Oracle® Cloud

Using the Amazon Simple Notification Service (SNS) Adapter with Oracle Integration 3

F92319-05
December 2025

Oracle Cloud Using the Amazon Simple Notification Service (SNS) Adapter with Oracle Integration 3,

F92319-05

Primary Author: Oracle Corporation

Contents

About This Content

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

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 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

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 Amazon Simple Notification Service (SNS) Adapter

Review the following topics to learn about the Amazon Simple Notification Service (SNS) 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:

Amazon Simple Notification Service (SNS) Adapter Capabilities

The Amazon Simple Notification Service (SNS) Adapter enables you to create an integration in Oracle Integration that connects to the Amazon Notification system. The Amazon Simple Notification Service (SNS) Adapter connects to the Amazon SNS distributed publish-subscribe messaging system from Oracle Integration and allows messages to be published and subscribed to from an Amazon SNS topic. The Amazon Simple Notification Service (SNS) Adapter can be configured as a trigger connection and an invoke connection in an integration in Oracle Integration.

The Amazon Simple Notification Service (SNS) Adapter provides the following capabilities:

- Serves as both a message publisher and message subscriber for Amazon SNS topics.
- Supports publishing and subscribing to messages in JSON, XML, and AVRO formats.
- Supports the publishing and subscription of JSON and XML messages.
- Supports the publishing of messages in opaque (stream reference) format.
- Provides seamless integration with webhooks provided for message subscription.
- Provides the option for configuring dead lettering.
- Supports AWS Signature Version 4 authentication for secure message publishing for invoke connections and AWS Signature Version 4 and RSA signature validation for trigger connections.
- Supports integrating with publicly-accessible resources (direct connectivity over the public internet) and private resources over the connectivity agent.

> **Note**
>
> The Amazon Simple Notification Service (SNS) Adapter extends connectivity agent support only for outbound connections.

- Supports configuring a filter while creating a subscription.
- Supports filtration functionality to manage message filtering within the Amazon Simple Notification Service (SNS) Adapter.

> **Note**
>
> The Amazon Simple Notification Service (SNS) Adapter handles message payloads of up to 256 KB in size.

The Amazon Simple Notification Service (SNS) Adapter is one of many predefined adapters included with Oracle Integration. See the Adapters page in the Oracle Help Center.

Amazon Simple Notification Service (SNS) Adapter Restrictions

Note the following Amazon Simple Notification Service (SNS) Adapter restrictions for this release.

- An Amazon Simple Notification Service (SNS) Adapter inbound connection does not support the following:
  - FIFO topics: Only the standard topic is supported, and not the FIFO topic.
  - Connectivity agent
- While configuring an Amazon Simple Notification Service (SNS) Adapter trigger connection in an integration, you must select the topic that supports signature version 2. By default, all topics created in Amazon SNS support signature version 1. You must explicitly make an API call to create/update the topic by setting the following attributes:
  - **Attributes.entry.1.key**: **SignatureVersion**
  - **Attributes.entry.1.value**:**2**
- On the Configuration page of the Adapter Endpoint Configuration Wizard, the Amazon Simple Notification Service (SNS) Adapter shows 100 topics for selection at a time.
- The Amazon Simple Notification Service (SNS) Adapter does not support sending multiple XML messages in one request.
- For all the number type message attributes, the Amazon Simple Notification Service (SNS) Adapter shows a string in the request mapper.

> **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 Amazon Simple Notification Service (SNS) 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	Decide where to work	• Work in a project (see why working with projects is preferred in *Using Integrations in Oracle Integration 3*). • Work outside a project.
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 an Amazon Simple Notification Service (SNS) 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 Amazon Simple Notification Service (SNS) 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 an Amazon Simple Notification Service (SNS) 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 Amazon Simple Notification Service (SNS) Adapter:

- Create an AWS Account
- Create the Inline Policy
- Create an IAM User and Obtain the Access Key and Secret Access Key
- Create the Client Identifier
- Configure the Client Application
- Add Roles to the Client Application

Create an AWS Account

1. Go to https://aws.amazon.com.
2. Click **Create an AWS Account**.
3. Enter a root user email address.
4. Enter a name for your account in the **AWS account name** field.
5. Click **Verify email address**.
6. Once the email address is verified, create your root user password.
7. In the subsequent steps, enter your contact information and billing information details.
8. Complete the transaction to successfully create a root user account.

You can now sign in to your AWS account using the root user credentials.

> **Note**
>
> The root user possesses unrestricted access to AWS resources. It is necessary to create an Identity and Access Management (IAM) user.

Create the Inline Policy

1. Log in to the AWS Console with your root user credentials.
2. Click **IAM** and select **Select the Users** under **Users**.
3. In the **Permissions** tab, click **Add permission** and select **Create Inline policy**.
4. Under **Inline policy**, select **SNS** as a **Service**.
5. To grant the user permission to list topics, under the **Access Level** section, select **List** and then select the **ListTopics** action.

> **Note**
>
> If you want to publish a message to a topic, the corresponding inline policy (publish) must be added to the new or existing policy. Likewise, if you want to subscribe to a topic, the corresponding inline policy (subscribe) must be added to the new or existing policy.

6. Click **Next**.
7. Enter the policy name and click **Create Policy**.
   The newly created policy is added to the list on the Policies page.

Create an IAM User and Obtain the Access Key and Secret Access Key

1. Log in to an AWS account using the root user credential.
2. In the search bar, enter `IAM`.
3. Click **IAM** and select **Users** under **Access management**.
4. Click **Create user**.
5. Enter a name for the user and click **Next**.
6. On the Set Permissions page that appears, perform the following:
   a. Select **Attach policies directly** as the **Permissions Options**.
   b. Select the permission policies that you created for this user and click **Next**. See Create the Inline Policy.
   c. (Optional step) Set a permissions boundary under **Set permissions boundary** and click **Next**.
7. (Optional step) Add tags to AWS resources.
8. Click **Create User**.
9. Navigate to **Dashboard**, then **Access management**, and then **Users**. The newly created user appears in the list.
10. Select the user in the **Username** column.
11. On the User Info page, select **Create access key** in the **Summary** section.
12. Under **Access key best practices & alternatives**, select the use case according to your requirement, and click **Next**.
13. (Optional step) Provide a description tag, if required, and click **Next**.
    The Access key-created message appears. The access key and secret access key are displayed.

14. Copy the access key ID and secret key.

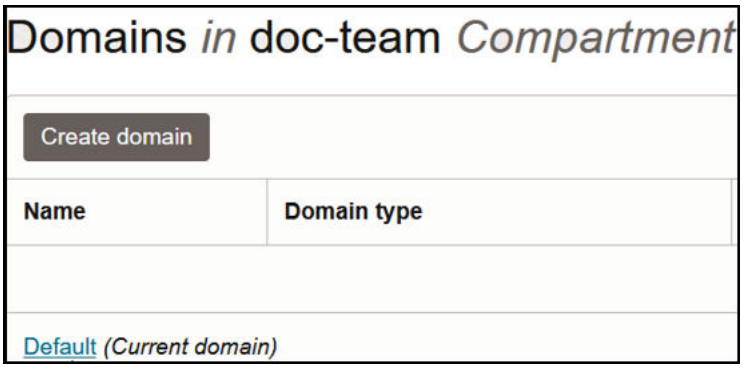
> **Note**
>
> You must enter the access key in the **Access Key** field and the secret key in the **Secret Access Key** field on the Connections page. See Configure Connection Security.

15. Alternatively, you can click **Download .csv file** to download a file that contains the access key ID and the secret key.
16. Click **Done**.

Create the Client Identifier

Access the identity domain in which to create the client application.

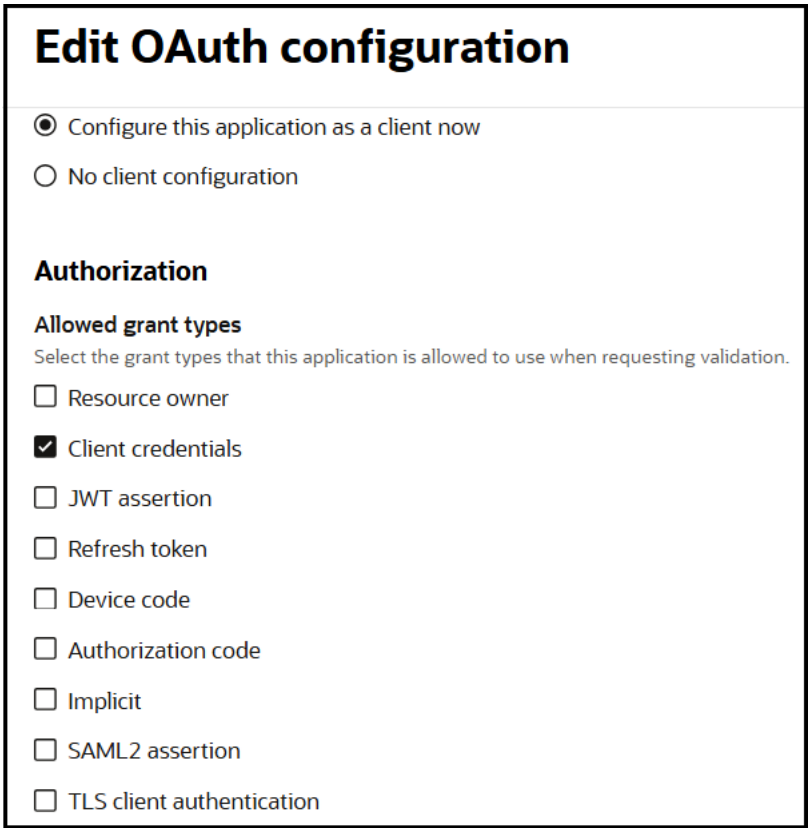
1. Log in to the Oracle Cloud Console with your identity domain administrator credentials.
   a. In the navigation pane, click **Identity & Security**.
   b. Click **Domains**.
   c. Select your compartment.
   d. Click the identity domain.



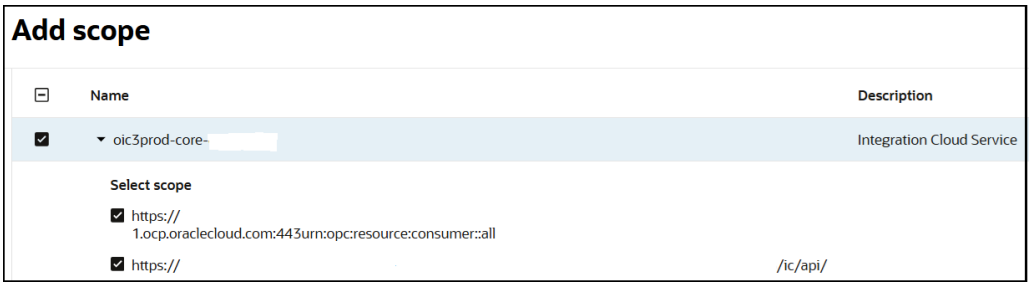
   e. In the navigation pane, click **Integrated applications**.
   This is the location at which you create the client application for your grant type.

Configure the Client Application

1. Click **Add application**.
2. Select **Confidential Application**, then click **Launch workflow**.
3. Enter a name. The remaining fields on this page are optional and can be ignored.
4. Click **Submit**.
5. Click the **OAuth configuration** tab, then the **Edit OAuth configuration** subtab.
6. In the **Client configuration** panel, select **Configure this application as a client now**.
7. Select the grant type to use:
   a. For client credentials, select **Client credentials** in the **Allowed grant types** section.



8. Complete the following steps for either grant type:
   a. Leave the **Redirect URL**, **Post-logout redirect URL**, and **Logout URL** fields blank.
   b. For **Client type**, ensure that **Confidential** is selected.
   c. Bypass several fields and scroll down to the **Token issuance policy** section.
   d. Select **Confidential** in the **Authorized resources** section.
   e. Click the **Add Resources** toggle.
   f. Click **Add scope**.
   g. Find and expand the Oracle Integration application for your instance.
   h. Select the two scopes appended with the following details:
      - **urn:opc:resource:consumer::all**
      - **ic/api/**



   i. Click **Add**.

The scopes are displayed in the **Resources** section.

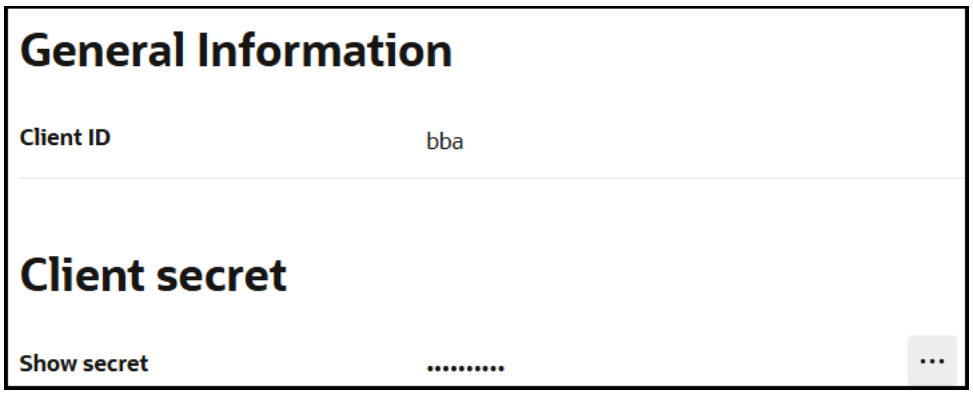
j. Ignore the **Add app roles** check box. This selection is not required.

k. Click **Submit**.

The details page for the client application is displayed.

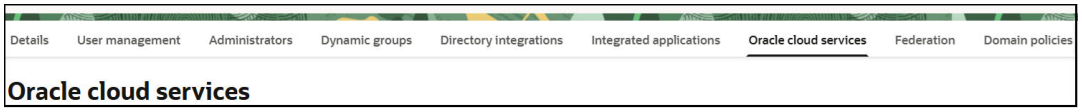
9. From the **Actions** menu at the top, select **Activate**, and then **Activate application** to activate the client application for use.

10. In the **General Information** section, note the client ID and client secret values.



Add Roles to the Client Application

1. In the menu bar, click **Oracle cloud services**.

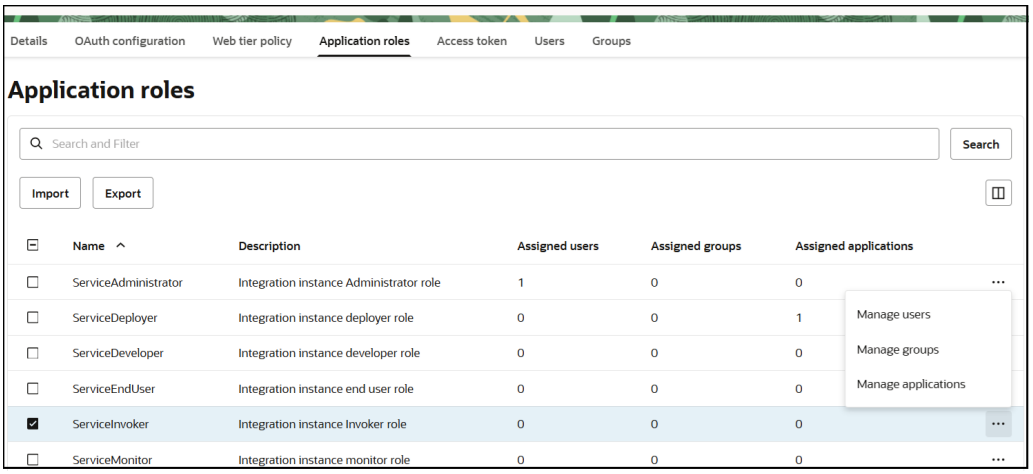


2. Click the specific application corresponding to the Oracle Integration instance.

3. In the menu bar, click **Application roles**.

4. If configuring the client credentials grant type, select the following:

a. Expand **ServiceInvoker**, then click **Actions** ⋮ next to **Assigned applications**.



b. Select to assign users, groups, and applications to the instance application.

Create a Connection

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

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

To create a connection in Oracle Integration:

1. Decide where to start:
   - Work in a project (see why working with projects is preferred).
     a. In the navigation pane, click **Projects**.
     b. Select the project name.
     c. Click **Integrations**.
     d. In the **Connections** section, click **Add** if no connections currently exist or **+** if connections already exist. The Create connection panel opens.
   - Work outside a project.
     a. In the navigation pane, click **Design**, then **Connections**.
     b. Click **Create**. The Create connection panel opens.
2. 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.
3. 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`).

Element	Description
Role	Select the role (direction) in which to use this connection. **Note**: *Only* the roles supported by the adapter you selected are displayed for selection. Some adapters support all role combinations (trigger, invoke, or trigger and invoke). Other adapters support fewer role combinations. 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.

4. Click **Create**.

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

5. Follow the steps to configure a connection.
   The connection property and connection security values are specific to each adapter. Your connection may also require configuration with an access type such as a private endpoint or an agent group.

6. Test the connection.

Configure Connection Properties

Enter connection information so your application can process requests.

1. Go to the **Properties** section.

2. In the **AWS Region** field, enter the region you selected in the AWS Management Console (for example, **ap-south-1**).

Configure Connection Security

Configure security for your Amazon Simple Notification Service (SNS) Adapter connection.

1. Go to the **Security** section.
2. In the **Access Key** field, enter the access key obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection
3. In the **Secret Key** field, enter the secret key obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.
4. In the **AWS Region** field, select the same AWS region that you entered in the **Properties** section. See Configure Connection Properties.

For a trigger connection, you must also provide the client identifier in the additional field configured. See Prerequisites for Creating a Connection. The client ID obtained from the **General Information** section must be entered in the **Client Identifier** field on the Connection page.

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

1. Go to the **Access type** section.
2. 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. a. Click **Associate agent group**. The Associate agent group panel appears. b. 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**.

3

Add the Amazon Simple Notification Service (SNS) Adapter Connection to an Integration

When you drag the Amazon Simple Notification Service (SNS) Adapter into the trigger or invoke area of an integration, the Adapter Endpoint Configuration Wizard is invoked. This wizard guides you through configuration of the Amazon Simple Notification Service (SNS) Adapter endpoint properties.

The following sections describe the wizard pages that guide you through configuration of the Amazon Simple Notification Service (SNS) Adapter as a trigger or an invoke in an integration.

Topics:

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.`

Configuration Page

Configure the trigger or invoke connection.

Trigger Connection

Element	Description
Select Topic Name	Enter the name of the topic to which you want to perform an operation. A topic name is required for creating and confirming a subscription.
Select Format	Select the notification format (that is, **Sample JSON**, **Sample XML**, or **AVRO Schema**). Upon choosing **Sample XML**, the **Enable XML Namespace** field is displayed. Upon selecting **Enable XML Namespace**, the **Enter XML Namespace** option is displayed. You must provide the valid XML namespace. For example: `http://www.oracleawssns.com`
Provide JSON Sample / Provide XML Sample / Provide AVRO Schema	Provide the notification sample.
Enable Decoding	Select this option if the incoming notification is base64-encoded. **Note**: For the **AVRO Schema** selection, **Enable Decoding** is not available.
Configure Message Attributes	Configuring message attributes helps you provide structured metadata items (such as timestamps, geospatial data, signatures, and identifiers) about the message.
Enable Subscription Filter Policy	A subscription filter policy allows you to apply filters based on values provided. The constituent fields are: • Upon selecting **JSON** as the format, you get **Message Attributes** and **Message Body** as the options for **Select Filter Policy Scope**. • Upon selecting **XML** as the format, you get **Message Attribute** as the only option for **Select Filter Policy Scope**. • Provide the JSON body for **Subscription Filter Policy**. • Upon selecting **AVRO Schema** as the format, **Message Attribute** is the only option for **Select Filter Policy Scope**.
Enable Redrive Policy	If there is a failure in the notification being sent to the subscriber, the notification gets stored in the **Dead Letter Queue**. There is a constituent field named **Provide Dead Letter Queue** (provide the SQS queue ARN).
Configure Delivery Policy	Configure the policy that defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. The following are constituent fields: • **Number of Retries** • **Retries without Delay** • **Minimum Delay** • **Maximum Delay** • **Minimum Delay Retries** • **Maximum Delay Retries** • **Maximum Receive Rate** • **Retry Back off Function**

Invoke Connection

Element	Description
Select Topic Name	Enter the name of the topic to which you want to perform an operation. A topic name is required for creating and confirming a subscription.
Do you want to specify message structure?	• Click **Yes** to provide the **JSON Sample**, **XML Sample**, or **AVRO Schema** and publish the message in JSON, XML, or AVRO format. • Click **No** to publish the message in opaque (stream reference) format.
How do you want to specify the message structure?	Select the notification format (that is, either **JSON Sample**, **XML Sample**, or **AVRO Schema**). Upon selecting **XML Sample**, the **Enable XML Namespace** field is displayed. Upon selecting **Enable XML Namespace**, the **Enter XML Namespace** option is displayed. You must provide the valid XML namespace. For example: `http://www.oracleawssns.com`
Provide JSON Sample /XML Sample /AVRO Schema	Provide the notification sample.
Enable Encoding	Select this option for base64-encoding the message to publish. **Note**: For the **AVRO Schema** format, **Enable Encoding** is not available.
Configure Message Attributes	Configuring message attributes helps you provide structured metadata items (such as timestamps, geospatial data, signatures, and identifiers) about the message.
Opaque (Stream Reference)	Publishes the files belonging to any format through the specified topic. **Note**: The message published in the topic is Base64-encoded, with the file size not exceeding 256 KB.

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 Amazon Simple Notification Service (SNS) Adapter

You can use the Amazon Simple Notification Service (SNS) Adapter to implement the following common pattern.

Topics:

Create a Product in Shopify by Subscribing to an SNS Topic

This use case describes how a product is automatically created in Shopify whenever an Amazon SNS topic is subscribed. When a message is published to the topic through an API or application, the integration workflow is initiated. The workflow maps the message data and invokes the Shopify API to create the product.

The following adapters and their operations are used in this use case.

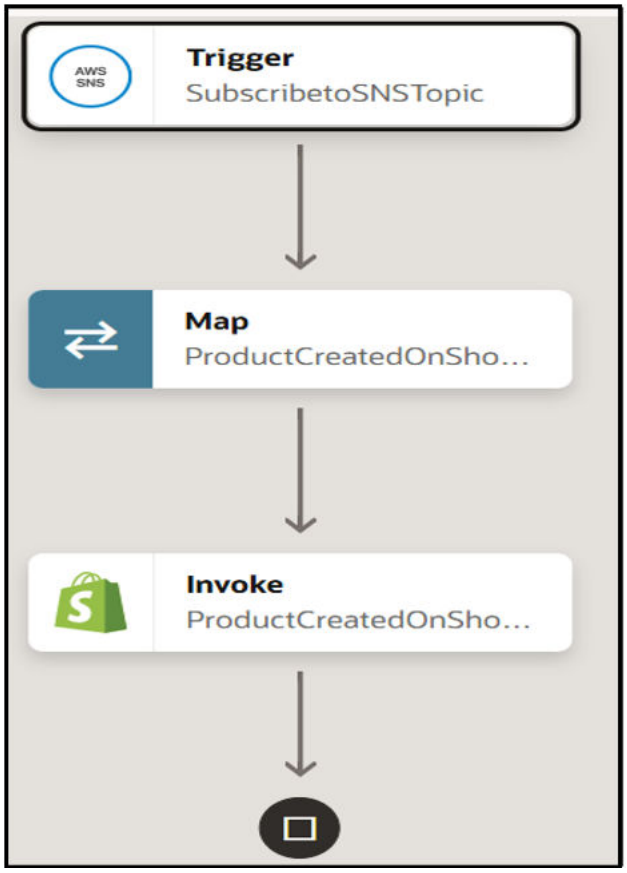
- Amazon Simple Notification Service (SNS) Adapter (configured as a trigger connection): Triggers the integration by subscribing to an SNS topic.
- Shopify Adapter (configured as an invoke connection): Invokes the Shopify API to create a new product.

This implementation pattern provides an overview of the steps.

1. Create an Amazon Simple Notification Service (SNS) Adapter trigger connection and Shopify Adapter invoke connection.
2. Create an application integration.
3. Drag the Amazon Simple Notification Service (SNS) Adapter into the integration canvas as a trigger connection.
4. Configure the Amazon Simple Notification Service (SNS) Adapter endpoint as follows:
    a. On the Basic Info page, provide a meaningful name.
    b. On the Configuration Page, select the topic on which you want to receive the message.
    c. Select the message format and provide a message sample.
    d. Select **Enable decoding** only if you have specified the message format as JSON or XML.
    e. Select **Enable Subscription Filter Policy**.
    f. Select **Enable Redrive Policy**.
    g. If necessary, select **Configure Message Attributes** and **Configure Delivery Policy**.
    h. On the Summary Page, review and confirm your selections.

5. Drag the Shopify Adapter into the integration canvas as an invoke connection.
6. Configure the Shopify Adapter endpoint as follows:
   a. On the Basic Info page, provide a meaningful name.
   b. On the Actions page, select **Create** as the action.
   c. On the Operations page, select **Product** as the **Module** and **Create Product** as the **Operation**.
   d. On the Summary Page, review and confirm your selections.
7. In the mapper, map the SNS message body to the Shopify product fields.
8. Once complete, activate the integration.

   The completed integration looks as follows:



Once activated, the integration is automatically triggered whenever a message is published to the configured SNS topic through an API or application. The subscribed integration processes the message and creates a new product in Shopify.