Contents

Preface ........................................................................................................................................... 1-1
  Audience ................................................................................................................................. 1-1
  Customer Support ................................................................................................................. 1-1
  Documentation ....................................................................................................................... 1-1
  Revision History ..................................................................................................................... 1-1

1 Pre-Installation ......................................................................................................................... 1-2

2 Install OPI 6.1.1.9 ..................................................................................................................... 2-3

3 Configuring OPI ........................................................................................................................ 3-1
  Certificates ............................................................................................................................. 3-5
    PSP - Client Side Certificates ............................................................................................ 3-6
    OPI - Server Side Certificates .......................................................................................... 3-10
    OPI - Client Side Certificates .......................................................................................... 3-13

4 Opera Configuration ............................................................................................................... 4-18
  Creating an EFT Interface ..................................................................................................... 4-18
  Configuring CHIP AND PIN (EMV) .................................................................................... 4-19
  Configuring the CC Vault ...................................................................................................... 4-23
  Cashiering Overview ............................................................................................................. 4-24
  Credit Card Payment Transaction Codes .............................................................................. 4-24
  Overview of Credit Card Payment Types .............................................................................. 4-25
  Configuring the Workstation ................................................................................................. 4-27
  Configuring the Hotel Property Interface (IFC8) instance to the OPERA Hotel Property Interface (IFC) ......................................................................................................................... 4-28
  Configuring Authentication for the Hotel Property Interface (IFC8) with OPI .................... 4-29
  Perform a Tokenization .......................................................................................................... 4-31
    Certificate Import using Microsoft Management Console .............................................. 4-32

5 OPI Maintenance & FAQ ............................................................................................................ 5-35
  OPI Services .......................................................................................................................... 5-35
  OPI Uninstallation / Re-installation ...................................................................................... 5-35
  OPI Additional Configuration .............................................................................................. 5-35
  OPI Log Files ........................................................................................................................ 5-36
  OPI Service Restart Task ...................................................................................................... 5-36
  OPI Password Maintenance ................................................................................................. 5-36
  OPI Configuration Logs ........................................................................................................ 5-37
Preface

This document is to guide users attempting to configure Oracle Payment Interfaces On Premise Token Exchange Service.

Audience

This document is intended to cover the additional steps required to setup OPI to handle the On Premise Token Exchange functionality.

This document covers only the configuration of the additional On Premise Token Exchange functionality, it does not cover in detail, installation of the OPI software and IFC8 merchant configuration, separate documentation already exists to cover this.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Documentation

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

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2017</td>
<td>• Initial publication</td>
</tr>
</tbody>
</table>
1 Pre-Installation

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

- OPERA Property Management System release 5.0.05.11 is the minimum release you can use to integrate with OPI.
- Upgrading to OPI 6.1.1.9 from any previous OPI is supported but MPG versions are not supported.
- Any previous version of MPG should be uninstalled prior to installing OPI 6.1.1.9.
- The application requires Microsoft.NET Framework version 4.0 or higher.
- OPI requires at least 6 GB of free disk space & you must install OPI as a System Administrator
2 Install OPI 6.1.1.9

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

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

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

4 Select the Oracle Hospitality product integrating with this OPI installation.
5  Setup the Microsoft Windows task scheduler to restart OPI service weekly.

6  Select the location to install OPI. You can change the folder name or you can keep the default folder name.
7 Select the open source project source code and license installation folder. You can keep the default location inside the OPI folder.

8 Select the Start Menu folder for OPI, you can keep the default location.
Install will begin installing OPI.
3 Configuring OPI

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

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

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

3. Click on add Property to add a new merchant configuration for OPERA.
4 To configure the OPERA merchant, enter the following information
   • The OPERA Vault Chain Code & Property Code; will form the SiteId value in the Token request messages.
   • The format of the SiteId field includes a pipe character to separate the two OPERA Vault Chain Code & Property Code values.
   • See the screenshot below where OPERA Vault chain code is “SHELL” and Property code is “O9SMALL1” so value in field will be “SHELL|O9SMALL1”
   • Select Generate Key. You must use this key to configure the Hotel Property Interface (IFC8).
   • Enter the IFC8 IP address and port number for the Hotel Property Interface (IFC8) server.
   • Enter the Merchant name, city, and country information.
   • Select Next.

Whilst the other populated settings are not directly related to the Token Exchange Service configuration, Token Exchange will not be possible if the IFC8 interface is not running, as OPI will not progress past the IFC8 startup if the IFC8 connection is not possible.
5 Enter the OPERA payment code for each card type & next.
The top half of the next page relates to communication from OPI to the PSP host, and the PSP Client certificate credentials.

**Key Password**: The password provided with the client .pfx file by the PSP.

**Certificate Password**: Is the password that when creating the Java Key Store (JKS) in the steps below.

**Certificates**

OPI on Premise Token Exchange requires three sets of certificates:

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

Refer to the sections below for further details.
PSP - Client Side Certificates

The communication from OPI to the PSP for token exchange uses HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed at PSP (server side) for HTTPS communication, PSP is also expected to provide a client side certificate to be deployed at OPI side. OPI will present this client certificate during HTTPS communication with PSP so that PSP can authenticate OPI properly.

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

- A client side certificate file in the name of “OPI_PSP_1.pfx”, this is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password. If the file provided by PSP has a different name, rename to “OPI_PSP_1.pfx” before deploying it to OPI.
- The root certificate file for the server side certificate that is deployed at PSP side. OPI needs to load this root certificate file into the Java Key store so that OPI can properly recognize and trust the server side certificate deployed at PSP side. We expect the root certificate file provided by PSP to be in the format of .cer or .crt. For the demo purpose in this document, we assume the file has the name “ca-cert.crt”.

Handling the client side certificate

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

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

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

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

In order to load the root certificate file for the PSP server certificate into the Java key store, perform the following steps:

Creating a JKS

From a command prompt change to the JRE bin folder, in order for the `keytool` command to be recognized.
The exact path of your JRE bin folder will depend on the environment on which you are running the commands, and the JRE version you have installed, but may be similar to the example path shown below:

![Command Prompt Window](image)

The three commands below, when run in sequence;
- Create a new Java keystore,
- Delete the default key created inside the Java Key Store
- Import the supplied root certificate in its place:

In the following example, the root .cer / .crt file is named ca-cert.crt, and is located in the folder `C:\Certificates`. Adjust file names and paths to be relevant to your details. OPI expects that the Java key store file that contains the root certificate for PSP server certificate to be in the name of “OPI_PSP_1Root”.

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

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

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

You should use the same key password as for the keystore password when prompted.
Configuring OPI

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

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

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

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

```
c:\Program Files\Java\jre1.8.0_111\bin>keytool -import -alias myrootca -file ca-cert.crt -keystore C:\Certificates\OPI_PSP_1Root -trustcacerts
Owner: CM=MerchantLink, DN=Certificate Authority, OU=MerchantLink Security, O=Merchantlink LLC, C=US, EMAIL=<redacted>@merchantlink.com
Issuer: CM=MerchantLink, DN=Certificate Authority, OU=MerchantLink Security, O=Merchantlink LLC, C=US, EMAIL=<redacted>@merchantlink.com
Serial number: 2E36D0F75E58A147927A84157F74
Certificate fingerprint:

Signature algorithm name: SHA1withRSA
Version: 3
```

```
Extensions:

1: ObjectID: 2.5.29.35 Criticality=false
   AuthorityKeyIdentifier { keyIdentifier { OID: 22 50 83 6D 16 EE 6A 7D CB 82 17 76 9F 31 2C "..." ..."..."..."...
   [0] 1C 0D 53 } }

2: ObjectID: 2.5.29.19 Criticality=false
   BasicConstraints:1
   PathLength:0

3: ObjectID: 2.5.29.15 Criticality=true
   KeyUsage :
     DigitalSignature
     KeyCertSign
   ExtKeyUsage :

4: ObjectID: 2.5.29.14 Criticality=false
   SubjectKeyIdentifier { keyIdentifier { OID: 22 50 83 6D 16 EE 6A 7D CB 82 17 76 9F 31 2C "..."..."..."...
   [0] 1C 0D 53 } }
   Intrust this certificate? tool: yes
   Certificate was added to keystore
```

C:\Program Files\Java\jre1.8.0_111\bin>
Verify the new Java keystore’s details by running the following command if required;

```
keytool –list –keystore c:\Certificates\OPI_PSP_1Root
```

OPI_PSP_1.pfx & OPI_PSP_1Root once ready, will need to be located in the folder; \\OraclePaymentInterface\key\n
Updating a JKS with a new PSP certificate

If this is an existing OPI On Premise Token Exchange installation, and you are importing a new PSP certificate prior to an existing key expiring, the current OPI_PSP_1.pfx & OPI_PSP_1Root, should be deleted from the \\OraclePaymentInterface\key\ folder prior to following the steps above to import new certificate file.
The lower half of the page relates to generating server side certificates used in communication from Opera to OPI.

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

Populate the fields with the relevant information. The password fields validate the passwords are complex, so the passwords will need to meet these requirements:

- Min 8 characters in length
- Min 1 Alpha Character
- Min 1 Numeric Character
- Min 1 Special Character from the following list !@#$%^&*
Once ready select *Generate*
This process will generate the MICROS_OperaToken.pfx & MICROSOperaToken.cer files in the folder; `\OraclePaymentInterface\key\`

Note: The OPI Server Side Certificates have a default expiry date of five years from the date of creation. Check the expiry date in the properties of the certificate files. The OPI Server Side Certificates will need updating prior to the expiry date to avoid downtime to the interface.

Copy the MICROSOperaToken.cer files to all of the Opera registered terminal that you will run the Token Exchange process from, and then import to Trusted Root Certification Authorities, using `mmc.exe` (see below for more info)

8 Close the Certificate generation screen, you should now see the green message `Token Certificate exists.`
OPI - Client Side Certificates

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

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

- Once values entered and ready click generate.
In the example above the certificates are named SHELL, which is picked up from the Chain Code entered in previous steps. The certificates you create may be named differently relative to the environment in which they are being installed.

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

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

- SHELL.crt import to Trusted Root Certification Authorities.

Note: The OPI Client Side Certificates have a default expiry date of five years from the date of creation. Check the expiry date in the properties of the certificate files. Be aware the OPI Server Side Certificates will need updating prior to the expiry date to avoid downtime to the interface.

10 Select Set Basic Authentication to configure the Header Authentication credentials used in communications from Opera > OPI.
11 Select OK to confirm the Authentication details and return to the PSP/Certificate Page.
• The Algorithm setting is the hashing method used to store the password at the OPI host machine; it is not set at the Opera side. The minimum supported method is **SHA-256**.

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

12 Select **Next** to continue.
13 Select Exit, and save the changes when prompted.
Creating an EFT Interface

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

1. Enter the following options, and then select OK:
   - **IFC Type**: EFT
   - **Name**: Oracle Payment Interface
   - **Product Code**: OPI
   - **Machine**: Select the machine
   - **License Code**: License code for interface
   - **IFC8 Prod Cd**: XML_OPI
2. Select the check box to enable the **CC Vault Function**.
3. Define the **Timeout** value as 210.

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

---

**Configuring CHIP AND PIN (EMV)**

To configure the Functionality Setup:

1. Go to **Setup > Application Settings > IFC Group > Parameters**, and enable CHIP AND PIN.
Opera Configuration
2. Go to Setup > Property Interfaces > Credit Card Interface > Functionality Setup.

- **Online Settlement.** Select this check box to allow online settlement. OPI is an online settlement. This must be checked to activate the Chip and PIN Application Setting.

- **Authorization at Check In.** Select the payment methods that will trigger an automatic credit card authorization at check-in.

- **Authorization Reversal Allowed.** Select the payment methods that can process authorization reversals. This provides a request transaction to the Payment Partner to remove the existing authorization on a guest credit card or debit card if the folio payment type is changed or at check-out a different payment method is used. For example, a guest checks-in on a reservation for a 5-night stay using a Visa credit card for payment type. At the time of authorization, a hold is put on the Visa credit card for the total cost of the stay. If the payment type is changed to another type on the reservation or the guest checks-out using cash or a different brand of credit card, OPERA will send a reversal request for the originally selected Visa credit card authorization. A partial reverse authorization is not supported.
• **Authorization During Stay/Deposit.** Select the payment methods that allow manual and automatic authorizations following check-in and prior to check-out and settlement. This option must be enabled in order to allow authorizations by the end-of-day routine.

• **Authorization Settlement at Check-Out.** Select the payment types that use credit card authorization and settlement in one transaction request. These are payment types that do not allow an authorization separate from the settlement/sale.
  - The payment types that are available in the multi-select list of values are only payment types configured as EFT payment types. Any one payment type can be selected for credit card specific rules of Authorization at check-in, Authorization Reversal, and Authorization during Stay/Deposit. If they are selected for these card specific rules, then the payment types will not be available for Authorization During Stay/Deposit.

• **Chip and PIN Enabled Payment Types.** When the IFC > Chip and PIN application parameter is set to Y this option is visible and selected by default. You may not unselect the check box. Select the LOV to choose the credit card payment types that will trigger a Chip and PIN message with or without credit card data to the EMV Device. Payment types that are configured here will not require that a credit card number or expiration date to be entered when selected as a payment method on the Reservation screen or on the Payment screen. This data can be provided in the response message from the Payment Partner.
Configuring the CC Vault

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

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

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

https://<ipaddress_opi_host>:5012/TokenOPERA

The CREDIT CARD VAULT ID is currently not used.

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

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

Credit Card Payment Transaction Codes

1. In OPERA go to Configuration > Cashiering > Codes > Transaction Codes to view the Credit Card Payments transaction codes setup.
2. Information for credit card payment transaction codes:
   - **EFT** selection is necessary to send credit card transactions out to the integrated payment partner for the specific Payment type.
   - **Manual** selection will not send out any transactions to the integrated payment partner.
   - **CC Code** will auto-populate once the transaction code is associated to a Payment Type.
   - **Display Code** can be populated to display a button when payment screen is accessed in OPERA PMS.

**Overview of Credit Card Payment Types**

The credit card payment types link with the transaction code:

1. In **OPERA Configuration > Cashiering > Payment Types**.
   - The **IFC CC Type** field has the credit card code used such as MC, VA, AX.
   - The **Trn Code** field has the credit card transaction code.
Configuring the Workstation

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

1. In OPERA > Setup > Workstations > edit your workstation selected.
2. Select the Chip & Pin Device Available check box to enable the device for this workstation (this allows the generic CP Payment Type to display in the LOV for a reservation).
Configuring the Hotel Property Interface (IFC8) instance to the OPERA Hotel Property Interface (IFC)

To configure the link between the interfaces:

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

You can find the OPERA IFC number in OPERA on the IFC Configuration of the related Hotel Property Interface (IFC) (Row_ID).
3. Go to the PMS1 tree in the Physical Layer.
4. Enter the port number into Parameter value Port. This is the port IFC8 uses to communicate with the opera IFC controller.
5. Select Enter and Apply to re-initiate IFC8, and then click Save.

![IFC8 Setup for Physical Layer](image)

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

You must secure the connection between OPI and Hotel Property Interface (IFC8) by exchanging encryption keys at startup.

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

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

   ![IFC8 Setup for XML_MFG](image)

2. Copy the generated key from Configuring OPI - OPERA merchant step 5, and add “FidCrypt051” to the generated key as prefix.
   For example: FidCrypt051xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
3. Copy this string into IFC8 Parameter IfcAuthKey value field.
4. Go to **IFC1** tree and select the **Physical Layer**.

5. Enter the port number in port value. This is the same port that was configured in OPI.

6. Click **Apply**, IFC8 reinitiates.

7. The **IfcAuthKey** value now shows an encrypted key and the entered string is now encrypted by IFC8.

8. Click **Save**, and then click **OK** to close the IFC8 Configuration form.

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

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

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

OPI only supports the Convert CC function; the other conversion options are not currently supported.
Certificate Import using Microsoft Management Console

1. Find and open mmc.exe from start menu
2 Select File > Add/remove snap in and add certificates to Selected snap-ins, select OK.

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

4 Right-click Certificates, select All Tasks, select Import.
• On the Certificate Import Wizard Welcome page, click Next.

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

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

• If imported is successful the certificates Common Name will be listed under the folder that was selected during import.
5  OPI Maintenance & FAQ

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

![OPI Services](image)

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

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

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

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

OPI Logs are found at the following path: \OraclePaymentInterface\Log\n
- Debug log

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

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

- Gateway.log

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

- System.log

Check the Oracle Payment Interface build number.

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

- Transaction log

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

OPI Service Restart Task

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

OPI Password Maintenance

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

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

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

**OPI Configuration Logs**

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

- Run `\OraclePaymentInterface\bin\AuditLogTool.exe`
- Select the date range required, and select View to see the required logs;