

Oracle® Payment Interface

Installation and Reference Guide



Release 19.1
F14997-03
November 2019

ORACLE®

Oracle Payment Interface Installation and Reference Guide, Release 19.1

F14997-03

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

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

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

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

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

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

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

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

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

Contents

Preface	6
<hr/>	
1 Pre-Installation Steps	1-1
<hr/>	
Databases	1-1
Supported Database Types	1-1
Java	1-2
Granting Permission in MySQL	1-2
Before Installing OPI	1-2
2 OPI Complete Installation	2-1
<hr/>	
3 OPI Custom Installation	3-1
<hr/>	
OPI Custom Install to Three PCs	3-1
4 Upgrading the OPI	4-1
<hr/>	
OPI Upgrade Steps	4-1
OPI 6.2 Upgrade Steps	4-4
5 Migration of DB Type	5-1
<hr/>	
Migrating the Data from 6.1 Database Schemas to 19.1	5-1
OPI Folder Structure	5-1
6 OPI User Administration	6-1
<hr/>	
User Roles	6-1
Creating a New User	6-1
New Users First Login	6-2
Editing Your User Profile	6-2
Editing Another User's Account	6-2
Forgotten Passwords	6-3
Purge Deactivated Users	6-4
7 Mutual Authentication	7-1
<hr/>	
Handling the Client Side Certificate	7-1
Handling the Root Certificate File	7-1
OPI Mutual Authentication – Summary	7-3
8 Audit	8-1
<hr/>	

Audit Trail Search	8-1
Audit Trail Purge	8-2
9 Silent Installation	9-1
Specify Alternative Response File	9-1
Specify Alternative Log File	9-1
10 OPI Services	10-1
OPI Config Service	10-1
OPI Service	10-1
OPI Utility Service	10-1
Changing the OPI Config Service Port	10-1
11 Settings Administration Tool	11-1
Using the Settings Administration Tool	11-1
Updating the OPI Schema Password	11-1
Updating the OPI Configuration Passphrase	11-2
12 Configuration Tools – Rotate Passphrase	12-1
Using the Rotate Passphrase Utility	12-1
13 OPI Client Certificate Creator Utility	13-1
Using the Client Certificate Creator	13-1
14 Pay@Table Certificate	14-1
Update Pay@Table PW	14-1
15 Import/Export OPI Configuration	15-1
Export Configuration	15-1
Import Configuration	15-1
Reset Security Data	15-1
16 Uninstallation and Modification of Install	16-1
Uninstalling OPI	16-1
Modifying OPI	16-1
17 Configuration Settings	17-1
Configuration Tool Settings	17-15
HTTP Support	17-22

18 Maintain OPI Environment	18-1
<hr/>	
Terminals	18-1
Pay at Table Devices	18-2
OPI Users	18-4
Payment Types	18-4
19 Troubleshooting and FAQs	19-1
<hr/>	
Troubleshooting	19-1
FAQs	19-3

Preface

Purpose

This document describes new features and functionality in OPI that are common to all supported POS types, OPERA, and Cruise SPMS. It is a supplement to the OPI installation guides that already exist for each of those products. It will not repeat the installation steps covered in those documents, but rather serve as a reference guide that covers in more detail the utilities and functionality that can be used as part of installation, configuration, and troubleshooting.

Audience

This document is intended for installers of the OPI and OGDH.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screenshots of each step you take

Documentation

Product documentation is available on the Oracle Help Center at

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

Revision History

Date	Description of Change
February 2019	Initial publication.
March 2019	Updated formatting with new Oracle template.
May 2019	Added new chapter on how to manage and maintain OPI environment.
July 2019	Updated security bugs in few chapters.
November 2019	Updated content in Terminal section

1

Pre-Installation Steps

IF UPGRADING OPI, YOU MUST READ THE [UPGRADING THE OPI](#) SECTION FIRST.

Databases

- In OPI 6.2 and higher, the OPI installer no longer includes MySQL, as OPI now supports multiple database types.
- A database is still required to hold the OPI configuration and audit event data, but must be installed separately prior to installing OPI.
- Root access to the database is required during the OPI installation, only to create a dedicated OPI database user, which can have a lower level of privilege than the Root user, and is used for OPI tasks once installation is complete.

Supported Database Types

The Oracle Payment Interface Installer release 19.1 supports the following database connections:

- MySQL Database 5.6 / 5.7
- Microsoft SQL Express Database 2008 / 2012
- Oracle Database 11g / 12c
- Microsoft SQL Database 2008 / 2012

NOTE:

During installation, OPI creates a database schema. OPI does not override the period of time this schema remains valid because the schema expiration date may already be defined by existing policies of the environment in which it is being installed.

By default, Microsoft SQL and MySQL do not define an expiration date for a schema. Oracle Database does define an expiration date of six months after creation.

Be aware that if the schema's password expires and OPI is subsequently unable to read from or write to the database, service interruptions should be expected.

Java

- In OPI 6.2 and higher, the OPI installer no longer includes Java.
- Java Platform, Standard Edition Runtime Environment (JRE) version 1.8, minimum update 152 should be installed prior to installation of OPI

Granting Permission in MySQL

A typical MySQL installation will not allow a connection by IP address or Name, therefore the default Name/IP: value should be left as localhost during the OPI installation. If it cannot be left as localhost (for example, when the database is installed on another PC), the “root” user will need to be given privileges so the database server will accept the connection when the IP address is passed.

1. Connect to the MYSQL Database as the “root” user.
2. Execute the following statements to grant privileges to “root” user.

```
use information_schema;
```

```
grant all privileges on *.* to 'root'@'%' identified by 'password' with grant option;
```

Example where real root user PW is entered in the command instead of the generic 'password':

```
mysql> use information_schema;
```

```
Database changed
```

```
mysql> grant all privileges on *.* to 'root'@'%' identified by 'password' with grant option;
```

Result = Query OK, 0 rows affected (0.00 sec)

Before Installing OPI

Complete the following tasks before installing:

- The OPI application requires Microsoft .NET Framework version 4.0 or higher.
- You cannot upgrade from previous versions of MPG to OPI 19.1. Upgrading from OPI 6.1 and higher to OPI 19.1 is supported. Upgrading from MGDH 6.1 and higher to OGDH 19.1 is supported.
- If an MGDH installation prior to version 6.1 exists, go to Programs and Features to uninstall the previous MGDH installation before installing the latest OGDH release.
- Ops.exe cannot be running during the MGDH uninstall.
- Verify with the merchant when setting up table service (TSR), quick service (QSR), or both. QSR does not support tips.
- Verify with the merchant if activating the Refund functionality. The merchant controls the privilege for this function.

- Verify with the merchant if they offer guests the option to get cash back with their purchase, then activate the Sale & Cash option. This is only available for QSR.
- Confirm Microsoft Visual C++ 2010 is installed on the computer where OGDH and OPI are installed.
- Oracle Payment Interface requires at least 6 GB of free disk space.
- You must install both OGDH and OPI as a System Administrator.
- You must enter the MICROS database user name and password to install OGDH.

During the installation, confirm the following:

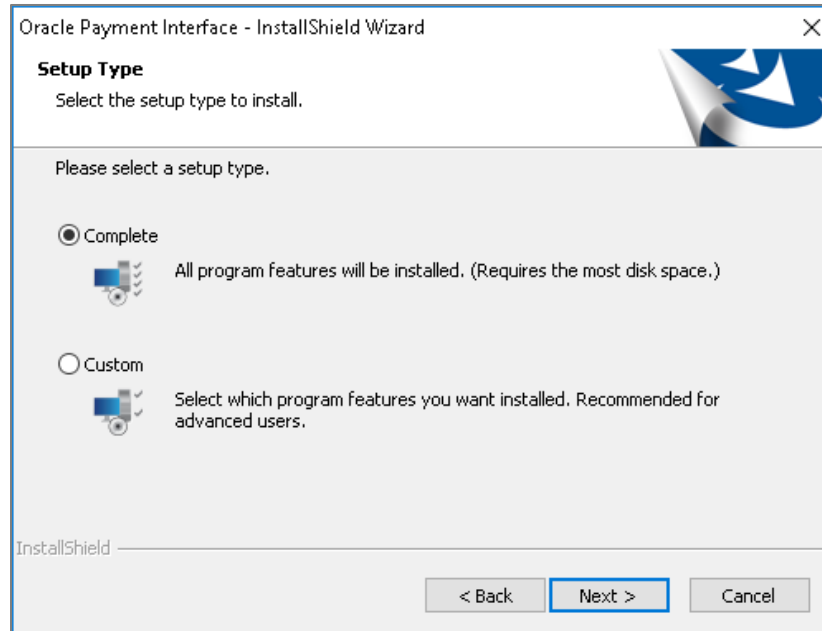
- Merchant ID's
- Receipt "Header" and "Trailer" details
- Tender Media numbers for each card type
- IP address of the OPI Server
- If there is an existing database installed, the root password is required
- Workstation IDs and IPs that integrate with the PIN pad

2

OPI Complete Installation

1. Right-click and Run as Administrator the `OraclePaymentInterfaceInstaller_19.1.0.0.exe` file to perform an installation.
2. Select the Language for the installation, and then click **OK**.
3. Click **Next** on the Welcome to the InstallShield Wizard screen to proceed with installation.
4. Prerequisites for the installation will be checked, including the required free drive space, details of the host environment, and the Java version that is present.
5. Select either the **Complete** or **Custom** installation option:
 - **Complete:** Installs the OPI Service Application, OPI Configuration Tools & Deploy the OPI database schema during the installation process.
 - **Custom:** Allows installation of only the modules selected. For example, if you want to install the OPI Service Application on one host and the Configuration Tools on a different host, you can run the installer on both machines, with only the relevant components selected for each machine.
 - Database Schema
 - OPI Services
 - Configuration Tool
 - Because the OPI database schema is deployed via network connection, deployment could also be included on one of these installations, or the installer could also be run a third time on another host to deploy only the database schema.

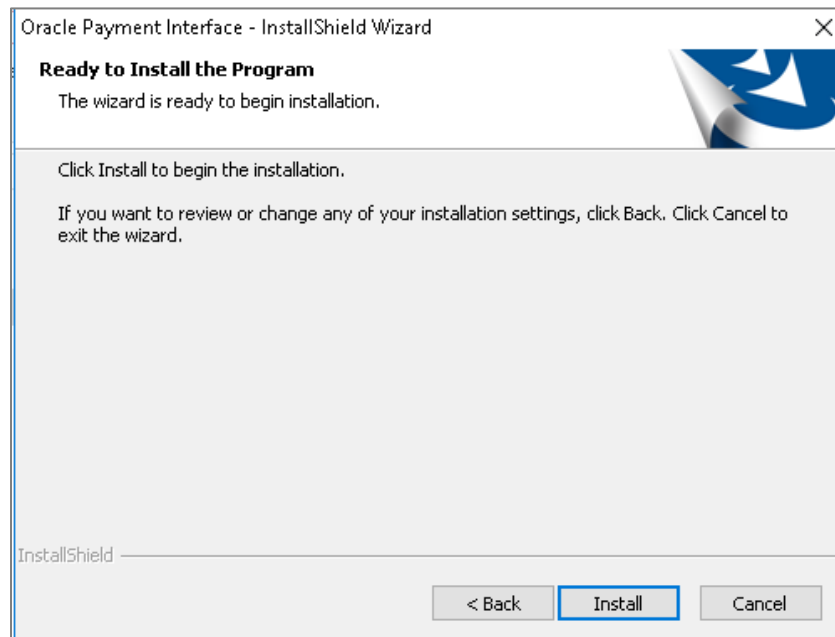
The steps below cover a Complete Installation. If you are installing the OPI components to different PCs, see the [OPI Custom Installation](#) section.



6. Click **Change** to amend the installation drive or path, if required and click **Next**.

7. Click **Install** to begin installation.

When the file transfer is finished, Setup prompts for the next set of configuration settings.



8. Select your Database type:

- MySQL
- SQL Server
- SQL Express
- Oracle DB

9. Enter the relevant connection details for your database type. Details can be provided by whomever installed/configured the database software.

 **NOTE:**

OPI uses the string OPIDB as a tablespace name, so OPIDB should not be used in the installation path or service names/IDs of any of the databases, otherwise conflicts may occur and the installation is likely to fail.

MySQL

Name/IP – The Hostname or IP Address used for communication to the database. If using MySQL this must be left at the default of localhost. If you cannot use localhost for the Name/IP field, (because you are installing the database schema on another computer), then some commands must be run manually on that MySQL database before proceeding. See the [Granting Permission in MySQL](#) section for instructions.

- **Port #** – The Port number used for communication to the database

SQL Server & SQL Express

Static

- **Name/IP:** The Hostname or IP Address used for communication to the database.
- **Port #:** The Port number used for communication to the database.
- **Instance:** The SQL named instance.

Dynamic

- **Name/IP:** The Hostname or IP Address used for communication to the database.
- **Instance:** The SQL named instance.

Oracle DB

SID

- **Name/IP:** The Hostname or IP Address used for communication to the database.
- **Port #:** The Port number used for communication to the database.
- **SID:** The unique name that uniquely identifies the Oracle database.

Service Name

- **Name/IP:** The Hostname or IP Address used for communication to the database.
 - **Port #:** The Port number used for communication to the database.
 - **Service:** The TNS alias used to connect to the Oracle database.
10. Confirm the database admin user used to connect to the database. The database admin user is only used to create an OPI database user, which is used after installation completes.
 11. Enter a username and password for the OPI database user creation. If the username already exists in the database, you will be prompted to select a different username.

The installer will attempt to connect to the database using the admin credentials supplied, and create the OPI database user.

12. Create a Super User System Admin level user account that can be used for configuring and maintaining the system. Enter the username and password that should be created.
13. Enter the **Host** and **Port** that should be used to connect to the OPI Config Service for the Merchant Configuration.

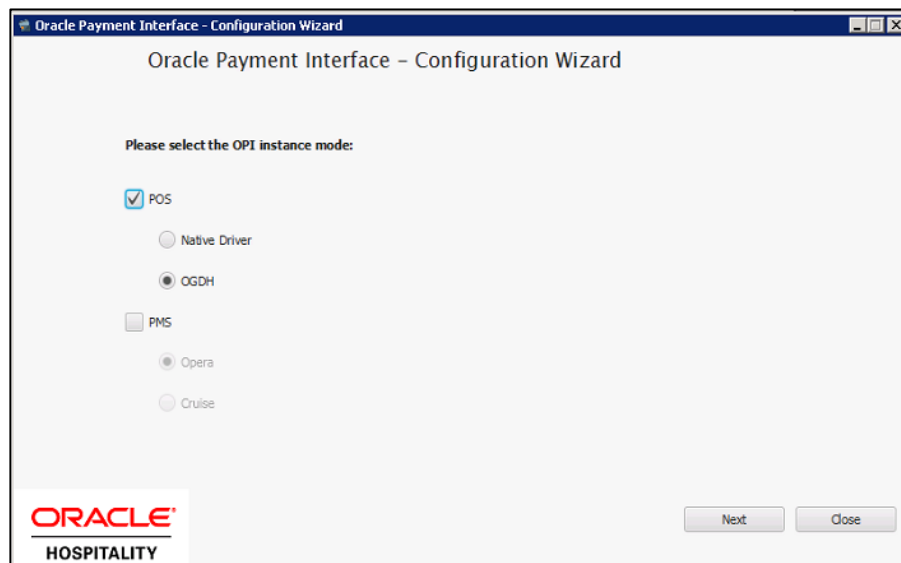
 **NOTE:**

In this step you are not configuring the port the service will listen on. Instead, it is prompting for the details of how to connect.

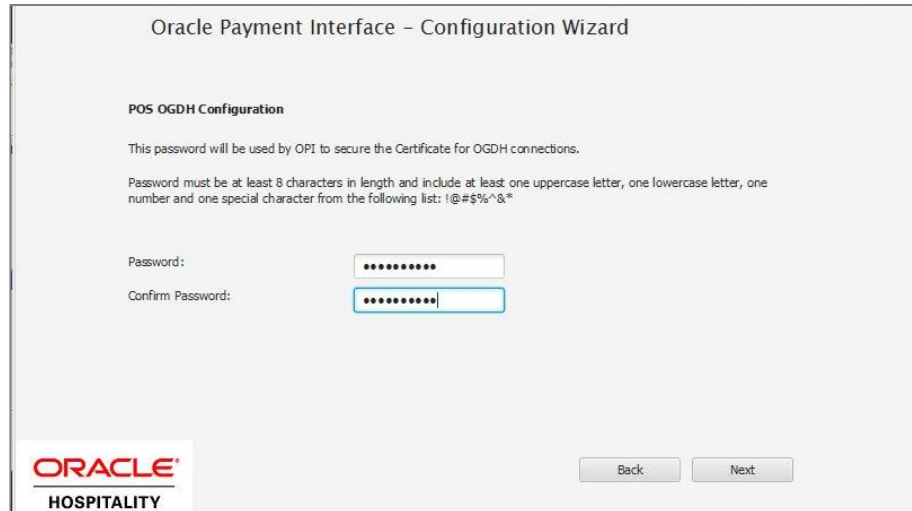
- The IP will depend on where the OPI Config Service is installed. If you are performing a complete installation, this can be left as the localhost address.
- The default port is 8090.

14. Set and confirm the passphrase value.

If the details entered for the connection to the **OPI Config Service** are correct, then the OPI installer will launch the configuration wizard.

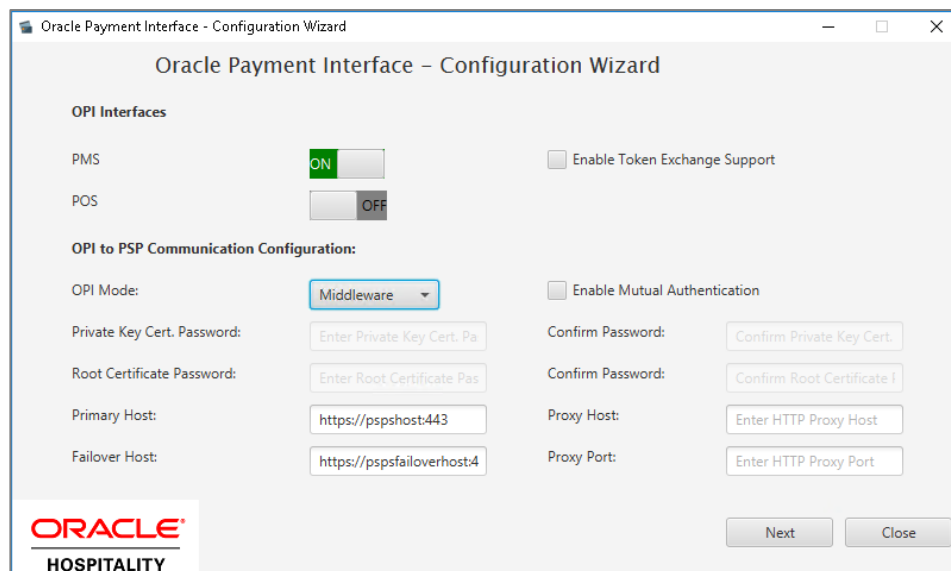


15. Select whether the installation will be used for POS and/or PMS merchants. If POS is required, you will also need to specify the POS driver type that will be used (**Native Driver or OGDH**).
16. Depending on the previous POS Type choice, you should provide either:
 - **Native Driver** - the passphrase that is used for authentication between POS and OPI.
 - **OGDH** - the password that will be assigned to the certificate on the POS Service listening port.



The OPI Interface screen appears. At this point the configuration screens displayed are same as what is seen if the configuration wizard is launched manually.
(:\OraclePaymentInterface\v19.1\Config\LaunchWizard.bat)

- Configure settings as required. For more details on how to use configuration wizard and configuration tool refer [Configuration Settings](#) section.



- Enable Mutual Authentication:** Enable this option only if the PSP has provided the certificates and passwords for it.
- Private Key Cert. Password:** Enter the password and confirm it.
- Root Certificate Password:** Enter the password and confirm it.
- Select the **OPI Mode** either as Middleware or Terminal.
 - Middleware:** Fill in the primary host connection information and the failover Host information (if provided).
 - Terminal:** Select correct Port. If using Mutual Authentication, see the [Mutual Authentication](#) section for more details.

 **NOTE:**

For Terminal Mode setup, special characters including "_", "|", and "=" cannot be used in the CHAINCODE or PROPERTYCODE. This will cause the EOD to fail in OPI.

22. Click **Next**. The Merchant configuration screen appears.
23. Merchant configuration is covered by the product-specific guides available at https://docs.oracle.com/cd/F14695_01/
24. Once merchant configuration is complete, the installer prompts you to reboot the host machine. If it is not practical to reboot the host machine, you must start the **OPI Service** manually.

3

OPI Custom Installation

OPI Custom Install to Three PCs

OPI has three components that can be installed all at once on one PC, or separately. The following is an example of the steps to install each of the three parts separately.

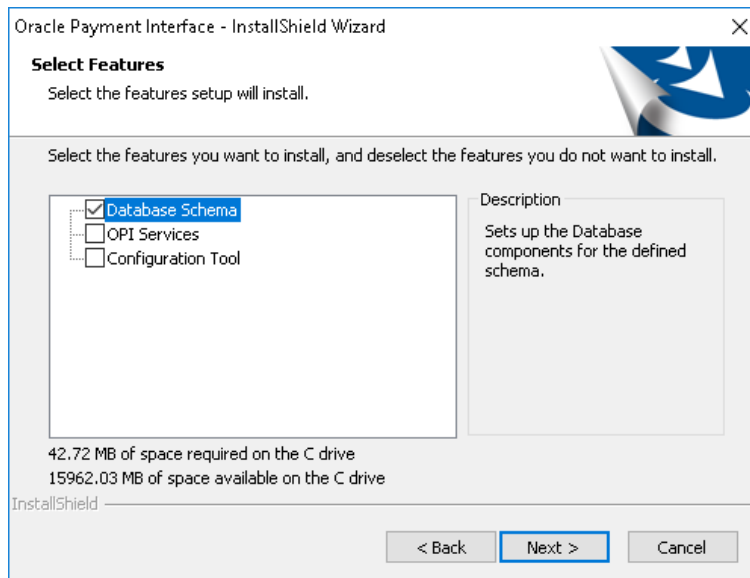
The correct order (required) for a custom install is:

1. **Schema**
2. **OPI Services**: must be able to communicate to the Schema PC during install.
3. **Configuration Tool**: must be able to communicate to Schema and OPI services PCs during install.

Part 1: Schema

Installs the OPI Utility Service and database schema.

1. Double-click **OraclePaymentInterface_19.1.0.0.exe**.
2. Select a language, and then click **OK**.
3. Click **Next** twice.
4. On Setup Type screen, click **Custom**, and then click **Next**.
5. Choose a destination, and then click **Next**.



6. On the Select Features screen, select **Database Schema**, and then click **Next**.



NOTE:

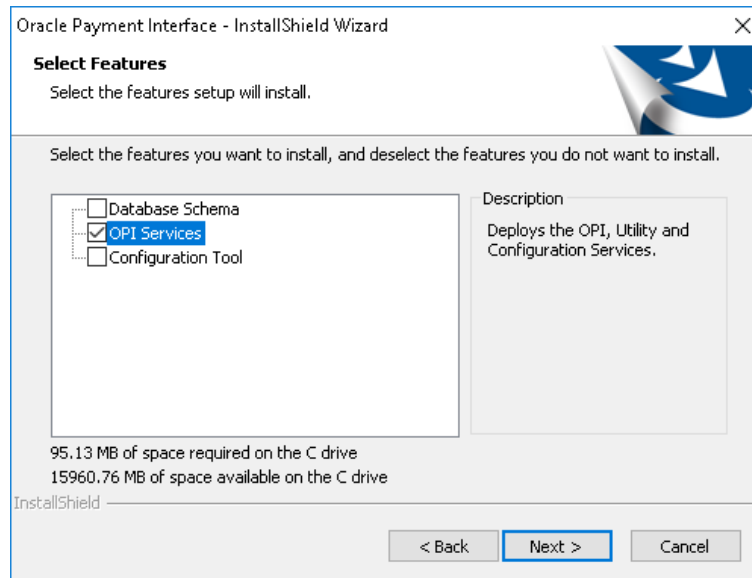
The database must already be installed on this PC.

7. Click **Install**.
8. Select your database type, and then click **Next**.
The following steps use MySQL as an example.
9. **Name/IP:** Leave as localhost, if the OPI database is installed on this PC. Otherwise, use the IP address of the database PC.
10. **Port:** Accept the default Port # of 3306 (for MySQL), and then click **Next**.
11. **DBA User**
Login ID: root (for MySQL)
Password: Enter the root user password, and then click **Next**.
12. **Database User Credentials**
User Name: Create a new user name.
Password: Enter a password, confirm it, and then click **Next**.
13. Click **Finish** and reboot the system.

Part 2: OPI Services

This will install the OPI service, the OPI Config service, and the OPI Utility service.

1. Double-click `OraclePaymentInterface_19.1.0.0.exe`.
2. Select a language, and then click **OK**.
3. Click **Next** twice.
4. On the Setup Type screen, select **Custom**, and then click **Next**.
5. Choose a destination, and then click **Next**.

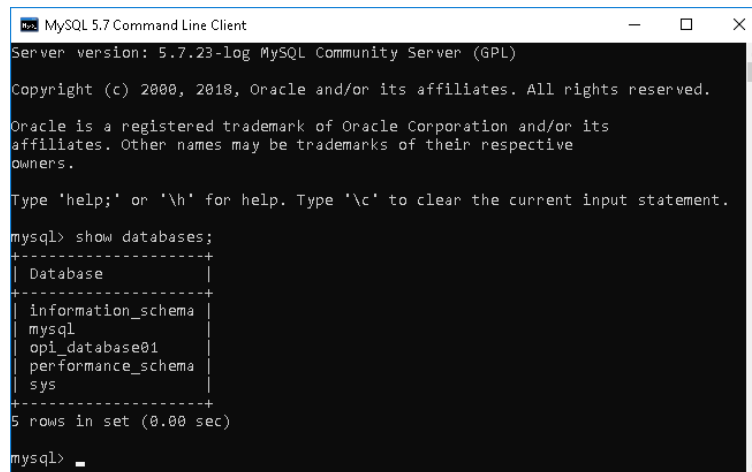


6. On the Select Features screen, select only **OPI Services**, and then click **Next**.
7. Click **Install**.
8. Select a database type, and then click **Next**.
9. **Name/IP:** Enter the IP address of the PC where the OPI database/schema is installed.

 **NOTE:**

If the database type is MySQL, and you cannot use localhost for the Name/IP field, then some commands must be run manually on that MySQL database before proceeding. See the [Granting Permission in MySQL](#) section for instructions. Setup will not complete if this is not done.

10. **Port #:** Accept 3306 (for MySQL), and then click **Next**.
11. On the Database Server Login screen, enter the name and password for the DBA user of the OPI database.
Login ID: root (for MySQL)
Password: Enter the root user's password.
12. On the Database Name screen, enter the database name, and then click **Next**. The database name will typically be **opi_database01**.
13. To verify the database name, connect to MySQL and run the show databases; command, as shown below.



```
MySQL 5.7 Command Line Client
Server version: 5.7.23-Log MySQL Community Server (GPL)
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| opi_database01 |
| performance_schema |
| sys |
+-----+
5 rows in set (0.00 sec)

mysql>
```

14. On the Configuration Tool Superuser Credentials screen:
 - User Name:** Enter a user name that will be used to access OPI applications as a super user.
 - Password:** Enter a password for the super user, confirm the password, and then click **Next**.
15. **Port:** Leave port set to 8090, and then click **Next**.
16. On the Configuration Tool Passphrase screen, enter and confirm a passphrase for the configuration tool, and then click **Next**.
17. Click **Finish** to allow reboot.

Part 3: Configuration Tool

This installs the OPI Utility service and OPI configurator.

1. Double-click `OraclePaymentInterface_19.1.0.0.exe`.
2. Select a language, and then click **OK**.
3. Click **Next** twice.
4. On Setup Type screen, select Custom, and then click **Next**.
5. Choose a destination, and then click **Next**.
6. On the Select Features screen, select only **Configuration Tool**, and then click **Next**.
7. Click **Install**.
8. On the Logon screen, enter the configuration tool super user name and password, and then click **Next**.
9. On the Configuration Tool Connection Settings screen, enter the Host and Port information, and then click **Next**.
 - Host:** Enter the IP address of the PC where the OPI Config Service is installed. This will be the PC where you selected “OPI Services” to be installed.
 - Port:** 8090
10. Enter and confirm the Configuration Tool Passphrase, and then click **Next**.

11. In the Oracle Payment Interface 19.1 – Configuration Wizard, select POS or PMS. If POS, also select either **Native Driver** or **OGDH**. This example will install POS Native Driver.

Click **Next**.

12. POS Native Driver Configuration

Passphrase: Enter and confirm the POS Native Driver passphrase.

Click **Next**.

13. OPI Interfaces

OPI Mode: Select either **Terminal** or **Middleware**. For Terminal mode, enter the correct port. For Middleware mode, enter the URL including port in the format shown in the dialog. This example selects Middleware.

Click **Next**.

14. POS Merchants

Click the blue + button in the upper right corner to create a merchant record. Fill in all merchant values. This example selects RES and enables Pay at Table.

Click **Next**.

15. Merchant Pay at Table Configuration

DB Host: Enter the IP address of the RES server.

DB Name: Enter the POS database name. ex: micros

Enter and confirm the DB user and password to connect to the RES/POS database.

Tender Media ID: Enter the tender media record numbers for each selection used.

The Service Charge value should be the Service Charge record number linked to tenders for tipping.

Click **Next**.

16. Pay at Table Devices

Click the blue + button in the upper right corner to add a Pay at Table device record.

Mobile Device ID: Enter the value/number used to identify this mobile device.

Query By: Select either table or check for the method this device will use to retrieve checks from the POS database.

Click **Next**.

17. Pay At Table Configuration

Service Port: Enter the port used to communicate to the Pay at Table terminals.

Certificate Password: Enter the certificate password provided by the PSP for Pay at Table.

Confirm Password: Confirm the certificate password.

Click **Next**.

18. POS Merchants

Click **Close** to complete the installation.

19. Click **Finish** to allow a reboot.

4

Upgrading the OPI

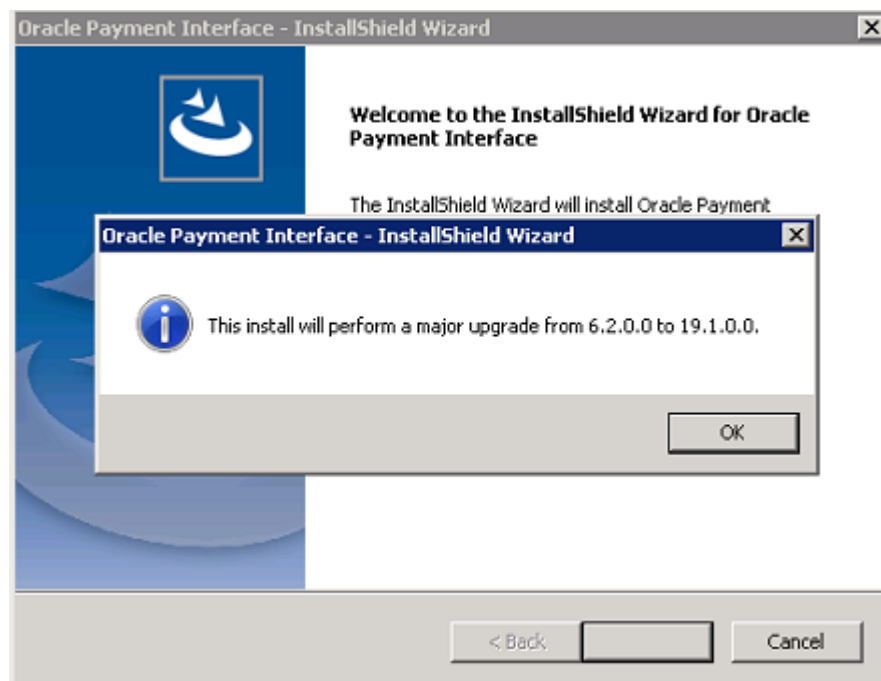
VERY IMPORTANT: Read and follow the upgrade directions.

 **NOTE:**

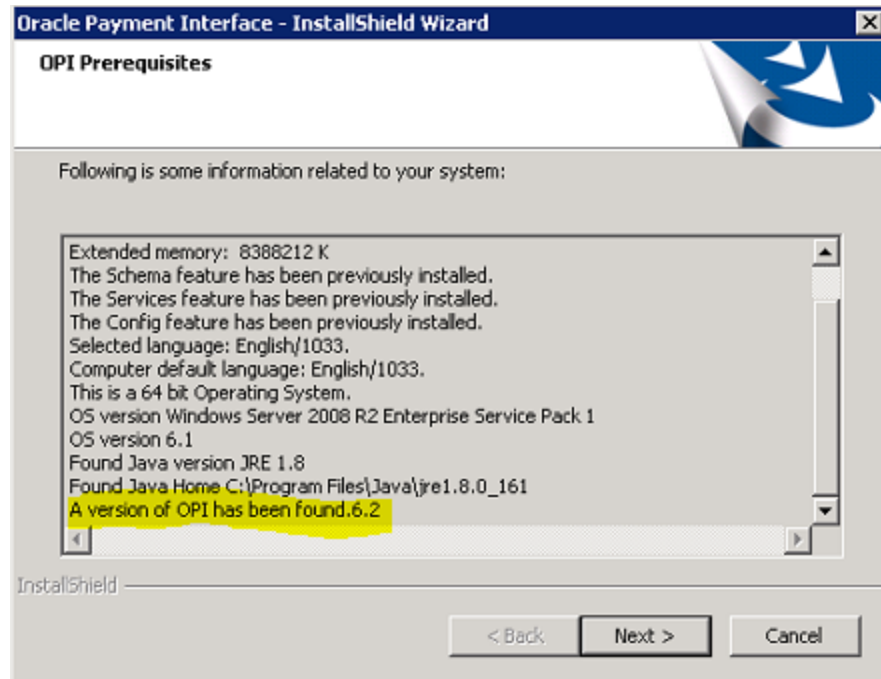
OPI 6.1 and higher can be upgraded to OPI 19.1.

OPI Upgrade Steps

1. Right-click and Run as Administrator the OraclePaymentInterfaceInstaller_19.1.0.0.exe file.
2. Select a language from the drop-down list, and then click **OK**.



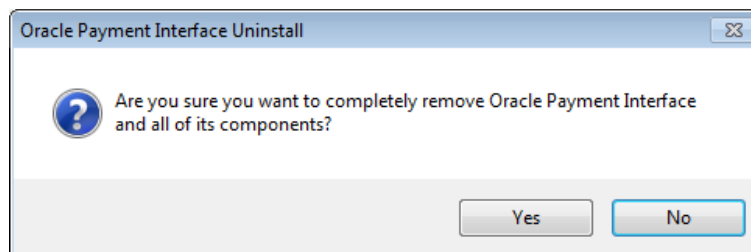
Click **OK** to the pop up message box. Click Next on the Welcome screen to proceed with the installation. Prerequisites for the installation will be checked, including the required free drive space, details of the host environment, and the Java version that is present.



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



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



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

IF YOU CLICK NO, YOU WILL HAVE BOTH OPI 6.1 AND OPI 19.1 INSTALLED AND NEITHER WILL WORK.

Explanation: OPI will migrate the existing MySQL configuration information, but all previous OPI applications will be removed before the new files are installed.

6. Choose a Destination Location. Accept the default installation location or click **Change...** to choose a different location.
7. Click **Next**.

The Ready to Install the Program screen displays.

8. Click Install.

The Setup Status screen displays for a few minutes.

Setup Type

For database type, select **MySQL**. No other database type is supported for upgrades.

Database Server

Name/IP: The Hostname or IP Address used for communication to the MySQL database. This must be left at the default of localhost.

Port #: The Port number used for communication to the database

Database Server Login

DBA user

Login ID: root

Password: root user password for MySQL database.

Database User Credentials

User Name: This must be a new user name. It cannot be the same user from the 6.1 install.

Password: Password for the new database user.

Configuration Tool Superuser Credentials

User Name: This can be any user name. It does not have to be a Windows account user.

Password: Create a password, and then confirm it.

Configuration Tool Connection Settings

Host: Enter the IP address or server name of the PC where the OPI Config Service is installed. This will be the PC where you selected "OPI Services" to be installed.

Port: Leave at 8090.

Configuration Tool Passphrase

Enter and confirm a passphrase.

Click **Next**.

The Configuration Wizard launches.

Continue to follow on-screen directions, verifying settings as you go.

POS Merchants

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

Verify the merchant settings are correct.

Merchant Pay At Table Configuration

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

Continue to follow the on-screen directions.

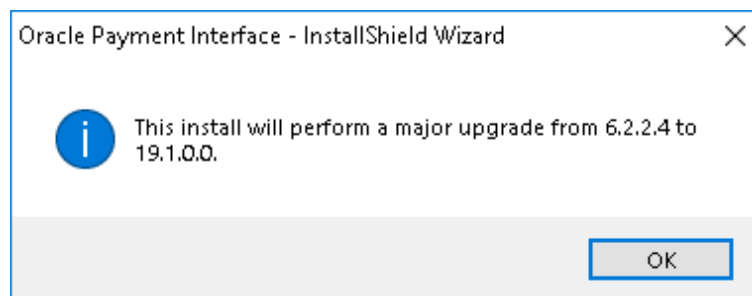
InstallShield Wizard Complete

Click **Finish** to allow a reboot.

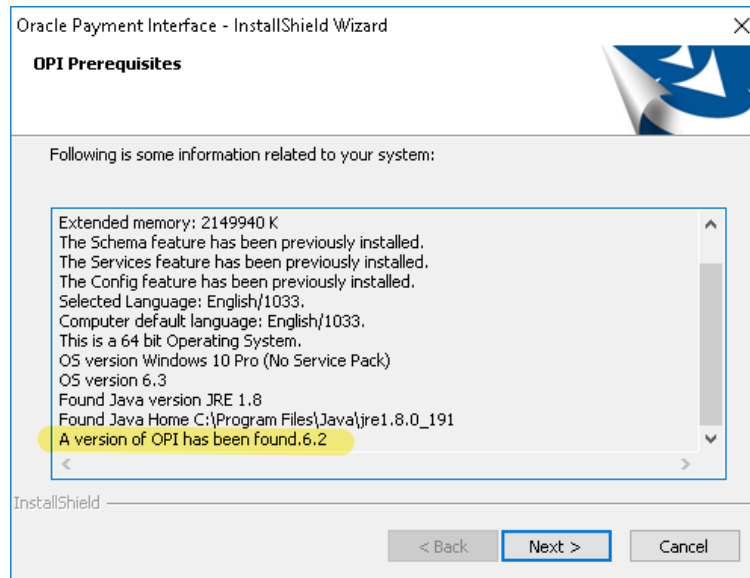
If you cannot immediately reboot, you must stop and then start the OPI Service for the current settings to take effect.

OPI 6.2 Upgrade Steps

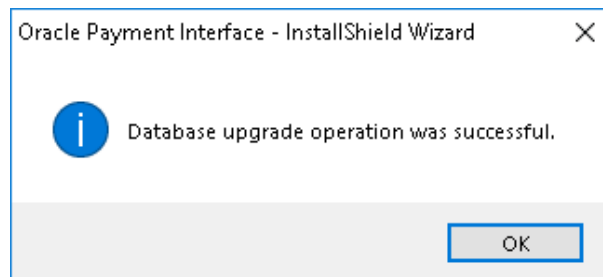
1. Right-click and Run as Administrator the `OraclePaymentInterfaceInstaller_19.1.0.0.exe` file to perform an upgrade.
2. Select a language from the drop-down list, and then click **OK**.
3. Click **Next** on the Welcome screen.
4. Click **OK** on the OPI Wizard screen.



5. Click **Next** on the OPI Prerequisites screen.
Prerequisites for the installation will be checked, including the required free drive space, details of the host environment, and the Java version that is present.



6. Choose a Destination Location. Accept the default installation location or click **Change...** to choose a different location.
7. Click **Next**.
The Ready to Install the Program screen displays.
8. Click **Install** to begin installation.
9. Click **OK** on the OPI database upgrade screen.



10. Enter the **Host** and **Port** that should be used to connect to the OPI Config Service for the Merchant Configuration.
11. Once installation is complete, the installer will prompt for a reboot of the host machine.

5

Migration of DB Type

The migration application runs as part of the 19.1 installation process when an upgrade from 6.1.x to 19.1 version is detected. The migration tool only supports migrating from MySQL to MySQL. Migrating from MySQL to any other database type is not supported.

NOTE:

The configuration data will be migrated. The transaction data will not be migrated. This means that all transactions must be closed and finalized/settled prior to upgrading to OPI 19.1.

Migrating the Data from 6.1 Database Schemas to 19.1

NOTE:

If you cancel an update in progress, all database configuration information will be lost.

1. Click `OraclePaymentInterfaceInstaller_19.1.0.0`.
The installer detects the old OPI version and asks you to continue the upgrade or cancel.
2. Click **OK** and the installer asks you to make sure you want completely remove old OPI.
3. Click **YES** to uninstall the old OPI from your machine.
The OPI 19.1 install begins after removing the previous version of OPI.
4. Select the OPI install folder, and then select the DB type.
When finished, the OPI 6.1 database schemas (`payment_v6` and `new_config`) have been migrated to the OPI 19.1 MySQL database.

OPI Folder Structure

It is possible to install OPI 19.1 as separate components, with the introduction of OPI's configuration API.

This also means the OPI Configuration Tools can now be installed on separate host machines to the main OPI Application, if required.

OPI Service

The Main OPI Service application remains with a similar folder structure to previous versions of OPI, however the default installation path is now:

```
: \OraclePaymentInterface\ v19.1 \Services\OPI
```

OPI Configuration Tools

The configuration tool default installation path is:

```
: \OraclePaymentInterface\ v19.1 \Config
```

In order to use the configuration API, the Configuration Tool installation includes a configuration wizard and full configuration tool.

`LaunchWizard.bat` – contains the most used settings that should be sufficient to allow configuration of a basic working merchant configuration.

`LaunchConfiguration.bat` – also contains some additional advanced settings that may be required in certain installations. See the [Configuration Tool Settings](#) section.

The configuration service is no longer part of the OPI service. As a result, there is now an additional authentication requirement handled post-installation by the new [Settings Admin Tool](#) and [Rotate Passphrase Tool](#). Refer to the relevant sections below for more information.

OPI Logs

The location of the OPI logs that are most commonly referenced is:

```
: \OraclePaymentInterface\ v19.1 \Services\OPI\log\
```

- debug.log
- gateway.log
- system.log
- transaction.log

```
: \OraclePaymentInterface\ v19.1 \LOGS\OPI_Installation.log
```

6

OPI User Administration

OPI 19.1 includes the functionality to manage its own user accounts, rather than integrating to the Windows environment as it did in OPI 6.1. The OPI installer will prompt you to create a “Super” System Administrator user that can be used to create additional users, if required.

User Roles

There are two User Roles in OPI:

- **System Administrator** – has full access to OPI configuration, users, and audit functions.
- **Merchant Administrator** – only has access to the OPI configuration.

Creating a New User

Only System Administrator users can create new users.

To create a new user:

1. Log in to the OPI Configuration tool as the System Administrator, select the **Users** tab, and then click the **Create New User Account** plus icon at the top right of the Users window.
2. Enter the required values to the relevant fields:
 - **Username** – the name the user will enter when logging into the OPI configuration tools.
 - **First Name** – First name of the new user.
 - **Last Name** – Last name of the new user.
 - **Role** – Select **Merchant Administrator** or **System Administrator**
 - **One-time password** – The password the new user will need to enter for their first login. The new user will be prompted to change their password during their first login.
 - **Confirm password** – Confirm the password the new user will need to enter for their first login.
3. **Save** the record when all fields have been completed.

New Users First Login

1. The first time you log in to any of the OPI configuration tools as a new user, you must enter a **Username** and a **One-time Password**.
2. On the Expired Password dialog, enter the **One-time Password** again, and then enter and confirm the **New Password**.
3. Click **OK**.
You can now log in.

Editing Your User Profile

Each user can change their own **First name**, **Last name**, and **Password**, if required. The Username cannot be edited once it has been created.

First Name and Last Name

You can edit your First Name and Last Name after logging in.

1. Select the **Profile** tab.
2. On the **User Information** page, update the values as required, and then click **Save**.

Changing Your Password

1. On the **Profile** tab, click select **Change Password**, enter the **Current password**, and then enter and confirm the **New Password**.
2. Click **Change** when finished.



NOTE:

After changing the password, you should immediately sign out of the configurator and then logon again using the new password. Failure to sign out after changing the password could cause the account to be locked out.

Editing Another User's Account

Only System Administrator users can edit another user's account.

1. Log in OPI configuration tool as the System Administrator user, and then select the **Users** tab.
2. From the list of current users, locate the relevant user and click the **Edit User Account** icon.

A System Administrator can change a user's **First name**, **Last name**, **Role**, **Activate/Deactivate** and **Unlock** an account. **Username** cannot be edited once it has been created.

First name and Last name

- Edit the **First name** and **Last name** as required, and then click **Save** when finished.

Role

- Select a **Role** for the user from the **Role** drop-down list, and then click **Save** when finished.

Deactivating a User Account

The System Administrator can deactivate a user account should it no longer be required.

1. Click the **Deactivate this user account** box to toggle whether the user account is active or not.
 - If the **Deactivate this user account** box is ticked – the account is deactivated
 - If the **Deactivate this user account** box is not ticked – the account is active

Unlocking a User Account

If a user has failed to log in correctly too many times, their account will become locked. An Account is locked out option will display in the Edit User Account window. The Account is locked out setting is not visible unless the user is currently locked out.

- Click the **Account is locked out** box to unlock the user account, and then click **Save** when finished.

Forgotten Passwords

Users

If a user forgets their password, they can select the **Forgot Password** link in the OPI Configuration tool. This will take them to a **Reset Password** page, where they enter their username, and enter and confirm the new password they wish to use.

The password reset request must be approved by a System Administrator before the user can log in using the new password. If the user attempts to log in before the password change request has been approved, they will see an error.

Approving a User's Password Reset Request

Only System Administrator users can approve user password reset requests.

1. Log in as the System Administrator user, and then log in to the OPI Configuration tool and select the **Users** tab.
2. From the list of current users, locate the user that requested a password reset
 - To **Approve** the password reset request click the **Tick** icon
 - To **Reject** the password reset request click the **Cross** icon

Super User

Keep the password for System Administrator secure. You should also create a backup System Administrator account in case the password to the original System Administrator is lost. If you lose the System Administrator credentials, OPI must be reinstalled.

Purge Deactivated Users

Allows System Administrator users to purge any deactivated users and their associated audit trails that have been deactivated for *longer than 90 days*.

- Select **Purge Deactivated Users**, and then click the **Purge** button to proceed.

7

Mutual Authentication

If Mutual Authentication is supported by the PSP and has been enabled within the OPI configuration, communication from OPI to the PSPs will then require a pair of private and public keys in a PKCS#12 – a .pfx file and a root certificate (both provided by the PSP).

- Server0Q.pfx: Used for client authentication of OPI to the PSP.
- Server0QRoot: Validates the public certificate(s) received from the PSPs.

Handling the Client Side Certificate

The communication from OPI to the PSP uses HTTPS with a client certificate for client authentication. OPI presents the client certificate upon request from the server during HTTPS negotiation with the PSP.

- The client side certificate must be called Server0Q.pfx in order for OPI to recognize the file. (Rename the file if it was not supplied with the expected filename.)
- This is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password.
- Upload the Server0Q.pfx to the OPI key subfolder.

Handling the Root Certificate File

- The PSP connection also requires a root key, which must be imported to a root certificate in the form of a JKS (Java Key Store).
- OPI needs this root certificate file in a Java Key store so that OPI can verify the chain of trust on the certificate chain supplied upon connection to the remote PSP server.
- The root certificate file provided by the PSP should be in the format of a .cer or .crt file.
- Upload the Server0QRoot generated to the OPI key subfolder. (Follow steps below to generate the Java Key Store file.)

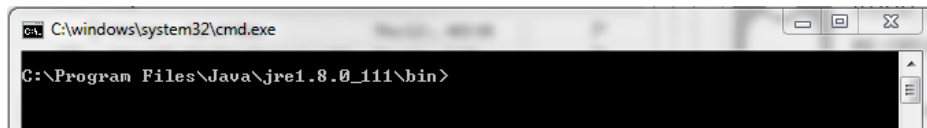
Updating a JKS with a New PSP Certificate

To import a new PSP certificate prior to the expiration of an existing key on an existing OPI installation, the current Server0Q.pfx & Server0QRoot should be deleted from the OPI key folder prior to importing a new certificate file.

Using Keytool

1. Open a command prompt, and change to the Java bin folder, otherwise you may find the *keytool* command is not be recognized.

The exact path of your Java bin folder will vary, but may be similar to the example path shown below:



```
C:\windows\system32\cmd.exe
C:\Program Files\Java\jre1.8.0_111\bin>
```

2. In order to import the root certificate supplied by the PSP into a Java keystore, perform the steps below in sequence:
 - a. Create a new Java keystore,
 - b. Delete the default key from the Java Key Store
 - c. Import the supplied root certificate in its place

In the following example commands, the root .cer/.crt file is named ca-cert.cer, when importing the production .cer/.crt into the JKS adjust filenames and paths to be relevant to your filenames and environment.

```
keytool -genkey -alias tempalias -keystore
D:\OraclePaymentInterface\v19.1\Services\OPI\key\Server0QRoot
```

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

The values will be removed in the next step so can be left blank, i.e. press enter at each prompt, watch out to confirm correct prompt.

To use the same key password for the keystore password when prompted, i.e. (RETURN if same as keystore password), press Enter

```
keytool -delete -alias tempalias -keystore
D:\OraclePaymentInterface\v19.1\Services\OPI\key\Server0QRoot
```

```
keytool -import -alias myrootca -file
D:\OraclePaymentInterface\v19.1\Services\OPI\key\ca-cert.cer -keystore
D:\OraclePaymentInterface\v19.1\Services\OPI\key\Server0QRoot -trustcacerts
```

4. View the new Java keystore details if required by running the following command:

```
keytool -list -keystore D:\OraclePaymentInterface\v19.1\Services\OPI\key\Server0QRoot
```

All certificate passwords must be configured within OPI once the certificates are uploaded to the OPI key subfolder;

- PSP Configuration | Private Key Cert. Password – Is the Server0Q.pfx password
- PSP Configuration | Root Certificate Password – Is the Server0QRoot password

 **NOTE:**

The Certificate expiration dates will vary depending on what was set when the certificates were created. You can check the expiration date in the properties of the certificate files.

The certificates must be updated prior to the expiration date to avoid downtime to OPI.

OPI Mutual Authentication – Summary

The diagram below shows the certificates used at each process during communication negotiation.

OPI		PSP
Client		Server
<p>Server0Q.cer PSP rootCa certificate loaded to JKS , equivalent of root certificate folder</p> <p>Server0Q.pfx (OPI Private & Public Key)</p>	<p>-----> Client Hello</p> <p><----- Server Hello</p> <p><----- Server Presents its host Certificate</p> <p>Client Validates Server Authenticity</p> <p><----- Server Requests Clients Host Certificate</p> <p>-----> Client Presents its host Certificate</p> <p>Server Validates Server Authenticity</p> <p>Server/Client negotiate encryption</p> <p>Secure communication negotiated</p>	<p>PSP Private Key</p> <p>OPI's Root Certificate</p>

8

Audit

OPI includes an Audit function to keep track of any configuration updates. Only System Administrator level users can view the Audit information. The System Administrator user should log in to the OPI Configuration tool, and go to the **Audit** tab.

Audit Trail Search

By default, no Audit Trail records are visible. Use the available filters to narrow the search criteria as required.

- Event type;
 - All
 - Application – Configuration related events
 - Security – User account related events
 - Setup – Events performed by installation process
- Description – Events containing the Description value entered
- Username – Events containing the Username value entered
- IP Address – Events containing the IP Address value entered
- From date – Enter the date to search from in the format yyyy-mm-dd, or click the calendar icon and select the required date.
- To date – Enter the date to search up to in the format yyyy-mm-dd, or click the calendar icon and select the required date.

Click the **Search** button to display the relevant Audit Trail Events.

If there are multiple pages of results, use the page numbers at the bottom of the window to navigate to a particular page, or the left and right arrows to move forward or backwards one page at a time.

By default, the search results are displayed in descending **Event Time** order. The search results can be sorted as required by clicking the relevant column header.

To view details of a particular event, click the **Show Event Details** magnifying glass icon on the relevant row.

Depending on the event type, you may see additional information in the **Pre-snapshot** and **Post-snapshot** fields, showing the before and after values, if the event was a configuration update.

Audit Trail Purge

Allows a System Administrator level user to purge any Audit Trail events that are older than 90 days.

- Click the **Purge** button to proceed.

9

Silent Installation

OPI 19.1 includes the ability to perform a Silent Installation of the OPI software. The silent installation does not currently include any merchant configuration, only the installation of the OPI software.

To perform a Silent install you must first perform a normal manual installation in record mode, which will produce a response file that can be used later by a silent mode software installation to complete without user intervention.

To execute the installer in the record or silent mode, execute it from a command prompt in the directory where the OPI installer is located, applying the relevant switch.

/r - Record mode stores information about the data entered and options selected by the user in a response file, which by default is called setup.iss, and is created in the system's Windows folder.

For Example;

```
OraclePaymentInterfaceInstaller_19.1.0.0.exe /r
```

/s - Silent mode reads information about the data to be entered and options to select, from a response file, which it expects by default to be called setup.iss, and to be located in the same folder you are executing the OPI installer from.

For Example;

```
OraclePaymentInterfaceInstaller_19.1.0.0.exe /s
```

Specify Alternative Response File

Using the /f1 option enables you to specify where the response file is (or where it should be created) and what its name is, as in `Setup.exe /s /f1"C:\Temp\Setup.iss"`. Specify an absolute path; using a relative path gives unpredictable results. The /f1 option is available both when creating a response file (with the /r option) and when using a response file (with the /s option).

Specify Alternative Log File

When running an InstallScript installation in silent mode (using the /s option), the log file Setup.log is by default created in the same directory and with the same name (except for the extension) as the response file. The /f2 option enables you to specify an alternative log file location and file name, as in `Setup.exe /s /f2"C:\Setup.log"`. Specify an absolute path; using a relative path gives unpredictable results.

If required the installation values, passwords, user names, etc. in the setup.iss file can be modified using a text editor.

10

OPI Services

The OPI 19.1 installation includes three windows services: OPI Config Service, OPI Service, and OPI Utility Service.

OPI Config Service

Deals with connections from applications used to configure OPI, such as OPI configuration Tool and Wizard.

OPI Service

- Is the main OPI Application service, listening for connections to OPI from POS/PMS and making connections to PSP
- Always restart the OPI Service after creating or changing any configuration.

OPI Utility Service

The OPI Utility Service handles any configuration values that are encrypted, such as passwords & passphrases.

Changing the OPI Config Service Port

During installation, the OPI Config Service Port is set to 8090. To change this port number, perform the following:

- Execute `:\OraclePaymentInterface\v19.1\Services\ConfigService\OPIConfigService.exe`
- Select the Java Tab
- Change the `-DserverPort=8090` value as required
- Restart the OPI Config Service

By default, the Configuration tools will still start with the value 8090. You must remember and re-enter the correct host details each time you start any of the configuration tools.

Settings Administration Tool

The Settings Administration Tool is the replacement for rwregistry. This new application is located in the following location:

`\OraclePaymentInterface\v19.1\Services\ConfigService\LaunchSettingsAdminTool.bat`

Using the Settings Administration Tool

1. To launch the application, execute **LauchSettingsAdminTool.bat** as Administrator
2. Select the desired language in the welcome screen, and then click Continue.

 **NOTE:**

The Settings Administration Tool does not allow users to change the Native Driver passphrase. The Native Driver passphrase can now be updated using the standard Configuration Tool.

Updating the OPI Schema Password

1. To change the DB credentials, use the **Database Settings** menu option.
2. Enter the OPI Schema **DB User**, the **New DB password** to be used, and the super user accounts **Username** and **Password**.
3. Only the super user account has the permissions to update DB settings.
4. Click **Update** when ready to change the password.

 **NOTE:**

This changes the database credentials in the OPI configuration, it does not update the credentials in the database itself, this should be performed by the sites database administrator.

Oracle Payment Interface Settings Administration

ORACLE Payment Interface

Update DB Settings Update

Database Settings

Configuration Passphrase

Update the OPI DB settings using the fields below.

The new password must comply with the following complexity requirements:
at least 8 characters in length and include at least one uppercase letter, one lowercase letter, one number and one special character from the following list: !@#\$%^&*

DB User:

New DB password:

Confirm new DB password:

Username:

Password:

- The application should report the Database settings have been updated successfully
5. If the message “The application was unable to save the changes, please make sure you are running the application as Administrator” appears, close the application, re-run as Administrator, and repeat the previous steps.

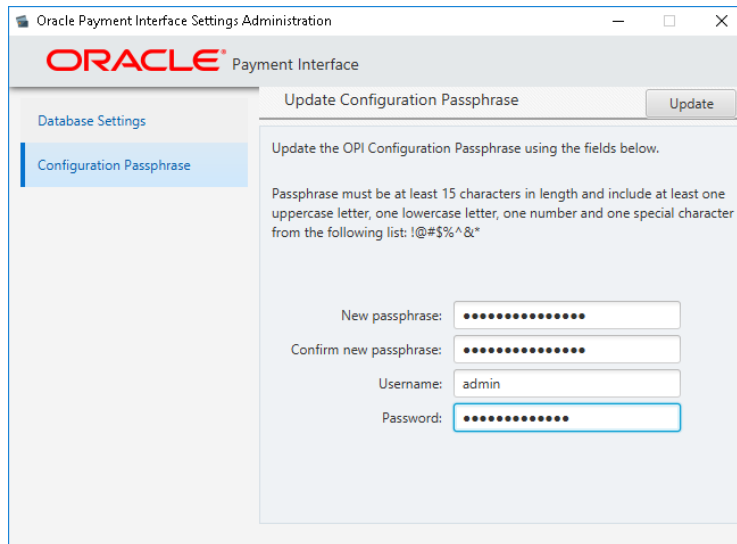
Updating the OPI Configuration Passphrase

To change the Configuration Passphrase, which is the passphrase used by Configuration Service to communicate with the Configuration Tool/Wizard:

1. Use the **Configuration Passphrase** menu option. Enter and Confirm the New passphrase, and the super user accounts **Username** and **Password**.
2. Click **Update** when ready to change the passphrase.

NOTE:

This changes the passphrase in the OPI configuration, it does not update the passphrase in the Configuration Tools/Wizard. This must also be updated to match the new passphrase using the Configuration Wizard Rotate Password utility.

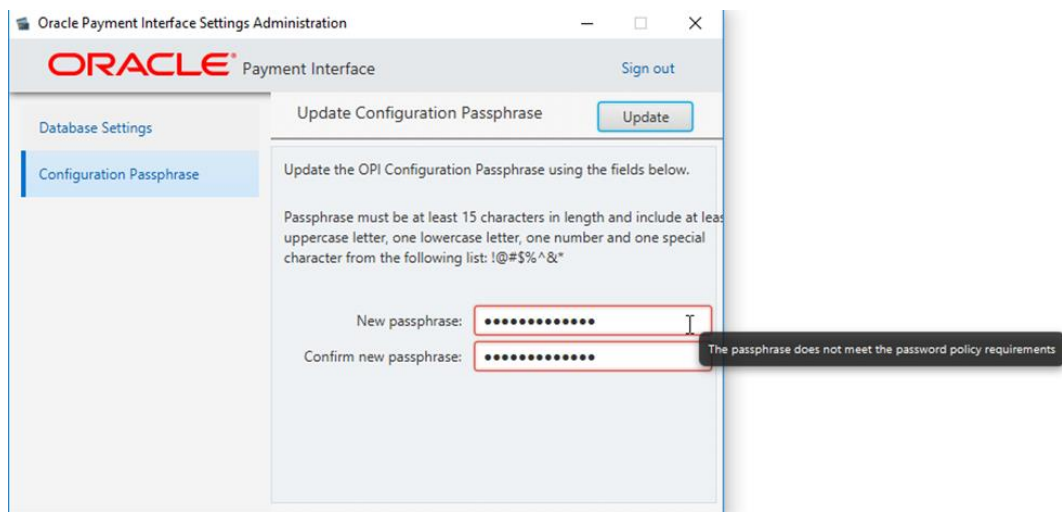


The application should report Passphrase has been updated successfully.

3. If the application reports “*The application was unable to save the changes, please make sure you are running the application as Administrator*”, close the application, re-run as Administrator, and repeat the previous steps.

 **NOTE:**

The application includes validations for password and passphrase complexity. If your password or passphrase does not meet the minimum requirements, the fields will be outlined in red. Hovering the cursor over the fields provides more information.



- The application will only prompt for Super User account credentials once. After that, you will be able to perform an action without entering the credentials again. Additionally, the Sign out option will be shown on the upper right corner of the application.
4. When finished, click **Sign out**.

12

Configuration Tools – Rotate Passphrase

If you change the OPI Configuration Service passphrase, you must also change the Configuration tool passphrase to match the new value that was set on OPI Config Service side so they can continue communicating.

Using the Rotate Passphrase Utility

The Rotate Password utility uses the OPI Configuration tool, launched in a different mode. Use the link in the config folder to start the Configuration tool in Rotate Passphrase mode:

```
: \OraclePaymentInterface\v19.1\Config\RotatePassphrase.bat
```

To launch the application, execute `RotatePassphrase.bat` as Administrator

1. Enter and confirm the New passphrase (this new passphrase must match the passphrase that was set on OPI Configuration Service side previously).
2. The **Host** and **Port** should match the details of the **OPI Config Service** that you are attempting to connect to.
3. Enter your **Username** and **Password** credentials, and then click **Update**.
4. Click **Update** to finalize the passphrase change.

Oracle Payment Interface - Configuration Wizard

Update Communication Passphrase

Update the communication passphrase using the fields below. The new passphrase must match the OPI's Configuration Service passphrase

Passphrase must be at least 15 characters in length and include at least one uppercase letter, one lowercase letter, one number and one special character from the following list: !@#\$%^&*

New passphrase: Confirm new passphrase:

Host:

Port:

Username:

Password:

Select Language:

ORACLE
HOSPITALITY

Update Close

- If the user credentials are correct and the new passphrase matches the OPI Config Service passphrase, the application will display the following message: *Passphrase has been updated successfully.*

- The OPI Configuration Tool/Wizard should now be able to communicate with OPI Config Service.
- If the new passphrase does not match the OPI Config Service passphrase, the application will display the following message: *Unable to communicate with configuration service, please make sure that the new passphrase matches the passphrase on the Configuration Service side.*
- If the user credentials are incorrect, the application will display the following message: *The username or password is incorrect.*
- If the application was not run as administrator, the application will display the following message: *The application was unable to update the passphrase, please make sure you are running the application as Administrator.*

13

OPI Client Certificate Creator Utility

The OPI Client Certificate Creator utility can be used to create self-signed certificates if required, and may be used to assist with installations of OPI

The Client Certificate Creator is primarily used for creating certificates for use by the Opera client. If a site uses Token Proxy (Self Hosted or Cloud Token Proxy), certificates required for the Opera client in an OnPremise Token Exchange situation are managed by the configuration tools.

The Client Certificate Creator could also be used to assist with setup of test environments, but it is not recommended for use in any public-facing situations because the certificates produced will only be self-signed.

Using the Client Certificate Creator

1. Navigate to the `:\OraclePaymentInterface\19.1\Config\` directory and run **CertCreator.jar**.
2. Complete the details as required, and then click **Create Certificate Files**.

Oracle Payment Interface - Client Certificate Creator

Chain Code:

Merchant Organization Department:

Merchant Organization Name:

Merchant City:

Merchant State:

Merchant Country:

Passwords are case sensitive.

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

Password:

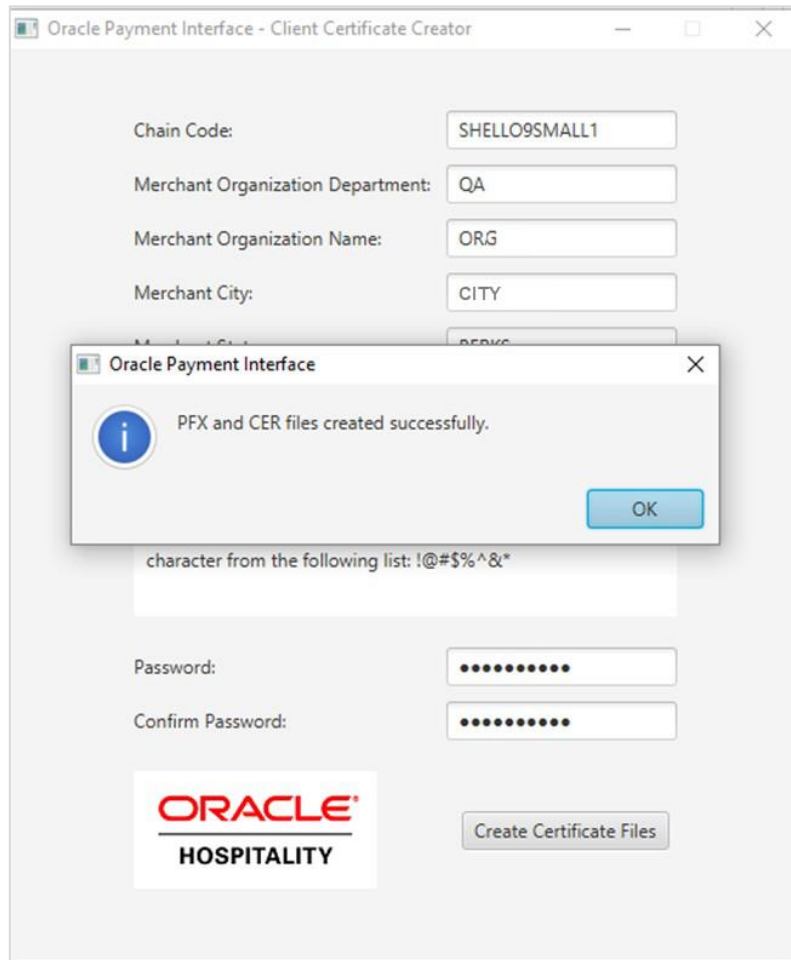
Confirm Password:

ORACLE
HOSPITALITY

Create Certificate Files

3. A standard Windows save file dialog box appears. Enter a name for the new certificate files and specify a save location.
4. If you do not see the save file popup, check the red text at the bottom of the window. The red text displays any incorrect values you entered.

Although the **Save as type** field shows (.pfx), both a .pfx and .cer will be created in the location specified when you save the files.



The certificate expiration dates will be 5 years from the date of creation.

The OPI Client Certificate Creator fields translate as follows to the standard certificate attributes:

Chain Code	> CN (CommonName)
Merchant Organization Department	> OU (OrganizationalUnit)
Merchant Organization Name	> O (Organization)
Merchant City	> L (Locality)
Merchant State	> S (StateOrProvinceName)
Merchant Country	> C (CountryName)

14

Pay@Table Certificate

Pay@Table in OPI 19.1 requires a certificate and matching password.

Update Pay@Table PW

If doing a new OPI installation on a live site, the PSP should provide a new Pay@Table certificate and the password that matches it. The certificate goes in C:\OraclePaymentInterface\v19.1\Services\OPI\key.

The password can be entered during the OPI install, or afterwards with these steps:

1. Double click \OraclePaymentInterface\v19.1\Config\LaunchConfiguration.bat and login with the SuperUser name and password.
2. Go to Pay at Table | Service Settings, and enter the Certificate password and then confirm it.
3. Save changes and restart the OPI service.

15

Import/Export OPI Configuration

The OPI import/export configuration functionality enables user to back up the OPI configuration data and/or duplicate it to another OPI instance.

Export Configuration

1. Log in to the OPI configuration tool as the System Administrator, select **Export Configuration**.
2. Click **Export**.
3. Choose an export location and filename, and then click **Save** to export the configuration to an XML file.

Do not change the XML file, except the following scenarios:

- The merchant configuration in XML file no need import to another OPI instance.
 - Open the XML file, go to <merchant> section, changes *import_enabled* flag to false.
- Changing site-specific information like IP, etc.

Import Configuration

1. Log in to the OPI configuration tool as the System Administrator, select **Import Configuration**.
2. Click **Import**.
3. Click **OK** on the prompt about backing up the database.
4. Select a saved XML configuration file, and then click **OK** to import the configuration.
5. Click **OK** on the prompt about import successful, and manually restart OPI service or reboot machine to make the new imported configurations effective.

Reset Security Data

Resetting security data is not mandatory for all imports. It is only needed when imported configuration changes modify the way OPI communicates with POS/PMS/Pay@Table/PSP, or when a new merchant has been imported.

1. Log in to the OPI configuration tool as the System Administrator, select **Import Configuration**, and then click **Reset**.
2. A screen appears with multiple options, similar to the following:

Merchant Options

When imported OPI configuration contain RES merchant information, and enabled “Pay at Table Service” on Core Configuration page, need reset RES DB credential.

- Select Merchant Type – **POS**, then select the specific Merchant ID to reset.
 - RES DB User: RES DB user for Pay at Table integration to use.
 - RES DB Password: password for the RES DB user.

When imported OPI configuration contain PMS merchant information, and disabled “OPERA Token Service” on Core Configuration page, need reset IFC8 key.

- Select Merchant Type – **PMS**, then select the specific Merchant ID to reset.
 - IFC8 Key: generates the IFC8 key to secure the communication between PMS IFC8 and OPI.

When imported OPI configuration contain PMS merchant information, and enabled “OPERA Token Service” on Core Configuration page, need reset IFC8 key and Token Exchange authentication.

- Select Merchant Type - **PMS**, then select the specific Merchant ID to reset.
 - IFC8 Key: generates the IFC8 key to secure the communication between PMS IFC8 and OPI.
 - Authentication User: authentication user for Token Exchange.
 - Authentication Password: password for the authentication user.
 - Certificates: generate the certificate for the Token Exchange, if needed.

When imported OPI configuration contain PMS merchant information, and enabled “Cruise PMS” on Core Configuration page, need reset IFC8 key.

- Select Merchant Type - **PMS**, then select the specific Merchant ID to reset.
 - IFC8 Key: generates the IFC8 key to secure the communication between PMS IFC8 and OPI.

POS Service Options

When the imported OPI configuration enabled “POS Service” on Core Configuration page, need reset OGDH driver certificate password, or reset native driver passphrase.

- If you select **OGDH** mode:
 - Certificate password: specify a password for the certificate. By default, the certificates are generated during the OPI installation.
- If select **Native Driver** mode:
 - Passphrase: passphrase that secures the communication between POS and OPI.



NOTE:

Native Driver mode does not require a certificate. However, the passphrase must match the POS configuration.

PSP Configuration Options

When the imported OPI configuration enabled “Mutual Authentication” on PSP configuration page, need reset certificate password and reimport certificate.

- Private Key Cert Password: private key password.
- Root Certificate Password: root certificate password.
- Import Certificate: imports certificates to the OPI key directory.

PSP Token Exchange Options

When the imported OPI configuration enabled “OPERA Token Service” on Core Configuration page, need reset certificate password and reimport certificate.

- Private Key Cert Password: private key password.
- Root Certificate Password: root certificate password.
- Import Certificate: imports certificates to the OPI key directory.

Pay at Table Options

When the imported OPI configuration enabled “Pay at Table Service” on Core Configuration page, need reset Pay at Table certificate password and reimport certificate.

- Certificate Password: password for the Pay at Table certificate.
- Import Certificate: imports certificates to the OPI key directory.

16

Uninstallation and Modification of Install

IF UPGRADING OPI, YOU MUST READ THE [UPGRADING THE OPI SECTION](#) FIRST.

Uninstalling OPI

To uninstall OPI you can either:

- Run `OraclePaymentInterfaceInstaller_19.1.0.0.exe` again. The installer detects the existing installation and gives you the option to **Remove** (uninstall) OPI.
- Use the **Add/Remove Programs** option via Programs and Features in Windows Control Panel.

During uninstallation you will be asked if you want to remove the OPI database schema. If this is required, you must provide the Root user credentials again, because the credentials are not stored during installation.

To complete the uninstallation of OPI, you must reboot of the host machine.

Modifying OPI

To modify your OPI installation, you can either:

- Run `OraclePaymentInterfaceInstaller_19.1.0.0.exe` again. The installer detects the existing installation and gives you the option to Modify (add/remove components) the install.
- Use the **Add/Remove Programs** option via Programs and Features in Windows Control Panel. Right-click the OPI entry, and then select **Change**.

During modification you will be asked which features you want to add or leave installed.

For example, on the **Select Features** page if you only have **OPI Services** component selected, and you wish to add the **Configuration Tool** component, you should select both OPI Services (To leave this installed) & Configuration Tool (To install this component).

If you were to only select **Configuration Tool**, the modification process will attempt to add the Configuration Tool component, but also to remove **OPI Service**.

17

Configuration Settings

You can configure POS/PMS merchants in the Configuration wizard and the configured settings are available in the Configuration tool (`LaunchConfiguration.bat`).

Section	Setting Name	Constraint	Default Value	Description
Merchant Configuration				
	ID		Blank	Will display the Merchant ID of any POS Merchants that are configured, and the Opera Chain Property Code for any PMS Merchants that have been configured
	Name		Blank	Will display the Name of any Merchants that have been configured
	Type		Blank	Will display the POS/PMS Merchant Type of any Merchants that have been configured
Merchants Merchant Information				
	POS Type	Only displayed for POS Merchants	Set during Merchant Configuration	Type of POS used by the Merchant
	Merchant Type	Only displayed for POS Merchants	Restaurant	Type of industry the Merchant belongs to Restaurant Retail
	Merchant ID	Only displayed for POS Merchants	Set during Merchant Configuration	Merchant Unique Identifier
	OPERA Chain	Only displayed for PMS Merchants	Set during Merchant Configuration	Opera Chain code for the Merchant
	Property Code	Only displayed for PMS Merchants	Set during Merchant Configuration	Opera Property code for the Merchant
	Name		Set during Merchant Configuration	Name of the Merchant

Section	Setting Name	Constraint	Default Value	Description
	City		Set during Merchant Configuration	City location of the Merchant
	State/ Province		Set during Merchant Configuration	State or Province location of the Merchant
	Country/Region		Set during Merchant Configuration	Country location of the Merchant
Merchants Settings				
	RES DB Host	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	192.0.2.1	RES Database hostname or IP Address
	RES DB Port	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	2638	RES Database port number
	RES DB Name	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	micros	RES DB Name
	RES DB User	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	Blank	RES Database Username
	Confirm RES DB User	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	Blank	RES Database Username
	RES DB Password	Only visible if the Merchant	Blank	RES Database Password

Section	Setting Name	Constraint	Default Value	Description
		POS Type = RES if Pay at Table Service = ON		
	Confirm RES DB Password	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	Blank	RES Database Password
	Initial DB Pool size	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	20	Number of connections created when database pool is initialized
	Max Active Connections	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	40	Max Number of connections allowed in database pool
	Connection wait time	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	20	Milliseconds database pool will wait for connection to be returned
	Min Idle Connections	Only visible if the Merchant POS Type = RES if Pay at Table Service = ON	10	Min Number of idle connections in the database pool
	Simphony Service URL	Only visible if the Merchant POS Type = Simphony	http://192.0.2.1:8080/EGateway/SimphonyPosApiWeb.asmx	URL of the Simphony Transaction Services POSAPI
	Tenders Employee Number	Only visible if the Merchant POS Type = Simphony	1	Employee Number used to retrieve the Tender definition from Simphony

Section	Setting Name	Constraint	Default Value	Description
	Users Employee Number	Only visible if the Merchant POS Type = Symphony	1	Employee Number used to retrieve the Employee definition from Symphony
	Tables Employee Number	Only visible if the Merchant POS Type = Symphony	1	Employee Number used to retrieve the Table definition from Symphony
Merchants IFC8 Settings		Only visible if the Merchant Type = IFC8		
	IFC8 Host		Set during Merchant Configuration	IFC8 machines Host name or IP Address
	IFC8 Port		Set during Merchant Configuration	IFC8 port number
	IFC8 Key		Generate during Merchant Configuration	Use to generate an IFC8 Communication key Apply FidCrypt0S prefix to the generated key when configuring the key in the IFC8 software
	Only Do Refund		Disabled	When enabled, OPI will always send a refund request to PSP whenever it receives a transaction request with a negative amount from OPERA. When disabled, OPI supports both void and refund.
	Tenders: AliPay		AB	PMS Tender mapping
	Tenders: Alliance		AL	PMS Tender mapping
	Tenders: American Express		AX	PMS Tender mapping
	Tenders: China UnionPay		CU	PMS Tender mapping
	Tenders: China UnionPay Debit		CD	PMS Tender mapping
	Tenders: Debit		DD	PMS Tender mapping

Section	Setting Name	Constraint	Default Value	Description
	Tenders: Diners Club		DC	PMS Tender mapping
	Tenders: Discover		DS	PMS Tender mapping
	Tenders: EC Chip		EC	PMS Tender mapping
	Tenders: Gift Card		GC	PMS Tender mapping
	Tenders: Giro Card		BC	PMS Tender mapping
	Tenders: JCB		JC	PMS Tender mapping
	Tenders: Maestro		ME	PMS Tender mapping
	Tenders: MasterCard		MC	PMS Tender mapping
	Tenders: MasterCard Debit		MD	PMS Tender mapping
	Tenders: PayPal		PC	PMS Tender mapping
	Tenders: Reserve-01		ZZ	PMS Tender mapping
	Tenders: Reserve-02		ZZ	PMS Tender mapping
	Tenders: Reserve-03		ZZ	PMS Tender mapping
	Tenders: Reserve-04		ZZ	PMS Tender mapping
	Tenders: Reserve-05		ZZ	PMS Tender mapping
	Tenders: Reserve-06		ZZ	PMS Tender mapping
	Tenders: Reserve-07		ZZ	PMS Tender mapping
	Tenders: Reserve-08		ZZ	PMS Tender mapping
	Tenders: Reserve-09		ZZ	PMS Tender mapping

Section	Setting Name	Constraint	Default Value	Description
	Tenders: Reserve-10		ZZ	PMS Tender mapping
	Tenders: Reserve-11		ZZ	PMS Tender mapping
	Tenders: Reserve-12		ZZ	PMS Tender mapping
	Tenders: Reserve-13		ZZ	PMS Tender mapping
	Tenders: Reserve-14		ZZ	PMS Tender mapping
	Tenders: Reserve-15		ZZ	PMS Tender mapping
	Tenders: Visa		VA	PMS Tender mapping
	Tenders: Visa Debit		VD	PMS Tender mapping
	Tenders: Visa Electron		VE	PMS Tender mapping
	Tenders: V Pay		VP	PMS Tender mapping
	Tenders: WeChat Pay		WE	PMS Tender mapping
Merchants Token Exchange Settings		Only displayed for OPERA Merchants		
	Authentication User		Set during Merchant Configuration	Username for Opera Authentication
	Authentication Password		Set during Merchant Configuration	Password for Opera Authentication
	Confirm Password		Set during Merchant Configuration	Password for Opera Authentication
Merchants Terminals		Only displayed if PSP Configuration Communication Mode = Terminal		

Section	Setting Name	Constraint	Default Value	Description
	Workstation ID		Set during Merchant Configuration	ID of the workstation using the PED
	Terminal IP/Host Name		Set during Merchant Configuration	IP Address/Host Name of the PED, the Workstation should use
Merchants Pay at Table Devices		Only displayed if Pay at Table Service = ON		
	Device ID		Set during Merchant Configuration	PED device unique identifier
	Query By		Set during Merchant Configuration	Whether the device will attempt to pick up a check using the Table Number of the Check Number
	Revenue Center ID		Set during Merchant Configuration	ID of the Revenue Center associated with the device
Core Configuration				
	POS Service		Set during install	Enables/Disables the POS Service
	OPERA IFC8 Service		Set during install	Enables/Disables the Opera IFC8 Service
	OPERA Token Service		Set during install	Enables/Disables the Opera Token Exchange Service
	Enable Cruise PMS		Disabled	Enables/Disabled the Cruise PMS Service
	Pay at Table Service		Set during install	Enables/Disables the Pay at Table Service
	Enforce TLS 1.2 protocol and above only		Enabled	Enforce TLS 1.2+ only on POS & OPERA Token Service NOTE: If using OGDH and CE workstations, this TLS 1.2 option has to be disabled since the CE workstations will not be able to communicate to OPI using TLS 1.2.

Section	Setting Name	Constraint	Default Value	Description
				Native driver sites can still uses CE workstations with TLS 1.2 enabled.
	Log retain days		30	Number of days the OPI wrapper log files will be retained. - OPISvcWrapper.YYYY-MM-DD.log - UtilitySvcWrapper.YYYY-MM-DD.log
	Transaction retention days		30	Number of days the transactions remain in the h_transline table. The default value is 30. After this time period, the data will be moved to the h_transhistory table.
	Transaction history retention days		365	Number of days the transactions remain in the h_transhistory table. The default value is 365. After this time period, the data will be purged from the database.
	Server time zone		Set during install	Time Zone used by the OPI Service Set during installation to match the time zone of the host machine
	Refresh OPI configuration at		00:29	Scheduled Hour & Minute for configuration refresh Note this does not restart the OPI Service, it will just re-read the configuration from the database
	HTTP Proxy Host		Blank	HTTP Proxy Host name or IP, if no proxy is needed leave this field empty
	HTTP Proxy Port		Blank	HTTP Proxy Port, if no proxy is needed leave this field empty
	Select language		English US	Language used for OPI's status/error messages sent back to POS/PMS
	Request Encoding		UTF-8	Encoding type of request messages
	Enable UTF-8 encoding of response messages		Disabled	Select to enable UTF-8 encoding of POS response messages
POS Service				
	Mode		Set during install	POS Service communication mode Native Driver or OGDH

Section	Setting Name	Constraint	Default Value	Description
	Port		5098	POS Service port number
	Use Check Open Time for CC Repost		Enabled	This should always be enabled otherwise repost will not work.
	Enable Secure Communication		Enabled	This should always be enabled for secure communication
	Passphrase	Only visible if Mode = Native Driver	Set during install	Passphrase for communication between POS & OPI
	Confirm Passphrase	Only visible if Mode = Native Driver	Set during install	Passphrase for communication between POS & OPI
	Certificate password	Only visible if Mode = OGDH	Set during install	Password of POS service certificate
	Confirm certificate password	Only visible if Mode = OGDH	Set during install	Password of POS service certificate
Opera Token Service				
	Mode		HTTPS Mina	Communication Mode - HTTPS Mina mode was introduced to resolve performance issues - HTTPS legacy mode
	Port		5012	
Opera IFC8 Service				
	Communication test interval		73	Test connection interval in seconds
	Enable test communication Heartbeat		Enabled	Select to periodically test the connection to IFC8
	Decoder timeout		1000	Milliseconds OPI will wait for full IFC8 message to be received
	Bulk Tokenization Batch Size		50	Number of items in a single tokenization request
	Enable Update Token Support		Enabled	The option is for Cruise PMS only. Select to enable Bulk Tokenization through the IFC8 channel. To allow Tokenization support for Cruise integration

Section	Setting Name	Constraint	Default Value	Description
				Does not affect Tokenization's coming from Opera
	Return receipt's full print data		Disabled	Select to return receipts full print data to IFC8 in Cross Reference fields To allow Print on Folio
	Enable UTF-8 for receipt's		Disabled	Select to enable UTF-9 encoding for PMS response messages
PSP Configuration				
	Communication Timeout		60	Seconds OPI will wait for a timeout from the PSP
	Connect Timeout		10	Seconds OPI will wait before initiating a connection to the PSP
	Enable Mutual Authentication		Disabled	
	Private Key Cert. Password	Only relevant if Enable Mutual Authentication = Enabled	Blank	Private Key certificate password for 2way authentication with PSP
	Confirm Private Key Cert. Password	Only relevant if Enable Mutual Authentication = Enabled	Blank	Private Key certificate password for 2way authentication with PSP
	Root Certificate Password	Only relevant if Enable Mutual Authentication = Enabled	Blank	Root certificate password for 2way authentication with PSP
	Confirm Root Certificate Password	Only relevant if Enable Mutual Authentication = Enabled	Blank	Root certificate password for 2way authentication with PSP
	Enable Top up authorization		Disabled	Select to enable Top up authorization transactions if the PSP supports this functionality. Relates only to POS Native Driver.
	Communication Mode		Set during installation	Terminal Mode - OPI maintains WS > PED mapping and communicates directly to PED Middleware Mode - PSP maintains

Section	Setting Name	Constraint	Default Value	Description
				WS > PED mapping and handles communication to PED
	Terminal Port	Only visible if Communication Mode = Terminal	443	Port Number for PSP devices
	Terminal Context	Only visible if Communication Mode = Terminal	Blank	If the PSP's device require a context in their connection url enter the context here. Leave blank if not required
	Enable TLS	Only visible if Communication Mode = Terminal	Enabled	This is enabled by default for all installations
	Primary Host	Only visible if Communication Mode = Middleware	https://pspsghost:443	The PSP Host URL for Financial Transactions
	Failover Host	Only visible if Communication Mode = Middleware	https://pspsfailoverhost:443	The PSP Failover Host URL for Financial Transactions If a failover URL is not available, leave this blank
	Enable Inquiry Mode for Transactions Reversal	Only visible if Communication Mode = Middleware	Enabled	Select to allow OPI to perform an inquiry to verify the status of a transactions before sending a reversal request to the PSP Inquiry mode is not supported in Terminal Mode, a reversal will always be sent.
PSP Token Exchange				
	Primary Host URL		Blank	The PSP Host URL for Token Exchange
	Failover Host URL		Blank	The PSP Failover Host URL for Token Exchange If a failover URL is not available, leave this blank
Pay at Table Service Settings				

Section	Setting Name	Constraint	Default Value	Description
	Mode		HTTPS	Select Communication Mode; HTTPS, HTTP, TCP Typically in a production environment this would be set to HTTPS. But it could be set to HTTP temporarily to trouble shoot communication problems.
	Enable Secure Connection	Only available if Pay at Table Mode = HTTP or TCP	Enabled	Select to enable secure connection through SSL
	TLS 1.2 protocol and above only		Enabled	Enforce TLS 1.2+ protocol for connections from Pay at Table devices
	Port		8992	Pay at Table Service port number
	Certificate password		Blank	Password of the Pay at Table certificate
	Confirm Certificate password		Blank	Password of the Pay at Table certificate
	Device Session Lifespan		30	Minutes Pay at Table device can remain idle before expiring
	Session Polling Interval		5	Device Session verification interval in minutes
Pay at Table POS API Settings				
	Mode		Expect 100-continue, not supported	Relates to the Transaction POSAPI that OPI will use. Default value should fit most situations, the 'supported' option was required for RES until version 4.7 Expect 100-continue, not supported - will send whole message content in one message Expect 100-continue, supported - will send the message headers first, then send the message content separately
	Communication Timeout		30	Number of seconds OPI will wait for a response from the POSAPI before timing out

Section	Setting Name	Constraint	Default Value	Description
	Return Printed Check		Disabled	Select to return printed check
	Enable UTF-8 for receipt's		Disabled	Select to enable UTF-8 encoding of Pay at Table response messages
	RES API URL	Only visible is Merchant POS Type = RES	http://192.0.0.1/ResPosApi Web/	URL of the RES POSAPI
	Tenders: AliPay		0	POS Tender object number mapping
	Tenders: Alliance		0	POS Tender object number mapping
	Tenders: American Express		0	POS Tender object number mapping
	Tenders: China UnionPay		0	POS Tender object number mapping
	Tenders: China UnionPay Debit		0	POS Tender object number mapping
	Tenders: Debit		0	POS Tender object number mapping
	Tenders: Diners Club		0	POS Tender object number mapping
	Tenders: Discover		0	POS Tender object number mapping
	Tenders: EC Chip		0	POS Tender object number mapping
	Tenders: Gift Card		0	POS Tender object number mapping
	Tenders: GiroCard		0	POS Tender object number mapping
	Tenders: JCB		0	POS Tender object number mapping
	Tenders: Maestro		0	POS Tender object number mapping
	Tenders: MasterCard		0	POS Tender object number mapping
	Tenders: MasterCard Debit		0	POS Tender object number mapping

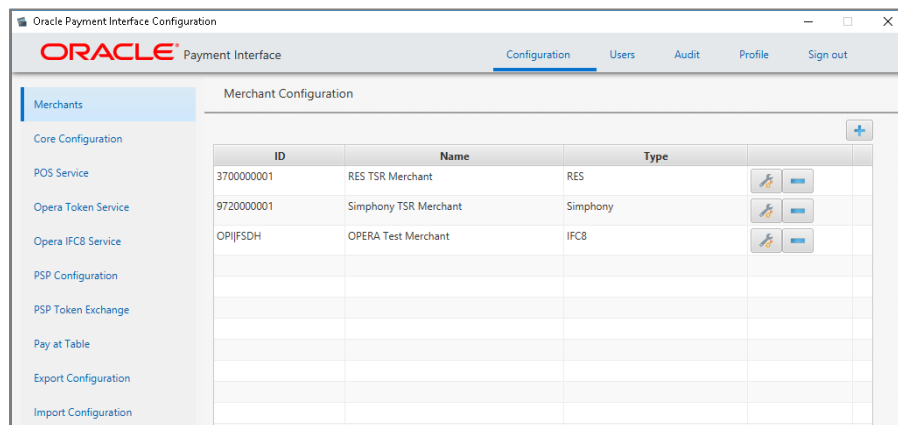
Section	Setting Name	Constraint	Default Value	Description
	Tenders: Paypal		0	POS Tender object number mapping
	Tenders: Print Check		0	POS Tender object number mapping
	Tenders: Reserver-01		0	POS Tender object number mapping
	Tenders: Reserver-02		0	POS Tender object number mapping
	Tenders: Reserver-03		0	POS Tender object number mapping
	Tenders: Reserver-04		0	POS Tender object number mapping
	Tenders: Reserver-05		0	POS Tender object number mapping
	Tenders: Reserver-06		0	POS Tender object number mapping
	Tenders: Reserver-07		0	POS Tender object number mapping
	Tenders: Reserver-08		0	POS Tender object number mapping
	Tenders: Reserver-09		0	POS Tender object number mapping
	Tenders: Reserver-10		0	POS Tender object number mapping
	Tenders: Reserver-11		0	POS Tender object number mapping
	Tenders: Reserver-12		0	POS Tender object number mapping
	Tenders: Reserver-13		0	POS Tender object number mapping
	Tenders: Reserver-14		0	POS Tender object number mapping
	Tenders: Reserver-15		0	POS Tender object number mapping
	Tenders: Service Charge		0	POS Tender object number mapping
	Tenders: Visa		0	POS Tender object number mapping

Section	Setting Name	Constraint	Default Value	Description
	Tenders: Visa Debit		0	POS Tender object number mapping
	Tenders: Visa Electron		0	POS Tender object number mapping
	Tenders: V Pay		0	POS Tender object number mapping
	Tenders: WeChat Pay		0	POS Tender object number mapping

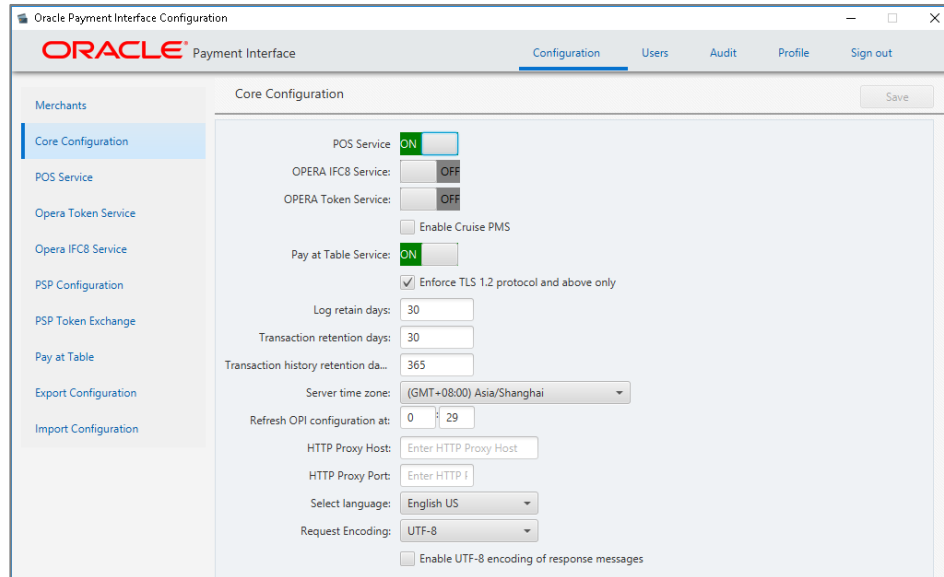
Configuration Tool Settings

The configurator provides expanded control in an easy to use format.

- Double click OraclePaymentInterface\v19.1\Config\LaunchConfigurator.bat.
- Sign in with Super User name and password created during installation.
- Hovering the mouse cursor over an option will give a brief description of it.



On the **Merchants** tab merchant records can be edited, added, and deleted.



Enforce TLS 1.2 protocol and above only: is enabled by default for all installations.

 **NOTE:**

If using OGDH and CE workstations, this TLS 1.2 option has to be disabled since the CE workstations will not be able to communicate to OPI using TLS 1.2.

Native driver sites can still uses CE workstations with TLS 1.2 enabled.

Log retain days: The number of days that OPI "Wrapper" log files will be retained before being deleted.

Ex: v19.1\Services\OPI\log\OPISvcWrapper.2017-10-23.log

Transaction retention days: The number of days that transaction data stored in database h_transline table. After this time period, the data will be moved to the h_transhistory table.

Transaction history retention days: The number of days that transaction data stored in database h_transhistory table. After this time period, the data will be purged from the database.

Refresh OPI configuration at: Refreshes data, so all changes are picked up.

The default time of 0:29 = 12:29 AM.

HTTP Proxy Host: The proxy host name or IP. If no proxy is needed, leave this field empty.

HTTP Proxy Port: The proxy port. If no proxy is needed, leave this field empty.

Request Encoding: UTF-8 is the default format that works with English and some other languages. But some foreign languages require UTF-16.

Enable UTF-8 encoding of response messages: For all Non-English languages, that use UTF-8, this option should be enabled. For English this setting has no effect.

Oracle Payment Interface Configuration

ORACLE Payment Interface Configuration Users Audit Profile Sign out

Merchants

Core Configuration

POS Service

Opera Token Service

Opera IFC8 Service

PSP Configuration

PSP Token Exchange

POS Service Configuration Save

Mode: Native Driver

Port: 5098

Use Check Open Time for CC Repost

Passphrase:

Confirm passphrase:

Mode: Native Driver or OGDH

Port: Port used for communication to OPI.

Use Check Open Time for CC Repost: Should always be on or repost will not work.

Passphrase: If Mode is Native driver, the **POS Native passphrase** can be changed here. If Mode is OGDH, the **OGDH certificate password** can be changed here.

Oracle Payment Interface Configuration

ORACLE Payment Interface Configuration Users Audit Profile Sign out

Merchants

Core Configuration

POS Service

Opera Token Service

Opera IFC8 Service

PSP Configuration

PSP Token Exchange

OPERA Token Configuration Save

Mode: HTTPS Mina

Port: 5012

Mode: HTTPS Mina is the default setting.

Oracle Payment Interface Configuration

ORACLE Payment Interface Configuration Users Audit Profile Sign out

Merchants

Core Configuration

POS Service

Opera Token Service

Opera IFC8 Service

PSP Configuration

PSP Token Exchange

OPERA IFC8 Configuration Save

Communication test interval: 73

Decoder timeout: 1000

Bulk Tokenization Batch Size: 50

Enable test communication Heartbeat

Enable Update Token Support

Return receipt's full print data

Enable UTF-8 for receipts

Communication test interval: Test connection interval, in seconds.

Decoder timeout: The number of milliseconds OPI will wait for an IFC8 message to be received.

NOTE:

Do not change the time values above unless you work for support and know why the change is being made.

Bulk Tokenization Batch Size: Size in number of cards.

Enable Update Token Support: Select this to enable bulk tokenization through the IFC8 channel.

Return receipt's full print data: Select this to return the receipt's full print data to IFC8 in cross reference fields.

Enable UTF-8 for receipts: Select this to return print data in UTF-8 encoding.

The screenshot shows the Oracle Payment Interface Configuration window. The main content area is titled "Payment Service Provider Configuration" and includes a "Save" button. The configuration fields are as follows:

- Communication Timeout: 60
- Connect Timeout: 10
- Enable Mutual Authentication
- Private Key Cert. Password: Enter Private Key Cert. Password
- Confirm Private Key Cert.Password: Confirm Private Key Cert. Passwo
- Root Certificate Password: Enter Root Certificate Password
- Confirm Root Certificate Password: Confirm Root Certificate Passwo
- Enable Top up authorization for POS
- Communication Mode: Terminal (dropdown menu)
- Terminal Port: 443
- Terminal Context: Insert terminal context
- Enable TLS

Communication Timeout: The number of seconds OPI will wait for a response from the PSP Host or Terminal before timing out.

Connect Timeout: The number of seconds OPI will wait when initiating a connection to the PSP Host or Terminal before timing out.

Enable Mutual Authentication: Mutual Authentication can be enabled here, and passwords entered. See the Mutual Authentication section of this document for more information.

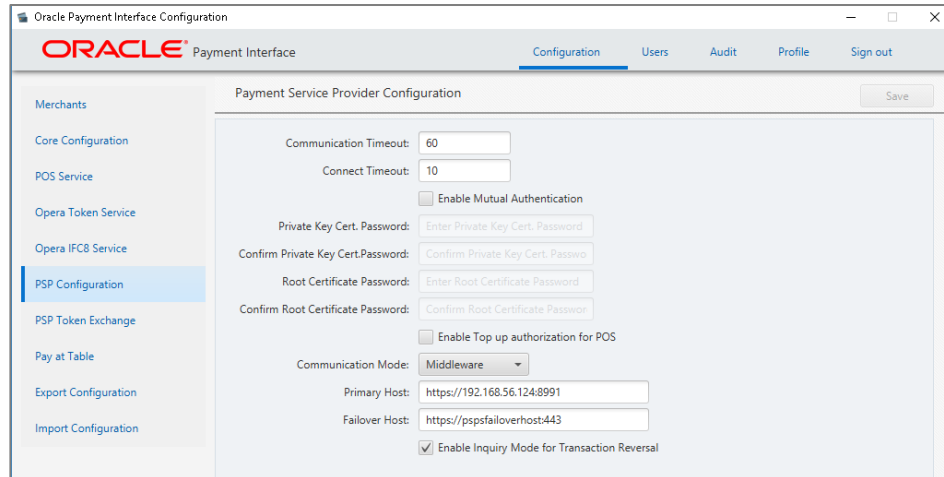
Enable Top up authorization for POS: Enable this if the PSP supports Top Up / incremental authorizations for POS. Top up is only supported by Native drivers, not OGDH.

Communication Mode: This can be changed from Terminal to Middleware as well as the port settings.

Terminal Port: Port used to communicate to PinPad terminal.

Terminal context: Some Terminal devices need to have a value appended to their URL. This is usually not needed. Ex: "/payment".

Enable TLS: This is enabled by default for all installations.



Middleware Mode.

Primary Host: The URL used to communicate to the PSP.

Failover Host: The backup URL used to communicate to the PSP.

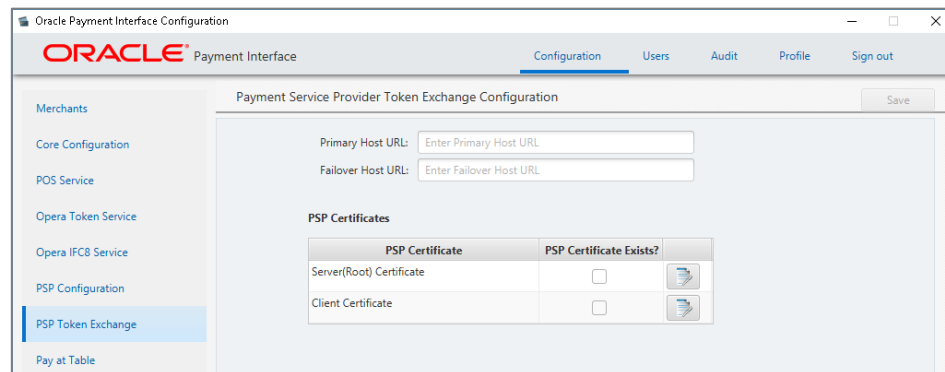
Enable Inquiry mode for transaction reversal:

Middleware mode:

ON = Before a sending a reversal, OPI sends an inquiry to the PSP to see if the transaction posted. If not posted, no reversal is sent.

OFF = It automatically sends the reversal.

Terminal mode: Inquiry is not supported, so it automatically sends a reversal.



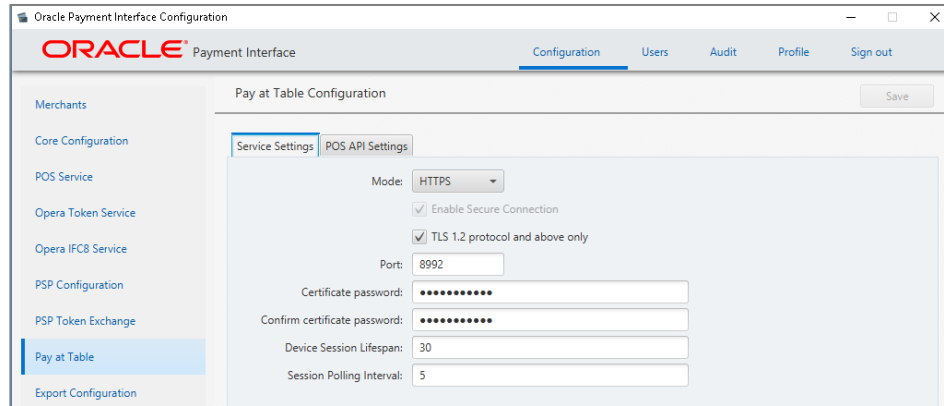
PSP Token Exchange for OPERA.

Primary Host URL - The PSP Host URL for Token Exchange

Failover Host URL - The PSP Failover Host URL for Token Exchange. If a failover URL is not available, leave this blank

Server (Root) Certificate - Import the Key Store containing the PSP Root Certificate, and setup password.

Client Certificate - Import the Client Side certificate provided by PSP, and setup password.



Pay at Table.

Mode: Typically would be set to **HTTPS**. But it could be set to **HTTP** temporarily to trouble shoot communication problems. HTTP could be used to verify the problem is not related to certificate issues.

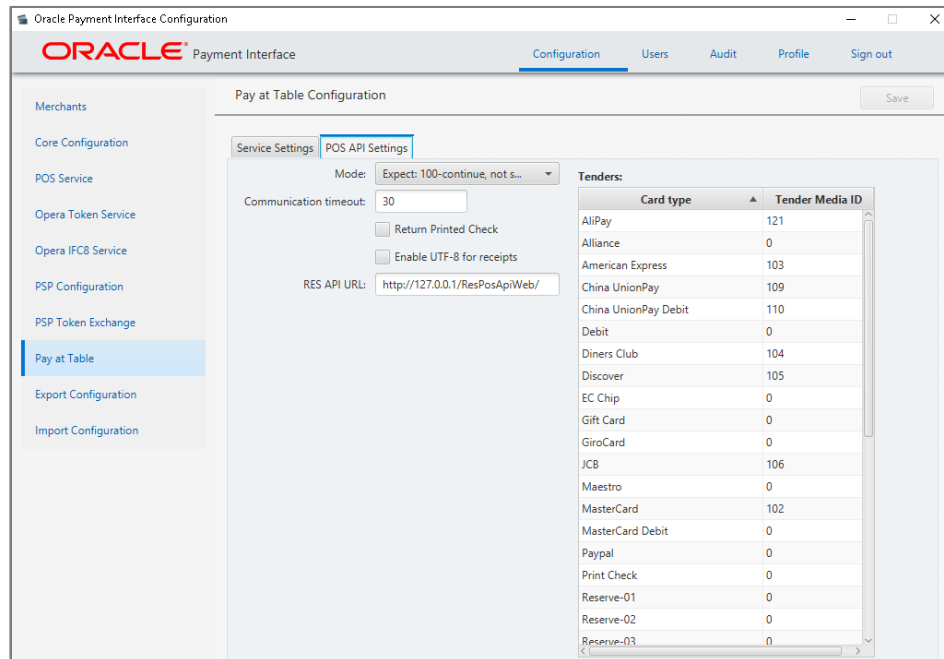
Using **TCP** is still secure if "**Enable Secure Connection**" is enabled.

If the terminal does not support SSL, you might have to use TCP.

TLS 1.2 protocol and above only: You would keep this on unless your P@T PED did not support TLS 1.2.

Port: The port used to communicate to the P@T PEDs.

Certificate Password: Used to secure communications between the P@T terminal and PSP.



Mode:

Expect: 100continue, not supported: This means all information is sent in 1 message.

Expect: 100continue, supported: This means send the header first, then the data in a 2nd message.

RES 4.7 and higher have to have this set to **Not supported**.

This would only be changed to supported if there were issues.

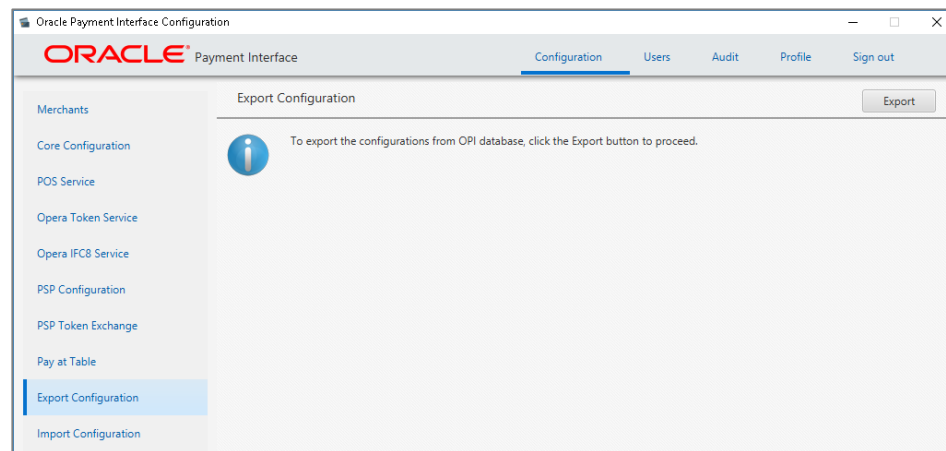
Communication Timeout: The number of seconds OPI will wait for a response from the POSAPI before timing out.

Return Printed Check: If this is ON, a copy of the check can print at the P@T device to present to the customer when the check is picked up from the POS.

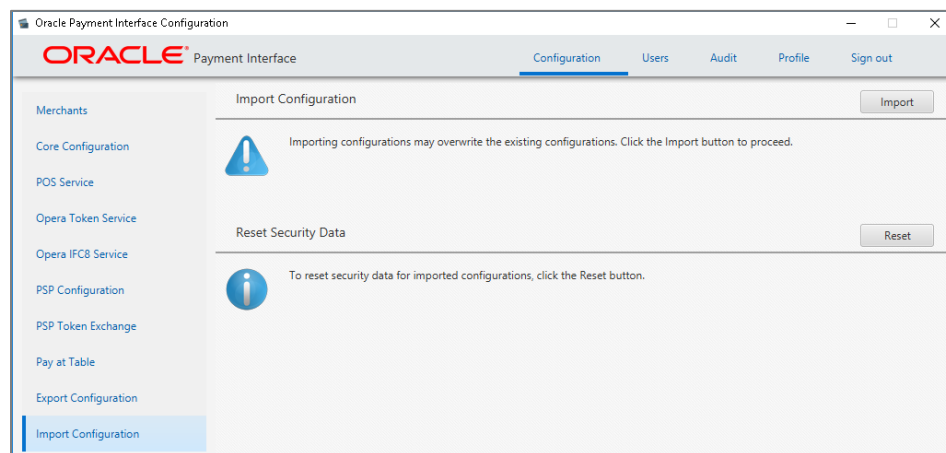
Enable UTF-8 for receipts: Select this to return print data in UTF-8 encoding

RES API URL: The URL of the RES API used for Pay at Table.

Tenders: The POS tenders that P@T posts payment to.



Export Configuration: Export current OPI configuration data to an XML file.



Import Configuration: Import OPI configuration data from an XML file. Will override existing configuration, except merchant information.

Reset Security Data: Reset security data after import configuration.

HTTP Support

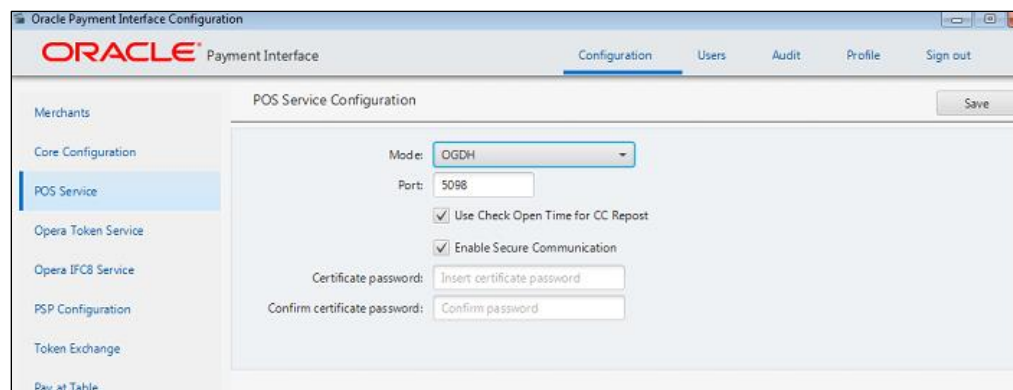
OPI 6.2.1 supports HTTP for communication between both POS/OGDH to OPI and from OPI to PSP.

 **NOTE:**

Oracle Hospitality recommends using HTTPS because sensitive information shared on unsecured HTTP connections could be compromised or stolen.

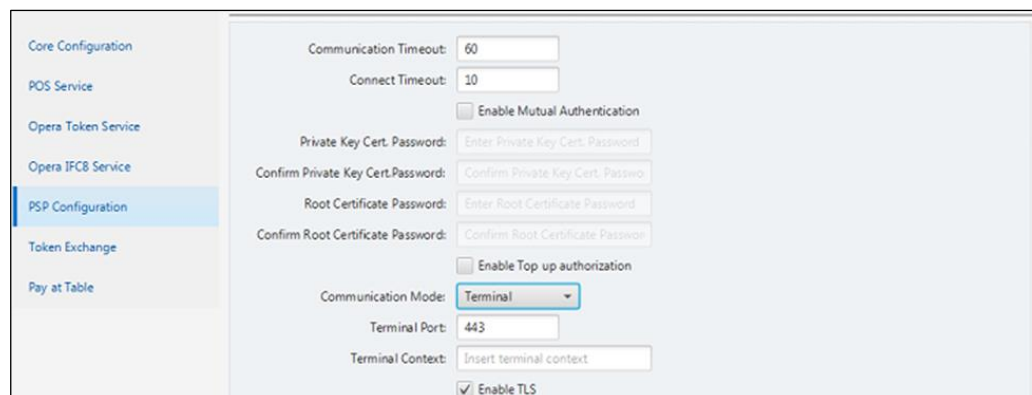
Configuring OGDH POS-OPI to Support HTTP

1. Configure the HOST1 = http://OPI Server IP in the **MGDH.inc** file for POS.
2. Open the OPI Configuration tool, click the **Configuration** tab, click **POS Service**, and then deselect **Enable Secure Communication**.



Configuring OPI to Send HTTP Requests to PSP

1. Open the OPI Configuration tool, click the **Configuration** tab, and then click **PSP Configuration**.
2. If the **Communication Mode** is set to Terminal, deselect **Enable TLS**.
3. If the **Communication Mode** is set to Middleware mode, the Host should be http://PSP info.



18

Maintain OPI Environment

This section explains on how to maintain and manage your OPI environment without any additional support from team.

- Add or edit Payment Terminals
- Add or edit Pay at Table Devices
- Add or edit number of OPI Users
- Edit Payment Types

Terminals

Terminals tab is displayed only if **PSP Configuration | Communication Mode = Terminal**. In the **Terminal** mode, OPI maintains WS > PED mapping and communicates directly to PED.

Adding Payment terminals

1. Log in to the OPI Configuration tool as the System Administrator, select the **Merchants** tab, and then click the **Edit Merchant** icon in the **Merchant Configuration** window.
POS Merchant Information window appears.
2. Select **Terminals** tab and then click the **blue plus button** in the upper right corner to add the payment terminal details.

Workstation ID	Terminal IP

3. **Workstation ID**: Enter the workstation ID using the PED.
4. **Terminal IP**: Enter the IP Address of the PED, the Workstation should use.
5. Once the details are provided, press **Enter** key to submit your changes.
6. **Save** changes and restart the OPI service.

Editing Payment Terminals

1. Log in to the OPI Configuration tool as the System Administrator, select the **Merchants** tab, and then click the **Edit Merchant** icon in the **Merchant Configuration** window.
POS Merchant Information window appears.
2. Select **Terminals** tab and then select the payment terminal record to be edited.
3. Make necessary changes and press **Enter** key to submit your changes.
4. **Save** changes and restart the OPI service.

Deleting Payment Terminals

1. Log in to the OPI Configuration tool as the System Administrator, select the **Merchants** tab, and then click the **Edit Merchant** icon in the **Merchant Configuration** window.
POS Merchant Information window appears.
2. Select **Terminals** tab and then select the payment terminal record to be deleted.
3. Click the **blue minus** button available on the Merchant Information window to delete the payment terminal details
4. Confirmation window pops up saying “Do you really want to delete the terminal for Workstation”. Click **Ok** to proceed with the deletion process.
5. **Save** changes and restart the OPI service.

Pay at Table Devices

Pay at Table Devices tab is displayed only if the **POS Type** is selected as **RES** or **Symphony** and **Enable Pay at Table** checkbox is selected in the configuration wizard.

Adding Pay at Table Devices

1. Log in to the OPI Configuration tool as the System Administrator, select the **Merchants** tab, and then click the **Edit Merchant** icon in the **Merchant Configuration** window.
POS Merchant Information window appears.
2. Select **Pay at Table Devices** tab and then click the **blue plus button** in the upper right corner to add a Pay at Table device record.

3. **Device ID:** Enter the value/number used to identify this mobile device.
4. **Query By:** Select either Table or Check for the method this device will use to retrieve checks from the POS database.
5. Once the details are provided, press **Enter** key to submit your changes.
6. **Save** changes and restart the OPI service.

Editing Pay at Table Devices

1. Log in to the OPI Configuration tool as the System Administrator, select the **Merchants** tab, and then click the **Edit Merchant** icon in the **Merchant Configuration** window.
POS Merchant Information window appears.
2. Select **Pay at Table Devices** tab and then select the Pay at Table device record to be edited.
3. Make necessary changes and press **Enter** key to submit your changes.
4. **Save** changes and restart the OPI service.

Deleting Pay at Table Devices

1. Log in to the OPI Configuration tool as the System Administrator, select the **Merchants** tab, and then click the **Edit Merchant** icon in the **Merchant Configuration** window.
POS Merchant Information window appears.
2. Select **Pay at Table Devices** tab and then select the Pay at Table device record to be deleted.
3. Click the **blue minus** button available on the Merchant Information window to delete the pay at table device details.
4. Confirmation window pops up saying “Do you really want to delete the device”. Click **OK** to proceed with the deletion process.
5. **Save** changes and restart the OPI service.

OPI Users

OPI user management is explained in [OPI User Administration](#) section, refer for more details.

Payment Types

Edit Tender Media ID - POS API Settings

You can edit the Tender Media ID in **POS API Settings** tab under **Pay at Table Configuration**. Each Card type is mapped with a Tender Media ID in the Opera configuration.

1. Log in to the OPI Configuration tool as the System Administrator, select the **Pay at Table** tab, and then click **POS API Settings** tab.
2. Select the Card type and double-click the **Tender Media ID** and edit the ID.
3. Press **Enter** key to submit your changes.
4. **Save** changes and restart the OPI service.

Edit Payment Code – IFC8 Settings

IFC8 settings is available only for PMS merchants. You can edit the Payment Code in **IFC8 Settings** tab under Pay at Table Configuration. Each Card type is mapped with a Payment Code in the Opera configuration.

1. Log in to the OPI Configuration tool as the System Administrator, select the **Merchants** tab, and then click **IFC8 Settings** tab.
2. If required, edit **IFC8 host** and **IFC8 Port**.
3. Select the Card type and double-click the **Payment Code** and edit the code.
4. Press **Enter** key to submit your changes.
5. **Save** changes and restart the OPI service.

19

Troubleshooting and FAQs

Troubleshooting

Tip: To increase logging at an OGDH workstation (for troubleshooting purposes), add this line to that workstation's OPI.inc file:

```
EnableIFClog = True
```

Log location?

```
Win32: Micros\res\pos\etc\MGDH_WS#.log
```

```
CE: Root of My Device\MGDH_WS#.log
```

Remove that line from OPI.inc when the issue is resolved.

Situation 1: "Communicate Error"

Test:

1. Verify you can telnet to the OPI PC on port 5098 from another PC.

Ex: From CMD prompt: telnet 192.0.2.1 5098

(Where 192.0.2.1 is the IP address of the OPI server.)

If you cannot telnet to the OPI port, try the following:

2. Restart the OPI Service.
3. Temporarily bypass the firewall.
4. Verify OPI is listening on port 5098.

Open CMD prompt: C:\>netstat -anob > c:\temp\ports.txt

Search ports.txt for "5098".

Cause 1: Pos\Etc\OGDH.inc. was pointing to wrong IP address for OPI server.

Cause 2: The windows Firewall on OPI server was enabled and incoming traffic on port 5098 was blocked.

Cause 3: LaunchConfiguration.bat | POS Service | Mode: = set to wrong value. OGDH vs Native Driver.

Cause 4: OPI service not listening on port 5098.

Solution: Verify Port is set correctly in LaunchConfiguration.bat | POS Service.

Restart OPI service, or reboot.

Situation 2: "Issuer or switch inoperative"

Cause 1: Simulator is not running.

Cause 2: OPI service not restarted after making config change.

Cause 3: Incorrect Proxy settings.

Cause 4: Incorrect settings in LaunchConfiguration.bat | PSP Configuration for Host and or Port.

Solution For Middleware mode:

- 1) Need to use https instead of http.
- 2) Need to append port to end of host value

Ex: Host = <https://192.0.2.1:8991>

Cause 5: Wrong IP address or port.

Solution for IP: LaunchConfiguration.bat | Merchants | Terminals. Verify IP is correct for terminals.

Solution for port: LaunchConfiguration.bat | PSP Configuration. Correct Terminal port value.

Situation 3: "Bad Terminal ID"

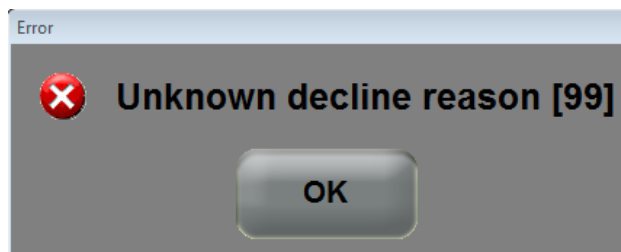
Cause 1: Wrong workstation number.

Cause 2: Wrong merchant ID.

Solution: LaunchConfiguration.bat | Merchants, verify Merchant ID and WS numbers.

Cause 3: Forgot to restart OPI service after making changes in

Situation 4:



This generic error message can be caused by several things.

Solution 1:

Restart the OPI Service and try again.

Solution 2:

If the debug.log shows: "ht is null" the cause may be that the wrong POS passphrase is in either OPI or the POS.

The solution is to change the POS passphrase at both the POS and OPI to be the same value.

Solution 3:

If the system.log shows the message below, and is not caused by the wrong POS passphrase mentioned above, then it might be due to a Java update.

(This should not be an issue in OPI 19.1, but leaving info, in case.)

```
[GATEWAY RESPONSE] GenericJSONProcessor: Cannot decrypt  
java.security.InvalidKeyException: Illegal key size
```

Not all Java updates will cause this error, but security updates have in previous versions.

1. Stop the OPI service.
2. Go to the link below and download jce_policy-8.zip.
<http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>
3. Unzip the file and copy the two files to your Java security folder.
 - Local_policy.jar
 - US_export_policy.jar

Ex: C:\Program files\Java\jre(your current version)\lib\security\
Some systems may have Java installed in Program Files (x86). If so, update the files there also.
4. Start the OPI service.

Solution 4:

If nothing is writing to the debug.log when you get the “Unknown decline reason [99]” error, then you may have the wrong POS Mode setting.

1. Open
OraclePaymentInterface\v19.1.1\Config\LaunchConfiguration.bat.
2. On POS Service tab, verify Mode: = Native Driver.
3. Save changes, and then restart OPI service.

FAQs

Q1: How is the signature verification prompt controlled?

A1: The PSP controls whether there will be a prompt for signature verification.

A2: If using the simulator, to disable the signature prompt:

1. Open open SimulatorRunnableDist\properties\SimulatorConfig.properties.
2. Add this line to the end: ENTRY_MODE=05
3. Restart the simulator.