OPERA Bridge

Installation and Support Guide

Shift4 PAYMENTS

Contents

Copyright Notice

Shift4 Payments
1491 Center Crossing Road
Las Vegas, NV 89144
702.597.2480

www.shift4.com | info@shift4.com

Document Title: OPERA Bridge Installation and Support Guide

Publication Date: October 22, 2020

Product Overview

Background

EMV and hotels:

- A few years ago, the credit card industry adopted the EMV standards for payment cards, and the chip cards that comply with those standards. This was done to reduce card present fraud.
- The chip is very difficult to counterfeit and works very well in stopping card present fraud, where a fake or duplicate card is physically presented to the merchant during the transaction.
- The credit card industry has given the various industries (retail, restaurants, and hotels, etc.) time to adjust to chip processing.
- However, chip read credit card transactions (or EMV dipped) are becoming extremely important for security and financial implications.
- A merchant will lose any chargeback request if a credit card payment transaction has the capability to be chip processed, but is not.
- Within the hotel payments environment, many transactions will always be card not present (CNP) and therefore never qualify as EMV/chip read. This includes the following:
    - OTA Virtual Card authorization and payments (i.e. Expedia and Priceline).
    - Refunds to guests. (Refunds are always processed as CNP in lodging as the guest has typically left.)
    - Extra Charges. (Extra Charges are also always processed as CNP in lodging as the guest has typically left.)
    - Card on File check-ins (where the clerk uses the guest's credit card or token that is attached to the reservation booking).
    - Due In (Arrival) Card Verification processes (where a hotel on the day of a guest arrival runs an authorization to ensure the credit card number provided in the reservation is good). If the authorization response to this transaction is used as the check-in authorization, the charge will end up ultimately as CNP qualified.
    - Post check-in charges posted to rooms on a split folio (where the guest isn't present).
    - Some mobile check in applications.
    - Split folios where the second folio does not obtain a card present read.
- However, when the customer and the chip card are present and available, the credit card payment authorization should be chip inserted/read.

Requirements

- For Tokenization:
    - Opera Version – 5.0.03.03 e43 or higher
    - Opera Version – 5.0.04.01 e24 or higher
    - Opera Version – 5.0.04.02 e17 or higher
    - Opera Version – 5.0.04.03 e10 or higher
    - Opera Version – 5.0.05.00 or higher
- For SHA2: Oracle Database 11.2.0.4 or higher
- For TLS1.2: Oracle Database 11.2.0.4.170531 or higher, Windows 2008 (with appropriate patch) or higher.

How OPERA Bridge Works

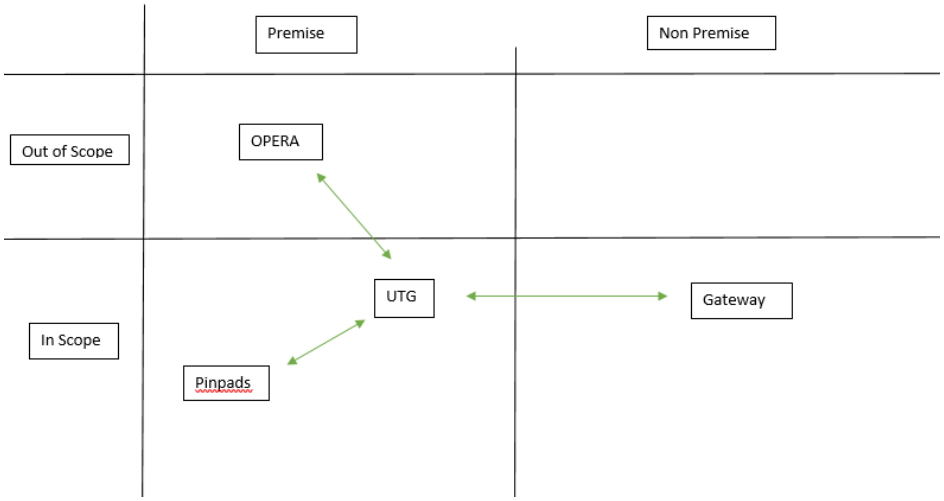
UTG Communication

There are two segments of communication in OPERA Bridge:

1. UTG to the gateway and to the PIN pads communication is not changing in any way.
2. OPERA to UTG.

- OPERA Bridge adds the ability of UTG to process messages using OPERA's Hotel Edition HTTP XML Credit Card Specification.
- OPERA Bridge allows hotels using OPERA to accept EMV without using Oracle's Payment Gateway (OPG) or Oracle's Payment Interface (OPI).

Overview of a Typical Hotel setup



Opera Communication

Overview of Transaction Process

Below is an overview of the transaction process.

- Normal Transactions:
  OPERA WS <-> OPERA system <-> UTG <-> Gateway
- Special Token Transactions: Single Get Token (manual entry enabled)
  OPERA WS/OXI <-> UTG <-> Gateway

Normal Transactions

A transaction is initiated by a workstation and is sent to the Opera Bridge API in UTG by the database. It is then sent to Shift4 gateway for processing.

NOTE: The UTG certificate located in the Oracle Database Wallet is used in this transaction.

Special Token Transactions

OXI and OPERA WS (manual entry in software) initiates get token or get CC to Opera Bridge API in UTG. For this to happen successfully, the UTG certificate needs to be installed on the workstation, OXI service, or OEDS service in respective servers.

NOTE: The UTG certificate imported into Windows Store is used in this transaction. Opera uses the Organization (O) value, which is the HOTEL ID, to find the certificate.

Installation Overview

Here is an overview of the steps to install OPERA Bridge.

1. Enable TLS 1.2 and disable old protocols (if supported).
2. Install UTG.
    - Configure API Interface.
    - Generate Certificate for OPERA.
    - Add Lanes.

Configure OPERA.

- Install Certificates.
    - Install Certificate on Workstations and Services.
    - Install Certificate in Oracle Database Wallet.
- Configuration of OPERA.
    - Create CCW interface.
    - Activate Vault.
    - Activate Chip and Pin.
    - Enable Online Settlement.
    - Setup Workstation.
    - Backup credit card table.
    - Verify functionality on a workstation.
    - Bulk Tokenization.
    - Verify functionality.

NOTE: Please ask the hotel to do a full backup of their system in case of issues before proceeding.

Pre-installation Steps

Overview

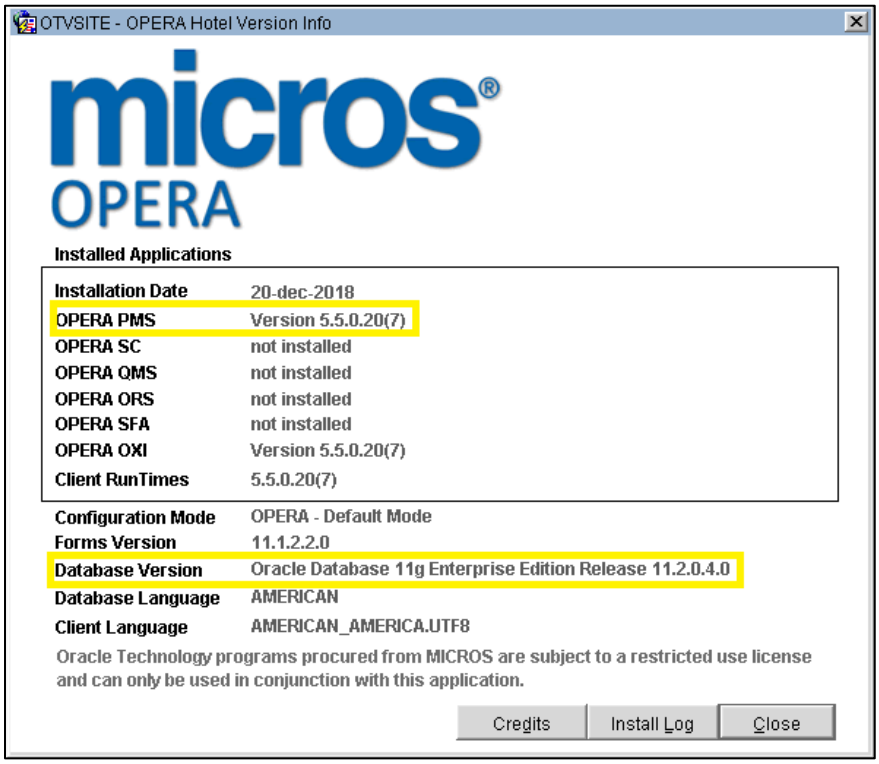
There are a few things that need to be done as part of pre-installation steps:

- Verify software version meets the minimum requirement.
- Purge old Credit Cards.
- Note Chain and Property code to do configuration.
- Check the Wallets folder.
- Settle In House Guests
- Settle Credit Card Batch
- Send EOD
- Print Downtime Report

Check OPERA Version

You can get more detailed information about the OPERA and the Oracle Database version by following the steps below:

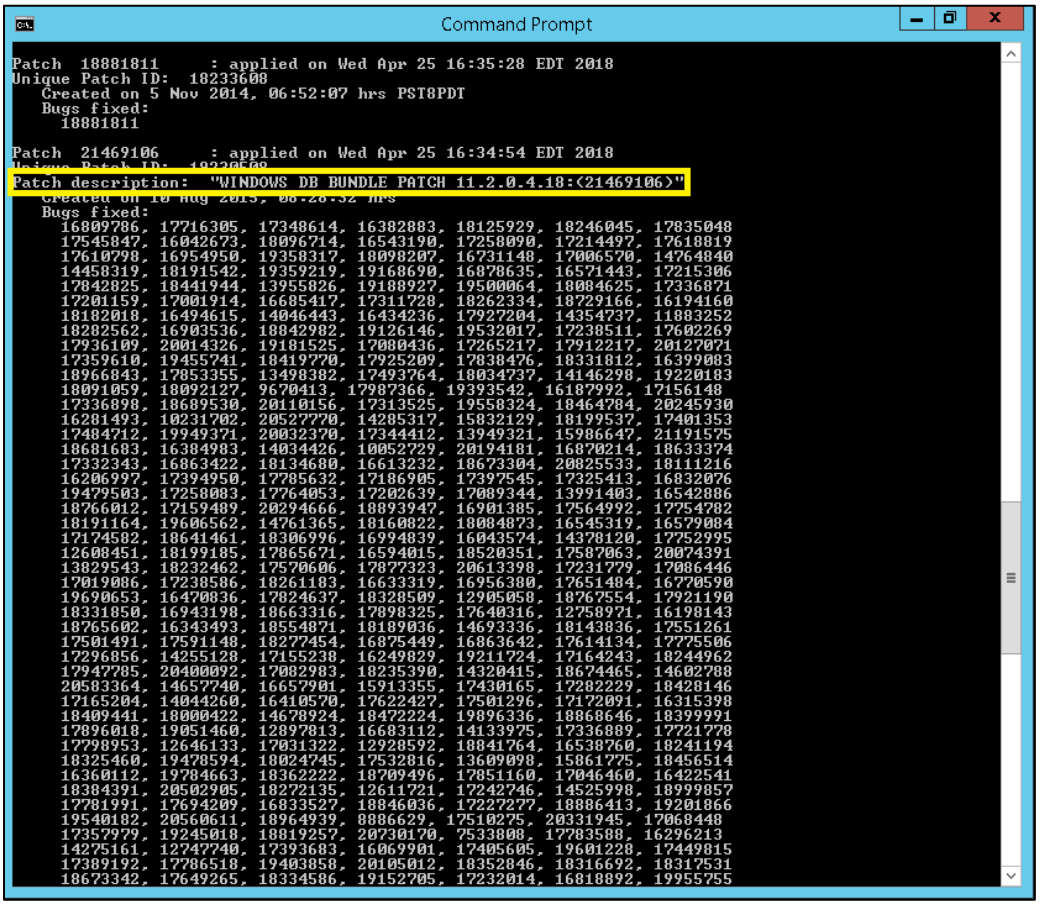
1. Log in to OPERA.
2. Click on **PMS**.
3. Select the resort and click **Login**.
4. Click on **Help > About OPERA**.



Check Oracle DB version

The major version is seen in the About OPERA dialog box, but to find the patch installed, please follow the steps below:

1. Open an administrative command prompt (steps depend on the version of Windows).
2. Set oracle_home parameter.
   set oracle_home=D:\Oracle\1120
   NOTE: Oracle Database might be installed in different locations. Change the command to point to the correct location.
   a. D:\Oracle\1120
   b. D:\Oracle\11204
3. Run opatch to show the version.
   %oracle_home%\opatch\opatch lsinventory
4. Check the Patch description for the full Oracle Database version.



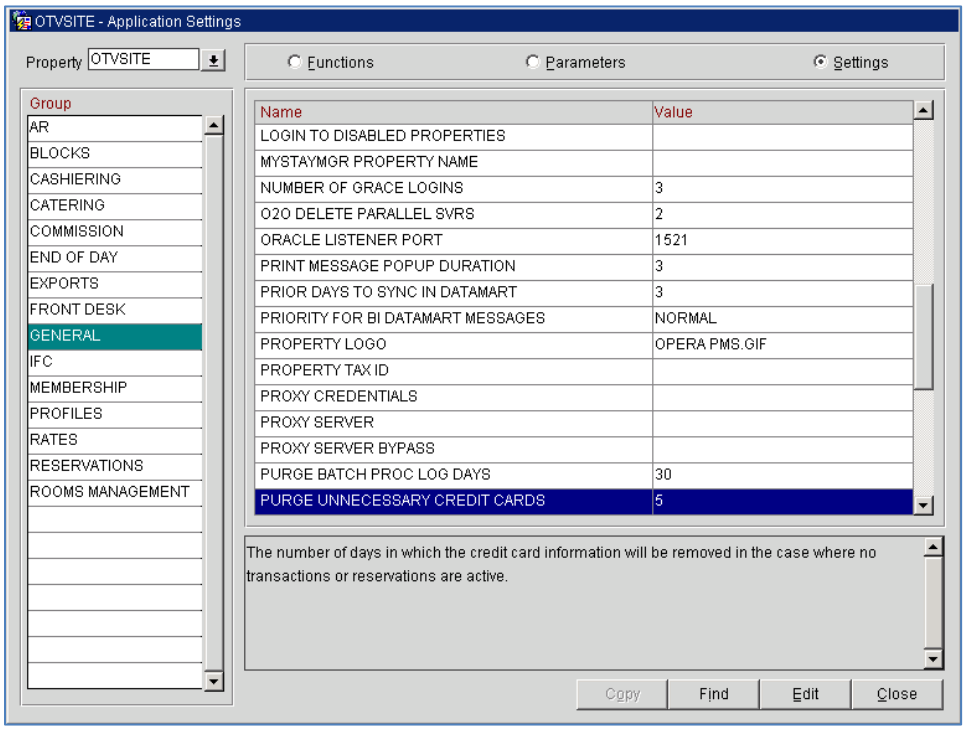
Purge Credit Cards

It is recommended to purge old and unnecessary card data so that the migration is smooth and quick. This is run during the night audit.

- Ask users to check frequently used profiles for any expired and unnecessary cards, and delete them manually.
- Check if the purge routine is configured.

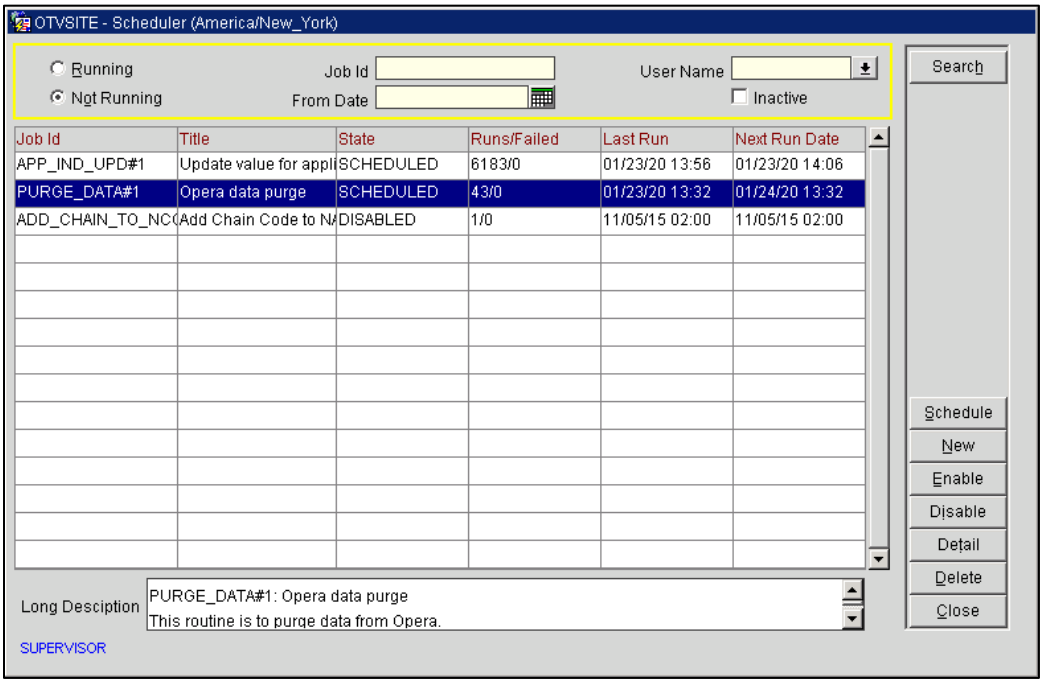
Verify that Purge is Configured

1. Log in to OPERA as manager or supervisor.
2. Click on **PMS**.
3. Select the resort and click **Login**.
4. Click on **Setup > Application Settings**.
5. Navigate to **General > Settings > Purge Unnecessary Credit Cards**.



6. Click **Edit**.
7. Type in the number of days before today for which you want to remove credit cards. Recommended: 30
8. Click **Close**.
9. Click **Exit** to close PMS.
10. Click on **Utilities**.
11. Select the resort and click **Login**.
12. Click on **Utilities > Opera Scheduler**.
13. Select the **Not Running** radio button. You should see the Purge Data purge routine.

14. Verify the state is set to Scheduled. If the State is set to Disabled, you can enable it by clicking on the Enable button on the right.



Check Chain and Property Code

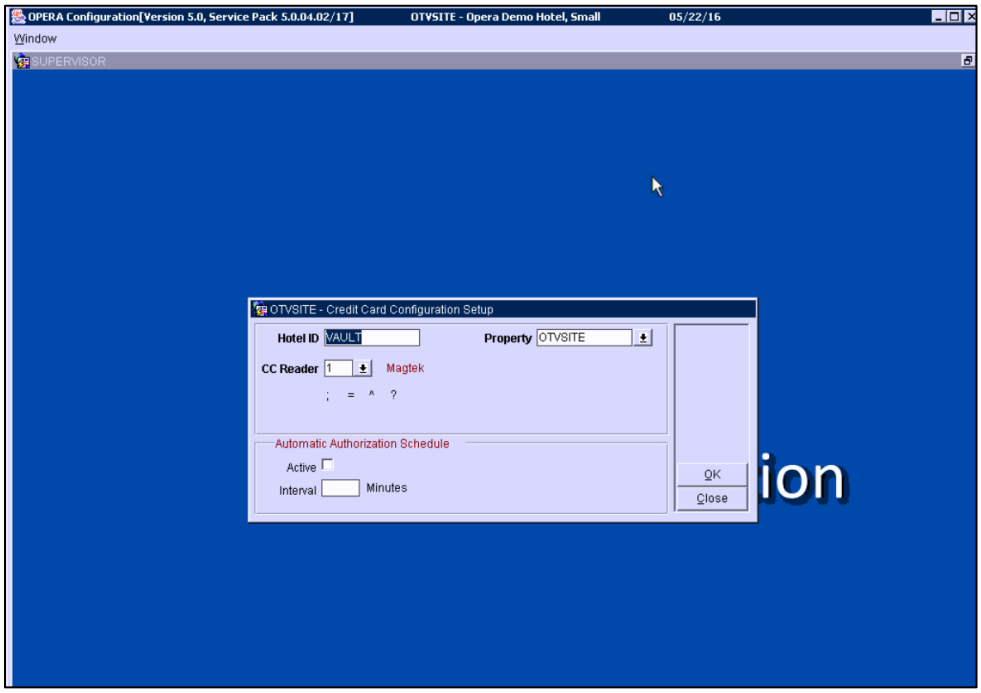
1. Log in to OPERA as manager or supervisor.
2. Click on Configuration.
3. Select the resort and click Login.
4. Go to **Setup > Property Interfaces > Credit Card Interface > General Parameters**.

5. Note the Hotel ID and Property ID of a site.

   NOTE:

   Hotel ID = COMP Code

   Property = SITE CODE



Check Wallets Folder

The database wallets are stored in subfolders in the following format:

<Base Folder>\<Product Code>\<Resort>

Normally the default directory is located in D:\Oracle\Admin\OPERA\Wallets, but sometimes it could be in a different location. For example, for resort NHSEQ with product code S4O, the wallet folder is:

D:\Oracle\Admin\OPERA\Wallets\S4O\NHSEQ\

You can find the base folder by following the steps below:

1. Log in to sqlplus as opera by running the following in a command prompt.

sqlplus opera/<password>@opera

2. Run the following command to find the wallets folder and make a note of it:
   select o_http_client.get_wallet_directory() from dual;
3. Make a note of the base folder.

Settle In house Guests

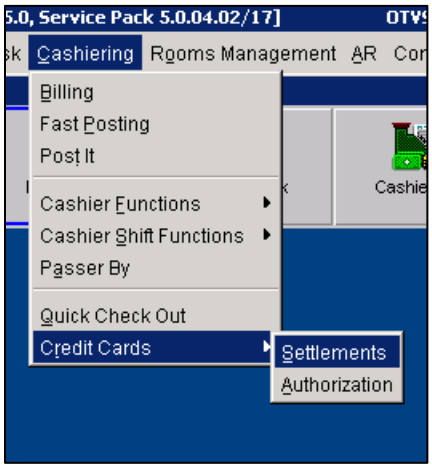
Ask the hotel to settle out any outstanding authorizations for in house guests. Outstanding authorizations will be lost during conversion.

Settle Credit Card Batch

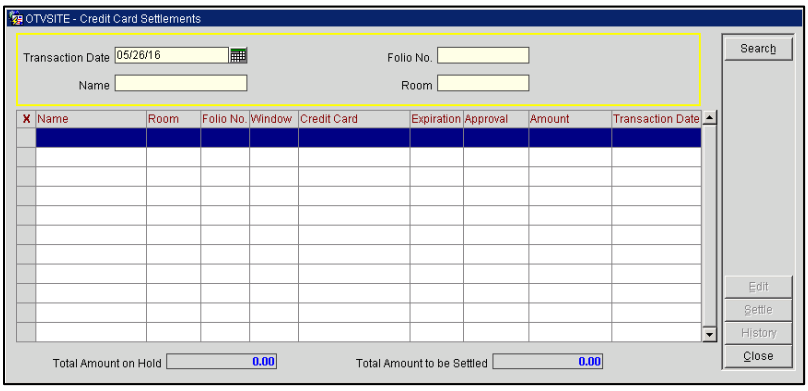
If the hotel is using Batch Settlement, the credit cards are stored in a batch settlement bin until it can be settled out. It is best to settle out these cards before doing the UTG install as UTG will not know about these transactions.

NOTE: Please have the hotel follow the steps below to settle any credit card transactions. It is recommended to go back at least 7 days or more and check for outstanding transactions.

1. Log in to OPERA.
2. Click on **PMS**.
3. Select the resort and click **Login**.
4. Click on **Cashiering > Credit Cards > Settlements**.



5. Select date and click **Search**.



6. Select the transaction and click on **Settle** to settle any outstanding transactions.

Send EOD/Batch Close

Some Processors/Gateway might need a batch close message to be sent from OPERA to close the batch on their end. Discuss with the merchant if this is needed and if they would like to send the batch close message.

To send the EOD,

1. Login to Configuration.
2. Go to **Setup > Property Interfaces > Interface Configuration**.
3. Select the old interface and click **Edit**.
4. Click on **Send EOD**.
5. Select the current business date and click **OK**.

Print Downtime Report

Please have the hotel print out their downtime reports so that they are ready to function without the PMS and to have historical data.

Please ask the hotel to perform the following steps:

1. Log in to PMS.
2. Click on **Miscellaneous > Reports**.
3. Search for Downtime Reports.
4. Click **OK**.
5. Click **Print**.

Enable TLS 1.2 for WinHTTP and SChannel

It is recommended that TLS1.2 be enabled for communication if it is supported. For the merchant to support TLS1.2 they need the following:

- Windows 7 and Windows 2008 with patches can support TLS1.2.
- Oracle Database is 11.2.0.4.170531 or higher.

For newer Windows 2012 Server, TLS 1.2 is enabled by default along with other encryption. It is recommended to disable the older encryption.

NOTE: It is recommended to create a Windows Registry backup or a Restore Point before implementing these changes.

WinHTTP and Internet Settings for TLS 1.2

Automatic

Apply the latest Windows Update, and apply the Easy Fix from the links below. This will enable both WinHTTP and Internet Settings support for TLS 1.2.

Windows Patches,

http://catalog.update.microsoft.com/v7/site/search.aspx?q=kb3140245

Easy Fix,

https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in

Manual

Or manually create or update the DefaultSecureProtocols and SecureProtocol registry entry in the following path:

WinHTTP Support for TLS 1.2 to Windows Registry

Create a DefaultSecureProtocols entry in the WinHttp sub-key below and set it to,

- DWORD value of a00 to enable TLS 1.1 and TLS 1.2 support.
- DWORD value of 800 to enable only TLS 1.2 support.

For 32-bit computers:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp

DWORD name: DefaultSecureProtocols

DWORD value: 0x00000a00 **For 64-bit computers:**

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp

DWORD name: DefaultSecureProtocols

DWORD value: 0x00000a00

Internet Settings Support for TLS 1.2 to Windows Registry

Create a SecureProtocols entry in the Internet Settings sub-key below and set it to,

- DWORD value of a00 to enable TLS 1.1 and TLS 1.2 support.
- DWORD value of 800 to enable only TLS 1.2 support.

For 32-bit Computers:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

DWORD name: SecureProtocols

DWORD value: 0x00000a00

For 64-bit Computers:

HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings

DWORD name: SecureProtocols

DWORD value: 0x00000a00

SCHANNEL for TLS 1.2 (Windows 7 and Windows 2008R2)

Create Enabled & DisabledByDefault entries in the appropriate Client sub-key below and, set the DWORD value to 0 to disable the sub-key or 1 to enable the sub-key.

Disable SSL 2.0 Client

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client

DWORD name: DisabledByDefault

DWORD value: 1

DWORD name: Enabled

DWORD value: 0

Disable SSL 2.0 Server

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server

DWORD name: DisabledByDefault

DWORD value: 1

DWORD name: Enabled

DWORD value: 0

Disable SSL 3.0 Client

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client

DWORD name: DisabledByDefault

DWORD value: 1

DWORD name: Enabled

DWORD value: 0

Disable SSL 3.0 Server

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server

DWORD name: DisabledByDefault

DWORD value: 1

DWORD name: Enabled

DWORD value: 0

Disable TLS 1.0 Client

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client

DWORD name: DisabledByDefault

DWORD value: 1

DWORD name: Enabled

DWORD value: 0

Disable TLS 1.0 Server

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server

DWORD name: DisabledByDefault

DWORD value: 1

DWORD name: Enabled

DWORD value: 0

Disable TLS 1.1 Client

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client

DWORD name: DisabledByDefault

DWORD value: 0

DWORD name: Enabled

DWORD value: 1

Disable TLS 1.1 Server

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server

DWORD name: DisabledByDefault

DWORD value: 0

DWORD name: Enabled

DWORD value: 1

Enable TLS 1.2 Client

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client

DWORD name: DisabledByDefault

DWORD value: 0

DWORD name: Enabled

DWORD value: 1

Enable TLS 1.2 Server

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server

DWORD name: DisabledByDefault

DWORD value: 0

DWORD name: Enabled

DWORD value: 1

Enable TLS 1.2 Communication

There are several OPERA components that check the IE and Java Settings to see if TLS 1.2 is enabled, such as the OXI Processor Windows Services (Uses IE Settings) and GetID operations from OPERA UI (uses Java Settings). The Internet Explorer settings must be updated to allow TLS 1.2 so that the OXI services will make the proper connection. Please see their appropriate documentation to enable these settings.

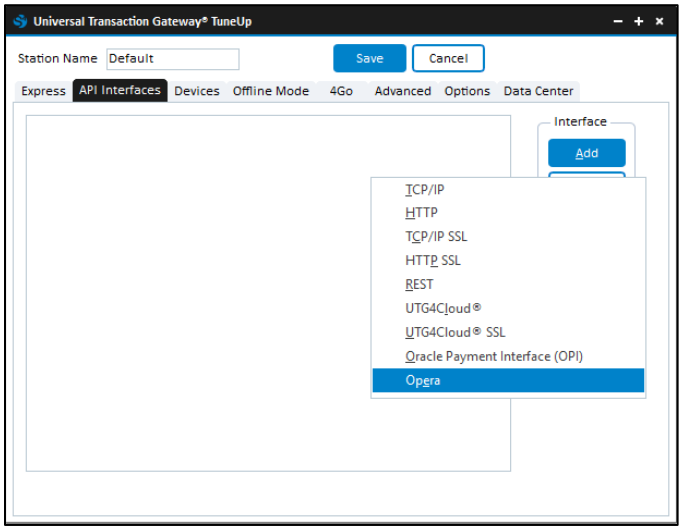
Installing UTG

Install UTG Software

Download and run the installer for UTG software. Please refer to the UTG Installation and Configuration Guide.

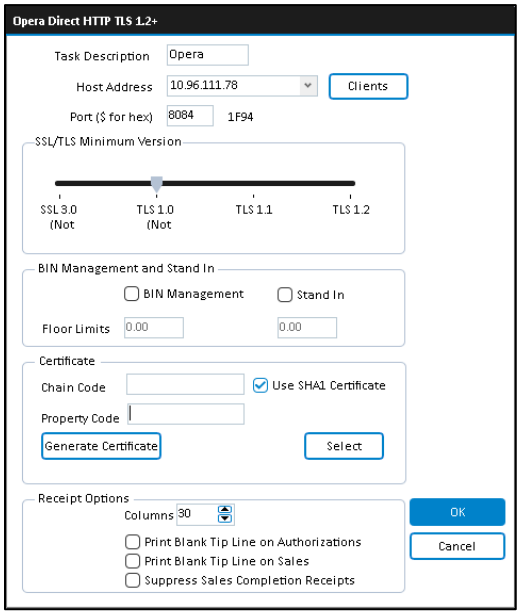
Configure OPERA Interface

1. Add the "OPERA" interface to API Interfaces.

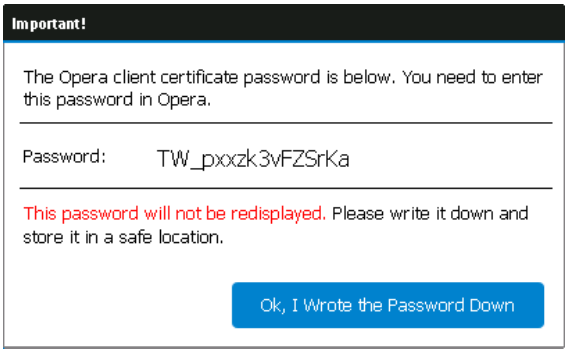


2. Fill the dialog box as noted below.
    a. The host address is the IP address of the OPERA server.
    b. Select the TLS version:
        i. Oracle DB 11.2.0.4 or lower: TLS 1.0
        ii. Oracle DB 11.2.0.4.170531 (OPERA 5.5 or higher): TLS 1.2
        iii. TLS is enabled on all WS and Server (see TLS section above)
    c. Enter the site's chain and property codes.
    NOTE: The chain code is provided by Shift4, the property code is the resort code in Opera.
    d. Select if you want to use SHA1 or SHA2:
        i. Oracle DB 11.2.0.3: SHA1
        ii. Oracle DB 11.2.0.4: SHA2
    e. Click **Generate Certificate**.

f. Save both the oputg2.pfx and ewallet.p12 file in UTG2 folder.



g. UTG will display the ewallet password. Make a note of the password and provide it to the merchant. **NOTE:** The password for the certificate will only appear once. It is the responsibility of the site to record and manage that password. The installer will need this password for the rest of the installation.

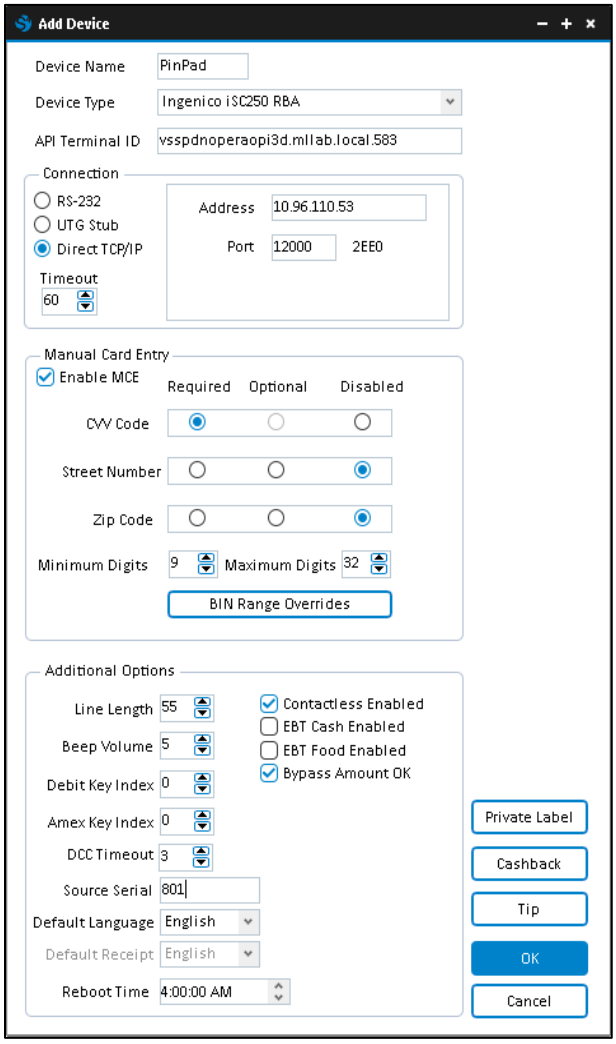


h. Click **OK, I Wrote the Password Down**.

3. Click **OK**.

Add Devices and Lanes

4. Go to the Devices tab and add the required number of pin pads to UTG.
    a. Select the device type, connection, and any communication parameter for the pin pad.
    b. Enter the API Terminal ID. It is the **last 32 of OPERA registered terminal ID** and must be provided by the site. One workstation ID must be provided per pinpad.
    c. Enable MCE and configure it as per the requirement of the merchant.



5. Click **OK**.

Installing Certificates

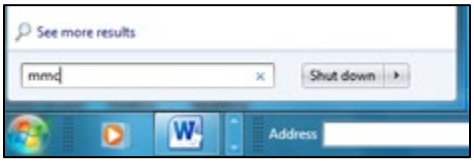
A certificate is needed on the WS and Services that talk to UTG.

NOTE: It is recommended that this be done at the day of the install as it requires the current certificates to be deleted.

Installing Certificates in OPERA Workstations and Services

Open Microsoft Management Console

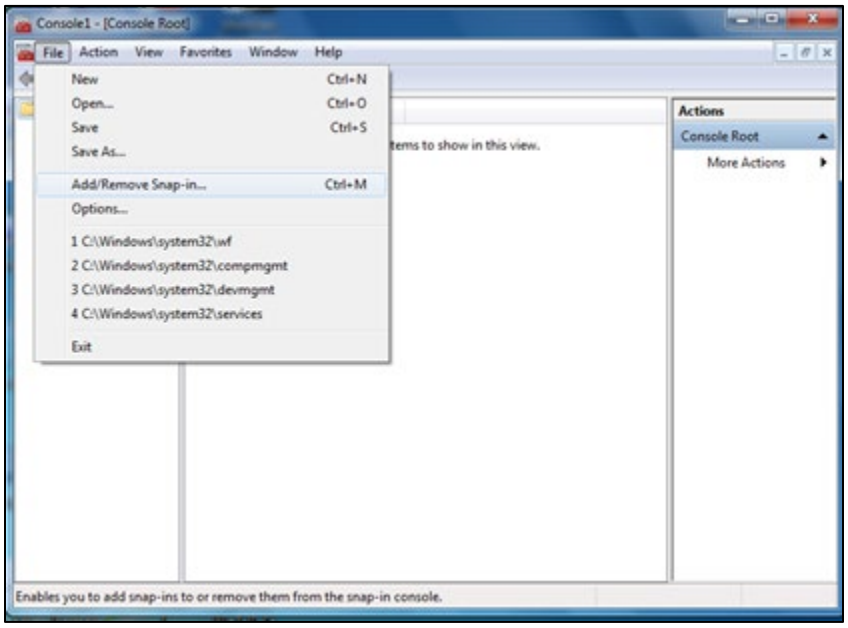
1. Press the Start button on the windows desktop.
2. Click on **Run…** The Run dialog box appears.
3. Type **mmc** in the text box.



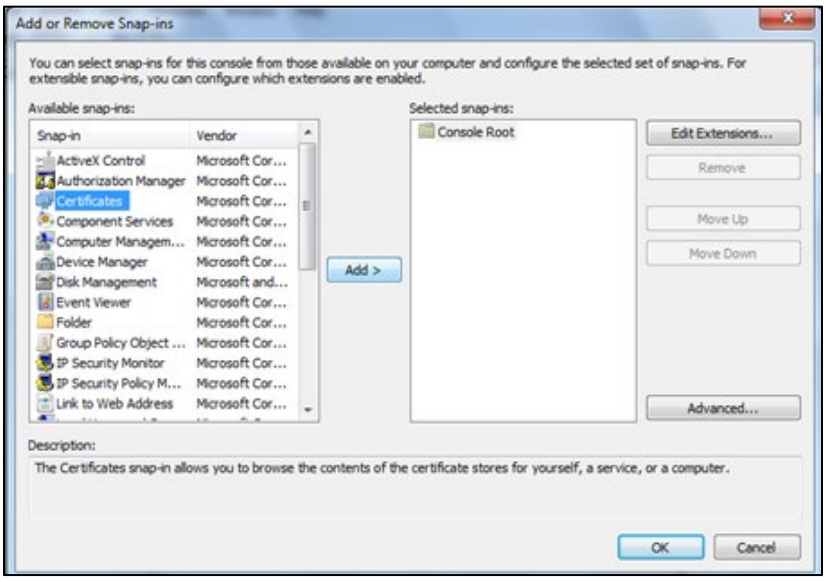
4. Press the Enter key or press the **OK** button. The Console 1 window displays.

Open User Account Certificate Store

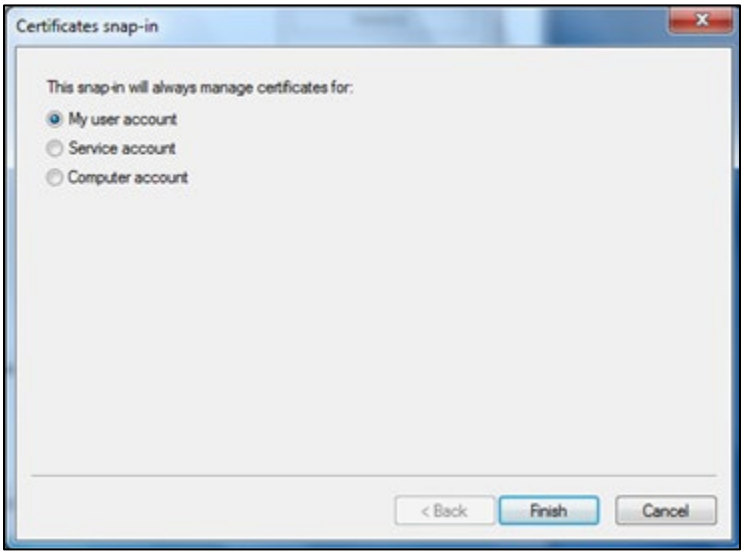
5. Select **File** from the menu bar.
6. Select **Add/Remove Snap-in…** from the menu.



7. The Add/Remove Snap-in dialog box displays.



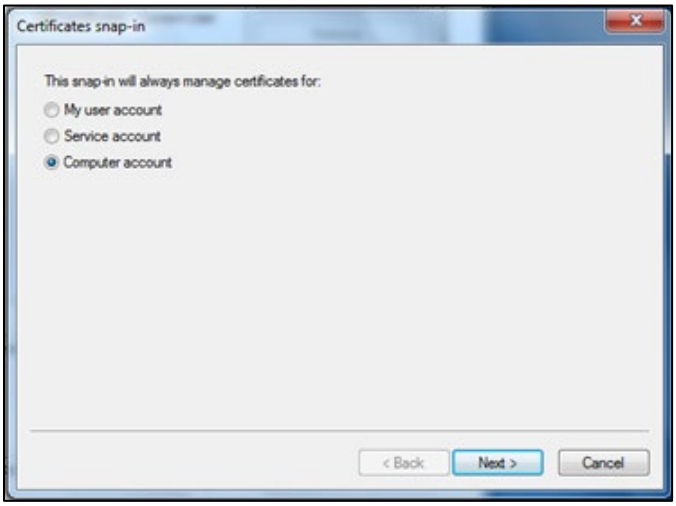
8. Press the **Add** button. The Add Standalone Snap-in dialog window displays.
9. Select **Certificates** from the list of snap-ins.
10. Click the **Add** button. The Certificates Snap-in wizard appears.



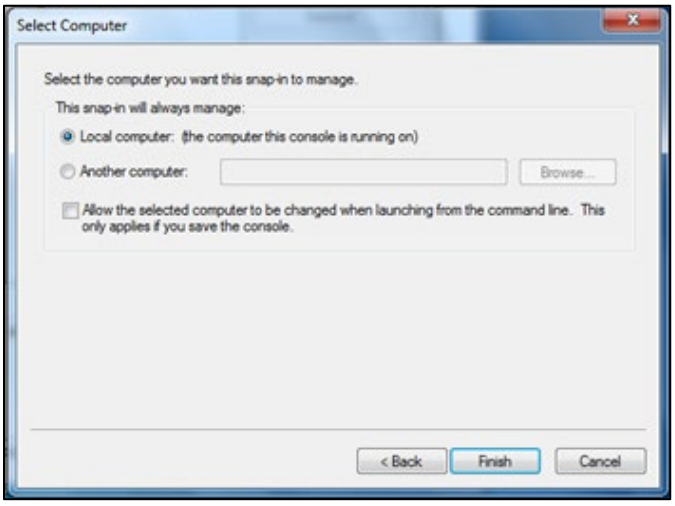
11. Ensure the option **My user account** is selected.
12. Press the **Finish** button.

Open Computer Account Certificate Store

13. In the Add Standalone Snap-in dialog window, select **Certificates**.
14. Press the **Add** button. The Certificates Snap-in wizard appears again.
15. Select the **Computer account** option.



16. Press the **Next** button. The final step of the wizard displays.
17. Ensure that the **Local computer: (the computer this console is running on)** option is selected.

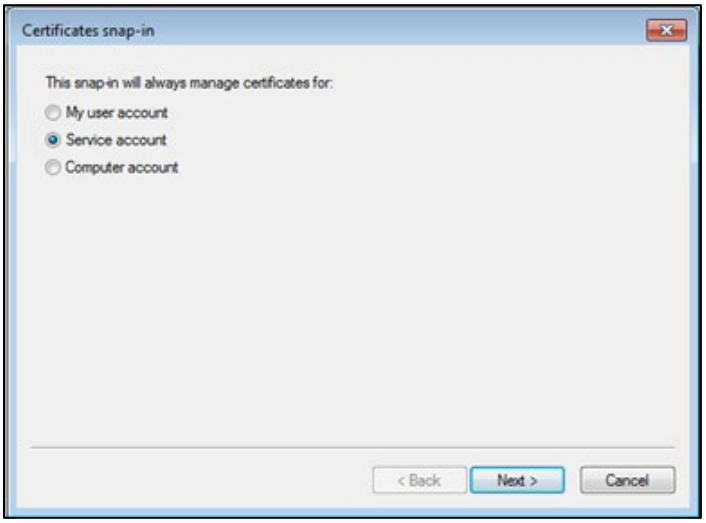


18. Press the **Finish** button.

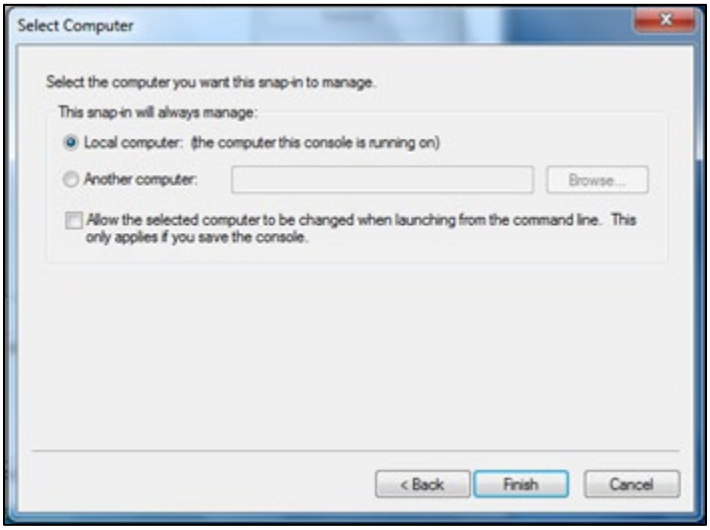
Open Service Account Certificate Store

NOTE: This is only required if there are services that will conduct transactions directly. For example, OPERA OXI and OEDS services.

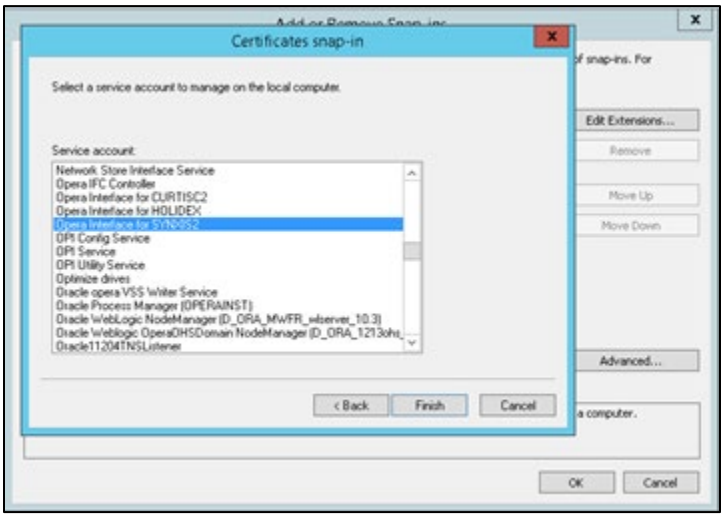
19. In the Add Standalone Snap-in dialog window, select **Certificates**.
20. Press the **Add** button. The Certificates Snap-in wizard appears again.
21. Select the **Service account** option.
22. Press the **Next** button.



23. Make sure **Local Computer: (the computer this console is running on)** option is selected.



24. Press the **Next** button. The list of services in the workstation is displayed.



25. Select the Oracle Service that deals with credit card data. Some common interfaces are the OPERA OXI and OEDS services.
26. Press the **Finish** button.
27. Repeat for any other services that will perform transactions.

Verify all Windows Stores Are Open

28. Click the **Close** button on the Add Standalone Snap-in dialog window.
29. Verify that you now have three certificate entries in the Selected snap-in section of Add/Remove Snap-in dialog:
    - Certificate – Current User
    - Certificates – (Local Computer).
    - Certificates – Service (<Service Name>) on Local Computer
30. Press **OK** to close the Add/Remove Snap-in dialog window.

Overview of Certificate Installation Steps

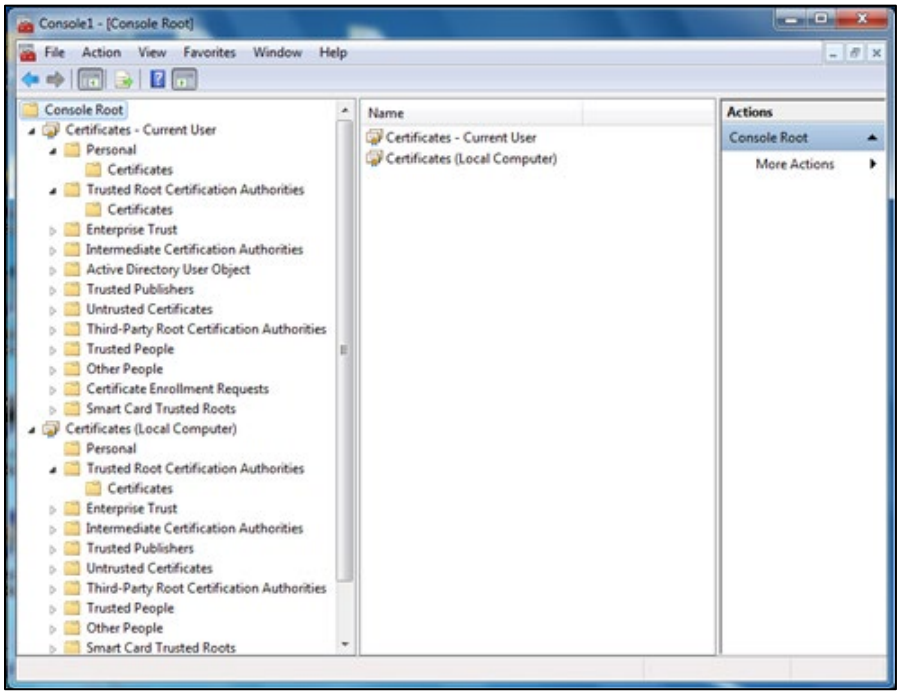
The UTG certificates will have to be installed in multiple certificate stores.

1. Remove all old and expired certificates.
2. Load certificates under Console Root - Certificates (Local Computer) under Trusted Root Certification Authorities – Certificates folder.
3. Repeat the same steps under the Console Root – Certificates (Current User).
4. Repeat the same steps under the Console Root – Certificates - Service (<Service Name>) on Local Computer. This is only required for interface servers like OPERA OXI and OEDS.

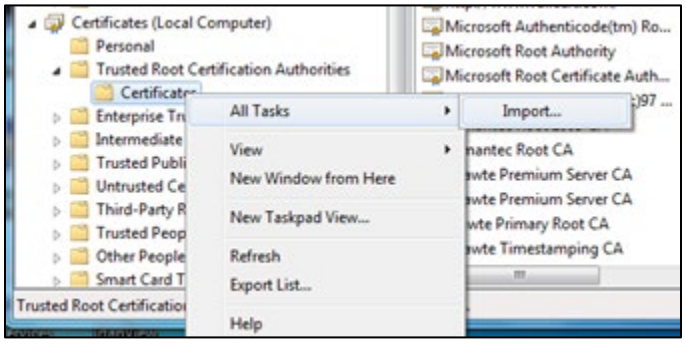
Import Certificates in Computer Account Certificate Store

Back in the Console1 window there will be three new entries under the Console Root folder in the left panel that corresponds to the certificate snap-ins you just created.

1. Expand the Certificates (Local Computer) entry under the Console Root entry.
2. Expand the Personal and Trusted Root Certificate folders. Each of these folders has a Certificates folder within.

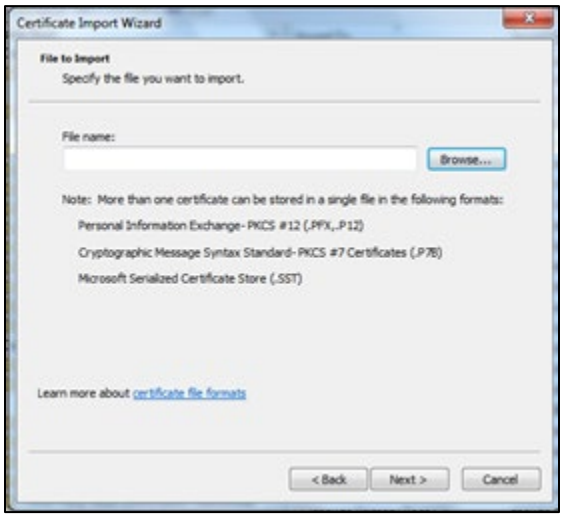


3. Check for any old UTG certificates in each of the folders and delete them.
4. Right-click the Certificates folder.
5. Select **All Tasks** from the menu.

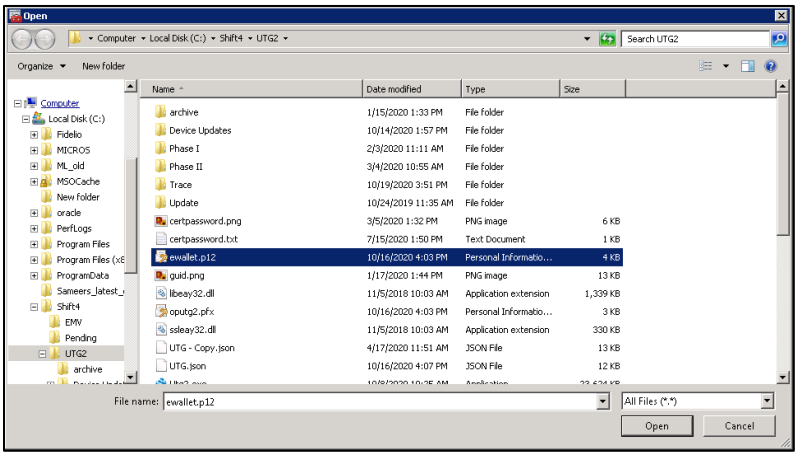


6. Select **Import**. The Certificate Import Wizard displays.

7. Press the **Next** button. The File to Import wizard panel displays.

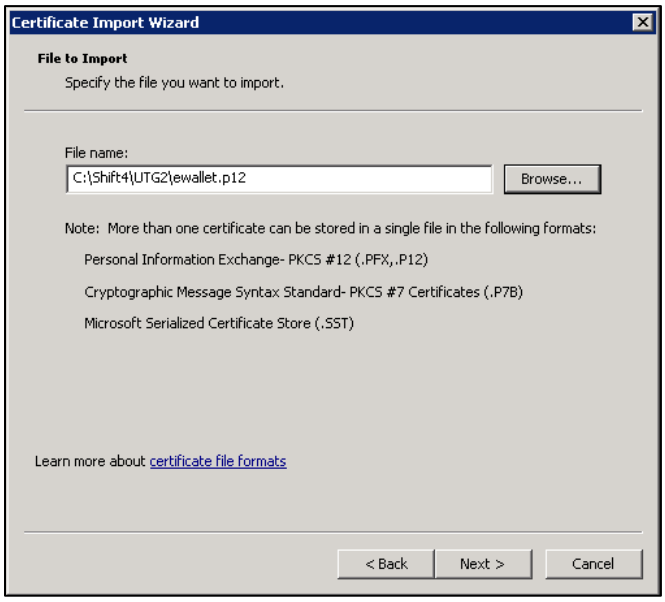


8. Press the **Browse** button. The Open dialog window appears.
9. Navigate to the folder where you saved the certificate files.
10. Click on the drop-down arrow in the Files type selection box and change it to **ALL files (*.*)**
11. The certificate files will now be visible in the file window.
12. Select the client certificate file ewallet.p12.

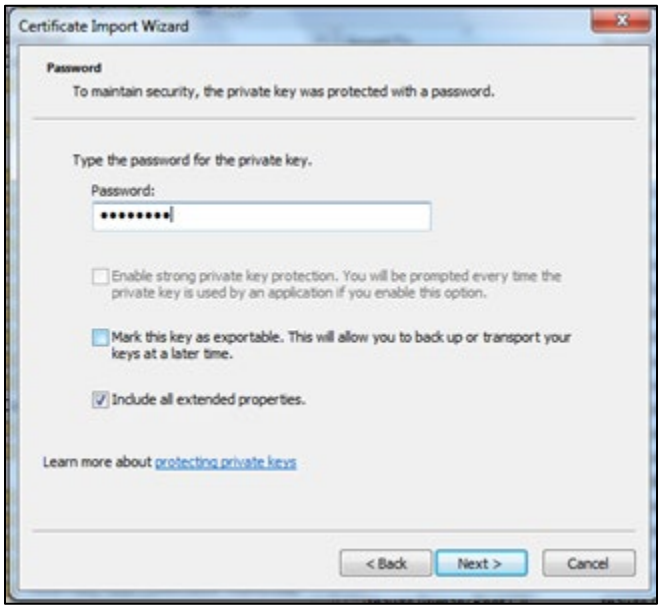


13. Press the **Open** button. The Open file dialog window closes.

14. The path to the file now appears in the File name field in the Certificate Import Wizard.

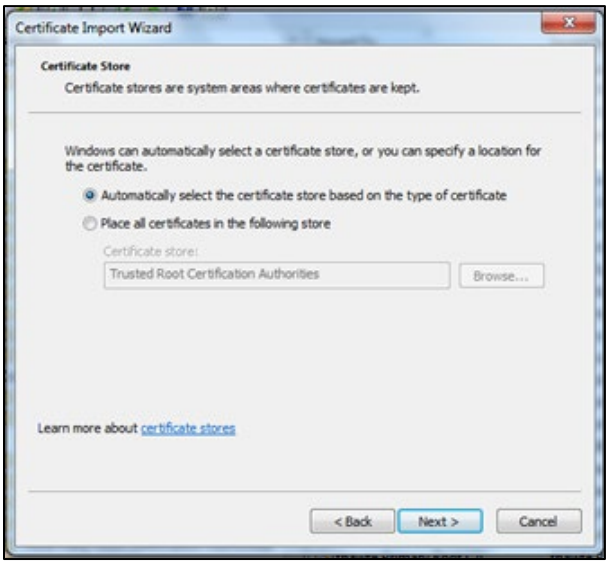


15. Press the **Next** button. The Password wizard page displays.



16. Enter the password. (Remember that the password is case-sensitive.)

17. Press the **Next** button. The Certificate Store wizard page displays.

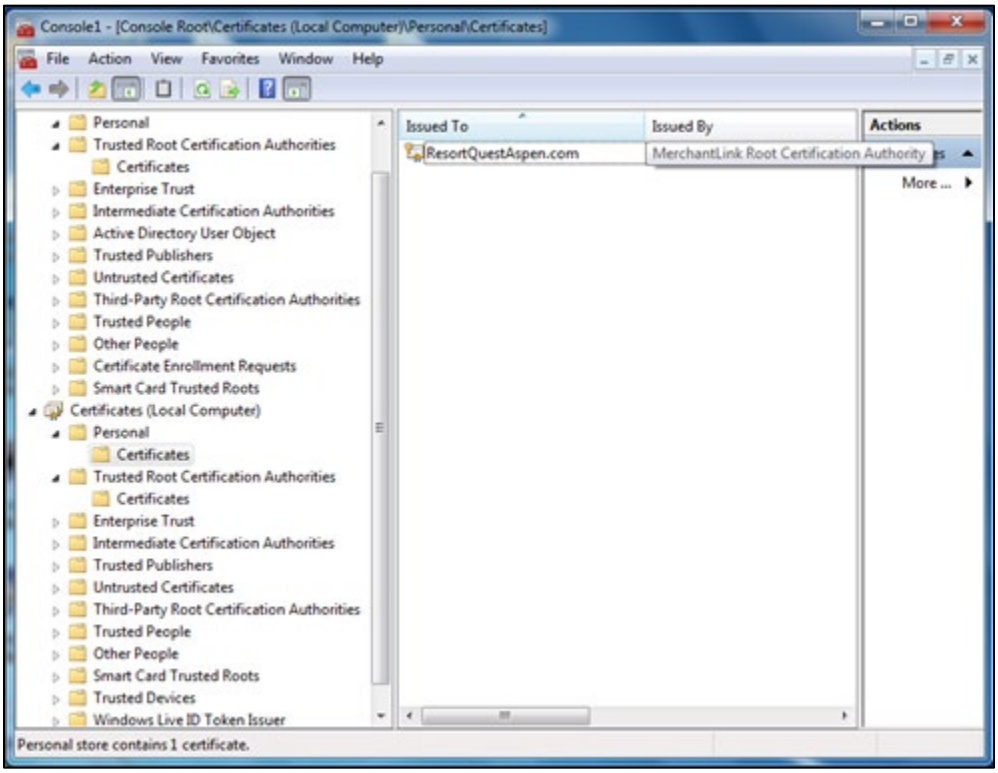


18. For service accounts, please select Place all certificates in the following store. For others please select Automatically select the certificate store based on the type of certificate.
19. Press the **Next** button. The Completing the Certificate Import Wizard page is displayed with a summary of the work done.
20. Press the **Finish** button. A dialog window will display stating **The import was successful**. Click **OK**.

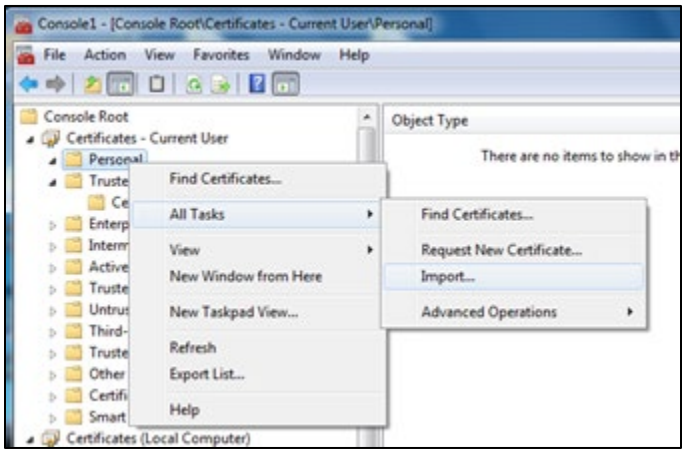
Import Certificates in User Certificate Store

21. Expand the Certificates – Current User entry in the Console Root window.
22. Expand the Trusted Root Certification Authorities and the Personal folders under the Certificates – Current User entry.
23. The Certificates folder displays only under the Trusted Root Certification Authorities folder. (Steps follow to add the certificates folder to the Personal folder below).

24. Repeat steps 1 - 20 in the section entitled *Import Certificates in Computer Account Certificate Store* –in the Certificates folder under Certificates – Current User.

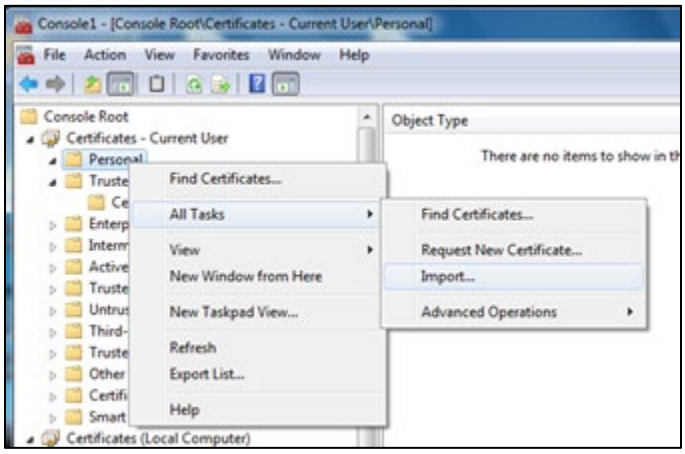


25. Right click the Personal folder under the Certificates – Current User entry.
26. Select **All Tasks** from the menu.
27. Select **Import** from the options on the next menu. The Certificate Import Wizard displays. Repeat steps 1 - 19 in the section above entitled *Installing Certificates in OPERA Workstations and Services*.



Import Certificates in Service Certificate Store

28. Expand the Certificates - Service (<service name>) on Local Computer entry in the Console Root window.
29. Expand the Trusted Root Certification Authorities and the Personal folders under the Certificates - Service (<service name>) on Local Computer entry.
30. The Certificates folder displays only under the Trusted Root Certification Authorities folder. (Steps follow to add the certificates folder to the Personal folder below).
31. Right click the Personal folder under the Certificates – Service (<service name>) entry.
32. Select **All Tasks** from the menu.
33. Select **Import** from the options on the next menu. The Certificate Import Wizard displays. Repeat steps 1 - 20 in the section above entitled *Import Certificates in Computer Account Certificate Store*.



NOTE: Please select Place all certificates in the following store in the Certificate Store step

Verify Certificates Are Installed in Certificate Stores

To view the loaded certificates, you may need to right click each Certificates folder and press Refresh from the menu. Ensure that each location below has an entry for the certificate:
Console Root

a. Certificates – Current User
    i. Personal
        1. Certificates
    ii. Trusted Root Certificate Authorities
        1. Certificates
b. Certificates (Local Computer)
    i. Personal
        1. Certificates
    ii. Trusted Root Certificate Authorities
        1. Certificates

c. Certificates - Service (<service name>) on Local Computer

i. Personal

1. Certificates

34. Save your work by selecting **File** from the menu.
35. Select **Save** from the menu.
36. Close the Console1 window.

Installing Certificates in Oracle Database Wallets

Overview

OPERA uses Oracle database as backend. The certificates have to be installed in the Oracle Database Wallets for it to properly communicate with UTG.

This wallet is normally used to do the following transactions.

- Additional authorizations
- CC final on checkouts
- Authorizations on tokens
- End of day (Batch Close) transactions

Version and Interface differences

The location of wallet has changed over the years based on the type of interface used. Normally the wallet is located in the following locations.

Interface	**Wallet Location**	**Password**
Classic CCW (Non vaulted)	D:\oracle\admin\OPERA\wallets	Application Settings > General > Settings > Default Wallet Password
UTG & LTV (Vaulted)	• Non cluster: D:\oracle\admin\OPERA\wallets\<Product Code>\<Resort Code> • Cluster: D:\oracle \admin\<Cluster Node>\wallets\<Product Code>\<Resort Code>	• For OPERA 5.5.20 and lower, password is located in Application Settings > IFC > Settings > Wallet Password • For OPERA 5.5.20 and higher, password is located in Configuration > Setup > Property Interfaces > Interface Configuration > <Select the interface> > click Edit > Navigate to Custom Data Tab > Wallet Password

Terminology

Product Code = It is the product code of the interface in the interface configuration of OPERA.

Cluster Node = Database cluster node, found in RAC environments.

Resort Code = Site code.

Steps to replace the certificates in OPERA database

The steps for certificates are similar between versions of OPERA, but the location of the wallet and password could differ as noted in the previous section.

1. Create wallet folder location on the database server.

D:\Oracle\admin\OPERA\wallets\S4O\<RESORT>\

2. Copy ewallet.p12 generated earlier to the folder above.
3. Make an auto login file (cwallet.sso).
    a. You can do this with the Oracle Wallet Manager, but make sure you are using the correct version of the Wallet Manager that matches your database version.
        i. Open Oracle Wallet Manager
        ii. Make sure the version of the Wallet Manager matches the database. You can do this by going to **Help > About**.
        iii. Click **Wallet > Open**. If you get a prompt stating that the default wallet folder does not exist, press **Yes** to continue.
        iv. Browse to the wallet folder location. (See *Version and Interface Differences* section for location)
        v. Type in the wallet password, and click **OK**.
        vi. Click File > Auto Login
        vii. Click File > Save
    b. You can also run the following command in the administrative command prompt for 11.2.0.4:
    D:\ORACLE\1120\bin\orapki wallet create wallet
    D:\Oracle\admin\OPERA\wallets\S4O\<resort>\ewallet.p12 -pwd <password> -auto_login
4. Update the security permission of the files. You can run the following command in the administrative command prompt:
    cacls D:\oracle\admin\Opera\wallets\S4O\<RESORT>*.* /e /g everyone:f
5. Update the password in OPERA.

Extra Steps to Import Other Certificates in Database Wallet

It might be required to import additional certificates into the database wallet. This database wallet is used by the database to communicate with other interfaces and systems.

To import a certificate into the wallet, either use the Oracle wallet manager or the orapki tool.

1. Open Oracle Wallet Manager.
2. Make sure the version of the Wallet Manager matches the database. You can do this by going to **Help > About**.
3. Click **Wallet > Open**. If you get a prompt stating that the default wallet folder does not exist, press **Yes** to continue.

4. Browse to the wallet folder location. (See *Version and Interface Differences* section for location)
5. Type in the wallet password, and click **OK**.
6. Click on **Operations > Import Trusted Certificate**.
7. Browse to the certificate and click **OK**.
8. Click **OK** again to close the dialog box.
9. Update security permission of the wallet by running the following command in an administrative command prompt.

cacls D:\oracle\admin\Opera\wallets\S4O\<RESORT>*.* /e /g everyone:f

Configuring OPERA

Stop Extra Services

It will be necessary to stop extra OPERA interfaces at this point. These are normally installed as services on their respective servers. Some examples of interfaces are,

- OXI interfaces: these are named as OPERA Interface for <Interface Name>
- OEDS interfaces: these services have OAP or OWS prefix

NOTE:

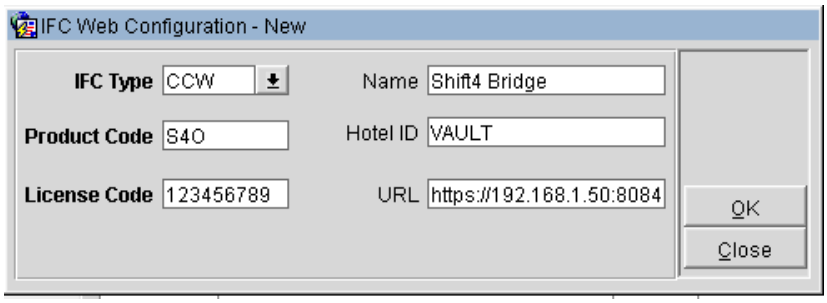
- Make a note of the services stopped so that they can be started.
- Some OEDS services have to be started in certain order. Look for start and stop scripts on desktop.

Create CCW Interface

1. Open Configuration from the OPERA login screen.

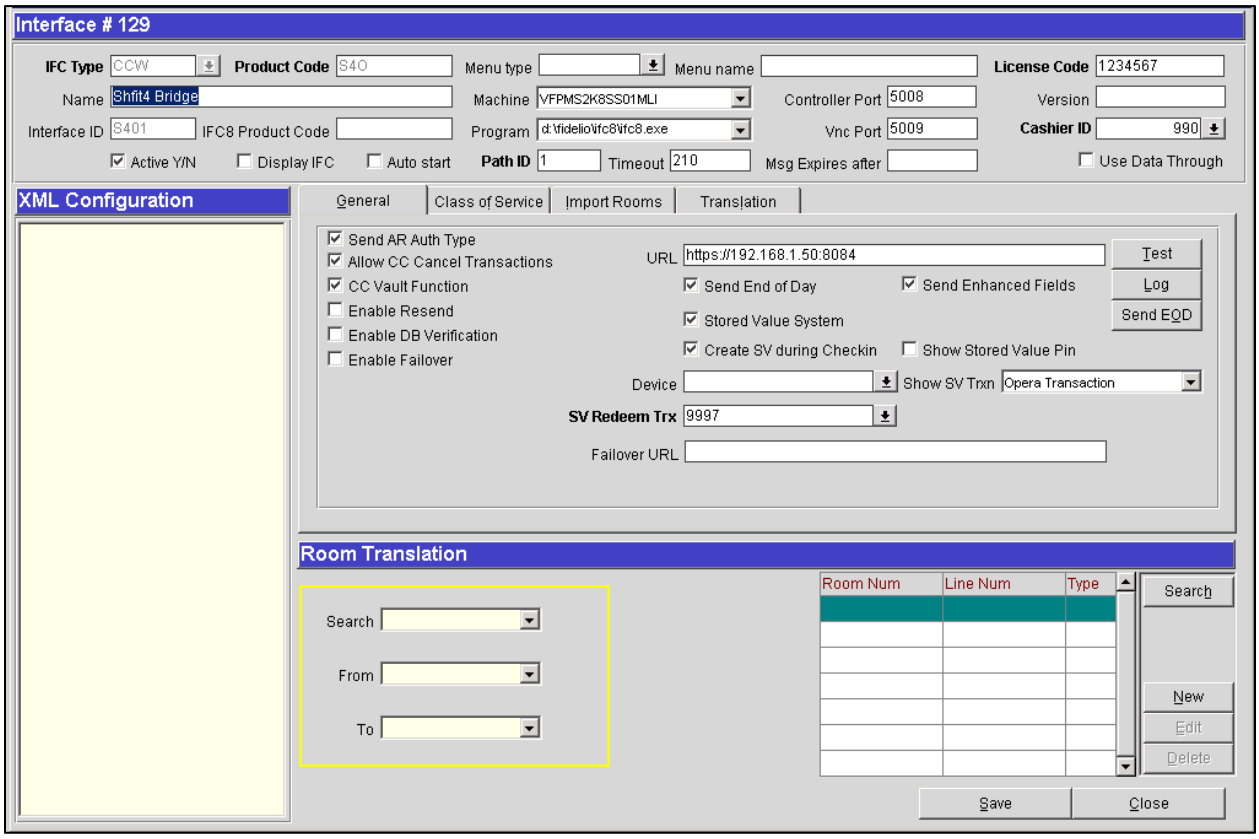
2. Go to Setup > Property Interfaces > Interface Configuration

3. Disable any current CCW Interface.
    a. Select the interface.
    b. Click on **Edit**.
    c. Uncheck **Active**.
    d. Click **Save**
    e. Click **Close**.
4. Click **New** and fill out the information as follows and click **OK**.
    a. IFC Type: CCW
    b. Name: Shift4 Bridge
    c. Product Code: S4O
    d. License code: any number
    e. Hotel ID: Same as found under “Credit Card Configuration Setup”
    f. URL is always the IP and port of the UTG. For example, https://10.96.111.35:8084



5. Make a note of the Interface Number on the top left side.
6. Further configure the interface
    a. Increase the timeout to 190 or higher.
    b. Click on the drop down for Machine and select an Interface Server.
    c. Select **Send AR Auth Type**.
    d. Select **Allow CC Cancel Transactions**.
    e. Select **Enable Resend**.
    f. Select **CC Vault Function**.
    g. Select **Send End of Day**.
    h. Select **Send Enhanced Fields**.
    i. Select **Stored Value System** if site is using Shift4 gift card.
    j. Select **Create SV during Checkin** if site is using Shift4 gift card.

k. Select **SV Redeem Trx** if site is using Shift4 gift card.



NOTE: Make a note of the Interface Number on the top left side of the interface.

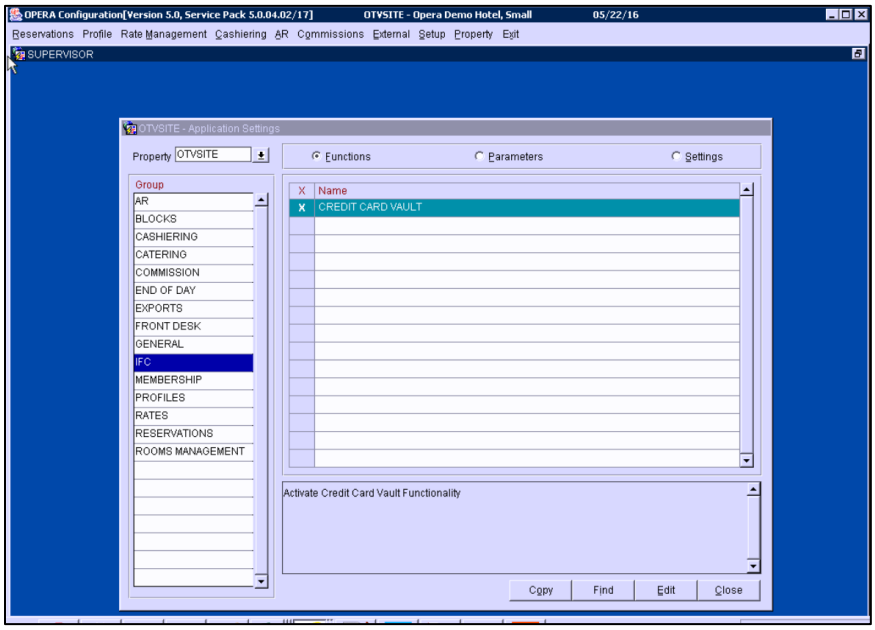
Application Settings

1. Go to **Setup > Application Settings**.

Credit Card Vault

This step could be different depending on the version of OPERA.

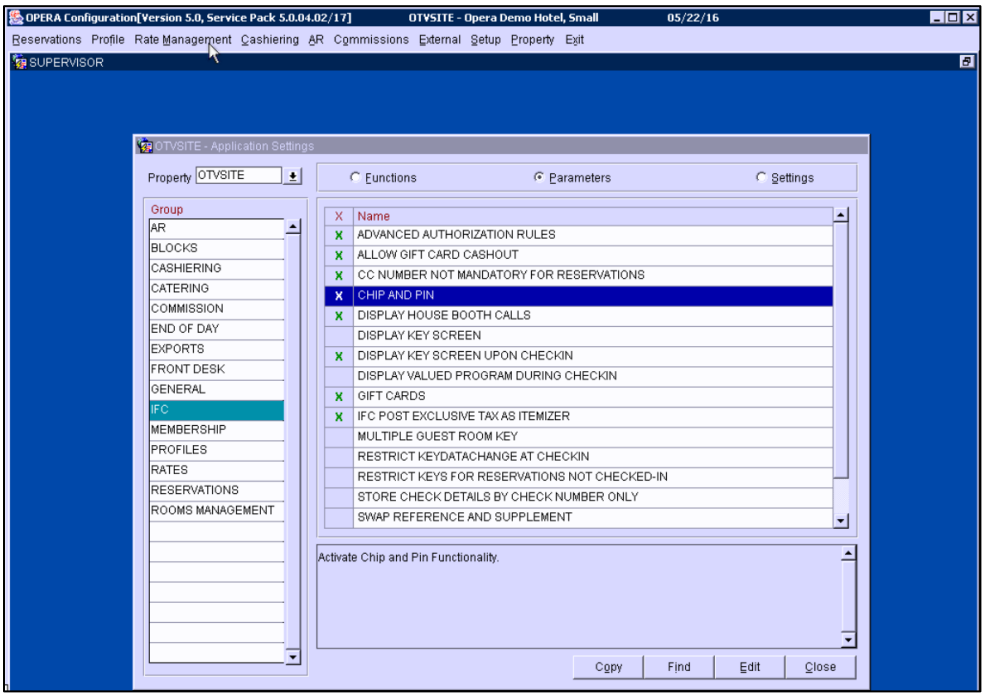
1. Navigate to **IFC > Functions > Credit Card Vault**.
2. Click **Edit**.



3. Select **Y**.
4. Click **OK**.

Chip and Pin

1. Navigate to **IFC > Parameters > Chip and Pin**.



2. Click **Edit**.
3. Select **Y**.
4. Click **OK**.

Configure Vault Specific Parameters

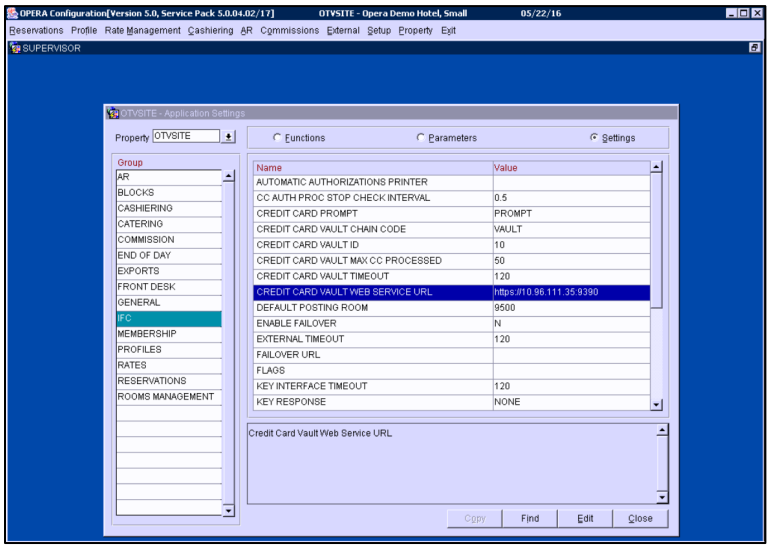
This step can differ depending on the version of OPERA.

- For OPERA 5.4 or lower, this setting is in the application setting
- For OPERA 5.5 or higher, this setting is in the Custom Data tab in the interface configuration

OPERA 5.4

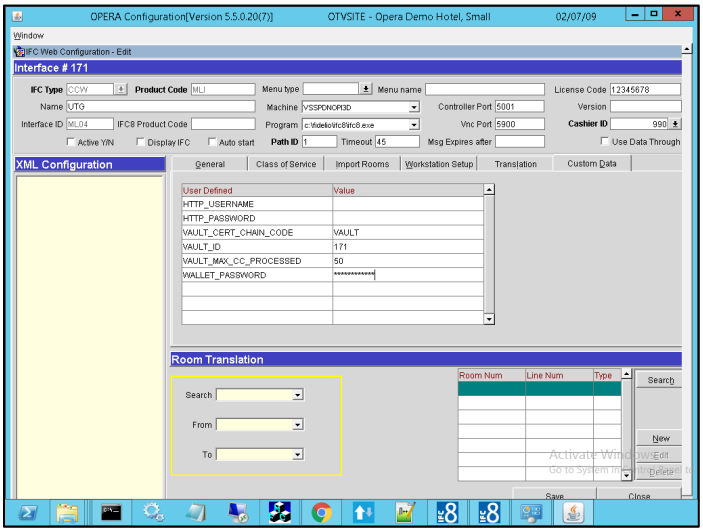
1. Navigate to **IFC > Settings**
2. Configure the settings as noted below.
    a. Wallet Password: <UTG generated password>
    b. Credit Card Vault Chain Code: HOTEL ID
    c. Credit Card Vault ID: <Interface Number>
    d. Credit Card Vault Max CC Processed: 50
    e. Credit Card Vault Timeout: 120 or higher

f. Credit Card Vault Web Service URL: <OPERA API URL and Port>



OPERA 5.5

1. Go to **Setup > Property Interfaces > Credit Card Interface > Interface Configuration**.
2. Select the UTG interface and click **Edit**.
3. Click **Custom Data** tab.
4. Configure the settings as noted below.
    a. VAULT_CERT_CHAIN_CODE: HOTEL ID
    b. WALLET_PASSWORD: <UTG generated password>
    c. VAULT_ID:<Interface number seen on the top left side>
    d. VAULT_MAX_CC_PROCESSED: 50

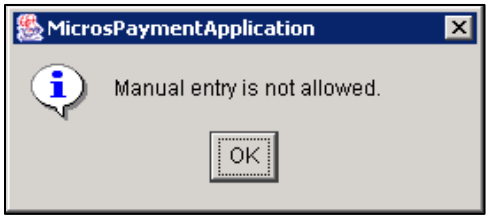


5. Click **Save**.

Disable Manual Entry

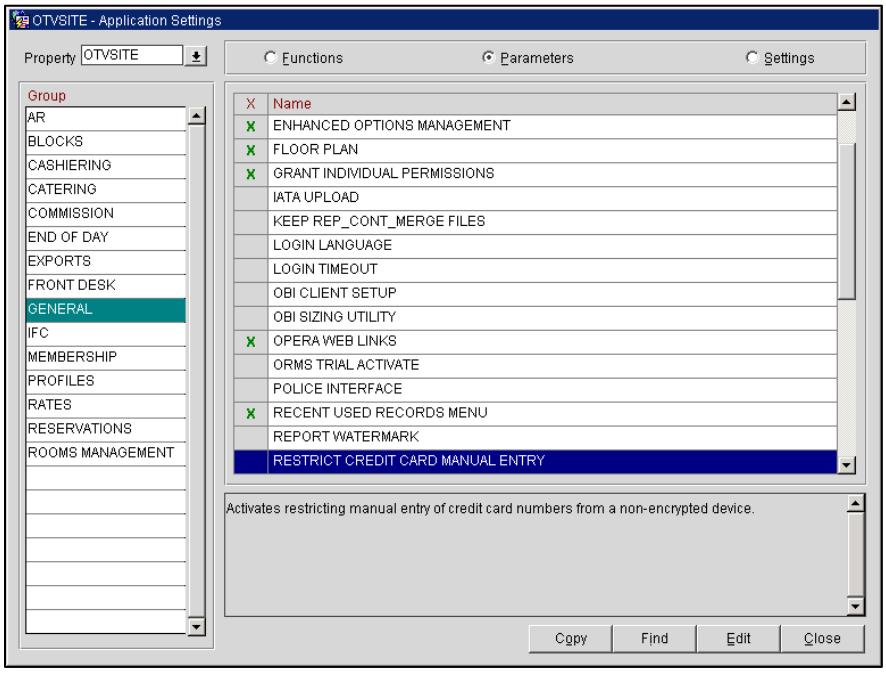
The hotel can disable manual entry of the credit card in the OPERA application and only use the EMV pin pad device or other P2PE device. They can do so by changing this configuration in OPERA.

Users will be greeted with the following dialog box if the card is manually entered.



To disable manual entry please follow the steps below,

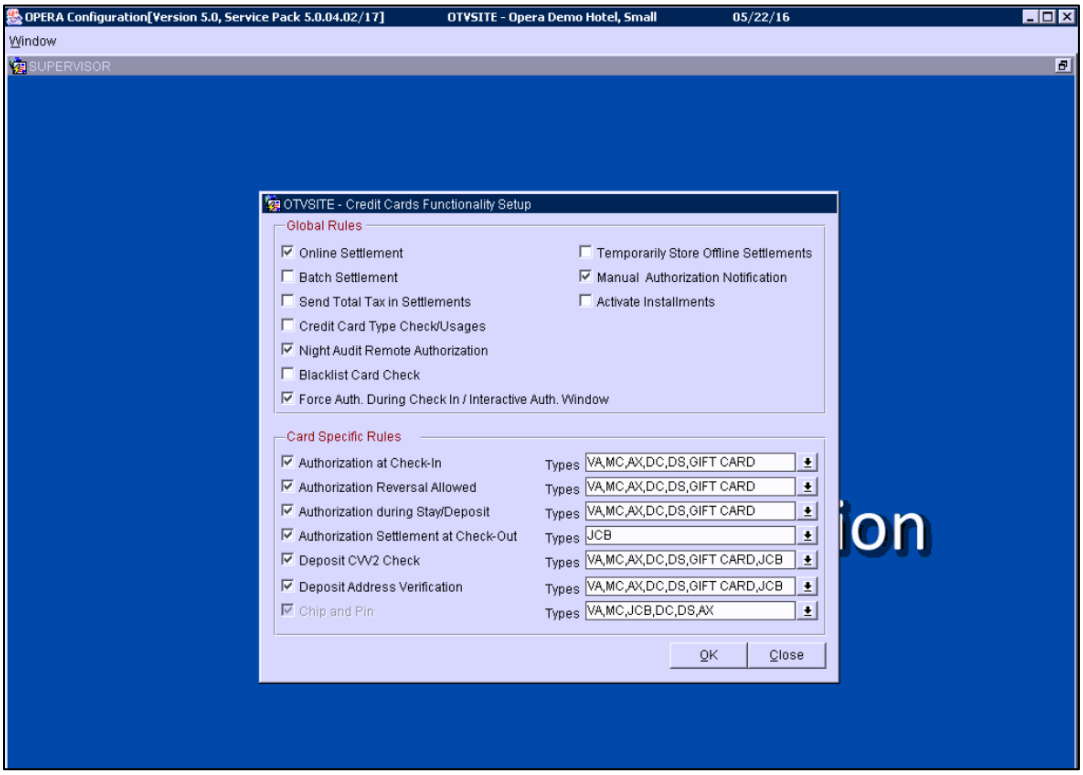
1. Go to **Setup > Application Settings**.
2. Go to **General > Parameters > Restrict Credit Card Manual Entry**.



3. Click **Edit**.
4. Select **Y**.
5. Click **OK**.

Credit Card Functionality Setup

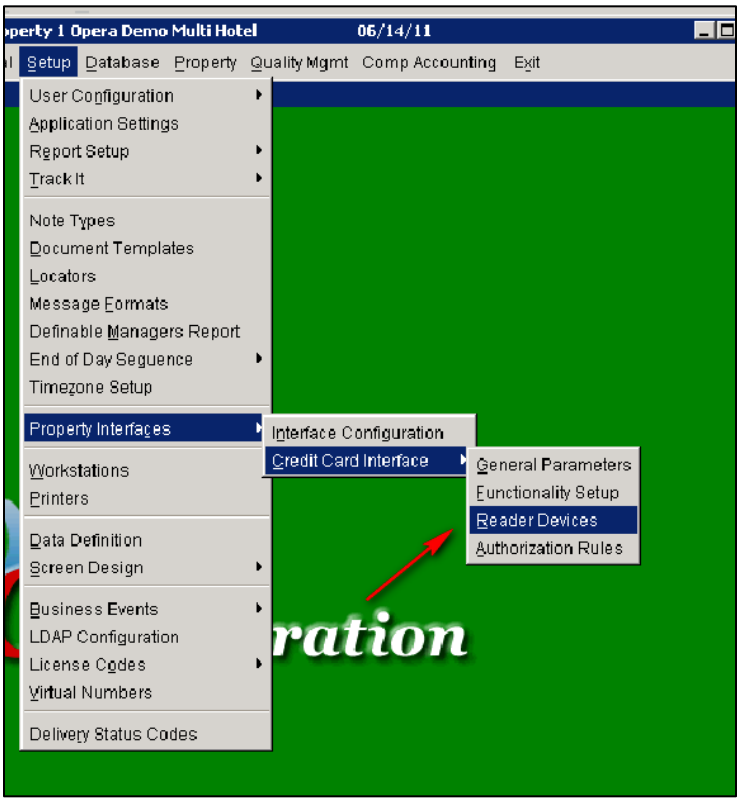
1. Login to OPERA Configuration
2. Go to **Setup > Property Interfaces > Credit Card Interface > Functionality Setup**.
    a. Select **Online settlement**.
    b. Select **Manual Authorization Notification**.
    c. Select **Force Auth. During Check In / Interactive Auth. Window** to only allow check in if there was a successful authorization.
    d. Select drop down for **Chip and Pin** and select all the cards you want to configure for pin pad transaction and Click **OK**.



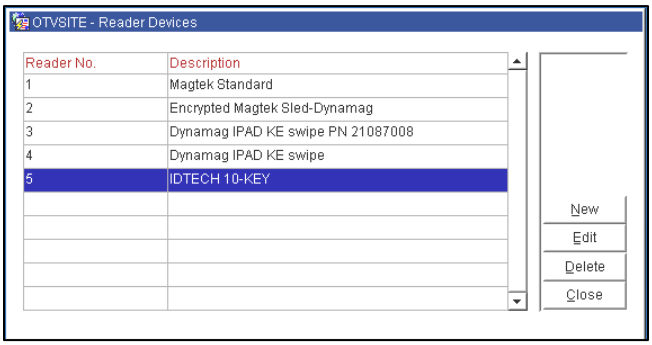
    e. Select drop down for **Authorization Reversal Allowed** and select all card types and click **OK**.

IDTECH swipe installation instructions

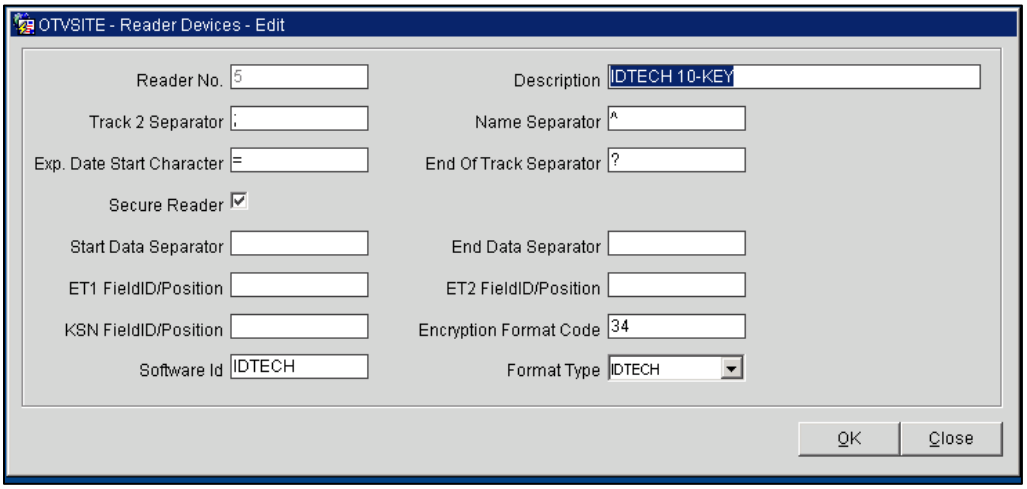
1. Login to OPERA Configuration
2. Navigate to the **Setup->Property Interface->Credit Card Interface->Reader Devices**



3. Click the **NEW** button



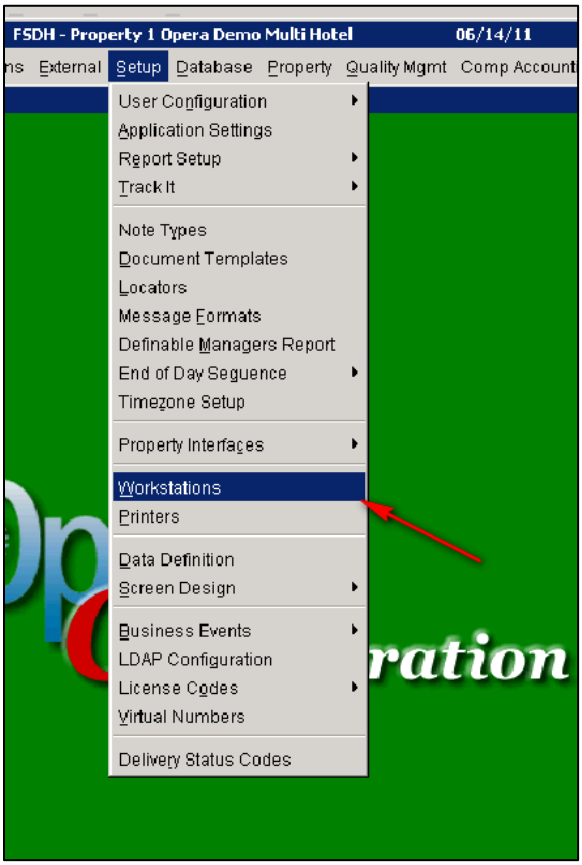
4. Then populate the form per the swipe requirements
    a. Reader No. – Next available reader #
    b. Description – name of swipe
    c. Track 2 separator - ;
    d. Exp. Date Start character - =
    e. Name Separator - ^
    f. End of Track Separator - ?
    g. Secure Reader – Check the box
    h. Start Data Separator – (leave blank)
    i. End Data Separator – (leave blank)
    j. ET1 Position – (leave blank)
    k. ET2 Field Position – (leave blank)
    l. KSN Field Position – (leave blank)
    m. Encryption Format Code – 34
    n. Software ID – IDTECH
    o. Format Type = IDTECH



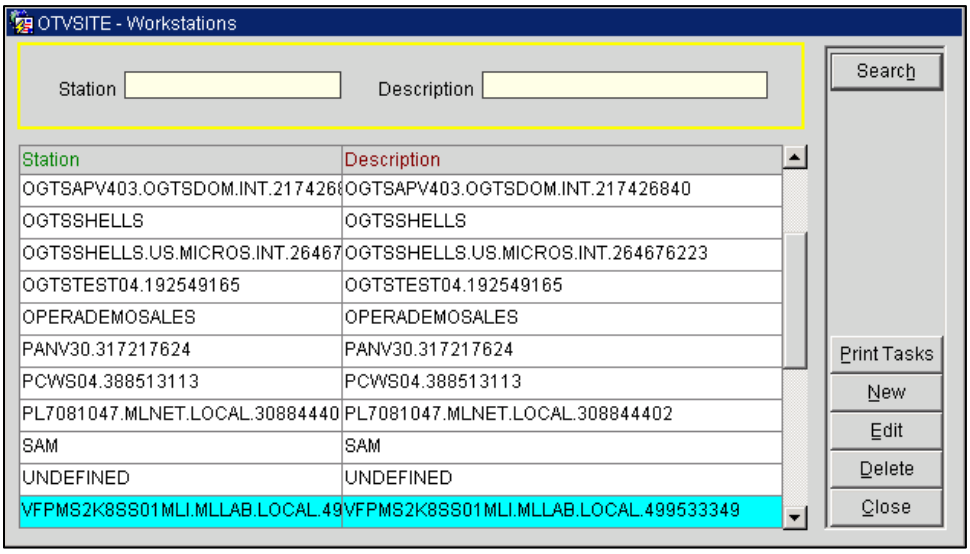
5. Click **OK** to save and close.
6. Click **Close** to close reader configuration.

Workstation Setup

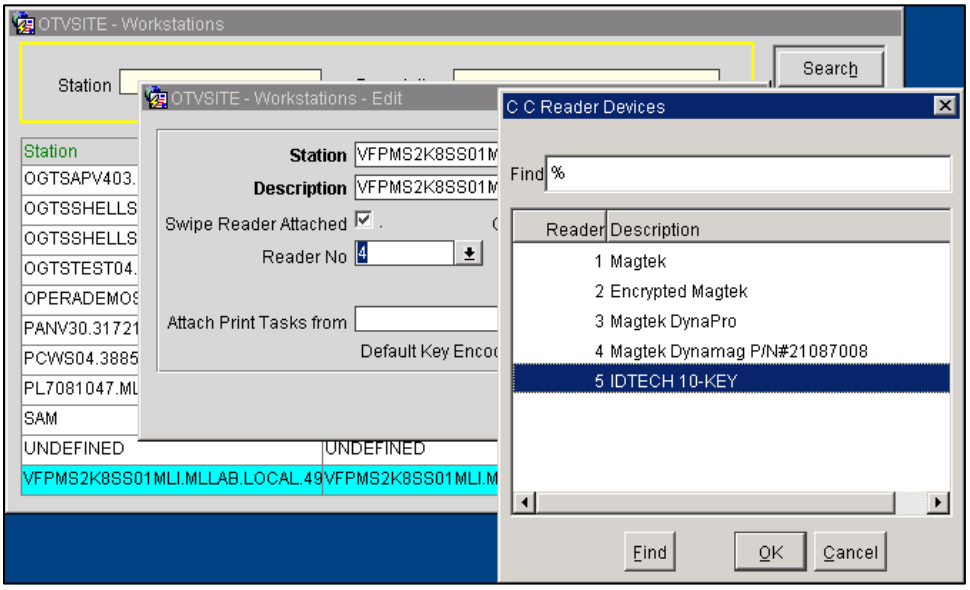
1. Click **Setup > Workstations**.



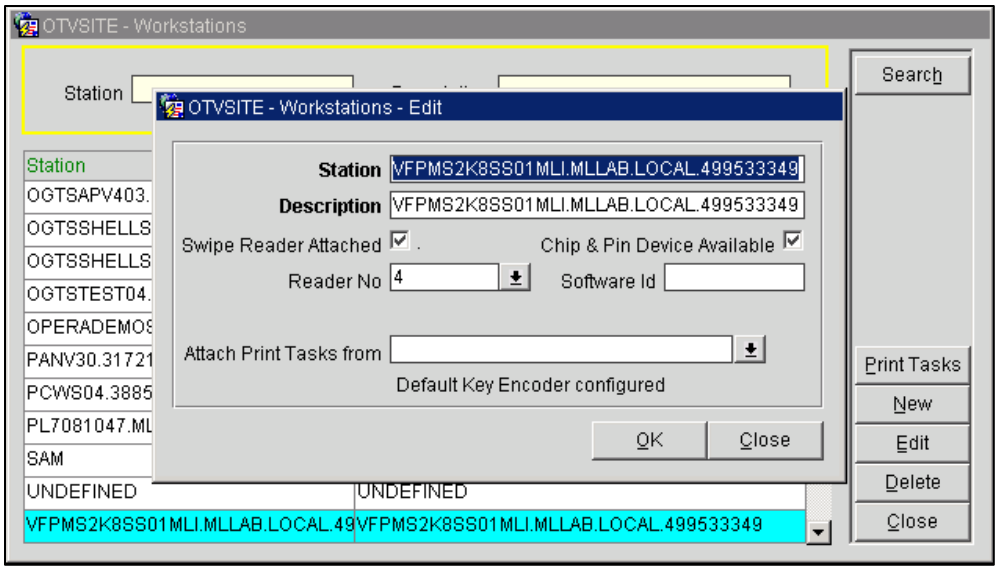
2. Select the workstation and click on **Edit**.



3. If the workstation also has an IDTECH device, select Swipe Reader Attached and click the drop down for Reader No, then select IDTECH and click **OK**.



4. If the workstation has EMV pin pad, select **Chip & Pin Device Available**.



5. Click **OK**.
6. Repeat the above steps for all workstations that need configuration.
7. Click **Close** to close out of Workstations.
8. Install the UTG certificate as noted in the certificate installation step.

Install DLL

For WS,

OPERA 5.5 or higher, the easiest way to reinstall this file is to install the OPERA Jinitcheck addon as administrator. It can be downloaded by navigating to the URL below on a WS.

1. Navigate to, https://<OPERAURL>/InstallJinitCheck.exe.
2. Save and run as administrator.

OPERA 5.4 or lower, check if the dll is located in the following location. Copy it from D:\Micros\Opera\Tools\Vault folder on the server if needed.

- C:\Program Files\Oracle\jinitiator 1.3.1.25\bin

For OXI, this DLL will need to be manually copied to the OXI binary folder. The DLL is located in D:\Micros\Opera\Tools\Vault folder on the server.

NOTE: In a 64-bt OS you will need to use a combination of the 32-bit DLL and the 64-bit DLL in specific locations on the OXI Server, as different components have different requirements. You MUST put the correct dll in the right location because 64-bit programs cannot load 32-bit DLLs and vice versa.

32-bit Java Library Locations

- C:\Windows\system32
- C:\Windows
- C:\Windows\System32\wbem

- C:\Windows\System32\WindowsPowerShell\v1.0
- D:\ORA\1120client\BIN (default 32-bit Oracle Application Server Home)
- C:\Program Files (x86)\Micros-Fidelio\OXChange\OXA

64-bit Java Library Locations

- D:\ORA\MWFR\wlserver_10.3\server\native\win\x64
- D:\ORA\MWFR\wlserver_10.3\server\bin
- D:\ORA\MWFR\modules\org.apache.ant_1.7.1\bin
- D:\ORA\JDK\jre\bin
- D:\ORA\JDK\bin
- D:\ORA\MWFR\11gappr2\BIN
- D:\ORA\MWFR\11gappr2\opmn\bin
- D:\ORA\MWFR\11gappr2\opmn\lib
- D:\ORA\MWFR\11gappr2\perl\bin
- D:\ORACLE\1120\BIN (11.2.0.3 DB only, exists only on DB server, applicable only for Single Servers)
- D:\ORACLE\11204\BIN (11.2.0.4 DB only, exists only on DB server, applicable only for Single Servers)

Verifying Chip Transactions and Installation

It is important to run a test transaction after installing the OPERA Bridge. A transaction should be run from a PIN pad and verified in Lighthouse Transaction Manager as “Card Present.”

The following transactions should be run and confirmed during the installation:

- Get Token (adding a card to a reservation)
- Authorization
- Settlement

Bulk Tokenization

It will be necessary to convert the current credit cards in the OPERA system to tokens. This is done by the bulk tokenization process.

To do a bulk tokenization, please follow the steps below. These steps might be different depending on the version of OPERA.

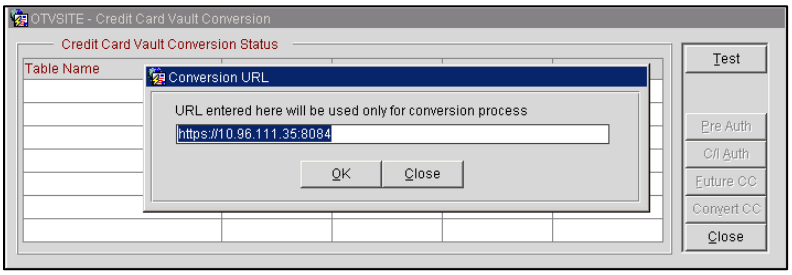
Check and Backup Table

1. Count number of cards to be tokenized in name$_credit_card table.
   select count(1)
   from name$_credit_card
   where purged_yn = 'N'
   and credit_card_number like '~%';

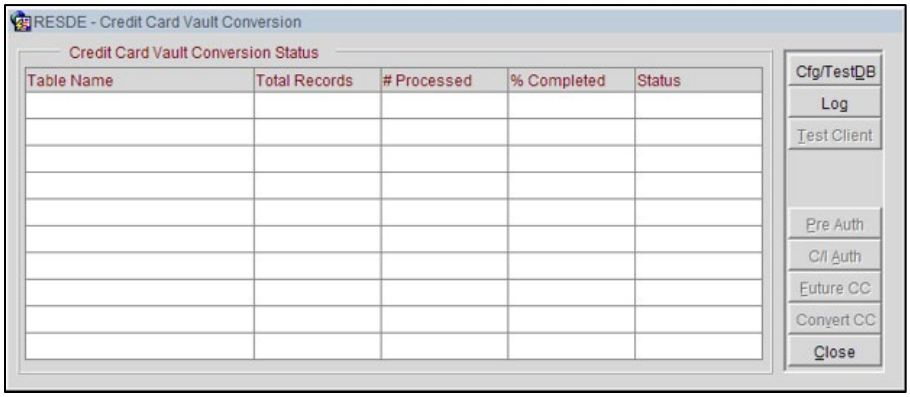
2. Backup the name$_credit_card table by running the following as OPERA database user.
   create table name$_credit_card_backup as select * from name$_credit_card;

Conversion

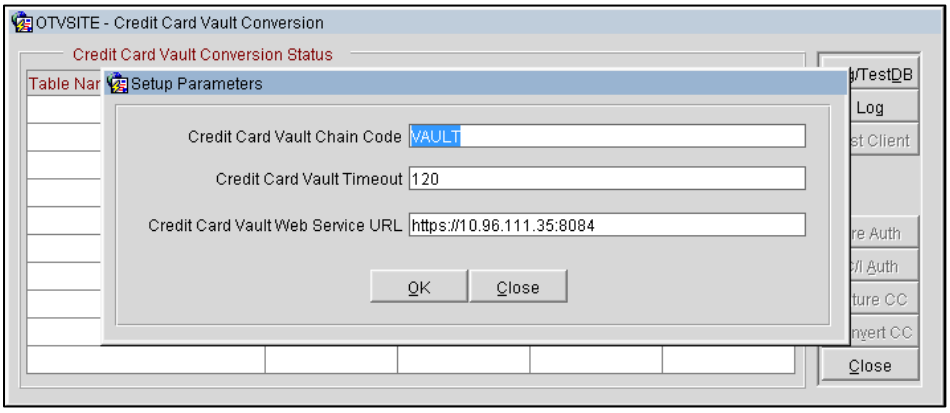
3. Log in to OPERA as manager or supervisor.
4. Click on **Utilities**.
5. Select the resort and click on **Login**.
6. Click on **Utilities > Convert Vault CC Information**.
7. Click **OK**.
   a. For OPERA 5.4,
      i. Click **Test**.
      ii. OPERA will ask to verify the URL, click **OK**.



      iii. OPERA will run a heartbeat test. If everything works it will show Passed.
   b. For OPERA 5.5,
      i. Click **Cfg/TestDB**.

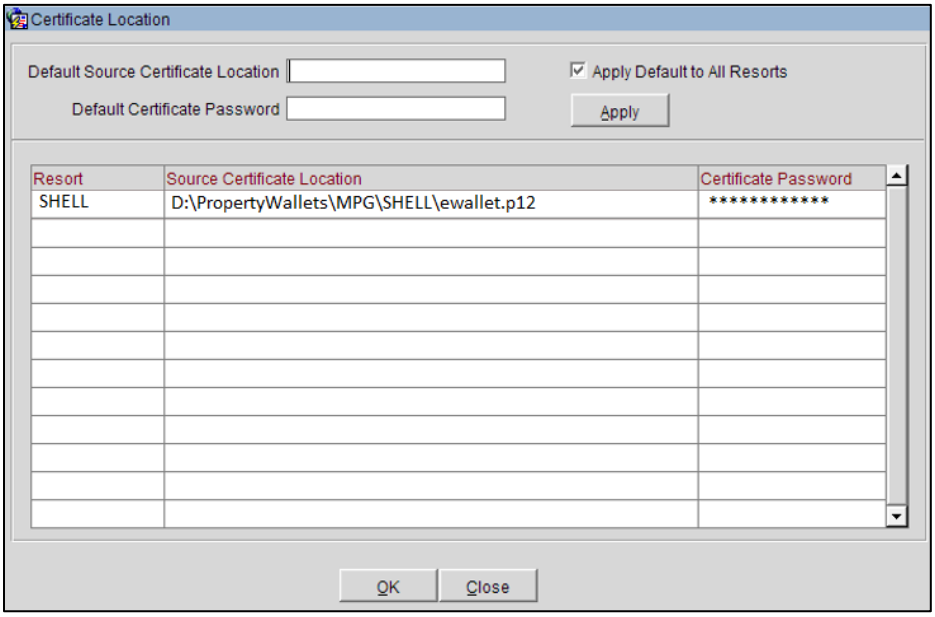


      ii. OPERA will pull the information from the configuration done previously and ask you to confirm it. Click **OK**.



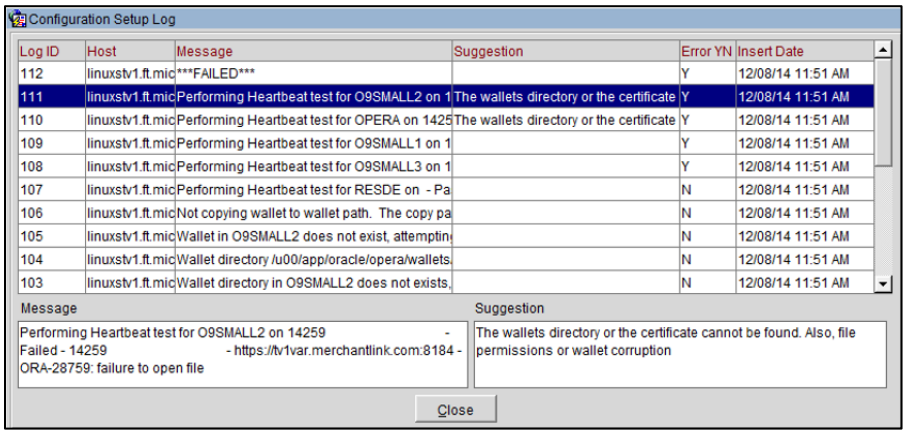
iii. Type in the default source certificate location (default: D:\Oracle\Admin\Opera\Wallets) and the certificate password, and click **Apply**.

NOTE: For multi property uncheck the Apply Default to All Resorts and type in the certificate location and password below.

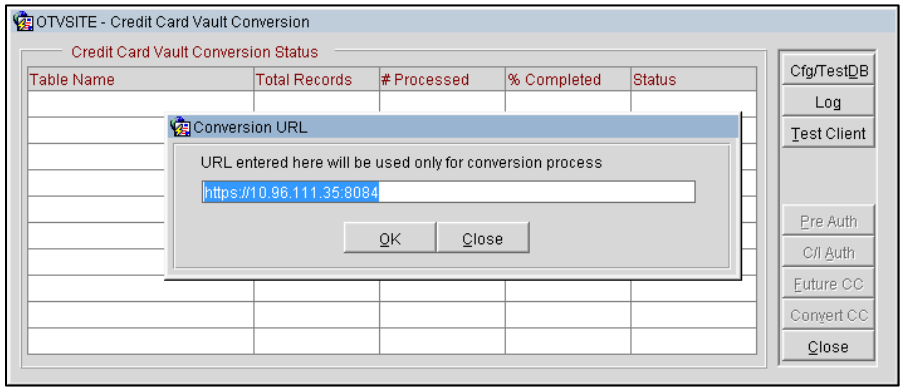


iv. Click **OK** to start configuration.
v. Opera will configure the ACL and show the dialog box below, click **OK**.

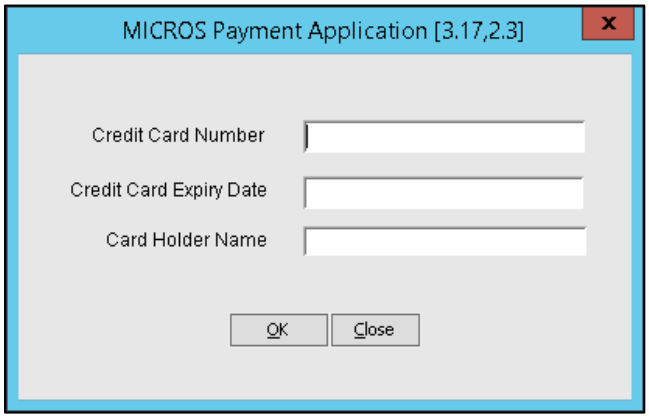
vi. You can click on the Log button to check for any errors.



vii. Click on **Test Client**.
viii. Click **OK** to confirm the URL.



ix. MICROS Payment Application will open. Type in credit card information and click **OK**.



x. OPERA will run a tokenization test and return Passed if successful.

8. If Pre-Authorization is enabled, click on **Pre Auth**, this will initiate a pre authorization for currently pre-authorized reservations.
9. Click **OK** once it is one.
10. Click on **C/I Auth (Convert In house guests)** to convert credit cards attached to reservations in house currently into tokens.
11. Click **OK** once it is done.
12. Let site know that they can resume regular operation at this time, but they will not be able to process future credit cards.
13. Click **Convert CC** to convert the rest of credit card data to tokens.
    NOTE: If the hotel is large with lots of credit card data (name$_credit_card table exceeds 700000 records), please run the Future CC and select the resort and arrival date in future you want to convert.
14. Click **Yes** when it prompts Have you done the Pre Auth and C/I Auth transactions?
15. Click **Yes** when it prompts This will start converting the Credit Card Data. Do you want to proceed?
16. Click **OK** when Conversion is complete dialog box shows.
17. If tokenization is successful drop backup table by running the following command as OPERA database user. If there are failed tokenizations please escalate
    drop table name$_credit_card_backup

Start Extra Services

Start all the extra OPERA interfaces that were stopped earlier. These are normally installed as services on their respective servers. Some examples of interfaces are:

- OXI interfaces: these are named as OPERA Interface for <Interface Name>
- OEDS interfaces: these services have OAP or OWS prefix

NOTE:

- Double check that the services stopped earlier are started.
- Some OEDS services have to be started in a certain order. Look for start and stop scripts on desktop.

Appendix A: Installation Troubleshooting

Oracle Database Errors

ORA-28759: failure to open file

The wallets directory or the certificate cannot be found. Check the location of the ewallet.p12. Make sure that it is in the correct folder. Also double check that the wallet has FULL CONTROL for EVERYONE permissions. Ensure that if S4O product code is in use, the folder used is S4O.

ORA-29106: Cannot import PKCS #12 wallet

The wallet password in Application Settings does not match the password for the wallet. Double check your password and confirm with Shift4 as needed.

ORA-29024: Certificate validation failure

Incorrect wallet password configured in Application Settings for that Resort. Go to **Application Settings > IFC > Settings > Wallet Password** and input the password.

Problem also could be due to incorrect wallet being used. Please double check the wallet.

ORA-29223: Cannot Create Certificate Chain

There was a problem with the packaging of the P12 because the signing certificate is not in the wallet. Contact Shift4 for a new P12 and password.

This can also be fixed by using the Oracle Wallet Manager to import additional root CA from the package provided.

ORA-28860: Fatal SSL Error

An ACL Profile exists but it is not configured. Assign Connection & Use-Client Certificate Privileges and assign the Wallet Path.

Problem also could be due to incorrect wallet being used. Please double check the wallet.

Problem also could be due to protocol error. Double check the Oracle database can support the TLS version.

ORA-53203 Security Violation

Too many attempts were made to access the certificate with the wrong password. You can wait for the lockout to expire or bounce the database.

Network Access Denied by Access Control List

No ACL Profile exists. Contact Oracle to create an ACL Profile, assign Connection & Use-Client Certificate Privileges, and assign the Wallet Path.

WS or OXI Failing Tokenization

Things to check:

1. Make sure the user is using the 32-bit version of IE
2. Check certificates are properly installed.

3. Make sure the cchttplib.dll is installed in proper location. This is automated in the newer versions of OPERA by installing OPERA JinitCheck module. This can be uninstalled from Add/Remove Programs so a new version gets loaded.
4. Check the logs in C:\MICROS and check the errors against knowledge base.
5. Make sure the HOTEL ID matches the O value in the certificate
6. Firewall blocking some part of the process.
7. Enable proper TLS 1.2 protocol if OPERA API is set to use TLS 1.2.

Check Logs

Additional logging is created on the C drive of every PC that has the Payment App open up in OPERA and the OXI server.

The log file is located in the C:\Micros\Logs directory and is named CcVaultYYYYMMDD.xml. The OXI Processor Log viewer can be used to view the log entries.

As a default, the logging will be set to ERROR, displaying only error conditions.

Check CCHttplib.dll file is installed

Check if the cchttplib.dll file is installed in all the locations noted in the DLL install section.

Common DLL errors

No Valid Certificate Found for <VAULT CODE>: Certificate could not be located. Make sure the Organization value (0) value is the HOTEL ID on the certificate.

Failed - Code Mismatch (when reverting back to non-vault environment), correct Hotel ID in Credit Card Interfaces > General Parameters > Hotel ID

ERROR IN DLL – USER CERTOPENSTORE 5 (ACCESS DENIED) or ERROR IN DLL - CERTOPENSTORE : 5 :

(WIN API CALL DID NOT RETURN ERROR TEXT): The OS User on the workstation does not have permission to access the Windows Certificate Store, this is sometimes seen at sites where security is too restrictive. Work with site IT to ensure that OS Users can access the certificate store where the Vault certificate is imported. The certificate permissions can also be changed from Windows Certificate Manager.

HTTPSENDREQUEST : 12157: (WIN API Call did not return error text), error due to certificate incorrectly installed or communication problem.

HTTPSENDREQUEST : 12185: This Window Error code means that the private key is missing or does not match the certificate in the Windows Certificate Store.

HTTPSENDREQUEST – 12186: This Windows Error code means that the private key is installed but the user or application does not have rights to access the private key. You may need to grant elevated permissions to the directory where MachineKeys are stored or you may need to reimport the .pfx and .cer using Run as Admin. Also grant permissions to the certificate for everyone in the certificate manager.

HTTPSENDREQUEST – -2146893016: This not a real Windows Error Code but it indicates a total communication failure. This could occur due to a corrupt certificate or incorrect certificate being imported, OS is not configured for the secure communication with the vendor or a DLL is not found in the location where OXI is looking. To resolve redo, the CcHttpLib.dll implementation, Remove/Reimport Certificates and Implement OS permissions and changes for TLS 1.2 communication.

Check Certificates are installed

Make sure the certificates are installed in the proper location. The Organization "O" value in the certificate must match the CC Vault Chain Code configuration in OPERA.

The steps outlined in installing certificates can be used to check if the certificates are installed.

Appendix B: Using OPERA EMV

Running Card Present Transactions

The main change from the perspective of the hotel staff with OPERA Bridge is how transactions are to be run. Please see the "How to Run Transaction in Opera with UTG" document for those steps.

Check-in from the Reservation Details Screen

There are generally two ways to check guests in Opera PMS.

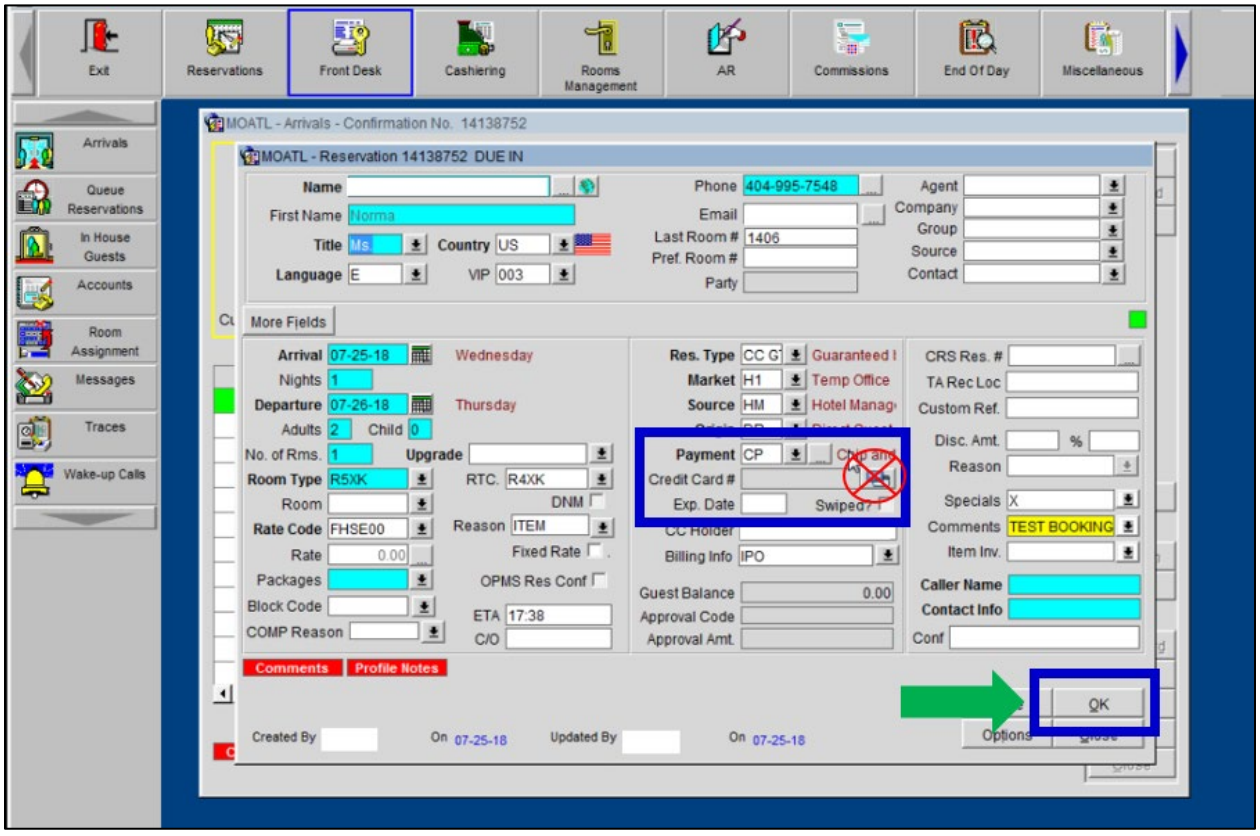
- From the Reservation Details screen and,
- From the Front Desk Arrivals screen.

Step 1 –Setting the Payment Type

- To perform a proper EMV transaction from the reservation details screen, the clerk needs to change the payment to CP (Chip and PIN).
- This can be done from the drop down arrow, or by just typing CP in the window.

Step 2 –Initiating the Chip and PIN Window

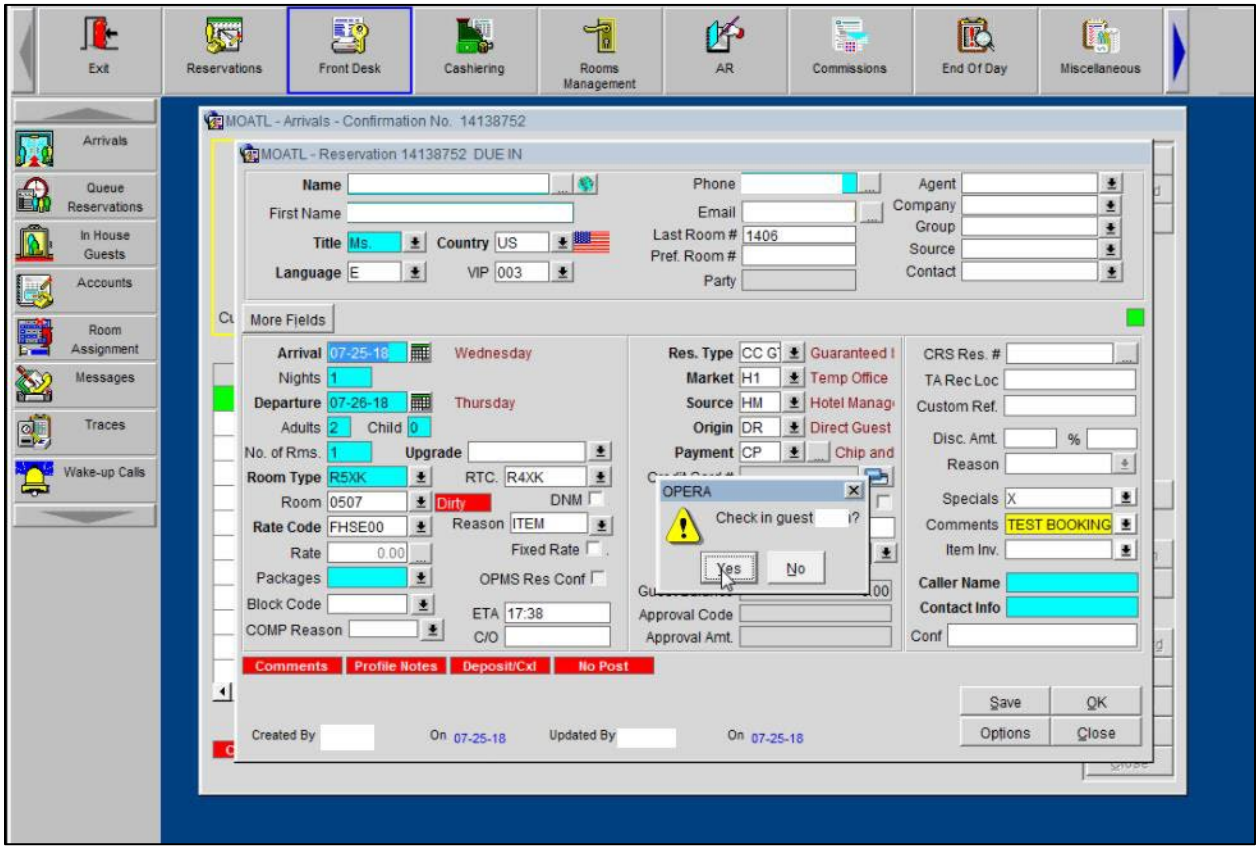
- Once CP is chosen, the credit card on file (usually from the reservation booking) disappears.
- Once the Payment Type has been set to CP, the clerk needs to press the **OK** button at the bottom right of the screen.



- DO NOT PRESS THE PAYMENT APPLICATION ICON TO THE RIGHT OF THE CREDIT CARD # FIELD.

Step 3 –Activating the Payment Method Window

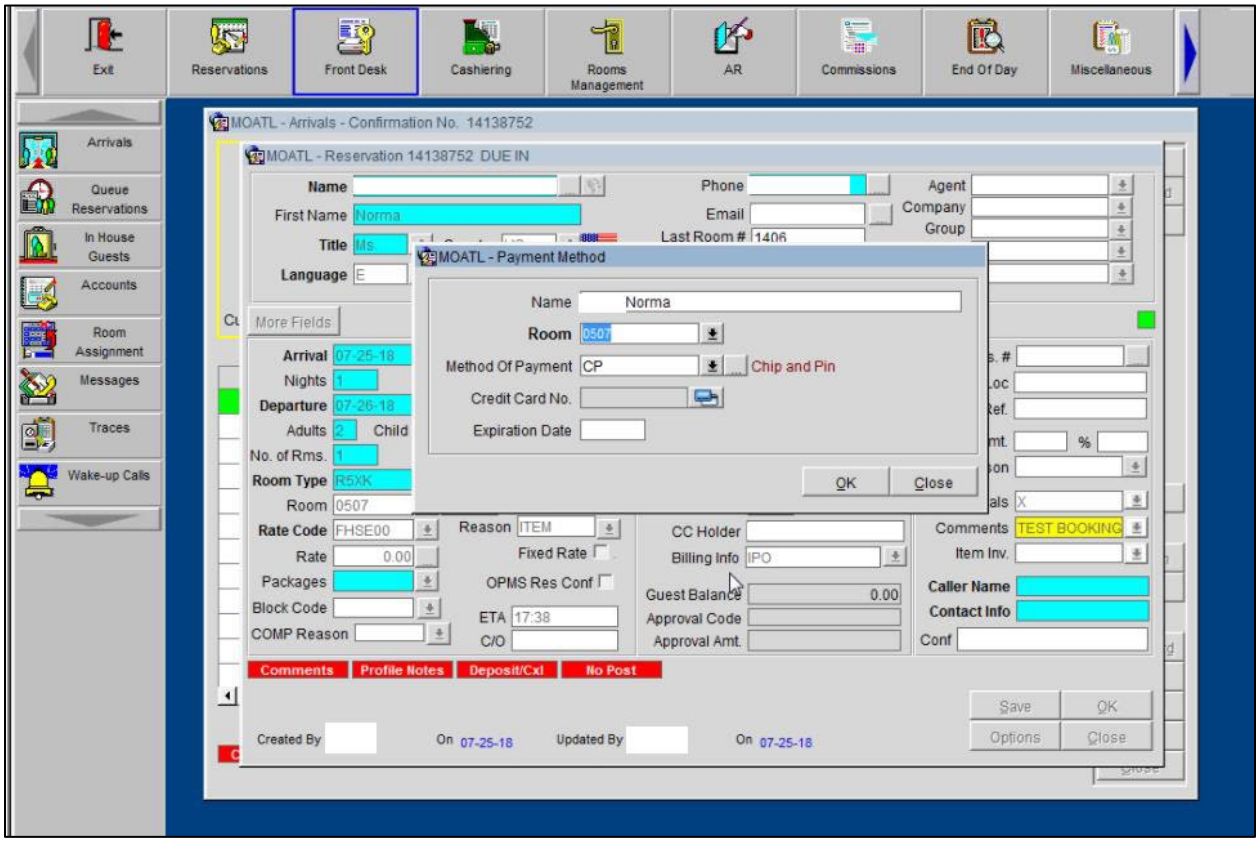
The clerk clicks **Yes** to confirm check in process.



Step 4 –Submitting a CP Authorization Request

- From the Payment Method screen, the clerk clicks **OK** to initiate a request for authorization.
- Notice there is no credit card attached.
- This action will light up the payment entry device (PED).

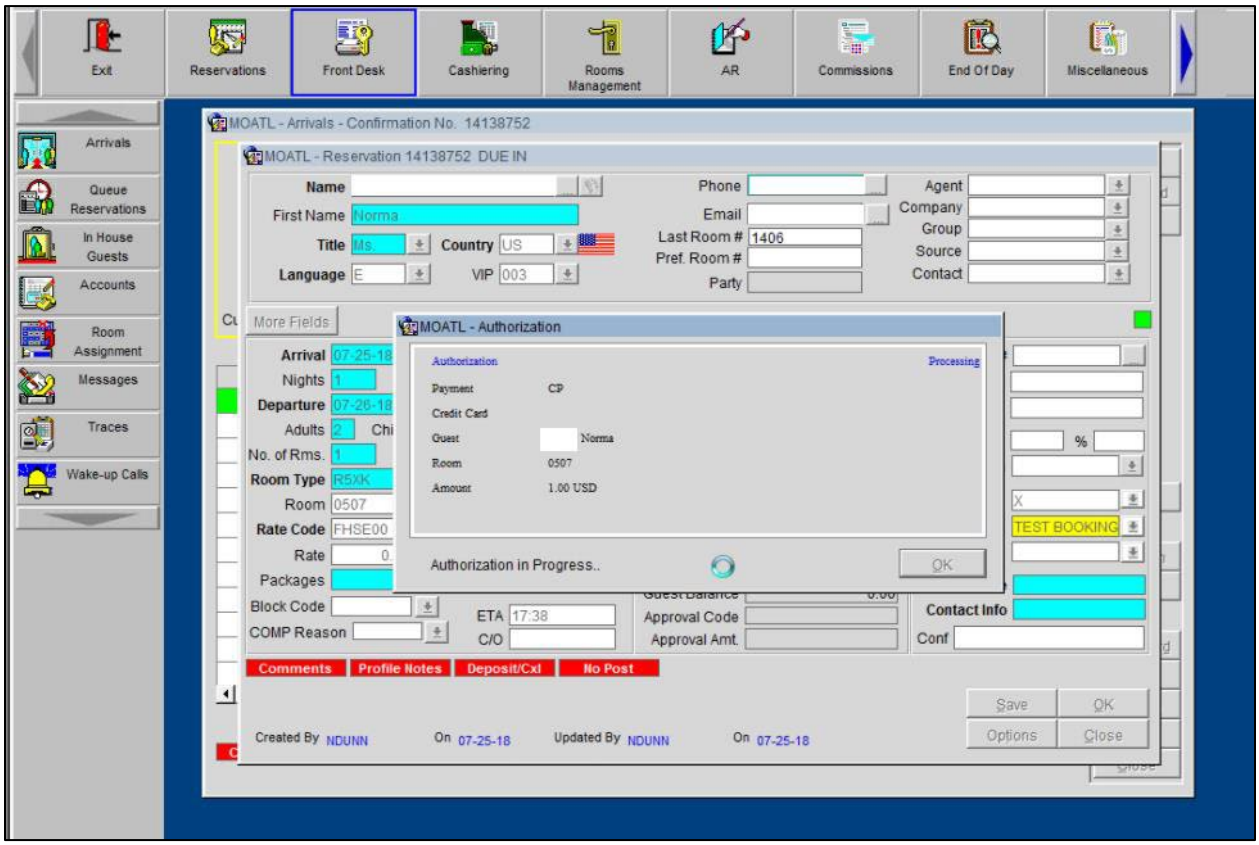
- **NOTE:** a room must be assigned to the guest before any of this process can be performed.



Step 5 –Acquiring the EMV Chip Data

- The Authorization window indicates that an authorization request has been sent to UTG, then to the PED.
- The PED should be lit and awaiting credit card insert.
- There is a 2 minute timeout for the guest to insert and process their card.

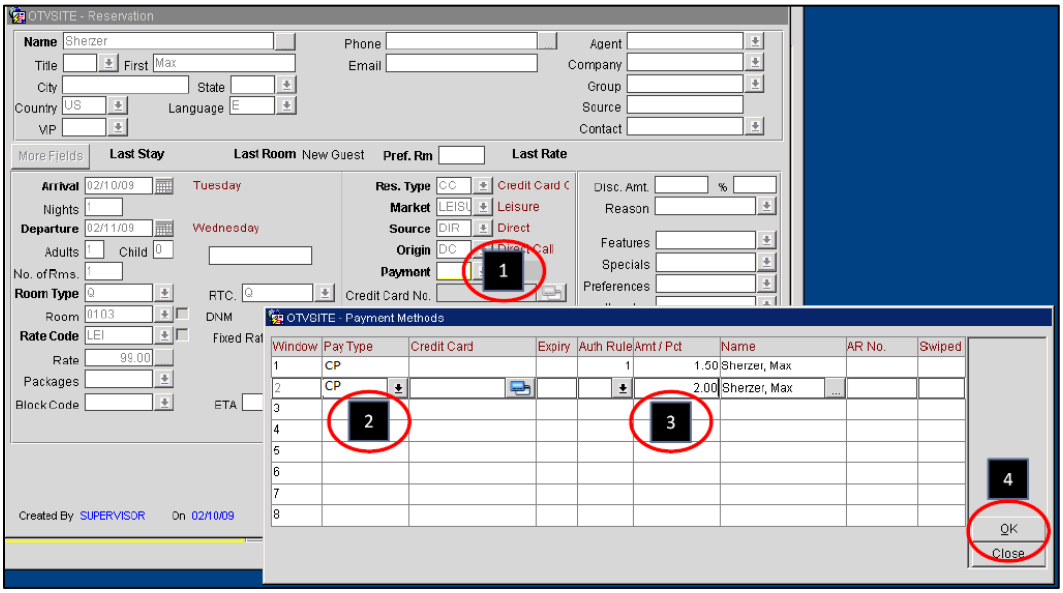
- After card insertion, the PED might prompt for the amount confirmation depending on the configuration. The guest needs to press green **Enter** key to initiate the EMV transaction.



Chip Transactions for Multiple Charges

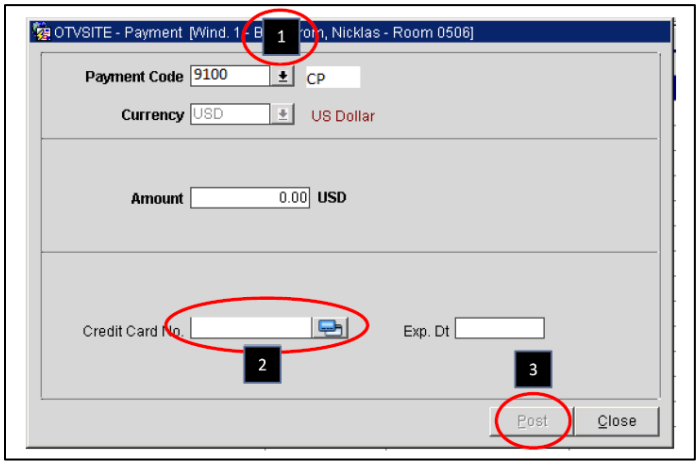
- Precondition: the customer and chip card must be present to perform the following transaction.
- When adding multiple charges and to have them both chip read, create the multiple charges window.
- Change the payment type to CP.
- Prefill in the Amt/Pct.
- Click the **OK** button.

- Opera will send two authorizations, one after the other, to the chip reader to perform the EMV/chip authorization.



Chip Transactions from the Billing Screen

- Precondition: the customer and chip card must be present to perform the following transaction.
- When performing a billing function, access the billing screen via Cashiering, and create the charge to the guest.
- In the Payment screen, choose **CP** for chip.
- Any credit card information will be wiped from this screen.
- Then click **Post**.
- The Opera system will send a payment authorization request to the PIN Pad for the chip insert.



Check-in from the Arrivals Screen

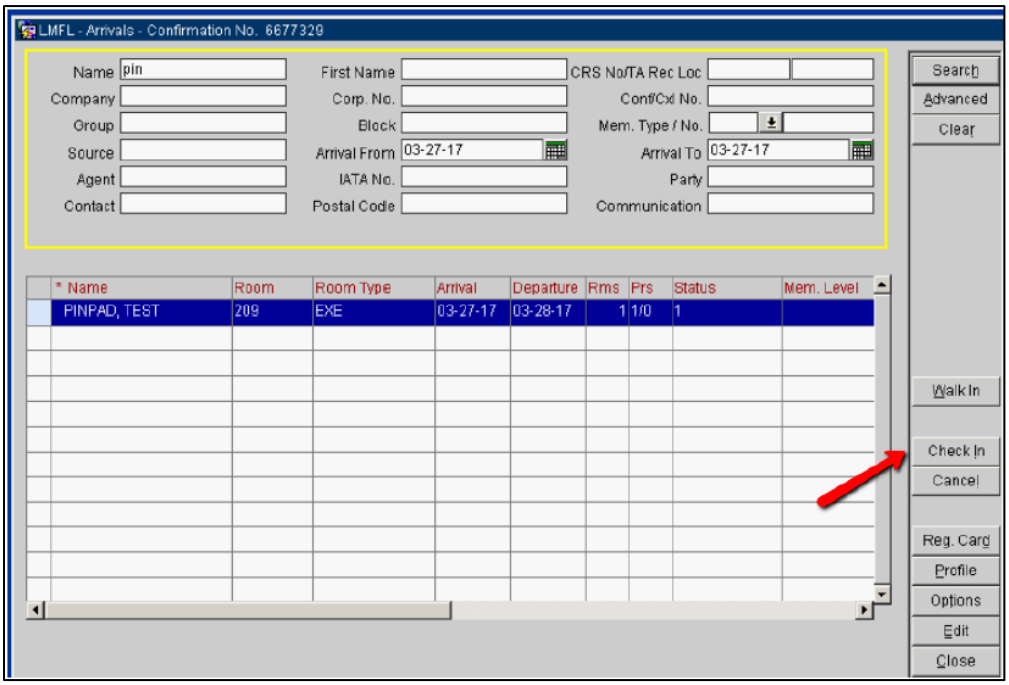
- The Arrivals window shows all the “Due Ins” that are expected for that day.
- Opera provides a “quick access” button to check guests in directly from the Arrivals screen instead of needing to access the Reservation window.
- All check in authorizations must have a room assignment before a transaction can be performed.

Step 1: Search and Display all Due In Guests

- From the Arrivals window, press search to display all the guests who are due to arrive.
- Guests who match these criteria will be listed in the grid on the lower half of the screen.
- Identify the guest you wish to check in.

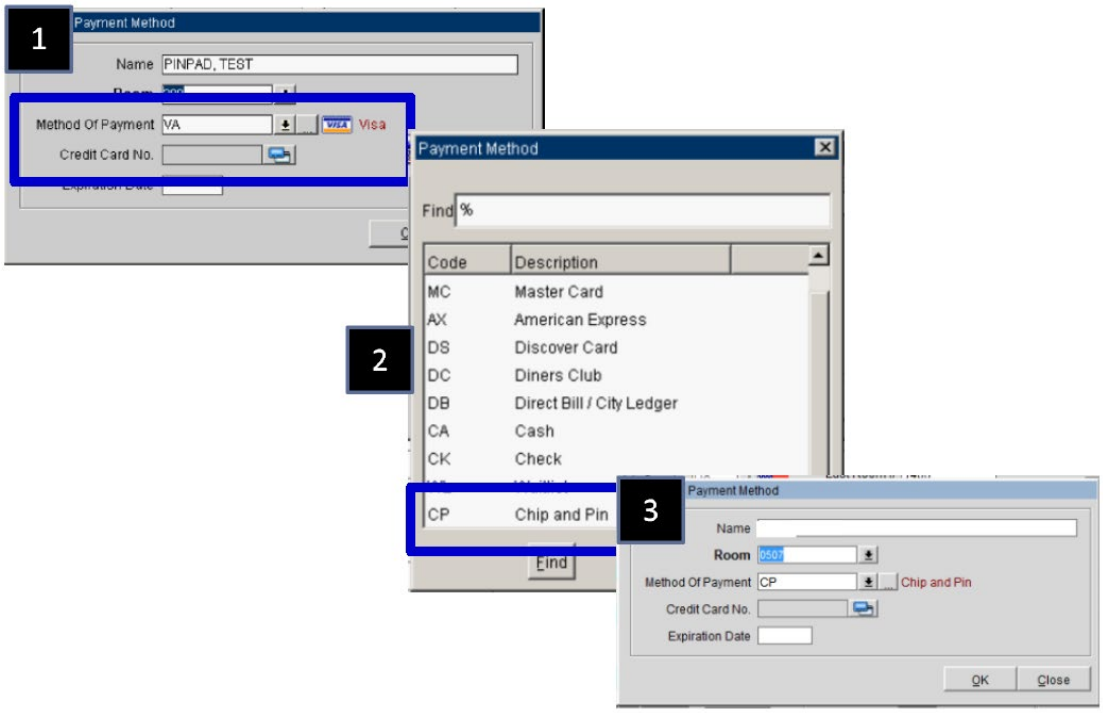
Step 2: Check-in Guest

Once the guest has been identified, the clerk should press the **Check In** button on the right (shown).



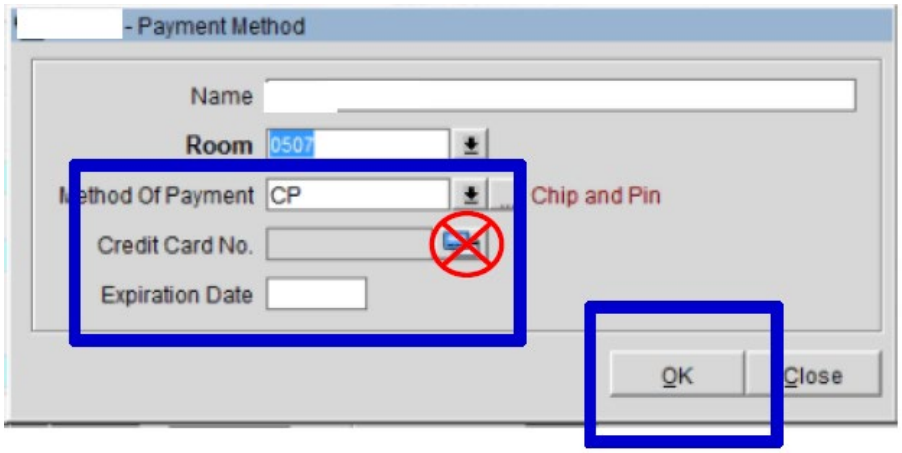
Step 3: Change the Payment Method to Chip and PIN

- After the Check In button has been pressed, the Payment Method window is initiated.
- To perform a proper EMV transaction, the clerk needs to change the payment to **CP** (Chip and PIN).
- Users can do this by the drop down arrow menu (shown), or by simply typing in CP into the Method of Payment field.



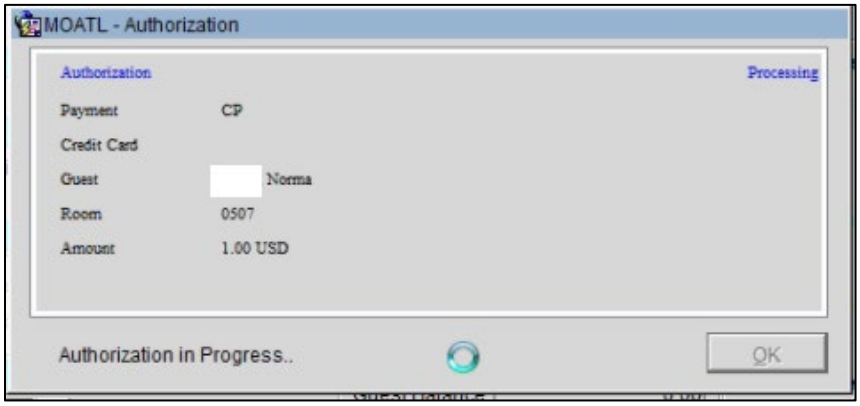
Step 4 –Submitting a CP Authorization Request

- Once the Payment Type has been set to CP, the clerk needs to press the OK button at the bottom right of the screen.
- DO NOT PRESS THE PAYMENT APPLICATION ICON TO THE RIGHT OF THE CREDIT CARD # FIELD.



Step 5 –Acquiring the EMV Chip Data

- The Authorization window indicates that an authorization request has been sent to UTG, then to the PED.
- The PED should be lit and awaiting credit card insert.
- There is a 2 minute timeout for the guest to insert and process their card.
- After card insertion, the PED will prompt for the amount confirmation. The guest needs to press **Enter** to initiate the EMV transaction.



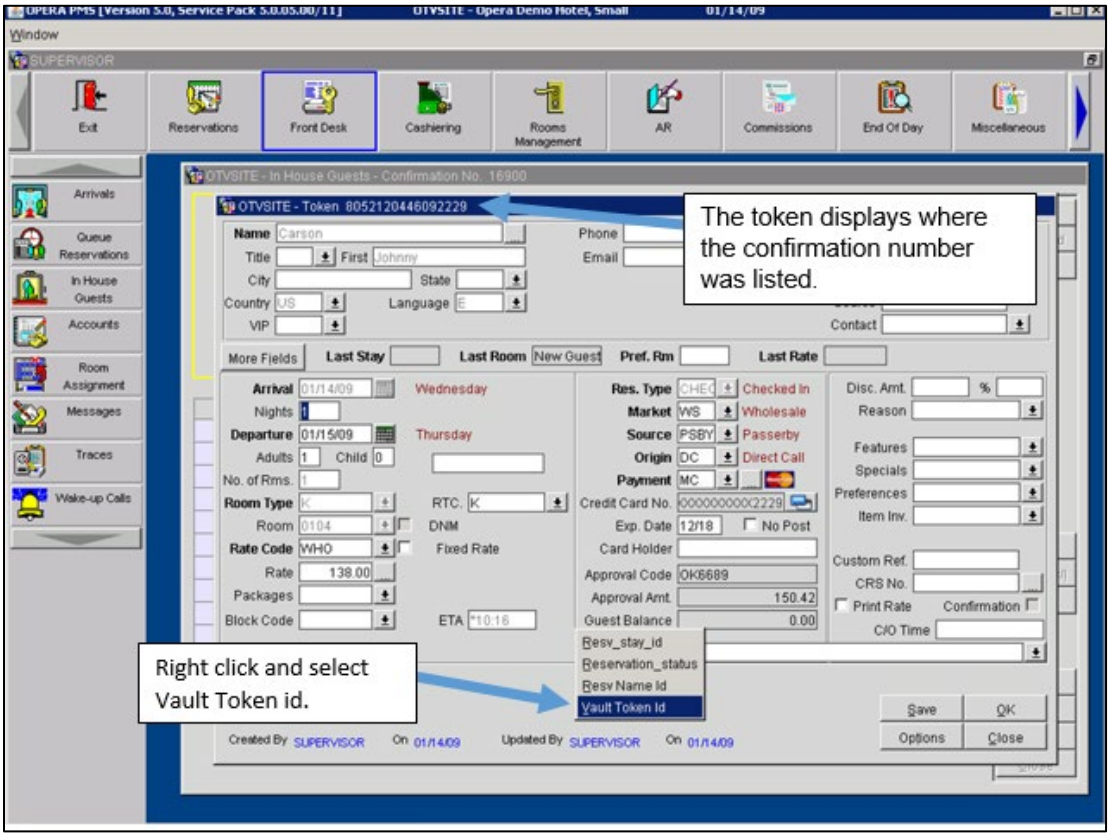
Troubleshooting Tokenization Issues

Viewing Tokens in OPERA

One of the first things that should be done when a tokenization issue is suspected is to verify the tokens on a reservation. There are several ways to view the tokens.

Viewing a Token with a Single Card on File:

When a reservation has only a single card on file, the token can easily be accessed from the reservation by right clicking and selecting Vault Token Id. The token will then be displayed in place of the confirmation number.

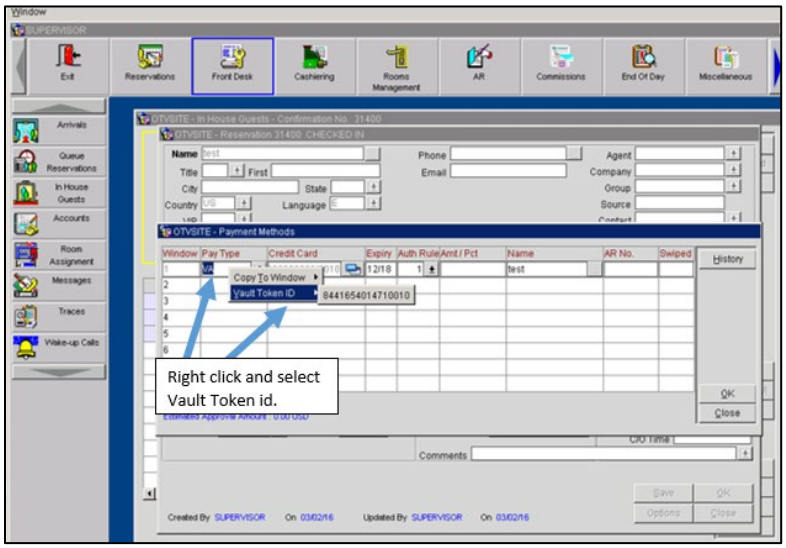


Viewing a Token with Multiple Cards on File:

There are two ways you can view token numbers on a reservation that has multiple credit cards on file. The first is to use the Multi-Pay Window on the reservation and the second is to use the Change Log.

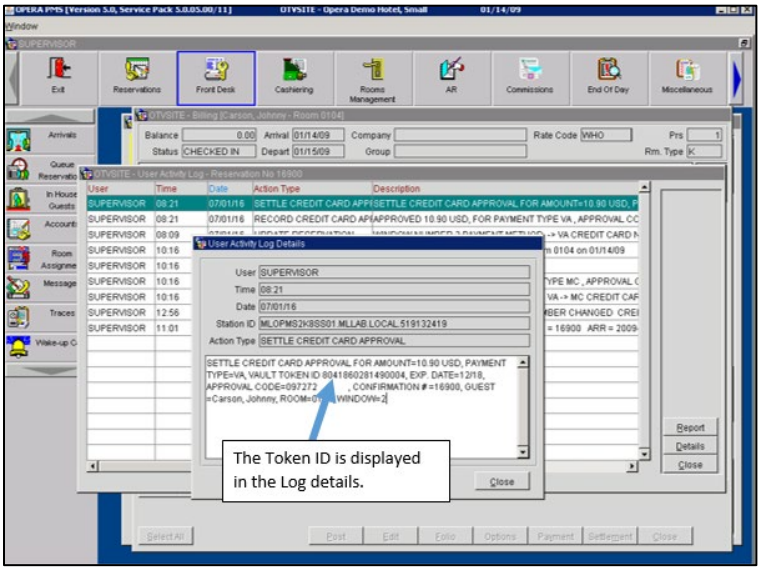
Using the Multi-Pay Window:

First access the multi-pay window from the reservation page. Right click on the card type of the credit card you wish to obtain the token for and select Vault Token Id.



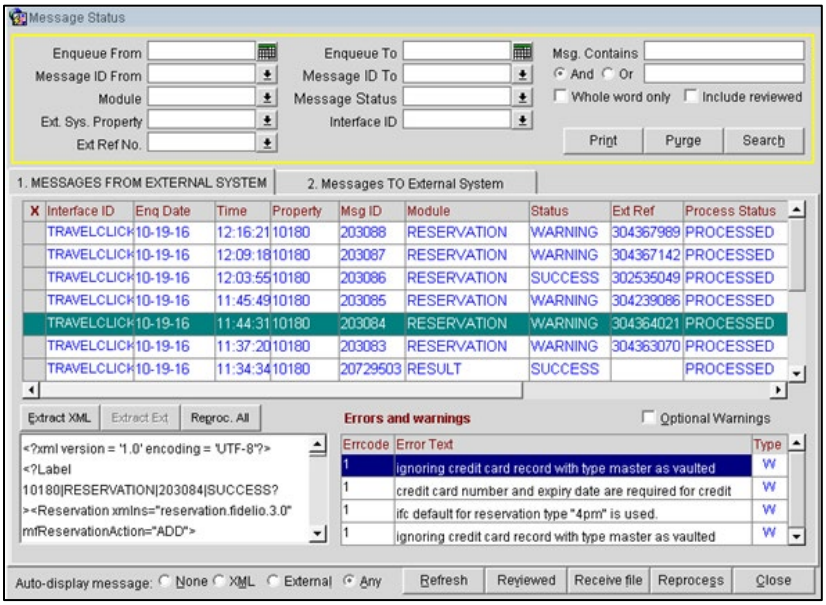
Using the Change Log:

To access the change log, open the reservation and select **Options**, and then **Changes**. Select the record of the authorization or payment and then click **Details**. This method is particularly helpful if a user is unsure of which card was used on a particular transaction.



Troubleshooting OXI Tokenization Issues

OXI stands for "OPERA Exchange Interface." It is a module that allows a site to receive external reservation data. For an OPERA site using tokenization, on rare occasions you'll get the following warning:



In short this is what is occurring:

1. OXI receives a reservation from a third party source.
2. OXI requests a token from UTG.
3. OXI formats the xml message incorrectly causing the credit card to fail a mod10 check or there is a communication failure to UTG
4. OXI inserts the reservation into the database defaulting the reservation to cash, since it did not receive a token and cannot insert a non-tokenized number into the database.

This error is well known to Oracle and several different solutions exist, including a hotfix. One version of a solution which does not involve a hotfix is summarized below:

1. Export the OXI interface SID data.
2. Uninstall the OXI Processor Shell.
3. Reinstall the OXI Processor Shell.
4. Re-import the OXI SID data with global settings.
5. Restart the 10GAPPR2ProcessManager.
6. Restart the OXI services.
7. Re-import the Shift4 provided P12 to certificate stores.
8. Acquire the latest version of CcHttpLib.DLL and copy it along the entire file path to D:\oracle\10gappr2\jdk\bin.
9. Redeploy the OXISerlets.war file.
10. Reload the microsifc.jar & messageinterceptor.jar files.
11. If there is a TLS 1.2 communication problem, apply the TLS 1.2 fix

Shift4 does not deploy the fix for this, but it is good to be able to explain what is actually occurring. Please contact Oracle to troubleshoot this in detail.

The only way to deal with this problem besides deploying one of the permanent fixes, is to have the site call the entity that provided the card number (Expedia, Priceline, etc.), and have them give that card verbally to the site.

Oracle ACL

Oracle ACL should not be troubleshot by Shift4 as it involves multiple database changes to OPERA. If there are problems with ACL, Oracle Technical Support should be engaged.

Appendix C: Rollback Procedures

CCW Interface - Non tokenized

In the event that an installation of OPERA Bridge fails on a site that already has an active CCW interface that is not tokenized the rollback steps are as follows:

- Disable the CCW interface communicating with UTG.
- Enable the old CCW interface.
- Revert the following changes if edited:
    - Chip and Pin
    - Credit Card Vault
    - Batch settlement method
    - Functionality setup
- If the site has a security certificate reinstall the original certificate that was in the OPERA wallet folder.

UTG does not need to be uninstalled and can continue to reside wherever it was installed. Once the URL is reverted, no traffic will go to UTG. Likewise the Oracle Wallet does not need to be removed because once “Chip and Pin” and “Credit Card Vault” are deactivated, the wallet will not be used.

CCW interface - Tokenized

In the event that an installation of OPERA Bridge fails on a site that already has an active CCW interface that is tokenized, the rollback steps are as follows:

- Disable the CCW interface communicating with UTG.
- Enable the old CCW interface.
- Revert the following changes if edited:
    - Chip and Pin
    - Batch settlement method
    - Functionality setup
- Reinstall the original certificate that was in the OPERA wallet.

UTG does not need to be uninstalled and can continue to reside wherever it was installed. Once the CCW interface is reverted, no traffic will go to UTG.