Oracle® Cloud

Using the GCP Storage Adapter with Oracle Integration 3

ORACLE®

Oracle Cloud Using the GCP Storage Adapter with Oracle Integration 3,

F86027-04

Contents

Preface

1   Understand the GCP Storage Adapter

2   Create a GCP Storage Adapter Connection

3   Add the GCP Storage Adapter Connection to an Integration

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
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 GCP Storage Adapter

Review the following topics to learn about the GCP Storage 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:

- GCP Storage Adapter Capabilities
- GCP Storage Adapter Restrictions
- What Application Version Is Supported?
- What Application Version Is Supported?

GCP Storage Adapter Capabilities

The GCP Storage Adapter enables you to create an integration in Oracle Integration that connects to Google Cloud Storage for storing different types of data. You can configure the GCP Storage Adapter as an invoke connection in an integration in Oracle Integration.

The GCP Storage Adapter provides the following capabilities:

- Establishes a connection to Google Cloud Storage in order to perform operations on/for a bucket, object, access controls, notifications, and so on.
- Provides support for performing Create, Update, Get, List, Delete, Patch, and other operations on the selected resource.
- Provides JSON format support for structured uploading and downloading of objects.
- Provides support for attachment upload and download.
- Supports OAuth Authorization Code Credentials authentication.

The GCP Storage Adapter is one of many predefined adapters included with Oracle Integration.

GCP Storage Adapter Restrictions

Note the following GCP Storage Adapter restriction.

- The GCP Storage Adapter does not currently support binary uploading through the FTP Adapter. See Troubleshoot the GCP Storage 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 a GCP Storage 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 Oracle Integration.	Go to `https://instance_URL/ic/home`
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.	Create a GCP Storage Adapter Connection
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 *Using Integrations in Oracle Integration 3* and Add the GCP Storage Adapter Connection to an Integration
4	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in *Using Integrations in Oracle Integration 3*
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 *Using Integrations in Oracle Integration 3*
6	Activate the integration.	Activate an Integration in *Using Integrations in Oracle Integration 3*
7	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in *Using Integrations in Oracle Integration 3*
8	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*
9	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in *Using Integrations in Oracle Integration 3*

2

Create a GCP Storage 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

You must satisfy the following prerequisites to create a connection with the GCP Storage Adapter:

- Create a project ID in the Google Cloud console. See Create a Google Cloud project.

- Register a web application in the Google Cloud console and obtain the client ID and client secret. See OAuth client ID credentials.

> ✏️ **Note:**
>
> You must enter the client ID in the **Google Client ID** field and the secret key in the **Google Client Secret** field on the Connections page. See Configure Connection Security.

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.
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 **Project ID** field, enter the project ID. See Prerequisites for Creating a Connection.

Configure Connection Security

Configure security for your GCP Storage Adapter connection.

1. Go to the **Security** section.

2. In the **Google Client ID** field, enter the Google client ID that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.

3. In the **Google Client Secret** field, enter the client secret that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.

4. In the **Google Authorization scope** field, enter a scope URL. For example: `https://www.googleapis.com/auth/devstorage.read_only`. See Scopes.

5. Click **Provide Consent** to verify the connection properties and get an access token.

   The GCP application log in page is displayed.

6. Enter your GCP login credentials.

7. Once you see an `Authenticated` message, you can test your connection.

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.
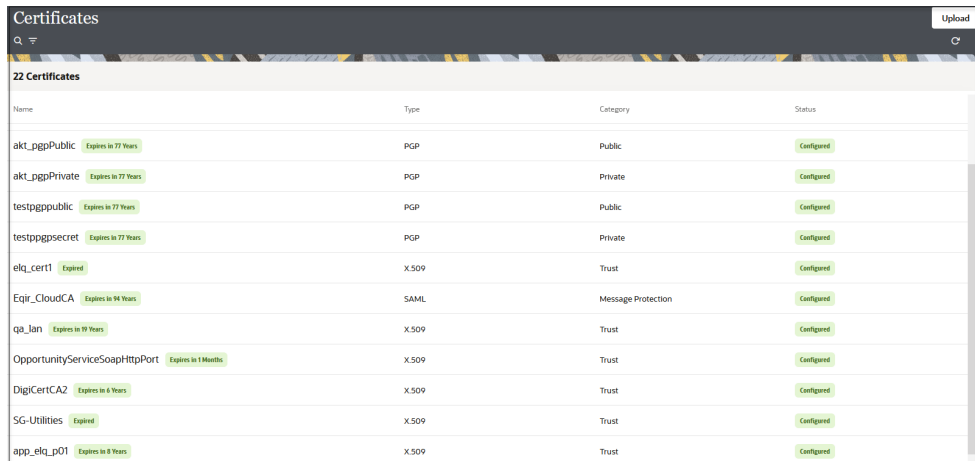
3. When complete, click **Save**.

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.

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**.

Refresh Integration Metadata

You can manually refresh the currently-cached metadata available to adapters that have implemented metadata caching.

Metadata changes typically relate to customizations of integrations, such as adding custom objects and attributes to integrations. There may also be cases in which integrations have been patched, which results in additional custom objects and attributes being added. This option is similar to clearing the cache in your browser. Without a manual refresh, a staleness check is only performed when you drag a connection into an integration. This is typically sufficient, but in some cases you may

know that a refresh is required. For these cases, the **Refresh Metadata** menu option is provided.

> **Note:**
>
> The **Refresh Metadata** menu option is only available with adapters that have implemented metadata caching.

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

2. Hover over the connection to refresh.

3. Click **Actions** ⋯, then select **Refresh metadata**.

   A message is displayed indicating that the refresh was successful.

3

Add the GCP Storage Adapter Connection to an Integration

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

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

Topics:

- Basic Info Page
- Invoke Configuration Page
- Summary Page

Basic Info Page

Specify a name, description, resource and operation on the Basic Info page of each invoke connection 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.
Select Resource	Select a resource: • Buckets • Bucket Access Controls • Default Object Access Controls • Object Access Controls • Objects • Notifications
Action	Select an operation such as Create Bucket, Upload Object, Download Structured Object, Get Notification Configuration, Delete Object ACL Entry, List Bucket ACL Entries, Patch Default Object ACL Entry, and so on. The operations available for selection are based on the resource selected.

Invoke Configuration Page

Select the bucket and other details to perform the operation.

> **Note:**
>
> - The options available for selection on the Configuration page depend upon the resource and operation selected on the Basic Info page.
> - When you select the Create Bucket or List Buckets operation on the Basic Info page, the Configuration page is not displayed.

Element	Description
Select Bucket	Select the bucket on which to perform the operation. You can also enter the beginning letters of the bucket to filter the display of buckets.
Select Object	Select an object.
Select Source Bucket	Select the source bucket.
Select Destination Bucket	Select the destination bucket.
Select Entity	Select an entity.
Provide JSON Sample	Enter sample JSON to describe the structure of data. It is required for structured objects.
Delete after download (Displays if you select **Download Object** and **Download Structured Object** on the Basic Info page.)	Select the check box to delete the object after downloading.

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 GCP Storage Adapter

You can use the GCP Storage Adapter to implement the following common pattern.

Topics:

- [Use the GCP Storage Adapter to Import Data Files into Google Cloud Storage](#)
-

> **Note:**
>
> Oracle Integration offers a number of prebuilt integrations, known as *recipes*, that provide you with a head start in building your integrations. You can start with a recipe, and then customize it to fit your needs and requirements. Depending upon the solution provided, a variety of adapters are configured in the prebuilt integrations.
> See the Recipes and Accelerators page on the Oracle Help Center.

Use the GCP Storage Adapter to Import Data Files into Google Cloud Storage

This use case describes how to import data files from an FTP server into Google Cloud Storage. Similarly, you can import data files from an application into Google Cloud Storage using the GCP Storage Adapter.

To perform this operation, you must create the REST Adapter, FTP Adapter, and GCP Storage Adapter connections in Oracle Integration.

1. Create an application integration.

2. Drag the REST Adapter into the integration canvas.

3. Configure the REST Adapter as follows.

    a. On the Basic Info page, provide the endpoint name.

    b. On the Resource Configuration page, the following details are specified or selected for this use case:

        i.   Provide the endpoint's relative resource URI (for example, `/upload/{fileName}`).

        ii. Select the **GET** action.

        iii. Select the **Add and review parameters for this endpoint** check box.

        iv. Select the **Configure this endpoint to receive the response** check box.

    c. On the Request Parameters page, select the **string** type.

    d. On the Response page, select **JSON Sample** in the **Select the response payload format** field.

    e. Click **inline** and provide a valid JSON payload.

    f. Review your selections on the Summary page.

4. Drag the FTP Adapter into the integration canvas.

5. Configure the FTP Adapter as follows:

    a. On the Basic Info page, provide a name.

    b. On the Operations page, select **Read a File** from the **Select operation** list.

    c. Select **Binary** from the **Select a Transfer Mode** list.

    d. Provide the input directory and file name.

    e. On the Schema page, select **No**.

    f. Review your selections on the Summary page.

6. In the mapper, map the source (REST) **File Name** to the target (FTP) **Filename**.

7. Drag the GCP Storage Adapter into the integration canvas.

8. Configure the GCP Storage Adapter as follows:

    a. On the Basic info page, provide an endpoint name, select **Objects** as a resource, and select **Upload Object** as an action.

    b. On the Configuration page, select the bucket name.

    c. On the Summary page, review your selections.

9. In the mapper, map the source (REST) **File Reference** element to the target (Google Cloud Storage) **Stream Reference** element and **Filename** to **name**.

10. In the REST Response mapper, map the source (**InvokeGCP Response**) to the target (**TriggerREST Response**) as follows.
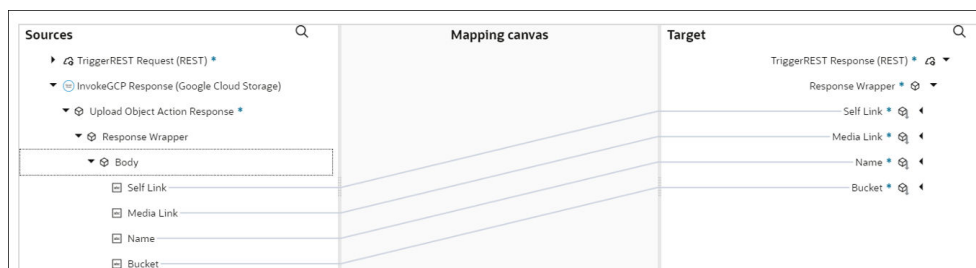
11. Add the tracking variable element in the **Business Identifier** field.

12. When complete, activate the integration. As a result, the GCP Storage Adapter inserts the file or object into the respective bucket.

The completed integration looks as follows.
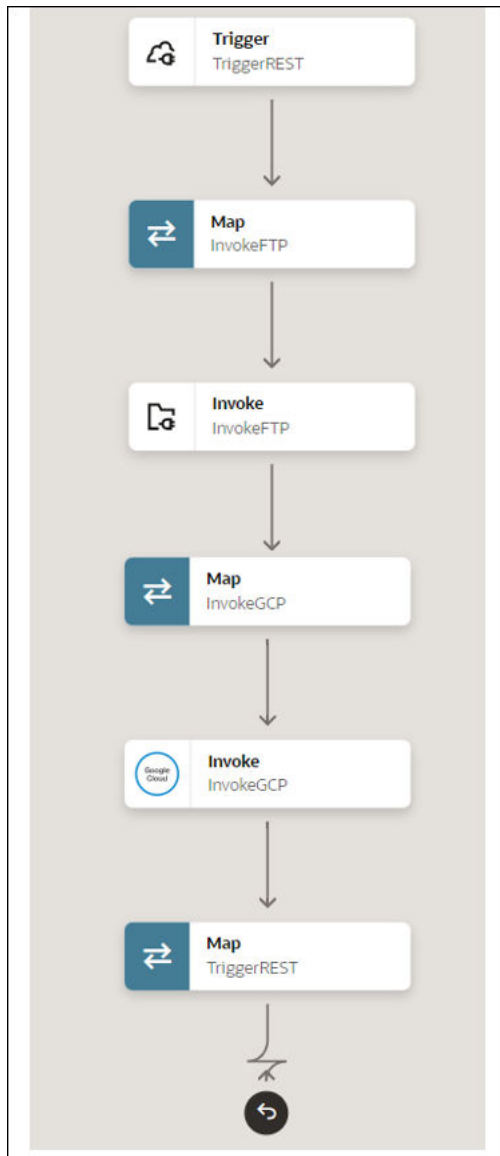
5

Troubleshoot the GCP Storage Adapter

Review the following topic to learn about troubleshooting issues with the GCP Storage Adapter.

Topic:

- Binary Uploading Through an FTP Adapter is Currently Not Supported

Binary Uploading Through an FTP Adapter is Currently Not Supported

The FTP Adapter transfers (reads and writes) files to any publicly accessible server in either binary or ASCII format. However, the GCP Storage Adapter does not currently support binary uploading through the FTP Adapter when you create an integration to transfer data from a certain FTP location (using the FTP Adapter) to Google Cloud Storage.

Workaround: As a workaround, you can use the REST Adapter in Oracle Integration for binary uploading instead of the FTP Adapter.