Oracle® Cloud

Using the Oracle Hospitality Adapter with Oracle Integration 3

F51357-03
April 2024

Oracle Cloud Using the Oracle Hospitality Adapter with Oracle Integration 3,

F51357-03

Primary Author: Oracle Corporation

Contents

Preface

This guide describes how to configure this adapter as a connection in an integration in Oracle Integration.

Note:

The use of this adapter may differ depending on the features you have, or whether your instance was provisioned using Standard or Enterprise edition. These differences are noted throughout this guide.

Topics:

Audience

This guide is intended for developers who want to use this adapter in integrations in Oracle Integration.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `https://www.oracle.com/corporate/accessibility/`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `https://support.oracle.com/portal/` or visit `Oracle Accessibility Learning and Support` if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation.

We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

See these Oracle resources:

- Oracle Cloud at `http://cloud.oracle.com`
- *Using Integrations in Oracle Integration 3*
- *Using the Oracle Mapper with Oracle Integration 3*
- Oracle Integration documentation on the Oracle Help Center.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Understand the Oracle Hospitality Adapter

Review the following conceptual topics to learn about the Oracle Hospitality Adapter and how to use it as a connection in integrations in Oracle Integration. A typical workflow of adapter and integration tasks is also provided.

Topics:

Oracle Hospitality Adapter Capabilities

The Oracle Hospitality Adapter lets you integrate an Oracle OPERA Cloud Property Management (PMS) application with other Oracle and non-Oracle applications.

Implement the Oracle Hospitality Adapter as follows:

- Integrate OPERA Cloud PMS with other Oracle Cloud applications such as Oracle ERP Cloud.
- Integrate OPERA Cloud PMS with any non-Oracle applications such as CRS applications.

The Oracle Hospitality Adapter provides trigger (inbound) and invoke (outbound) support. This enables you to trigger an integration in Oracle Integration to get OPERA Cloud PMS business events or invoke OPERA Cloud PMS using the available REST APIs.

Both inbound and outbound services use the REST APIs that the Oracle Hospitality Integration Platform (OHIP) exposes. All inbound and outbound service structure is exposed using REST only (no SOAP support).

To successfully create a connection with the Oracle Hospitality Adapter, you must first register your application within the OHIP Customer Portal. See the Hospitality Documentation page.

OAuth 2.0 Support

The Oracle Hospitality Adapter uses the OHIP security policy, which is based on the Open Authorization (OAuth 2.0) security policy for REST-based connections. This enables you to configure the Oracle Hospitality Adapter to consume an API protected with OAuth 2.0 token-based authentication.

Most HTTP or HTTPS services typically use the OAuth authorization framework to protect their resources. In accordance with the OAuth 2.0 specification, the OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service. This is either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service or by enabling the third-party application to obtain access on its own behalf.

Under token-based authentication, the adapter supports both OAuth Resource Owner Password Credentials based on the following:

- Oracle Hospitality Shared Security Domain (SSD) ecosystem
- OAuth Client Credentials based on the OPERA Cloud Identity and Access Management (OCIM) ecosystem

These policies are useful because the Basic Authentication security policy is not sufficient. Depending on the authentication ecosystem configured in OPERA Cloud, you see different configurations under the Environment Credentials on the OHIP Customer Portal.

To configure the OAuth 2.0 authentication exposed by the Oracle Hospitality Integration Platform (OHIP), see Configure Connection Security.

The Oracle Hospitality Adapter is one of many predefined adapters included with Oracle Integration. See the Adapters page in the Oracle Help Center.

Oracle Hospitality Adapter Restrictions

Note the following Oracle Hospitality Adapter restrictions.

- The Oracle Hospitality Adapter can only be used with the OPERA Cloud PMS Cloud Application. An active Oracle Hospitality Integration Platform (OHIP) subscription is required. The Oracle Hospitality Adapter officially supports both the Property and Nor1 Upgrades API categories.
- To poll OPERA Cloud business events using a trigger connection, you must install the connectivity agent in a compute instance and associate it with the adapter connection. If you want to poll business events without a connectivity agent, you must use a scheduled integration in which you use the Oracle Hospitality Adapter as an invoke connection and use the respective poll Business Events API. See Implement Common Patterns Using the Oracle Hospitality Adapter.

> **Note:**
>
> There are overall service limits for Oracle Integration. A service limit is the quota or allowance set on a resource. See Service Limits.

What Application Version Is Supported?

For information about which application version is supported by this adapter, see the Connectivity Certification Matrix.

Workflow to Create and Add an Oracle Hospitality Adapter Connection to an Integration

You follow a very simple workflow to create a connection with an adapter and include the connection in an integration in Oracle Integration.

This table lists the workflow steps for both adapter tasks and overall integration tasks, and provides links to instructions for each step.

Step	Description	More Information
1	Access the OHIP Customer Portal.	Go to the following URL: `https://customer.hospitality-portal.`*`region`*`.ocs.oraclecloud.com/`*`instance`*`/ui` Replace *region* and *instance* with the appropriate values.
2	Register an application and make note of the application key.	See Registering an Application in the *User Guide* for the Oracle Hospitality Integration Platform.
3	Subscribe your application to the **API Catalog** subscription.	See Editing an Application Subscription in the *User Guide* for the Oracle Hospitality Integration Platform.
4	Make note of the environment credentials.	See Viewing the Client Secret in the *User Guide* for the Oracle Hospitality Integration Platform.
5	Access Oracle Integration.	Go to `https://`*`instance_URL`*`/ic/home`
6	Create the adapter connections for the applications you want to integrate. The connections can be reused in multiple integrations and are typically created by the administrator.	Create an Oracle Hospitality Adapter Connection
7	Create the integration. When you do this, you add trigger (source) and invoke (target) connections to the integration.	Create Integrations in *Using Integrations in Oracle Integration 3* and Add the Oracle Hospitality Adapter Connection to an Integration
8	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in *Using Integrations in Oracle Integration 3*
9	(Optional) Create lookups that map the different values used by those applications to identify the same type of object (such as gender codes or country codes).	Manage Lookups in *Using Integrations in Oracle Integration 3*
10	Activate the integration.	Activate Integrations in *Using Integrations in Oracle Integration 3*
11	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in *Using Integrations in Oracle Integration 3*
12	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Track Integration Instances in *Using Integrations in Oracle Integration 3*
13	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in *Using Integrations in Oracle Integration 3*

2
Create an Oracle Hospitality Adapter Connection

A connection is based on an adapter. You define connections to the specific cloud applications that you want to integrate. The following topics describe how to define connections.

Topics:

- Prerequisites for Creating a Connection
- Create a Connection
- Upload a Certificate to Connect with External Services

Prerequisites for Creating a Connection

You must satisfy the following prerequisites to create a connection with the Oracle Hospitality Adapter:

Before you configure the Oracle Hospitality Adapter:

- Ensure that you have an Oracle OPERA Cloud PMS user with access to the integration APIs.
- Ensure that you have an account on the Developer Portal of the OHIP platform. See the Oracle Hospitality Integration Platform documentation.
- Know the OHIP Gateway URL that you want to use.
- Ensure that you have registered an application in OHIP and have the corresponding credentials (application key, client ID, and client secret) from the OHIP Customer Portal.
- Ensure that your OHIP application subscribes to the API Catalog plan on the OHIP Customer Portal. See your OHIP Documentation.
- For polling OPERA Cloud business events (when the Oracle Hospitality Adapter is used as a trigger connection), ensure that you set up the connectivity agent. See Download and Run the Connectivity Agent Installer in *Using Integrations in Oracle Integration 3*.

Create a Connection

Before you can build an integration, you must create the connections to the applications with which you want to share data.

To create a connection in Oracle Integration:

1. In the navigation pane, click **Design**, then **Connections**.
2. Click **Create**.

> **Note:**
>
> You can also create a connection in the integration canvas. See Define Inbound Triggers and Outbound Invokes.

3. In the Create connection panel, select the adapter to use for this connection. To find the adapter, scroll through the list, or enter a partial or full name in the **Search** field.
4. Enter the information that describes this connection.

Element	Description
Name	Enter a meaningful name to help others find your connection when they begin to create their own integrations.
Identifier	Automatically displays the name in capital letters that you entered in the **Name** field. If you modify the identifier name, don't include blank spaces (for example, `SALES OPPORTUNITY`).
Role	Select the role (direction) in which to use this connection (trigger, invoke, or both). Only the roles supported by the adapter are displayed for selection. When you select a role, only the connection properties and security policies appropriate to that role are displayed on the Connections page. If you select an adapter that supports both invoke and trigger, but select only one of those roles, you'll get an error when you try to drag the adapter into the section you didn't select. For example, assume you configure a connection for the Oracle Service Cloud (RightNow) Adapter as only an **invoke**. Dragging the adapter to a **trigger** section in the integration produces an error.
Keywords	Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
Description	Enter an optional description of the connection.

Element	Description
Share with other projects	**Note**: This field only appears if you are creating a connection in a project. Select to make this connection publicly available in other projects. Connection sharing eliminates the need to create and maintain separate connections in different projects. When you configure an adapter connection in a different project, the **Use a shared connection** field is displayed at the top of the Connections page. If the connection you are configuring matches the same type and role as the publicly available connection, you can select that connection to reference (inherit) its resources. See Add and Share a Connection Across a Project.

5. Click **Create**.

   Your connection is created. You're now ready to configure the connection properties, security policies, and (for some connections) access type.

Configure Connection Properties

Enter connection information so your application can process requests.

1. Go to the **Properties** section.
2. In the **Gateway Hostname (OHIP)** field, enter the URL of the OHIP Gateway server that is associated with your OPERA Cloud instance. The URL is also provided in your environment details in the OHIP Developer Portal.

   ```
   https://name.hospitality-api.us-region.com
   ```

Configure Connection Security

Configure security for your Oracle Hospitality Adapter connection by selecting the security policy.

1. Go to the **Security** section.
2. View the security policy. **OHIP Security Policy** is the only security policy supported to connect to OPERA Cloud and cannot be deselected.
3. Enter the client ID and client secret provided in your environment details in the OHIP Developer Portal.
4. Enter the application key provided when you registered you application within the OHIP Developer Portal. If you request a new application key, you must update this field.
5. Expand **Optional security**.

> **Note:**
>
> It is not possible to use both identity providers. You need to enter either the user name and password *or* the scope and enterprise ID. Any other combination causes the internal validation to fail and you cannot test the connection.

6. If you are using the SSD identity provider authentication method, enter your user name and password. This is the OPERA Cloud user with access to the integration APIs, also known as the Integration User.
7. If you are using the OCIM identity provider authentication method, enter your scope and enterprise ID. These are provided in your environment details in the OHIP Developer Portal.
8. Click **Save**.

Configure the Endpoint Access Type

Configure access to your endpoint. Depending on the capabilities of the adapter you are configuring, options may appear to configure access to the public internet, to a private endpoint, or to an on-premises service hosted behind a fire wall.

Select the Endpoint Access Type

Select the option for accessing your endpoint.

Option	This Option Appears If Your Adapter Supports ...
Public gateway	Connections to endpoints using the public internet.
Connectivity agent	Connections to on-premises endpoints through the connectivity agent. 1. Click **Associate agent group**. The Associate agent group panel appears. 2. Select the agent group, and click **Use**. To configure an agent group, you must download and install the on-premises connectivity agent. See Download and Run the Connectivity Agent Installer and About Creating Hybrid Integrations Using Oracle Integration in *Using Integrations in Oracle Integration 3*.

Test the Connection

Test your connection to ensure that it's configured successfully.

1. In the page title bar, click **Test**. What happens next depends on whether your adapter connection uses a Web Services Description Language (WSDL) file. Only some adapter connections use WSDLs.

If Your Connection...	Then...
Doesn't use a WSDL	The test starts automatically and validates the inputs you provided for the connection.
Uses a WSDL	A dialog prompts you to select the type of connection testing to perform: • **Validate and Test**: Performs a full validation of the WSDL, including processing of the imported schemas and WSDLs. Complete validation can take several minutes depending on the number of imported schemas and WSDLs. No requests are sent to the operations exposed in the WSDL. • **Test**: Connects to the WSDL URL and performs a syntax check on the WSDL. No requests are sent to the operations exposed in the WSDL.

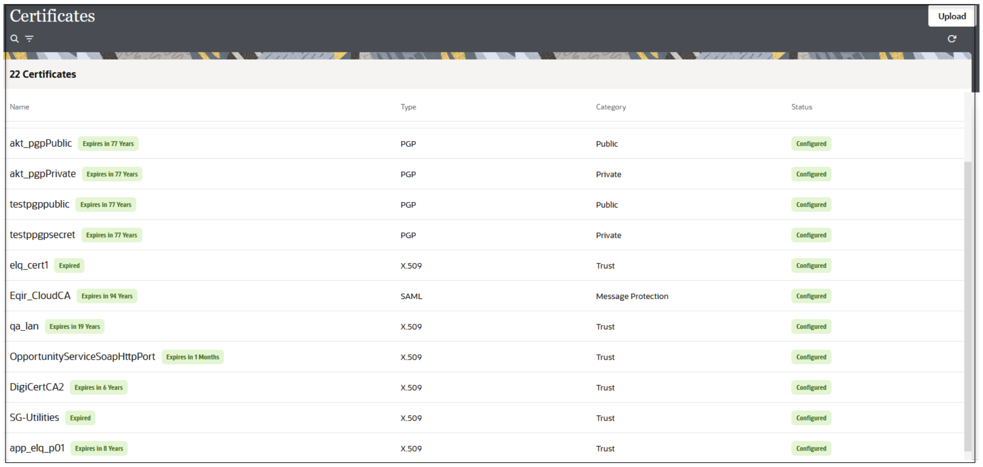
2. Wait for a message about the results of the connection test.
   - If the test was successful, then the connection is configured properly.
   - If the test failed, then edit the configuration details you entered. Check for typos and verify URLs and credentials. Continue to test until the connection is successful.
3. When complete, click **Save**.

Upload a Certificate to Connect with External Services

Certificates allow Oracle Integration to connect with external services. If the external service/ endpoint needs a specific certificate, request the certificate and then import it into Oracle Integration.

If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception error is thrown. In that case, you must upload the appropriate certificate. A certificate enables Oracle Integration to connect with external services. If the external endpoint requires a specific certificate, request the certificate and then upload it into Oracle Integration.

1. Sign in to Oracle Integration.
2. In the navigation pane, click **Settings**, then **Certificates**.
   All certificates currently uploaded to the trust store are displayed on the Certificates page.
3. Click **Filter** to filter by name, certificate expiration date, status, type, category, and installation method (user-installed or system-installed). Certificates installed by the system cannot be deleted.



22 Certificates

Name	Type	Category	Status
akt_pgpPublic Expires in 77 Years	PGP	Public	Configured
akt_pgpPrivate Expires in 77 Years	PGP	Private	Configured
testpgppublic Expires in 77 Years	PGP	Public	Configured
testppgpsecret Expires in 77 Years	PGP	Private	Configured
elq_cert1 Expired	X.509	Trust	Configured
Eqir_CloudCA Expires in 94 Years	SAML	Message Protection	Configured
qa_lan Expires in 19 Years	X.509	Trust	Configured
OpportunityServiceSoapHttpPort Expires in 1 Months	X.509	Trust	Configured
DigiCertCA2 Expires in 6 Years	X.509	Trust	Configured
SG-Utilities Expired	X.509	Trust	Configured
app_elq_p01 Expires in 8 Years	X.509	Trust	Configured

4. Click **Upload** at the top of the page.
   The Upload certificate panel is displayed.
5. Enter an alias name and optional description.
6. In the **Type** field, select the certificate type. Each certificate type enables Oracle Integration to connect with external services.
   - Digital Signature
   - X.509 (SSL transport)
   - SAML (Authentication & Authorization)
   - PGP (Encryption & Decryption)
   - Signing key

Digital Signature

The digital signature security type is typically used with adapters created with the Rapid Adapter Builder. See Learn About the Rapid Adapter Builder in Oracle Integration in *Using the Rapid Adapter Builder with Oracle Integration 3*.

1. Click **Browse** to select the digital certificate. The certificate must be an X509Certificate. This certificate provides inbound RSA signature validation. See Implement Digital Signature Validation (RSA) in *Using the Rapid Adapter Builder with Oracle Integration 3*.
2. Click **Upload**.

X.509 (SSL transport)

1. Select a certificate category.
   a. **Trust**: Use this option to upload a trust certificate.
      i. Click **Browse**, then select the trust file (for example, `.cer` or `.crt`) to upload.
   b. **Identity**: Use this option to upload a certificate for two-way SSL communication.
      i. Click **Browse**, then select the keystore file (`.jks`) to upload.

ii. Enter the comma-separated list of passwords corresponding to key aliases.

> **Note:**
>
> When an identity certificate file (`.jks`) contains more than one private key, all the private keys must have the same password. If the private keys are protected with different passwords, the private keys cannot be extracted from the keystore.

iii. Enter the password of the keystore being imported.

c. Click **Upload**.

SAML (Authentication & Authorization)

1. Note that **Message Protection** is automatically selected as the only available certificate category and cannot be deselected. Use this option to upload a keystore certificate with SAML token support. Create, read, update, and delete (CRUD) operations are supported with this type of certificate.
2. Click **Browse**, then select the certificate file (`.cer` or `.crt`) to upload.
3. Click **Upload**.

PGP (Encryption & Decryption)

1. Select a certificate category. Pretty Good Privacy (PGP) provides cryptographic privacy and authentication for communication. PGP is used for signing, encrypting, and decrypting files. You can select the private key to use for encryption or decryption when configuring the stage file action.
   a. **Private**: Uses a private key of the target location to decrypt the file.
      i. Click **Browse**, then select the PGP file to upload.
      ii. Enter the PGP private key password.
   b. **Public**: Uses a public key of the target location to encrypt the file.
      i. Click **Browse**, then select the PGP file to upload.
      ii. In the **ASCII-Armor Encryption Format** field, select **Yes** or **No**.
         - **Yes** shows the format of the encrypted message in ASCII armor. ASCII armor is a binary-to-textual encoding converter. ASCII armor formats encrypted messaging in ASCII. This enables messages to be sent in a standard messaging format. This selection impacts the visibility of message content.
         - **No** causes the message to be sent in binary format.
      iii. From the **Cipher Algorithm** list, select the algorithm to use. Symmetric-key algorithms for cryptography use the same cryptographic keys for both encryption of plain text and decryption of cipher text. The following supported cipher algorithms are FIPS-compliant:
         - AES128
         - AES192
         - AES256

    - TDES

   c. Click **Upload**.

Signing key

A signing key is a secret key used to establish trust between applications. Signing keys are used to sign ID tokens, access tokens, SAML assertions, and more. Using a private signing key, the token is digitally signed and the server verifies the authenticity of the token by using a public signing key. You must upload a signing key to use the OAuth Client Credentials using JWT Client Assertion and OAuth using JWT User Assertion security policies in REST Adapter invoke connections. Only PKCS1- and PKCS8-formatted files are supported.

1. Select **Public** or **Private**.
2. Click **Browse** to upload a key file.
   If you selected **Private**, and the private key is encrypted, a field for entering the private signing key password is displayed after key upload is complete.
3. Enter the private signing key password. If the private signing key is not encrypted, you are not required to enter a password.
4. Click **Upload**.

3

Add the Oracle Hospitality Adapter Connection to an Integration

When you drag the Oracle Hospitality Adapter into the trigger or invoke area of an integration, the Adapter Endpoint Configuration Wizard is invoked. In the background, the wizard fetches the APIs available for your application. The wizard guides you through configuration of the Oracle Hospitality Adapter endpoint properties.

The following sections describe the wizard pages that guide you through configuration of the Oracle Hospitality Adapter as a trigger or invoke in an integration.

Topics:

- Basic Info Page
- Trigger Business Events Page
- Invoke Category Page
- Invoke Module Page
- Invoke Operations Page
- Summary Page

Basic Info Page

You can enter a name and description on the Basic Info page of each adapter in your integration.

Element	Description
What do you want to call your endpoint?	Provide a meaningful name so that others can understand the responsibilities of this connection. You can include English alphabetic characters, numbers, underscores, and hyphens in the name. You can't include the following characters: • No blank spaces (for example, `My Inbound Connection`) • No special characters (for example, `#;83&` or `righ(t)now4`) except underscores and hyphens • No multibyte characters
What does this endpoint do?	Enter an optional description of the connection's responsibilities. For example: `This connection receives an inbound request to synchronize account information with the cloud application.`

Trigger Business Events Page

Select the business event details for the endpoint.

Element	Description
Hotel ID	Provide your hotel ID. This is the ID associated with your property. This ID is used for both authentication purposes and to retrieve business events for this hotel ID.
External System ID	Provide your external system ID. This is the ID configured in your OPERA Cloud that references your system.
Polling Interval (Secs)	Enter the number of seconds that you want the adapter to poll for business events from OPERA Cloud. Enter a number between `5` and `600` seconds.
Polling Option	Select an option: • **Fetch just for given Hotel ID**: Gets business events for the given hotel ID only. • **Fetch for all Hotel IDs of the tenant associated to the given External System ID**: Gets business events for all hotel IDs associated with the given external system ID.
Event Limit (1 - 20)	Select a number between **1** and **20**. OHIP business event APIs are limited to a maximum number of 20 events in each API call.

Invoke Category Page

Select the category of the OHIP operation to perform.

Element	Description
Select the Category of the OHIP operation	Select the category of the OHIP operation from the list that is executed by this invoke connection. You only see the categories that you can access on the OHIP Developer Portal.

Invoke Module Page

Select the module of the OHIP operation of the category you selected on the Category page.

Element	Description
Select the Module of the OHIP operation of the previously selected Category	Select the module for the previously selected category of OHIP operation that is executed by this invoke connection. You only see the modules that you can access on the OHIP Developer Portal.

Invoke Operations Page

Specify the invoke operation.

Element	Description
API Lifecycle	Filter the operations by API version (for example **All**, **v0**, and **v1**).
Method	Filter the operations by HTTP method (for example **ALL**, **GET**, **PUT**, **POST**, and others).
Operation	Select the operation for the previously selected category and module of OHIP operation to be executed by this invoke operation. You only see the operations that you can access on the OHIP Developer Portal.

Summary Page

You can review the specified adapter configuration values on the Summary page.

Element	Description
Summary	Displays a summary of the configuration values you defined on previous pages of the wizard. The information that is displayed can vary by adapter. For some adapters, the selected business objects and operation name are displayed. For adapters for which a generated XSD file is provided, click the XSD link to view a read-only version of the file. To return to a previous page to update any values, click the appropriate tab in the left panel or click **Go back**. To cancel your configuration details, click **Cancel**.

4

Implement Common Patterns Using the Oracle Hospitality Adapter

You can use the Oracle Hospitality Adapter to implement the following common patterns.

Topics:

Update or Retrieve Information from OPERA Cloud

To update or retrieve business information (get reservations, create a profile, and others) from OPERA Cloud, use the Oracle Hospitality Adapter as an invoke connection and select the required operation. In this example, you create an integration that is invoked by a third party with REST to retrieve a hotel reservation.

Use an Application Integration to Update or Retrieve Information from OPERA Cloud (Invoke Connection)

1. Configure the Oracle Hospitality Adapter as an invoke connection (no connectivity agent is required).
2. Create an application integration.
3. Configure the REST Adapter as a trigger connection according to your business requirements.
4. Drag the Oracle Hospitality Adapter to the second position. This connection uses the Oracle Hospitality Adapter invoke connection configured in Step 1 to get the business information about a hotel reservation.
5. Configure the adapter accordingly.
   a. Use the OPERA Cloud Integration Processor APIs to get reservation details from OPERA Cloud (**property** > **Reservation** > **GetReservation**).
   b. Check your OHIP Customer Portal for details about these APIs.
6. Configure both the request and response map actions according to your business requirements, namely the **Hotel ID**, **Reservation ID**, and others for the request. The response payload schema of the reservation is available in the response map. Therefore, it can be used/transformed, as required.

Fetch Business Events from OPERA Cloud

To fetch business events from OPERA Cloud using the Oracle Hospitality Adapter, you have two options:

- Use the Connectivity Agent to Poll for Business Events from OHIP (Trigger Role)

- Created a Schedule Integration to Poll for Business Events from OHIP (Invoke Connection)

Use the Connectivity Agent to Poll for Business Events from OHIP (Trigger Role)

1. In the navigation pane, click **Design**, then **Agents**.
2. Create an agent group.
3. Configure a connection for the Oracle Hospitality Adapter and select the agent group.
4. In the navigation pane, click **Design**, then **Integrations**.
5. Create an application integration.
6. Drag the Oracle Hospitality Adapter to the trigger position.
7. Configure the Oracle Hospitality Adapter accordingly.
    a. On the Basic Info page, specify a name and optional description.
    b. On the Business Events page, specify the hotel ID, external system ID, polling interval (in seconds), polling option, and event limits.

> **Note:**
>
> OPERA Cloud business event consumption (trigger connection) is only supported with the connectivity agent. The connectivity agent is required because it polls for events from the OHIP platform at the configured interval. Event payload processing is delegated to the Oracle Hospitality Adapter in the integration flow after polling.

Created a Schedule Integration to Poll for Business Events from OHIP (Invoke Connection)

1. Configure a connection for the Oracle Hospitality Adapter (no agent group is required).
2. Create a schedule integration.
3. Drag the Oracle Hospitality Adapter to the first location. This adds the Oracle Hospitality Adapter as an invoke connection that receives business events.
4. Configure the Oracle Hospitality Adapter accordingly.
    a. Select the property category, the Integration Processor module, and the **getBusinessEvents** operation or the **getBusinessEventsByExternalSystem** operation if you want to fetch by Hotel ID or by External System ID (multiple Hotel IDs). Check your OHIP Customer Portal for details on these APIs.
    b. Configure both the request and response map actions according to your needs. **Hotel ID** and **External System ID** are mandatory fields for the request. Without them, the API call fails at runtime. The **Event Limit** field is optional, but it is applied the default value by OHIP if not mapped. The response payload schema of the business events is available on the response map to be used to get/transform the required information.
5. Configure OPERA Cloud accordingly.

a. Configure the business events of interest in OPERA Cloud so the Oracle Hospitality Adapter can receive them.

b. Check the OHIP/OPERA Cloud documentation. See Polling API (pull) in the *User Guide*.

5

Troubleshoot the Oracle Hospitality Adapter

Review the following topics to learn about troubleshooting issues with the Oracle Hospitality Adapter.

Topics:

Cannot Successfully Test the Oracle Hospitality Adapter Connection Credential Properties

There can be several reasons why you cannot successfully test the connection, but the majority are related to being unable to get the request OAuth access token. Here are some of the most common problems when configuring the Oracle Hospitality Adapter connection.

Topics:

CASDK-0005: A connector specific exception was raised by the application

If you receive the following error, you likely inserted values in both the SSD authentication-dedicated fields (**Username** and **Password**) and the OCIM authentication-dedicated fields (**Scope** and **Enterprise ID**).

```
CASDK-0005: A connector specific exception was raised by the application.
OAUTH security provider is not provided hence generic OAUTH is not supported.
```

You cannot use both authentication methods, which causes the adapter to fail with this error when validating the connection configuration. This error is especially comment when migrating from SSD to OCIM. Because Oracle Integration cannot sometimes handle deleting the user name and password and inserting the scope and enterprise ID, the user interface may appear correct, but the underlying values are still there. The best practice is to recreate the connection.

Solution:

1. Recreate the connection providing the OHIP security policy information with the user name and password for the SSD identity provider or the scope and enterprise ID for the OCIM identity provider.

2. Retest the connection.

Error: The connection test failed. Check your connection and credential properties

If you receive the following error, the information provided likely does not match the credentials provided by OHIP or the user name/password or scope/enterprise ID are wrong.

```
The connection test failed. Check your connection and credential
properties.
```

Solution:

1. Confirm the information provided for the OHIP security policy (**Gateway URL**, **Client ID**, **Client Secret**, **Application Key**, **Username**, and **Password** or **Scope** and **Enterprise ID**).
2. Retest the connection.

Troubleshoot Other Generic Errors

If you receive a different error, the best way to test and troubleshoot the connection is to try to get the OAuth token through Postman, curl, or another API REST-capable tool. The following example shows how to use curl to test your configurations:

```
# SSD identity provider
curl --location '<gateway_URL>/oauth/v1/tokens' --header 'x-app-key:
<app-key>' --header 'Content-Type: application/x-www-form-urlencoded'
--header
'Authorization: Basic <base64_client_id:client_secret>' --data-
urlencode 'username=<user_name>' --data-urlencode
'password=<password>' --data-urlencode
'grant_type=password'
# OCIM identity provider
curl --location '<gateway_URL>/oauth/v1/tokens' --header 'x-app-key:
<app_key>' --header 'enterpriseId: <enterprise_id>' --header 'Content-
Type:
application/x-www-form-urlencoded' --header 'Authorization: Basic
<base64_client_id:client_secret>' --data-urlencode 'scope=<scope>' --
data-urlencode
'grant_type=client_credentials'
```

Where:

Element	Description
gateway_URL	The gateway URL provided in your environment details in the OHIP Developer Portal.

Element	Description
`base64_client_id:client_secret`	The base64-encoded `client_id` and `client_secret`. Both values are provided in your environment details in the OHIP Developer Portal.
`app_key`	The application key provided in your application details within the OHIP Developer Portal.
`user_name`	The Integration User user name created in OPERA Cloud if using the SSD identity provider.
`password`	The Integration User password created in OPERA Cloud if using the SSD identity provider.
`scope`	The scope provided in your environment details in the OHIP Developer Portal if using the OCIM identity provider.
`enterprise_id`	The enterprise ID provided in your environment details in the OHIP Developer Portal if using the OCIM identity provider.

Solution: Troubleshoot by making the OAuth call with curl, Postman, or a different tool.

Cannot Successfully Run the Oracle Hospitality Adapter Connection

There can be several reasons why you cannot successfully run the adapter on an integration. Most are related to being unable to get the request OAuth access token at runtime or issues invoking the OHIP API that provide information about the available APIs of the application and respective interface at design time (when the wizard is open). Here are some of the most common problems when running the adapter:

Topics:

- Generic Error on the Basic Info Page During Invoke Role Configuration with the Adapter Endpoint Configuration Wizard
- Generic Summary Page Error During Invoke Role Configuration with the Adapter Endpoint Configuration Wizard
- HTTP 406 Not Acceptable - CASDK-0041 An error occurred while invoking the REST endpoint

Generic Error on the Basic Info Page During Invoke Role Configuration with the Adapter Endpoint Configuration Wizard

This error can occur when the available APIs fail to be obtained for your application to build the Adapter Endpoint Configuration Wizard pages.

Ensure that you followed all the steps in the workflow. See Workflow to Create and Add an Oracle Hospitality Adapter Connection to an Integration.

Solution: Ensure that you subscribed your application to the API Catalog subscription in the OHIP Developer Portal and the connection is well-defined and successfully tested.

Generic Summary Page Error During Invoke Role Configuration with the Adapter Endpoint Configuration Wizard

This error occurs when the interface fails to be obtained for the operation chosen because of an `OHIP 5xx` return code. Unfortunately, there isn't a well-defined solution that can be used with the Oracle Hospitality Adapter for this issue.

You can cancel and retry the Adapter Endpoint Configuration Wizard and delete the just-added action and add a new action starting from scratch. If it's possible to solve the issue, in the worst-case scenario, use the REST Adapter to make the REST calls to OHIP.

Solution: Retry the Adapter Endpoint Configuration Wizard starting from scratch and open a service request (SR). You can use the REST Adapter as a temporary adapter alternative. See Use the REST Adapter as an Alternative Connection.

HTTP 406 Not Acceptable - CASDK-0041 An error occurred while invoking the REST endpoint

This error can occur when fetching business events and mapping the event message with another request message and no business events are fetched (queue is empty). The trigger connection appears as successfully executed, but subsequent mapping activities appear as failed.

Solution: When using the Oracle Hospitality Adapter as a trigger connection, you must validate the content of the response message received. If the response is similar to the one below, it means the Oracle Hospitality Adapter was able to invoke OHIP, but there were no events for the given configuration (there may be business events on future polling activities).

```
<execute xmlns="http://xmlns.oracle.com/cloud/adapter/
oraclehospitality/BUSINESS_EVENTS/types">
  <request-wrapper
xmlns="http://xmlns.oracle.com/cloud/adapter/oraclehospitality/
BUSINESS_EVENTS/types">
    <pollingStatus>NO_CONTENT</pollingStatus>
  </request-wrapper>
</execute>
```

Miscellaneous Oracle Hospitality Adapter Errors

This section describes how to troubleshoot miscellaneous Oracle Hospitality Adapter errors.

- Use the REST Adapter as an Alternative Connection

Use the REST Adapter as an Alternative Connection

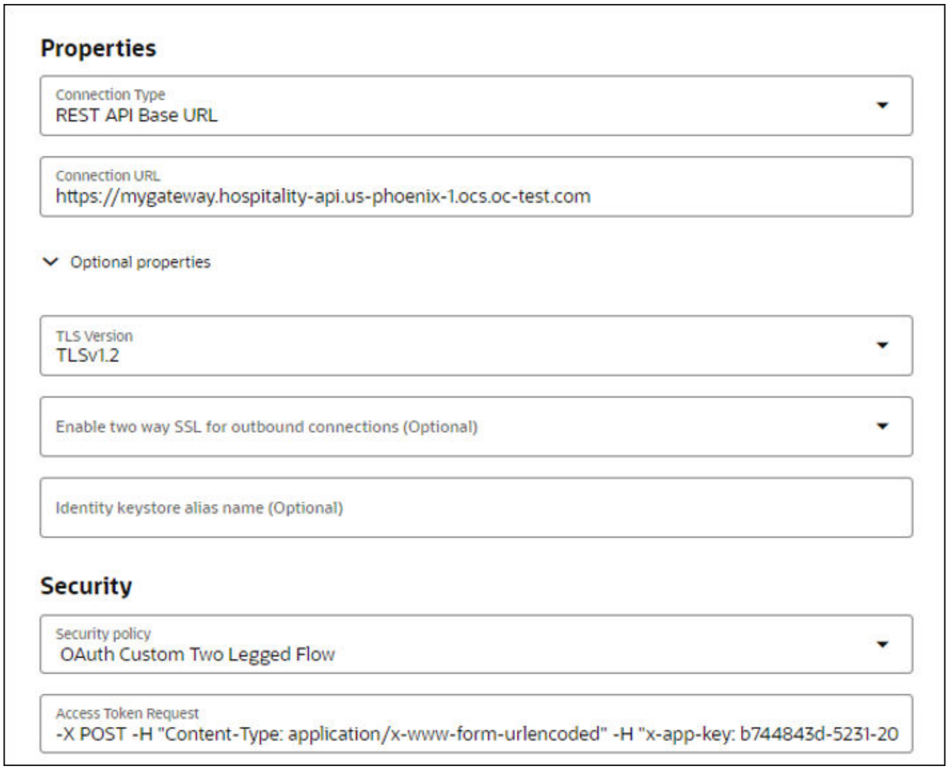
The main role of the Oracle Hospitality Adapter is to facilitate the integration with the OPERA Cloud/OHIP product. In some extreme situations, you may want to temporarily use the REST Adapter (for example, to troubleshoot connection problems). This section describes the equivalent connection configuration for the SSD and OCIM identity provider authentication topologies of the REST Adapter.

Topics:

- OCIM Identity Provider
- SSD Identity Provider

OCIM Identity Provider

Configure the REST Adapter connection as follows.



Properties

Connection Type: REST API Base URL

Connection URL: https://mygateway.hospitality-api.us-phoenix-1.ocs.oc-test.com

TLS Version: TLSv1.2

Enable two way SSL for outbound connections (Optional)
Identity keystore alias name (Optional)

Security

Security policy: OAuth Custom Two Legged Flow

Access Token Request: -X POST -H "Content-Type: application/x-www-form-urlencoded" -H "x-app-key: b744843d-5231-20

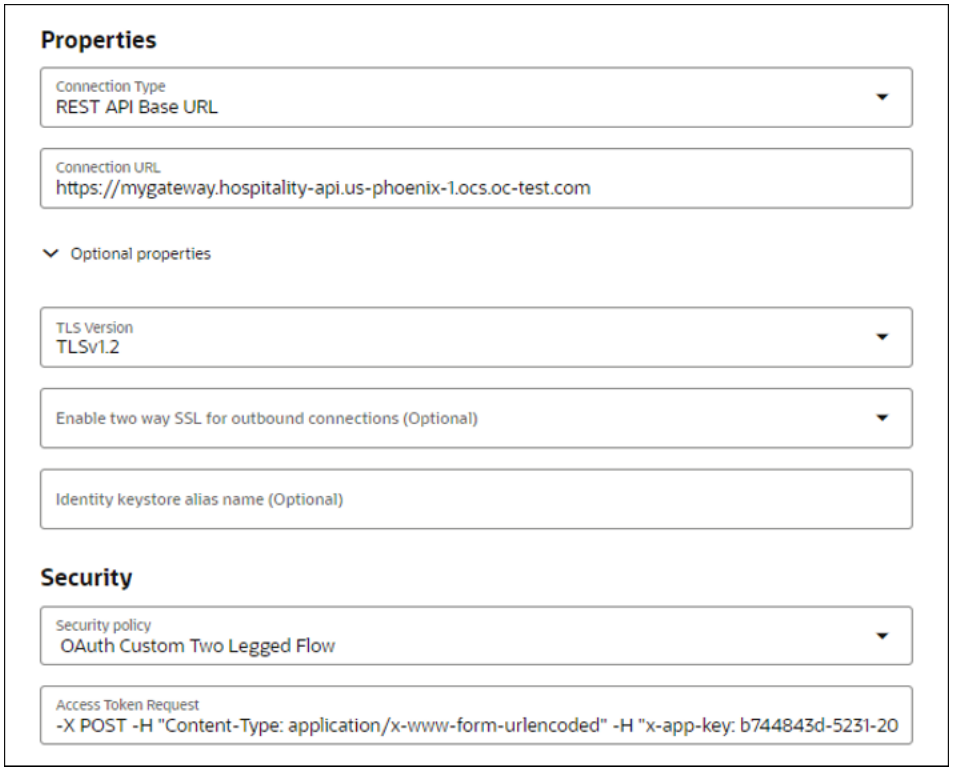
Where:

Element	Description
Connection Type	Select **REST API Base URL**.

Element	Description
Connection URL	Enter your OHIP gateway found on the ENV in the OHIP Developer Portal. For example: `https://mygateway.hospitality-api.us-phoenix-1.ocs.oc-test.com`
TLS Version	Select **TLSv1.2**.
Security policy	Select **OAuth Custom Two Legged Flow**.
Access Token Request	Enter the following: `-X POST -H "Content-Type: application/x-www-form-urlencoded" -H "x-app-key: <app_key>" -H "enterpriseId: <enterprise_id>" -H "Authorization: Basic <base64_clientid:clientesecret>" -d "scope=<scope>&grant_type=client_credentials" "<ohip_gateway>/oauth/v1/tokens"` Where: • `<app_key>` is your app key found on the APP in the OHIP Developer Portal (for example, `b744843d-5231-2095-8ae9-cea0f1aca20f`). • `<enterprise_id>` is your enterprise ID found on the ENV in the OHIP Developer Portal. • `<base64_clientid:clientesecret>` is the base 64 encoding of your client ID and client secret, found on the ENV in the OHIP Developer Portal, separated by a colon symbol (for example, `Y2xpZW50aWQ6Y2xpZW50ZXNlY3JldA==`). • `<scope>` is your scope found on the ENV in the OHIP Developer Portal. Don't forget to URL-encode it (for example, `urn%3Aopc%3Aabcd%3Aws%3A__myscopes__`). • `<ohip_gateway>` is again your OHIP gateway found on the ENV in the OHIP Developer Portal. This is the same as the connection URL.

SSD Identity Provider

Configure the REST Adapter connection as follows.



Properties

Connection Type
REST API Base URL

Connection URL
https://mygateway.hospitality-api.us-phoenix-1.ocs.oc-test.com

Optional properties

TLS Version
TLSv1.2

Enable two way SSL for outbound connections (Optional)

Identity keystore alias name (Optional)

Security

Security policy
OAuth Custom Two Legged Flow

Access Token Request
-X POST -H "Content-Type: application/x-www-form-urlencoded" -H "x-app-key: b744843d-5231-20

Where:

Element	Description
Connection Type	Select **REST API Base URL**.
Connection URL	Enter your OHIP gateway found on the ENV in the OHIP Developer Portal. For example: `https://mygateway.hospitality-api.us-phoenix-1.ocs.oc-test.com`
TLS Version	Select **TLSv1.2**.
Security policy	Select **OAuth Custom Two Legged Flow**.

Element	Description

Access Token Request	Enter the following:
	`-X POST -H "Content-Type:`
	`application/x-www-form-urlencoded"`
	`-H "x-app-key: <app_key>" -H`
	`"Authorization: Basic`
	`<base64_clientid:clientesecret>"`
	`-d`
	`"username=<username>&password=<password>&grant_type=password"`
	`"<ohip_gateway>/oauth/v1/tokens"`
	Where:
	• `<app_key>` is your app key found on the APP in the OHIP Developer Portal (for example, `b744843d-5231-2095-8ae9-cea0f1aca20f`).
	• `<base64_clientid:clientesecret>` is the base 64 encoding of your client ID and client secret, found on the ENV in the OHIP Developer Portal, separated by a colon symbol (for example, `Y2xpZW50aWQ6Y2xpZW50ZXNlY3JldA==`).
	• `<username>` is your Oracle Integration user name created in OPERA Cloud.
	• `<password>` is your Oracle Integration password created in OPERA Cloud.
	• `<ohip_gateway>` is again your OHIP gateway found on the ENV in the OHIP Developer Portal. This is the same as the connection URL.