User Guide | V0 Import Journal Entries | Amazon S3/Oracle Financials Cloud (ERP Cloud)

1. Introduction

a. Purpose

This document describes setting up an integration flow where a file from a cloud Amazon S3 location is downloaded to the Oracle Integration Cloud, processed and sent to the Oracle Financials Cloud (ERP Cloud). This is a scheduled orchestration.

Then the application driven orchestration comes, where a log file is uploaded in the Oracle Integration Cloud, processed and uploaded back in the Amazon S3 location.

This flow is a combination of scheduled and application driven orchestrations.

It makes use of a standard REST and Oracle ERP Cloud adapters in Oracle Integration Cloud.

b. Audience

This document is written for Oracle Financials Cloud (Oracle ERP Cloud) and Amazon S3 administrators who are configuring the integration between these two systems. Readers of this document should have experience with both.

This document describes only how to configure integrations of these two systems. For information about other configurations please see related documentation.

c. Prerequisites

This part describes the prerequisites for a successful integration.

Required Versions: A successful integration requires the following versions (or higher) of these products:

- Oracle Integration Cloud: 19.3.1.0.0 (190624.1100.29532)

- Oracle ERP Cloud: 19A (11.13.19.01.0)
- Amazon S3

Access Rights: To configure integration, you need to access three systems with required privileges:

- Oracle Integration Cloud Service, which enables you to map the attributes between Oracle Financials Cloud (Oracle ERP Cloud) and a cloud Amazon S3 location.
- Oracle Financials Cloud (Oracle ERP Cloud), which enables you to configure receiving requests from an Invoke and to configure endpoint to send data from ERP to a Trigger.

  Note: for ERP required privileges please see: https://docs.oracle.com/en/cloud/paas/integration-cloud/erp-adapter/prerequisites-creating-connection.html#GUID-B861559A-DECE-4F7B-82CA-AA48263CA159
- Amazon S3, which enables you to configure receiving requests from an Invoke.

Assumptions: this integration makes the following functional assumptions:

- It is assumed that user name is the same for Oracle ERP Cloud and for Oracle Integration Cloud
- It is assumed Amazon S3 is configured and accessible (see part 4 of this User Guide)
    - you have an IAM user created - you need to store the keys for later connection setup
    - you have a bucket and a file created

d. Architectural Overview

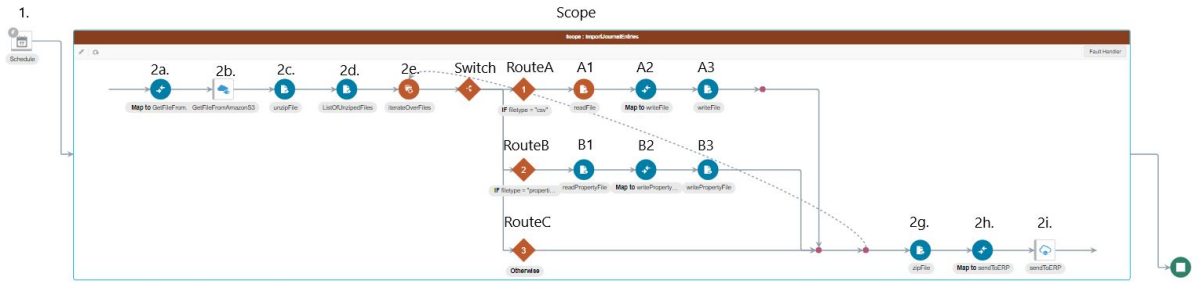
This integration is between the Oracle Financials Cloud (Oracle ERP Cloud) and a cloud Amazon S3 infrastructure.

The message flow of business data goes from Amazon S3 through Oracle Integration Cloud to Oracle Financial Cloud (Oracle ERP Cloud) and back to the cloud Amazon S3 location.

Oracle Financials Cloud uses Oracle ERP Cloud adapter.

Amazon S3 uses REST adapter for the Invoke.

Integration Scheme for a Scheduled Orchestration Part:



Integration Scheme Steps for a Scheduled Orchestration Part:

1. Schedule containing parameters: emailTo, filename, bucketName.
2. Scope:

   2a. Mapping: mapping to get a file from Amazon S3,

   2b. Invoke Amazon S3: getting a file from Amazon S3,

   2c. Stage File:

   Operation: Unzip,

   2d.Stage File:

   Operation: List Files,

   2e. For Each:

   Repeating Element: ICS File

   Current Element Name: ICS File,

   2f. Switch:

   RouteA: file type = CSV:

   A1: Stage File:

   Operation: Read

   Segmentation: Enabled,

   A2: Mapping: mapping to write a file,

   A3: Stage File:

   Operation: Write,

   RouteB: file type = properties:

B1: Stage File:

Operation: Read

Segmentation: Disabled,

B2: Mapping: mapping to write a property file,

B3: Stage File:

Operation: Write,

RouteC: otherwise,

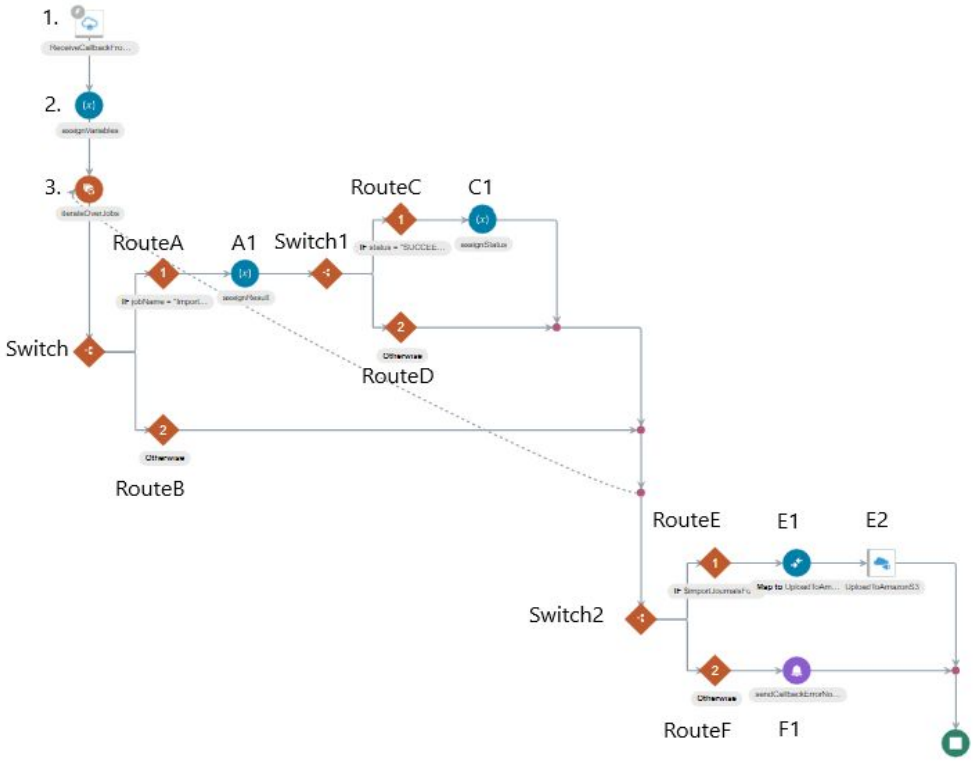
2g. Stage File:

Operation: Zip,

2h. Mapping: mapping to send files to ERP,

2i. Invoke Oracle ERP Cloud: sending files to ERP.

Integration Scheme for Import Journal Callback AmazonS3 - an Application Driven Orchestration: Integration Scheme Steps for Import Journal Callback - an Application Driven Orchestration:



Integration Scheme Steps for Import Journal Callback AmazonS3 - an Application Driven Orchestration:

1. Trigger Oracle ERP Cloud: receiving callback from ERP.
2. Assign variables: assigning values to the following variables: importJournalsFound, importJournalsSuccess, bucketName.

   Note: These are pre-set.
3. For Each:

   Repeating Elements: jobs,

   Current Element Name: job.
4. Switch:

   RouteA: Job Name = Import Journals.

   A1: Assign variables: assigning value to the following variable: importJournalsFound.

   Note: This value is pre-set.

   RouteB: otherwise.
5. Switch1:

   RouteC: Import Journals process succeeded

   C1: Assign: assigning value to importJournalsSuccess

   RouteD: otherwise
6. Switch2:

   RouteE: Import Journals process succeeded and Import Journals Found

   E1: Mapping: mapping to upload a log file to Amazon S3

   E2: Invoke Amazon S3: uploading a log file to Amazon S3

   RouteF: otherwise

   F1: Import journal callback integration flow error notification

e. Features

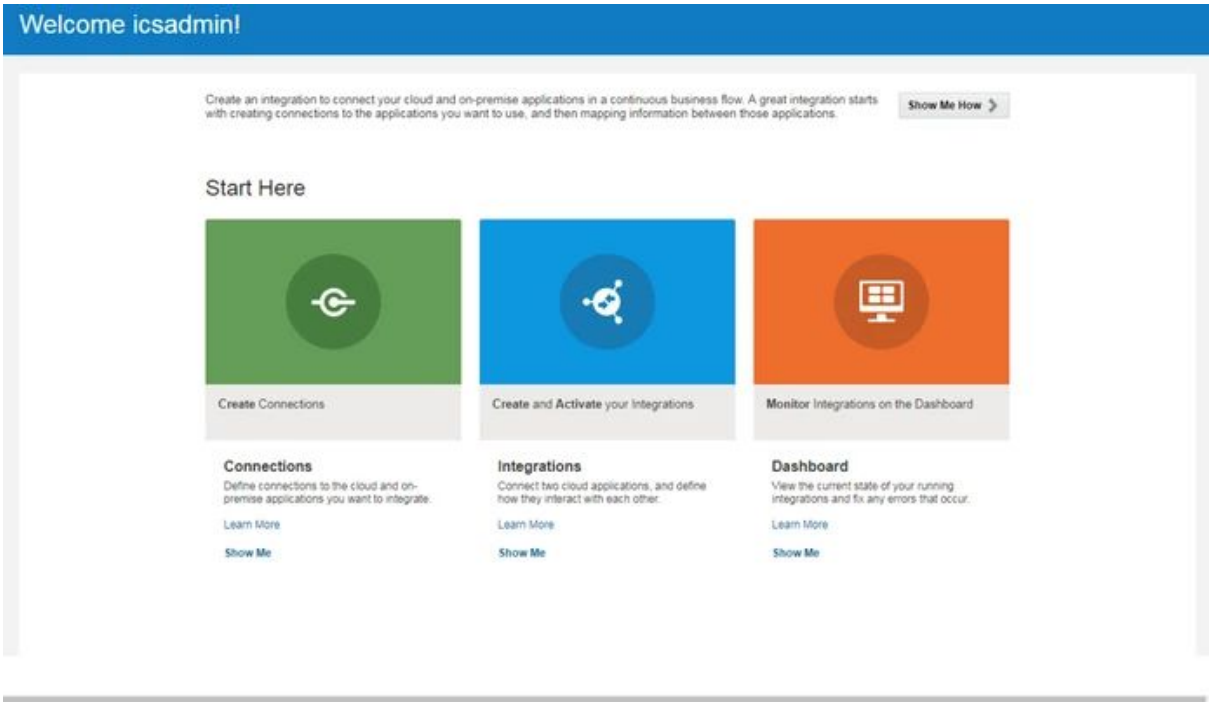
This product is a ready-made integration between Oracle Financials Cloud (Oracle ERP Cloud) and Amazon S3. It is easily installed and requires minimal configuration.

2. Configuring connections

For the integration to work properly, you need to configure connections for the applications among which you want to share data.

1. **Download** the Integration package from Oracle Marketplace to your local disk.

2. **Log in** to your OIC service as an admin user and open the “Integrations” page.



3. On the top right, click Import, then select “.iar”. Click **Import** to import the archive to your OIC from your local disk, as shown below.

4. Once imported you will see the integration flow created.

You must **configure the connections** for the Oracle Financials Cloud (ERP Cloud) - a Trigger and an Invoke and an Invoke for your Amazon S3. To do this, follow these steps:

a. Amazon Invoke Connection:

a. **Log in** your account at the Oracle Integration Cloud Service home page using a valid user name and password and click **Connections**.

b. Find the appropriate connection. **Open** it.

c. Fill in the email address in the **Connection Administrator.** (You can receive email notifications when problems or changes occur in this connection. Enter the email address to receive these notifications.).

d. Configure **Connection Properties:** Click **Configure Connectivity** to specify information to connect to your application/endpoint and process requests.

- In **Connection Type** select: **REST API Base URL**
- In **Connection URL** enter**:**
    - http://s3.**yourAWSRegion**.amazonaws.com

Click **OK**.

e. Configure Connection **Security**: Click **Configure Security** to specify the login credentials to access your application/endpoint.

- **Security Policy** select: AWS Signature Version 4
- **Secret Key:** you will get the key when creating an IAM user in Amazon S3 (see Assumptions)
- **Confirm Secret Key:** confirm your Secret Key

- **AWS region:** select your AWS region
- **Service Name:** select Amazon Simple Storage Service (Amazon S3)

Click **OK**.

f. Click **Save**.

g. Click **Test** to see whether the connection is working properly.

If **successful**, the progress indicator shows 100%.

If your connection was **unsuccessful**, an **error message** is displayed with details.

Verify that the configuration details you entered are correct.

h. When complete, click **Save,** then click **Close.**

b. Oracle ERP Cloud Trigger/Invoke Connection:

a. **Log in** your account at the Oracle Integration Cloud Service home page using a valid user name and password and click **Connections**.

b. Find the appropriate connection. **Open** it.

c. Fill in the email address in the **Connection Administrator.** (You can receive email notifications when problems or changes occur in this connection. Enter the email address to receive these notifications.).

d. Configure **Connection Properties**: Click **Configure Connectivity** (on the right hand side of Connection Properties) -> Enter information for

- **ERP Services Catalog WSDL URL**:

  https://<**yourERPinstance>**/fscmService/ServiceCatalogService?WSDL

- **ERP Events Catalog URL (optional):**

  https://<**yourERPinstance>**/soa-infra

- **Interface Catalog URL:**

  https://<**yourERPinstance>**/fscmRestApi/otherResources/latest/interfaceCatalogs

e. Configure Connection **Security**: Click **Configure Security** (on the right hand side of Security to specify the login credentials to access your application/endpoint) ->

- **Security Policy**: Select - **Username Password Token**

f. Configure **Security Credentials**:

- **Username**
- **Password**
- **Confirm Password**

Note: these are your **Oracle ERP Cloud** credentials.

g. Click **OK**.

h. Click **Save**.

i. Click **Test:**

If **successful**, the progress indicator shows 100%.

If your connection was **unsuccessful**, an **error message** is displayed with details.

Verify that the configuration details you entered are correct.

j. When complete, click **Save,** then click **Close.**

3. Configuring Oracle Financials Cloud (ERP Cloud) for the Integration

Financials Cloud (ERP Cloud) Trigger/Invoke system at your ERP instance:

- There is no need to configure Oracle Financials Cloud (ERP Cloud) for this integration flow.

4. Configuring Amazon S3 for the Integration

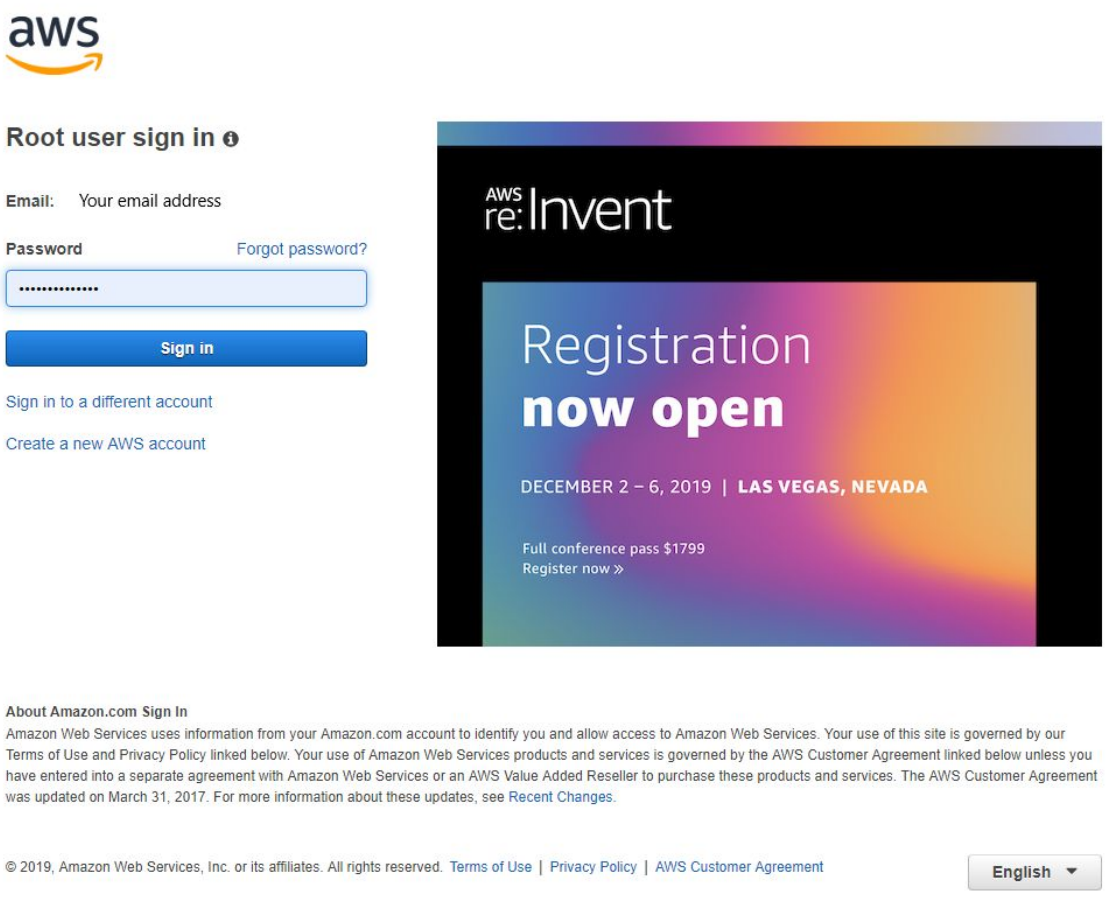
Amazon S3 Invoke System:

a. Setting up an **IAM User**:

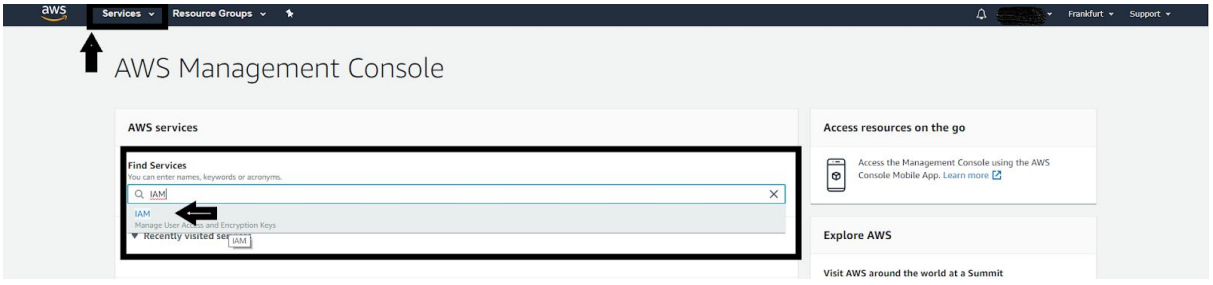
Note: There are two ways of setting up the IAM User -

A:

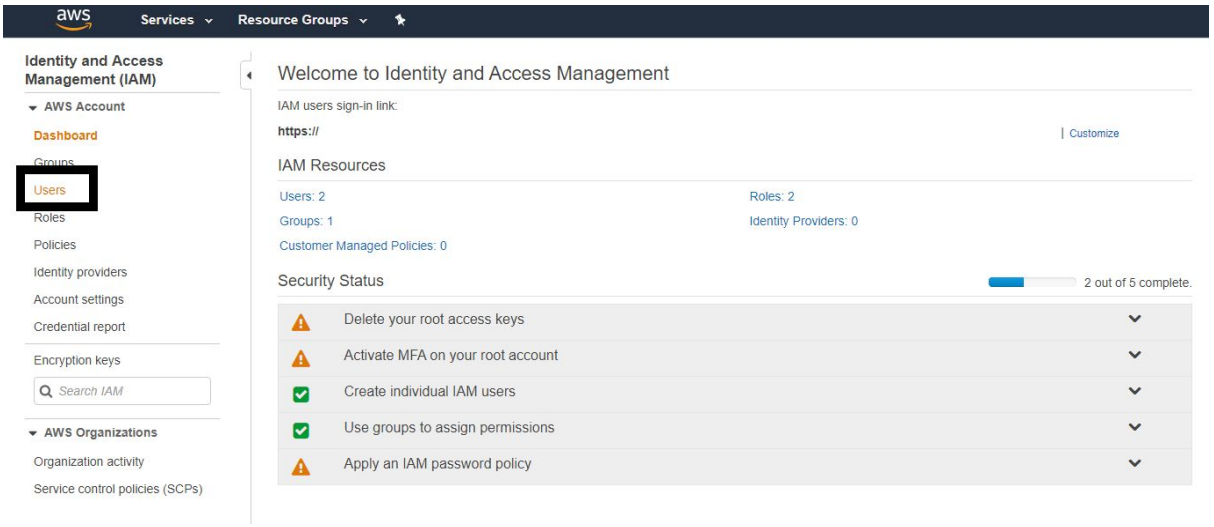
- **Log in** your Amazon S3 account using a valid user name and password.



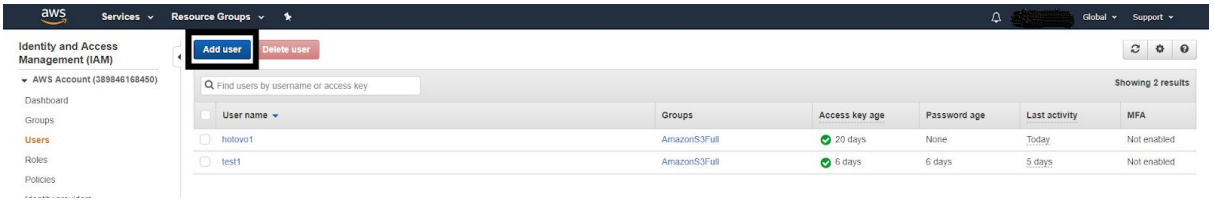
- Select **Services**. In the search bar at the top write **IAM** and select it from the list.



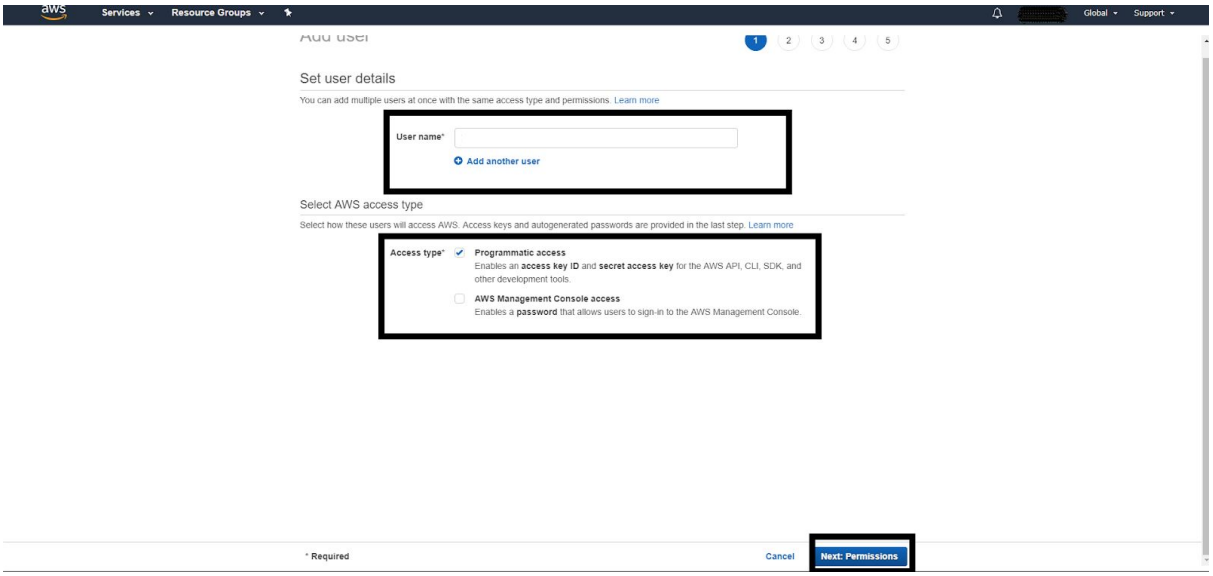
- Select **Users** from the list on the left hand side and click on it.



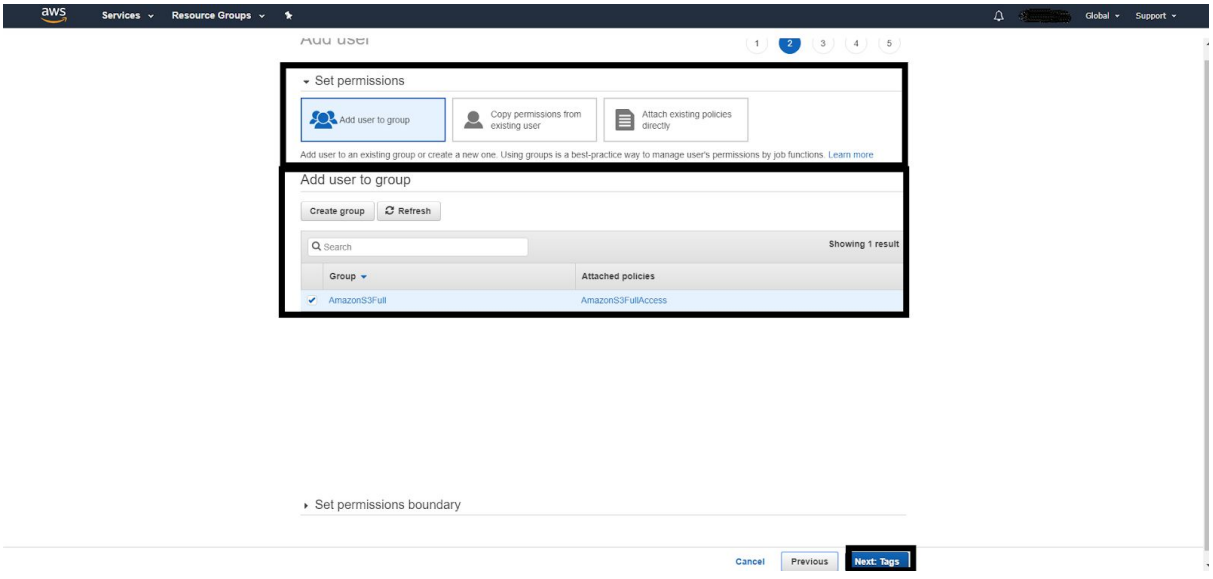
- Click on **Add user**.



- Set **user details**:
    - User name
    - Access Type - select Programmatic Access
    - Click Next.

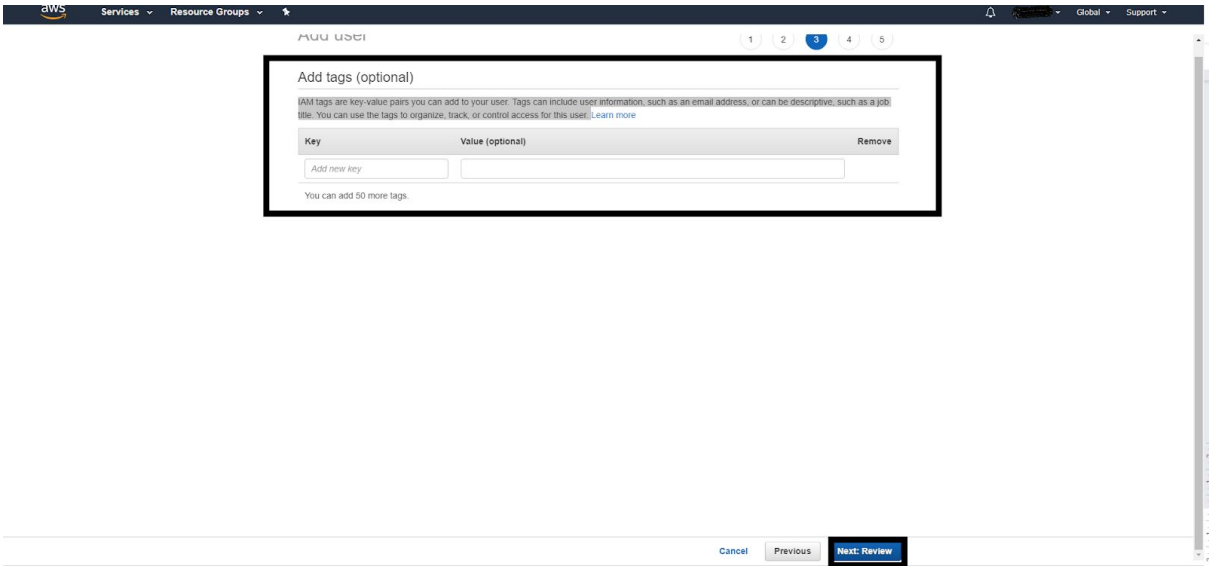


- Set **user permissions**:
    - Select from:
        - Add user to a group,
        - Copy permissions from existing user, or
        - Attach existing policies directly
    - Select, or create Group
    - Click Next.

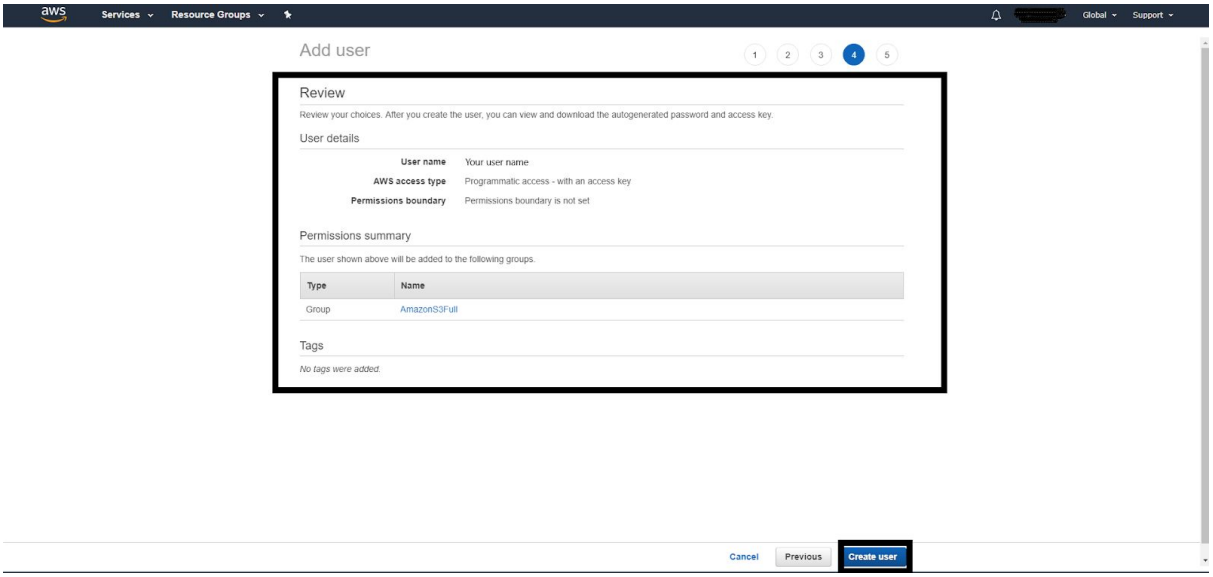


- **Add Tags** - this is optional (IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user.)

- Click Next.

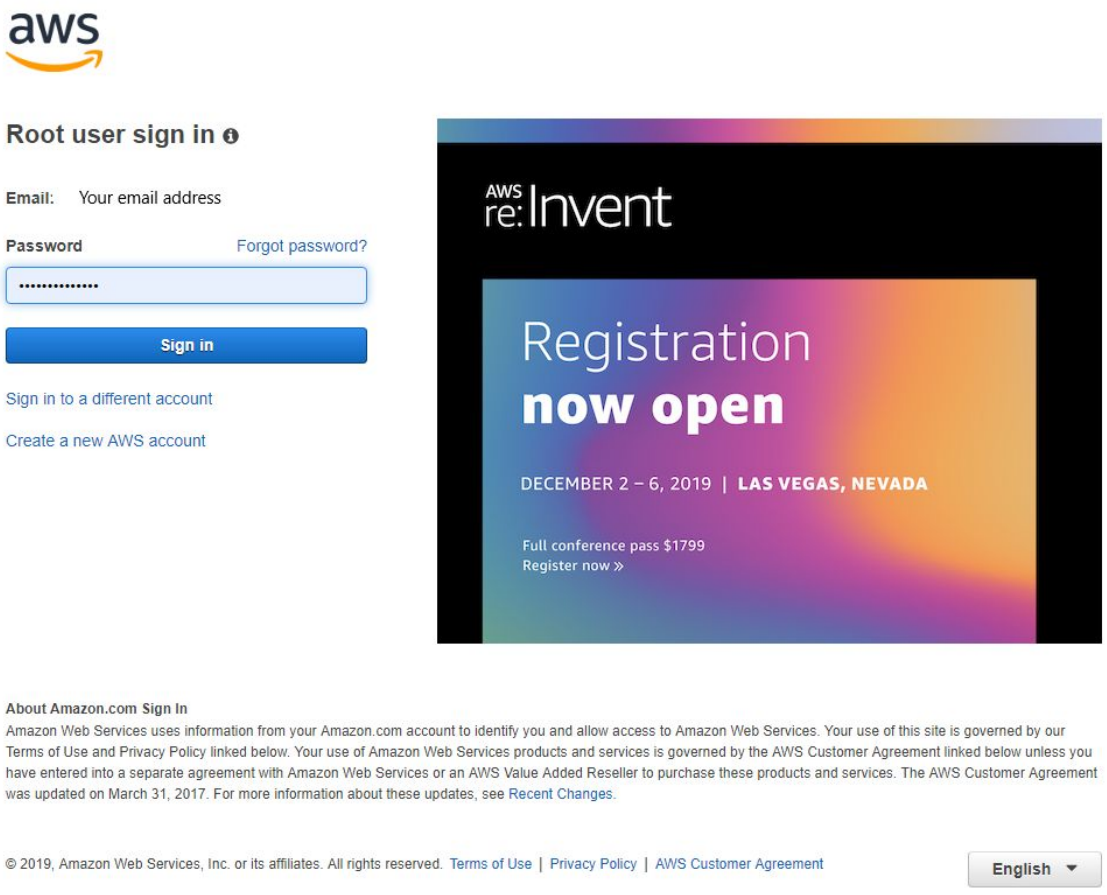


- Check the review page and click **Create user**.

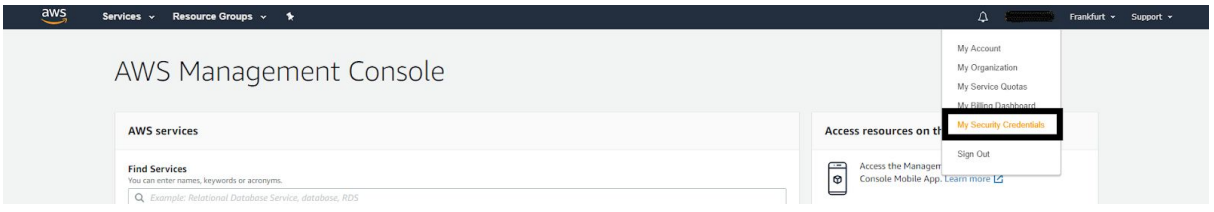


B.

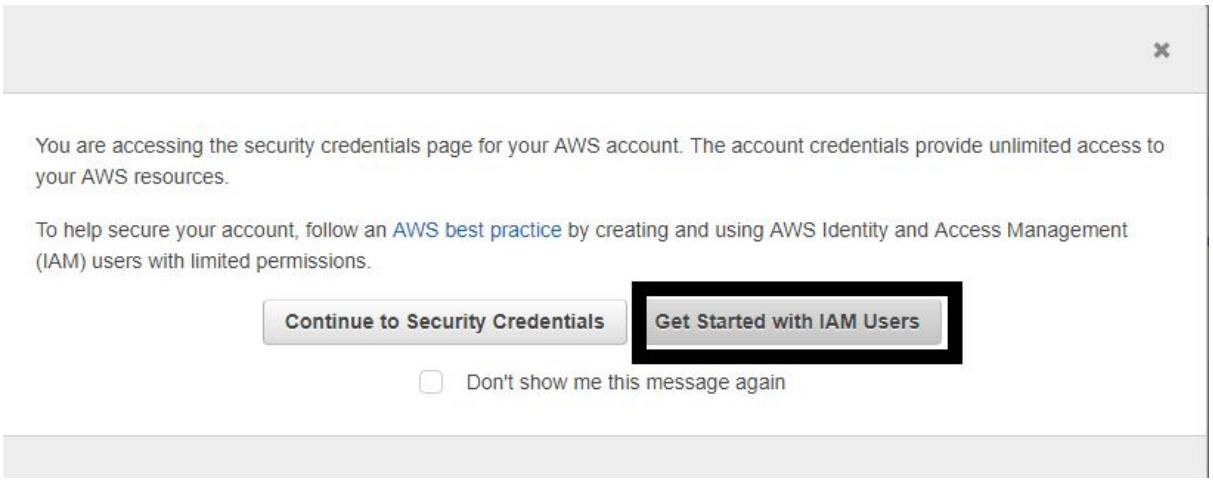
- **Log in** your Amazon S3 account using a valid user name and password.



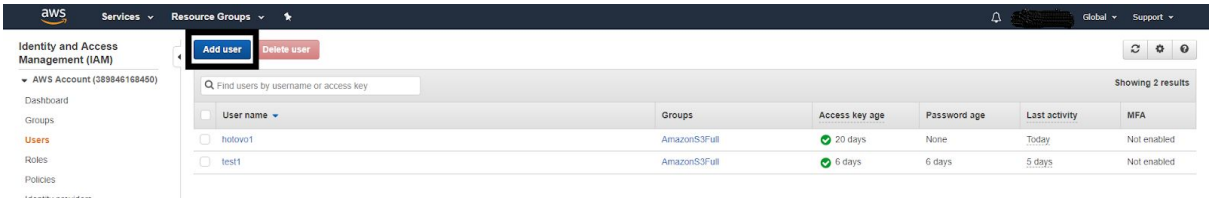
- Click on a little arrow next to your account name and select **My Security Credentials.**



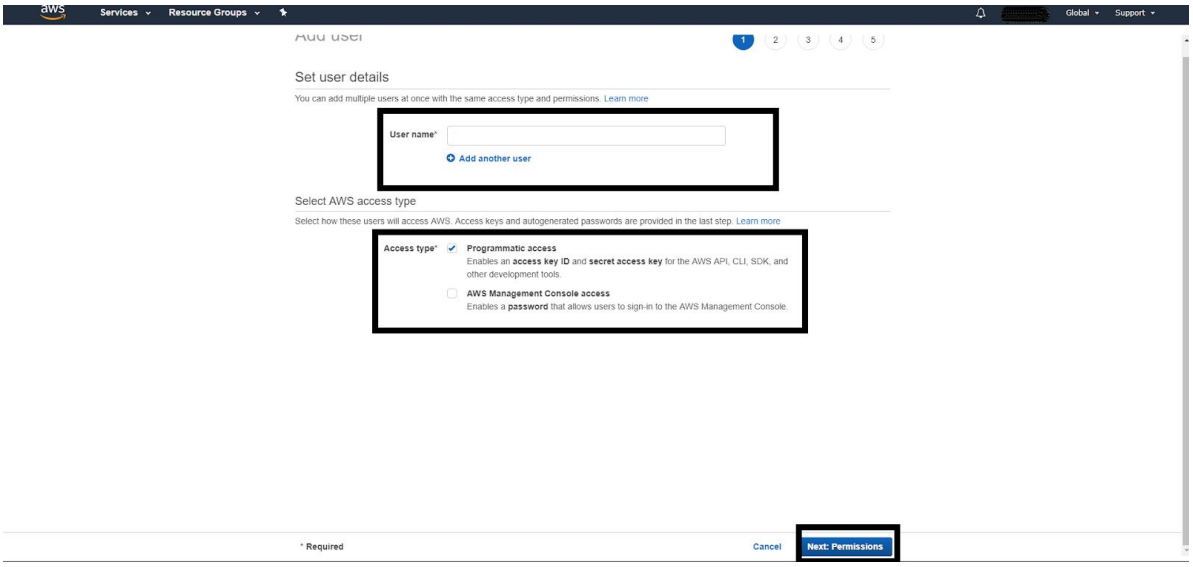
- In the modal window select **Get Started with AIM Users**.



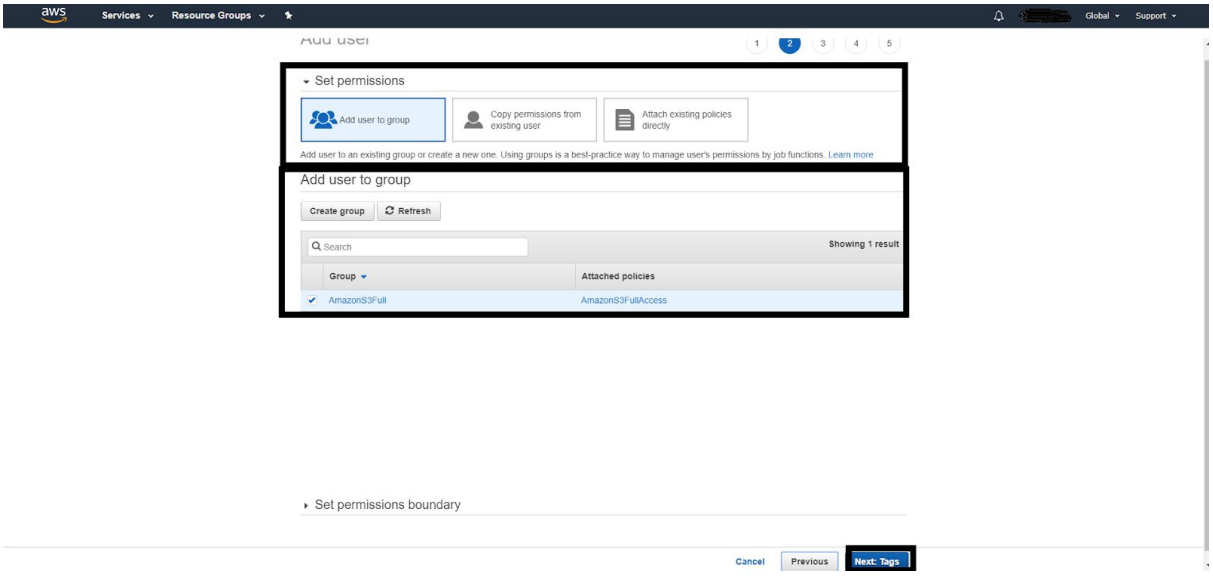
- Click on **Add user**.



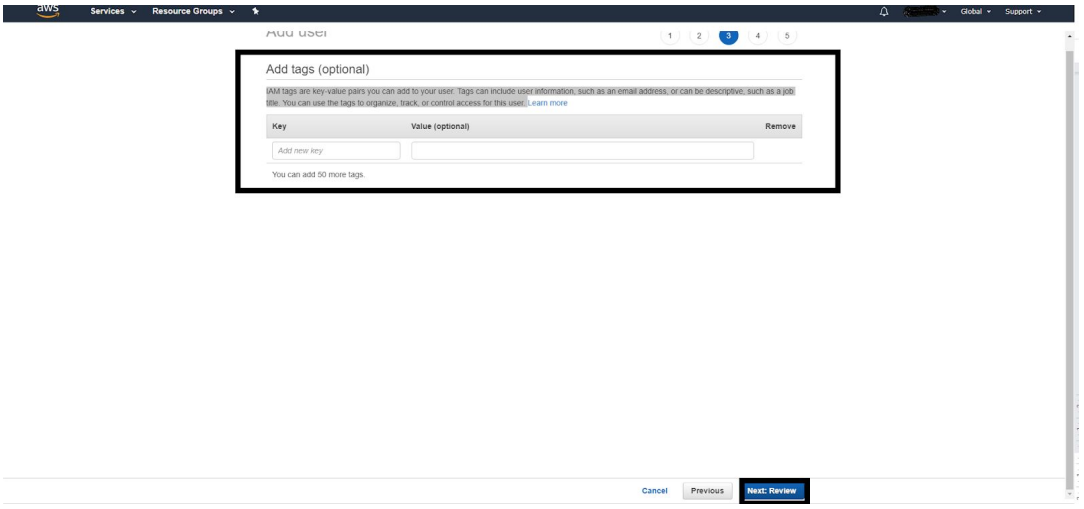
- Set **user details**:
    - User name
    - Access Type - select Programmatic Access
    - Click Next.



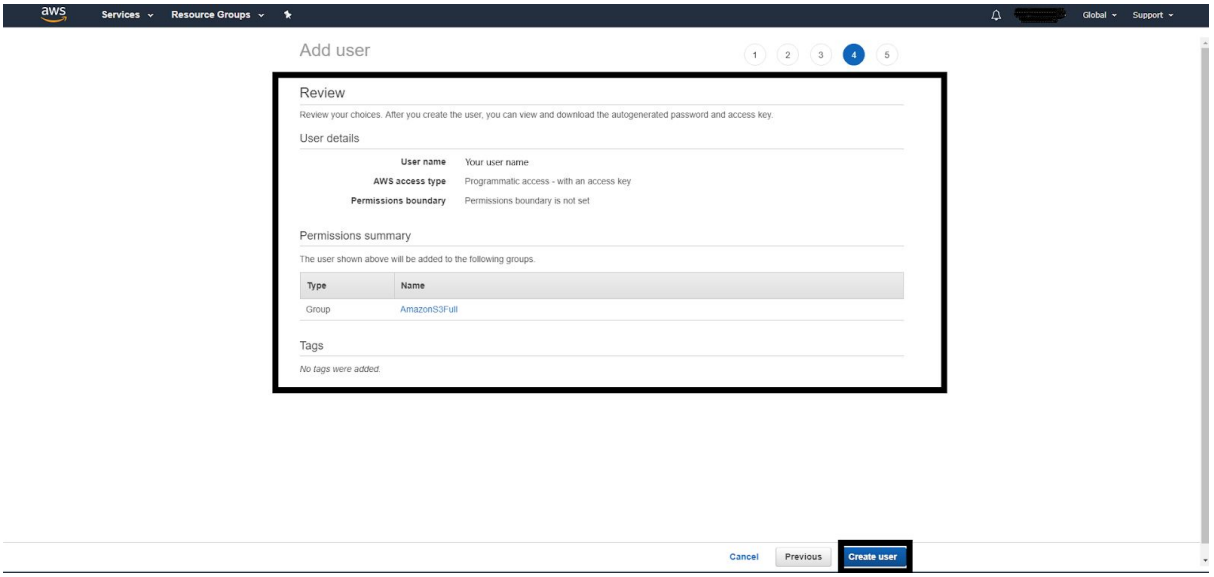
- Set **user permissions**:
    - Select from:
        - Add user to a group,
        - Copy permissions from existing user, or
        - Attach existing policies directly
    - Select, or create Group
    - Click Next.



- **Add Tags** - this is optional (IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user.)
    - Click Next.

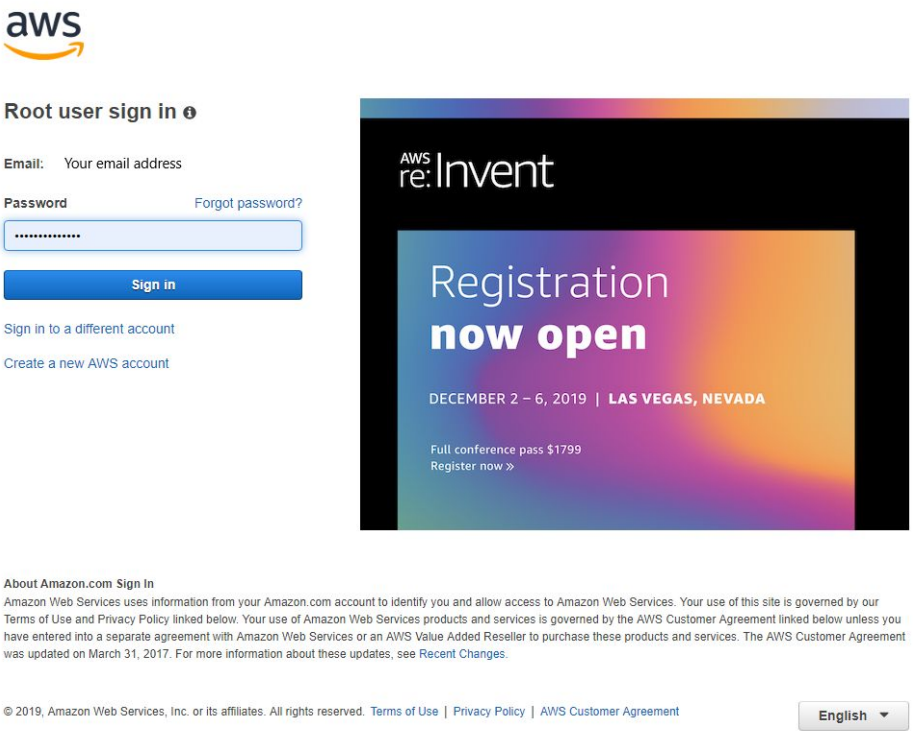


- Check the review and click **Create user**.

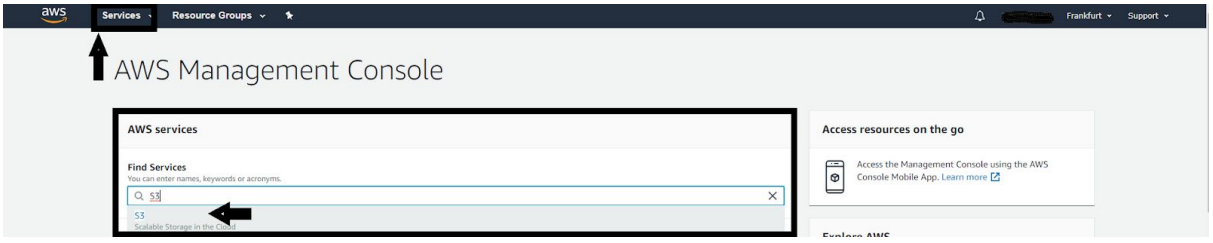


b. Setting up **Bucket**:

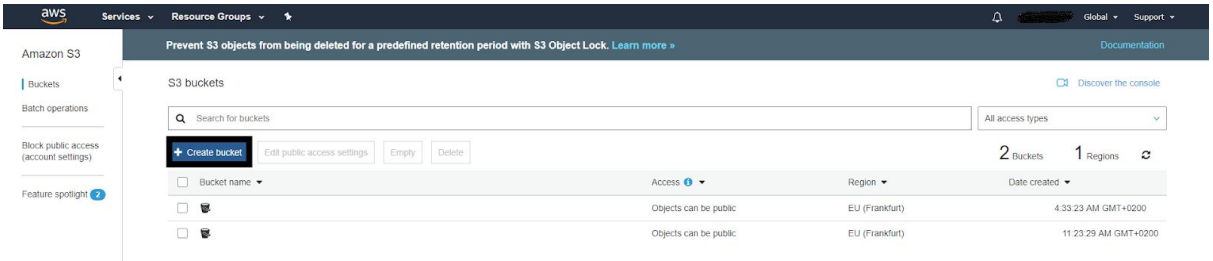
- **Log in** your Amazon S3 account using a valid user name and password.



- Select **Services**, write **S3** in the search bar at the top and select it from the list.

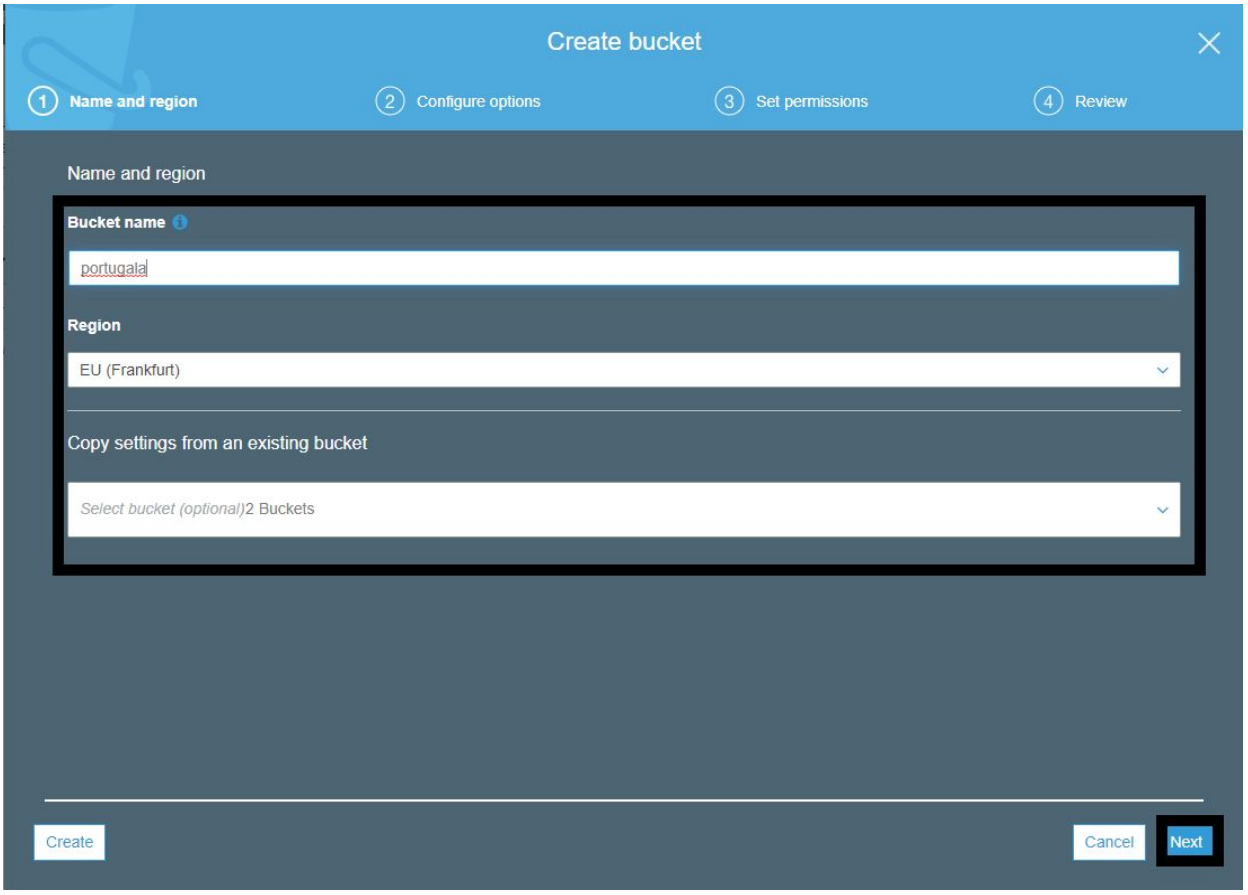


- Select **Create bucket**.



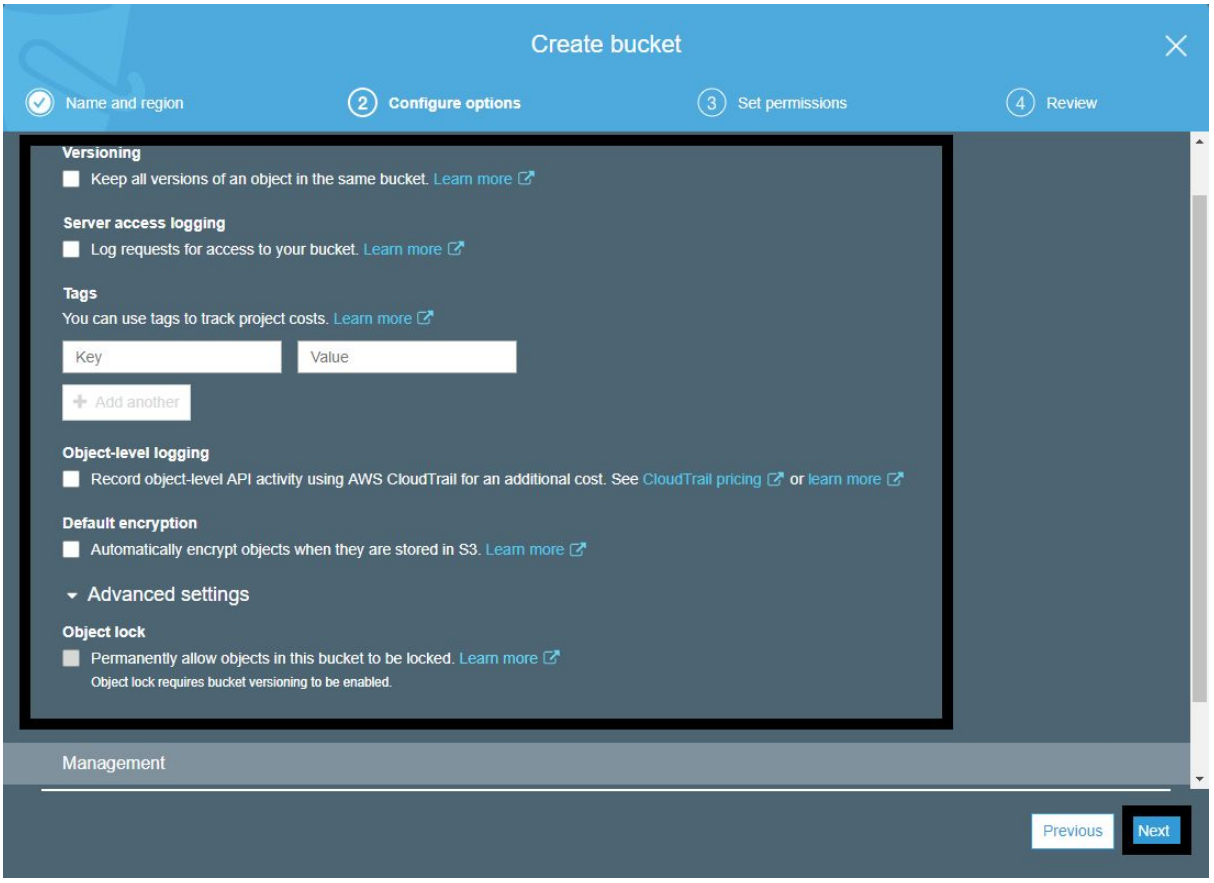
- Set **Name and Region**:
    - Bucket Name (Enter DNC complaint bucket name).

      Note: The bucket name must be unique across all existing bucket names in Amazon S3. Bucket used as an origin point for Amazon Cloudfront distribution have specific restrictions.
    - Region (select your region).
    - Select to copy settings from an existing bucket (optional).
    - Click Next.

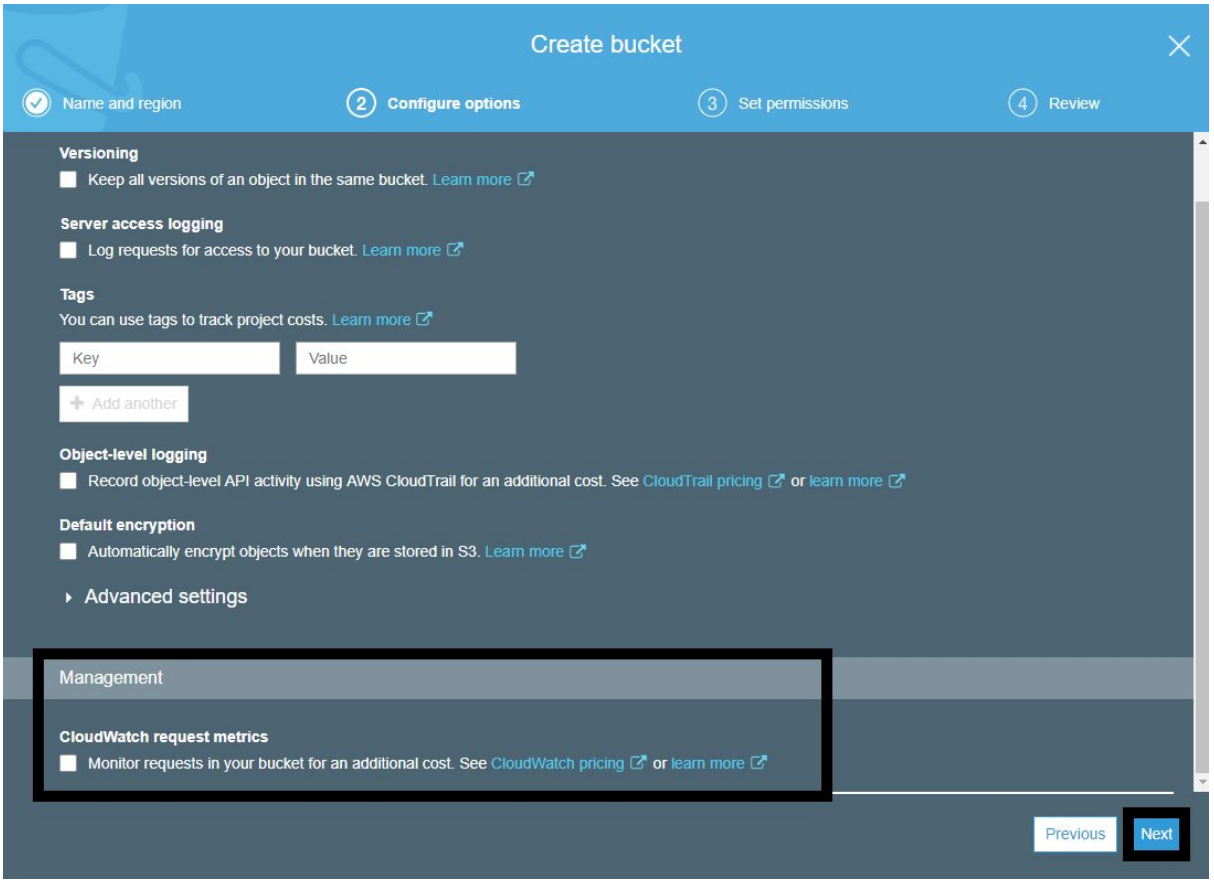


- **Configure options**:
    - Select/unselect Versioning (Keep all versions of an object in the same bucket).
    - Select/unselect Server access logging (Log requests for access to your bucket).

- Enter Tags (You can use tags to track project costs).
- Select/unselect Object-level logging (Record object-level API activity using AWS CloudTrail for an additional cost).
- Select/unselect default encryption (Automatically encrypt objects when they are stored in S3).
- You can choose to configure Advanced Settings by clicking on it, where you can:
    - Select/unselect Object look (Permanently allow objects in this bucket to be locked). Note: Object lock requires bucket versioning to be enabled.



- Select/unselect CloudWatch request metrics (Monitor requests in your bucket for an additional cost).
- Click Next.



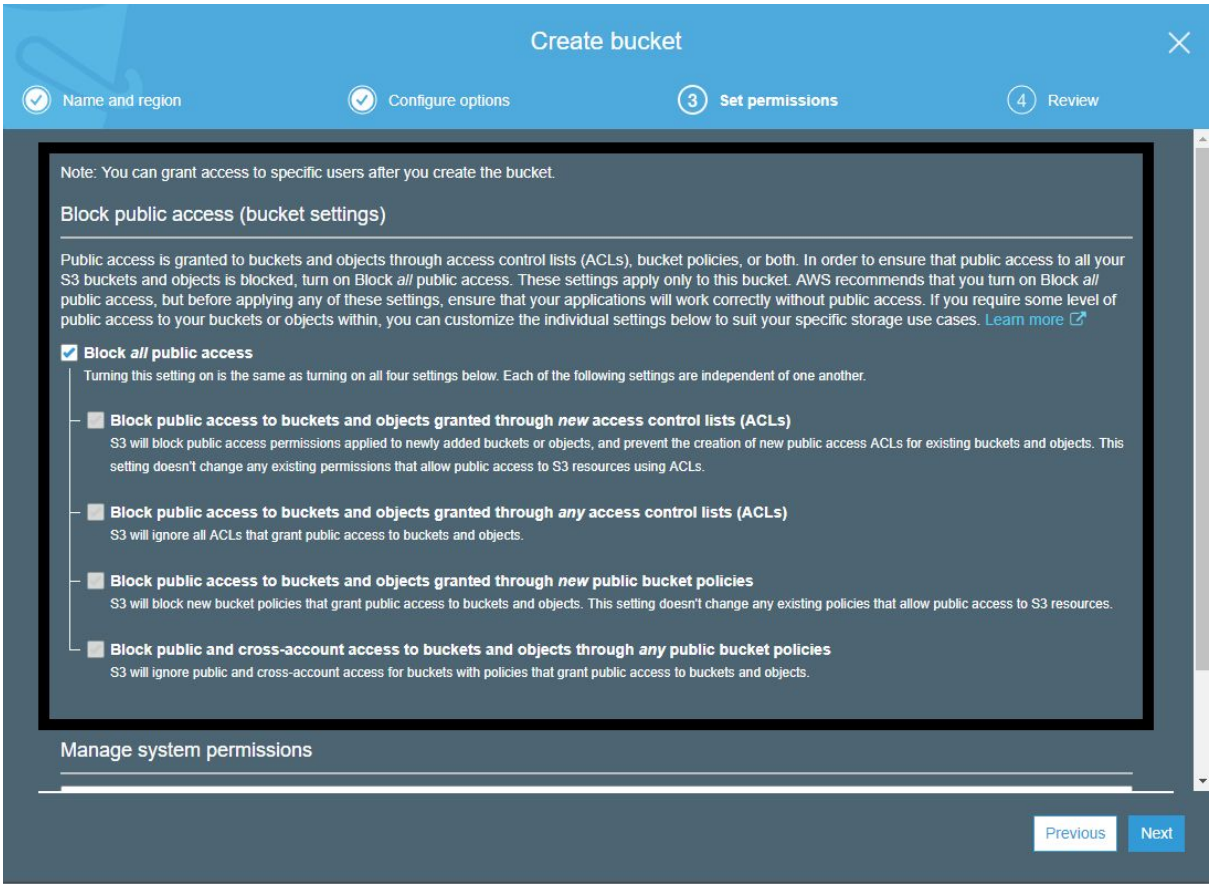
- Set **permissions**:

  Note: You can grant access to specific users after you create the bucket.

  - Configure Block public access (bucket settings):
  - Select/unselect:
    - **Block *all* public access** Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another
      - **Block public access to buckets and objects granted through *new* access control lists (ACLs)** S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
      - **Block public access to buckets and objects granted through *any* access control lists (ACLs)** S3 will ignore all ACLs that grant public access to buckets and objects.
      - **Block public access to buckets and objects granted through *new* public bucket policies** S3 will block new bucket policies that grant public access to buckets and

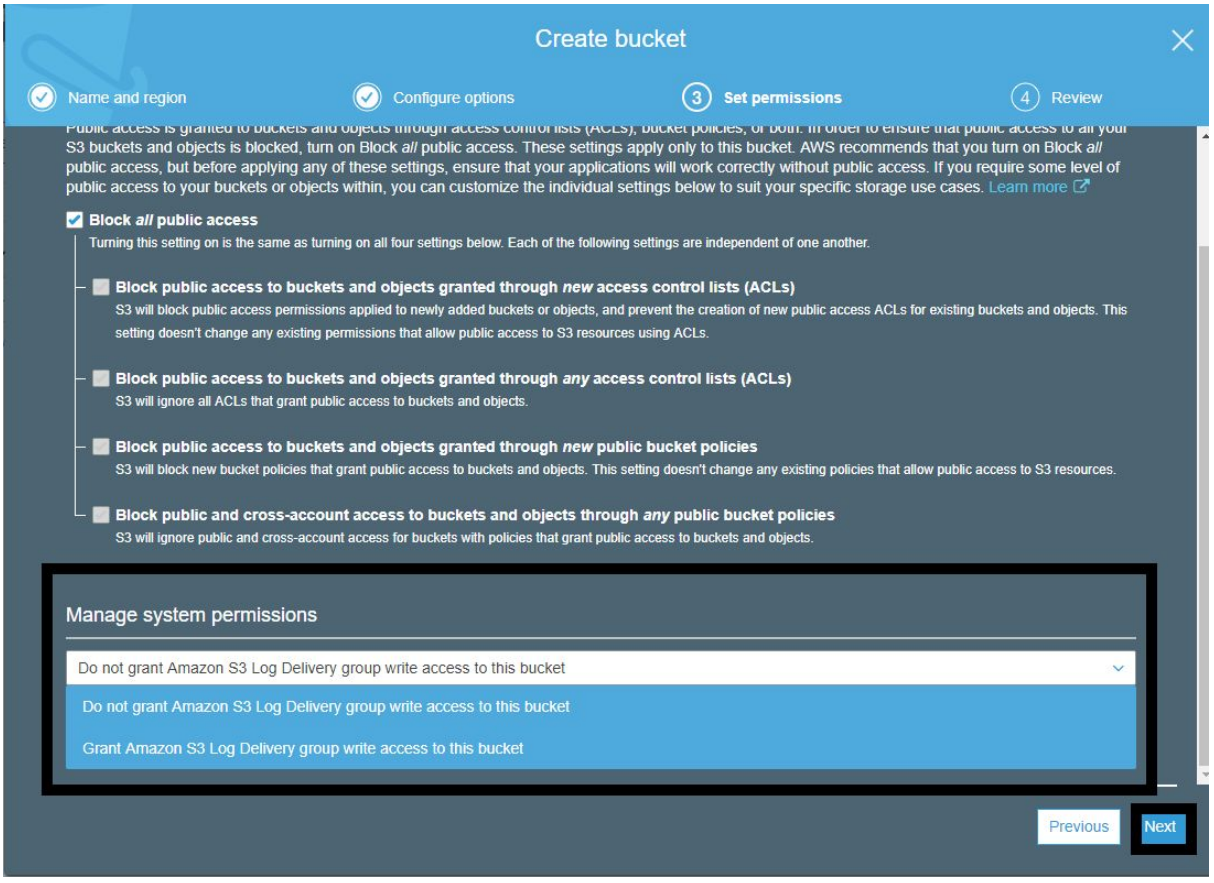
objects. This setting doesn't change any existing policies that allow public access to S3 resources.

- **Block public and cross-account access to buckets and objects through *any* public bucket policies** S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.



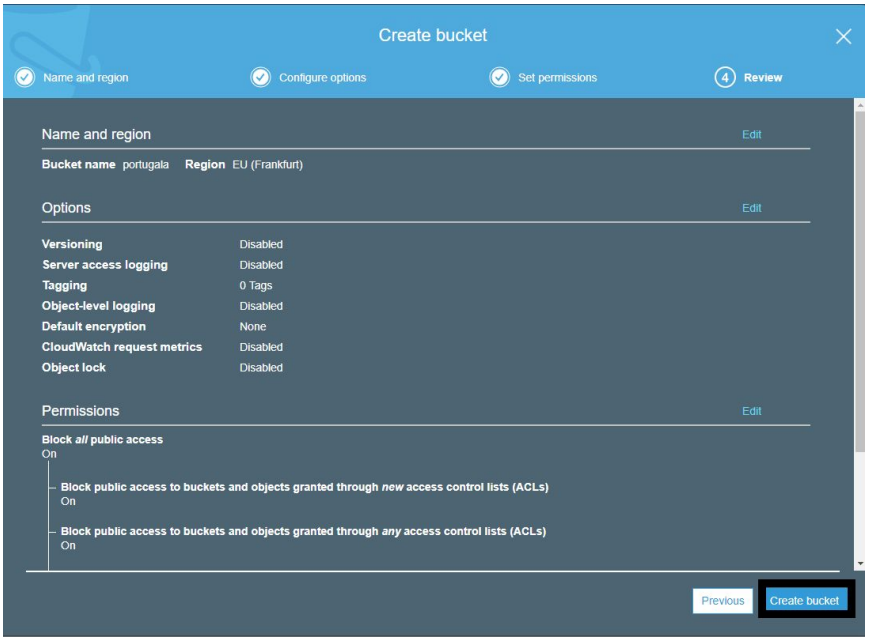
- Select from Manage system permissions:
    - Do not grant Amazon S3 Log Delivery group write access to this bucket, or
    - Grant Amazon S3 Log Delivery group write access to this bucket

- Click Next.



- Check the final Review page and click **Create Bucket.**

  Note: You can still edit your preferences at this step by clicking on Edit links on the right hand side.



5. Configuring Integration

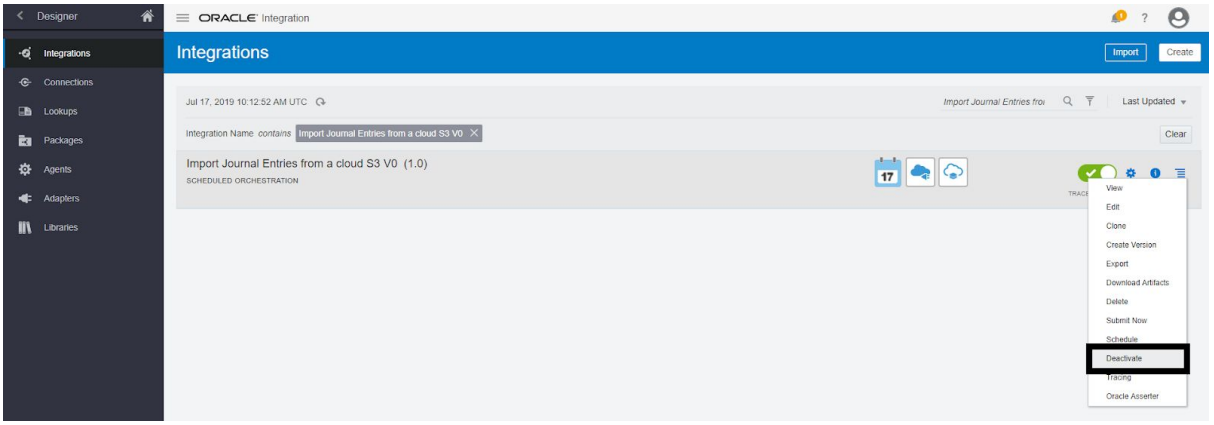
A. For the integration to work properly, you need to configure the following **parameters: bucketName, emailTo, filename** where they refer to:

- **bucketName**: this is a folder in Amazon S3, where the file with data and property file are downloaded from and uploaded to,
- **emailTo**: an email address, where all the notifications go should anything wrong happen within the integration process,
- **filename**: select a file name under which you will see this file in the Amazon S3,

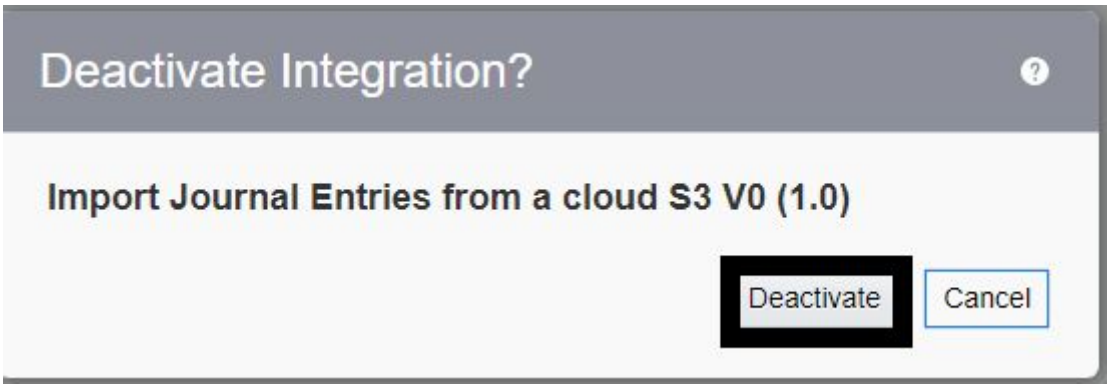
Note: Scheduled parameters are available across all scheduled runs of an integration and can be used to facilitate processing of data from one run to the next. For example, when performing batch processing a schedule parameter can be used to track the current position of batched data between runs.

1. **Log in** to your OIC service as an admin user and open the “Integrations” page.
2. Select **Import Journal Entries from a cloud S3 V0 (1.0).**

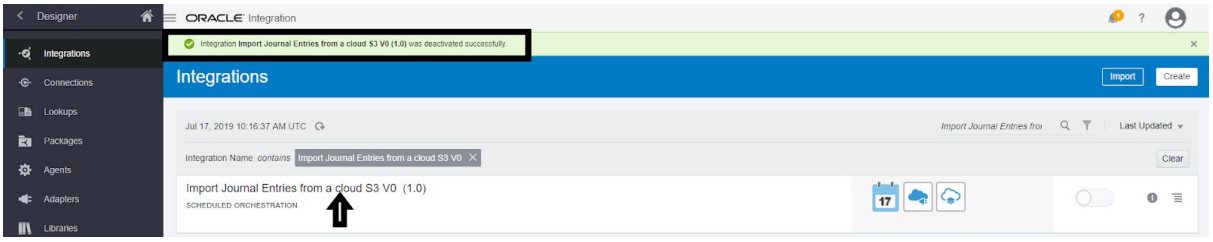
   Note: To configure the integration it must be deactivated.
3. To deactivate the integration from the menu bars on the right select **Deactivate**.



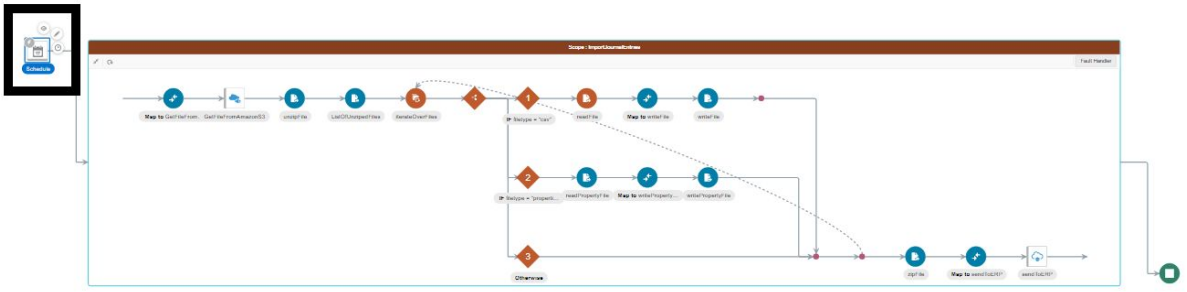
4. Deactivation window appears - select **Deactivate.**



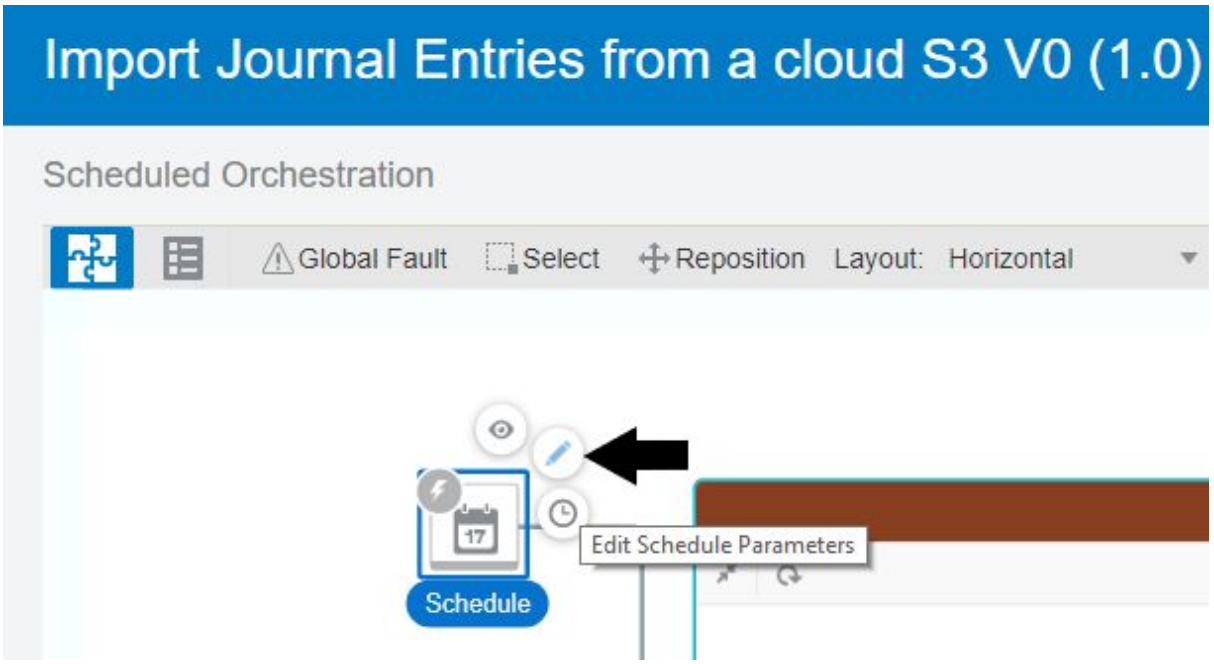
5. When the integration is deactivated, the **confirmation** note appears. Click on the flow name to open it.



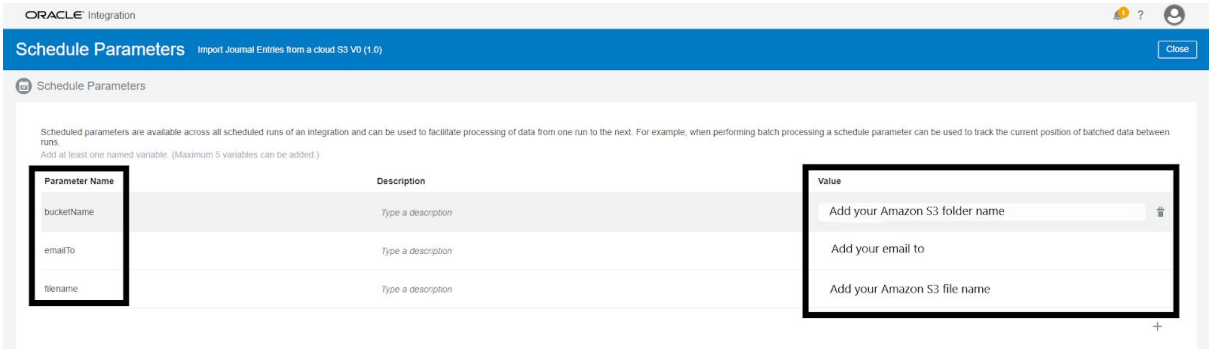
6. When it is opened select **Schedule** section.



7. Three little icons appear next to it - select a **pencil** icon for editing.



8. You will see the schedule parameters page, where in the value column click on the line for editing and adding values for the following parameters: bucketName, emailTo, filename. When done, click **Close** and **Save**.



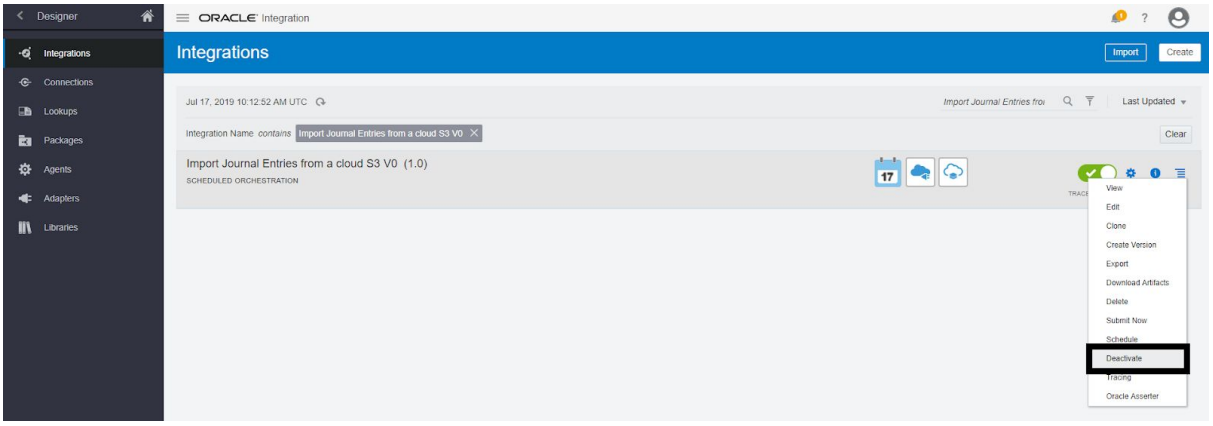
B. To set up the **schedule**, please follow these steps (Note: there are 3 possibilities to do so):

B1: Setting the Schedule via Integration

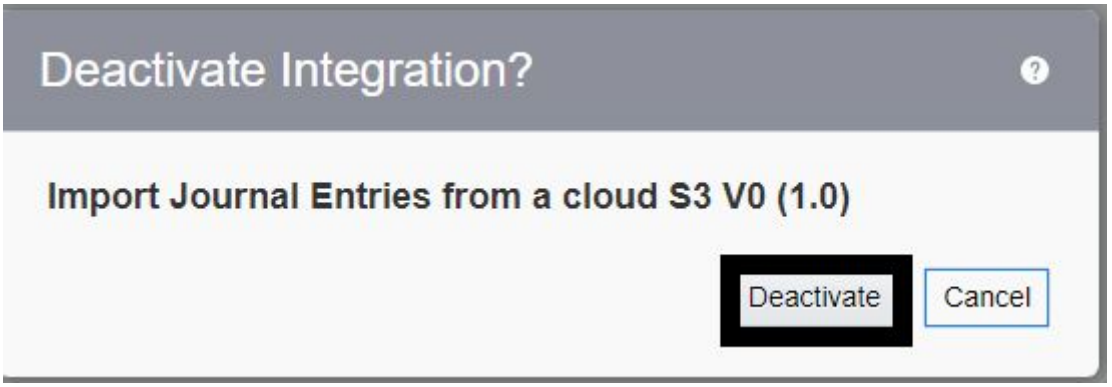
- **Log in** to your OIC service as an admin user and open the “Integrations” page.
- Select **Import Journal Entries from a cloud S3 V0 (1.0).**

Note: To configure the integration it must be deactivated.

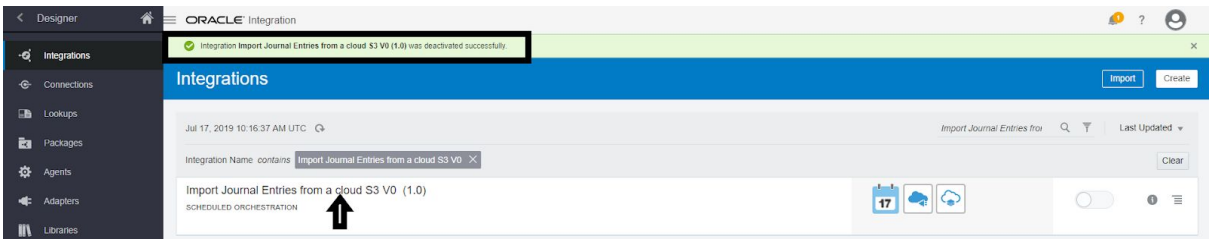
- To deactivate the integration from the menu bars on the right select **Deactivate**.



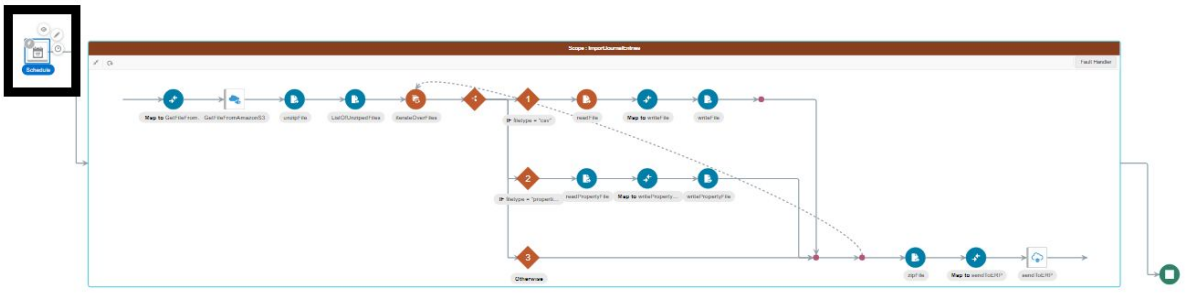
- Deactivation window appears - select **Deactivate.**



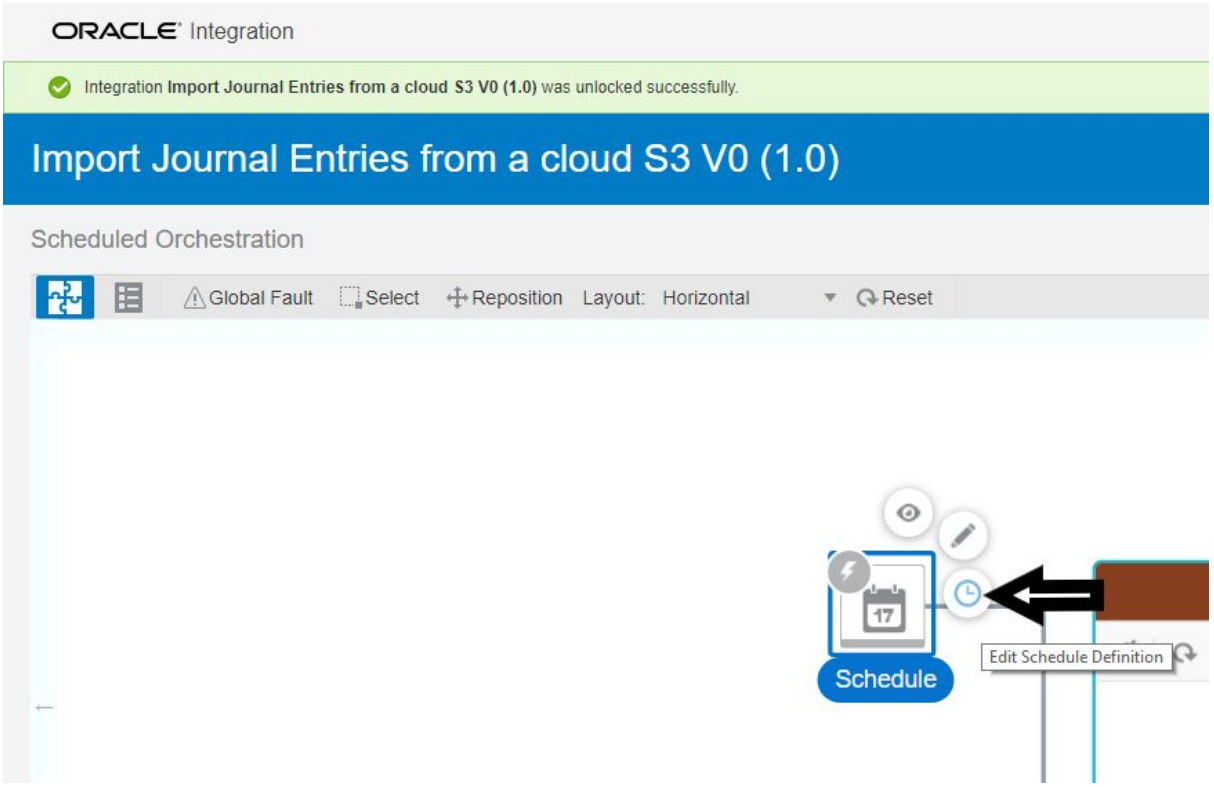
- When the integration is deactivated, the **confirmation** note appears. Click on the flow name to open it.



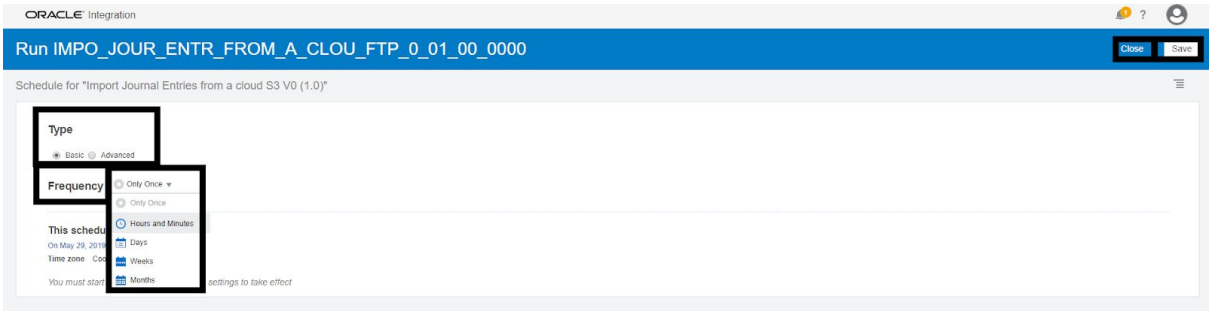
- When it is opened select **Schedule** section.

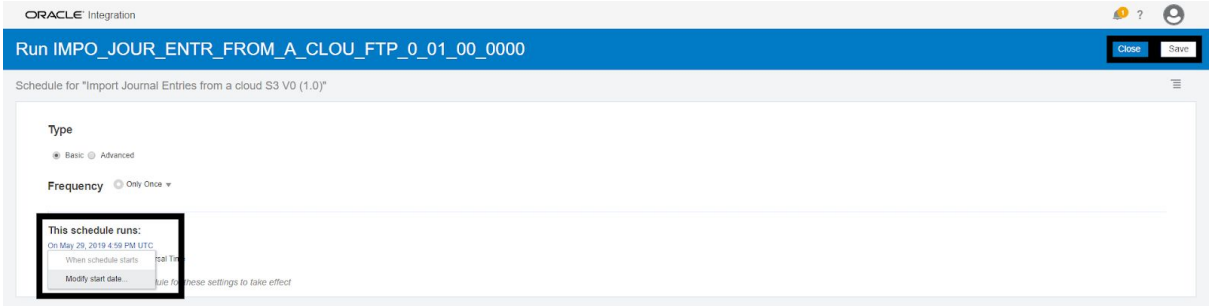


- Three little icons appear next to it - select a **clock** icon for editing.



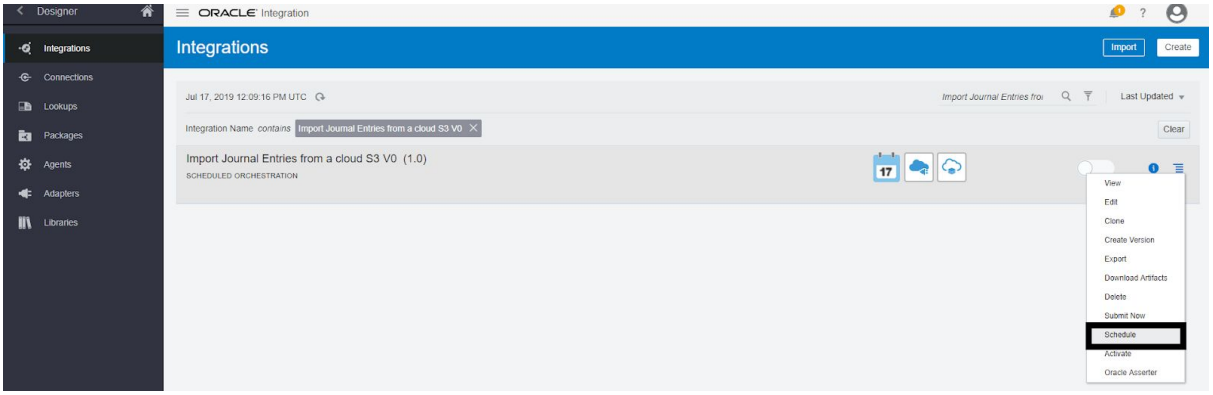
- Select **Type, Frequency** and **Scheduler Start Date** and click **Save** and **Close.**



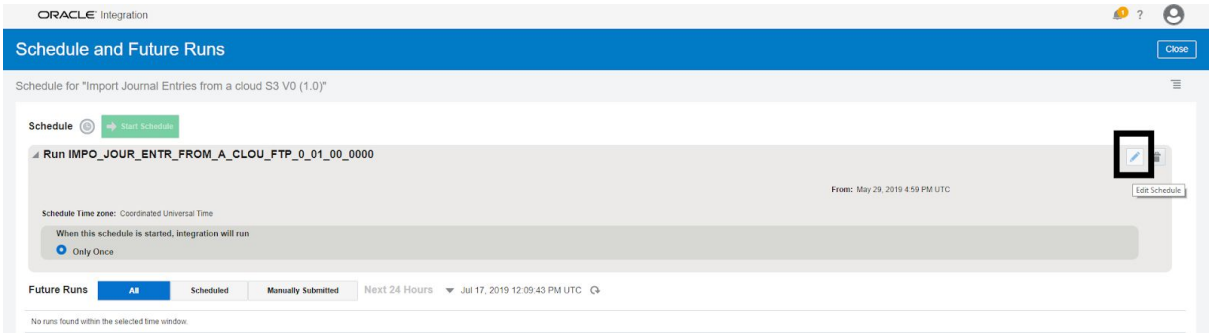


B2: Setting the schedule via the Actions bar:

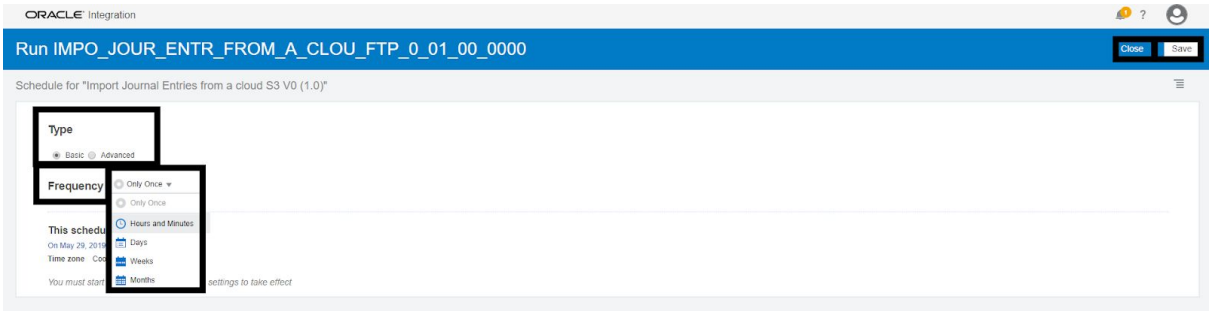
- On the integration page from the Actions bar select **Schedule** and click on it.

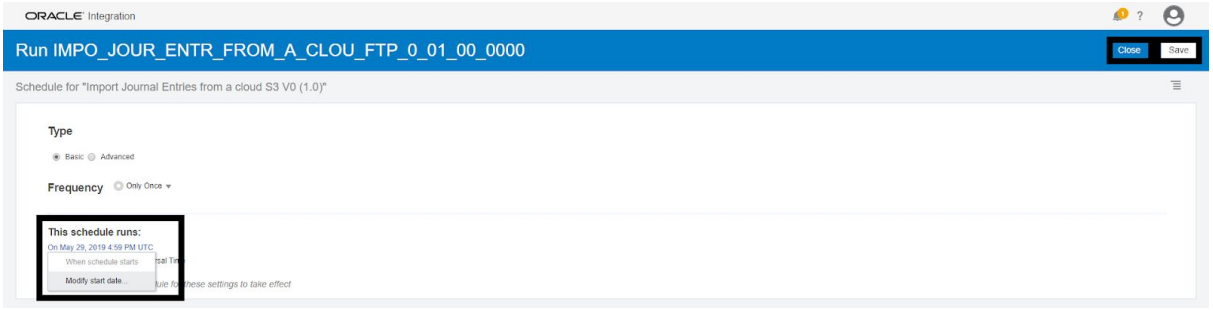


- Click on the little pencil icon on the top right hand side for editing.



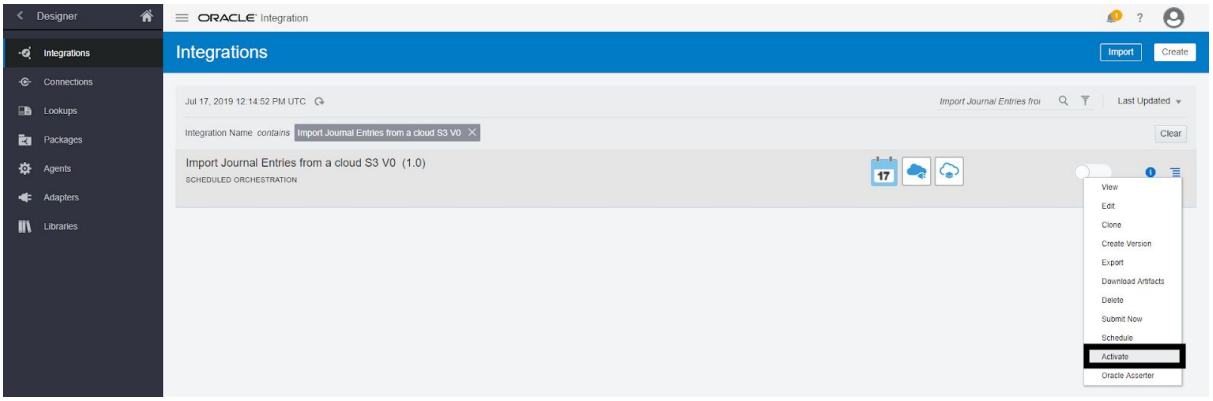
- Select **Type, Frequency** and **Scheduler Start Date** and click **Save** and **Close.**



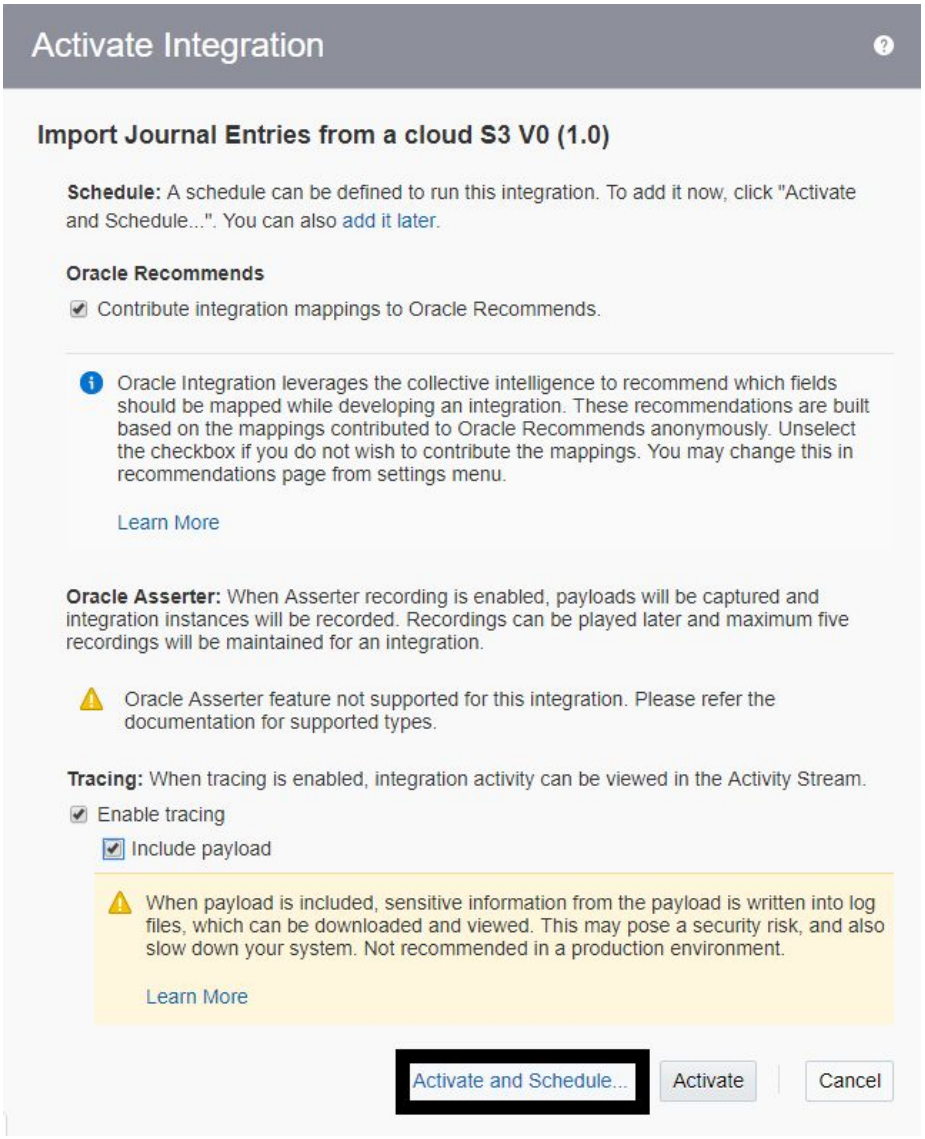


B3. Setting the Schedule when Activating the flow:

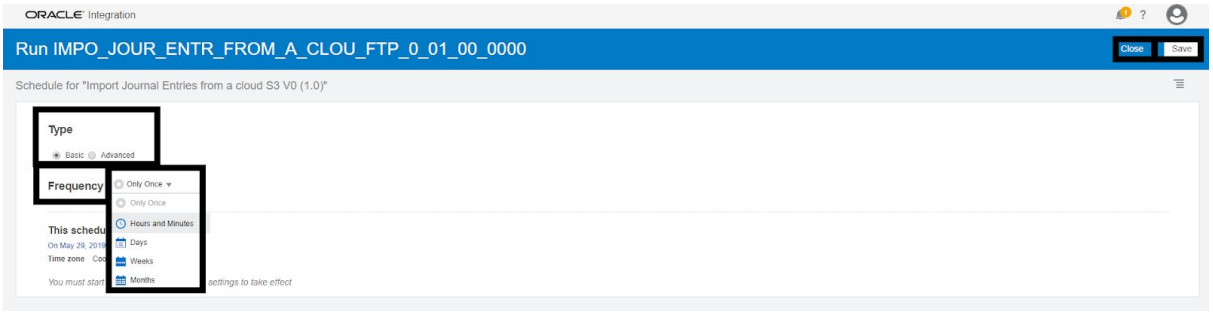
- **Log in** to your OIC service as an admin user and open the “Integrations” page.
- Select the integration flow called **Import Journal Entries from a cloud S3 V0 (1.0)** and then select **Activate** from the Actions menu bar on the right hand.

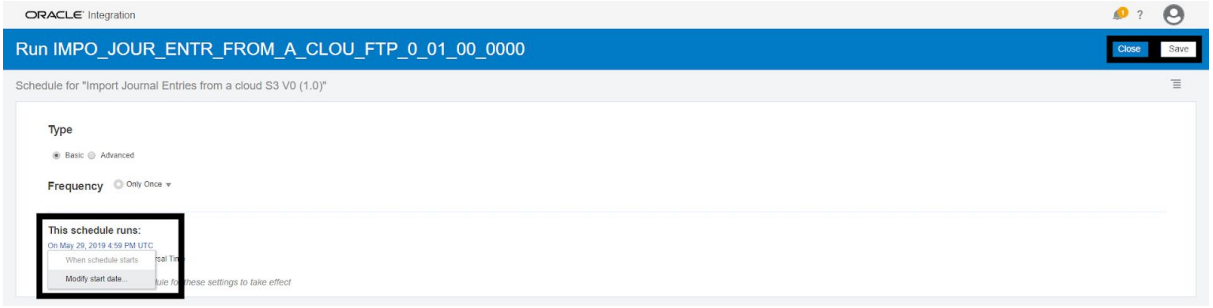


- In the modal window select **Activate and Schedule.**

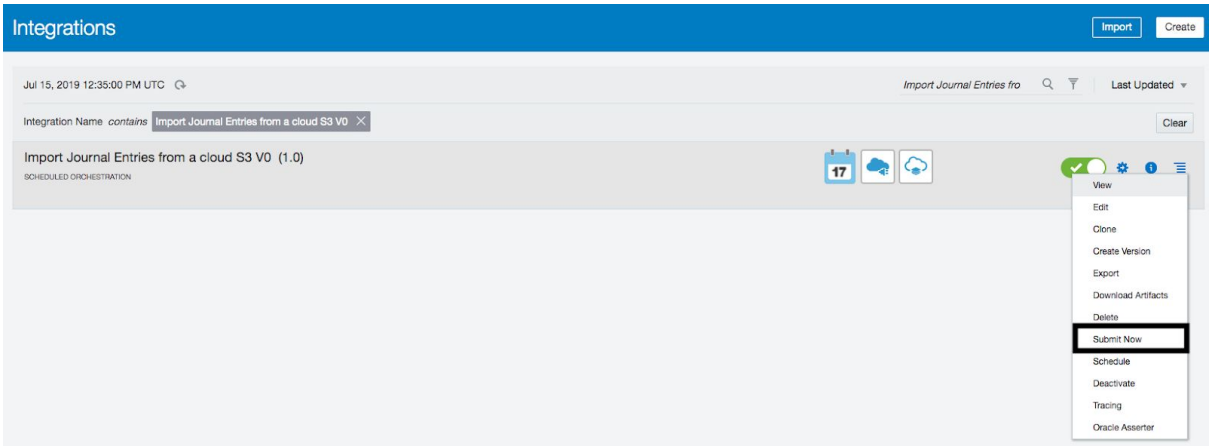


- Select **Type, Frequency** and **Scheduler Start Date** and click **Save** and **Close.**





C. After configuring and Activating the flow, you need to **Submit** it.



D. You need to acquire a **Trust Certificate** and a **Message Protection Certificate**.

Certificates can be obtained via **EM of EDGV**. Please download the certificates and upload into your OIC instance as explained below:

1. Go to OIC -> Integrations -> **Settings** -> **Certificates** -> **Upload** -> in the popup choose **Certificate Type** as "**Trust Certificate**" and upload certificate. The certificate could have a name e.g. like this: "**edgd_cloudca_TrustedCertificate.crt**"

2. Similarly choose "**Message Protection Certificate**" and upload remaining two certificates. They could be named e.g. like this: "**edgd_orakey_cloud9ca.crt**" and "**edgd_orakey_sign_cloud9ca.crt**"

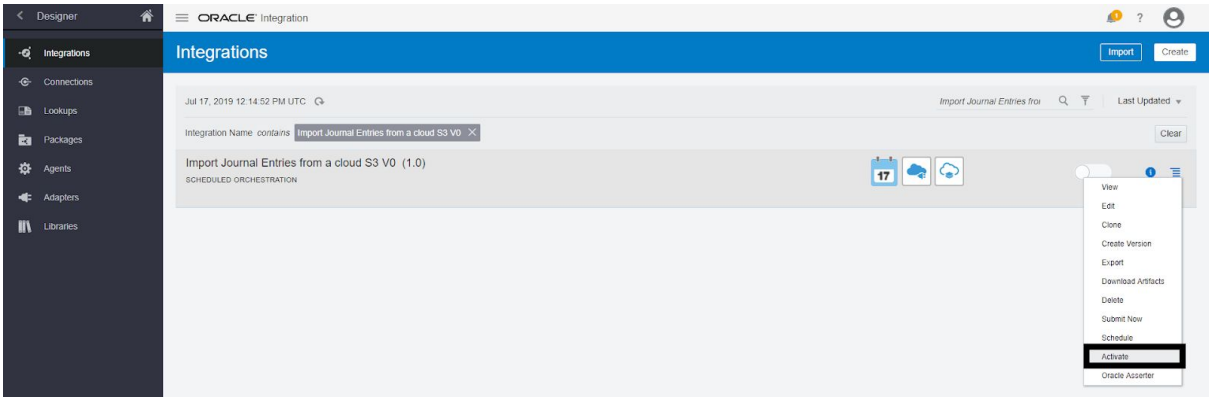
3. For more information regarding Managing security certificates please refer to the following guide: https://docs.oracle.com/en/cloud/paas/integration-cloud/erp-adapter/prerequisites-creating-connection.html#GUID-C179F26D-7409-43D7-B87B-E508A1DF7314

6. Activating Integration

Activating Import Journal Entries from a cloud FTP V0 (1.0)

1. **Log in** to your OIC service as an admin user and open the "Integrations" page.

2. Select the integration flow called **Import Journal Entries from a cloud S3 V0 (1.0)** and then select **Activate** from the menu bar on the right hand side - the on/off icon will go green when activated.



3. In the Activate Integration modal window select from the following options:

   Select/unselect **Contribute integration mappings to Oracle Recommends**.

   Note: Oracle Integration leverages the collective intelligence to recommend which fields should be mapped while developing an integration. These recommendations are built

based on the mappings contributed to Oracle Recommends anonymously. Unselect the checkbox if you do not wish to contribute the mappings. You may change this in recommendations page from settings menu.

- Select/unselect **Tracing** and **Payload.**

Note: When tracing is enabled, integration activity can be viewed in the Activity Stream.

Not recommended in a production environment.

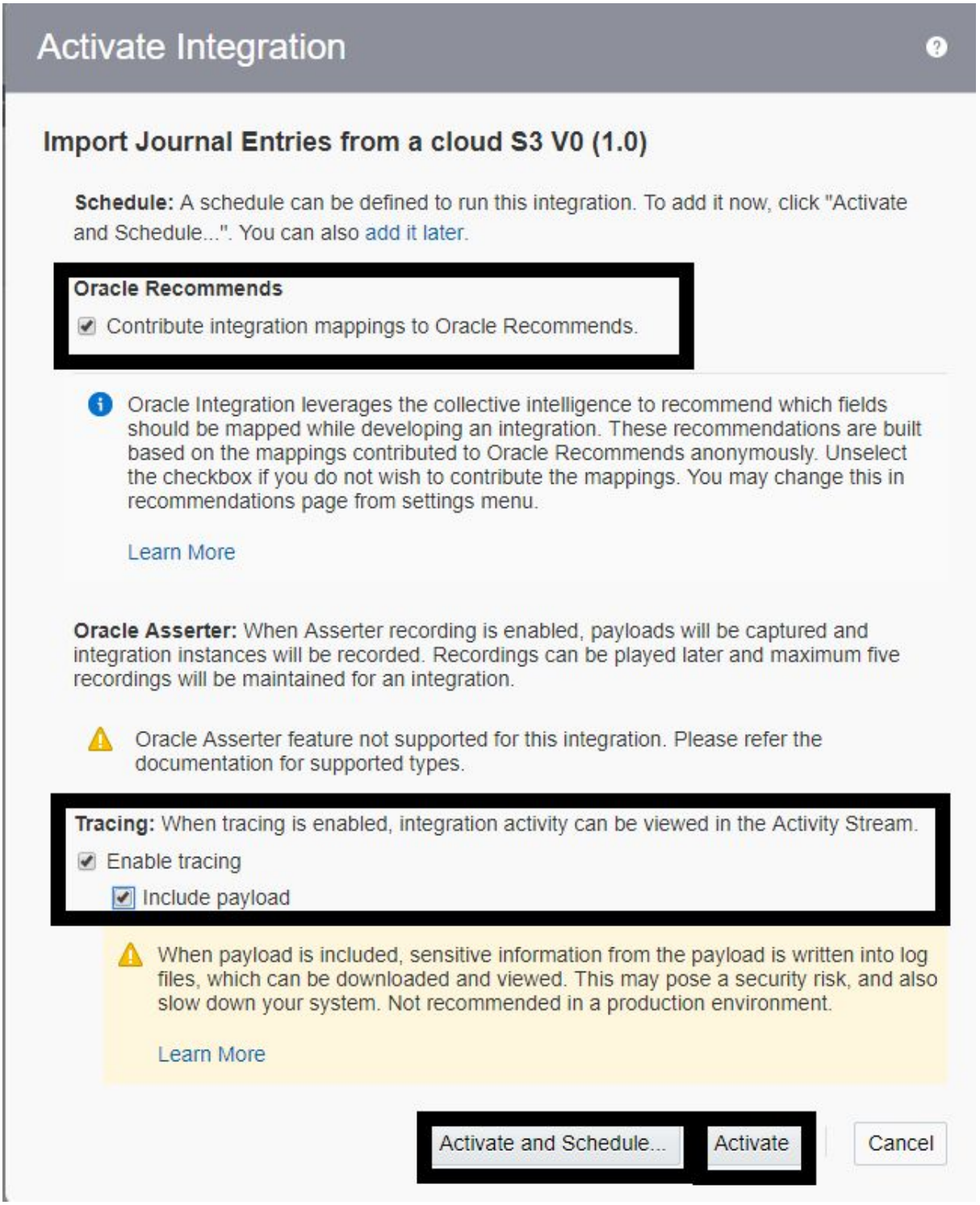
Note: When payload is included, sensitive information from the payload is written into log files, which can be downloaded and viewed. This may pose a security risk, and also slow down your system.

Not recommended in a production environment.

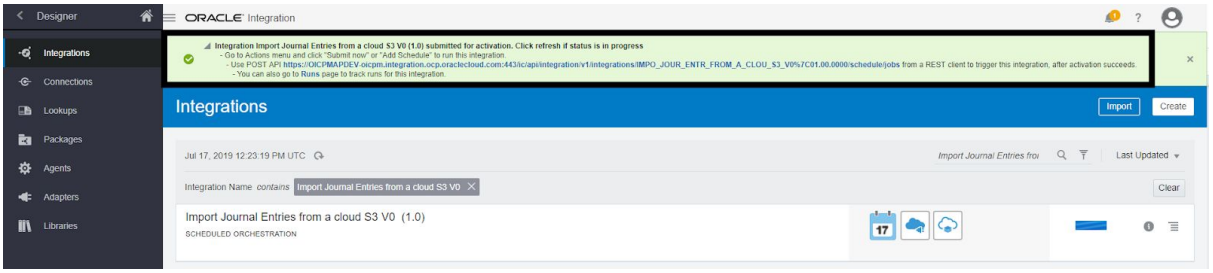
- Select either **Activate** or **Activate and Schedule.**

Note: When selecting **Activate** the flow will be **activated.**

When selecting **Activate and Schedule** you will be redirected to the Schedule part of the flow where you can set up the schedule for this integration flow and it will be **activated.**



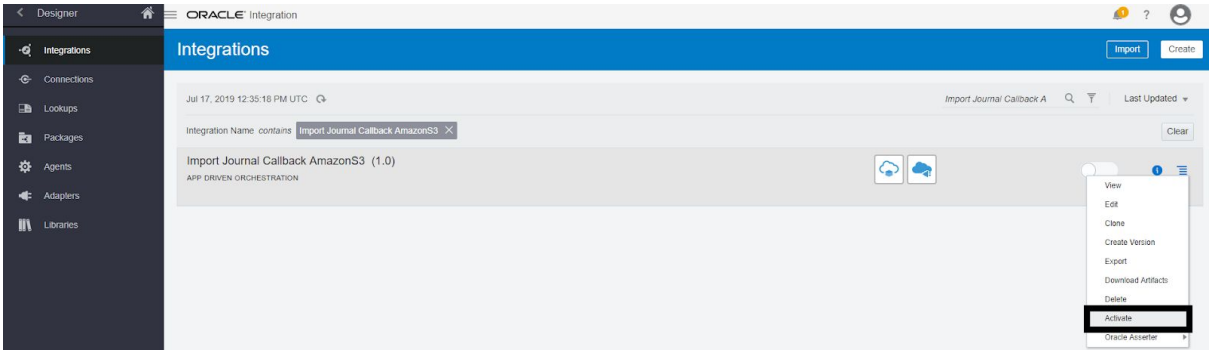
4. The **confirmation** note appears at the top, the flow is activated.



Note: After activating **Import Journal Entries from a cloud S3 V0 (1.0)** you have to also activate **Import Journal Callback AmazonS3 (1.0)** for the flow to work properly.

Activating Import Journal Callback AmazonS3 (1.0)

1. **Log in** to your OIC service as an admin user and open the “Integrations” page.
2. Select the integration flow called **Import Journal Callback AmazonS3 (1.0)** and then select **Activate** from the menu bar on the right hand side - the on/off icon will go green when activated.



3. In the Activate Integration modal window select from the following options:
    - Select/unselect **Contribute integration mappings to Oracle Recommends**.

    Note: Oracle Integration leverages the collective intelligence to recommend which fields should be mapped while developing an integration. These recommendations are built based on the mappings contributed to Oracle Recommends anonymously. Unselect the checkbox if you do not wish to contribute the mappings. You may change this in recommendations page from settings menu.

    - Select/unselect **Oracle Asserter.**

Note: When Asserter recording is enabled, payloads will be captured and integration instances will be recorded. Recordings can be played later and maximum five recordings will be maintained for an integration.

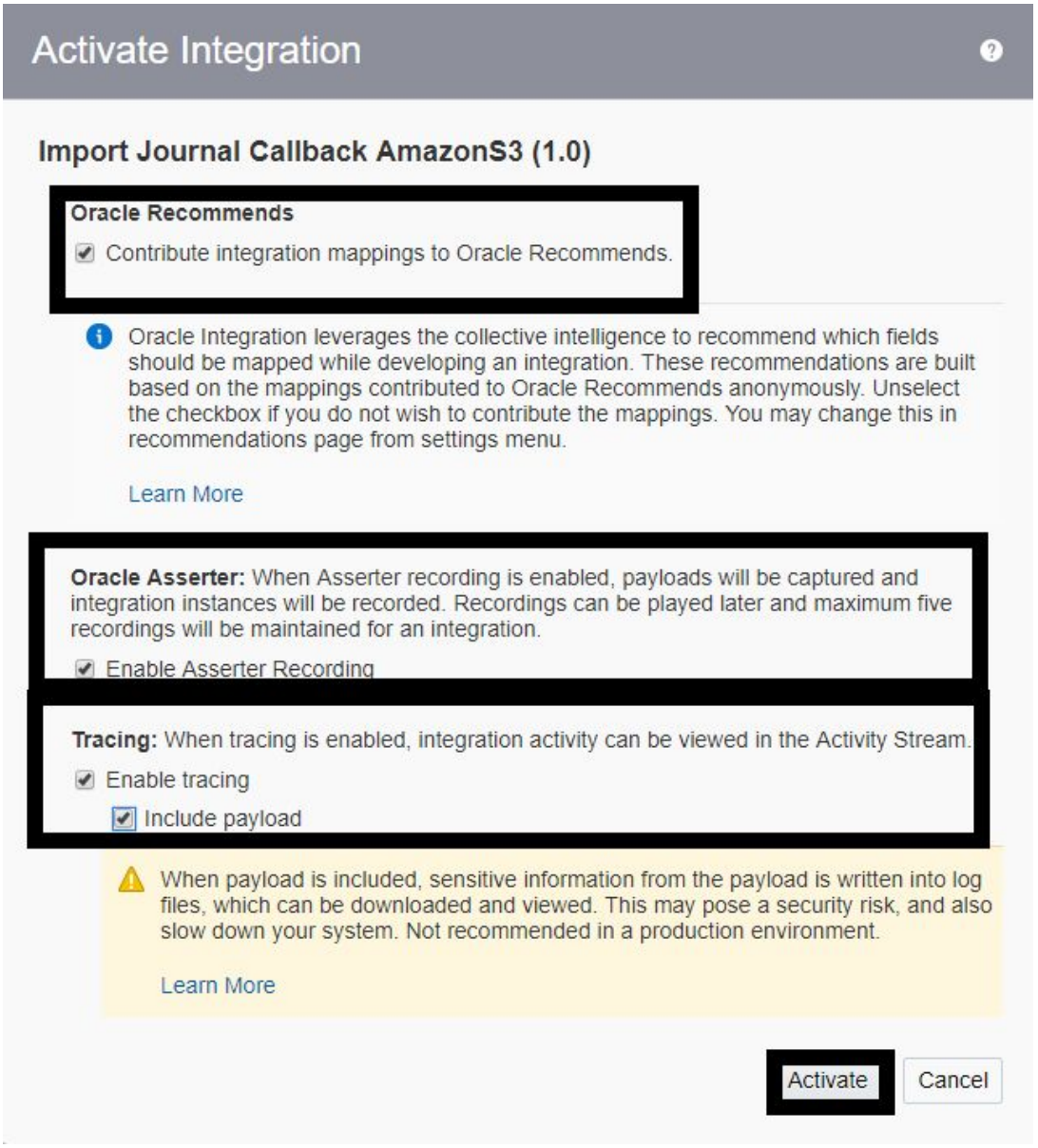
- Select/unselect **Tracing** and **Payload.**

Note: When tracing is enabled, integration activity can be viewed in the Activity Stream.

Not recommended in a production environment.

Note: When payload is included, sensitive information from the payload is written into log files, which can be downloaded and viewed. This may pose a security risk, and also slow down your system.

Not recommended in a production environment.



7. Appendix - Mappings

Mappings for Import Journal Entries from a cloud FTP V0 (1.0):

a. Mapping to get a file from Amazon S3

Name	Source	Target
Map to GetFileFromAmazonS3	$bucketName	/nstrgmpr:execute/nstrgmpr:TemplateParameters/ns2:bucketName
	$filename	/nstrgmpr:execute/nstrgmpr:TemplateParameters/ns2:fileName

b. Mapping to write a file

Name	Source	Target
Map to writeFile	$readFile/nsmpr3:ReadResponse/ns5:GeneralLedger/ns5:record	/nstrgmpr:Write/ns8:recordset/ns8:record
	ns5:C1	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C1
	ns5:C2	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C2
	ns5:C3	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C3
	ns5:C4	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C4
	ns5:C5	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C5
	USD	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:currency
	ns5:C7	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C7
	ns5:C8	/nstrgmpr:Write/ns8:recordse

		t/ns8:record/ns8:C8
	ns5:C9	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C9
	ns5:C10	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C10
	ns5:C11	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C11
	ns5:C12	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C12
	ns5:C13	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C13
	ns5:C14	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C14
	ns5:C15	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C15
	ns5:C16	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C16
	ns5:C17	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C17
	ns5:C18	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C18
	ns5:C19	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C19
	ns5:C20	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C20
	ns5:C21	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C21
	ns5:C22	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C22
	ns5:C23	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C23
	ns5:C24	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C24
	ns5:C25	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C25
	ns5:C26	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C26

	ns5:C27	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C27
	ns5:C28	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C28
	ns5:C29	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C29
	ns5:C30	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C30
	ns5:C31	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C31
	ns5:C32	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C32
	ns5:C33	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C33
	ns5:C34	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C34
	ns5:C35	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C35
	ns5:C36	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C36
	ns5:C37	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C37
	ns5:C38	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C38
	ns5:C39	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C39
	ns5:C40	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C40
	ns5:C41	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C41
	ns5:C42	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C42
	ns5:C43	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C43
	ns5:C44	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C44
	ns5:C45	/nstrgmpr:Write/ns8:recordse

		t/ns8:record/ns8:C45
	ns5:C46	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C46
	ns5:C47	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C47
	ns5:C48	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C48
	ns5:C49	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C49
	ns5:C50	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C50
	ns5:C51	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C51
	ns5:C52	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C52
	ns5:C53	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C53
	ns5:C54	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C54
	ns5:C55	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C55
	ns5:C56	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C56
	ns5:C57	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C57
	ns5:C58	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C58
	ns5:C59	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C59
	ns5:C60	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C60
	ns5:C61	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C61
	ns5:C62	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C62
	ns5:C63	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C63

	ns5:C64	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C64
	ns5:C65	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C65
	ns5:C66	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C66
	ns5:C67	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C67
	ns5:C68	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C68
	ns5:C69	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C69
	ns5:C70	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C70
	ns5:C71	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C71
	ns5:C72	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C72
	ns5:C73	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C73
	ns5:C74	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C74
	ns5:C75	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C75
	ns5:C76	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C76
	ns5:C77	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C77
	ns5:C78	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C78
	ns5:C79	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C79
	ns5:C80	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C80
	ns5:C81	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C81
	ns5:C82	/nstrgmpr:Write/ns8:recordse

		t/ns8:record/ns8:C82
	ns5:C83	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C83
	ns5:C84	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C84
	ns5:C85	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C85
	ns5:C86	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C86
	ns5:C87	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C87
	ns5:C88	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C88
	ns5:C89	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C89
	ns5:C90	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C90
	ns5:C91	/nstrgmpr:Write/ns8:recordset/ns8:record/ns8:C91

c. Mapping to write a property file

Name	**Source**	**Target**
Map to writePropertyFile	$readPropertyFile/nsmpr3:ReadResponse/ns5:list/ns5:record	/nstrgmpr:Write/ns9:list/ns9:record
	ns5:C1	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C1
	ns5:C2	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C2
	ns5:C3	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C3
	ns5:C4	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C4
	ns5:C5	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C5

	ns5:C6	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C6
	ns5:C7	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C7
	ns5:C8	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C8
	ns5:C9	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C9
	ns5:C10	/nstrgmpr:Write/ns9:list/ns9:record/ns9:C10

d. Mapping to send a file to ERP

Name	**Source**	**Target**
Map tosendToERP	$zipFile/nsmpr3:ZipResponse/ns8:ZipResponse/ns0:ICSFile/ns0:FileReference	/nstrgmpr:importBulkData/nstrgdfl:importBulkData/ns0:ICSFile/ns0:FileReference
	$zipFile/nsmpr3:ZipResponse/ns8:ZipResponse/ns0:ICSFile/ns0:Properties/ns0:filetype	/nstrgmpr:importBulkData/nstrgdfl:importBulkData/ns0:ICSFile/ns0:Properties/ns0:filetype
	$zipFile/nsmpr3:ZipResponse/ns8:ZipResponse/ns0:ICSFile/ns0:Properties/ns0:directory	/nstrgmpr:importBulkData/nstrgdfl:importBulkData/ns0:ICSFile/ns0:Properties/ns0:directory
	$zipFile/nsmpr3:ZipResponse/ns8:ZipResponse/ns0:ICSFile/ns0:Properties/ns0:filename	/nstrgmpr:importBulkData/nstrgdfl:importBulkData/ns0:ICSFile/ns0:Properties/ns0:filename
	$zipFile/nsmpr3:ZipResponse/ns8:ZipResponse/ns0:ICSFile/ns0:Properties/ns0:lastModifiedTime	/nstrgmpr:importBulkData/nstrgdfl:importBulkData/ns0:ICSFile/ns0:Properties/ns0:lastModifiedTime
	$zipFile/nsmpr3:ZipResponse/ns8:ZipResponse/ns0:ICSFile/ns0:Properties/ns0:creationTime	/nstrgmpr:importBulkData/nstrgdfl:importBulkData/ns0:ICSFile/ns0:Properties/ns0:creationTime
	$zipFile/nsmpr3:ZipResponse/ns8:ZipResponse/ns0:ICSFile/ns0:Properties/ns0:size	/nstrgmpr:importBulkData/nstrgdfl:importBulkData/ns0:ICSFile/ns0:Properties/ns0:size

	$zipFile/nsmpr3:ZipResponse/ns8:ZipResponse/ns0:ICSFile/ns0:Properties/ns0:checksum	/nstrgmpr:importBulkData/nstrgdfl:importBulkData/ns0:ICSFile/ns0:Properties/ns0:checksum

Mappings for Import Journal Callback AmazonS3 (1.0):

a. Mapping to upload a log file to Amazon S3

Name	Source	File
Map to UploadToAmazonS3	dvm:lookupValue ("tenant/resources/dvms/ImportJournalsAmazon", "Property_name", "bucketName", "Property_value", "")	/nstrgmpr:execute/nstrgmpr:TemplateParameters/ns8:bucketName
	concat (concat (dvm:lookupValue ("tenant/resources/dvms/ImportJournalV0", "Property_name", "uploadFileName", "Property_value", ""), concat ("_", xp20:format-dateTime (fn:current-dateTime(), "[YYYY]-[MM]-[DD]-[HH]-[mm]-[ss]"))), ".zip")	/nstrgmpr:execute/nstrgmpr:TemplateParameters/ns8:fileName
	/nssrcmpr:onJobCompletion/ns3:onJobCompletionRequest/ns0:ICSFile/ns0:FileReference	/nstrgmpr:execute/ns6:streamReference