

# Oracle® Cloud

## Using the FHIR Adapter with Oracle Integration 3



F99964-01  
August 2024



Oracle Cloud Using the FHIR Adapter with Oracle Integration 3,

F99964-01

Copyright © 2024, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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 is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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

---

Audience	iv
Documentation Accessibility	iv
Diversity and Inclusion	iv
Related Resources	v
Conventions	v

## 1 Understand the FHIR Adapter

---

FHIR Adapter Capabilities	1-1
FHIR Adapter Restrictions	1-2
What Application Version Is Supported?	1-2
Workflow to Create and Add a FHIR Adapter Connection to an Integration	1-2

## 2 FHIR Concepts

---

Supported FHIR Capabilities	2-1
-----------------------------	-----

## 3 Create a FHIR Adapter Connection

---

Prerequisites for Creating a Connection	3-1
Create a Connection	3-2
Configure Connection Properties	3-3
Configure Connection Security	3-4
Configure the Endpoint Access Type	3-9
Test the Connection	3-10
Upload a Certificate to Connect with External Services	3-10

## 4 Add the FHIR Adapter Connection to an Integration

---

Invoke Basic Info Page	4-1
Configure Interaction Page	4-1
Summary Page	4-3

# 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](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Related Resources](#)
- [Conventions](#)

## 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
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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 FHIR Adapter

Review the following topics to learn about the FHIR 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:

- [FHIR Adapter Capabilities](#)
- [FHIR Adapter Restrictions](#)
- [What Application Version Is Supported?](#)
- [Workflow to Create and Add a FHIR Adapter Connection to an Integration](#)

## FHIR Adapter Capabilities

The FHIR Adapter enables you to create an integration between a Fast Healthcare Interoperability Resources (FHIR) application server and Oracle Integration. The FHIR Adapter is similar to the REST Adapter, but with a FHIR-specific configuration experience. You can configure the FHIR Adapter as an invoke connection in an integration in Oracle Integration.

An important aspect of integrating healthcare use cases with Oracle Integration is the ability to allow Oracle Integration to call a FHIR application server. FHIR is a standard used to access and exchange healthcare data. FHIR provides clinicians and patients with access to information in a patient's electronic health records.

The FHIR Adapter provides the following capabilities:

- Supports FHIR version 4.0.1.
- Supports outbound invocations of FHIR endpoints processed by a FHIR application server.
- Supports creating, reading, updating, deleting, or searching a FHIR resource.
- Supports FHIR standard definition resources with the following maturity levels; normative, 5, 4, and 3.
- Supports the packaged delivery of all FHIR resources to and from the FHIR base specification.
- Supports custom and standard headers.
- Supports customized query parameters.
- Supports the same security policies for outbound invocations as the REST Adapter. See [Configure Connection Security](#).
- Works exclusively with Oracle Integration for Healthcare to create integrations that interact with healthcare organizations that use FHIR. See Introduction to Oracle Integration for Healthcare in *Using Oracle Integration for Healthcare in Oracle Integration 3*.

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

# FHIR Adapter Restrictions

Note the following FHIR Adapter restrictions.

- Trigger (inbound) connections are not supported. To achieve this functionality, use the REST Adapter.
- Only creating, reading, updating, deleting, or searching a FHIR resource is supported. Other interactions such as history and custom operations are not supported.
- The FHIR Adapter is visible in the Create connection panel regardless of whether your Oracle Integration instance includes the Healthcare edition. The FHIR Adapter is unusable without the Healthcare edition.
- Bundle resources with heterogeneous resource objects in the entry array are not supported.
- FHIR profiles are not supported with the FHIR Adapter in this release.
- The FHIR resource extension is not supported.
- When updating a FHIR resource, the PATCH operation is not supported.



## 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 a FHIR Adapter Connection to an Integration

You follow a very simple workflow to create a connection with a FHIR 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 Oracle Integration.	Go to your login URL.
2	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.	<a href="#">Create a FHIR Adapter Connection</a>
3	Create the integration. When you do this, you add trigger (source) and invoke (target) connections to the integration.	Understand Integration Creation and Best Practices in <i>Using Integrations in Oracle Integration 3</i> and <a href="#">Add the FHIR Adapter Connection to an Integration</a>

Step	Description	More Information
4	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in <i>Using Integrations in Oracle Integration 3</i>
5	(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 <i>Using Integrations in Oracle Integration 3</i>
6	Activate the integration.	Activate an Integration in <i>Using Integrations in Oracle Integration 3</i>
7	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in <i>Using Integrations in Oracle Integration 3</i>
8	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Track Integration Instances in <i>Using Integrations in Oracle Integration 3</i>
9	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in <i>Using Integrations in Oracle Integration 3</i>



# 2

## FHIR Concepts

The FHIR Adapter supports many capabilities of FHIR. You configure these capabilities for the FHIR Adapter in the Adapter Endpoint Configuration Wizard. This section provides a conceptual overview of key supported capabilities.

### Topics:

- [Supported FHIR Capabilities](#)

## Supported FHIR Capabilities

This section provides a conceptual overview of key FHIR capabilities supported by the FHIR Adapter.

- [FHIR](#)
- [FHIR Standard Definition Support](#)
- [FHIR Resources](#)
- [FHIR Interactions](#)
- [Standard and Custom Request and Response Headers](#)
- [Search Parameters](#)
- [Bundle Support](#)

### FHIR

HL7 Fast Healthcare Interoperability Resources (FHIR) is a standard for accessing and exchanging healthcare data between different computer systems regardless of how it is stored in those systems. FHIR has the potential to improve patient care by providing clinicians and patients with timely access to information in a patient's electronic health records. FHIR enables healthcare information, including clinical and administrative data, to be available securely to those who have a need to access it for the benefit of a patient receiving care.

See [HL7 FHIR](#).

### FHIR Standard Definition Support

The FHIR standard schema definition is a published set of XSDs that the FHIR standard organization uses to model healthcare resources such as patient, observation, and others. It provides an extension framework that allows different consumers to extend the model to support different attributes while still complying with the schema.

The standard schema definition is automatically selected for you when configuring the FHIR Adapter in the Adapter Endpoint Configuration Wizard. See [Configure Interaction Page](#).

### FHIR Resources

FHIR divides healthcare data into categories such as patients, laboratory results, insurance claims, and many others. Each category is represented by a FHIR resource, which defines the

details that comprise an exchangeable patient record. Resources satisfy most common healthcare patient use cases.

See [Resource Index](#).

Oracle Integration supports a number of FHIR resources. You select a supported resource when configuring the FHIR Adapter in the Adapter Endpoint Configuration Wizard. See [Configure Interaction Page](#).

### FHIR Interactions

FHIR interactions are the set of actions to take on FHIR resources. Interactions can be grouped according to whether they act upon an instance, a type, or the whole system. FHIR supports interactions at the individual instance level (such as getting an individual resource, updating an individual resource, and deleting an individual resource) and interactions at the resource level (such as search and create).

The following interactions are supported:

- Read: Accesses the current contents of a resource.  
See [read](#).
- Update: Creates a new current version for an existing resource or creates an initial version if no resource already exists for the given ID.  
See [update](#).
- Delete: Removes an existing resource.  
See [delete](#).
- Create: Creates a new resource in a FHIR server-assigned location.  
See [create](#).
- Search: Searches a set of resources based on a filter criteria. Use the search interaction to retrieve resources from the FHIR resource repository.  
See [search](#).

You select the interaction to perform when configuring the FHIR Adapter in the Adapter Endpoint Configuration Wizard. See [Invoke Basic Info Page](#) and [Configure Interaction Page](#).

### Standard and Custom Request and Response Headers

FHIR provides a number of standard headers that control the way the FHIR server returns data. FHIR also specifies a syntax for defining custom headers.

See [HTTP Headers](#) and [Custom Headers](#).

You can select standard headers and create custom request and response headers when configuring the FHIR Adapter in the Adapter Endpoint Configuration Wizard. See [Configure Interaction Page](#).

### Search Parameters

A filter parameter can be used with the search operation. Filter requests have access to the same set of search parameters that are available to the search operation in that resource context on the FHIR server.

See [Filter Parameter](#) and [Search](#).

You can specify search parameters when configuring the FHIR Adapter in the Adapter Endpoint Configuration Wizard. See [Configure Interaction Page](#).

## Bundle Support

Search results are returned in a bundle, which is another resource within the FHIR standard definition. A bundle is a predefined container resource that can contain an array of entries of the same resources (homogenous set of resource instances) or different resources (heterogeneous mixture of resource instances).

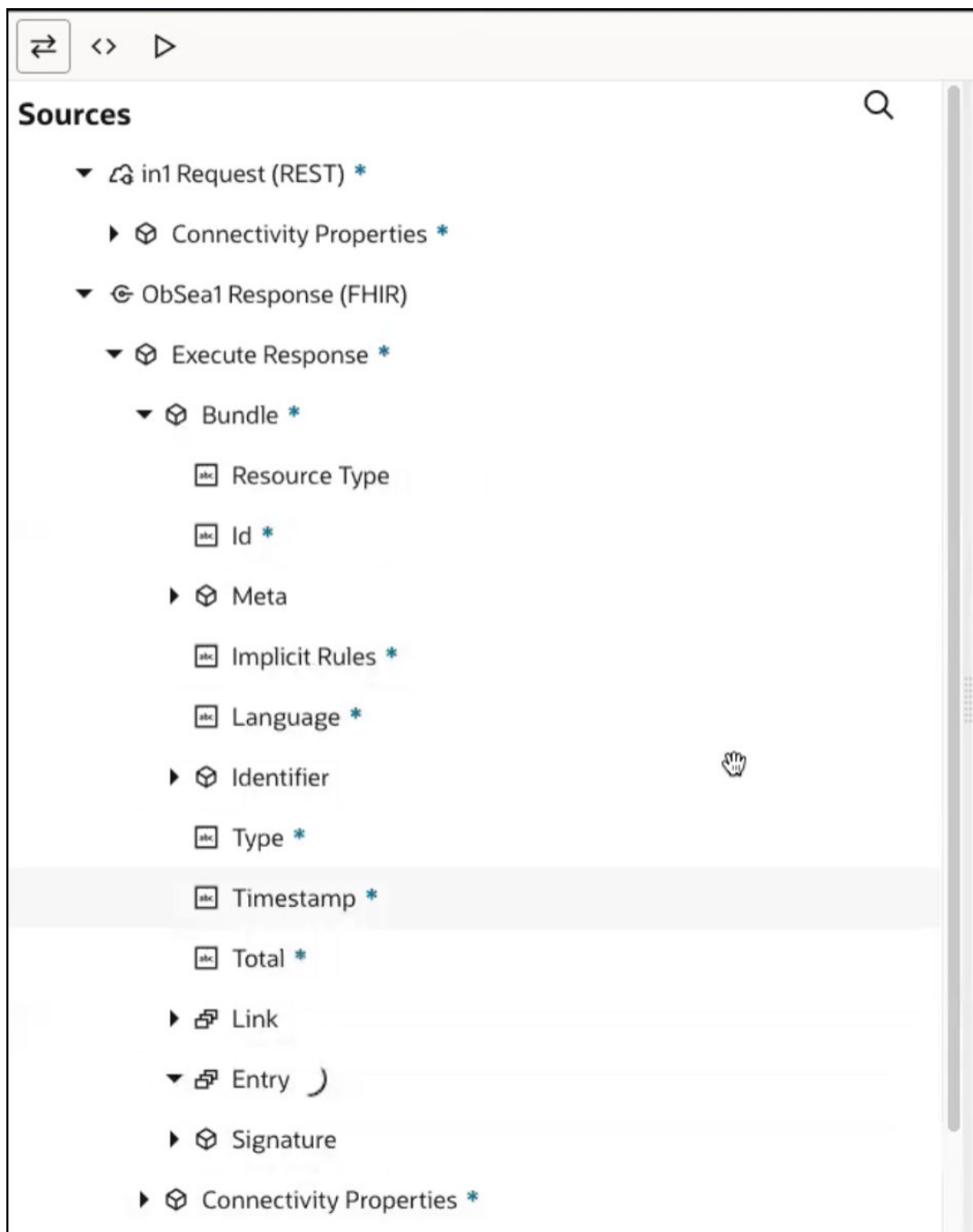
The bundle creation for the case of search or other type of interactions that may use the bundle can be internal and does not need any user selection or configuration. The only selection that drives the overall schema creation is the resource selection.

The following example shows the response schema generated by the FHIR Adapter for a search result with a homogenous set of resource instances in the mapper.

- For the request, the search parameters in the mapper look as follows:



- For the response, the bundle in the mapper looks as follows:



# 3

## Create a FHIR Adapter Connection

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

### 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 FHIR Adapter. The FHIR Adapter is similar to the REST Adapter and supports many of the same security policies.

- [OAuth Security Policies Use](#)
- [SSL Endpoints Use](#)
- [JWT Assertions Outbound Use](#)

### OAuth Security Policies Use

If you are using one of the OAuth security policies, you must already have registered your client application to complete the necessary fields on the Connections page. The Basic Authentication and No Security Policy security policies are exempted.

Before a client application can request access to resources on a resource server, the client application must first register with the authorization server associated with the resource server.

The registration is typically a one-time task. Once registered, the registration remains valid, unless the client application registration is revoked.

At registration time, the client application is assigned a client ID and a client secret (password) by the authorization server. The client ID and secret are unique to the client application on that authorization server. If a client application registers with multiple authorization servers (for example, Facebook, Twitter, and Google), each authorization server issues its own unique client ID to the client application.

@ref: <http://tutorials.jenkov.com/oauth2/authorization.html>

For OAuth configuration, read the provider documentation carefully and provide the relevant values.

### SSL Endpoints Use

For SSL endpoints, obtain and upload a server certificate. See [Upload a Certificate to Connect with External Services](#).

### JWT Assertions Outbound Use

Perform the following prerequisites to use JWT assertions.

- Manually create a signing key for upload on the Certificates page. See [Upload a Certificate to Connect with External Services](#). The service provider typically provides instructions on how to generate the signing keys and the format. For an example, see [Required Keys and OCIDs](#).
- Create the JWT header and JWT payload JSON files. You upload both files on the Connections page when configuring the FHIR Adapter to support JWT assertions. See Prerequisites for Creating a Connection in *Using the REST Adapter with 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
<b>Name</b>	Enter a meaningful name to help others find your connection when they begin to create their own integrations.
<b>Identifier</b>	Automatically displays the name in capital letters that you entered in the <b>Name</b> field. If you modify the identifier name, don't include blank spaces (for example, SALES OPPORTUNITY).

Element	Description
<b>Role</b>	<p>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.</p> <p>For example, assume you configure a connection for the Oracle Service Cloud (RightNow) Adapter as only an <b>invoke</b>. Dragging the adapter to a <b>trigger</b> section in the integration produces an error.</p>
<b>Keywords</b>	Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
<b>Description</b>	Enter an optional description of the connection.
<b>Share with other projects</b>	<p><b>Note:</b> This field only appears if you are creating a connection in a project.</p> <p>Select to make this connection publicly available in other projects. Connection sharing eliminates the need to create and maintain separate connections in different projects.</p> <p>When you configure an adapter connection in a different project, the <b>Use a shared connection</b> 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.</p>

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 **Connection URL** field, enter the FHIR server base URL to use.

```
https://FHIR_server/fhir/r4/
```

3. If you want to specify optional details for TLS, two-way SSL, or an identity keystore alias name, click **Optional properties**.

Element	Description
<b>TLS Version</b>	<p>If no value is selected, the default value used for outbound connections is Transport Layer Security (TLS) version 1.3. It's up to your discretion and the end application's requirements to select either TLS version 1.2 or 1.1 as the default.</p> <ul style="list-style-type: none"> <li>• <b>TLSv1.1</b></li> <li>• <b>TLSv1.2</b></li> </ul> <p>TLSv1 is no longer supported. If you previously configured a connection in a version prior to Oracle Integration 3 to use TLSv1.1, either update the connection by not selecting a value for this field or select TLSv1.2.</p> <p>The TLS protocol provides privacy and data integrity between two communicating computer applications.</p> <p>For trigger-only connections, you cannot select a TLS version. Oracle Integration accepts what it receives as long as it's TLSv1.1 or TLSv1.2.</p>
<b>Enable two way SSL for outbound connections (Optional)</b>	<p>If you are configuring the FHIR Adapter for use with a two-way SSL-enabled server, select <b>Yes</b>.</p>
<b>Identity keystore alias name (Optional)</b>	<p>Enter the key alias name from the keystore file that you specified when importing the identity certificate.</p> <p>The alias name to provide must match the name provided for the private key entry in the JKS file.</p>

## Configure Connection Security

Configure security for your FHIR Adapter connection.

1. Go to the **Security** section.
2. Select the security policy and specify the required details.

Selected Security Policy	Fields
Basic Authentication	<ul style="list-style-type: none"> <li>• <b>Username</b> — The name of a user who has access to the destination web service.</li> <li>• <b>Password</b> — Enter the password.</li> <li>• <b>Confirm Password</b> — Reenter the password.</li> </ul>



Selected Security Policy	Fields
OAuth Client Credentials	<ul style="list-style-type: none"><li>• <b>Access Token URI</b> — The URL from which to obtain the access token.</li><li>• <b>Client Id</b> — The client identifier issued to the client during the registration process.</li><li>• <b>Client Secret</b> — The client secret.</li><li>• <b>Confirm Client Secret</b> — Reenter the client secret.</li><li>• <b>Scope</b> — The scope of the access request. Scopes enable you to specify which type of access you need. Scopes limit access for the OAuth token. They do not grant any additional permission beyond that which the user already possesses.</li><li>• <b>Auth Request Media Type</b> — The format of the data you want to receive. This is an optional parameter that can be kept blank. For example, if you are invoking Twitter APIs, you do not need to select any type.</li><li>• <b>Client Authentication</b> — You can optionally configure OAuth flows with client authentication. This is similar to the Postman user interface feature for configuring client authentication.<ul style="list-style-type: none"><li>– <b>Send client credentials as basic auth header:</b> Pass the client ID and client secret in the header as basic authentication.</li><li>– <b>Send client credentials in body:</b> Pass the client ID and client secret in the body as form fields.</li></ul></li></ul>
OAuth Authorization Code Credentials	<ul style="list-style-type: none"><li>• <b>Client Id</b> — The client identifier issued to the client during the registration process.</li><li>• <b>Client Secret</b> — The client secret.</li><li>• <b>Confirm Client Secret</b> — Reenter the client secret.</li><li>• <b>Authorization Code URI</b> — The URI from which to request the authorization code.</li><li>• <b>Access Token URI</b> — URI to use for the access token.</li><li>• <b>Scope</b> — The scope of the access request. Scopes enable you to specify which type of access you need. Scopes limit access for the OAuth token. They do not grant any additional permission beyond that which the user already possesses.</li><li>• <b>Client Authentication</b> — You can optionally configure OAuth flows with client authentication. This is similar to the Postman user interface feature for configuring client authentication.<ul style="list-style-type: none"><li>– <b>Send client credentials as basic auth header:</b> Pass the client ID and client secret in the header as basic authentication.</li><li>– <b>Send client credentials in body:</b> Pass the client ID and client secret in the body as form fields.</li></ul></li></ul>

Selected Security Policy	Fields
OAuth Custom Three Legged Flow	<ul style="list-style-type: none"> <li data-bbox="769 212 1463 380">• <b>Authorization Request</b> — The client application URL to which you are redirected when you provide consent. The authorization server sends a callback to Oracle Integration to obtain an access token for storage. When you create your client application, you must register a redirect URI where the client application is listening.</li> <li data-bbox="769 386 1463 470">• <b>Access Token Request</b> — The access token request to use to fetch the access token. Specify the request using CURL syntax. For example: <pre data-bbox="818 512 1377 569" style="margin-left: 20px;">-X POST method -H headers -d string_data access_token_uri?query_parameters</pre> </li> <li data-bbox="769 596 1463 701">• <b>Refresh Token Request</b> — The refresh token request to use to fetch the access token. This request refreshes the access token if it expires. Specify the request using CURL syntax. For example <pre data-bbox="818 743 1377 800" style="margin-left: 20px;">-X POST method -H headers -d string_data refresh_token_uri?query_parameters</pre> </li> <li data-bbox="769 827 1463 911">• <b>Sauth_code</b> — Use regex to identify the authorization code. <pre data-bbox="818 890 873 911" style="margin-left: 20px;">code</pre> </li> <li data-bbox="769 938 1463 1022">• <b>Saccess_token</b> — Use a regular expression (regex) to retrieve the access token. <pre data-bbox="818 1043 1024 1064" style="margin-left: 20px;">access.[tT]oken</pre> </li> <li data-bbox="769 1092 1463 1176">• <b>Srefresh_token</b> — Use regex to retrieve the refresh token. <pre data-bbox="818 1155 1040 1176" style="margin-left: 20px;">refresh.[tT]oken</pre> </li> <li data-bbox="769 1203 1463 1287">• <b>Sexpiry</b> — Use regex to identify when the access token expires. <pre data-bbox="818 1308 954 1329" style="margin-left: 20px;">expires_in</pre> </li> <li data-bbox="769 1356 1463 1440">• <b>Stoken_type</b> — Use regex to identify the access token type. <pre data-bbox="818 1419 1013 1440" style="margin-left: 20px;">token.?[tT]ype</pre> </li> <li data-bbox="769 1470 1463 1747">• <b>access_token_usage</b> — Specify how to pass the token as multiple headers or multiple query parameters to access a protected resource. You cannot pass a mix of headers and query parameters. For headers: <pre data-bbox="818 1663 1321 1747" style="margin-left: 20px;">-H Authorization: \${token_type} \$ {access_token} -H validity: 30000 -H signature: ok</pre> </li> </ul>

---

**Selected Security Policy**

**Fields**

---

You can optionally specify quotes for headers:

```
-H 'Authorization: ${token_type} $  
{access_token}' -H 'validity: 30000' -H  
'signature: ok'
```

For query parameters:

```
?token=$  
{access_token}&validity=3000&signature=ok
```

Selected Security Policy	Fields
OAuth Custom Two Legged Flow	<ul style="list-style-type: none"> <li data-bbox="769 212 1463 390"> <p>• <b>Access Token Request</b> — The access token request to use to fetch the access token. Specify the request using CURL syntax. For example:</p> <pre data-bbox="818 331 1377 390">-X POST method -H headers -d string_data access_token_uri?query_parameters</pre> </li> <li data-bbox="769 415 1463 625"> <p>• <b>Refresh Token Request</b> — The refresh token request to use to fetch the access token. This request refreshes the access token if it expires. Specify the request using CURL syntax. For example</p> <pre data-bbox="818 567 1377 625">-X POST method -H headers -d string_data refresh_token_uri?query_parameters</pre> </li> <li data-bbox="769 651 1463 743"> <p>• <b>Saccess_token</b> — Use regex to identify the access token.</p> <pre data-bbox="818 718 1029 743">access.[tT]oken</pre> </li> <li data-bbox="769 768 1463 861"> <p>• <b>Srefresh_token</b> — Use regex to identify the refresh token.</p> <pre data-bbox="818 835 1045 861">refresh.[tT]oken</pre> </li> <li data-bbox="769 886 1463 1012"> <p>• <b>Sexpiry</b> — Use regex to identify when the access token expires.</p> <pre data-bbox="818 982 964 1012">expires_in</pre> </li> <li data-bbox="769 1037 1463 1129"> <p>• <b>Stoken_type</b> — Use regex to identify the access token type.</p> <pre data-bbox="818 1100 1013 1129">token.?[tT]ype</pre> </li> <li data-bbox="769 1155 1463 1432"> <p>• <b>access_token_usage</b> — Specify how to pass the token as multiple headers or multiple query parameters to access a protected resource. You cannot pass a mix of headers and query parameters.</p> <p>For headers:</p> <pre data-bbox="818 1339 1321 1432">-H Authorization: \${token_type} \${access_token} -H validity: 30000 -H signature: ok</pre> <p>You can optionally specify quotes for headers:</p> <pre data-bbox="818 1549 1370 1642">-H 'Authorization: \${token_type} \${access_token}' -H 'validity: 30000' -H 'signature: ok'</pre> <p>For query parameters:</p> <pre data-bbox="818 1759 1386 1812">?token=\${access_token}&amp;validity=3000&amp;signature=ok</pre> </li> </ul>

Selected Security Policy	Fields
OAuth Client Credentials using JWT Client Assertion  <b>Note:</b> This policy is typically used to invoke application- driven APIs.	<ul style="list-style-type: none"> <li>• <b>Access token URI</b> — Enter the URL to which to send a request to obtain the access token. For example:  <code>https://accounts.google.com/o/oauth2/token</code></li> <li>• <b>JWT headers in JSON format</b> — Upload the JWT header file in JSON format.</li> <li>• <b>JWT payload in JSON format</b> — Upload the JWT payload file in JSON format.</li> <li>• <b>JWT private key alias</b> — Enter the JWT private key alias. This is the same alias you specified when uploading the signing key certificate on the Certificates page.</li> <li>• <b>Scope</b> — (Optional) Enter the scopes.</li> <li>• <b>Access token request</b> — (Optional) Enter the request to obtain the access token. The format you specify can vary by service provider. See Variations of JWT Usage by Service Providers in <i>Using the REST Adapter with Oracle Integration 3</i>.</li> </ul>
OAuth using JWT User Assertion  <b>Note:</b> This policy is typically used on behalf of a user.	<ul style="list-style-type: none"> <li>• <b>Access token URI</b> — Enter the URL to which to send a request to obtain the access token. For example:  <code>https://accounts.google.com/o/oauth2/token</code></li> <li>• <b>JWT headers in JSON format</b> — Upload the JWT header file in JSON format.</li> <li>• <b>JWT payload in JSON format</b> — Upload the JWT payload file in JSON format.</li> <li>• <b>JWT private key alias</b> — Enter the JWT private key alias. This is the same alias you specified when uploading the signing key certificate on the Certificates page.</li> <li>• <b>Scope</b> — (Optional) Enter the scopes.</li> <li>• <b>Access token request</b> — (Optional) Enter the request to obtain the access token. The format you specify can vary by service provider.</li> </ul>
No Security Policy	If you select this security policy, no additional fields are displayed. For example, you need to access a HAPI FHIR server that requires no security policy.

## 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 ...
<b>Public gateway</b>	Connections to endpoints using the public internet.

Option	This Option Appears If Your Adapter Supports ...
<b>Connectivity agent</b>	<p>Connections to on-premises endpoints through the connectivity agent.</p> <ol style="list-style-type: none"> <li>1. Click <b>Associate agent group</b>. The Associate agent group panel appears.</li> <li>2. Select the agent group, and click <b>Use</b>.</li> </ol> <p>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 <i>Using Integrations in Oracle Integration 3</i>.</p>

## 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	<p>A dialog prompts you to select the type of connection testing to perform:</p> <ul style="list-style-type: none"> <li>• <b>Validate and Test:</b> 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.</li> <li>• <b>Test:</b> Connects to the WSDL URL and performs a syntax check on the WSDL. No requests are sent to the operations exposed in the WSDL.</li> </ul>

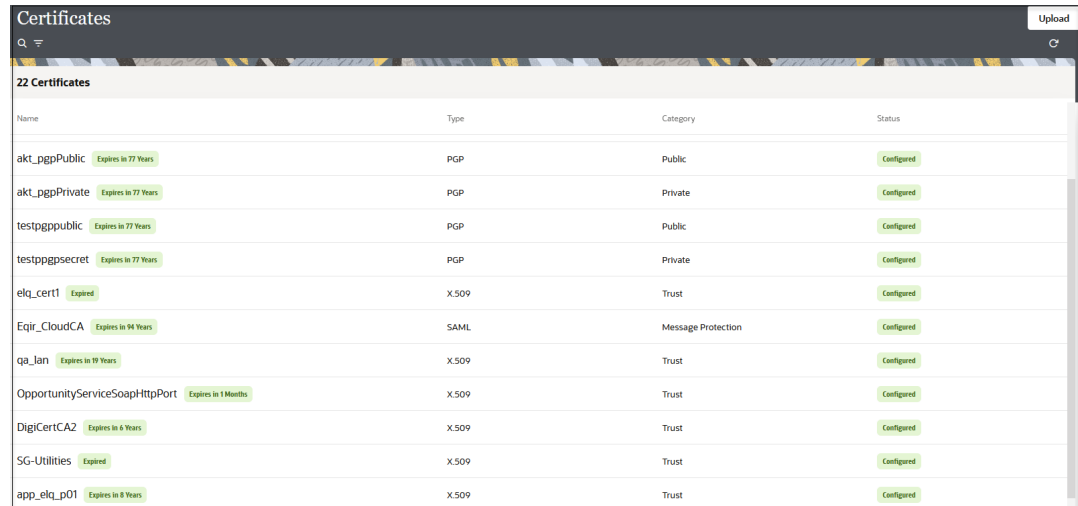
2. Wait for a message about the results of the connection test.
  - If the test was successful, then the connection is configured properly.
  - If the test failed, then edit the configuration details you entered. Check for typos and verify URLs and credentials. Continue to test until the connection is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



Name	Type	Category	Status
akt_pgpPublic <small>Expires in 77 Years</small>	PGP	Public	Configured
akt_pgpPrivate <small>Expires in 77 Years</small>	PGP	Private	Configured
testpgppublic <small>Expires in 77 Years</small>	PGP	Public	Configured
testpgppsecret <small>Expires in 77 Years</small>	PGP	Private	Configured
elq_cert1 <small>Expired</small>	X.509	Trust	Configured
Eqir_CloudCA <small>Expires in 94 Years</small>	SAML	Message Protection	Configured
qa_lan <small>Expires in 99 Years</small>	X.509	Trust	Configured
OpportunityServiceSoapHttpPort <small>Expires in 1 Months</small>	X.509	Trust	Configured
DigiCertCA2 <small>Expires in 6 Years</small>	X.509	Trust	Configured
SG-Utilities <small>Expired</small>	X.509	Trust	Configured
app_elq_p01 <small>Expires in 8 Years</small>	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 [RSA Signature Validation 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**.

# 4

## Add the FHIR Adapter Connection to an Integration

When you drag the FHIR Adapter into the invoke area of an integration, the Adapter Endpoint Configuration Wizard is invoked. This wizard guides you through configuration of the FHIR Adapter endpoint properties.

The following sections describe the wizard pages that guide you through configuration of the FHIR Adapter as an invoke in an integration.

### Topics:

- [Invoke Basic Info Page](#)
- [Configure Interaction Page](#)
- [Summary Page](#)

## Invoke Basic Info Page

Specify a name, description, and action for the invoke connection.

Element	Description
<b>What do you want to call your endpoint?</b>	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: <ul style="list-style-type: none"><li>• No blank spaces (for example, My Inbound Connection)</li><li>• No special characters (for example, #;83&amp; or righ(t)now4) except underscores and hyphens</li><li>• No multibyte characters</li></ul>
<b>What does this endpoint do?</b>	Enter an optional description of the connection's responsibilities.
<b>What would you want to do?</b>	Select an interaction to perform: <ul style="list-style-type: none"><li>• <b>Create, Read, Update, Delete a FHIR Resource</b></li><li>• <b>Search FHIR Resource</b></li></ul>

## Configure Interaction Page

Select the resource, operation, and request and response headers for the FHIR Adapter.

For conceptual information about the fields described on this page, see [Supported FHIR Capabilities](#).

Element	Description
<b>FHIR Schema Source</b>	<b>Standard Schema Definition</b> is displayed. This value cannot be changed.

Element	Description
<b>FHIR Resource</b>	<p>Select one of the supported resources.</p> <ul style="list-style-type: none"> <li>• <b>Patient</b></li> <li>• <b>Practitioner</b></li> <li>• <b>Organization</b></li> <li>• <b>Location</b></li> <li>• <b>Appointment</b></li> <li>• <b>AppointmentResponse</b></li> <li>• <b>Schedule</b></li> <li>• <b>Slot</b></li> <li>• <b>Observation</b></li> <li>• <b>AllergyIntolerance</b></li> <li>• <b>Condition</b></li> <li>• <b>Procedure</b></li> <li>• <b>DiagnosticReport</b></li> <li>• <b>ImagingStudy</b></li> <li>• <b>QuestionnaireResponse</b></li> <li>• <b>MedicationRequest</b></li> <li>• <b>MedicationStatement</b></li> <li>• <b>Medication</b></li> <li>• <b>Immunization</b></li> <li>• <b>CapabilityStatement</b></li> <li>• <b>StructuredDefinition</b></li> <li>• <b>SearchParameter</b></li> <li>• <b>OperationDefinition</b></li> <li>• <b>CodeSystem</b></li> <li>• <b>ValueSet</b></li> <li>• <b>ConceptMap</b></li> <li>• <b>Provincance</b></li> <li>• <b>Audit Event</b></li> <li>• <b>DocumentReference</b></li> <li>• <b>Binary</b></li> <li>• <b>Bundle</b></li> <li>• <b>OperationOutcome</b></li> <li>• <b>Parameters</b></li> <li>• <b>MessageHeader</b></li> <li>• <b>Subscription</b></li> <li>• <b>Questionnaire</b></li> </ul> <p>See <a href="#">Resource Index</a>.</p>
<p><b>FHIR Interaction</b> This field is displayed if you selected <b>Create, Read, Update, Delete a FHIR Resource</b> on the Basic Info page.</p>	<p>Select the operation to perform.</p> <ul style="list-style-type: none"> <li>• <b>update</b></li> <li>• <b>read</b></li> <li>• <b>create</b></li> <li>• <b>delete</b></li> </ul>
<p><b>HTTP Verb</b> This field is displayed if you selected <b>Search FHIR Resource</b> on the Basic Info page.</p>	<p>Select the operation to perform.</p> <ul style="list-style-type: none"> <li>• <b>POST</b></li> <li>• <b>GET</b></li> </ul>

Element	Description
<b>Configure Request Headers</b>	<p>Select the request HTTP headers to add.</p> <ul style="list-style-type: none"> <li>• <b>Standard</b></li> <li>• <b>Custom</b></li> </ul> <p>When you click <b>Continue</b>, a page is displayed to specify the headers to use.</p> <ul style="list-style-type: none"> <li>• For standard HTTP headers, click <b>Add</b>, then double-click the row to display a drop-down list with the following selections: <ul style="list-style-type: none"> <li>– <b>If-Match</b></li> <li>– <b>If-Modified-Since</b></li> <li>– <b>If-None-Match</b></li> <li>– <b>If-None-Exist</b></li> </ul> </li> <li>• For custom HTTP headers, click <b>Add</b>, then double-click to add a custom header name and description.</li> </ul> <p>See <a href="#">HTTP Headers</a> and <a href="#">Custom Headers</a>.</p>
<b>Configure Response Headers</b>	<p>Select the response HTTP headers to add.</p> <ul style="list-style-type: none"> <li>• <b>Standard</b></li> <li>• <b>Custom</b></li> </ul> <p>When you click <b>Continue</b>, a page is displayed to specify the headers to use.</p> <ul style="list-style-type: none"> <li>• For standard HTTP headers, click <b>Add</b>, then double-click the row to display a drop-down list with the following selections: <ul style="list-style-type: none"> <li>– <b>ETag</b></li> <li>– <b>Last Modified</b></li> <li>– <b>Location</b></li> <li>– <b>Content Location</b></li> </ul> </li> <li>• For custom HTTP headers, click <b>Add</b>, then double-click to add a custom header name and description.</li> </ul> <p>See <a href="#">HTTP Headers</a> and <a href="#">Custom Headers</a>.</p>
<b>Search Parameters</b> This field is displayed if you selected <b>Search FHIR Resource</b> on the Basic Info page.	<p>Specify search parameters for the FHIR endpoint.</p> <p>Click the <b>Add</b> icon to display a row for entering the parameter name.</p> <p>Click the <b>Remove</b> icon to delete a selected row.</p> <p>See <a href="#">Filter Parameter</a>.</p>

## Summary Page

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

Element	Description
<b>Summary</b>	<p>Displays a summary of the configuration values you defined on previous pages of the wizard.</p> <p>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.</p> <p>To return to a previous page to update any values, click the appropriate tab in the left panel or click <b>Go back</b>.</p> <p>To cancel your configuration details, click <b>Cancel</b>.</p>