

Oracle® Retail Integration Cloud Service

Technical Implementation Instructions for SI/ Customers



Release 23.1.401.0

F87057-01

October 2023

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Retail Integration Cloud Service Technical Implementation Instructions for SI/Customers, Release 23.1.401.0

F87057-01

Copyright © 2023, Oracle and/or its affiliates.

Primary Author:

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Send Us Your Comments

Preface

Audience	vii
Documentation Accessibility	vii
Customer Support	vii
Improved Process for Oracle Retail Documentation Corrections	viii
Oracle Retail Documentation on the Oracle Help Center (docs.oracle.com)	viii
Conventions	viii

1 RICS implementation

Pre-Provisioning	1-1
Provisioning	1-1
Access OCI IAM	1-1
Validate Cloud Service Access	1-2
Register Customer Support Identifier	1-2
Create End User Accounts	1-2
Post Provisioning	1-3
RIB CS Self-Service instructions for SI/Customer	1-3
Application: rib-sim	1-3
Application: rib-rms	1-3
Application: rib-tafr	1-3
Application: rib-ext	1-4
Application: rib-rob	1-6
Application: rib-lgf	1-7
Application: rib-rwms (primary)	1-8
Application: BDI Process-Flow	1-9
RFI CS Self-Service instructions for SI/Customer	1-10
Application: RFI-web-app	1-10
USM CS Self-Service instructions for SI/Customer	1-11
Application: USM-LGF	1-12

Application: DDS	1-15
Poison Message Processing steps for SI/Customer	1-15
Support	1-20
Leverage Oracle Support	1-20
Get Connected	1-20
Frequently Asked Questions	1-20
OCI IAM Activation	1-20

Index

List of Figures

1-1	Update the Facilities	1-4
1-2	Ping Service URL	0
1-3	Configure External Injector Service Error	1-5
1-4	Secured User Name and Password	1-5
1-5	Oauth2 Token Generation	1-6
1-6	URL Error	1-6
1-7	Configure ROB Injector Service	1-7
1-8	URL Error	1-7
1-9	Update Creds for CustomerOwned Alias	1-8
1-10	Configure Injector URL for soap-app	1-9
1-11	Configure POM Callbacks	1-10
1-12	Update Credentials For Customer Owned aliases	1-11
1-13	Update the CFIN Integration URL	1-11
1-14	Configure Initial Project	1-12
1-15	Select external_env_info.LogFireIntegration	1-13
1-16	Edit USM Configuration	1-13
1-17	Update CompanyCode_dvm.LogFireIntegration	1-14
1-18	UpdateFacilityCode_dvm.LogFireIntegration	1-14
1-19	Configure Initial Security Setup	1-15
1-20	Selected Schema Tables	1-15
1-21	Retail Platform Services	1-16
1-22	FTS Wrapper Page	1-16
1-23	List of Prefixes	1-17
1-24	Parameters	1-17
1-25	Server Response	1-18
1-26	Create Pre-Authenticated Request	1-18
1-27	Server Response	1-18
1-28	Generate the Pre-Authenticated Request	1-19
1-29	Server Response	1-19

Send Us Your Comments

Oracle® Retail Integration Cloud Service Technical Implementation Instructions for SI/ Customers, Release 23.1.401.0.

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).



Note:

Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available in the Oracle Help Center (docs.oracle.com). It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com.

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at <http://www.oracle.com>.

Preface

When starting a Retail Predictive Application Server Cloud Edition (RPAS CE) implementation, there are a number of key considerations and actions the Customer/System Integrator will need to take to complete the new provisioning.

Audience

This Technical Implementation Instructions for SI/Customers is intended for the customer's service administrator and the customer's System Integrator. The service administrator is the key person in your business that manages your Integration cloud service. Oracle will target important communications to the service administrator, such as the initial welcome e-mail that is described in this document. If the person who receives this e-mail is not the person or part of the group of people that will be taking responsibilities for the tasks in this document, please work with your Customer Success Manager (CSM) to have that the name updated.

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.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times not be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Help Center (docs.oracle.com), or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Help Center (docs.oracle.com) at the following URL:

<https://docs.oracle.com/en/industries/retail/index.html>

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of a document with part number E123456-01.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Help Center (docs.oracle.com)

Oracle Retail product documentation is available on the following web site:

<https://docs.oracle.com/en/industries/retail/index.html>

(Data Model documents can be obtained through My Oracle Support.)

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

RICS implementation

When starting a Retail Predictive Application Server Cloud Edition (RPAS CE) implementation, there are a number of key considerations and actions the Customer/System Integrator will need to take to complete the new provisioning.

Pre-Provisioning

Pre-provisioning is the period after contracts are signed, but before receiving your environments, where some key activities can occur related to your upcoming implementation. For Integration Cloud Service implementations, your Customer Success Manager (CSM) will be your main point of contact for these activities.

Provisioning

Once your environments are ready for you, the person designated as your service administrator will receive a welcome e-mail: one for each cloud service and each environment (stage, production, and so on).

Follow all instructions in the **Action Required: Access and Administer Production/Stage/Test Environment...** e-mail.

This environment access e-mail contains critical details required for you to access and administer your Cloud Service. You will receive an e-mail for each provisioned environment. Save these e-mails.

Log in to your Cloud Service. Use the Identity Management URL, username and temporary password provided in the environment access e-mail to verify access to your service. At your first login attempt, create a new password and make note of it because at this point you are the only one with access!

You will receive a separate e-mail for each provisioned environment, and the password for each environment is maintained separately. In addition, please note that you will not be able to access the Retail applications until you grant the appropriate application roles to your user.

It is recommended that you save this e-mail for future reference, because at this point the service administrator is the only person with access.

Access OCI IAM

Once you receive your welcome e-mail, it is recommended that you, as the system administrator, log into OCI IAM to verify your access and create a new password. You will also be assigned the application administrator group for each Retail Integration service in both your production and pre-production environments. Note that the group for pre-production will have an added extension (`_PREPROD`) in order to differentiate between the two. These should not be deleted.

It is also recommended that you add additional administrators in order to have a backup administrator and share in user management administration, as at this point no one else in

your organization will have access to OCI IAM or the Retail Integration solutions. For assistance in creating users or adding them to groups, see the following documents:

- Managing Users, User Accounts, and Roles
- Adding Identity Domain Administrators

 **Note:**

You may notice that there are a number of other user IDs set up in OCI IAM for Retail Integration (for example, `bdi_admin`, `jos_admin`). These users were seeded by the Oracle Cloud Operations team for use in Merchandising batch and integration processes. These users will be managed by the Oracle Cloud Operations team.

Validate Cloud Service Access

Next, you should validate that you are able to access and successfully log into each of the Retail Integration Cloud Services for which you have been provisioned using the URLs provided in the e-mail, along with the username and password.

Register Customer Support Identifier

The welcome e-mail will also include your Customer Support Identifier (CSI). This should be registered with My Oracle Support (MOS), which you will use to log questions or issues about these services. Follow link in the e-mail or access support.oracle.com to create a new account. If you already have a MOS account, remember to add your new CSI to your existing MOS account.

The first person to request access to a CSI will be checked by Oracle to ensure the domain of their e-mail address matches the domain associated with the CSI. Once approved, they will be made the Customer User Administrator of that CSI, and can approve others to use it. If someone else has already been made the administrator of that CSI, then the request will be e-mailed to him or her for approval. For more information on the Customer User Administrator, see **MOS Doc ID 1544004.2**.

 **Note:**

You will not be able to register your CSI number until your production environment has been provisioned.

Create End User Accounts

Before end users can access the Cloud Service application it is necessary to provision each user access to the system, and assign roles to each user to control what functionality will be available to them. The access provisioning is done using Oracle Identity Management (OIM). Instructions for end user account creation are documented in an Administration Guide, found in an online Documentation library at this location:

<http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html>

Post Provisioning

Once your RICS environments are ready there are addition configuration steps that are Self-Service. Many, if not most, are now Auto-Wired during the Provisioning process, the following section are a checklist of the steps for each of the RICS Product Domains that are not auto-wired.

RIB CS Self-Service instructions for SI/Customer

The following sections list by application the RIB CS Self-Service instructions for SI/Customers.

Application: rib-sim

Instructions

Not Applicable (Auto-wired)

Owner: Who configures in Production

Not Applicable

Application: rib-rms

Instructions

Not Applicable (Auto-wired)

Owner: Who configures in Production

Not Applicable

Application: rib-tafr

Instructions

Perform the following steps to Update the Facilities.

- Go to **Manage Configurations > system options** tab
- Click **Add**.
- Insert a new **Facility ID**.

Example: key - facility_id.PROD.12345 value - 1

 **Note:**

Update the facilities as needed using the previous steps.

Figure 1-1 Update the Facilities

Add new property here

facility_id.PROD.12345

1

Save icon

Owner: Who configures in Production

Service Implementer /Customer

Application: rib-ext

Instructions**Prerequisite:**

Get the Injector URL and credential details from the external apps team.

Perform the following steps to Configure External Injector Service.

- Go to **Manage Configurations >System Options** tab.
- Update the Injector Service URL with the customer provided value .
Example: Host-rgbu-phx-lbint-379.us.oracle.com Port-80
- Update the value for ping Service URL (injector.service.endpoint.ping.url). URL should point to ping service provided by external application.
(e.g.- https://<host:port>/rib-injector-services-web/resources/injector/ping)

Figure 1-2 Ping Service URL

injector.service.appType

rest-app

injector.service.endpoint.ping.url

https://rgbu-test

injector.service.endpoint.url

https://rgbu-test

- Click **Save**.

For third party integration where the injector service is hosted on OIC/on-prem, the below property in RIB_JAVA_OPTIONS needs to be added while patching the environment using RPT.

- Doauth2.url.path.wo.vrc=<context root of injector service>
Important: context root of injector service is any word in injector service url which can identify service uniquely.

For example:

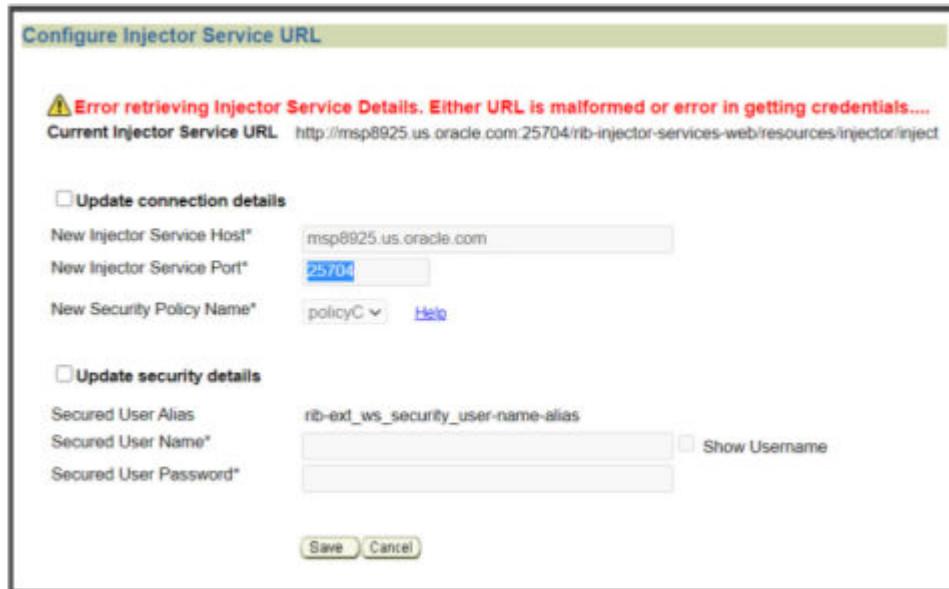
For the following injector service url https://<external-lb>/ external-injector-services/external/ribinjector/inject. The java_option would be

oauth2.url.path.wo.vrc=ribinjector

Perform the following steps to Update Creds for CustomerOwned Alias

- Perform the following steps for Oauth2 Authentication
 - Go to **Manage Configurations > Injector Service** tab.
Update the Secured User Name and Secured User Password. Set username and password empty for oauth2 calls.

Figure 1-3 Configure External Injector Service Error



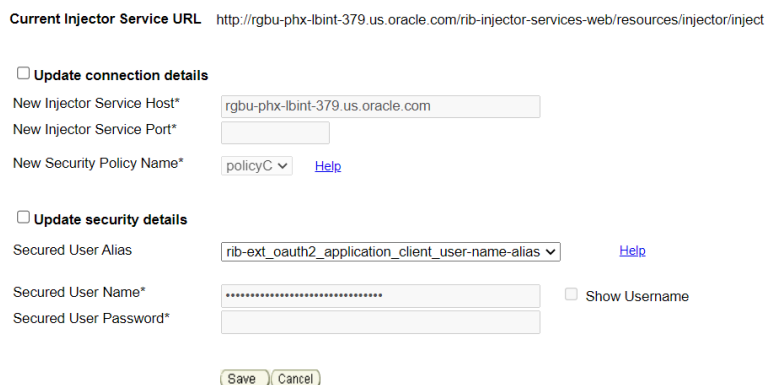
1. Select rib_ext_oauth2_application_client_user_name_alias from the dropdown.
2. Update the Secured User Name with Client Id and Secured User Password with the Client Secret.

Example:

User Name - 18927c74-fed6-45e9-8198-977c5a758ac5

Password - 18927c74-fed6-45e9-8198-977c5a758ac5

Figure 1-4 Secured User Name and Password



3. Click **Save**.
4. Update system options
5. Go to Manage Configurations > System Options tab
6. Update IDCS host url needed for oauth2 token generation and scope of access for inject calls.

Figure 1-5 OAuth2 Token Generation



7. Click Save.

Owner: Who configures in Production

Service Implementer /Customer

Application: rib-rob

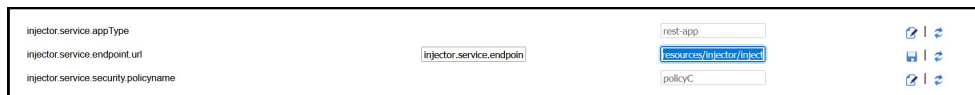
Instructions

Prerequisite:

Get the Injector URL and credential details from the order broker team.

Perform the following steps to Configure ROB Injector Service

- Go to **Manage Configurations > System Options** tab
- Update the property injector.service.endpoint.url as per the following value - `https://<host>:<port>/<OB_SUB_NAMESPACE>/rib-injector-services- web/orcos/resources/injector/inject`



• Click **Save**.

Perform the following steps to Update Creds for CustomerOwned Alias

1. Authentication (OAuth2)

- Go to **Manage Configurations > Injector Service** tab.
- Select `rib_rob_ws_security_user_name_alias` from the dropdown.
- Update the Secured User Name and Secured User Password
- User and Password should be set empty for OAuth2 scope.
- Click **Save**.

Figure 1-6 URL Error



Figure 1-7 Configure ROB Injector Service

Current Injector Service URL <https://omni.retail.us-phoenix-1.ocs.oc-test.com/rgbu-omni-eit-stg99-obcs/rib-injector-services-web/orcos/resources/injector/inject>

Update connection details

New Injector Service Host*

New Injector Service Port*

New Security Policy Name* [Help](#)

Update security details

Secured User Alias [Help](#)

Secured User Name*

Secured User Password*

Show Username

2. Oauth2 Authentication

Go to **Manage Configurations > Injector Service** tab

- Select **rib_rob_oauth2_application_client_user_name_alias** from the dropdown.
- Select **rib_rob_oath2_application_client_user_name_alias** from the dropdown.

Update the Secured User Name with Client Id and Secured User Password with the Client Secret.

Example:

User Name - 18927c74-fed6-45e9-8198-977c5a758ac5

Password - 18927c74-fed6-45e9-8198-977c5a758ac5

Click **Save**.

Figure 1-8 URL Error

Current Injector Service URL <https://omni.retail.us-phoenix-1.ocs.oc-test.com/rgbu-omni-eit-stg99-obcs/rib-injector-services-web/orcos/resources/injector/inject>

Update connection details

New Injector Service Host*

New Injector Service Port*

New Security Policy Name* [Help](#)

Update security details

Secured User Alias [Help](#)

Secured User Name*

Secured User Password*

Show Username

Owner: Who configures in Production

Service Implementer

Application: rib-igf

Instructions

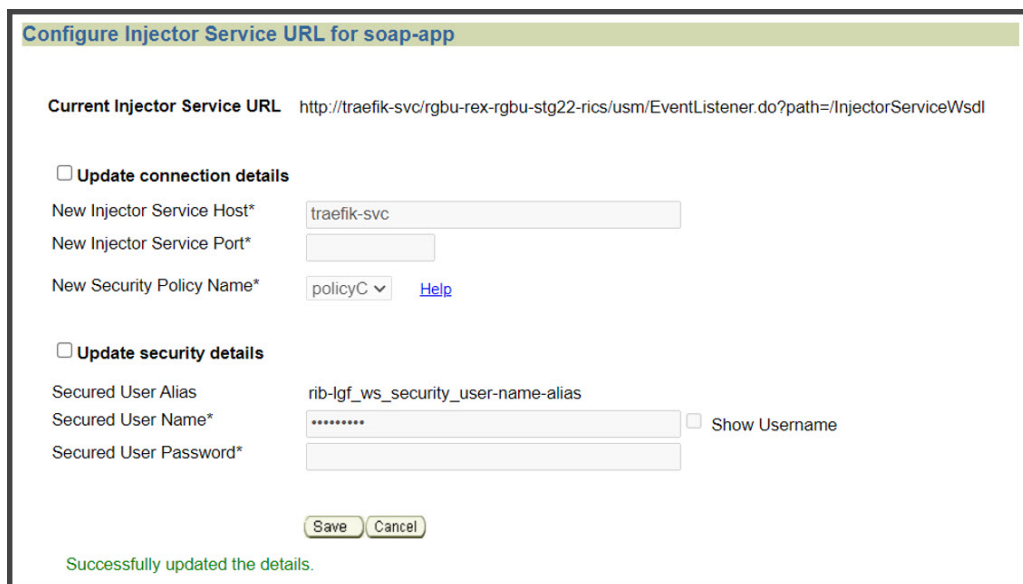
Prerequisite:

Get the credentials from the log-fire team.

Perform the following steps to Update Creds for CustomerOwned Alias

- Authentication
 - Go to **Manage Configurations > Injector Service** tab
 - Update the Secured User Name and Secured User Password
- Example:
- User Name - rgbu6_admin
- Password - welcome1
- Click **Save**.

Figure 1-9 Update Creds for CustomerOwned Alias



Configure Injector Service URL for soap-app

Current Injector Service URL http://traefik-svc/rgbu-rex-rgbu-stg22-rics/usm/EventListener.do?path=/InjectorServiceWsd

Update connection details

New Injector Service Host* traefik-svc

New Injector Service Port*

New Security Policy Name* policyC [Help](#)

Update security details

Secured User Alias rib-lgf_ws_security_user-name-alias

Secured User Name* Show Username

Secured User Password*

Successfully updated the details.

Owner: Who configures in Production

Not Applicable

Application: rib-rwms (primary)

Instructions

Instructions

Prerequisite:

Get the rib-rwms (on-premise) secondary connection details from the customer. Get the credentials for user (belonging to ribAdminGroup) on rib-rwms secondary install.

Perform the following steps to update connection details and Creds for CustomerOwned Alias

- Authentication
 - Go to Manage Configurations > Injector Service tab
 - Update host and port to point to rib-rwms secondary
 - Update the Secured User Name and Secured User Password.

Example:

User Name - ribadmin

Password - welcome1

- Click **Save**.

Figure 1-10 Configure Injector URL for soap-app

Configure Injector Service URL for soap-app

Current Injector Service URL `https://ribu-phx-300.srphwprshared1.gbuocdsint2.phx.oraclevcn.com:7022/PlsqApplicationMessageInjectorServiceBean/PlsqApplicationMessageInjectorServiceBeanService/`

Update connection details

New Injector Service Host* `ribu-phx-300.srphwprshared1.gbuocdsint2.phx.orc`

New Injector Service Port* `7022`

New Security Policy Name* `policyA` [Help](#)

Update security details

Secured User Alias `rib-rwms_ws_security_user-name-alias`

Secured User Name* `*****` Show Username

Secured User Password* `*****`

Owner: Who configures in Production

Service Implementer /Customer

Application: BDI Process-Flow

Instructions

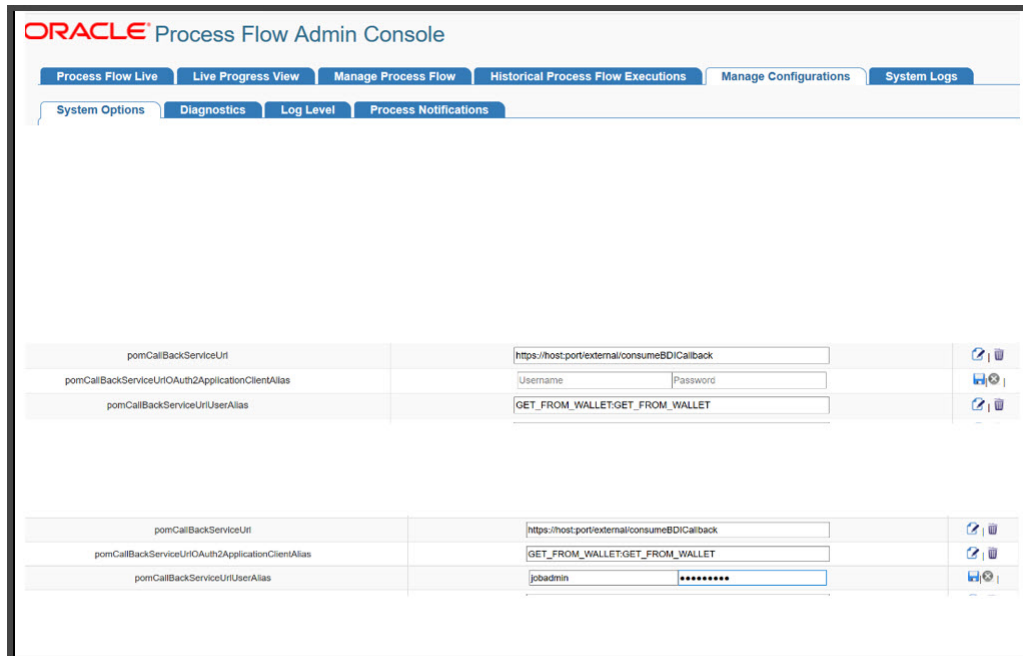
Perform the following steps to Configure POM callbacks and update credentials for **customerOwned Alias**, **pomCallBackServiceUr-lUserAlias**, **pomCallBackServiceUrl**, **pomCallBackServiceUrlOAuth2ApplicationClientAlias**.

Go to **PF UI > Manage Configurations > System Options** tab.

Select `pomCallBackServiceUrlUserAlias` and click **Edit**.

Enter the Username and password provided by the POM and click **Save**.

Repeat the same steps for updating **pomCallBackServiceUrl** and **pomCallBackServiceUrlOAuth2ApplicationClientAlias**.

Figure 1-11 Configure POM Callbacks**Owner: Who configures in Production**

Service Implementer /Customer

This may not be needed if you use the application scope for Oauth.

RFI CS Self-Service instructions for SI/Customer

The following sections list by application the RFI CS Self-Service instructions for SI/Customer.

Application: RFI-web-app

Instructions

Perform the following steps to Update Credentials For customer Owned aliases.

- Navigate to **Manage Configurations > Service Configurations**.
- Select **CFIN** in the RFI Integrated application dropdown.
- Check the **Update Security Details** check box.
- In the Secured User Name enter: **CFIN username**.
- In the Secured User Password enter **CFIN pwd**.
- Click **Save**.

Figure 1-12 Update Credentials For Customer Owned aliases

Update security details

Secured User Alias financialUtilServiceUserNameAlias

Secured User Name* Show Username

Secured User Password* _____

Owner: Who configures in Production

Service Implementer /Customer

Instructions

Perform the following steps to Update the CFIN Integration URL

- Navigate to **Manage Configurations > Service Configurations**.
- Select **CFIN** in the RFI Integrated application dropdown.
- Check the **Update Connection Details** check box.
- Update the CFIN Service Host and Port.
- Click **Save**.

Figure 1-13 Update the CFIN Integration URL**Current Service Integrations for CFIN**

Financial Service URL <https://customer.new.env.oraclecorp.com/fscmService/ErpIntegrationService?WSDL>
GL Account Validation URL <https://customer.new.env.oraclecorp.com:443/fscmService/AccountCombinationService?WSDL>

 Update connection details

New CFIN Service Host*
 New CFIN Service Port*

Owner: Who configures in Production

Service Implementer /Customer

USM CS Self-Service instructions for SI/Customer

The following sections list by application the USM CS Self-Service instructions for SI/Customer.

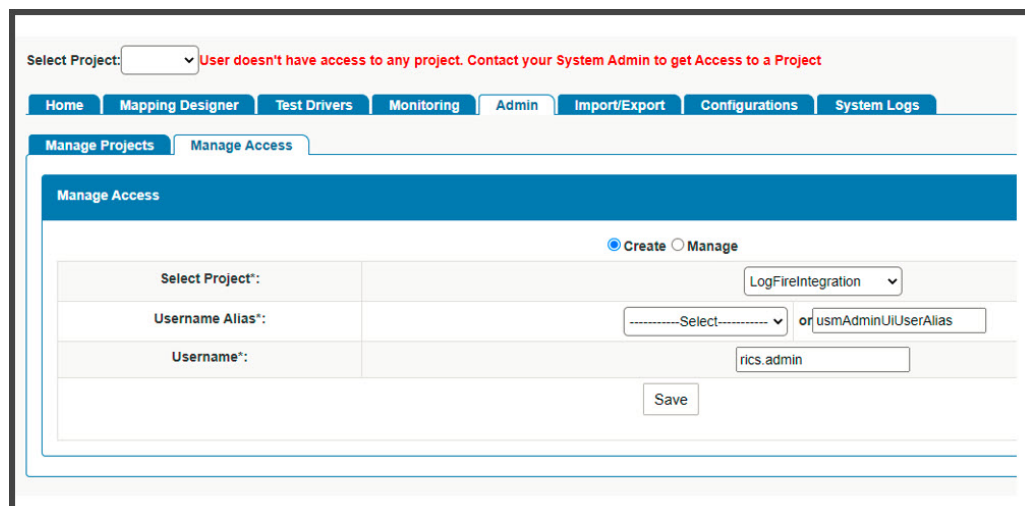
Application: USM-LGF

Instructions

Log in to USM UI as an admin and perform the following steps to Configure Initial Project.

- Go to **Admin > Manage Access** tab.
- Select Project: **LogFireIntegration**
- Username Alias: **usmAdminUiUserAlias**
- UserName: **rics.admin**(Give the admin username)
- Click **Save**.

Figure 1-14 Configure Initial Project



The screenshot displays the 'Manage Access' configuration interface. At the top, there is a 'Select Project:' dropdown menu with a red error message: 'User doesn't have access to any project. Contact your System Admin to get Access to a Project'. Below this, there are navigation tabs: Home, Mapping Designer, Test Drivers, Monitoring, Admin, Import/Export, Configurations, and System Logs. The 'Admin' tab is active, and within it, 'Manage Access' is selected. The 'Manage Access' section has a blue header and contains a form with the following fields:

- Select Project*:** A dropdown menu with 'LogFireIntegration' selected.
- Username Alias*:** A dropdown menu with 'usmAdminUiUserAlias' selected.
- Username*:** A text input field containing 'rics.admin'.

There are radio buttons for 'Create' (selected) and 'Manage'. A 'Save' button is located at the bottom of the form.

Owner: Who configures in Production

Service Implementer /Customer

Instructions

Perform the following steps for External JSON updates.

- Go to **Configurations > Edit Usm Configuration**.
 - Select **external_env_info.LogFireIntegration** from the dropdown and click **Edit**.
 - Enter the following:
 - name: LogFire_Host_Url_Key
 - value: The logFire Host URL
- Example: https://intqa.wms.ocs.oraclecloud.com:443/lgf_int_qa

 **Note:**

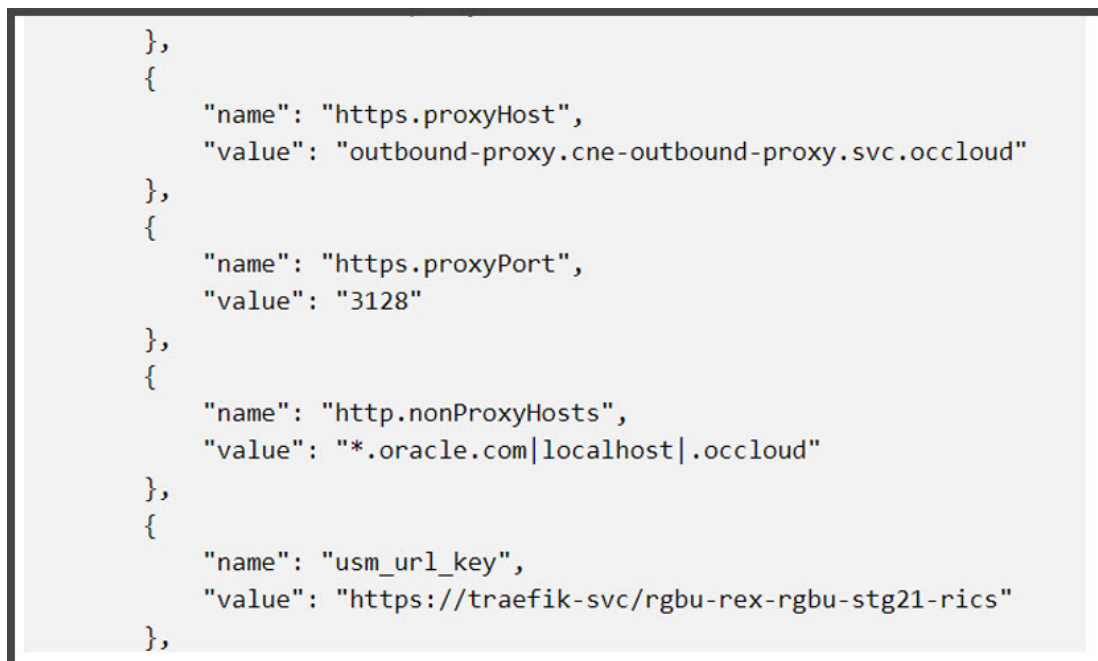
The URL may change as per the customer's LGF instance.

- Click **Save**.

Figure 1-15 Select external_env_info.LogFireIntegration



Figure 1-16 Edit USM Configuration



Owner: Who configures in Production

Service Implementer /Customer

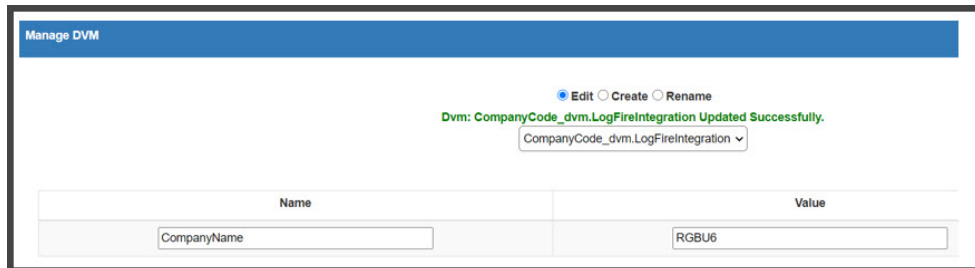
Instructions

Perform the following steps to Update DVM.

- Go to **Configurations > Manage DVM** tab.

- Select **CompanyCode_dvm.LogFireIntegration** from the dropdown.
- Click **Edit** on the row that you want to edit.
- Update the value of **CompanyName** that is set in LogFire application
Example - CompanyName value - RGPU6

Figure 1-17 Update CompanyCode_dvm.LogFireIntegration



- Click **Save**.
- Select **FacilityCode_dvm.LogFireIntegration** from the dropdown.
- Click **+** to add a new row with the details of **FacilityId**, **FacilityType**, and **FacilityTimeZone** as configured in LogFire application

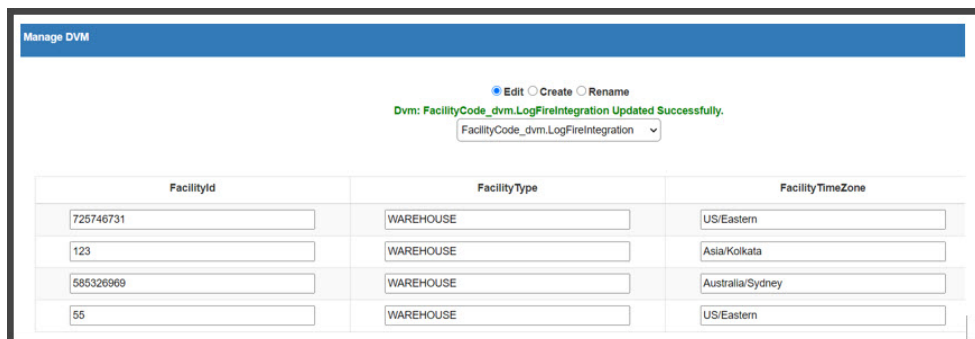
Example:

FacilityId - 55

FacilityType - WAREHOUSE

FacilityTimeZone - US/Eastern

Figure 1-18 UpdateFacilityCode_dvm.LogFireIntegration



Owner: Who configures in Production

Service Implementer /Customer

The following sections list by application the RICS Tools CS Self-Service instructions for SI/Customer.

Application: DDS

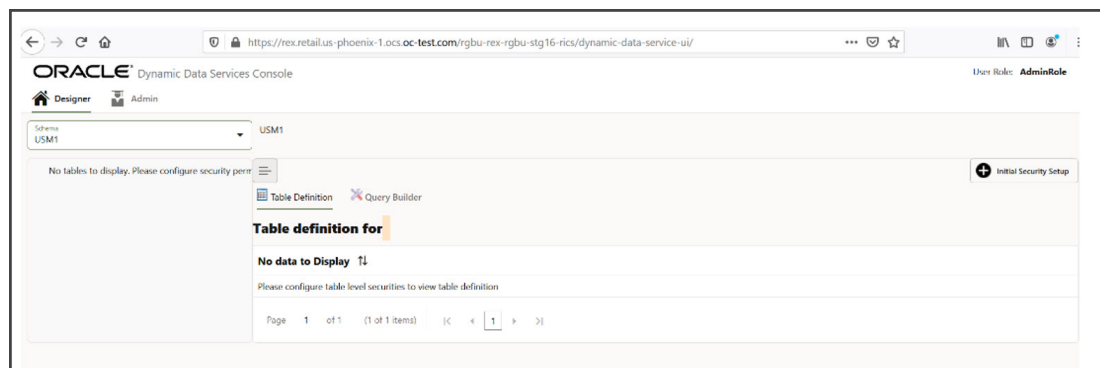
Instructions

Perform the following steps to Configure Initial Security Setup.

Log in to DDS UI as an Admin and then go to the Designer tab.

Select the schema from dropdown.

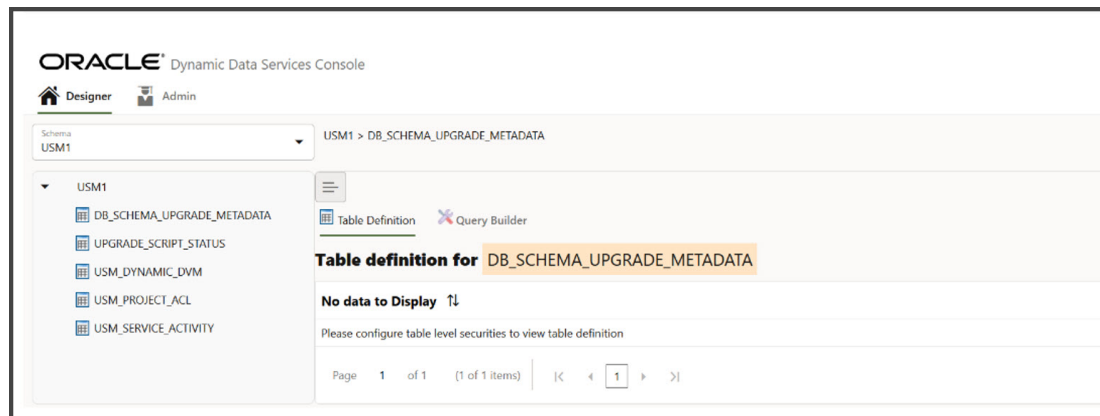
Figure 1-19 Configure Initial Security Setup



Click **Initial Security Setup**.

All tables for the schema selected should be displayed.

Figure 1-20 Selected Schema Tables



Poison Message Processing steps for SI/Customer

In CFS, poison messages are archived and uploaded to object store periodically. The SI/Customer needs to download the archive, correct the RIBMessage and upload it back to object storage using the RetailAppsPlatformServices UI. RIB downloads the customer uploaded messages and processes it.

Below are steps:

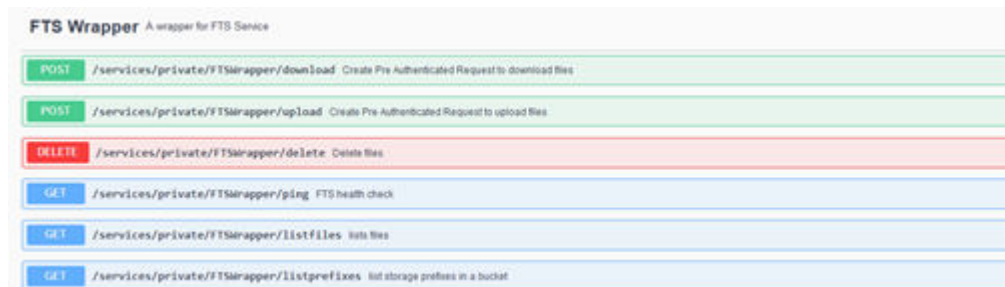
1. Login to RetailAppsPlatformService using IdcsUser credentials.
[https:// rex.retail.us-<region>.ocs.oraclecloud.com /<subnamespace>/RetailAppsPlatformServices/swagger-ui/##](https://rex.retail.us-<region>.ocs.oraclecloud.com /<subnamespace>/RetailAppsPlatformServices/swagger-ui/##)

Figure 1-21 Retail Platform Services



2. Search for FTS Wrapper Services.

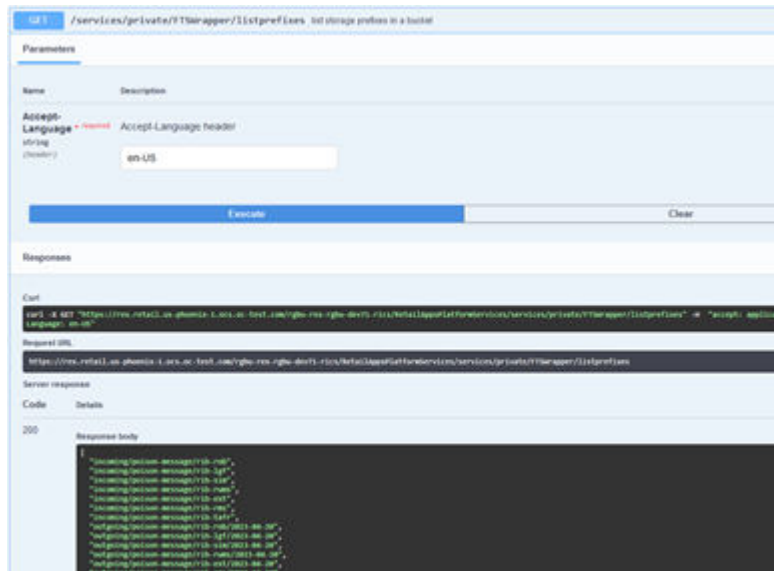
Figure 1-22 FTS Wrapper Page



3. List prefixes and pick the needed prefix.

Example: If you want to download the poison message for a specific rib-ext on 2023-04-20 choose the prefix: **"outgoing/poison-message/rib-ext/2023-04-20"** or under **"outgoing/poison-message/rib-ext"**

Figure 1-23 List of Prefixes



- List the files to know file name to be downloaded from object store.

Input: outgoing/poison-message/rib-ext/2023-04-20(The prefix picked in step 3) and outgoing/poison-message/rib-ext

Output: PoisonMsg_rib-ext_2023-04-19T05:16:38.zip

Figure 1-24 Parameters

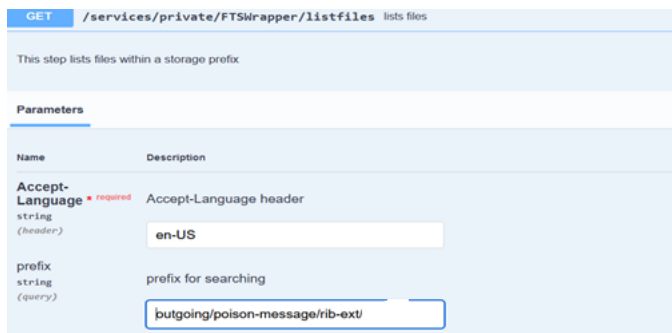


Figure 1-25 Server Response



5. Create Pre-Authenticated Request to download files.
Choose the accessUri from json response. And this is valid for 5 mins only.

Figure 1-26 Create Pre-Authenticated Request

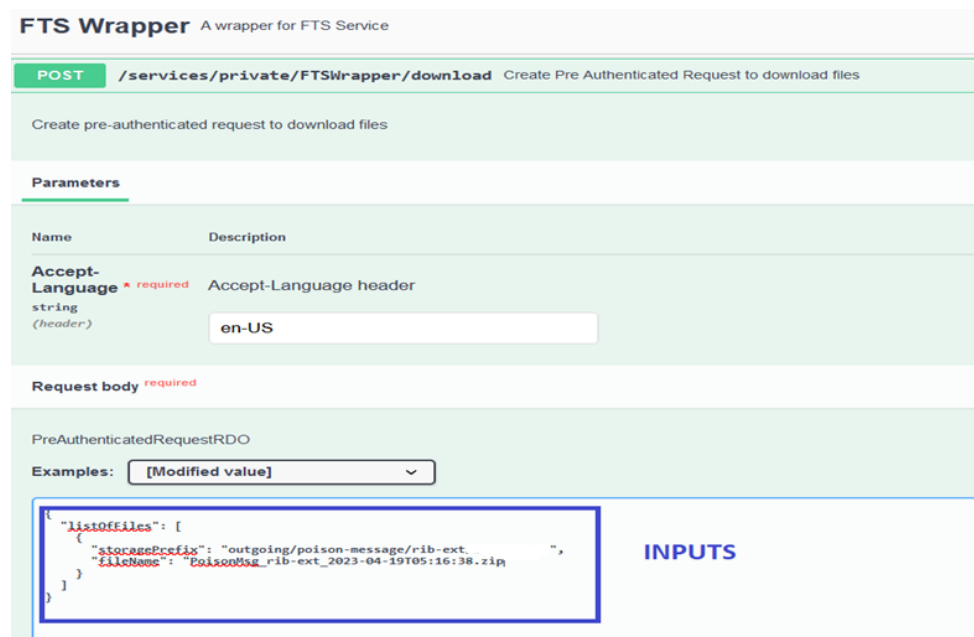
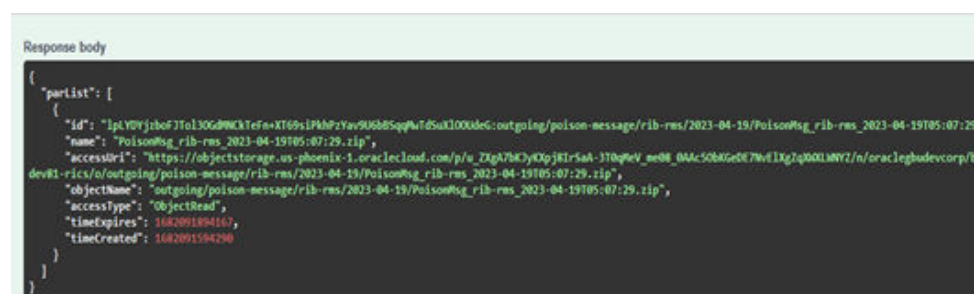


Figure 1-27 Server Response



6. Download the file.
Use the accessUri from the previous step to download the zip file.
curl <accessUri> -o <fileName>.zip
7. Extract the archive file. Do not change the file name but change extension of all files to .xml. Correct the RibMessage in each xml file. Archive the all the .xml files. This file needs to be uploaded back to object store.
8. Generate the Pre-Authenticated Request to upload files to object store.
storagePrefix pattern: incoming/poison-message/rib-<app>

Figure 1-28 Generate the Pre-Authenticated Request

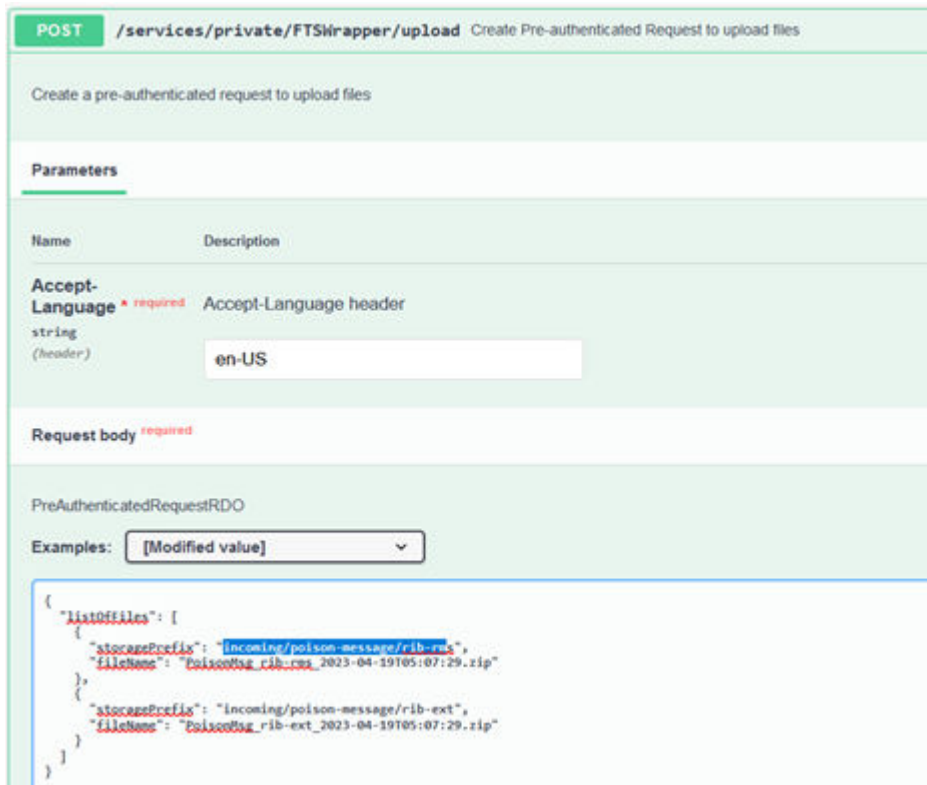
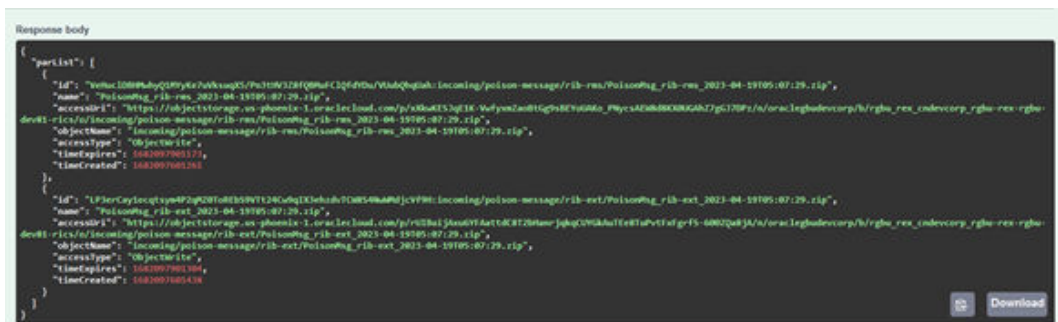


Figure 1-29 Server Response



9. Upload the files using accessUri from above response.
curl <accessUri> --upload-file <unique_filename>.zip
10. RIB periodically downloads the file from incoming/poison-message storagePrefix and extracts it to needed location in RIBDomain.
11. Subscribing retry adapter processes the RibMessage present in the extracted file.

Owner: Who configures in Production

Service Implementer /Customer

Support

Leverage Oracle Support

Attend a session on Working Effectively with Support (WEWS) to learn about support policies and best practices when working with Oracle Support. Oracle Support representatives are ready 24/7 to answer questions and address issues about your service. Access the Oracle Support Contacts Global Directory to find the Oracle Support Hotline for your country, and explore the page on Working Effectively with Oracle Support - Best Practices found on My Oracle Support under **Doc ID 166650.1**.

Get Connected

Register for RGPU support communities:

- Use My Oracle Support Community (**Doc ID 2299812.1**) to post technical questions and get resolution on technical issues.
- See "Getting Started" to learn how to use the Support Community.
- Use The RACK to view informative resources and participate in discussions around Retail Solutions.

Frequently Asked Questions

OCI IAM Activation

Since the Retail Integration cloud services are installed using the activated OCI IAM details, it is important to ensure any activation concerns are resolved during the pre-provisioning/provisioning period, as making changes after your Retail Integration cloud services are provisioned may require extended downtime.

What should I do if I cannot activate OCI IAM into an existing Oracle Cloud Account?

Inform your CSM or sales representative if you run into issues, providing the following information:

- Existing Oracle Cloud Account name
- Subscription ID of a service in the account

- Administrator e-mail for the account

What do I do if I experience errors or failures while attempting to activate OCI IAM?

The administrator e-mail address must match the e-mail which received the activation notification. If this does match and you are still running into issues, inform your CSM or sales representative, providing the following information:

- Intended activation approach (new Oracle Cloud Account or activate within an existing)
- Any error or failure messages received - include screen shots if possible

Can I use another identity management solution?

Only OCI IAM is supported in Retail Integration Cloud Service implementations, however OCI IAM could also be integrated with external identity management providers, like Active Directory, using its APIs.

I have multiple pre-prod environments and want to have different security configurations for the same users/roles in each, can I do that?

The recommended approach is to create roles in OCI IAM (and ORAAC) that reflect the configuration needs for each environment. Or you could consider creating two user IDs for the same person to reflect the different role configurations that they need to test.

Why do I see other users in my OCI IAM instance (for example, batchuser)?

The Oracle Cloud Operations team will also seed a set of integration users required by the solutions as part of the provisioning process. These are users used for integration or internally for batch and other processing and should not be deleted.

Index