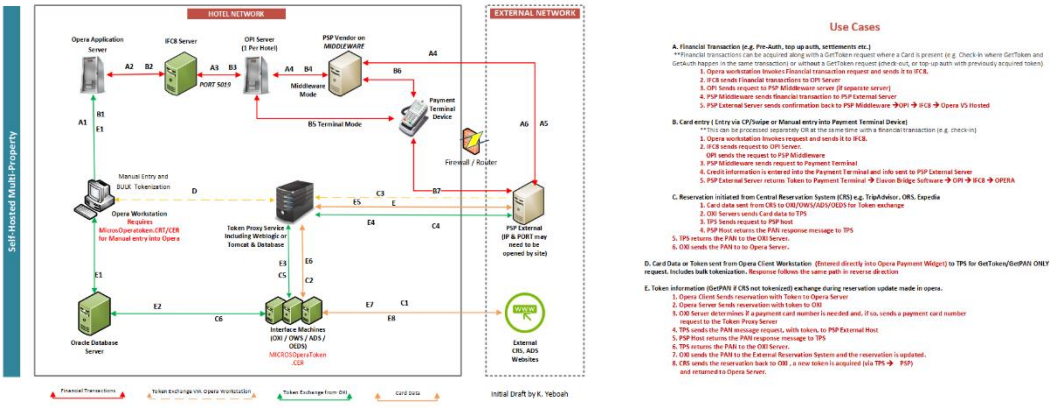


Figure 4-3 Self Hosted Multi-Property (ORS & PMS Share Database)



5
Installing the OPI

> **NOTE:**
>
> OPI deployment for ORS, requires Token Proxy Service to be installed as ONLY GetToken transactions will be performed. CHIP&PIN setup is NOT required unless a Payment Terminal Device (PinPad Device) will be used for entry of credit card data into ORS.

Please refer the Oracle Documentation Website locations for the latest Oracle payment Interface & Self Hosted Token Proxy installation document:

6

OPERA (ORS) Configuration

Creating an EFT Interface

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

Each time you need to configure a property specific setting (transaction code, payment methods etc.) this is at the property level and the Specific Property needs to be selected

Figure 6-1 Interface Status Find Property

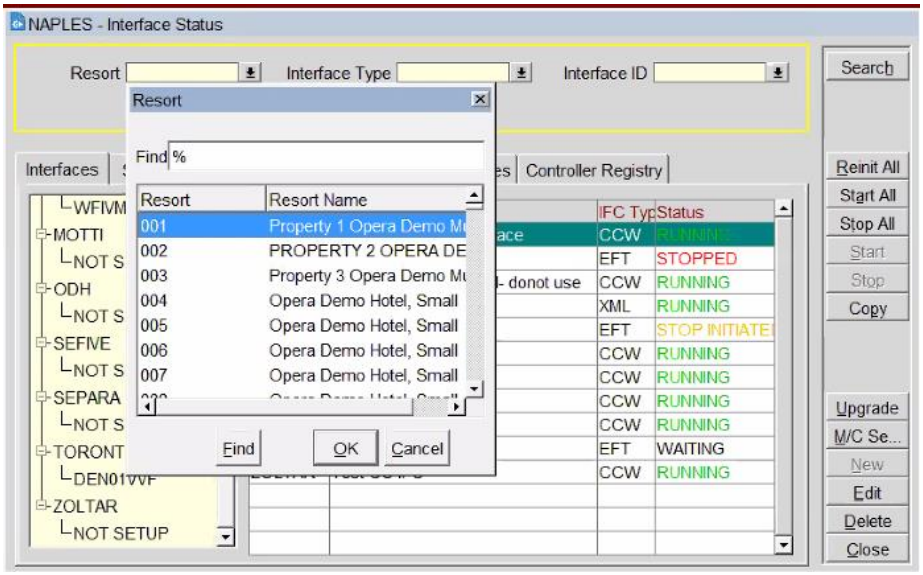


Figure 6-2 Interface Status

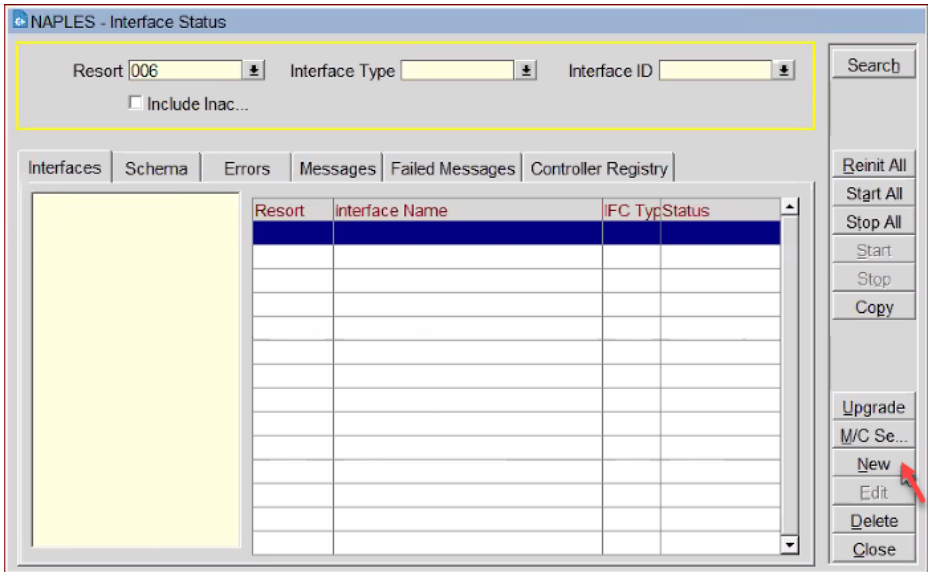
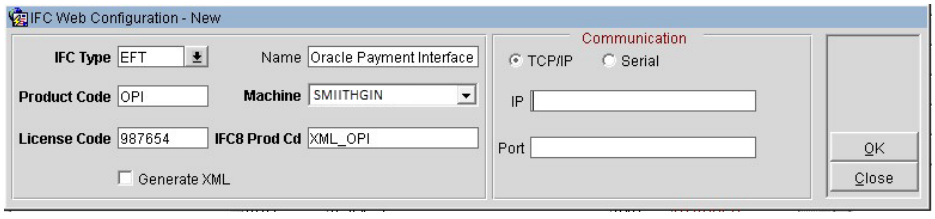


Figure 6-3 IFC Web Configuration



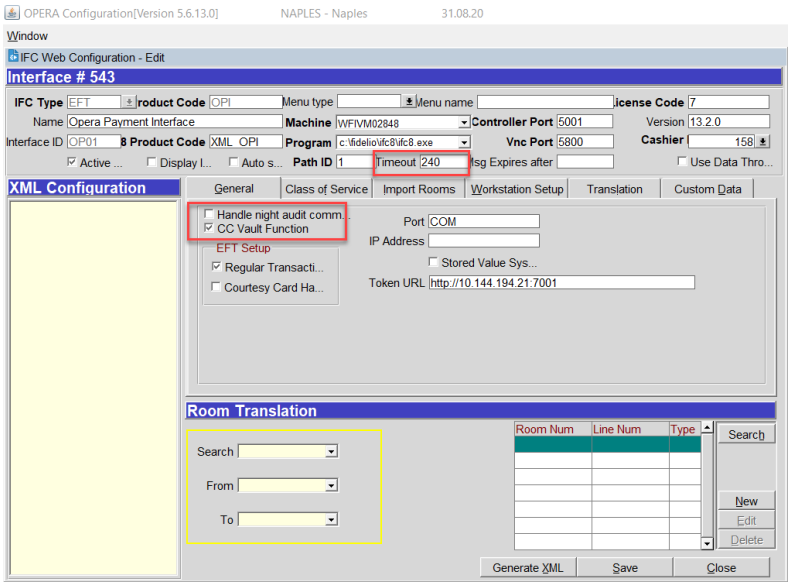
3. Enter the following options, and then click **OK**:

   - **IFC Type**: EFT
   - **Name**: Oracle Payment Interface for ORS

- **Product Code**: OPI
- **Machine**: Select the machine
- **License Code**: License code for interface
- **IFC8 Prod Cd**: XML_OPI

4. On the configuration screen below, select the following:

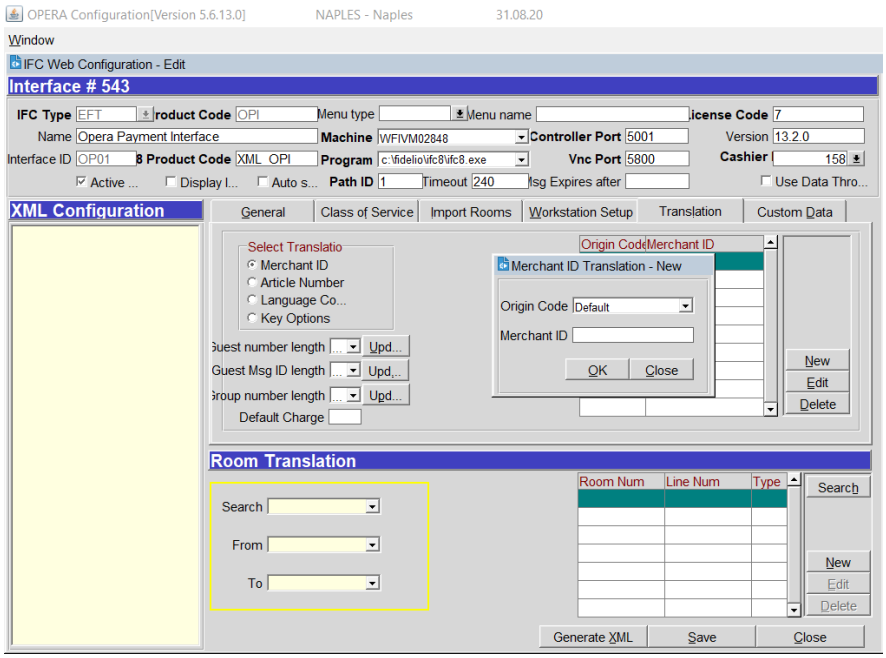
Figure 6-4 IFC Web Configuration Edit



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

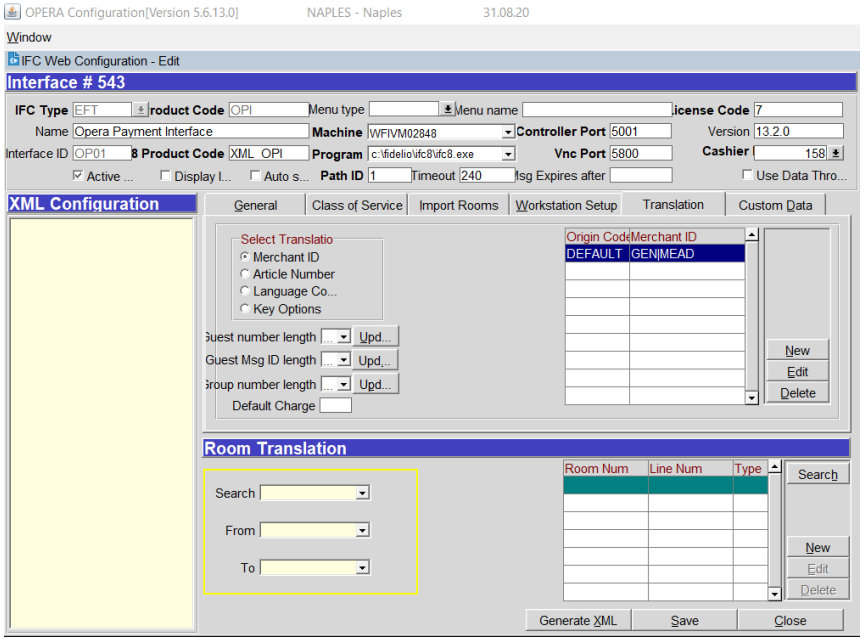
5. Select the **Translation** tab, and then click **Merchant ID**.

Figure 6-5 IFC Web Configuration Edit – Merchant ID Translation



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

Figure 6-6 IFC Web Configuration Edit - Room Translation



Configuring CHIP AND PIN (EMV)

NOTE:

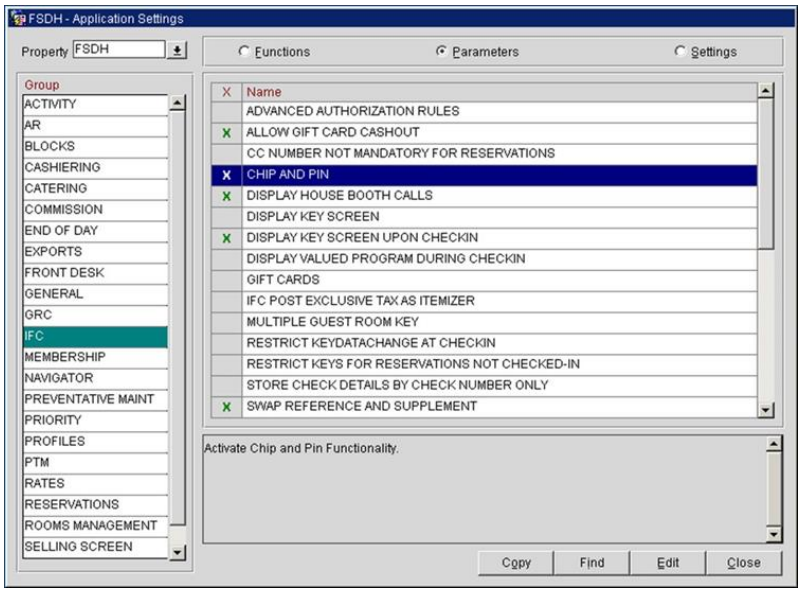
For OPI deployment for ORS, an Chip&Pin setup is ONLY required if a Payment Terminal Device (PinPad Device) will be used for entry of credit card data into ORS.

If ALL entry will be performed directly into ORS and not using a Payment Terminal Device, all that is required to be setup is the Configuration within the ORS with a direct URL link to the Token Proxy Service (TPS).

Configuring the Functionality Setup:

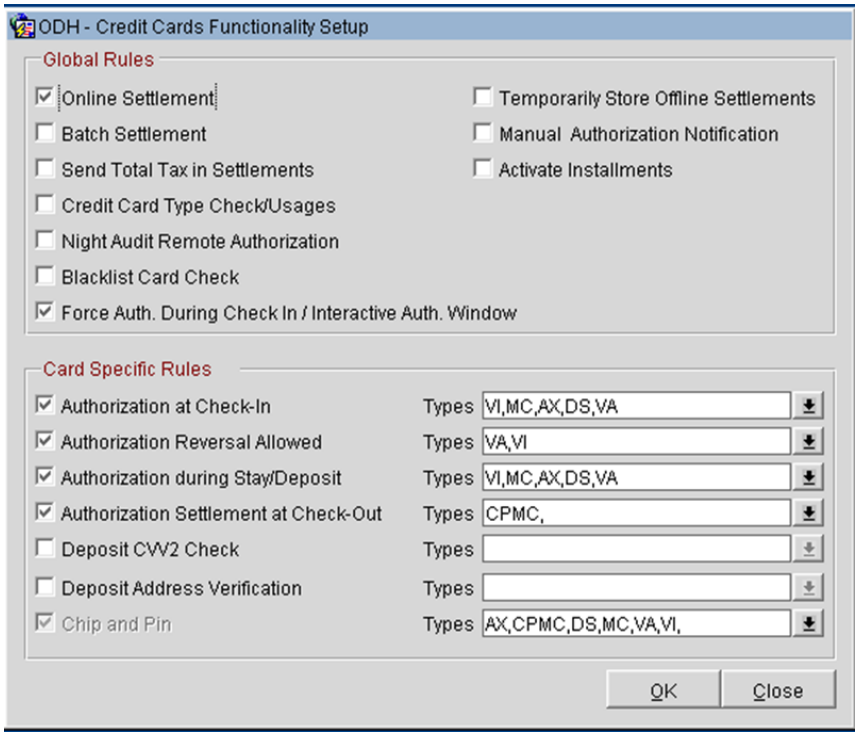
1. Go to **Setup** | **Application Settings** | **IFC Group | Parameters**, and enable **CHIP AND PIN.**

Figure 6-7 Enable CHIP AND PIN



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

Figure 6-8 Credit Cards Functionality Setup



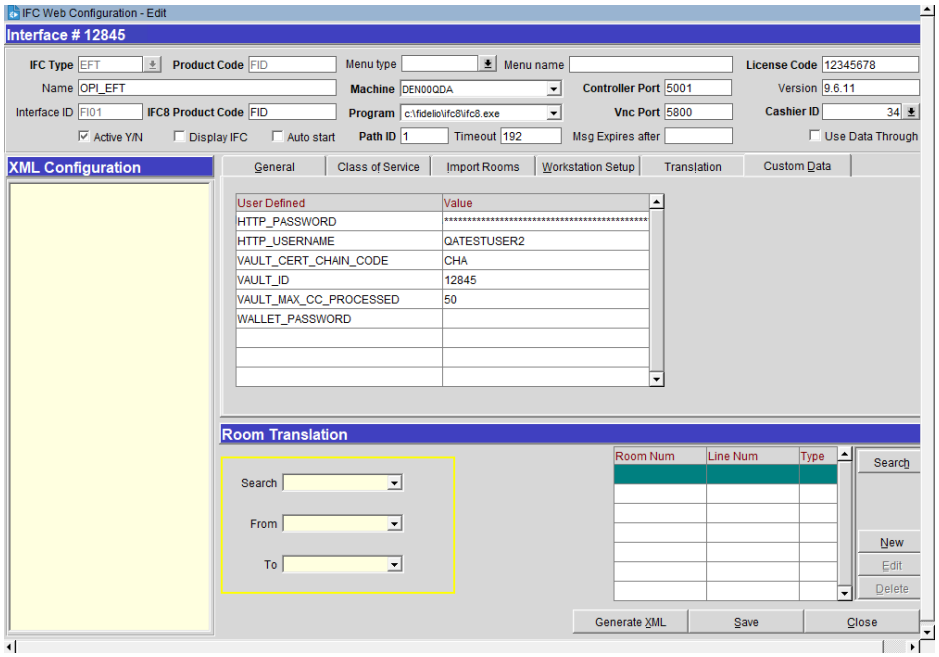
- **Online Settlement**: Select this check box to allow online settlement. OPI is an online settlement. This must be checked to activate the Chip and PIN Application Setting.
- **Authorization at Check-In**: Select the payment methods that will trigger an automatic credit card authorization at check-in.
- **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 - Settings as per property

1. Log into ORS
2. Go to **Configuration** | **Setup** | **Property Interfaces** | **Interface Configuration** | **edit EFT IFC OPI** | **Custom Data tab**.
3. Token URL is accessible from **Configuration | Setup | Property Interfaces | Interface Configuration** | edit **EFT IFC OPI | General**.

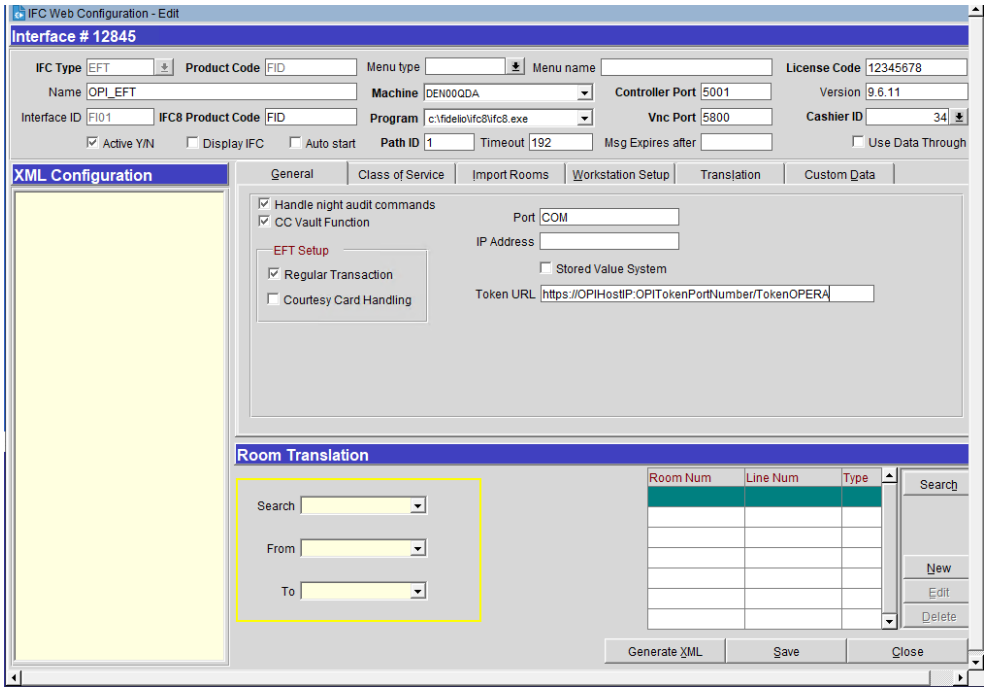
Figure 6-9 IFC Web Configuration Edit



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

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

Figure 6-10 Token URL



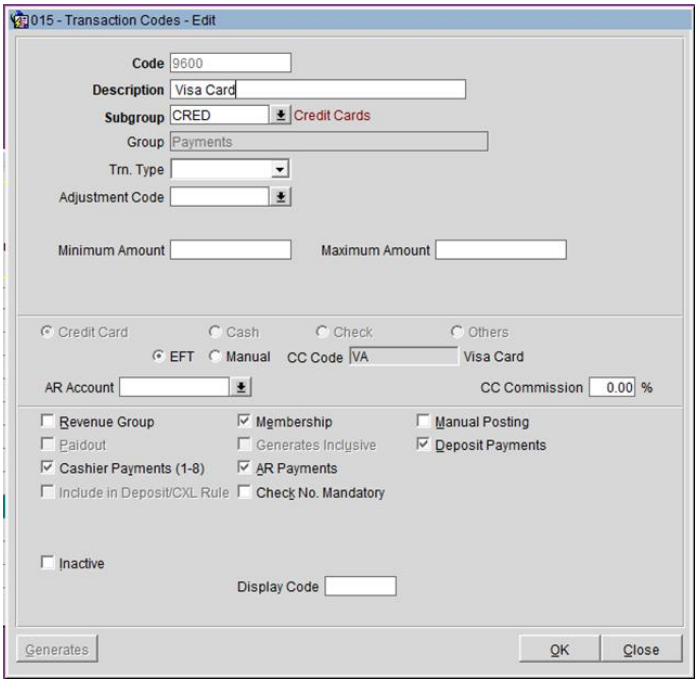
- The CREDIT CARD VAULT ID is currently not used.
- The CREDIT CARD MAX CC PROCESSED is set to what the Payment Partner can support for the number of rows sent in one Token (GetID/GetCC) request. This is used during the bulk tokenization process and when multiple folio windows exist on OPERA Reservations. 50 is the default used when nothing is set here (This is determined by Payment Partner/Vendor; please verify with Partner/Vendor, the number of credit cards that can be processed per batch).
- The CREDIT CARD VAULT TIMEOUT is set to the timeframe to wait for a response from the Token Proxy Service. At least 45 is recommended.

Cashiering Overview

Credit Card Payment Transaction Codes

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

Figure 6-11 Transaction Codes



2. Information for credit card payment transaction codes:

    a. **EFT** selection is necessary to send credit card transactions out to the integrated payment partner for the specific Payment type.

    b. **Manual selection** will not send out any transactions to the integrated payment partner.

    c. **CC Code** will auto-populate once the transaction code is associated to a Payment Type.

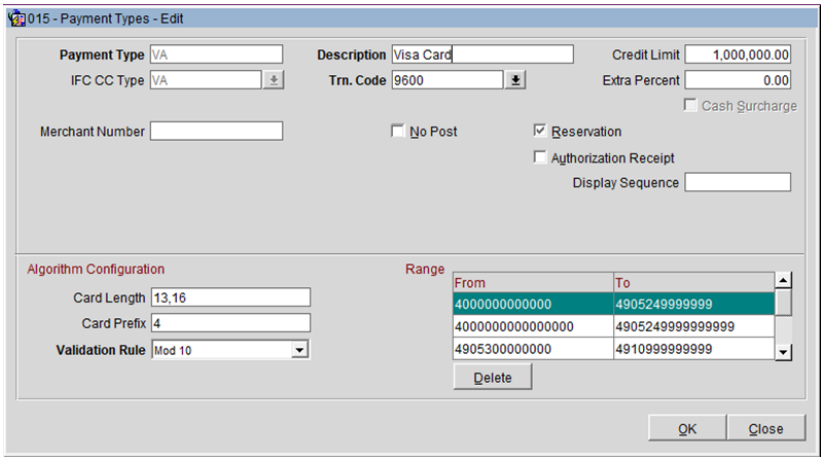
    d. **Display Code** can be populated to display a button when payment screen is accessed in OPERA PMS.

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

Figure 6-12 Payment Types



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.

Payment Types - Customer Present (Chip & PIN)	Description	Capture Method
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.
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)

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

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

Individual Card Functions

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

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

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

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

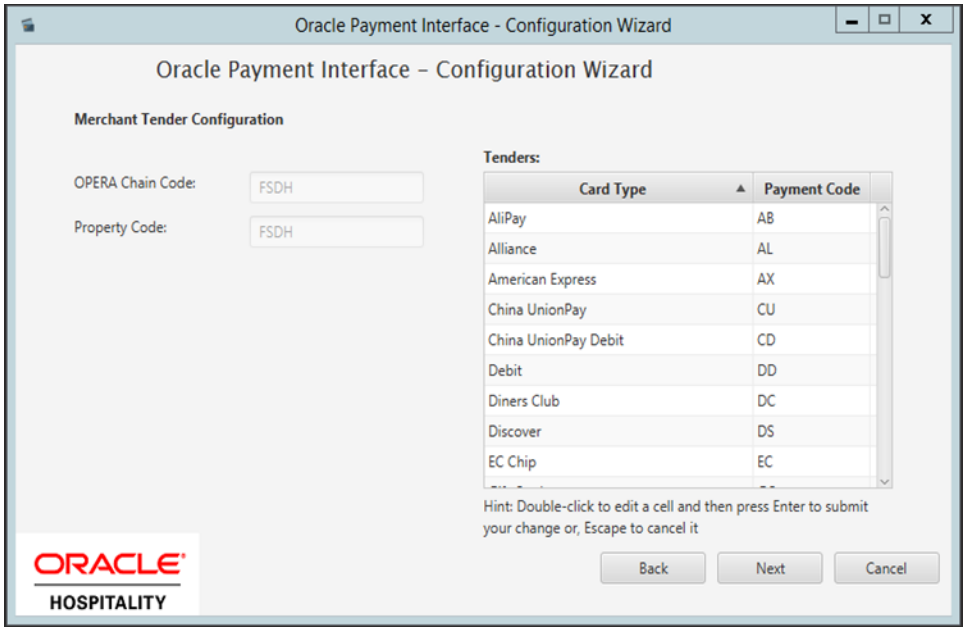
Important Considerations

- Transaction codes for Chip & 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**.

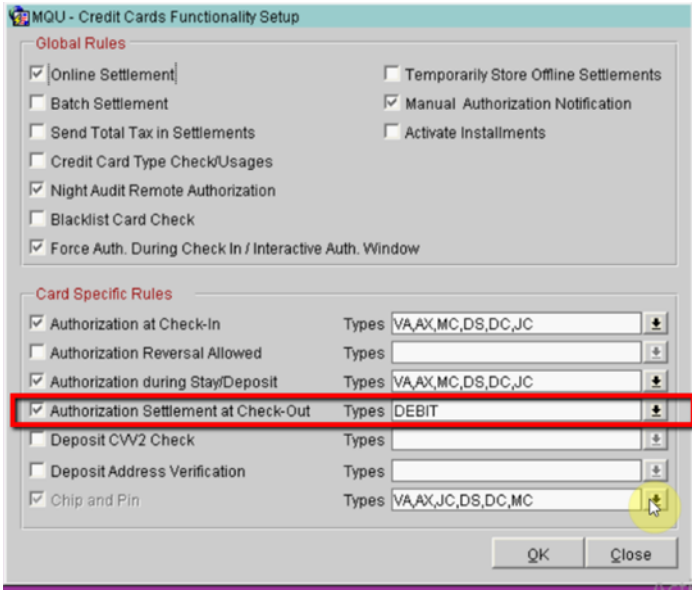
Figure 6-13 OPI Configuration Wizard



Update Functionality settings for Chip & Pin and PayOnly

- Selection for Chip & Pin and PayOnly cards.

Figure 6-14 Credit Cards Functionality Setup

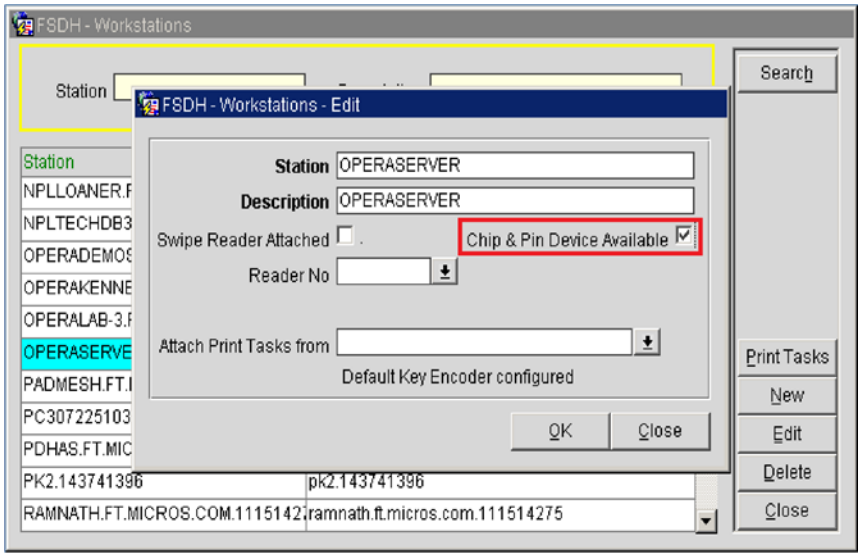


Configuring the Workstation

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).

Figure 6-15 Workstations Edit



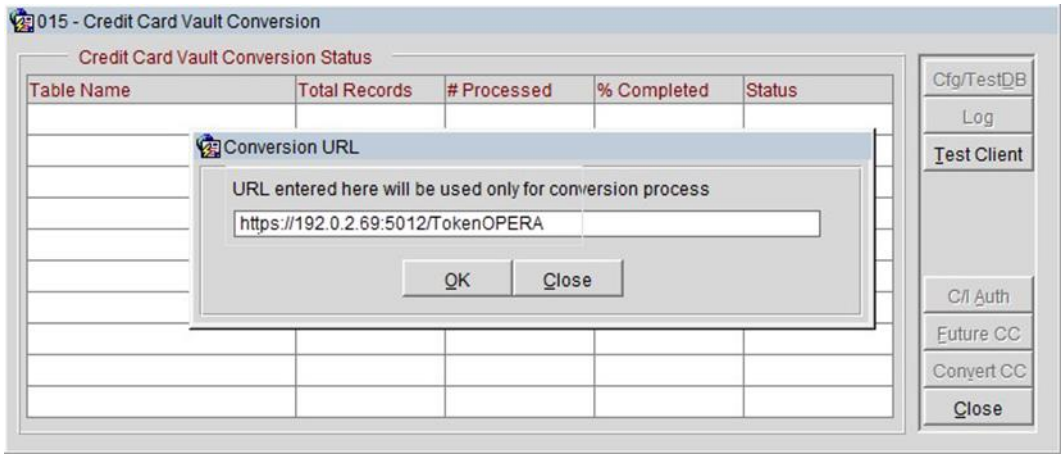
Configuring the Hotel Property Interface (IFC8) - Instance to the OPERA Hotel Property Interface (IFC)

This Step is NOT required as only GetToken will be performed by ORS

Perform a Tokenization

1. Go to **Utilities→Convert CC→Convert Vault CC Information→Test Client**

Figure 6-16 Credit Card Vault Conversion

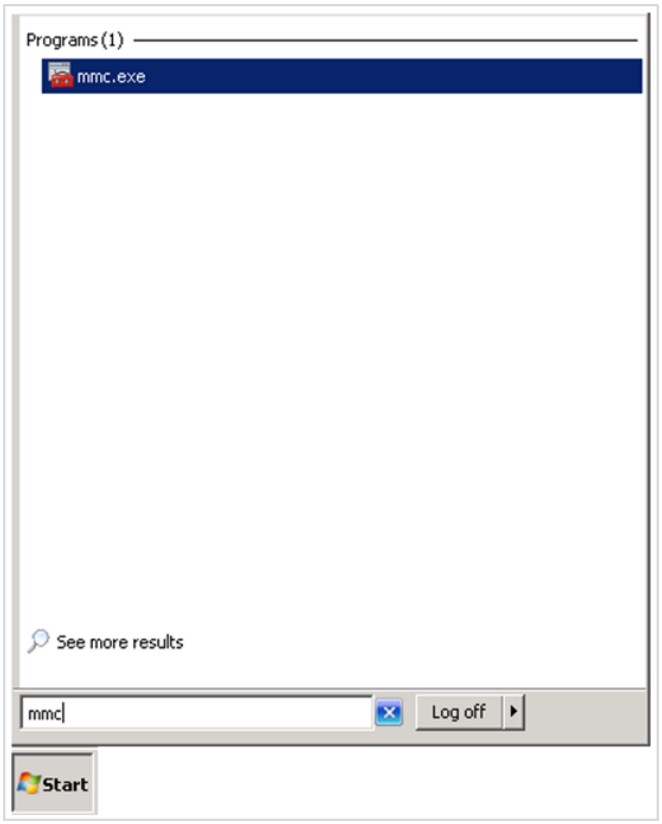


2. Complete the **Test Client** conversion to enable the **Credit Card Vault Conversion** functions.

Certificate Import using Microsoft Management Console

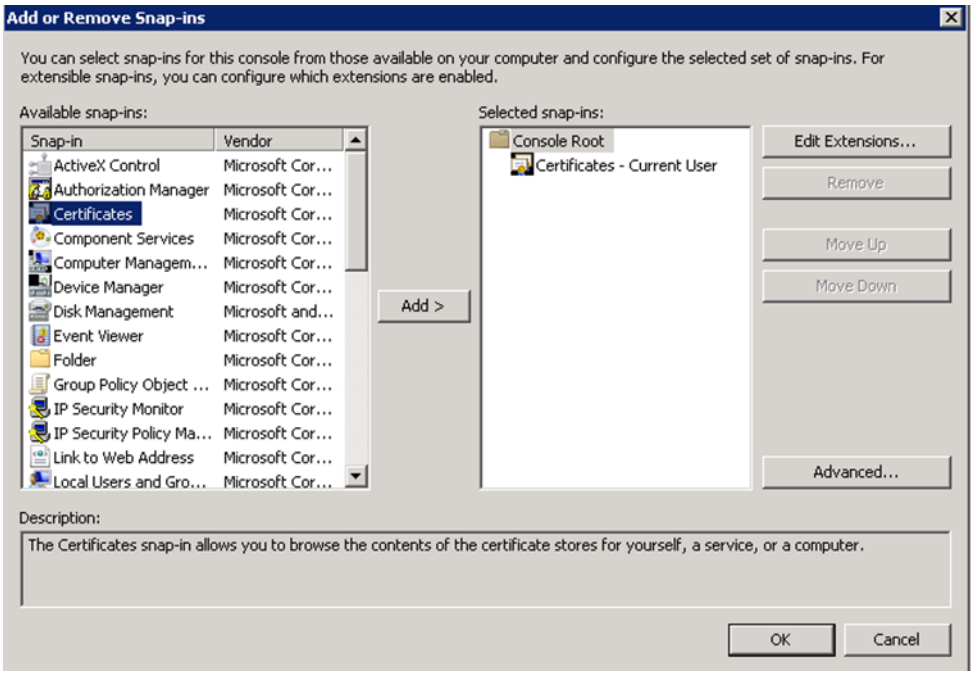
1. Find and open mmc.exe from Start menu.

Figure 6-17 Microsoft Management Console



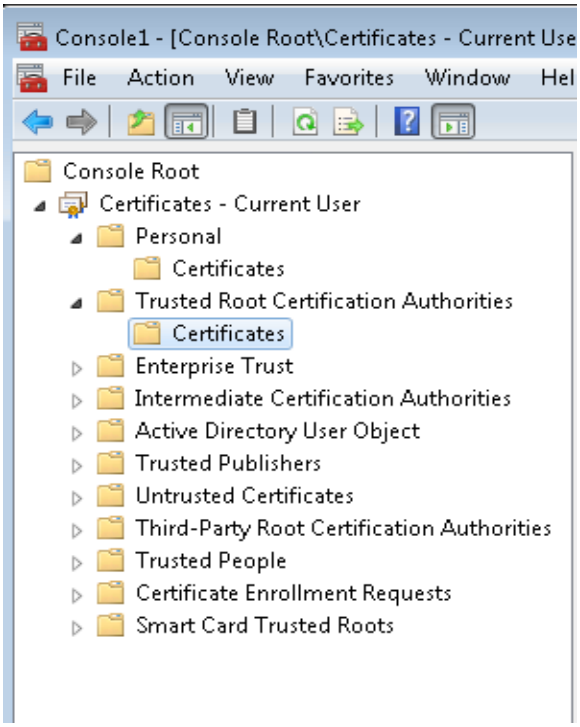
2. Go to **File** | **Add or Remove Snap-ins**, add certificates to Selected snap-ins, and then click **OK**.

Figure 6-18 Add or Remove Snap ins



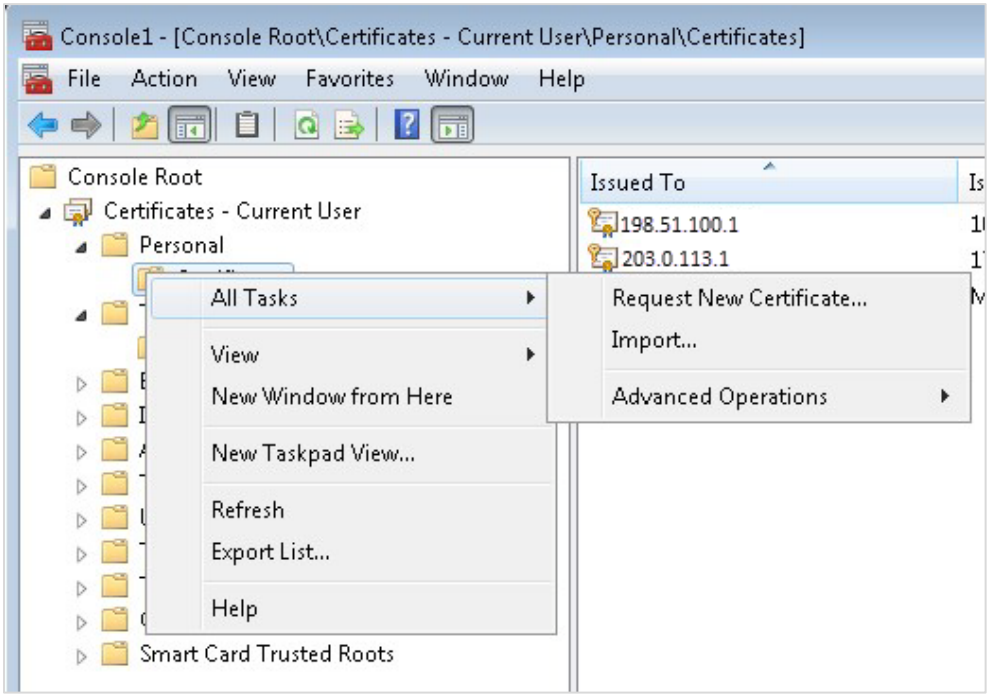
3. Expand Certificates, expand Personal or Trusted Root as required, and then select **Certificates**.

Figure 6-19 Certificates



4. Right-click **Certificates**, select **All Tasks**, and then select **Import**.

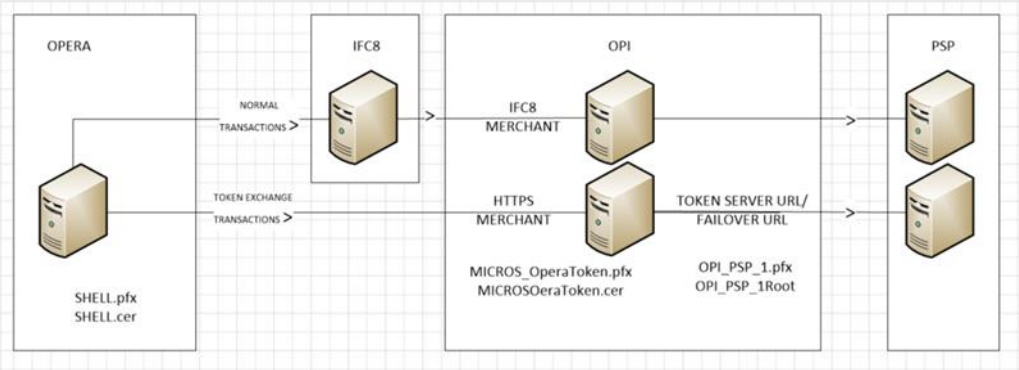
Figure 6-20 Certificates - All Tasks



- On the **Certificate Import Wizard Welcome** page, click **Next.**
- Browse to the location of the certificate file, and then click **Next**.
- If required enter the password relevant to the certificate you are importing, and then click **Next**.
- If the import is successful, then the certificates, common Name will be listed under the folder that was selected during import.

7 Certificates

Figure 7-1 Opera - IFC8 - OPI - PSP Flow Diagram



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.

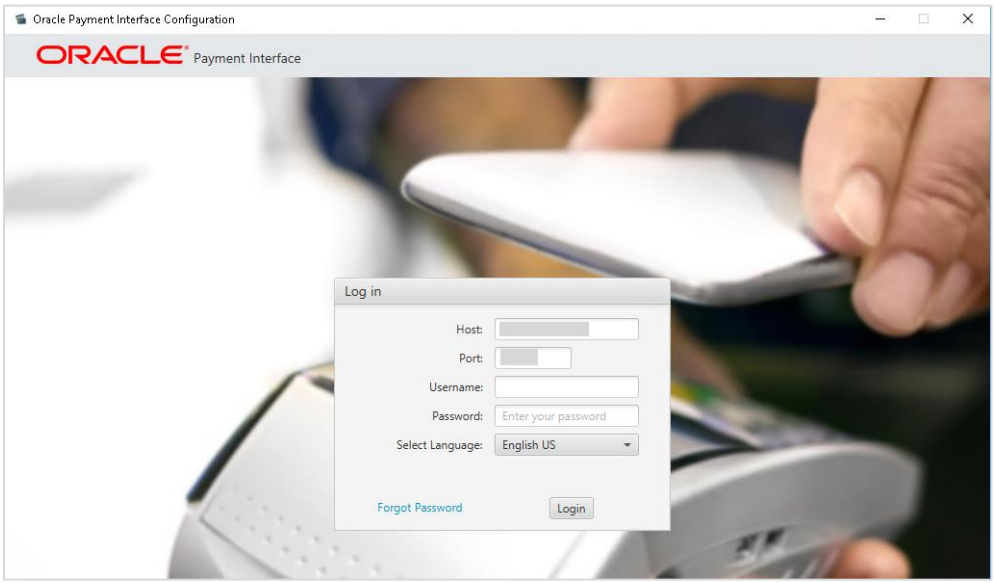
In order to achieve this, PSP is required to provide two files:

- A client side certificate file, this is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password.
- The root certificate file for the server side certificate that is deployed at PSP side. OPI needs to load this root certificate file into the Java Key store so that OPI can properly recognize and trust the server side certificate deployed at PSP side. The root certificate file provided by the PSP should be in the format of .cer or .crt.

To deploy the client certificate on the OPI side:

1. Run \OraclePaymentInterface\v19.1\Config\LaunchConfiguration.bat
2. Log in as the Super user you created during OPI installation.

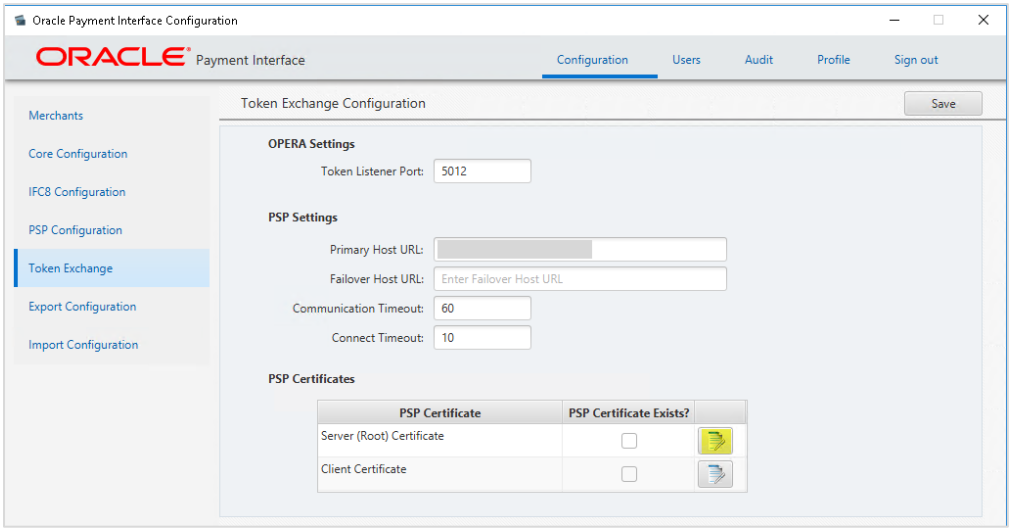
Figure 7-2 OPI Login Page



Handling the Root Certificate File by OPI Configuration Tool.

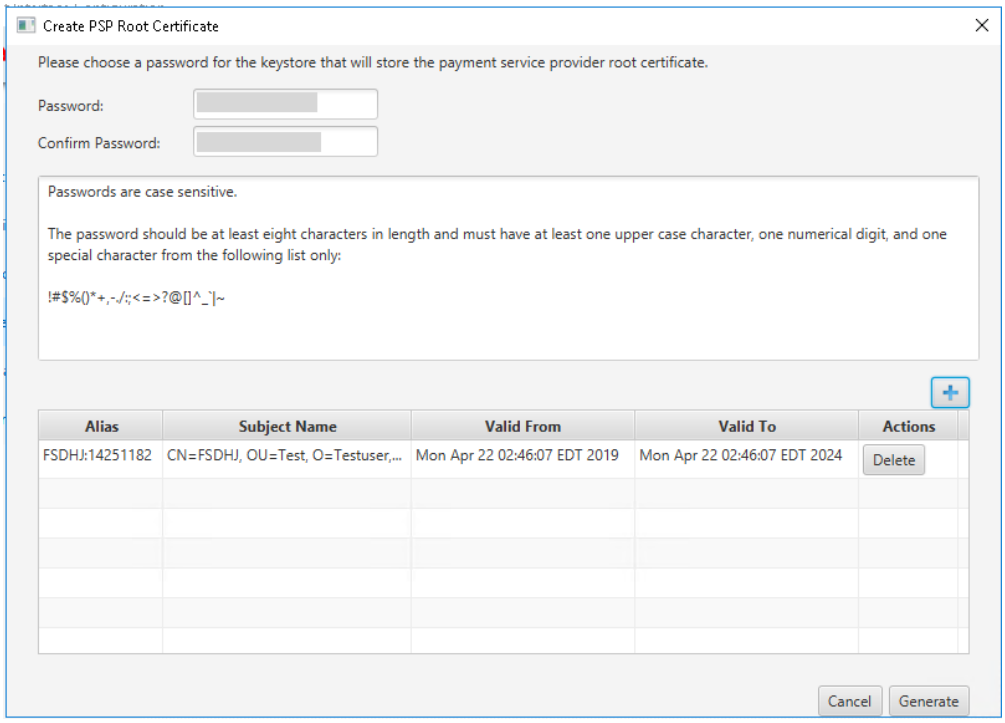
3. Select **PSP Token Exchange**, and then edit the **Server (Root) Certificate**.

Figure 7-3 OPI Token Exchange Configuration



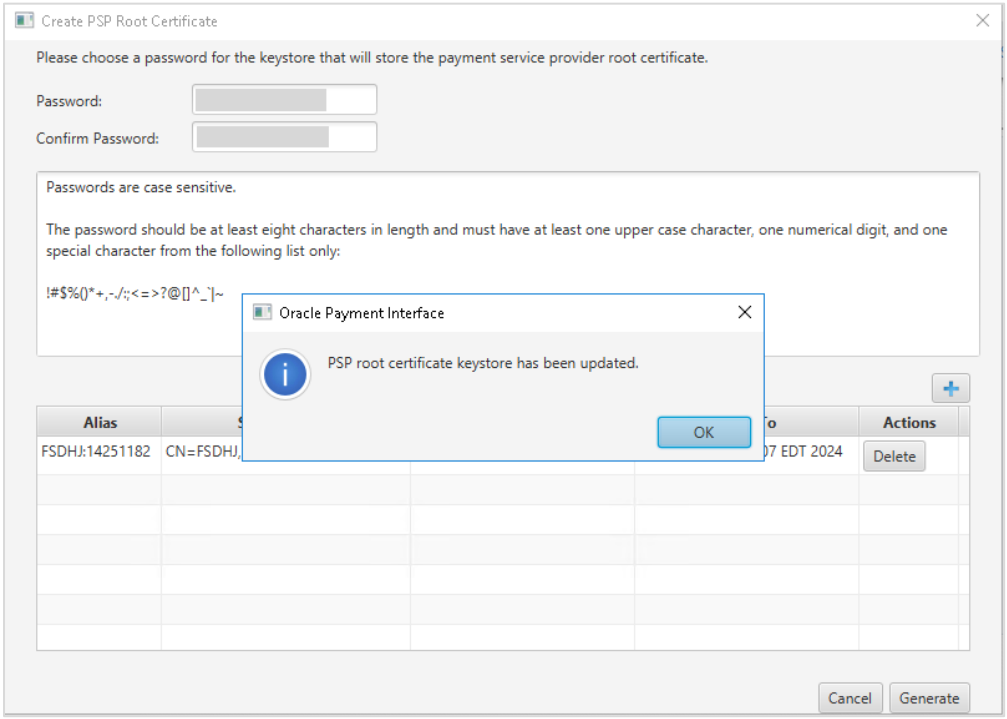
4. Enter the password for the keystore, and then browse to the location of the certificate you wish to import from add icon available or drag and drop the .cer or.crt.

Figure 7-4 Create PSP Root Certificate



5. Click **Generate**.

Figure 7-5 Certificate Updated message

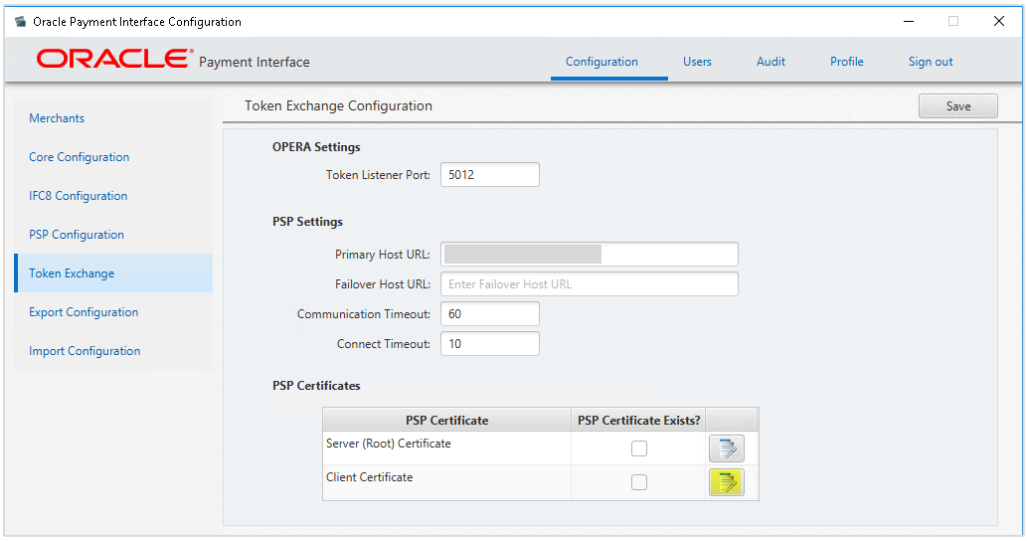


OPI_PSP_1Root is created under \OraclePaymentInterface\v20.1\Services\OPI\key

Handling the Client Side Certificate

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

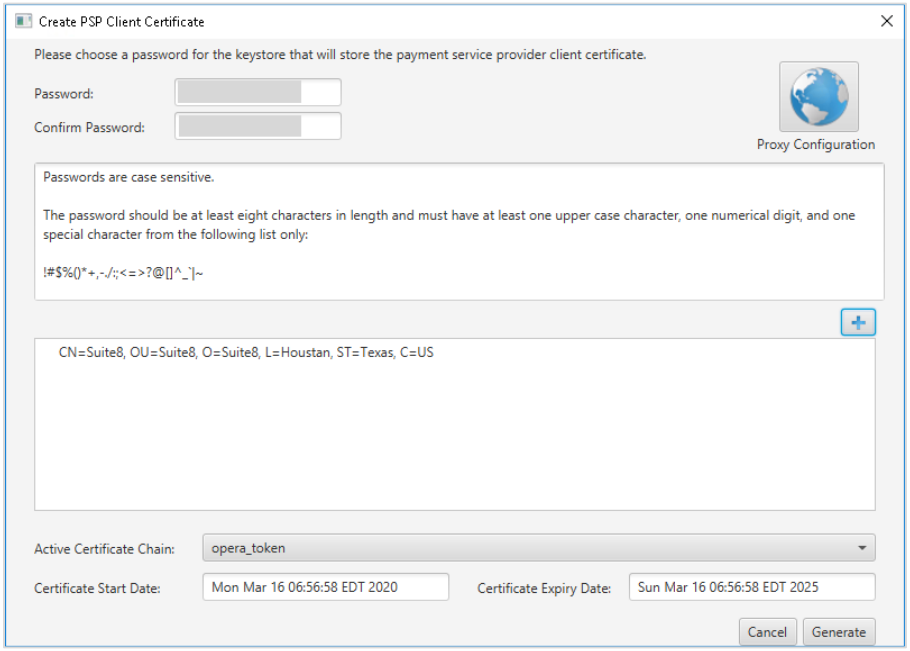
Figure 7-6 Token Exchange Configuration



7. Enter the password for the keystore then browse to the location of the certificate you wish to import from add icon available or drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below or it will not be possible to enter the details to the OPI configuration.

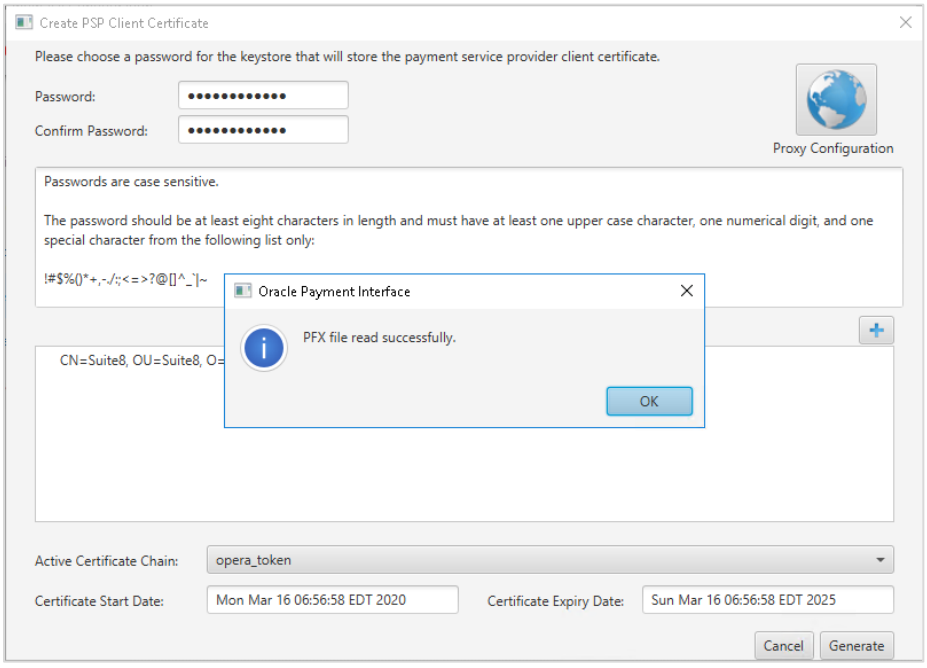
> **NOTE:**
>
> The PSP Client Side Certificates expiration date will vary depending on what the PSP set during creation of the certificate. Check the expiration date in the properties of the certificate files. Be aware the PSP certificates must be updated prior to the expiration date to avoid downtime to the interface.

Figure 7-7 PSP Client Certificate



8. Click **Generate**.

Figure 7-8 PFX File successful message



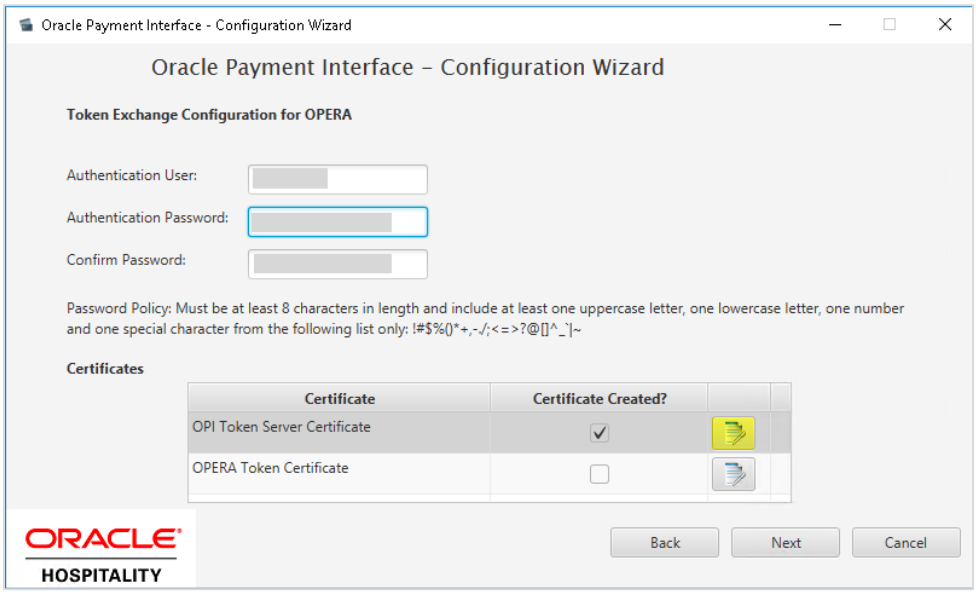
OPI_PSP_1.pfx is created **under \OraclePaymentInterface\v20.1\Services\OPI\key** folder.

OPI - Server Side Certificates

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

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

Figure 7-9 OPI Configuration Wizard



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;

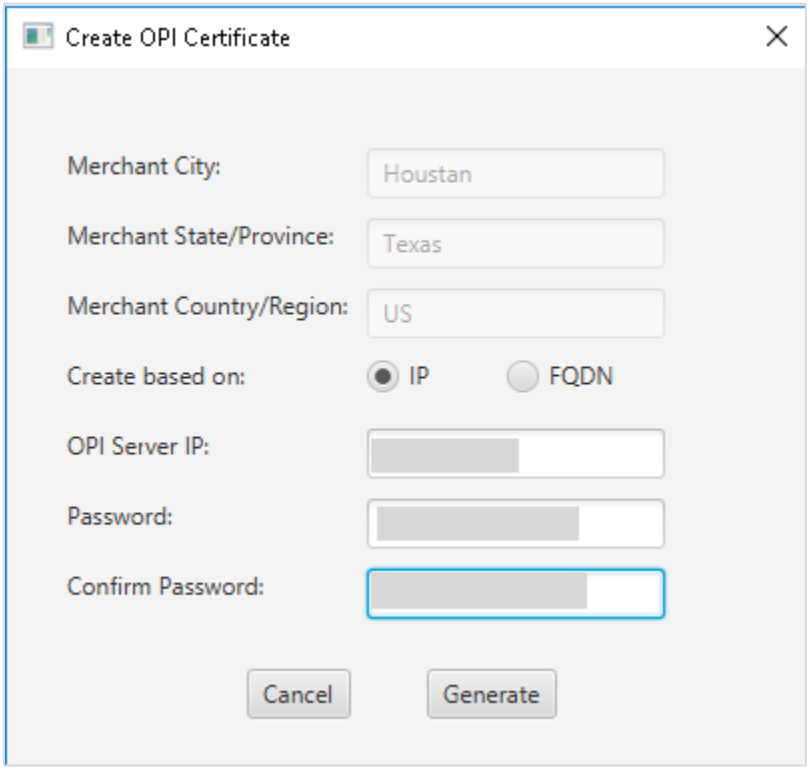
   a. Min 8 characters in length

   b. Min 1 Alpha Character

   c. Min 1 Numeric Character

   d. Min 1 Special Character from the following list !@#$%^&*

Figure 7-10 Create OPI Certificate

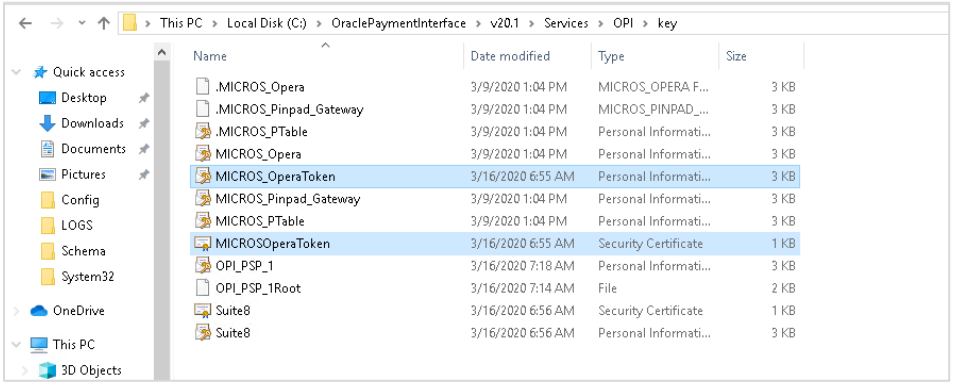


3. Click **Generate** to continue.

This process will generate the MICROS_OPERAToken.pfx & MICROSOPERAToken.cer files in the following folder:

\OraclePaymentInterface\v20.1\Services\OPI\key

Figure 7-11 Folder Path



> **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 Certificate (*.cer) file 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.