

Oracle® Banking Microservices Architecture

SaaS to PaaS Data Replication User Guide



Innovation Release 14.8.2.0.0

G54091-03

April 2026

ORACLE®

Copyright © 2026, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

Contents

1 SaaS Self Service UI

1.1	Initiate Data Export	3
1.1.1	Profile Flow	4
1.1.1.1	Key Management System(KMS) Selection	4
1.1.2	Initiate Data Export	7
1.2	Integrated Extract	10
1.2.1	Extract Management	11
1.2.1.1	Create Extract	12
1.2.1.2	Manage Extract	13
1.2.1.3	CSN Based Extract Creation	16
1.2.2	Checkpoint	19
1.2.3	Parameters	20
1.2.4	Statistics	21
1.2.5	Report	21
1.3	KMS Profile Management	22
1.4	Key Management	25
1.5	Administration Service	27
1.5.1	Operator User Creation	27
1.5.2	Trails	28
1.5.3	TranData	29
1.6	Distribution Service	31
1.6.1	Path Info	32
1.6.2	Path Stats	33

2 Data Replication PaaS Setup

2.1	Overview	1
2.2	OCI Setup	1
2.2.1	Administration	2
2.2.2	Identity and Security	3
2.2.3	OCI Policies	4
2.2.4	Network Setup	5
2.2.5	OCI Vault Setup	9
2.2.5.1	Create a Vault	9

2.2.5.2	Create Master Encryption Key	11
2.2.6	OCI Autonomous Database Setup	12
2.2.6.1	Create and Configure the ATP Instance	12
2.2.6.2	Connect to the ATP Instance	16
2.3	Import Data from Object Storage	17
2.3.1	Downloading dump with PAR URL	17
2.3.2	Database Setup	19
2.3.3	Troubleshooting	20
2.4	OCI GoldenGate Deployment Setup	21
2.4.1	Create an OCI GoldenGate Deployment	21
2.4.2	Create the Connection	26
2.4.3	Configure OCI GoldenGate	29
2.4.4	Target Initiated Distribution Path	36
2.4.4.1	Target OCI GoldenGate Deployment in devcorp	41

3 Functional Activity Codes

Index

Preface

- [Purpose](#)
- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Conventions](#)
- [Screenshot Disclaimer](#)
- [Acronyms and Abbreviations](#)
- [Disclaimer](#)

Purpose

This guide provides a step-by-step approach for Oracle Banking Cloud Services SaaS users to replicate data securely from OCI SaaS tenancy to their OCI PaaS tenancy.

Audience

This Guide is primarily for users who are responsible for provisioning and activating Oracle Banking Cloud Services, for adding other users who would manage the services, or, who want to develop Oracle Banking Cloud Service.

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

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 user supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that user enter.

Screenshot Disclaimer

Information used in the interface or documents are dummy, it does not exist in real world, and its only for reference purpose.

Acronyms and Abbreviations

The following acronyms and abbreviations are used in this guide:

Table Acronyms and Abbreviations

Acronym/ Abbreviation	Description
API	Application Programming Interface
OCI	Oracle Cloud Infrastructure
KMS	Key Management System

Disclaimer

User should make a note of the following:

1. Customers opting out of BYOK will not have their OCI Vault profiles enabled.
2. Non-subscribed customers will not see the Data Replication menu.
3. Expired PAR URLs require regeneration through the UI.

1

SaaS Self Service UI

This topic describes about SaaS self service UI.

The SaaS users lack direct access to their data schemas. Hence, by following the data replication process, it enables creation of local data copies via a secure and configurable replication process. It also facilitates use of replicated data for reporting, backups, or custom workflows.

The objective is to provide user with tools to:

- Export data from SaaS tenancy.
- Securely store and manage replicated data.
- Monitor and manage replication configurations via a self-service UI.

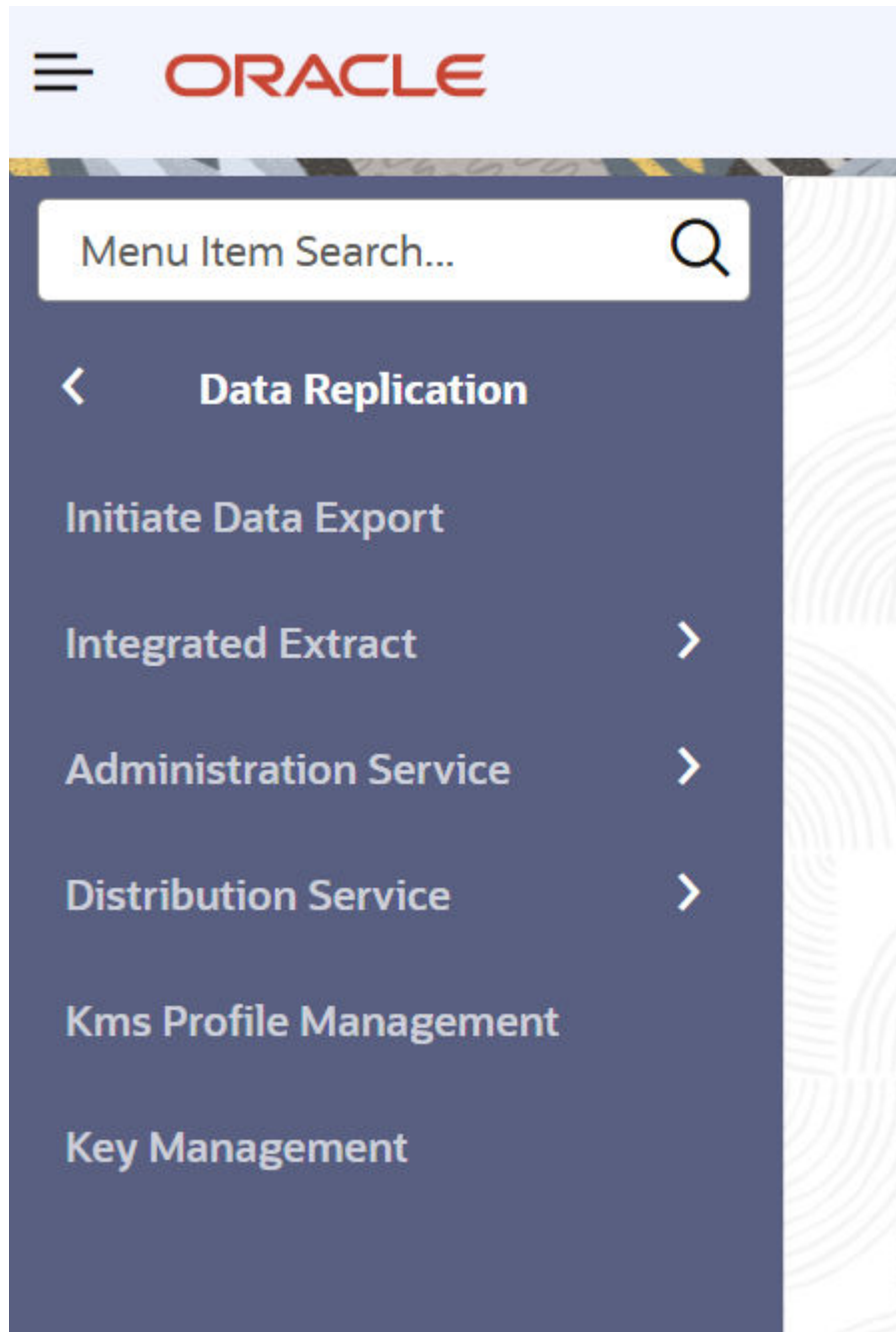
The technologies used are as follows:

- **Backend:** Spring Boot
- **Frontend:** Oracle JET (OJET)
- **Database:** Oracle Database with OCI GoldenGate

This topic outlines the tasks and responsibilities that the customer must fulfill to successfully enable SaaS-to-PaaS data replication using **Oracle Cloud Infrastructure** (OCI) GoldenGate.

To ensure proper configuration, security, and functionality of the data replication system, refer the topics below.

Figure 1-1 Data Replication Home Page



- [Initiate Data Export](#)
This topic describes the systematic instructions to initiate the data export.
- [Integrated Extract](#)
This topic provides information on integrated extracts.
- [KMS Profile Management](#)
This topic provides information about KMS profile management.
- [Key Management](#)
This topic provides information about key management.

- [Administration Service](#)
This topic describes the systematic instructions about Administration Service.
- [Distribution Service](#)
This topic provides information on distribution service

1.1 Initiate Data Export

This topic describes the systematic instructions to initiate the data export.

To begin the data replication process, users must first complete the following key steps:

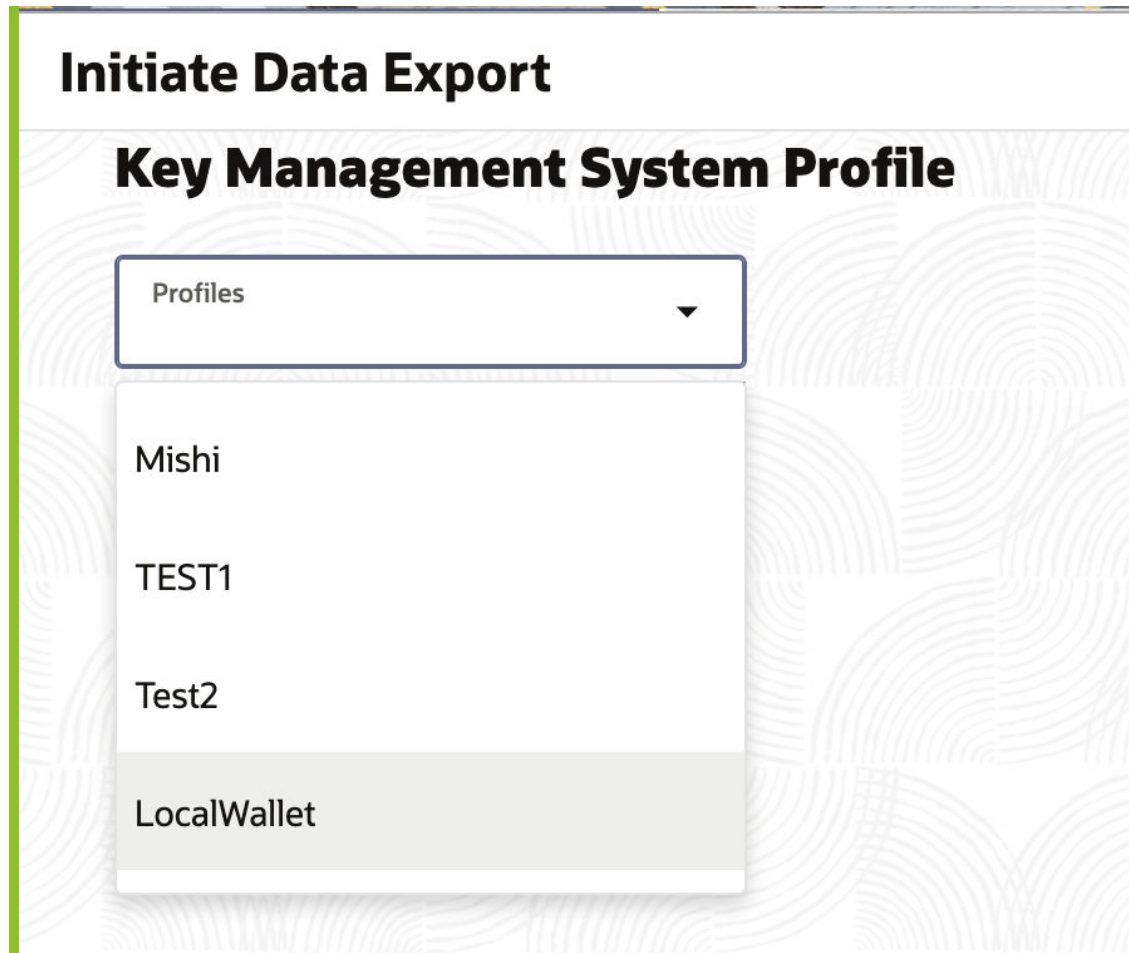
- Select a Profile
- Create an Operator user
- Perform Data Export initialization.

These can be performed through the Self-Service UI by following the steps below:

Seed Data Setup Overview:

- Generate an initial dump of the SaaS database by using the Self-Service UI. Users can select their preferred schema during this process.
- Utilize the Pre-Authenticated Request (PAR) URLs provided by Oracle to securely download the initial dump files from Oracle Cloud Infrastructure (OCI) Object Storage.
- Import the downloaded data into the target environment using the Oracle `impdp` utility, specifying the designated encryption password as required

Figure 1-2 Data Export Landing Page



- [Profile Flow](#)
This topic provides information on profile flows.
- [Initiate Data Export](#)
This topic describes the systematic instructions to initiate an export.

1.1.1 Profile Flow

This topic provides information on profile flows.

To encrypt the export DMP files and trial files, KMS profile allows the customer to configure the below Encryption Profile Type:

- [Key Management System\(KMS\) Selection](#)
This topic provides information about KMS profile .

1.1.1.1 Key Management System(KMS) Selection

This topic provides information about KMS profile .

To ensure the encryption of exported Dump and trial files, the KMS profile enables customers to configure one of the following Encryption Profile Types:

- Local Wallet
- OCI Vault
- [Local Wallet](#)
This topic provides information on local wallet.
- [OCI Vault](#)
This topic provides information on OCI vault.

1.1.1.1.1 Local Wallet

This topic provides information on local wallet.

A **Local Wallet Profile** is a **secure profile** stored within a GoldenGate **deployment's local wallet**.

It defines **how GoldenGate authenticates and encrypts** internal and external communication.

If the customer has not subscribed to the BYOK SKU, the system automatically assigns the **Local Wallet** type as the default encryption profile for that customer. User can paste **Public Key** and the **preferred schema list** for export, then click **Next** to proceed.

Steps to **generate an SSH key pair and convert them to PEM format**

1. Create a new SSH key pair using the `ssh-keygen` command:

```
ssh-keygen -t rsa -b 4096 -f my_ssh_key
```

2. Convert the SSH **Public Key** to PEM Format

```
ssh-keygen -f my_ssh_key.pub -e -m PKCS8 > my_ssh_key.pub.pem
```

3. Convert the SSH Private Key to PEM Format

```
ssh-keygen -p -m PEM -f my_ssh_key
```

A sample public key in PEM format will look like the following:

```
cat my_ssh_key_public.pem
```

Figure 1-3 Sample public key in PEM format

```

-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAtuhgVpQmjWAdiA9ei+fc
CfhSIAGME857ZCIj3PwyZIbdiKmpvfFetl2s/77azy6LkfhWT14ZvvJxmZzPi8BO
rPubrhPvNpjgg05934fQKb2YQKSTKTtNh+UhcXWhqtUIzgDrCXyRB9K6j1AqW0cI
SIPIeat5Xn04MzdLI2A7bX2SL151hh4oRyhxFmfqKJrCe5wueRpuoZ3vr4jm8gc0
5j5e1Rur41CC/wCpjn9nxfVoJLI0d1pvUnbF0HekctXQ6bzFQHFhw3nhmFqJf2Jm
Y1ZmurfWFx5/+vOKY48of/fLT+3cNm9A7PfTzGM5xgZc+LOLL7kwleVhP6UaSPG
wQvu4JArQWsn908hJzEcnSJms6vVMcwFXwv/OpvQayFHBA+iEFNwvWdmL47Cw/O
pCwMJJsONdtFm3cCcL79/eGud0EwBlS04AYvLbPr9wAXcEFgaEHU0ga9jq0tUq6bN
UY2wxHDDcMf7QM8E1Y4B3w4YVHjIDLbEc4MVJW8B6pu7dTYVwWwpg1uvMLhSdqwj
nSm08Yg0ddeGjzdSs/0l8R8z8d1QYTh7x/4q5kkwoMTFnRWm+I6/BRflecQ2TGTD
xSCwwzQeA7uzHrY6aAvON9G4lGlrJhFs6HG3jZFzFQzoKjUevw+RmuwSeRBn+c6p
kcqya3y6ahJNi15y+CWEF1ECAwEAAQ==
-----END PUBLIC KEY-----

```

Note

Encryption Profile Type **Local Wallet** comes with OCI GoldenGate deployment and Customer will not be able to create multiple KMS Profile with Encryption Profile Type **Local Wallet**.

Figure 1-4 Local Wallet Operation

Initiate Data Export

Local Wallet Profile

Profile Name	Description
LocalWallet	Local Wallet
Encryption Profile Type	Default Profile
Local Wallet	yes ▼
Paste Public Key (PEM Format)	
<div>-----BEGIN PUBLIC KEY----- MIICIj</div> <div>Required</div>	
<div>Next</div>	

1.1.1.1.2 OCI Vault

This topic provides information on OCI vault.

If the customer has opted for **BYOK**, Users can select the **KMS Profile** that they want to use to encrypt the initial export dump files. Before performing this step, a KMS profile must be created in the **KMS Profile Management** page. Follow the steps outlined in **Section 1.3 – KMS Profile Management** to create the required profiles.

Figure 1-5 OCI Vault

The screenshot shows the 'Initiate Data Export' form with the following fields and values:

Field	Value
Profile Name	TEST1
Encryption Profile Type	ocikms
Default Profile	no
Crypto Endpoint URL	https://bzscrc3qaabha-crypto.kms.us-phoenix-1.oracleclo...
Tenancy OCID	ocid1.tenancy.oc1.aaaaaaaamuhda4xcynzumstqiwxb5d...
Key OCID	ocid1.key.oc1.phx.bzscrc3qaabha.abyhqljrzdrlrpekkqkqdat...
User OCID	ocid1.user.oc1.aaaaaaaahajictilebosivzb7sctn6i6mqvjvjk...
API Signing Key	TEST1_alias
Key Fingerprint	14:a0:e3:6f:f0:82:c5:8c:e3:5e:cf:df:2b:99:82:e8
Tenant Environment	dev
Schema List	<input type="text"/>

At the bottom left is an 'Initiate' button. At the bottom right of the Schema List field is a 'Required' label.

1.1.2 Initiate Data Export

This topic describes the systematic instructions to initiate an export.

The user can export data from the **SaaS tenancy** to **Object Storage** with **encryption**.

To initiate data export:

1. Select the encryption profile from the following options:
 - **OCI Vault:** Available for BYOK customers.
 - **Local Wallet:** Default option for other customers.
2. Pass the list of required Schemas in the **Initiate Export** screen as given below
3. Initiate the export process and wait for the **Export Status** to be **SUCCESSFUL**..
4. Retrieve PAR URLs for:

- Data dump files.
 - Encryption keys (ciphertext and AES-256 key).
5. Download the exported data using the provided PAR URLs.

Figure 1-6 Initiate Data Export

Initiate Data Export

Profile Name

LocalWallet

Description

Local Wallet

Encryption Profile Type

Local Wallet

Default Profile

yes

Data Export

Tenant Environment

dev

Schema List

PARTY_BP

Required

Initiate

If this is the first time performing the export, the user will receive a **confirmation** that the export has been successfully initiated.

If an export has been run previously, the UI will display a **summary of the last initiated export** instead of starting a new one. In this case, the user can view the **Data Export Status** page, which shows details of the prior export, such as the **timestamp, status, and PAR links**.

Figure 1-7 Initiate Data Export Status

Initiate Data Export

Data Export Status

Request ID

18052

Export Status

SUCCESSFUL

Seed Data PAR URL

View URL(s)

Seed Dump Expiration

2025-10-23T09:40:30.000+00:00

Encryption PAR URL

View URL(s)

Encryption Expiry

2025-10-23T09:40:35.000+00:00

Cwallet.SSO PAR URL

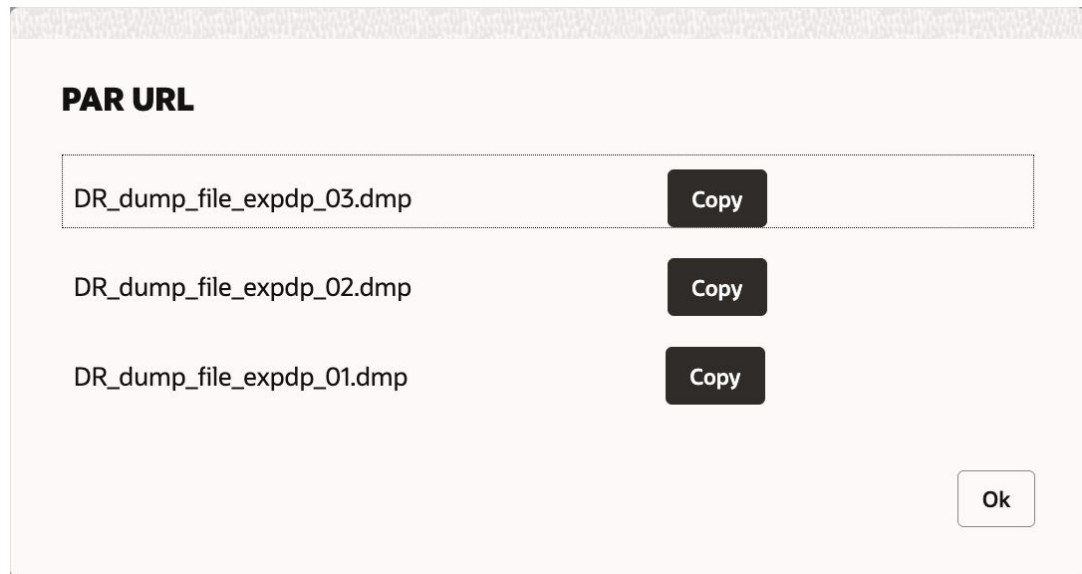
View URL(s)

Cwallet Expiration

2025-10-23T09:40:40.000+00:00

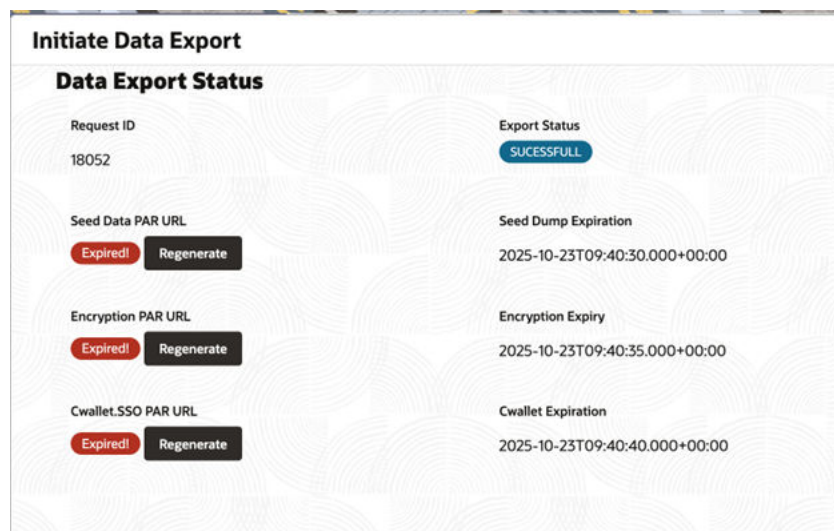
Users can click on **View URL** to retrieve the Pre-Authenticated Request (PAR) URLs for the respective **objects and dump files**.

Figure 1-8 PAR URL - objects and dump files



The PAR URLs generated for the dump files are **time-sensitive** and remain valid for approximately **2 hours** from the time of generation. If a PAR URL expires before the file is downloaded, a new URL can be generated by clicking the **Regenerate PAR URL** button on the Data Export Status page.

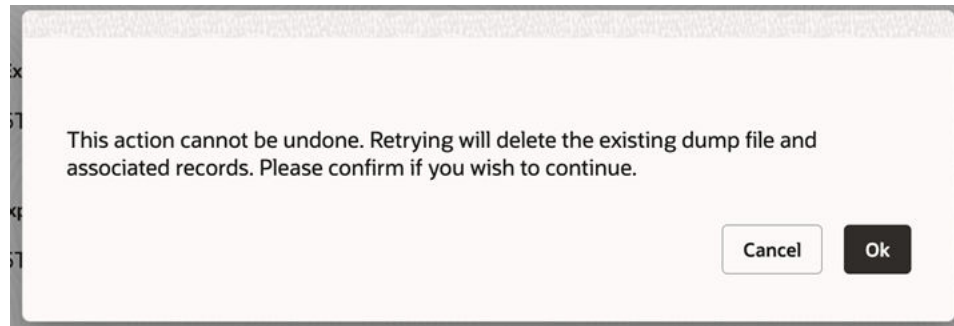
Figure 1-9 Regenerate PAR URL



Additionally, the **exported dump files** remain available in Object Storage for **7 days** from the time of export. After this retention period, the files are automatically expired and removed, and the export process must be re-initiated to generate the files again. Users can

also re-run the Initial Export at any time by clicking the Retry Export option available in the top-right corner of the page.

Figure 1-10 Retry Export option



Prerequisites Before Proceeding:

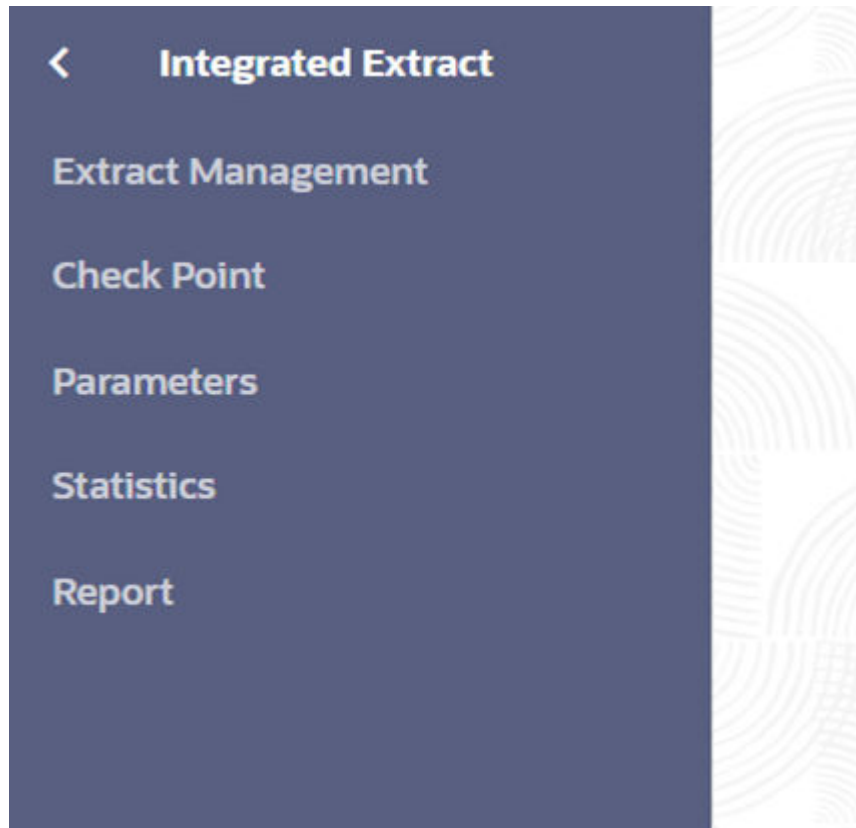
Before proceeding further to configure ongoing replication (GoldenGate Extract), ensure the following:

- Target **PaaS environment** is set up as per the *Data Replication PaaS Setup Guide*.
- **Oracle Autonomous Database** exists in the target tenancy for importing the dump.
- **OCI GoldenGate deployment** is configured in the SaaS tenancy.
- Required **network connectivity** and **IAM policies** are in place.

1.2 Integrated Extract

This topic provides information on integrated extracts.

Figure 1-11 Integrated Extract menu



Once the initial data export is complete and the target environment is ready, the next step is to configure **ongoing replication** of incremental changes.

This is done by setting up an **Integrated Extract** in GoldenGate through the self-service UI. The extract continuously captures transactions from the **source SaaS database** and streams them to the **target**.

The UI provides options to **create, view and manage** this extract process. The main operations for controlling the extract are described in the following sections.

- [Extract Management](#)
This topic describes the systematic instructions to Extract Management.
- [Checkpoint](#)
This topic provides information about checkpoint.
- [Parameters](#)
This topic provides information about view/edit parameters.
- [Statistics](#)
This topic provides information about statistics.
- [Report](#)
This topic provides information about report files.

1.2.1 Extract Management

This topic describes the systematic instructions to Extract Management.

- [Create Extract](#)
This topic describes the systematic instructions to create an extract.
- [Manage Extract](#)
This topic describes the systematic instructions to manage an extract.
- [CSN Based Extract Creation](#)
This topic describes the systematic instructions to create CSN Based Extract Creation.

1.2.1.1 Create Extract

This topic describes the systematic instructions to create an extract.

The user can create a new extract by selecting the **preferred start time** and **encryption profile**, then clicking **Create**.

Once initiated, the system sets up the GoldenGate extract in the backend. This process may take a short time.

If the extract is created successfully, it will appear in the UI with its **details and status**. Initially, the extract will typically be in a **Stopped** state (not yet running).

Note

A user can have **only one active extract** at a time for a given source. The UI will prevent creating a second extract if one already exists. To recreate an extract, the existing one must be **deleted first**. If no extract exists, the UI will indicate this, and the **Create Extract form** will be available.

Figure 1-12 Create Extract

Integrated Extract

Process Name	Begin
<input type="text" value="EXTRACT"/>	<input type="text" value="Now"/>
Trail Name	Trail Subdirectory
<input type="text" value="it"/>	<input type="text" value="traildir"/>
Select a KMS Profile	Operator User
<input type="text" value="LocalWallet"/>	<input type="text" value="bs123456"/>
Registration Options	
CSN	Share
<input type="text"/>	<input type="text" value="Automatically"/>
CSN List	
<input type="button" value="Create Extract"/>	

The above page is displayed when the user has **not created any extracts or Deletes an existing Extract**.

The user can create a new **Integrated Extract** through the self-service UI by either selecting **Begin**

Now to start immediately or specifying a **CSN (Commit Sequence Number)** to begin capturing

changes from a particular point in the source database.

- **Begin Now:** The extract starts immediately from the current point in the source database.
- **CSN:** The extract begins capturing changes from a specific System Change Number.

For CSN option the user can select an CSN from the available values by clicking the **CSN list** option located below the CSN registration Option field. The same is explained in detail in **Section 1.2.1.3 – CSN Based Extract Creation**

For **Begin Now**, the CSN field under the CSN registration Option can be left **empty**, as the extract will start immediately from the current point in the source database.

Figure 1-13 CSN Details

CSN Details			✕
Start SCN	Date of Build	Name	
45714000933857	10/22/2025 10:41:54	+RECO/E9H1POD/ARCHIVELOG/2...	
45709776024633	10/21/2025 10:41:52	+RECO/E9H1POD/ARCHIVELOG/2...	

Figure 1-14 Extract Details Page

Extract Management

Trail Name

DR

Trail Subdirectory

traildir

Encryption Profile

LocalWallet

Encryption Profile Type

localWallet

Operator User

OperatorINT2

Default Profile

Status

Process Name

DEVTRAT

Status

Running

Begin Value

now

View Details

Start

Stop

Force Stop

Delete

1.2.1.2 Manage Extract

This topic describes the systematic instructions to manage an extract.

Once the extract is successfully created, the user will see the **extract details** in the UI along with operational buttons, including **Start**, **Stop**, **Force Stop**, **Delete**, and **View Details**.

The functions of the operational buttons are explained in detail below:

- **Start** : Furthermore, the extract can be started based on the user's choice by selecting either **Last Checkpoint(default)** to start from Extract creation point or **Now** option to start immediately or specifying a **CSN** to begin from a particular commit point in the source database or specifying to start **After CSN**. Once the extract starts successfully, its status will be updated to **Running**. While running, the extract continuously writes captured transactions to **trail files**, which are then delivered to the target through GoldenGate.

Figure 1-15 Start Extract with options

Select Start Type

Choose when to start the replication

Last Checkpoint (default)

Now

CSN

After CSN

Discard Submit

After selecting the desired action, a **Start Confirmation** prompt will appear. Click **Yes** to proceed with starting the extract.

Figure 1-16 Start Extract

Integrated Extract

Trail Name	Trail Subdirectory	Status	Process Name	Encryption Profile	Encryption Profile Type	Status
np	preprod		TESTEXR1	testprofiledev1		

Operator User: admin9

Start Confirmation

Are you sure to Start the Replication

No Yes

View Details View Parameters Start Stop Force Stop Delete

- **Delete** : This action permanently removes the extract process configuration. It is **irreversible** and deletes the extract completely. The user cannot delete an extract when its status is **Running**. The extract must first be stopped before it can be deleted.

Figure 1-17 Delete Extract



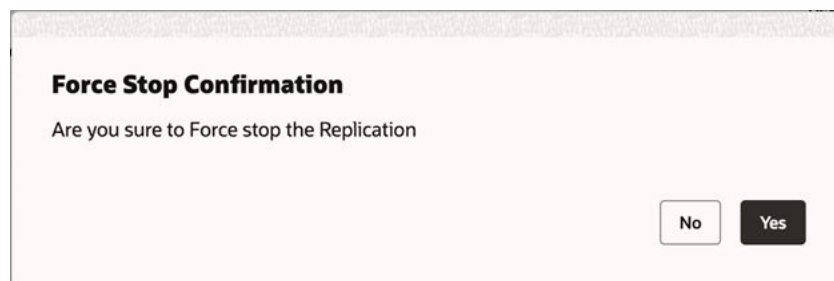
- **Stop** : This action gracefully stops the extract process, allowing it to complete any ongoing operations before halting. Once the extract is successfully stopped, its status is updated to **Stopped**.
The user can also use this action to **pause replication temporarily** without deleting the configuration — for example, during maintenance activities.

Figure 1-18 Stop Extract



- **Force Stop Extract**: This action immediately terminates the extract process without waiting for ongoing operations to complete. Once the extract is forcefully stopped, its status is updated to **Abended**.

Figure 1-19 Force Stop Extract



- **View Details**: This action displays detailed information about the extract, including the **trail name**, **lag details**, **trail sequence** and **trail size**.

Figure 1-20 View Details

Extract Details	
Trail Name	Trail Sequence
it	83
Trail Size	Trail Subdirectory
500	traildir
Since Lag Reported (sec)	Lag (sec)
6	80
Last Started (UTC)	
2025-10-23T09:15:41.694Z	

1.2.1.3 CSN Based Extract Creation

This topic describes the systematic instructions to create CSN Based Extract Creation.

When creating an **extract** in Oracle GoldenGate, the **CSN (Commit Sequence Number)** option allows the user to start capturing transactions from a **specific point in the source database**. This Ensures the replication begins from a well-defined commit point, which is useful for resuming replication after maintenance, downtime, or for selectively capturing a subset of transactions.

To use the **CSN option** for an existing SaaS database, follow the steps below:

1. In PaaS OCI Goldengate Console:
 - Customer stops the existing Target-Initiated Distribution Path and records Source Sequence Number and RBA Offset.
2. In OBCS SaaS Self-Service UI:
 - Delete the existing Extract
 - Use the **SCN List** button below the registration Options to view available SCNs
 - Select an **SCN** and create a new Extract

Figure 1-21 Status



- Register the **SCN** in **Registration Options** and Select **Begin as Now** from the UI

Figure 1-22 Register SCN

Integrated Extract

Process Name <input type="text" value="EXTRACT"/>	Begin <input type="text" value="Now"/>
Trail Name <input type="text" value="it"/>	Trail Subdirectory traildir
Select a KMS Profile <input type="text" value="LocalWallet"/>	Operator User bs123456

- **Start** the Extract with Last Checkpoint(default) option and verify the Extract by checking the **Reports** in the Extract View.
- Wait for the extract to position to the **current timestamp** as below, then **Stop** the Extract.

Figure 1-23 Current Timestamp

```

2026-02-18 06:42:57 INFO OGG-01971 The previous message, 'INFO OGG-02776', repeated 1 times.
2026-02-18 06:42:57 INFO OGG-01052 No recovery is required for target file vu000000000, at RBA 0 (file not opened).
2026-02-18 06:42:57 INFO OGG-01478 Output file vu is using format RELEASE 191/211/231.
=====
** Run Time Messages **
=====
2026-02-18 06:42:57 INFO OGG-30594 Extract BxFormatter thread is resumed.
2026-02-18 06:42:57 INFO OGG-30594 Extract BxAsyncTrans Reader thread is resumed.
2026-02-18 06:42:57 INFO OGG-01515 Positioning to begin time Feb 18, 2026 6:42:30 AM.

```

- Now click the **Edit Extract** option in top right corner the UI to reposition the Extract to the chosen **SCN**.

Figure 1-24 Edit Extract option

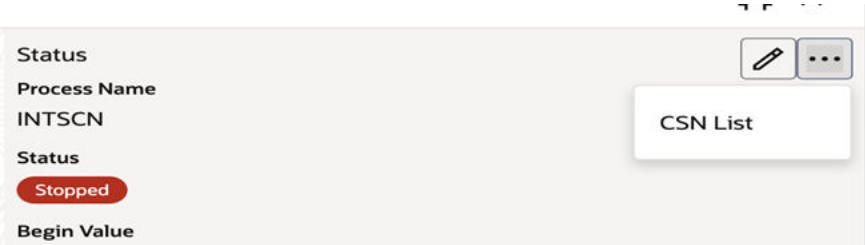


Figure 1-25 Alter Extract



- Restart the Extract with **CSN option** by providing **CSN** Value and confirm repositioning via **Reports and Checkpoint lag**.

Figure 1-26 Select Start Type

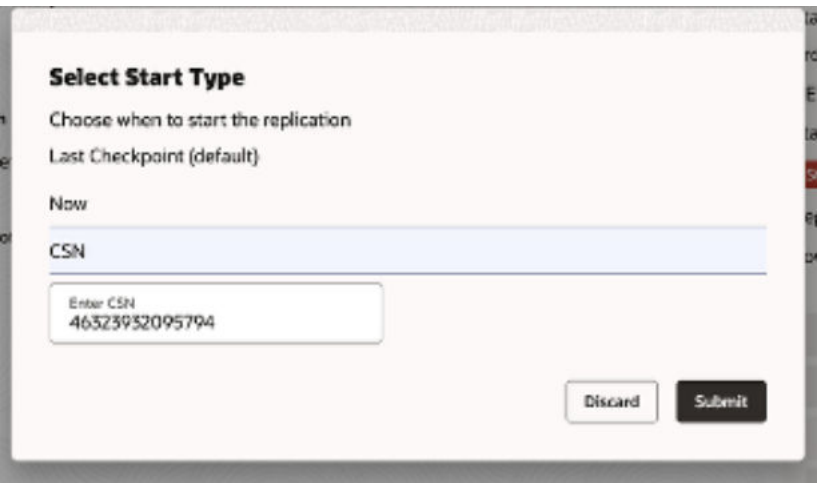


Figure 1-27 Select Start Type

```

2026-02-18 06:50:37 INFO  OGG-01056 Recovery initialization completed for target file vu000000000, at RBA 7157, CSN
46324165158970.

2026-02-18 06:50:37 INFO  OGG-01478 Output file vu is using format RELEASE 19.1/21.1/23.1.

2026-02-18 06:50:38 INFO  OGG-02776 Native data capture is enabled for Oracle NUMBER data type.

2026-02-18 06:50:38 INFO  OGG-01026 Rolling over remote file vu000000000.

*****
**      Run Time Messages      **
*****

2026-02-18 06:50:38 INFO  OGG-30594 Extract IXFormatter thread is resumed.

2026-02-18 06:50:38 INFO  OGG-30594 Extract IXAsyncTrans Reader thread is resumed.

2026-02-18 06:50:38 INFO  OGG-02823 Positioning to SCN 46323932095794.

2026-02-18 06:50:47 INFO  OGG-02845 Position of first record processed Sequence 0, RBA 0, SCN 46323932095806,
Time Feb 18, 2026 5:55:48AM.

2026-02-18 06:50:52 INFO  OGG-02557 Heartbeat table GGADMIN.GG_HEARTBEAT_SEED metadata is resolved and will
write to trail file vu.

```

- As the lag decreases, the **Statistics** keeps updating with the historical data capture metrics
3. In PaaS OCI Goldengate Console:
- Create a new Target-Initiated Distribution Path using the Source Sequence Number and RBA Offset captured earlier.
 - Start and validate historical data capture in Statistics
 - Delete the previous stopped distribution path

1.2.2 Checkpoint

This topic provides information about checkpoint.

Checkpoint

The **Checkpoint** option on the Extract Detail page in Oracle GoldenGate allows the user to view and manage the extract's **current replication position, Recovery position, Trail Position and Checkpoint Updates**.

Figure 1-28 Check Point

Check Point

Filename: it
Timestamp: 2025-10-23T15:37:21.178Z
Sequence: 85
Offset: 556283
Trail Subdirectory:

Input Checkpoints

Checkpoint	Timestamp:	Thread	Sequence	Offset	CSN
starting	2025-10-23T15:31:09.000Z	1	0	0	N/A
recovery	2025-10-23T15:36:44.000Z	8	18321	9269441624	45718751074662
current	2025-10-23T15:37:19.000Z	8	18321	9336472116	45718753674794
boundedRecoveryPrevious	2025-10-23T15:31:11.377Z	1	0	0	N/A
boundedRecoveryBegin	2025-10-23T15:31:11.377Z	1	0	0	N/A
boundedRecoveryEnd	2025-10-23T15:31:11.377Z	1	0	0	N/A

Output Checkpoints

Checkpoint	Timestamp:	Offset	Name	Trail Subdirectory	Sequence	Sequence Length
current	2025-10-23T15:37:21.178Z	556283	it	N/A	85	9

1.2.3 Parameters

This topic provides information about view/edit parameters.

View/ Edit Parameters

The **Extract Parameter View** page in Oracle GoldenGate displays all the configuration parameters for a specific **extract process**. It allows users to review and verify settings. Additionally, the user can click the **edit** icon in the top-right corner to modify the extract parameter file as needed and click **Submit**.

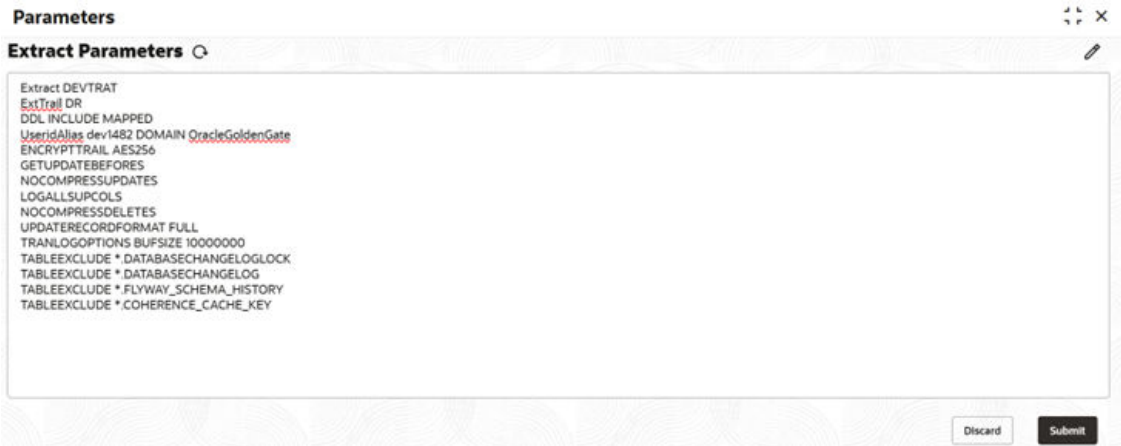
Figure 1-29 View Parameters

Parameters

Extract Parameters

Extract DEVTRAT
ExtTrail DR
DDL INCLUDE MAPPED
UserIdAlias dev1482 DOMAIN OracleGoldenGate
ENCRYPTTRAIL AES256
GETUPDATEBEFORES
NOCOMPRESSUPDATES
LOGALLSUPCOLS
NOCOMPRESSDELETES
UPDATERECORDFORMAT FULL

Figure 1-30 Edit Extract Parameters



1.2.4 Statistics

This topic provides information about statistics.

Statistics

The **Statistics** option on the Extract Detail page in Oracle GoldenGate provides **quantitative metrics** about the extract's performance and activity. It displays the number of **table operations**, including **inserts**, **updates**, and **deletes**, captured by the extract.

User can select from three options , Whether they want last hour stats, or daily or Total stats.

Figure 1-31 Statistics

Statistics Table

Hourly Daily Total

Filter

Table Name	Inserts	Updates	Inserts	Deletes	Truncates
DDL	115	0	0	0	0
PLATO_RULE_PLATO_TM_RULESLOG	423115	0	0	0	0
PLATO_ORCHTASK_ALLOC_CTRL	296	158817	0	0	0
SMS_PLATO_EVENTHUB_IN_LOG	57077	57077	0	0	0
SMS_SMS_TB_RBAC_LOG	75947	0	0	0	0
PLATO_ORCHTASK	78430	302716	0	34	0
PLATO_ORCHWORKFLOW	20805	49039	0	17	0
OBARACCPACC.CDDA_PP_TM_CUSTOMER_ACCOUNT_BASIC_DETAILS	2125	6255	0	0	0
OBARACCPACC.CDDA_PP_TM_ACCOUNTSTATUS	1551	37	0	0	0
OBARACCPACC.CDDA_PP_TM_ACCOUNTSTATUS	1518	270	0	0	0

Refresh Interval

1.2.5 Report

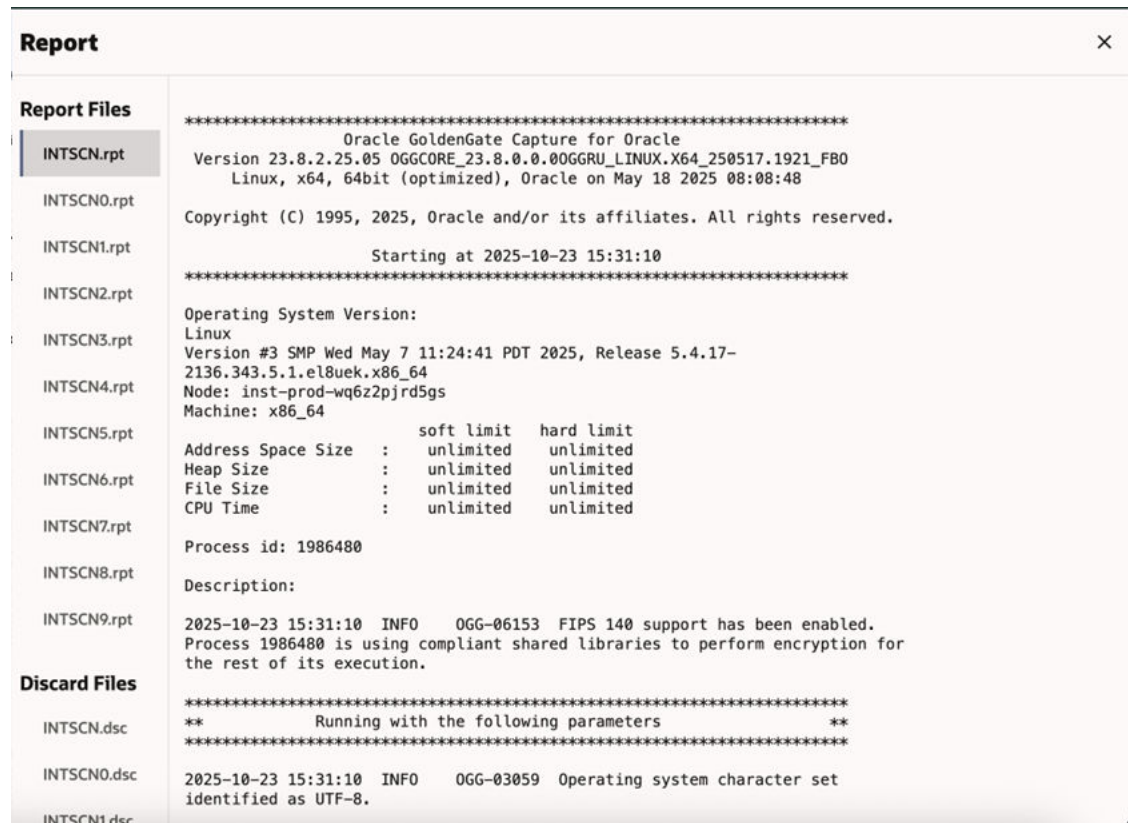
This topic provides information about report files.

Report Files

The **Report** option provides a detailed view of the extract's operational metrics and configuration. The user can view **real-time process details and logs** for the extract by

clicking on the **.rpt** or **.dsc** file on the page. This provides a live view of extract operations, including transaction capture, trail file generation, and any warnings or errors.

Figure 1-32 Report Files



1.3 KMS Profile Management

This topic provides information about KMS profile management.

In the **KMS Profile Management** view, the user can manage **encryption profiles** used for **data export** and **trail file encryption**. This allows secure handling of sensitive data during export and replication by leveraging encryption keys managed in the **OCI Key Management Service (KMS)**.

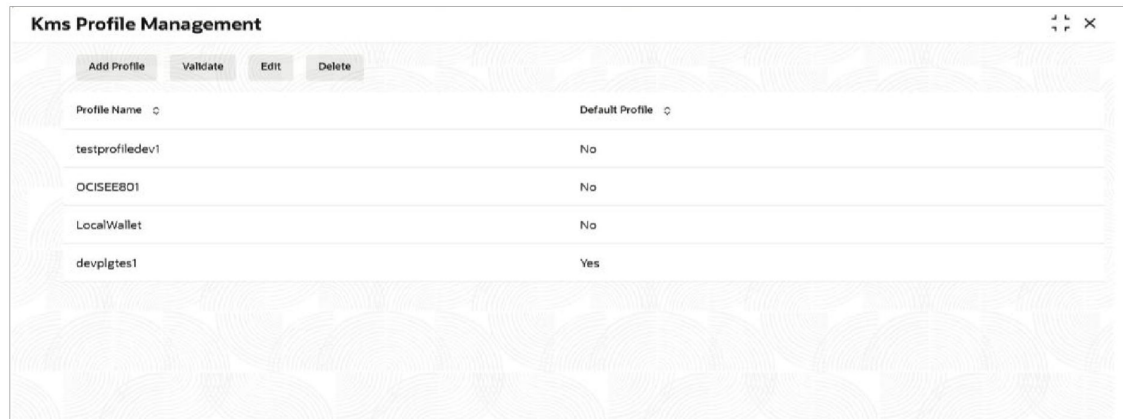
Steps to Create a KMS Profile:

- The customer must create an OCI service account (an OCI IAM user account without a password) and generate an associated API key for authentication.
- Click **Create Profile** to open the **Create KMS Profile** section.

If KMS Profiles already exist, the user can simply select an existing profile from the drop-down list and click **Save** to proceed.

Note: The customer can create multiple **KMS Profiles** with the **Encryption Profile Type** set to **OCI Vault**.

Figure 1-33 KMS Profile



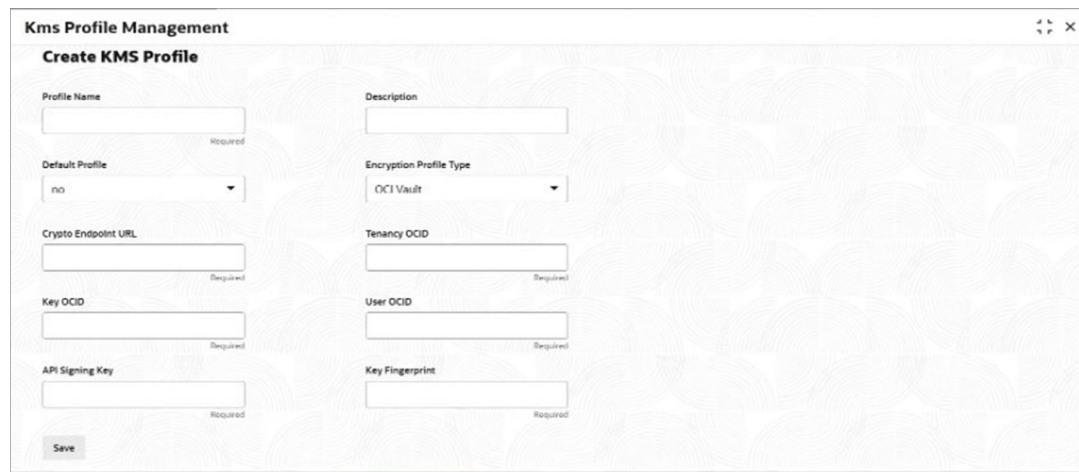
The screenshot shows the 'Kms Profile Management' window with a table of profiles. The table has two columns: 'Profile Name' and 'Default Profile'. There are five rows of data.

Profile Name	Default Profile
testprofiledev1	No
OCISEE801	No
LocalWallet	No
devplgtes1	Yes

A user can perform the following actions on the profiles:

- **Create Profile:** This action allows the user to create a new encryption profile for managing data encryption. The user must provide the **Profile Name**, select whether it is a **Default Profile**, specify the **Crypto Endpoint URL**, and enter the **Key OCID**. Once all required details are entered, click **Next** to proceed with profile creation.

Figure 1-34 Create KMS Profile



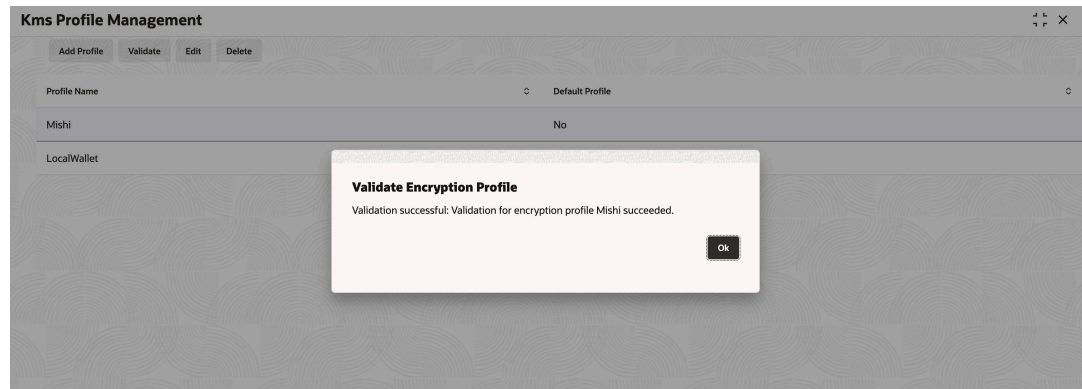
The screenshot shows the 'Create KMS Profile' form. It contains several input fields and a 'Save' button. The fields are arranged in two columns.

Field Name	Field Type	Required
Profile Name	Text Input	Required
Description	Text Input	Optional
Default Profile	Dropdown Menu	Optional
Encryption Profile Type	Dropdown Menu	Optional
Crypto Endpoint URL	Text Input	Required
Tenancy OCID	Text Input	Required
Key OCID	Text Input	Required
User OCID	Text Input	Required
API Signing Key	Text Input	Required
Key Fingerprint	Text Input	Required

A 'Save' button is located at the bottom left of the form.

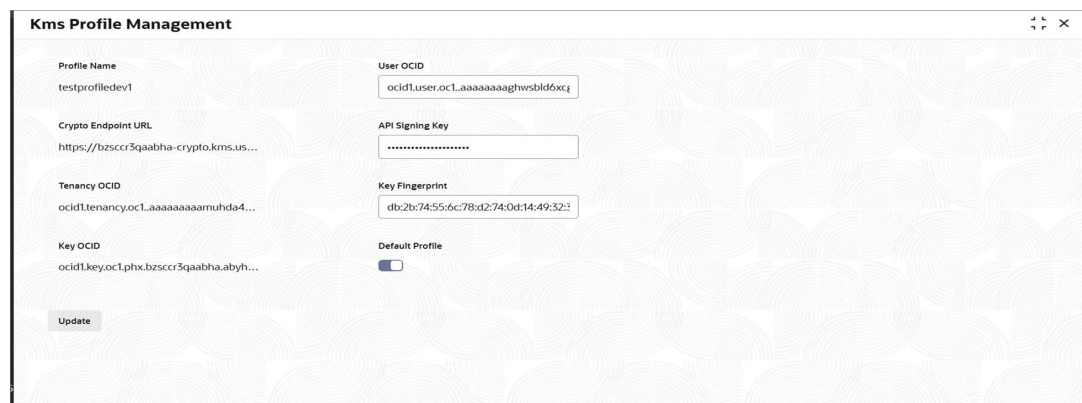
- **Validate:** This action allows the user to verify the provided profile details. Upon successful validation of the entered values, a "**Validation Successful**" message is displayed, confirming that the encryption profile is correctly configured.

Figure 1-35 Validate KMS Profile



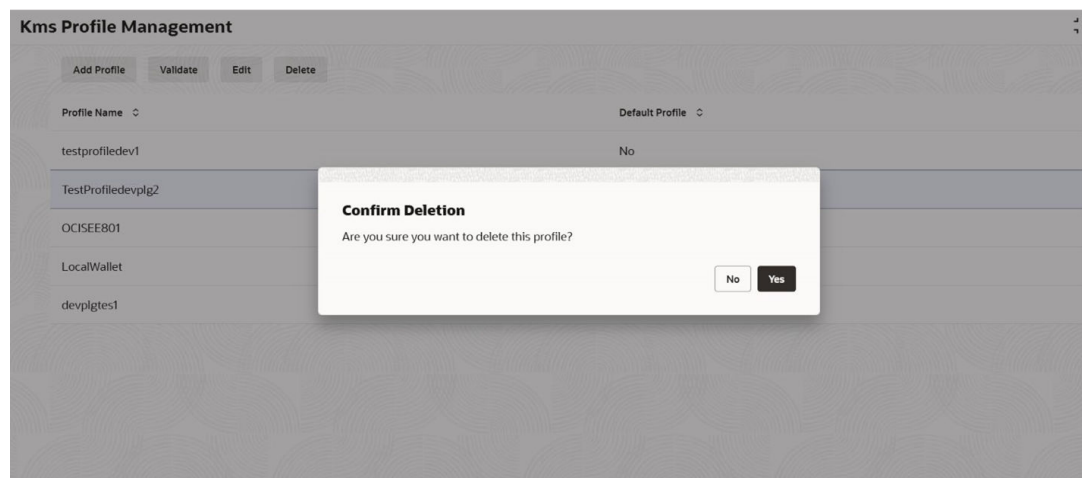
- **Edit:** This action allows the user to set or remove a profile as the default. Additionally, if any configuration issues were identified during the validation process, the user can modify the necessary fields and save the updated profile details.

Figure 1-36 Edit KMS Profile



- **Delete:** This action allows the user to delete the profile.

Figure 1-37 Delete KMS Profile









1.4 Key Management

This topic provides information about key management.

The master key is a central component of the data encryption framework, ensuring the security of data captured and replicated across heterogeneous systems. It serves as the primary key used to encrypt and decrypt other encryption keys, providing a layered and secure approach to data protection. User can manage the master keys for Local Wallet encryption.

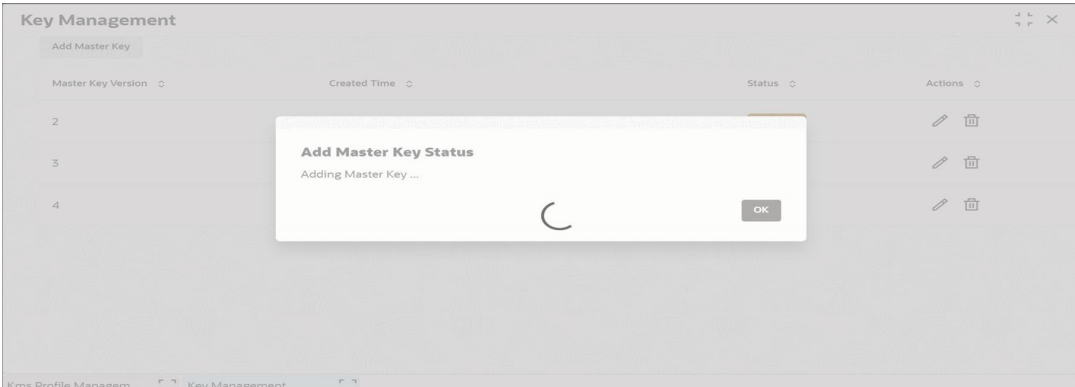
Figure 1-38 Master Keys

Key Management			
Add Master Key			
Master Key Version	Created Time	Status	Actions
2	2025-03-07T05:41:42.000+00:00	Unavailable	 
3	2025-03-07T05:41:56.000+00:00	Available	 
4	2025-03-08T15:11:04.000+00:00	Current	 

A user can perform the following actions:

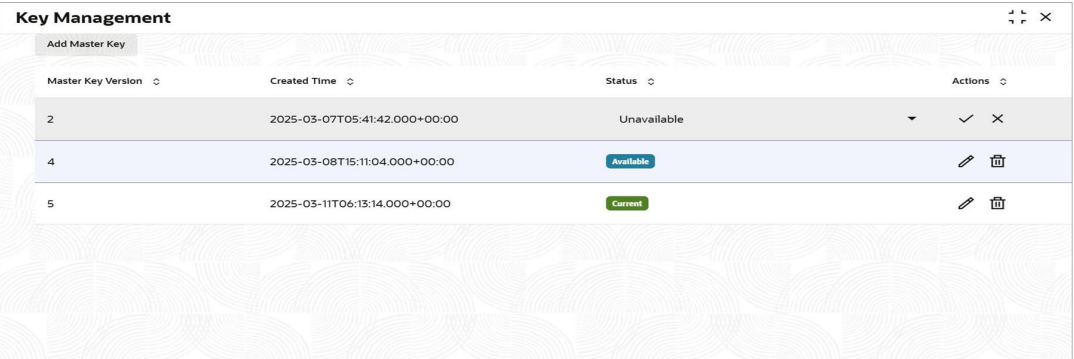
- Add Master Key:** Regularly rotating master keys reduces the risk of unauthorized access to encrypted data. By periodically introducing new master keys, user ensures that even if an encryption key is compromised, the exposure is limited.

Figure 1-39 Add Master Key



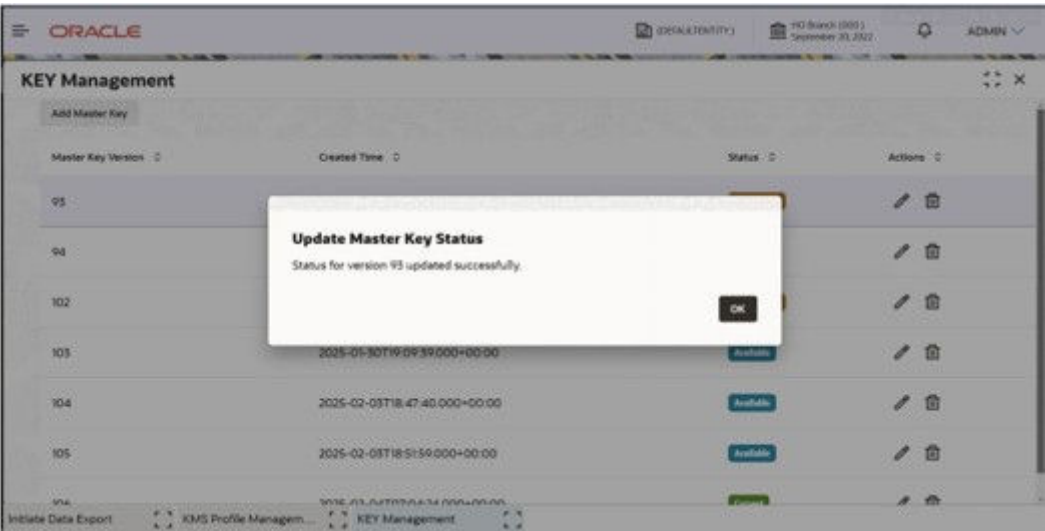
- Update:** This action allows the user to rotate different versions of the master key and make older versions unavailable or change an available version to current version or vice-versa.

Figure 1-40 Update Master Key



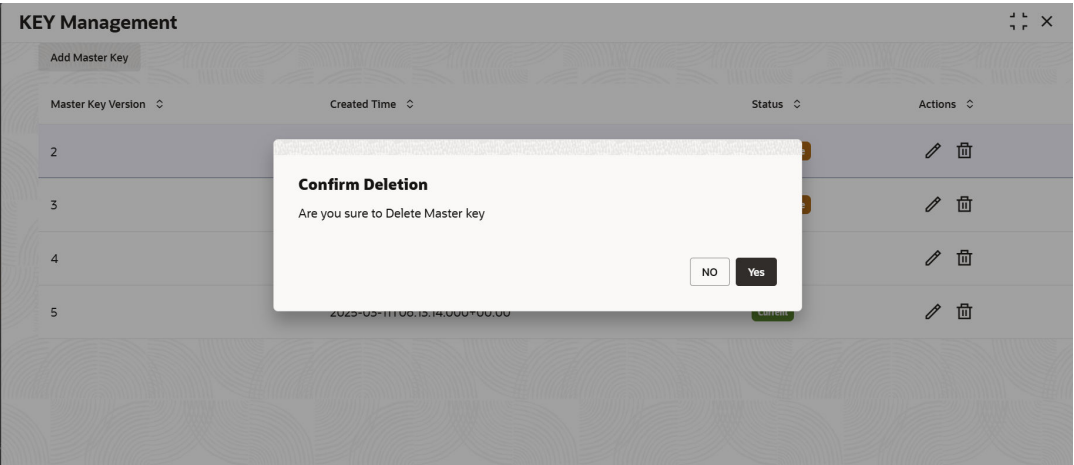
Master Key Version	Created Time	Status	Actions
2	2025-03-07T05:41:42.000+00:00	Unavailable	✓ ✕
4	2025-03-08T15:11:04.000+00:00	Available	✎ ✕
5	2025-03-11T06:13:14.000+00:00	Current	✎ ✕

Figure 1-41 Update Confirmation



- **Delete:** This action allows the user to delete the unused versions of the master key.

Figure 1-42 Delete Master Key

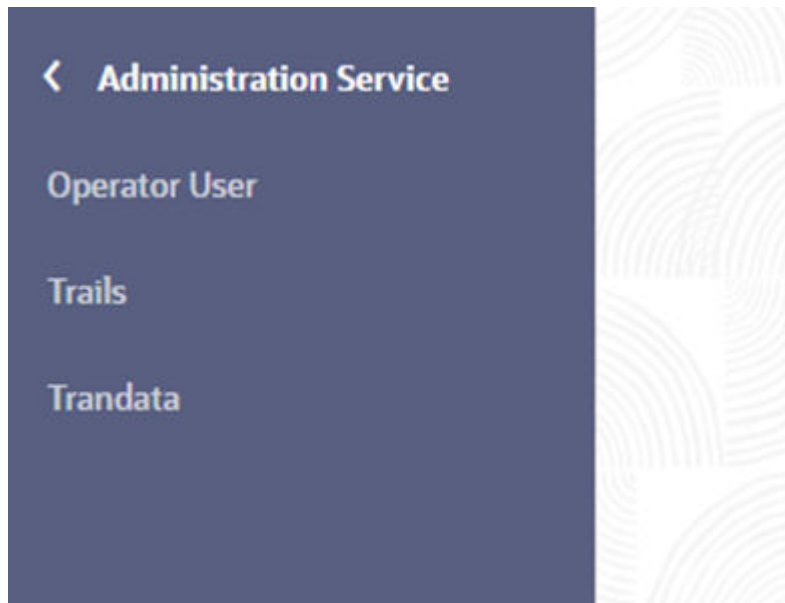


1.5 Administration Service

This topic describes the systematic instructions about Administration Service.

The **Oracle GoldenGate Administration Service** is a REST-based service that provides configuration and management capabilities for a GoldenGate deployment. It is used to manage operator users and add TranData for the schemas passed while user creation.

Figure 1-43 Administration Service



- [Operator User Creation](#)
This topic describes the systematic instruction on operating the user creation.
- [Trails](#)
This topic provides information about trails.
- [TranData](#)
This topic provides information about TranData.

1.5.1 Operator User Creation

This topic describes the systematic instruction on operating the user creation.

The customer must create a **user with the Operator role** in the **source deployment (SaaS tenancy)**. This user will be used to establish a connection with the **target deployment (customer tenancy)**.

The user must enter the **Username** and **Password** then click **Create** to proceed.

Note

Ensure that you provide the list of schemas that align with your replication use case. The Support Team can provide the list of available schemas in the source database.

If additional schemas need to be included in replication, we can add the required schemas using the **TranData view(refer section 2.5.3)** before configuring the Extract, or stop and restart the Extract after adding TranData.

Figure 1-44 Operator User Creation

The screenshot shows a web form titled "Operator User". It contains three input fields: "Operator User" with the value "OperatorUser1236", "Password" with the value "Welcome@12345", and "Schema List" with the value "PARTY, PARTY_BP,SMS". Below the "Schema List" field, there is a small text label "Schema List for Enabling Supplemental Logging". A "Create" button is located at the bottom left of the form.

Figure 1-45 Operator User Creation

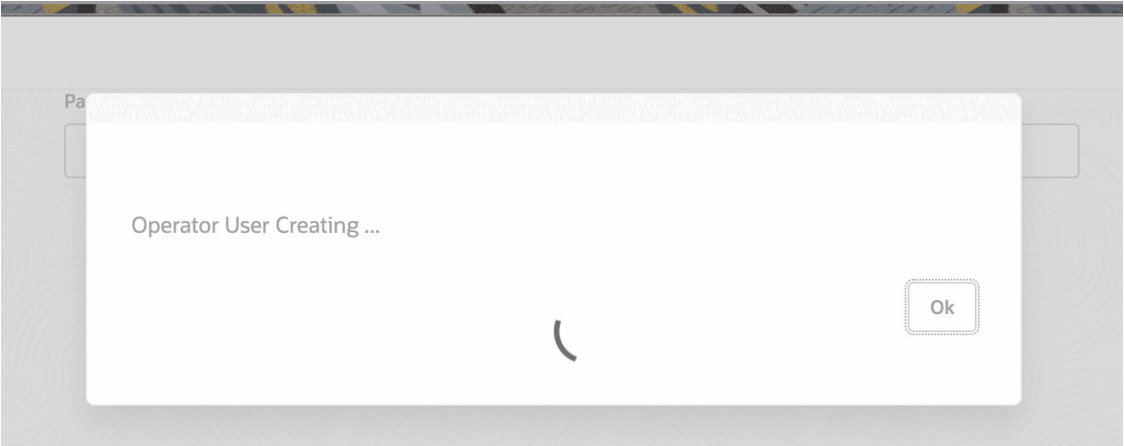


Figure 1-46 Operator User Creation

The screenshot shows a table titled "Operator User". The table has three columns: "S.No", "Username", and "Actions". There is one row of data with "1" in the "S.No" column and "OperatorUser1236" in the "Username" column. The "Actions" column contains an edit icon.

S.No	Username	Actions
1	OperatorUser1236	

1.5.2 Trails

This topic provides information about trails.

Trails in Oracle GoldenGate are files that store captured database change data in a structured format. They act as an intermediate storage between the Extract and Replicate processes to ensure reliable and efficient data replication.

Figure 1-47 Trails



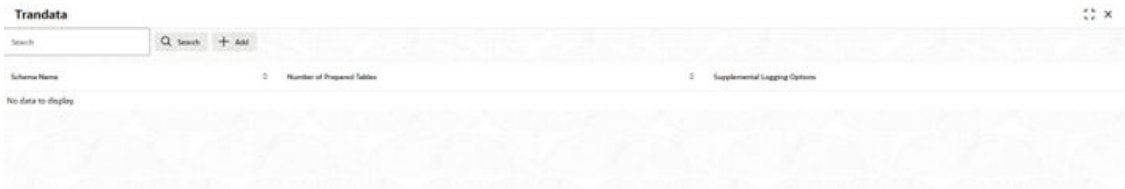
S.No	Trail Name	Producer	Consumer	Max Size (MB)	Space Used (MB)	Sequences (Min-Max)	Actions
1	DR	DEVTRAT		2000	NaN	0-0	

1.5.3 TranData

This topic provides information about TranData.

Oracle GoldenGate TRANDATA enables supplemental logging on source tables so that sufficient row information (such as primary or unique keys) is written to the transaction logs. This allows GoldenGate Extract to correctly capture and replicate INSERT, UPDATE, and DELETE operations.

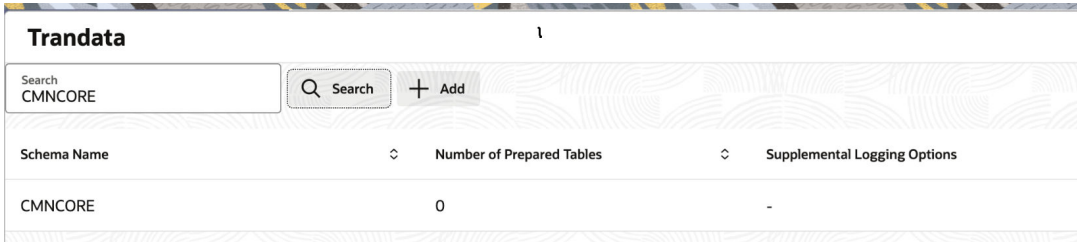
Figure 1-48 Trandata



Schema Name	Number of Prepared Tables	Supplemental Logging Options
No data to display		

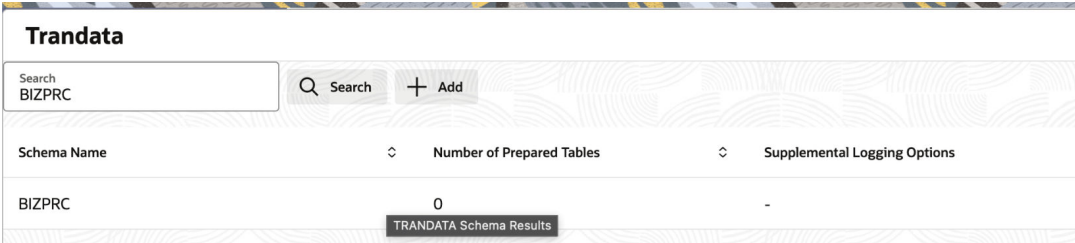
- Search for Trandata (Before Addition) : Searching the source database to check whether TRANDATA is already enabled on the specified tables before adding it.

Figure 1-49 Search for Trandata (Before Addition)



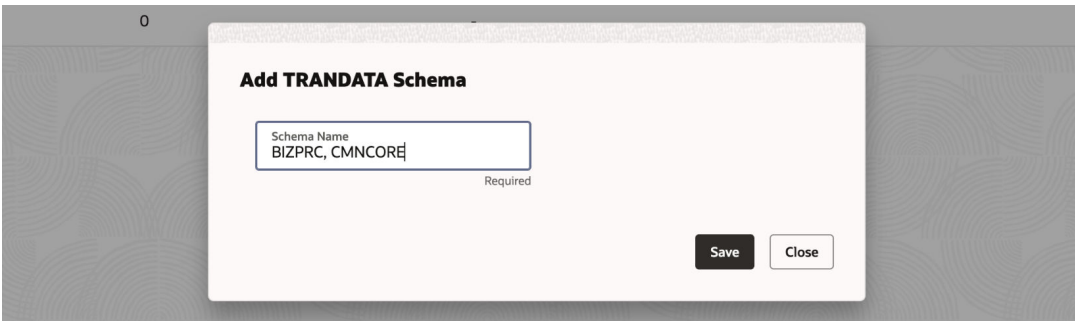
Schema Name	Number of Prepared Tables	Supplemental Logging Options
CMNCORE	0	-

Figure 1-50 Search for Trandata (Before Addition)



- Add Trandata: Enables TRANDATA on selected schemas to ensure the necessary supplemental logging is available for accurate GoldenGate replication.

Figure 1-51 Add Trandata



- Search for Trandata (After Addition)

Figure 1-52 Search for Trandata (After Addition)

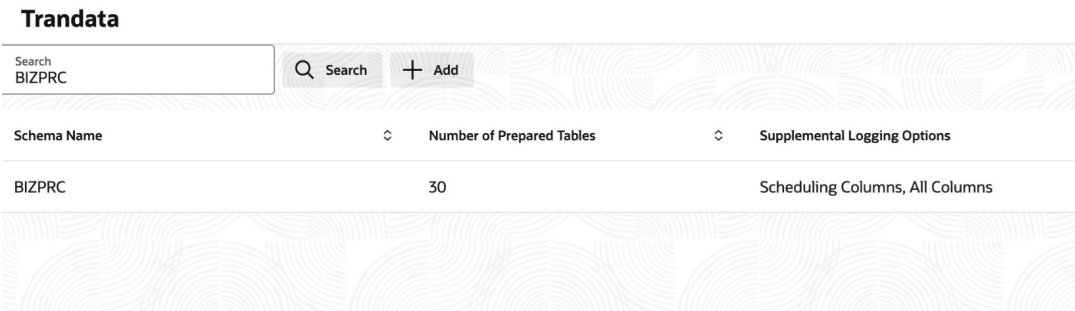
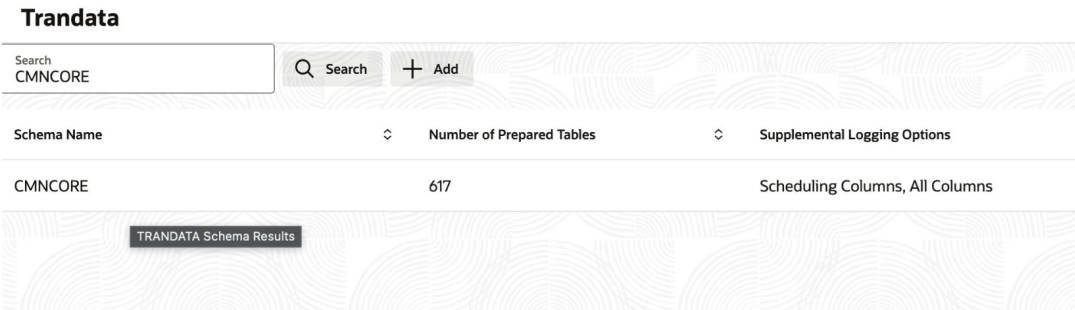


Figure 1-53 Search for Trandata (After Addition)



Note

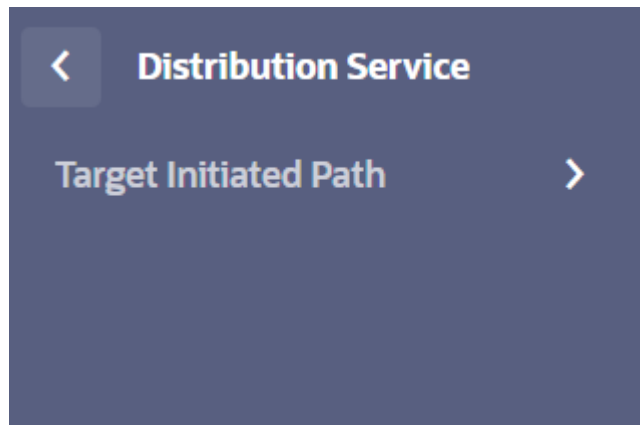
When adding TranData for an existing replication, the Extract process must be stopped and restarted after all required TranData entries are configured.

1.6 Distribution Service

This topic provides information on distribution service

The **Distribution Service** in Oracle GoldenGate securely routes and sends trail files from the source deployment to the target deployment. It manages data transmission, compression, and encryption to ensure reliable and efficient data delivery.

Figure 1-54 Distribution Service



User has a choice to view either Path Info or Path Stats.

Figure 1-55 Target Initiated Path



- [Path Info](#)
This topic provides information about Path Info.
- [Path Stats](#)
This topic provides information about target path stats.

1.6.1 Path Info

This topic provides information about Path Info.

Target-Initiated Path: This function allows users to map or view target path information without logging into the target GoldenGate deployment. It includes two main actions:

- Mapping the Target Path - Associates the target path with the extract for viewing the path information and Stats.

Figure 1-56 Target Path Info

Target Path Info



- Viewing Path Statistics and Information Post-Mapping – Provides details on replication status, trail files, and performance metrics after the mapping is established.

Figure 1-57 Mapping the Target Path

Target Path Info

ING1481 Target-Initiated Path

Reset

Extract Name

INTGEX

Database Name

VPHBTCF4STCOJSP_DVC0940ATP028

Database Instance

e9h1pod3

Encryption Profile

LocalWallet

Started At

2026-03-06T05:39:17.236Z

Lag (sec)

0

Since Lag Reported (sec)

16

Process ID

63

Thread ID

339089

1.6.2 Path Stats

This topic provides information about target path stats.

Figure 1-58 Target Path Stats

Target Path Stats

ING1481 Target-Initiated Path

Reset Refresh Interval

LCR Table

Type	Count
LCR Received	7092449
LCR Sent	7092449
DDL Received	0
DDL Sent	0
Procedure	0

DML Summary Table

Type	Insert	Update	Upsert	Delete
DMLs	920227	8E71029	0	400995

Statistics Table

Filter

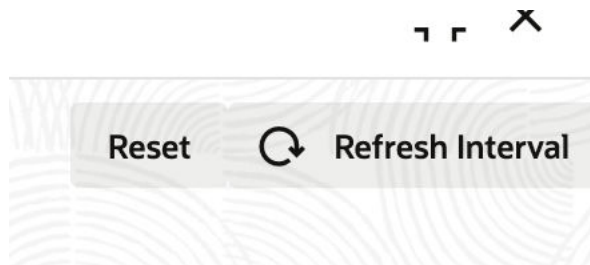
Table Name	Insert	Update	Upsert	Delete
OBFCFMDM_TIMER_JOB_PARAM	0	319855	0	0
OBFCFMDM_C2B_H_AUTO_JOB_PARAM	0	2208702	0	0
DGX_CFSIDX_SC_SCHEDULER_STATE	0	447096	0	0
OBFCNODE_MANAGER_STORE	0	92560	0	0
OBFCQRTZ_FRED_TRIGGERS	295839	162449	0	295839
OBFCQRTZ_TRIGGERS	16368	872107	0	16373

Note

This option requires that the PaaS-side Target Path be created and configured before it can be used. This mapping can also be Reset if there is any change in the Path Configuration in the PaaS.

Click **Reset** to configure a new Target Path.

Figure 1-59 Configuring a new Target Path



2

Data Replication PaaS Setup

This topic provides information about data replication PaaS setup.

To enable **Data Replication**, the user must perform a series of configurations to ensure that updates made in the **source database** are accurately and efficiently reflected in the **target database**.

Thereby maintaining data consistency across both systems.

- [Overview](#)
This topic provides information on PaaS setup.
- [OCI Setup](#)
This topic provides information on OCI setup.
- [Import Data from Object Storage](#)
This topic provides information on importing the data.
- [OCI GoldenGate Deployment Setup](#)
This topic provides information on OCI GoldenGate deployment setup.

2.1 Overview

This topic provides information on PaaS setup.

PaaS data replication setup involves certain prerequisites that a customer has to consider before proceeding with the extract creation in the self-service UI.

The required prerequisites are:

- OCI PaaS tenancy
- An Autonomous Transaction Processing (ATP) instance in OCI for importing the initial data dump
- A configured OCI GoldenGate instance within the PaaS tenancy
- OCI Vault setup for BYOK - used for encrypting the export dump and trail files using key from Customer's OCI Vault .

Note

OCI Vault will still be required in case Oracle Managed Keys/Non-BYOK.

2.2 OCI Setup

This topic provides information on OCI setup.

Setting up a **Customer OCI target environment** for **OCI GoldenGate data replication** involves multiple steps. The following guide provides a detailed walkthrough for configuring the OCI environment.

- [Administration](#)
This topic describes the systematic instructions on administration details.
- [Identity and Security](#)
This topic describes the systematic instructions on identity and security.
- [OCI Policies](#)
This topic provides information policies of OCI.
- [Network Setup](#)
This topic describes the systematic instructions on network setup.
- [OCI Vault Setup](#)
This topic provides information on OCI vault setup.
- [OCI Autonomous Database Setup](#)
The below topic demonstrates on the process of setting up the OCI autonomous database from the OCI console.

2.2.1 Administration

This topic describes the systematic instructions on administration details.

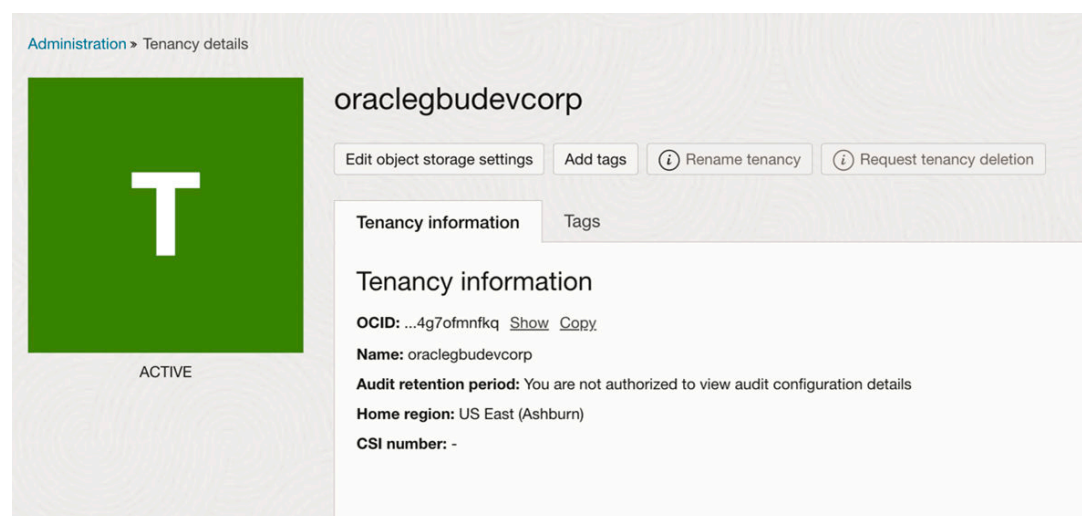
In this section, the user will learn how to **gather the Tenancy OCID**.

Follow these steps to create the **source and target networking path**:

1. Select the **Tenancy Details** option.
2. Copy the **Tenancy OCID** and **Name**. This information is required to create the source and target network paths.
3. Ensure that the user is in the **appropriate region**, regardless of the span of the customer tenancy.

Ensure that the user is in the appropriate region, regardless of the customer tenancy span.

Figure 2-1 Administration

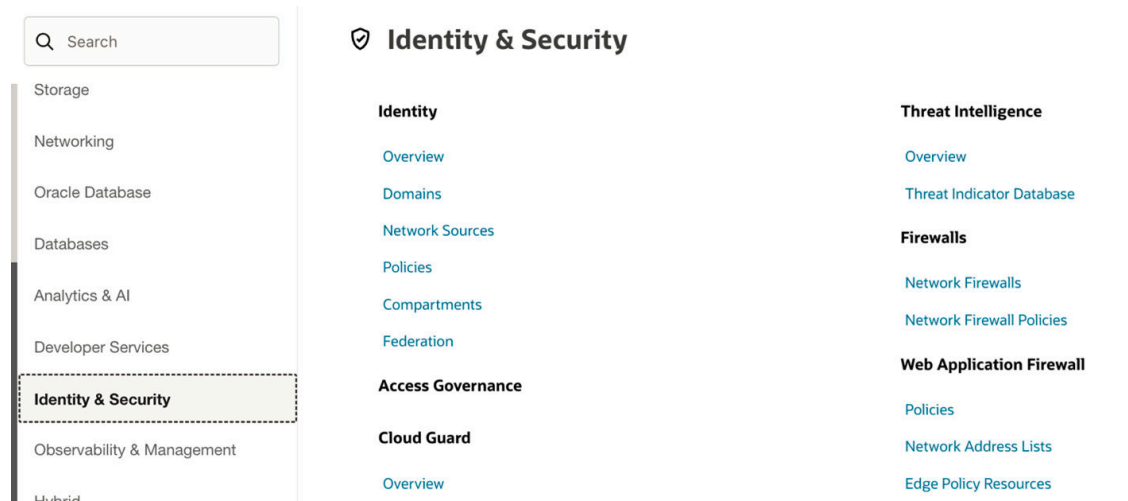


2.2.2 Identity and Security

This topic describes the systematic instructions on identity and security.

OCI Identity and Security refers to the Identity and Access Management (IAM) capabilities within Oracle Cloud Infrastructure (OCI). It enables users to control who can access which resources in their cloud environment, effectively managing user identities and their associated security permissions.

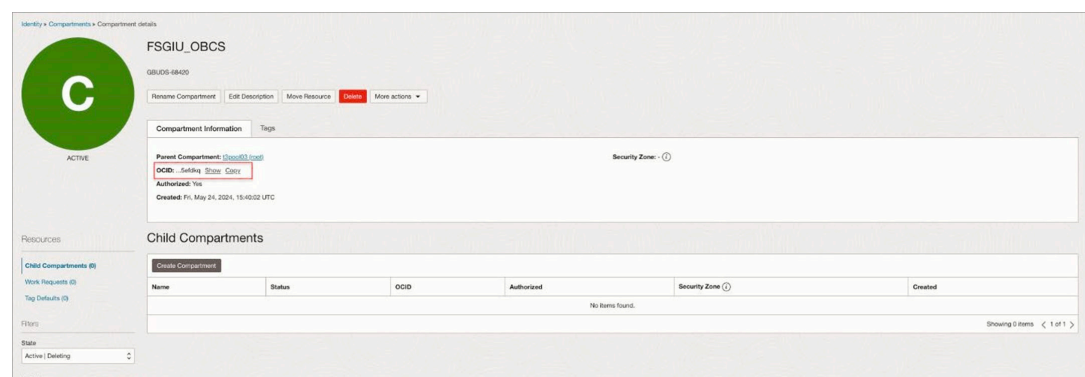
Figure 2-2 Identity and Security



Follow the steps below to configure **network and security settings**:

1. Create a new **compartment** by following the standard process.
 - Copy and note the Compartment's OCID. This information is required for creating source and target network path.
 - Note the **Compartment Name**, as this information is required for configuring the **security policies**.

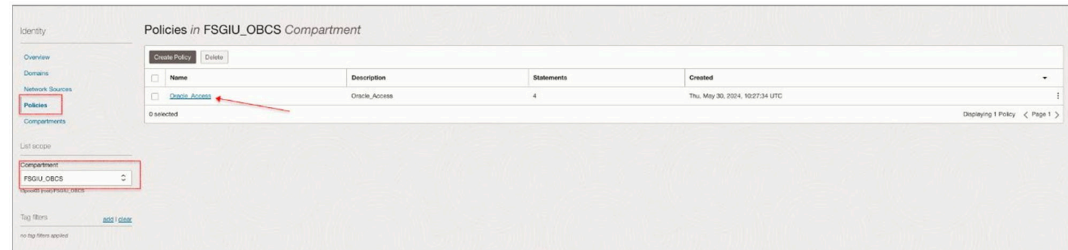
Figure 2-3 Compartment Information



2. Create the security policies that will allow the Oracle to create the Public Endpoint in the compartment.

Figure 2-4 Policies

Figure 28: Policies



3. Create the following policies:

OCI Policies

```
allow service ORACLE_INDUSTRY_SAAS to manage vnics in compartment
<Customer Compartment Name> allow service ORACLE_INDUSTRY_SAAS to use
subnets in compartment
<Customer Compartment Name> allow service ORACLE_INDUSTRY_SAAS to use
network-security-groups in compartment
<Customer Compartment Name> allow service ORACLE_INDUSTRY_SAAS to inspect
work-requests in compartment
<Customer Compartment Name>
```

Note

- Policy names must be unique across compartments.
- The **Policy Builder wizard** does not support all valid policy types; therefore, the user should use **Show Manual Editor** for full configuration.
- Replace <Customer Compartment Name> with your actual **compartment name**.

Figure 2-5 Oracle Access



2.2.3 OCI Policies

This topic provides information policies of OCI.

Oracle Cloud Infrastructure (OCI) policies are essential components of OCI's Identity and Access Management (IAM) system, enabling administrators to define and manage permissions for users and groups within an OCI environment.

OCI Policies

allow service ORACLE_INDUSTY_SAAS to manage vnics in compartment <Customer Compartment Name>

allow service ORACLE_INDUSTY_SAAS to use subnets in compartment <Customer Compartment Name>

allow service ORACLE_INDUSTY_SAAS to use network-security-groups in compartment <Customer Compartment Name>

allow service ORACLE_INDUSTY_SAAS to inspect work-requests in compartment <Customer Compartment Name>

2.2.4 Network Setup

This topic describes the systematic instructions on network setup.

Setting up a network in Oracle Cloud Infrastructure (OCI) involves creating and configuring several components to ensure secure, reliable, and efficient connectivity for cloud resources.

Follow the steps below to setup the network:

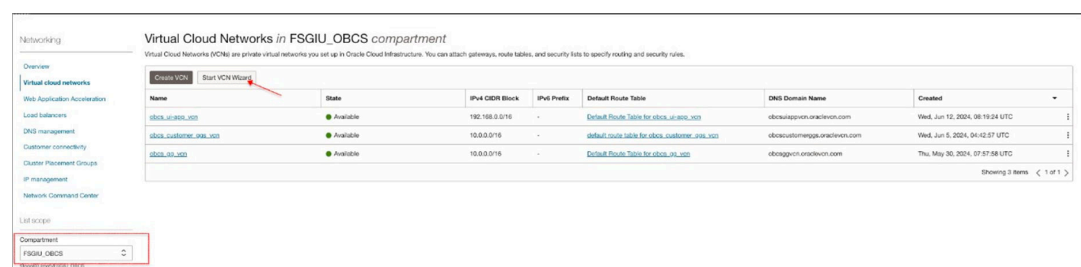
1. Ensure that the network configuration allows connectivity between the source and target environments.

Figure 2-6 Networking



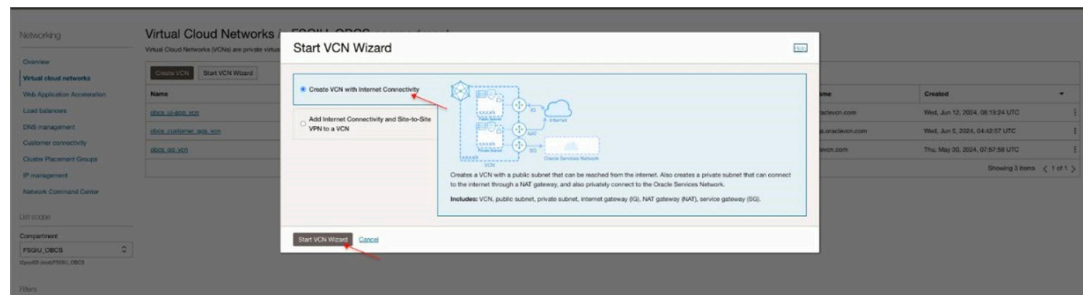
2. Create a **VCN** (Virtual Cloud Network) and subnet in the target tenancy if they are not already available.

Figure 2-7 Virtual Cloud Network



3. Select the **Create VCN with Internet Connectivity** option.

Figure 2-8 Start VCN Wizard



4. Specify a **VCN Name**, accept all other defaults, and click **Next**.

Figure 2-9 Create a VCN Internet Connectivity

Create a VCN with internet connectivity

Configuration

Resource availability checked successfully.

Basic information

VCN name:

Compartment:

VCN IP v4 CIDR block:

IPv6 prefix: Optional

☐ Enable IPv6 in this VCN

DNS resolution

☒ Use DNS hostnames in this VCN

Configure public subnet

IP address type:

IPv4 CIDR block:

Example: 192.168.0.0/16

Maximum number of items added:

Configure private subnet

IP address type:

IPv4 CIDR block:

Example: 192.168.0.0/16

VCN with internet connectivity

Includes:

- Virtual cloud network (VCN)
- Public subnet
- Private subnet
- Internet gateway (IG)
- NAT gateway (NAT)
- Service gateway (SG)

5. Review the resources and note the CIDR on the Subnet.
User's Target environment resources will be associated with the subnet.

Figure 2-10 Review and Create

Create a VCN with internet connectivity

1 Configuration
2 Review and create

Review and create

1 Resource availability checked successfully. Close

Oracle VCN

Name: obcs_poc_vcn
Compartment: F50IU_OBCS
Tags: VCN: VCN-2024-06-28T11:17:45
IPv4 CIDR block: 192.167.0.0/16
DNS label: obcsapocvn
DNS domain name: obcsapocvn.oraclecloud.com

Subnets

Public subnet

Subnet name: public-subnet-obcs_poc_vcn
IPv4 CIDR block: 192.167.1.0/24
Security list name: default-security-list-for-obcs_poc_vcn
Route table name: default-route-table-for-obcs_poc_vcn
DNS label: sub0028119110

Private subnet

Subnet name: private-subnet-obcs_poc_vcn
IPv4 CIDR block: 192.167.2.0/24
Security list name: security-list-for-private-subnet-obcs_poc_vcn
Route table name: route-table-for-private-subnet-obcs_poc_vcn
DNS label: sub0028119111

Gateways

Name	Gateway type	Used by
Internet gateway-obcs_poc_vcn	Internet gateway	public-subnet-obcs_poc_vcn
NAT gateway-obcs_poc_vcn	NAT gateway	private-subnet-obcs_poc_vcn
Service gateway-obcs_poc_vcn	Service gateway	private-subnet-obcs_poc_vcn

Previous Create Cancel

6. User can view all the resources that are built successfully.

Figure 2-11 Created VCN

Create a VCN with internet connectivity

1 Configuration
2 Review and create

Created VCN

Creating resources

VCN creation complete

- ▶ Create VCN (1 resolved) Done ✓
- ▶ Create subnets (2 resolved) Done ✓
- ▶ Create internet gateway (1 resolved) Done ✓
- ▶ Create NAT gateway (1 resolved) Done ✓
- ▶ Create service gateway (1 resolved) Done ✓
- ▶ Create route table for private subnet (1 resolved) Done ✓
- ▶ Create security list for private subnet (1 resolved) Done ✓
- ▶ Update route tables (2 resolved) Done ✓
- ▶ Update private subnet (1 resolved) Done ✓

View VCN

7. User can view the **Virtual Cloud Network** by following the process below:
- Copy and note the VCN's OCID and name. This information is required for the Network Path Creation.
 - Select the subnet where the user would like the Target environment resources to be located.

Figure 2-12 OBCS_POC_VCN

Figure 36: OBCS_POC_VCN

Networking > Virtual cloud networks > Virtual Cloud Network Details

obcs_poc_vcn

Move resource | Add tags | Delete

VCN Information | Tags

Compartment: FSGIU_OBCS
Created: Fri, Jun 28, 2024, 11:19:39 UTC
IPv4 CIDR Block: 192.167.0.0/16
IPv4 Prefix: -

OCID: [ocid1vcn... Show | Copy](#)
DNS Resolver: [ocid1res... Show | Copy](#)
Default Route Table: [default route table for obcs_poc_vcn](#)
DNS Domain Name: obcs.poc.oraclecloud.com

Resources

Subnets (2)

Subnets in FSGIU_OBCS compartment

Name	State	IPv4 CIDR Block	IPv4 Prefixes	Subnet Access	Created
private-subnet-obcs_poc_vcn	Available	192.167.2.0/24	-	Private (Regional)	Fri, Jun 28, 2024, 11:19:39 UTC
public-subnet-obcs_poc_vcn	Available	192.167.1.0/24	-	Public (Regional)	Fri, Jun 28, 2024, 11:19:39 UTC

Showing 2 items < 1 of 1 >

8. Copy and note the Subnet's OCID and name. This information is required for the Network Path Creation.
9. Select the **Default Security** list associated with the subnet.

Figure 2-13 Public Subnet-OBACS_POC_VCN

Networking > Virtual cloud networks > obcs_poc_vcn > Subnet Details

public-subnet-obcs_poc_vcn

Edit | Move resource | Add tags | Create path analysis | Terminate

Subnet Information | Tags

OCID: [ocid1sbn... Show | Copy](#)
IPv4 CIDR Block: 192.167.1.0/24
IPv4 Prefix: -
Virtual Router MAC Address: 00:00:17:5C:39:DA
Subnet Type: Regional

Compartment: FSGIU_OBCS
DNS Domain Name: sub002b119115... Show | Copy
Subnet Access: Public Subnet
DHCP Options: [Default DHCP Options for obcs_poc_vcn](#)
Route Table: [default route table for obcs_poc_vcn](#)

Resources

Security Lists (1)

Security Lists

Name	State	Compartment	Created
Default Security List for obcs_poc_vcn	Available	FSGIU_OBCS	Fri, Jun 28, 2024, 11:19:39 UTC

Showing 1 item < 1 of 1 >

Tag Items: [Add | Clear](#)
no tag items applied

10. User can add an Ingress Rule to the default Security list, using the Subnet CIDR noted above in Step 5. The rule must allow ingress of TCP on 443.

Note

The Security Rule is prerequisite of the environment creation.

Figure 2-14 Add Ingress Rule

Add Ingress Rules

Ingress Rule 1 ✕

Allows TCP traffic for ports: all

Stateless ⓘ
☐

Source Type: CIDR
Source CIDR: Example: 10.0.0.0/16
IP Protocol ⓘ: TCP

Source Port Range: Optional ⓘ: All
Examples: 80, 20-22

Destination Port Range: Optional ⓘ: All
Examples: 80, 20-22

Description: Optional
Maximum 255 characters

+ Another Ingress Rule

Add Ingress Rules Cancel

2.2.5 OCI Vault Setup

This topic provides information on OCI vault setup.

Oracle Cloud Infrastructure (OCI) Vault is a comprehensive key management service that enables you to securely store and manage encryption keys and secrets used to protect your data and applications in the cloud.

- [Create a Vault](#)
This topic describes the systematic instructions to create a vault.
- [Create Master Encryption Key](#)
This topic describes the systematic instructions to create a master encryption key.

2.2.5.1 Create a Vault

This topic describes the systematic instructions to create a vault.

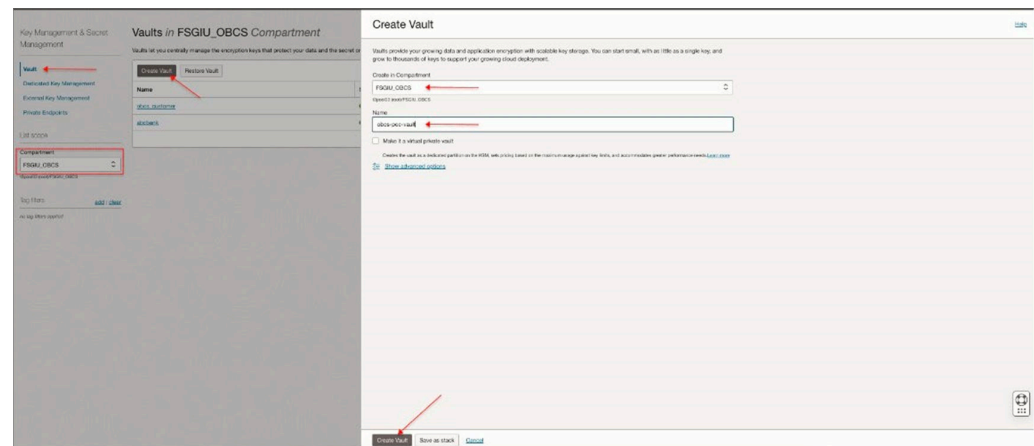
User can create and configure the OCI Vault.

Follow the steps below to create and configure the OCI vault:

User can create a Vault by following the process:

1. Navigate to the Oracle Cloud Infrastructure console.
2. From the **Menu**, select **Identity & Security**, and then **Vault**.

- ### Figure 2-16 Create Vault



- April 17, 2026
Page 10 of 42

Figure 2-17 Vaults in FSGIU_OBCS Compartment

Figure 41: Vaults in FSGIU OBCS Compartment

The screenshot shows the AWS IAM console interface for managing vaults. The main heading is "Vaults in FSGI_OBCS Compartment". Below this, a message states: "Vaults let you centrally manage the encryption keys that protect your data and the secret credentials that you use to securely access resources." with links to "Learn more" and "View all".

The left sidebar contains the navigation menu with the following items: "Vaults", "Dedicated Key Management", "External Key Management", "Private Endpoints", "List scripts", "Compartment", and "FSGI_OBCS". The "Vaults" item is highlighted.

The main content area displays a table of vaults. The table has the following columns: "Name", "State", "Virtual Private", and "Created". There are three rows of data:

Name	State	Virtual Private	Created
aws-ec2-cm	Active	No	Mon, Jul 1, 2024, 05:49:58 UTC
aws-ec2-cm2	Active	No	Wed, Jun 5, 2024, 04:18:36 UTC
aws-ec2-cm3	Active	No	Thu, May 30, 2024, 00:21:02 UTC

At the bottom right of the table, it says "Showing 3 items" and "1 of 1".

2.2.5.2 Create Master Encryption Key

This topic describes the systematic instructions to create a master encryption key.

User can follow the process below to create a master encryption key:

1. To navigate to the vault, click on the vault created.
2. Create a Key by following the process below:
 - a. From the **Keys** section, click **Create Key**.
 - b. Provide a name and description for the key.
 - c. Select the key shape (AES-256 is a common choice).
 - d. Click **Create Key**.

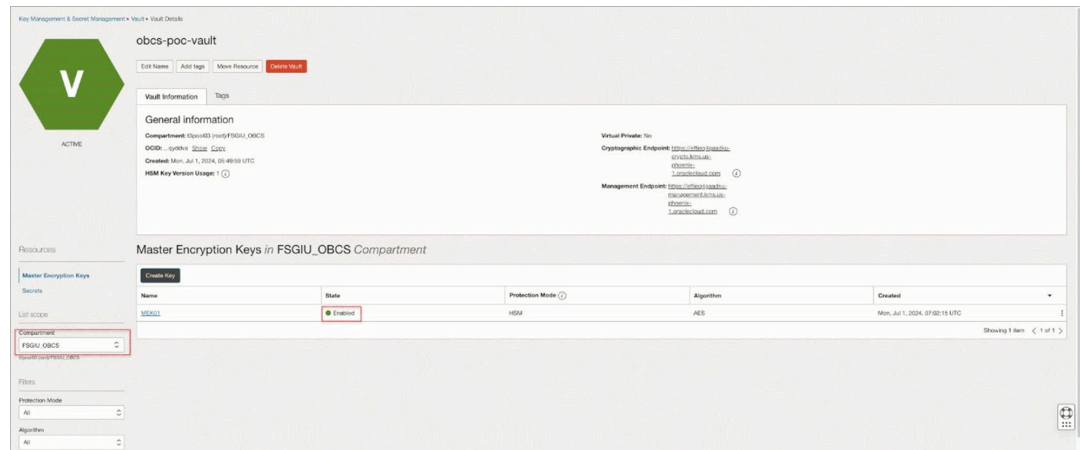
Figure 2-18 Create Key

The screenshot shows the AWS IAM console interface for creating a new master encryption key. The user 'obcs-poc-vault' is selected, and the 'Create Key' page is displayed. The page includes a sidebar with navigation options like 'Master Encryption Keys', 'Secrets', and 'Users'. The main content area shows the key's details, including its name 'FSGIU_OBCS', protection mode 'HSM', and key size '2048 bits'. The 'Create Key' button is highlighted with a red arrow.

Note

User should ensure the key is enabled and available for use.

Figure 2-19 OBCS_POC_Vault



Follow the steps below to create a **Secret**:

3. To navigate to the vault, click on the vault created.
4. Create a Key by following the process below:
 - a. From the **Keys** section, click **Create Key**.
 - b. Provide a name and description for the key.
 - c. Select the key shape (AES-256 is a common choice).
 - d. Click **Create Key**.

2.2.6 OCI Autonomous Database Setup

The below topic demonstrates on the process of setting up the OCI autonomous database from the OCI console.

- [Create and Configure the ATP Instance](#)
This topic describes the systematic instructions to create and configure the ATP.
- [Connect to the ATP Instance](#)
This topic provides information on connecting the ATP instance.

2.2.6.1 Create and Configure the ATP Instance

This topic describes the systematic instructions to create and configure the ATP.

User can setup the OCI Autonomous database by following the process below:

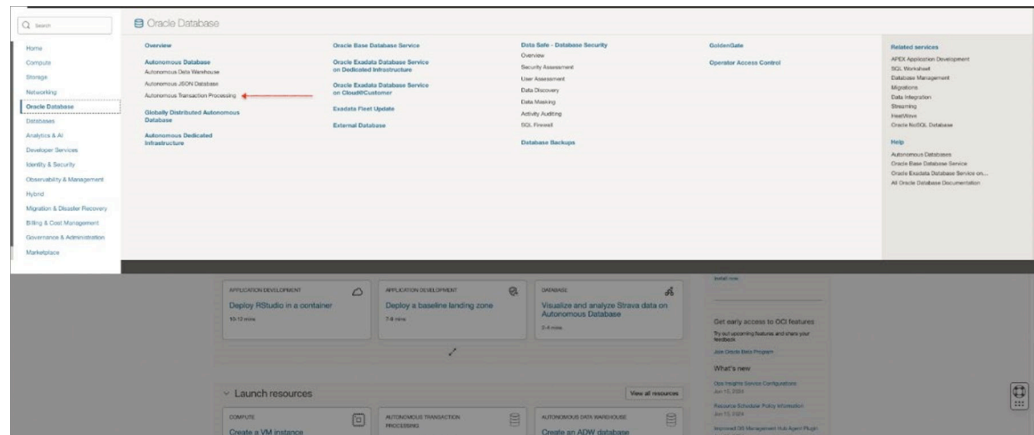
1. Create a **Virtual Cloud Network (VCN)** and **Subnet**.

Note

User can create a separate VCN for ADB's in their tenancy.

2. Create an ATP Instance by following the process below:
 - a. User can navigate to the Autonomous Transaction Processing.
 - b. From the **Menu**, under **Databases**, select **Autonomous Database**.

Figure 2-20 Oracle Database



- c. Create **Autonomous Database** by following the process below:
- i. Click **Create Autonomous Database**.
 - ii. Select the **Autonomous Transaction Processing** option.

Figure 2-21 Create Autonomous Database

- d. User should provide the following database details:

Table 2-1 Database Details

Field	Description
Compartment	Select the compartment where the ATP instance will be created.
Display Name	Provide a display name for the instance.
Database Name	Provide a database name.
Workload Type	Ensure Transaction Processing is selected.
OCPUs	Specify the number of OCPUs.
Storage (TB)	Specify the storage size.

Figure 2-22 Create Autonomous Database Details

- e. Configure the following network access:

Table 2-2 Network Access

Field	Description
Choose Network Access	Select the Virtual Cloud Network.
VCN and Subnet	Select the VCN and subnet created earlier.
Access Type	Select between Private Endpoint (for private access) or Public Endpoint (for public access).

Figure 2-23 Create Autonomous Database – Private endpoint access only

- f. Configure the following database options:

Table 2-3 Database Options

Field	Description
License Type	Select the appropriate license type.
Auto Scaling	Enable or disable auto scaling based on your needs.
Tags	Optionally, add tags for resource management.

- g. Create ATP instances by clicking the **Create Autonomous Database** button.
- h. Configure the ATP Instance by following the process below:
 - i. User can access the ATP Instance. Once the ATP instance is created, navigate to its details page from the **Autonomous Database** section.
 - ii. Download the Wallet. For secure connectivity, download the database wallet by clicking **DB Connection** and then **Download Wallet**. Also, provide a password to secure the wallet.
 - iii. Setup the security rules. If using a private endpoint, ensure the network security groups (NSGs) or security lists allow necessary traffic to and from the ATP instance.

Note

Port 1522 should be allowed.

Figure 2-24 OBCS_POC_ATP1

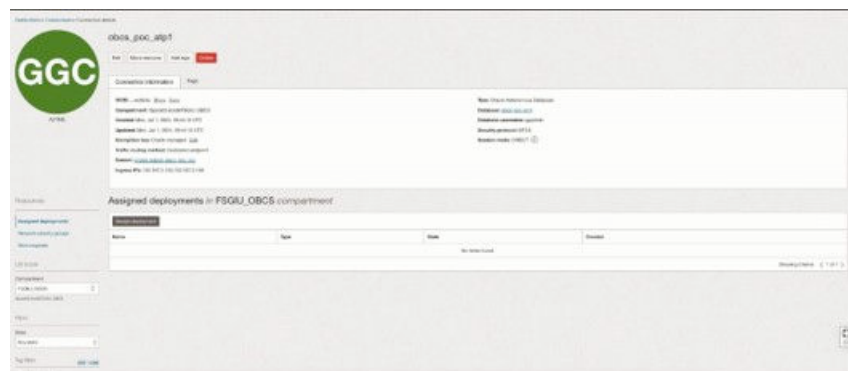
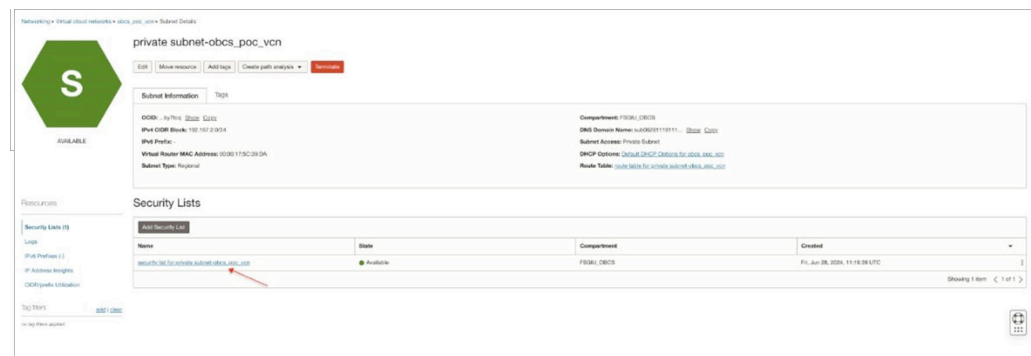


Figure 2-25 Private Subnet-OBCS_POC_VCN



- i. User can access the ATP Instance. Once the ATP instance is created, navigate to its details page from the **Autonomous Database** section.
- ii. Download the Wallet. For secure connectivity, download the database wallet by clicking **DB Connection** and then **Download Wallet**. Also, provide a password to secure the wallet.

- iii. Setup the security rules. If using a private endpoint, ensure the network security groups (NSG's) or security lists allow necessary traffic to and from the ATP instance.

Note

Port 1522 should be allowed.

Figure 2-26 SL - Add Ingress Rules

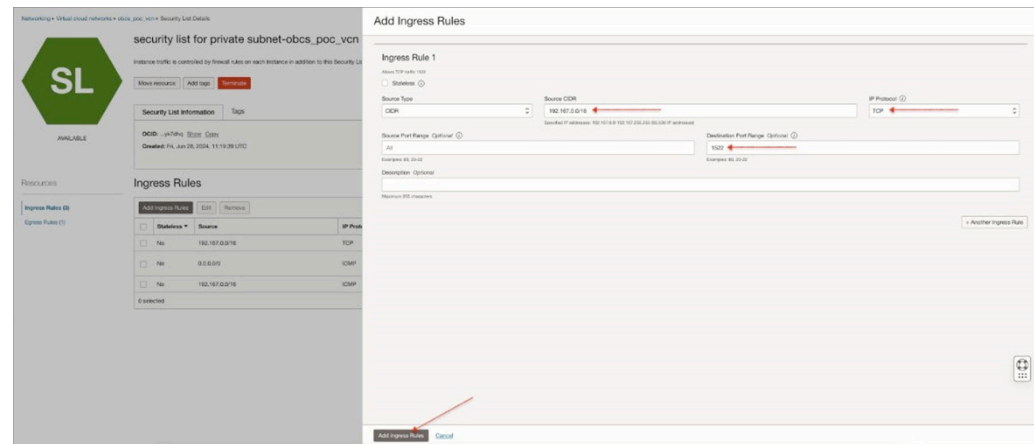
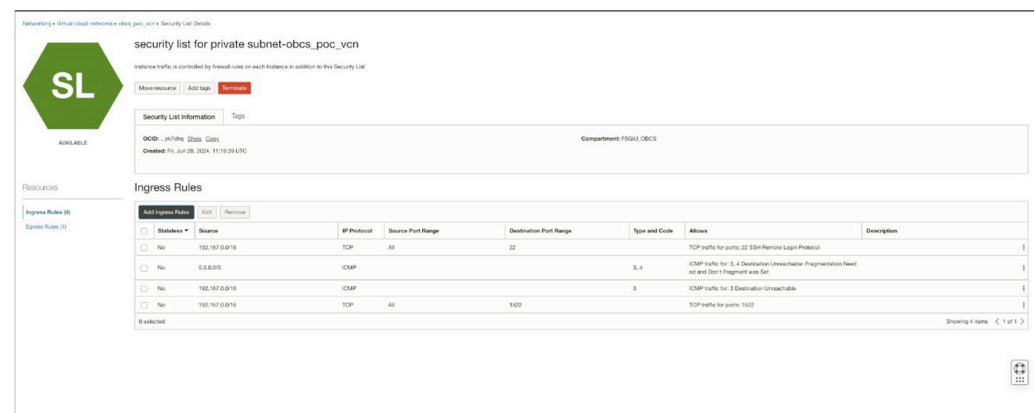


Figure 2-27 Security List for Private Subnet-OBSC_POC_VCN



2.2.6.2 Connect to the ATP Instance

This topic provides information on connecting the ATP instance.

User can connect to the ATP instance by following the process below:

1. Install **Oracle Instant Client**.

Note

If connecting from a client machine, install the **Oracle Instant Client**.

2. Configure the required connection. User can see the downloaded wallet to configure the connection settings. Also, user needs to update the tnsnames.ora file with the connection details provided in the wallet.
3. Connect Using SQL Developer or SQL*Plus. Here, the user can use tools like SQL Developer or SQL*Plus to connect to the ATP instance using the wallet and connection details.

Note

If the ATP instance is created with Private Endpoint (for private access), then follow the documentation from 4 Ways to Connect to Autonomous Database on a Private Network [4 Ways to Connect to Autonomous Database on a Private Network](#). Import DMP files downloaded from OCI Object Store PAR URL. For more information, refer **Exporting initial seed data set**.

2.3 Import Data from Object Storage

This topic provides information on importing the data.

- [Downloading dump with PAR URL](#)
This topic describes about downloading dump using PAR URL.
- [Database Setup](#)
This topic describes the systematic instructions to setup database
- [Troubleshooting](#)
This topic provides information on troubleshooting.

2.3.1 Downloading dump with PAR URL

This topic describes about downloading dump using PAR URL.

User can get an initial dump before proceeding with the database import.

1. Pre-authenticated Request (PAR) URL received from OBCS SaaS for the dump files in Object Storage.
2. Decrypt the Cipher text DEK: User can perform the Decrypt Cipher text DEK using the same Vault and Key as follows:
 - The tenant uses the same vault and master encryption key to decrypt the cipher text DEK.
 - The API returns the plain text DEK.
 - The source code for Decrypt Data Using Cipher text are as follows:

```
filename: oci-vault-dek-request-sdk-ciphertext-decrypt.py
# This is an automatically generated code sample.
# To make this code sample work in your Oracle Cloud tenancy,
# please replace the values for any parameters whose current values do
# not fit
# your use case (such as resource IDs, strings containing 'EXAMPLE' or
# 'unique_id', and
# boolean, number, and enum parameters with values not fitting your use
# case).
import oci
```



```
# Create a default config using DEFAULT profile in default location
# Refer to https://docs.cloud.oracle.com/en-us/iaas/Content/API/Concepts/sdkconfig.htm
#SDK_and_CLI_Configuration_File# For more info

config = oci.config.from_file(file_location="~/oci/config")
service_endpoint = "<replace with Cryptographic Endpoint of Vault from Customer's tenancy>"

# Initialize service client with default config file

key_management_client = oci.key_management.KmsCryptoClient( config,
service_endpoint=service_endpoint)

# Send the request to service, some parameters are not required, see API
# doc for more info

decrypt_response = key_management_client.decrypt
( decrypt_data_details=oci.key_management.models.DecryptDataDetails(ciphertext="QZGCZ05MM9VlAOOrKPXL9r<----
readacted--->lAC5NhEcQgeFslxpPBPI89WCIEJlLcaryZlKJgAAAAA=",
key_id="<replace with key OCID of Master Encryption Key in the Vault from Customer's tenancy>",
encryption_algorithm="AES_256_GCM"))
# Get the data from response
print(decrypt_response.data)
```

3. Exporting initial seed data set: For performing this action, users should check for the following:

- Oracle Data Pump version 19.9 or later
- tnsnames.ora
- Policies to access Customer OCI Vault
- Decrypt Cipher text DEK using SDK/API/OCI CLI - Decrypt Cipher text DEK - Customer's will be shared with Cipher text DEK in the PAR URL.

Note

Customers will be shared with a PAR URL to the Exported DMP files on object storage. The user can download the DMP files and run impdp to import to their target ATP.

Follow the steps below to execute:

1. Connect to Target ATP.
2. Create a directory to store the dump files containing the exported data.
Create a directory

```
CREATE DIRECTORY data_export_dir as 'data_export';
```

Run Data Pump Import with the dump file parameter set to the list of file URLs on your Cloud Object Storage. The Data Pump supports using an Oracle Cloud Infrastructure Object Storage pre-authenticated URL for the dump file parameter.

Note

- If a user provides a pre-authenticated URL, the credential parameter is required, and impdp ignores it.
- If a user employs a pre-authenticated URL for the dump file, then user may utilize a NULL value for the credential in the subsequent step.

IMPDP

```
impdp admin/<replace with ADMIN password>@<replace with atp instance name service
name - high> \ directory=data_export_dir \ credential=NULL \
dumpfile=<PRE_AUTHENTICATED_OBJECT_STORAGE_URL> \ parallel=16 \
ENCRYPTION_PASSWORD=\"<use the plaintext DEK generated in prerequisite step>\" \
exclude=cluster,indextype,db_link
```

Note

PRE_AUTHENTICATED_OBJECT_STORAGE_URL - Seed Data PAR URL from Data Export Status screen.

The working use case is depicted in the image below:

Figure 2-28 Working Use Case

```
Copyright (c) 1982, 2024, Oracle and/or its affiliates. All rights reserved.

Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Master table "ADMIN"."SYS_IMPORT_FULL_01" successfully loaded/unloaded
Starting "ADMIN"."SYS_IMPORT_FULL_01": admin/*****@vcs0948rpb@cloudorchestr2.to directory=data_export_dir credential=NULL dumpfile=https://oracleghudevcorp.objectstorage.us-phoenix-1.o
ci.customer-oci.com/p/_9pWcXG5511ShdVgZ2d4BndafgIanc-803Pd79kz7z8uajgT_H0f1s3zV00L/v/oracleghudevcorp/8/fqbu_0bdc6a_cndevcorp_atlp/a/exportdb/exportfu_dep_parallel=16 ENCRYPTION_PASS
WORD=***** EXCLUDE=cluster,indextype,db_link
Processing object type SCHEMA_EXPORT/USER
Processing object type SCHEMA_EXPORT/SYSTEM_GRANT
Processing object type SCHEMA_EXPORT/ROLE_GRANT
Processing object type SCHEMA_EXPORT/DEFAULT_ROLE
Processing object type SCHEMA_EXPORT/TABLESPACE_QUOTA
Processing object type SCHEMA_EXPORT/PASSWORD_HISTORY
Processing object type SCHEMA_EXPORT/PRE_SCHEMA/PRODOACT_SCHEMA
Processing object type SCHEMA_EXPORT/SHADOW/SHADOW
Processing object type SCHEMA_EXPORT/TYPE/TYPE_SPEC
ORA-39346: data loss in character set conversion for object TYPE "DBFC"."TV_CUST_SOURCE"
ORA-39346: data loss in character set conversion for object TYPE "DBFC"."PARAMETER"
ORA-39346: data loss in character set conversion for object TYPE "DBFC"."TV_UTIL_MASTER"
ORA-39346: data loss in character set conversion for object TYPE "DBFC"."REC_ERROR"
ORA-39346: data loss in character set conversion for object TYPE "DBFC"."TV_GETPARAMETER"
ORA-39346: data loss in character set conversion for object TYPE "DBFC"."KEYS"
ORA-39346: data loss in character set conversion for object TYPE "DBFC"."TV_REQUEST_DETAILS"
ORA-39346: data loss in character set conversion for object TYPE "DBFC"."TV_UTILS"
Processing object type SCHEMA_EXPORT/SEQUENCE/SEQUENCE
Processing object type SCHEMA_EXPORT/TABLE/PRODOACT_INSTANCE
```

2.3.2 Database Setup

This topic describes the systematic instructions to setup database

The process or steps for importing the data from the object storage are as follows:

1. User should ensure the following necessary credentials and configuration files are set up:
 - OCI tenancy OCID
 - User OCID

- Compartment OCID
 - Object Storage namespace
 - API key configuration
2. Connect to Target ATP.
 3. Create a directory to store dump files containing exported data.

Create a directory

```
CREATE DIRECTORY data_export_dir as 'data_export';
```

Note

Ensure the necessary privileges are granted to the target ATP instance to access and read from the Object Storage bucket.

4. Run the Data Pump Import with the dumpfile parameter set to the list of file URLs on your Cloud Object Storage.
 - Run the Data Pump Import using the `dumpfile` parameter set to the list of file URLs on your Cloud Object Storage
 - When user uses a pre-authenticated URL, providing the `credential` parameter is required and `impdp` ignores the `credential` parameter.
 - When user uses a pre-authenticated URL for the `dumpfile`, you can use a `NULL` value for the `credential` in the next step.

IMPDP

```
impdp admin/<replace with ADMIN password>@<replace with atp instance name  
service name - high> \ directory=data_export_dir \ credential=NULL \  
dumpfile=<PRE_AUTHENTICATED_OBJECT_STORAGE_URL> \ parallel=16 \  
ENCRYPTION_PASSWORD=\"<use the plaintext DEK generated in prerequisite step>\"  
\ exclude=cluster,indextype,db_link
```

Note

`PRE_AUTHENTICATED_OBJECT_STORAGE_URL` - Seed Data PAR URL from Data Export Status screen.

5. Check the status of the import job and ensure it is completed successfully

The log file is available in the specified Object Storage bucket. User can download and review the log file to verify the import process.

2.3.3 Troubleshooting

This topic provides information on troubleshooting.

The following are some of the instances noted below for troubleshooting the issues:

Table 2-4 Troubleshooting

Failures	Solution
Job Failure	Users must check the log file in the Object Storage bucket for detailed error messages.
Network Issues	Users must ensure the ATP instance can communicate with the Object Storage endpoint.
Permissions	User must verify that the ATP instance has the necessary permissions to read from the Object Storage bucket.

2.4 OCI GoldenGate Deployment Setup

This topic provides information on OCI GoldenGate deployment setup.

Oracle GoldenGate is a comprehensive software package for real-time data integration and replication, enabling the transfer of data across heterogeneous systems with minimal impact on performance. Deploying Oracle GoldenGate involves setting up its Microservices Architecture, which provides a flexible and scalable framework for data replication.

- [Create an OCI GoldenGate Deployment](#)
This topic describes the systematic instructions to create an OCI GoldenGate deployment.
- [Create the Connection](#)
This topic describes the systematic instructions to create the connection.
- [Configure OCI GoldenGate](#)
This topic describes the systematic instructions to configure OCI GoldenGate.
- [Target Initiated Distribution Path](#)
This topic provides information on target distribution path.

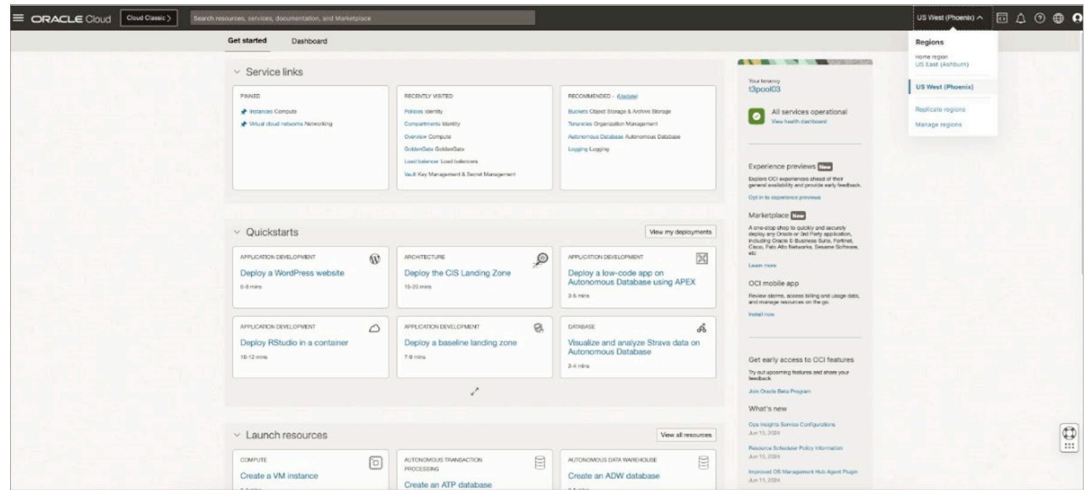
2.4.1 Create an OCI GoldenGate Deployment

This topic describes the systematic instructions to create an OCI GoldenGate deployment.

User can create an OCI GoldenGate Deployment by following the process below:

1. Navigate to the **Oracle Cloud Infrastructure** console.
2. Select the region where the user wants to create the GoldenGate deployment.

Figure 2-29 Get Started - Regions



3. Click **Create Deployment**, to create a GoldenGate Deployment

Figure 2-30 Create Deployment

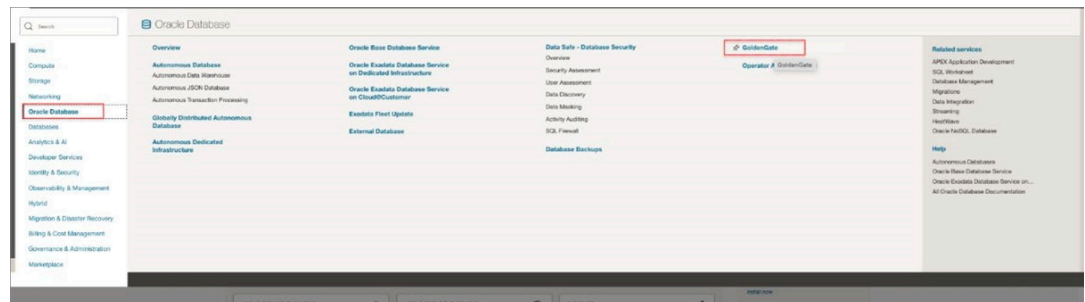


Figure 2-31 GoldenGate

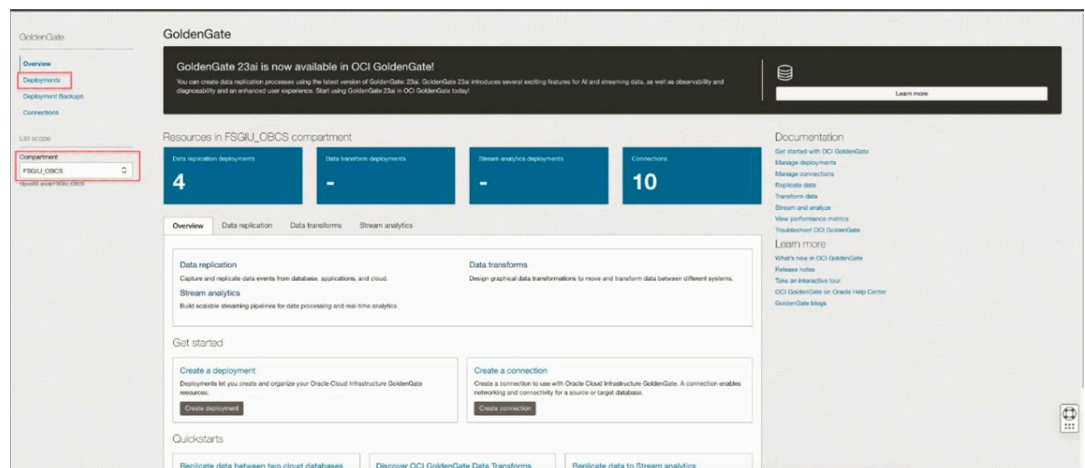


Figure 2-32 Deployments in FSGIU_OBCS Compartment

Name	State	Substate	Type	OCPU count	Created
obcs-prod-1	Active	---	Oracle Database	1	Mon, Jun 10, 2024, 09:10:48 UTC
obcs-prod-2	Inactive	---	Oracle Database	1	Wed, Jun 5, 2024, 04:53:19 UTC
obcs-prod-3	Active	---	Oracle Database	1	Thu, May 30, 2024, 14:46:34 UTC
obcs-prod-4	Inactive	---	Oracle Database	1	Thu, May 30, 2024, 08:07:50 UTC

4. Select **Oracle GoldenGate** and provide necessary details like name, compartment, and network information.

Figure 2-33 Create Deployment

Create deployment

General information

Name: obcs-prod-1

Description: Optional

Compartment: FSGIU_OBCS

Production (Selected) | **Development or testing**

OCPU count: 4

Subnet in FSGIU_OBCS (Change connection)

private-subnet-obcs-prod-1

Choose a license type

Bring Your Own License (BYOL) | **License included** (Selected)

Network (Selected) | **Tags**

private-subnet-obcs-prod-1

5. Select the appropriate compute shape and configure other deployment settings.
6. Click **Create**.

Figure 2-34 Create Deployment

Create deployment

Advanced options

Compute shape: VM.Standard3.2

Data destination: none

Stream endpoint: none

Other settings

Subnet: private-subnet-obcs-prod-1

License type: Bring Your Own License (BYOL)

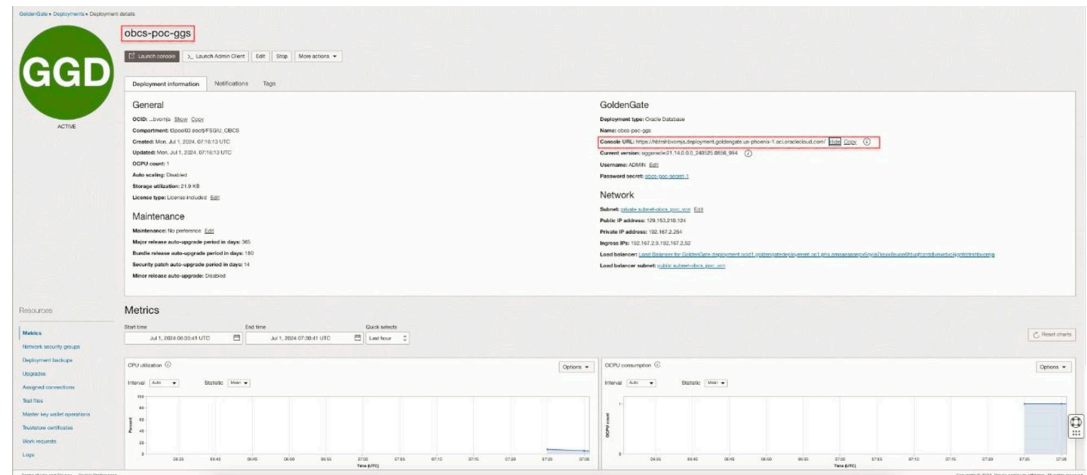
License included: Yes

Network: private-subnet-obcs-prod-1

Tags: none

Once the deployment is created, configure it. Note down the Admin URL and credentials.

Figure 2-35 OBCS_POC_GGS



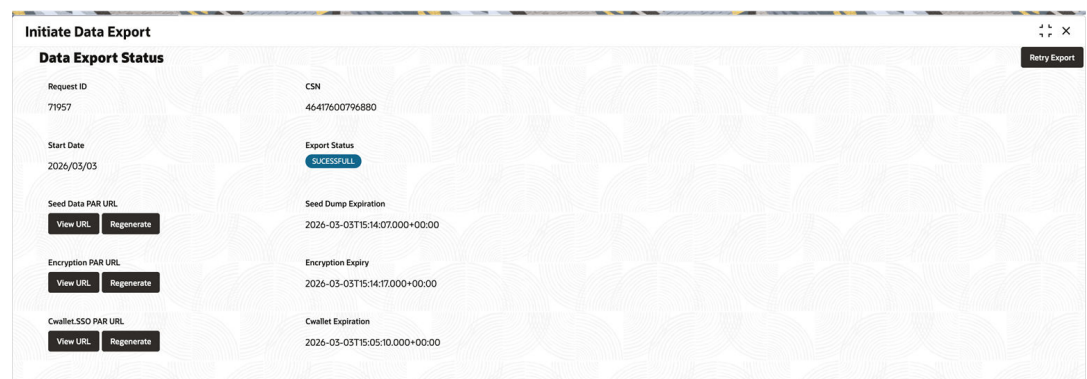
Once the deployment is **Active and Running**, customers who have **not opted for BYOK (Bring Your Own Key)** must perform a few additional setup steps in the **OCI PaaS console**.

Oracle Cloud Infrastructure GoldenGate allows users to encrypt trail files using local master key wallets that are stored within a GoldenGate deployment. These master encryption keys are used to encrypt trail files that are distributed to other GoldenGate deployments.

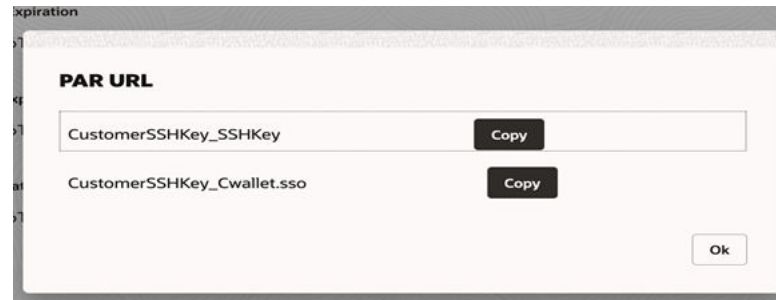
The **master encryption key wallet** can also be **exported and imported** between source and target GoldenGate deployments to ensure secure trail file exchange.

7. Login to the **Self-Service Appshell UI** and navigate to **Data Replication** and click **Initiate Data Export**.
8. On the **Export Status** landing page, find for the **CWALLET.sso PAR URL** file and click on the **Vire URL's**.

Figure 2-36 Initiate Data Export



9. In the pop up window select and copy the **cwallet.sso PAR URL** and download the file from your browser.

Figure 2-37 PAR URL

10. Base64 encode the cwallet.sso using this command:

```
base64 -b 0 -i cwallet.sso
```

11. In the **Oracle Cloud console**, open the navigation menu, and select **Identity & Security**, and then select **Vault**, and then click **Secret and Create Secret**.
12. In the **Create Secret** panel, complete the fields as follows:
 - Specify the **Name** for the secret.
 - Specify the **Description** for the secret.
 - For Encryption Key in <compartment-name>, select the master encryption key created in the Before you begin steps.
Click **Change compartment** to select a master encryption key located in a different compartment.
 - For **Secret type template**, select **Plain-Text**.
 - For **Secret contents**, paste the **cwallet.sso base64** encoded string from step 10.
 - Click **Create Secret**.
The **Secret** appears in the Secrets list.
13. Import the master encryption key wallet to the target OCI GoldenGate deployment.
14. Navigate back to **OCI Goldengate Services**, then click **Deployments** in OCI Console.
15. On the **Deployments** page, select the deployment in which to import the master encryption key wallet.
16. On the **Deployment** details page, under **Resources**, click **Master encryption key wallet** actions.
17. Click **Import** and in the Import dialog box add the following information:
 - For Wallet secret in <compartment-name>, select the wallet secret to import.
Click **Change compartments** to select a wallet secret from a different compartment.
 - Select **Backup** existing wallet;
 - If selected, then under **Backup** wallet and for the **Name**, specify the name for the backup wallet.
 - Specify the description.
 - For Encryption key in <compartment-name>, select the encryption key to use.
Click **Change compartment** to select an encryption key in a different compartment.
 - Click **Import** and wait for the system to confirm that the process is successful.
18. Verification on **Goldengate** Console:

- Login to the **Goldengate** Console UI with the Admin User.
- Navigate to **Encryption** , then click **LocalWallet**.
The **LocalWallet** view provides exported **MasterKey**'s version.

2.4.2 Create the Connection

This topic describes the systematic instructions to create the connection.

User can create the Oracle Database connection by following the process below:

1. From the **OCI GoldenGate Overview** screen, click **Connections**.

Note

User can also click **Create Connection** under the Get started section and move to next step

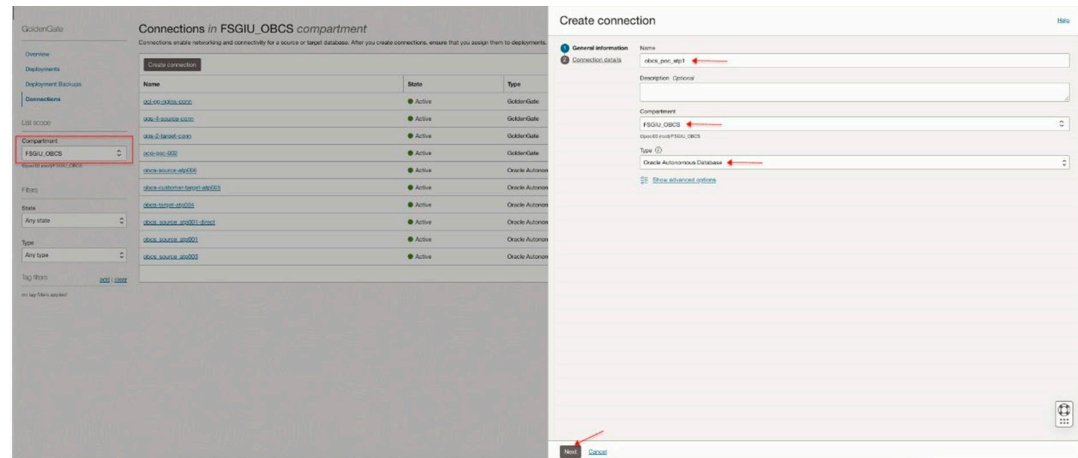
2. On the **Connections** page, click **Create Connection**.
3. In the **Create Connection** tab, complete the **General Information** fields as follows:

Table 2-5 General Information

Field	Description
Name	Specify a name for the connection.
Description	Optional Specify a description that helps you distinguish this connection from others.
Compartment	Select the compartment in which to create the connection.
Type	From Oracle , select Oracle Database .
Show advances options	Optional Click the link to manage keys or add tags.

4. From **Security**, select one of the following:
 - Select Use Oracle-managed encryption key, to leave all encryption key management to Oracle.
 - Select Use Customer-managed encryption key, to select a specific encryption key stored in the OCI Vault to encrypt the user's connection credentials.
5. From **Tags**, add tags to organize the resources
6. Click **Next**.

Figure 2-38 Create Connections



7. Complete the Connection Details fields as follows:
 - a. Select an existing database in the selected compartment and complete the rest of the fields as needed.
 - b. Click **Change Compartment**, to select a database in a different compartment. Also, maintain the following details:

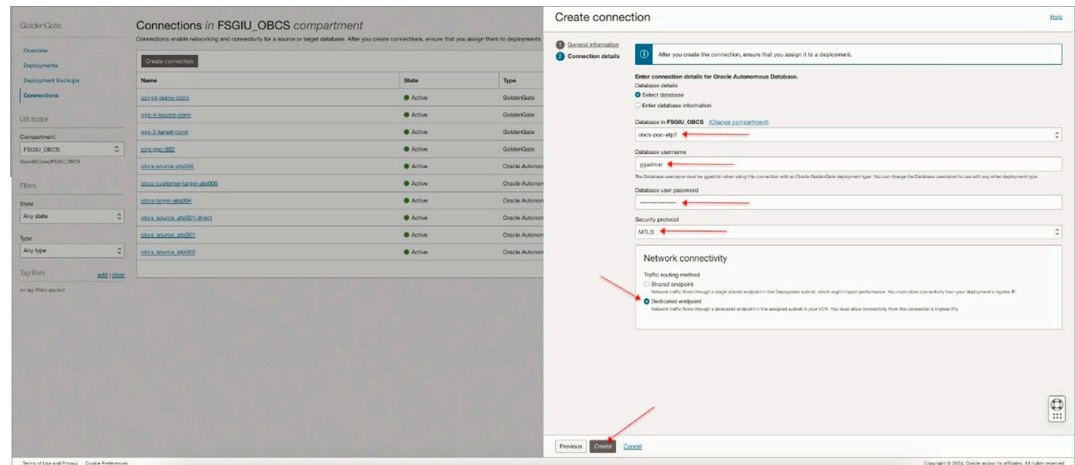
Table 2-6 Compartment Details

Field	Description
Database Information	Specify the database details.
Database Connection String	Optional Specify the database's connection string.
Database Username	Specify the username to connect to the database.
Database Password	Specify the password associated to the username provided in the previous step.
Database Wallet	Optional Drag-drop or select the wallet.zip for the database.

- **Network Connectivity:** Select a traffic routing method as follows:
 - **Shared endpoint:** To share an endpoint with the assigned deployment. User must allow connectivity from the deployment's ingress IP.
 - **Dedicated endpoint:** For network traffic through a dedicated endpoint in the assigned subnet in the VCN. User must allow connectivity from this connection's ingress IPS.
 - Select a Session mode.
 - Direct, to use the local listener running on a single database node, and then select the required subnet.
 - Redirect, to use the SCAN listener used in Oracle Real Application Cluster (RAC) deployments, and then select the required subnet.

- c. Click **Create**.

Figure 2-39 Create Connection



8. Assign the deployment details.

Figure 2-40 OBCS_POC_ATP1

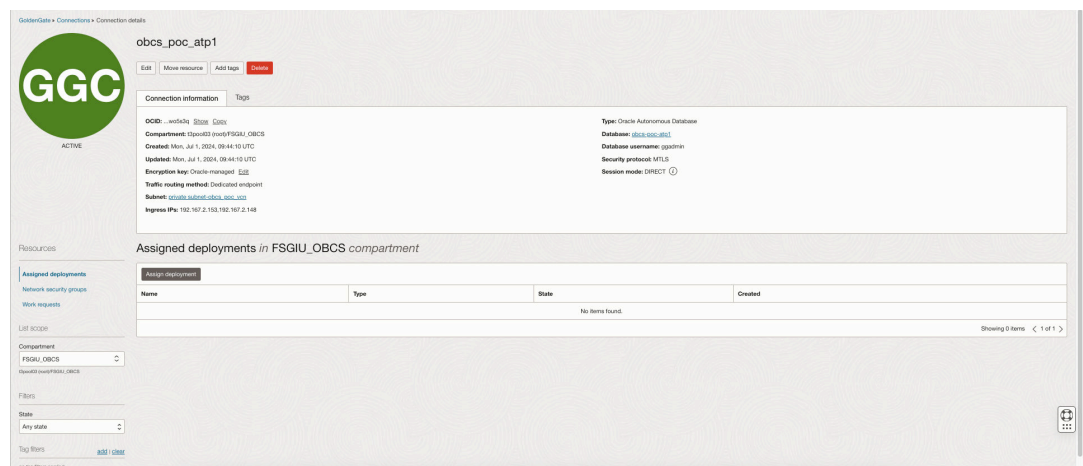
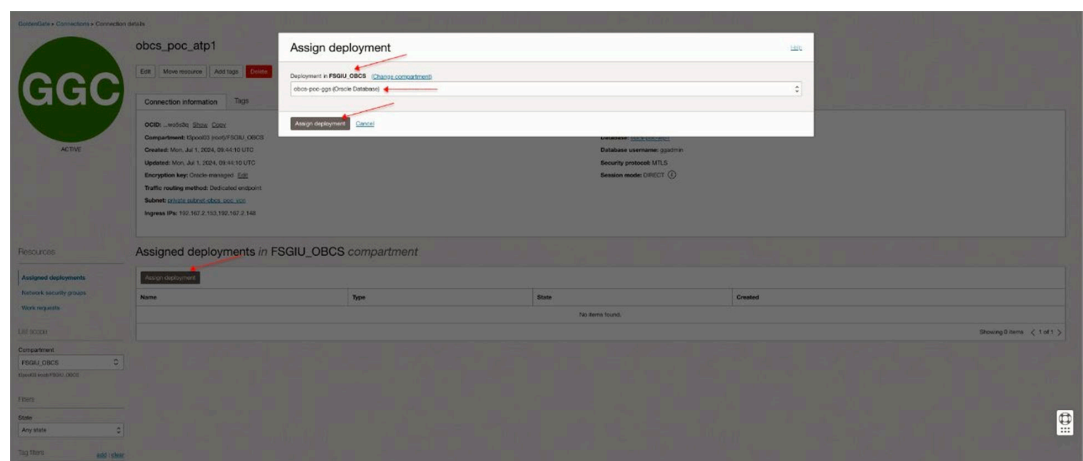
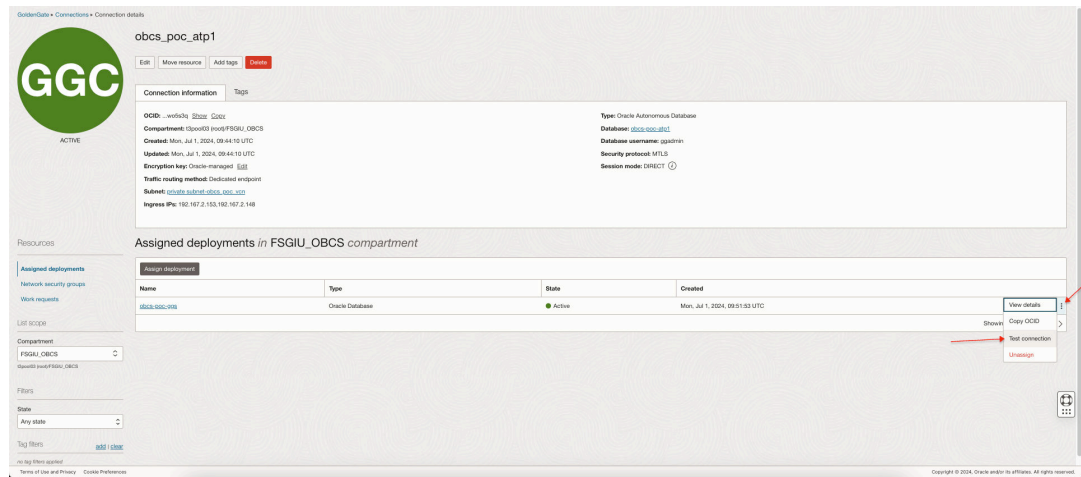


Figure 2-41 Assign Deployment



Click **Options** icon to the extreme right, for the assigned deployment and click **Test connection**.

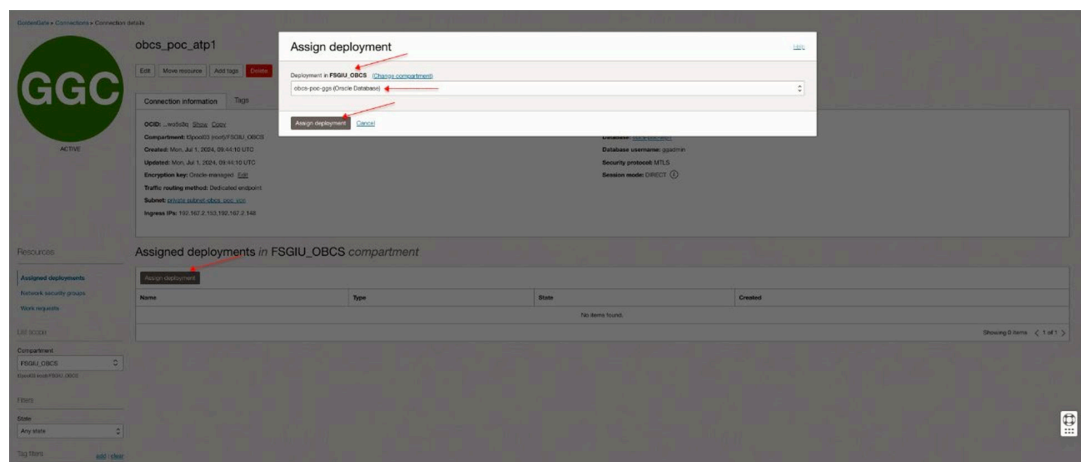
Figure 2-42 GGC - OBCS_POC_ATP1



Note

- If an error message **Network-level connectivity test failed!** is displayed, then you need to allow ingress rule for port 1522. For more information, refer [OCI Autonomous Database Setup](#).
- The user should also unlock the GGADMIN account before testing the connection.

Figure 2-43 Test Connection



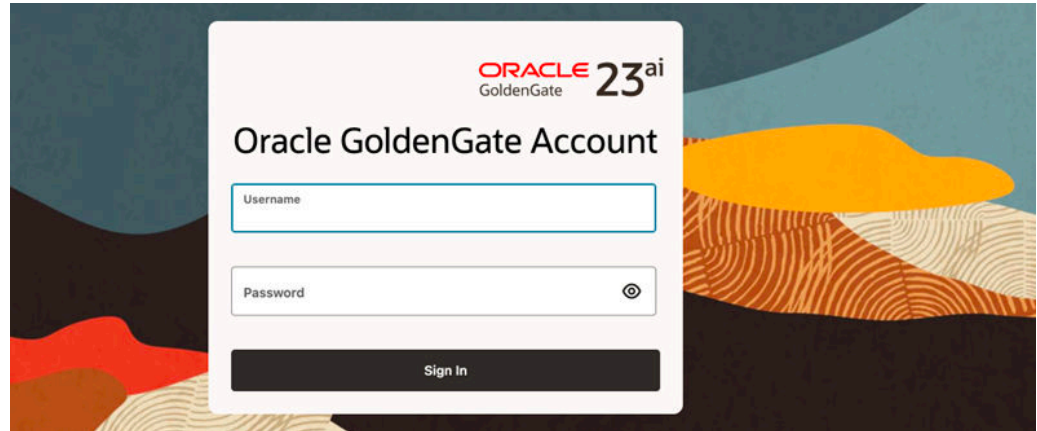
2.4.3 Configure OCI GoldenGate

This topic describes the systematic instructions to configure OCI GoldenGate.

User can configure the OCI GoldenGate by following the process below:

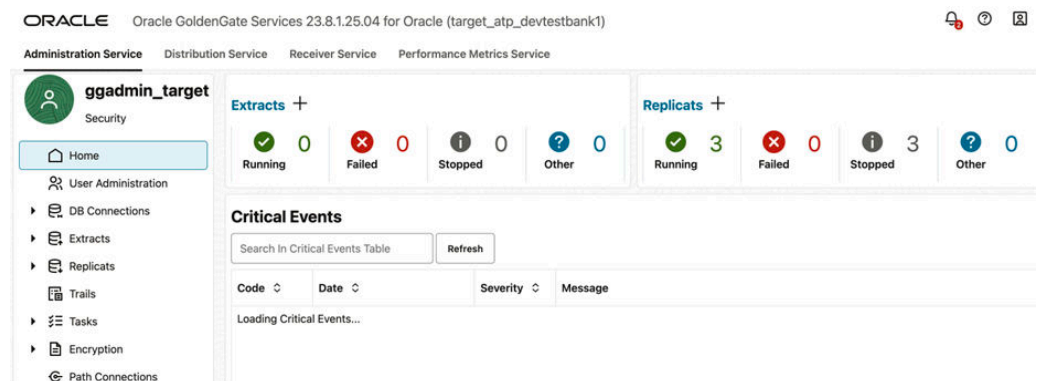
1. Access the GoldenGate Console by follows:
 - a. Use the Admin URL to access the GoldenGate console.
 - b. Login using the GGADMIN credentials.

Figure 2-44 Oracle GoldenGate Administration Service



- c. Click the **Hamburger** icon on the top left.

Figure 2-45 Administration Service



- d. To setup the target DB connection in the OCI Golden Gate Admin console, then follow the process below:
 - i. In the GoldenGate console, navigate to **DB Connections**.
 - ii. Click **Create Connection**.
 - iii. Select the database type as **Oracle Database** and provide connection details.
 - iv. Test the connection to ensure it is properly configured.

From DB Connections, in the **Actions** column of your connection, click **Connect to Database** and scroll down to **Checkpoint** Option and Click “+” to add a new **Checkpoint**.

Figure 2-46 Connection to DB

Domain	Alias	User ID	Actions
OracleGoldenGate	targettpdevtestbank1	ggadmin@DESCRIPTION=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.100)(PORT=1521)))(CONNECT_DATA=(SID=orcl))	Connect to Database: targettpdevtestbank1

Figure 2-47 Checkpoint

Checkpoint Table

The Replicat Group may require a checkpoint table. Provide the name of the Database Checkpoint Table.

Checkpoint Table
"GGADMIN"."CHKPT"

Checkpoint table to use. Required for exactly once apply semantics.

Submit

Figure 2-48 Checkpoint Details

ADMIN Security

Overview
Configuration
Profile
Debug Log
Diagnosis
Administrator

Database Key Management Parameter Files Tasks

Credentials +

Domain	Alias	User ID	Action
OracleGoldenGate	obcs_poc_atp1	ggadmin@DESCRIPTION=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.100)(PORT=1521)))(CONNECT_DATA=(SID=orcl))	

Checkpoint +

Checkpoint Table	Action
"GGADMIN"."CHKPT"	

TRANSDATA Information +

Schema Table Procedure

Search for Schema

Heartbeat +

2. Add User for Path Connection:

- Add the user for the path connection. This user should be the same as the Operator User that was created earlier in the SaaS Self-Service UI.
- In the **Administration Service** on the Left Menu's scroll down to select **Path Connection** icon and Click on "+" to create a new **Path Connection**.

- Enter the details as depicted in the image and click **Submit**.

Figure 2-49 Path Connections

Things to Consider for Path Connection Creation:

- **Credentials** – `<tenantenv>_ggnet` – The user ID and password are defined by the **source OBCS SaaS replication configuration** and are used to authenticate the **credential alias**.
- This credential alias is **exclusively used** for the **target-initiated distribution path** between the **source OBCS SaaS** and the **target OCI GoldenGate**.
- The **user ID and password** are securely shared by the **OBCS SaaS team** and must be **stored as a credential alias** on the target GoldenGate deployment.

Note

Since the path connection uses **basic authentication** for establishing the distribution path between the **extract** and **replicat**, it is important to maintain the same credentials. If the username and/or password is modified without proper communication or update in both environments, the **data replication process will break**.

3. Create KMS profile(applicable only for BYOK opted customers). This is the OCI vault details which was shared to OBCS SaaS. For creating the profile, follow the process below:
 - a. In the GoldenGate console, navigate to **Encryption** and select **Profile**.
 - b. In the Oracle Cloud Infrastructure section Click “+” to add a new profile.

Figure 2-50 Create an Encryption Profile

Create Encryption Profile

Create an encryption profile for encrypting trails using a masterkey saved in OCI Key Management Service (KMS). Specify the crypto endpoint URL, tenancy OCID, key OCID, user OCID and the API key and fingerprint. Please also add the OCI KMS CA cert (via the ServiceManager) to the deployment truststore.

Profile Name Required

Description

Encryption Profile Type
Oracle Cloud Infrastructure (OCI)

Default Profile ☐

Crypto Endpoint URL Required

Tenancy OCID Required

Key OCID Required

User OCID Required

API Key Required

Key Fingerprint Required

Submit

4. Create Replicat, by following the process below:
 - a. In the OCI GoldenGate Admin console, navigate to **Administration Service**, and click **Home**.
 - b. Click **Add** next to **Replicats** to create a Replicat task that will apply data to the target database.
 - c. In the Replicat Options provide the details as instructed below,
 - **TrailName** : This can be the same trail name used in the **SaaS Self-Service UI**, or the user can specify a different trail name. The **same trail name** must be used later when creating the **Target-Initiated Path** to ensure proper linkage between the source and target environments.
 - **Encryption Profile**: Select the appropriate encryption profile based on your configuration:
 - **LocalWallet** – For **non-BYOK** (Bring Your Own Key) users.
 - **Desired Profile** – For **BYOK** users, select the encryption profile created under **KMS Profile Management**.
 - **Target Credentials**: Select the desired **Target Credentials** and its corresponding **Credential Alias** from the list.
 - **Checkpoint Table**: Select the desired **Checkpoint** from the list.
 - **Parameter File**: Create the parameter file as per the requirement and Click **Create** to create the Replicat.

Figure 2-51 Administration Service Home

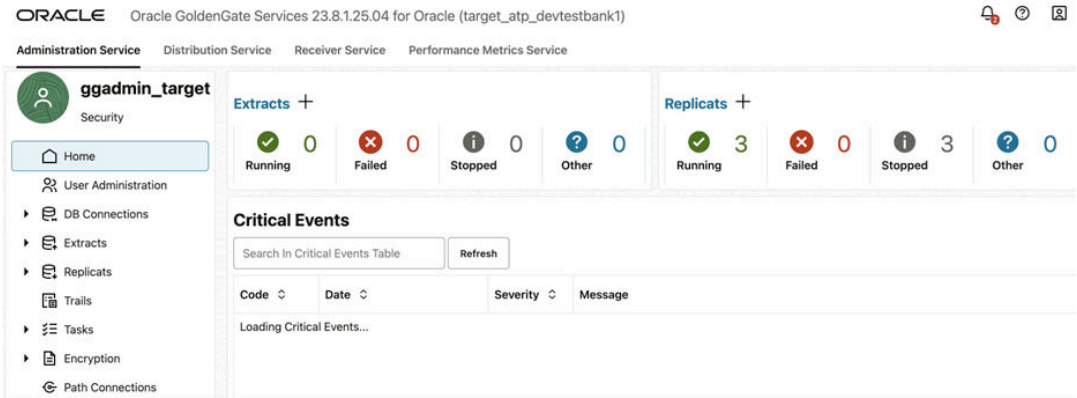


Figure 2-52 Replicat Type

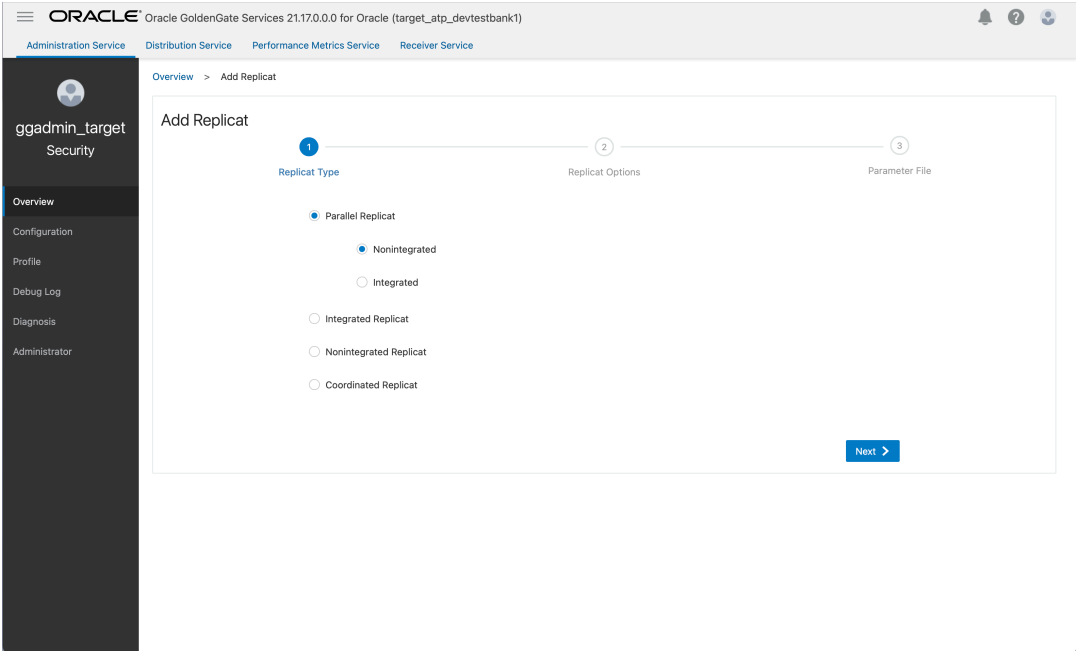


Figure 2-53 Replicat Options

The figure consists of three screenshots of the 'Add Replicat' wizard, showing steps 1, 2, and 3 of the configuration process.

Step 1: Replicat Information

The Replicat requires Trail Details and Target Credentials. Specify the required Replicat details.

Replicat Trail

Name: np Subdirectory: Encryption Profile: LocalWallet

Target Credentials

Domain: OracleGoldenGate Alias: targetatp998

Checkpoint Table: "GGADMIN"."TARGETCHKPT"

Begin: Position in Log

Buttons: Back, Next

Step 2: Managed Options

There are additional management options for Replicat. It is optional to add the AutoStart and AutoRestart details.

Profile Name: Default Critical to deployment health: ☐

Auto Start: Start after 0 sec delay

Auto Restart: Restart when process fails after 5 mins delay and will be attempted within 24 hrs window and maximum 200 retries

Buttons: Back, Next

Step 3: Parameter File

The most basic setting for the Replicat parameter file is provided. The parameter settings for the Replicat Group can be customized.

Parameter File Content:

```
REPLICAT TestR
USERID ALIAS targetatp998 DOMAIN OracleGoldenGate
MAP ** , TARGET **;
```

5. To Start the Replicat, click on the Options(...) and select Start with Options, using the AFTERCSN parameter with the snapshot SCN obtained from the self-service UI.

Note

When the target database is hydrated using an export snapshot. This ensures that Replicat skips all trail records prior to the snapshot point and begins processing only new changes. Using AFTERCSN prevents data overlap between the initial load and ongoing replication, thereby avoiding duplicate operations and potential Replicat abends.

Figure 2-54 Start Replicat with Options

Start Replicat with Options

Allows you to change the Replicat start point, CSN, filter duplicates, and threads options, then starts the Replicat.

Start Point:
At CSN

CSN

Filter Duplicates:
☒

Threads:

Submit

2.4.4 Target Initiated Distribution Path

This topic provides information on target distribution path.

The target receiver server must establish a connection path to the source distribution server. This setup enables the OCI GoldenGate deployment to pull trail files from the source to the target OCI GoldenGate environment.

To create a Target-Initiated Distribution Path, follow the steps below:

1. In the OCI GoldenGate self-service console, go to the **Receiver Service** section.
2. Under the Receiver Service page, locate and select the **Target-Initiated Path** option.
3. Click on the “+” symbol to create a new Target-Initiated Path.
4. **Enter the Path Details** as shown in the images below, and then click **Create Path** to complete the configuration.
 - a. **Path Name** – Enter a unique name for the path.
 - b. **Source Host / Endpoint** – Specify the source distribution server hostname or IP.
 - c. **Port** – Enter the listener port of the source distribution service.
 - d. **Authentication Details** – Provide the Operator username and password from the source deployment.
 - e. **Encryption Profile** – Select the required encryption profile (OCI Vault or Local Wallet).

Figure 2-55 Add Receiver path



Figure 2-56 Create Path

Add Path

1 Path Information 2 Source Options 3 Target Options 4 Advanced Options 5 Filtering Options 6 Managed Options

Controlled by the target system, the target initiated Path routes trail data from the source to the target system. Provide a name for the Path.

Path Name: PATHNAME Description: Path Description

Next

Add Path

Different protocols (WSS, and WS) are required for the Target Initiated Path. Specify the desired protocol and add the required source details.

Source Protocol: WSS Reverse proxy enabled: ☐

Source Host: obcsipresales.obcs.ocs.oc-test.com Port Number: 443

Trail Name: ap Subdirectory:

Edit Source Path: prod/ggs/services/v2/sources?trail=ap Encryption Profile: LocalWallet

Source Authentication Method: UserID Alias

Domain: #Size:

Back Next

Add Path

Trail Name: ap Subdirectory:

Edit Source Path: prod/ggs/services/v2/sources?trail=ap Encryption Profile: LocalWallet

Source Authentication Method: UserID Alias

Domain: Network Alias: OperatorUser Required

Begin Position in Log:

Source Log: Sequence Number: 0 RSA Offset: 0

Back Next

Add Path

1 Path Information 2 Source Options 3 Target Options 4 Advanced Options 5 Filtering Options 6 Managed Options

The Target initiated Path requires the Trail location at the target system. Specify the Trail file and directory.

Trail Name: ap Subdirectory: Trail Size (MB): 500

Target Encryption Algorithm: NONE Change Encryption: ☐

Generated Target URI: trail://localhost/services/recv/v2/targets?trail=ap

Target Type: GGSFormat

Back Next

Add Path

1 Path Information 2 Source Options 3 Target Options 4 Advanced Options 5 Filtering Options 6 Managed Options

Advanced Network Options may be required. Adjust advanced Network options if needed.

Inhibit Network Compression: ☐ Compression Threshold: 100

SO Delay (milliseconds): 10 Checkpoint Frequency: 10

TCP Flush Bytes: TCP Flush Seconds:

DSCP: DEFAULT TOS: DEFAULT

FCB_MODELAY: ☐ Queue ACK: ☐ TCP_NODELAY: ☐

Back Next

Add Path

1 Path Information 2 Source Options 3 Target Options 4 Advanced Options 5 Filtering Options 6 Managed Options

Rules are used for filtering within the Trail. Exclude and include the specified types and provide the necessary details to it.

Rule Name: Rule Action: ☒ Exclude ☐ Include

Filter Type: Object Type

Object Types: Negative: ☐

Add

Back Next

Add Path

1 Path Information 2 Source Options 3 Target Options 4 Advanced Options 5 Filtering Options 6 Managed Options

Additional AutoRestart Options can be added to the DistPath. Adjust the AutoRestart Retries and Delays if needed.

Critical: Auto Restart:

User should note the following configuration settings while creating the **Target-Initiated Distribution Path**:

- **Reverse Proxy Enabled?** → Off
- **Source Authentication Method** → UserID Alias
- **Source** → WSS
- **Source Host** → <host:port> (provided by the OBCS SaaS team via Service Request)
- **Source Trail Name** → <trail name> (same as the trail name used in Extract)
- **Source Alias** → *dt1np_ggnet alias created in the Credentials step above*
- **Target Trail Name** → np (can be any two-letter name)
- **Auto Restart** → On

Note

Adding the OBCS App unique URI path in the source breaks the Generated Source URI.

Hence, make sure the Generated Source URI is edited as shown below: `wss://obcspresales.obcs.ocs.oc-test.com/nonprod/ggs:443/services/v2/sources?trail=np`

Change to

`wss://obcspresales.obcs.ocs.oc-test.com:443/non-prod/ggs/services/v2/sources?trail=np`

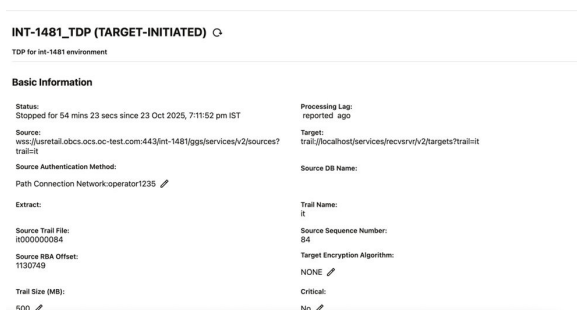
After successfully creating the Distribution Path, the newly created path will be displayed on the Target-Initiated Distribution Path page.

Figure 2-57 Receiver current State



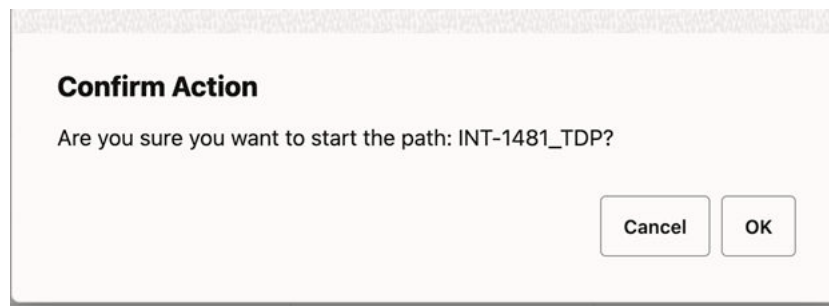
- To validate the **Target-Initiated Path**, navigate to the **Target-Initiated Path** menu on the left, click on the **started path**, and then select **Path Statistics**.
- You should now be able to view the **Path statistics**, displaying details such as **DDL changes**, **table updates**, and other relevant replication metrics.

Figure 2-58 Receiver current Details



- Navigate back to Target Initiated Path and from the **Action** list for the Path, select **Start**.

Figure 2-59 Start Receiver Service



- Once the path is **up and running**, navigate to **Target-Initiated Path** from the left-hand menu and click on the **created path** to view its details.

Figure 2-60 Target-Initiated Path

INT-1481_TDP	Running	0 sec	ⓘ ⌵ 🗑️ ⋮
--------------	---------	-------	--

- To validate the **Target-Initiated Path**, navigate to the **Target-Initiated Path** menu on the left, click on the **started path**, and then select **Path Statistics**.
- You should now be able to view the **Path statistics**, displaying details such as **DDL changes**, **table updates**, and other relevant replication metrics.

Figure 2-61 Path statistics

Statistics						
LCR Table		DDL Table				
Type	Current Value	Type	Inserts	Updates	Upserts	Deletes
LCR Read from Trails	11	DMLs	4	6	0	0
LCR Sent	11					
LCR Filtered	0					
DDL Read from Trails	0					
DDL Sent	0					
DDL Filtered	0					
Procedure	0					
Statistics Table						
Search in Statistics Table						
Table Name	Inserts	Deletes	Updates	Upserts	LCR Read	LCR Sent
PARTY.PERCENTAGE_COMPLETION	2	0	2	0	4	4
PARTY.PLATO_DATALOAD_FILE_UPLOAD_ENTRY	2	0	4	0	6	6

- This confirms that the **SaaS-to-PaaS Data Replication** has been successfully established and that the **target** is actively **pulling trail files** from the **SaaS** environment.
- [Target OCI GoldenGate Deployment in devcorp](#)
This topic provides information on target OCI goldengate deployment.

2.4.4.1 Target OCI GoldenGate Deployment in devcorp

This topic provides information on target OCI goldengate deployment.

Due to the limitation of devcorp, the t3 tenancy will not be accessible to the Oracle Internal Network which includes devcorp. The above Target Environment setup will work on GBUPROD.

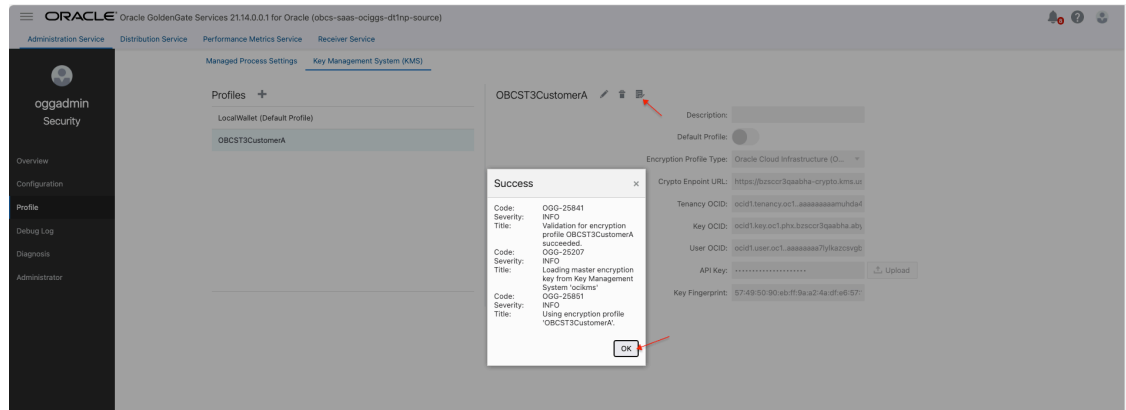
To demonstrate the end-to-end Customer to SaaS data replication via Target Initiated Distribution Path, there is a provision for another OCI GoldenGate Deployment in devcorp environment itself under the compartment CNE_DB.

Note

Add a KMS Profile in Source OCI GoldenGate Deployment.

Figure 2-62 Key Management System Profile

The screenshot displays the Oracle GoldenGate Services 21.17.0.0.0 for Oracle (target_atp_devtestbank1) interface. The left sidebar shows the navigation menu with 'Profile' selected. The main content area is titled 'Managed Process Settings' and 'Key Management System (KMS)'. It features a 'Profiles' section with a '+' icon and a list of profiles, including 'LocalWallet (Default Profile)'. The right panel shows the configuration form for a new profile, 'testProfile'. The form includes fields for 'Profile Name', 'Description', 'Default Profile' (a toggle switch), 'Encryption Profile Type' (set to 'Oracle Cloud Infrastructure (O...)', 'Crypto Endpoint URL', 'Tenancy OCID', 'Key OCID', 'User OCID', 'API Key' (with an 'Upload' button), and 'Key Fingerprint'. At the bottom, there are 'Cancel' and 'Submit' buttons.

Figure 2-63 Success Message

If user gets multi-level exception such as Vault Not Found or User is Unauthorized, then it could be due to some glitch on the devcorp or a copy paste error in the details that has been entered. To resolve, delete the Profile and recreate it.

3

Functional Activity Codes

This topic provides the functional activity codes available in data replication.

Table 3-1 Functional Activity Codes

Screen Name	Functional Activity Codes	Description
Initiate Data Export	INITIATE_DATA_EXPORT_FA	Steps for initiating data export.
Integrated Extract	INTEGRATED_EXTRACT_FA	Accessing the extract process API.
KMS Profile Management	KMS_PROFILE_MANAGEMENT_FA	Accessing the KMS profile management API.
Key Management	KEY_MANAGEMENT_FA	Accessing the encryption keys API.
Administration Service	ADMINISTRATION_SERVICE_FA	Accessing Operator User page to create Operator user and add TranData
Distribution Service	DISTRIBUTION_SERVICE_FA	FA for accessing Distribution Service related pages that included Target path information and statistics

Index

A

Administration, [2](#)
Administration Service, [27](#)

C

Checkpoint, [19](#)
Configure OCI GoldenGate, [29](#)
Connect to the ATP Instance, [16](#)
Create a Vault, [9](#)
Create an OCI GoldenGate Deployment, [21](#)
Create and Configure the ATP Instance, [12](#)
Create Extract, [12](#)
Create Master Encryption Key, [11](#)
Create the Connection, [26](#)
CSN Based Extract Creation, [16](#)

D

Data Replication PaaS Setup, [1](#)
Database Setup, [19](#)
Distribution Service, [31](#)
Downloading dump with PAR URL, [17](#)

E

Extract Management, [11](#)

F

Functional Activity Codes, [1](#)

I

Identity and Security, [3](#)
Import Data from Object Storage, [17](#)
Initiate Data Export, [3](#), [7](#)
Integrated Extract, [10](#)

K

Key Management, [25](#)
Key Management System(KMS) Selection, [4](#)
KMS Profile Management, [22](#)

L

Local Wallet, [5](#)

M

Manage Extract, [13](#)

N

Network Setup, [5](#)

O

OCI Autonomous Database Setup, [12](#)
OCI GoldenGate Deployment Setup, [21](#)
OCI Policies, [4](#)
OCI Setup, [1](#)
OCI Vault, [7](#)
OCI Vault Setup, [9](#)
Operator User Creation, [27](#)

P

Parameters, [20](#)
Path Info, [32](#)
Path Stats, [33](#)
Profile Flow, [4](#)

R

Report, [21](#)

S

SaaS Self Service UI, [1](#)
Statistics, [21](#)

T

Target Initiated Distribution Path, [36](#)
Target OCI GoldenGate Deployment in devcorp, [41](#)
Trails, [28](#)
TranData, [29](#)

Troubleshooting, [20](#)