Oracle® Banking Microservices Architecture

SaaS to PaaS Data Replication User Guide

Innovation Release 14.8.1.0.0
G45838-02
October 2025

Oracle Banking Microservices Architecture SaaS to PaaS Data Replication User Guide, Innovation Release 14.8.1.0.0

G45838-02

Copyright © 2025, 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

2 Data Replication PaaS Setup

Copyright © 2025, Oracle and/or its affiliates.

3 Functional Activity Codes

Index

Copyright © 2025, Oracle and/or its affiliates.

Preface

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

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:

Copyright © 2025, Oracle and/or its affiliates.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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 Managnement 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.

Copyright © 2025, Oracle and/or its affiliates.

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.

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

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:

Copyright © 2025, Oracle and/or its affiliates.

- 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 1-1 Data Export Landing Page

- Profile Flow
  This topic provides information on profile flows.
- Operator User Creation
  This topic describes the systematic instruction on operating the user creation.
- Initiate 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) Profile
  This topic provides information about KMS profile .

1.1.1.1 Key Management System(KMS) Profile

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.

Copyright © 2025, Oracle and/or its affiliates.

- 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 -e -m PEM -f my_ssh_key.pub > my_ssh_key_public.pem
   ```

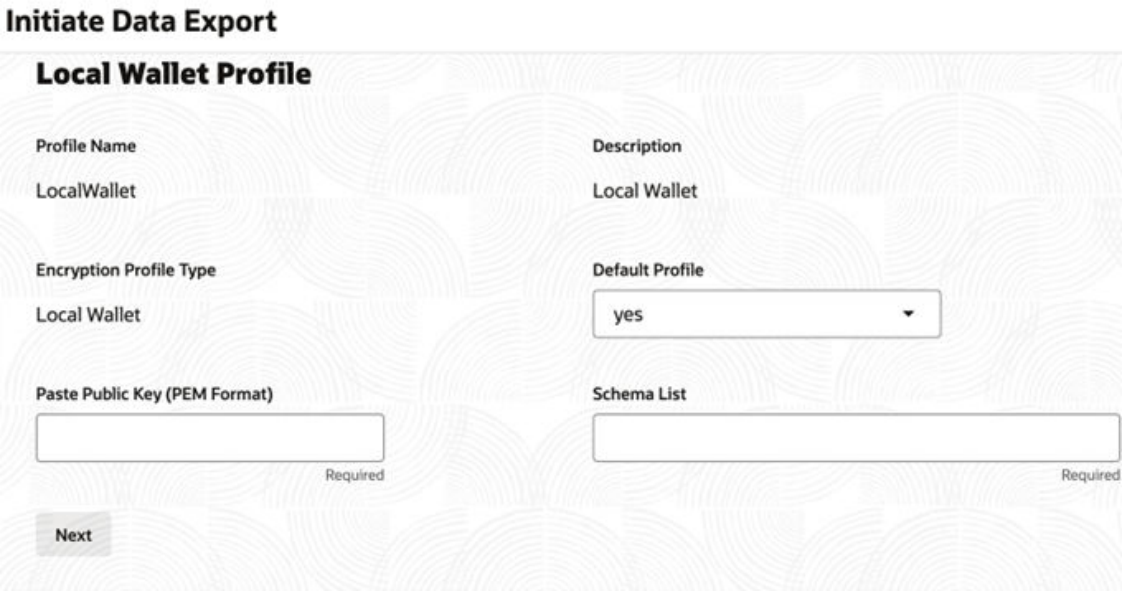
3. Convert the SSH Private Key to PEM Format

   ```
   ssh-keygen -p -m PEM -f my_ssh_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**.

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-2 Local Wallet Operation



1.1.1.1.2 OCI Vault

This topic provides information on OCI vault.

If the customer has opted for **BYOK**, they can create a new **KMS Profile** with the **Encryption Profile type** set to OCI Vault.

Steps to Create a KMS Profile:

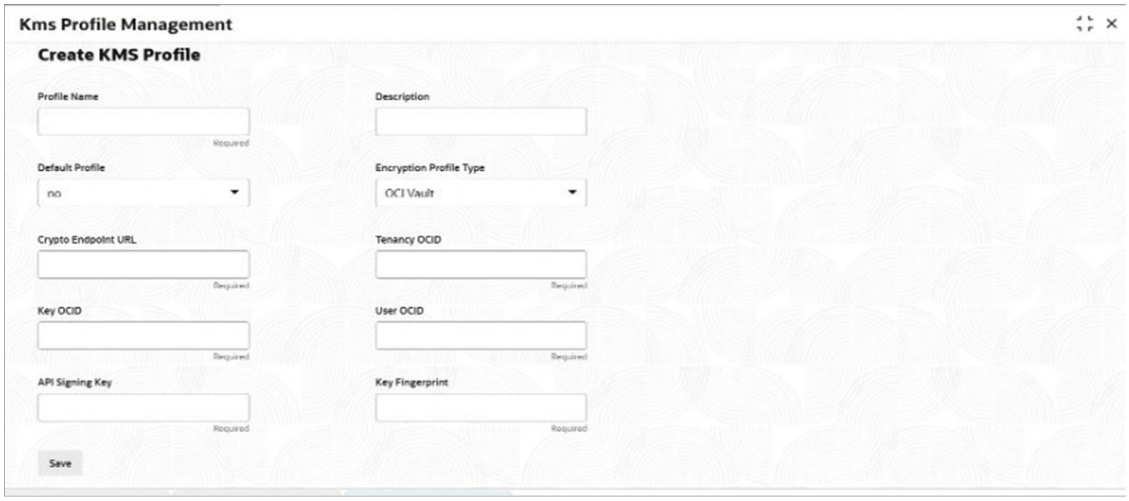
1. The customer must create an **OCI service account** (an **OCI IAM user account without a password**) and generate an **associated API key** for authentication.
2. Click **Create Profile** to open the Create KMS Profile section.

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**.

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-3 Create KMS Profile



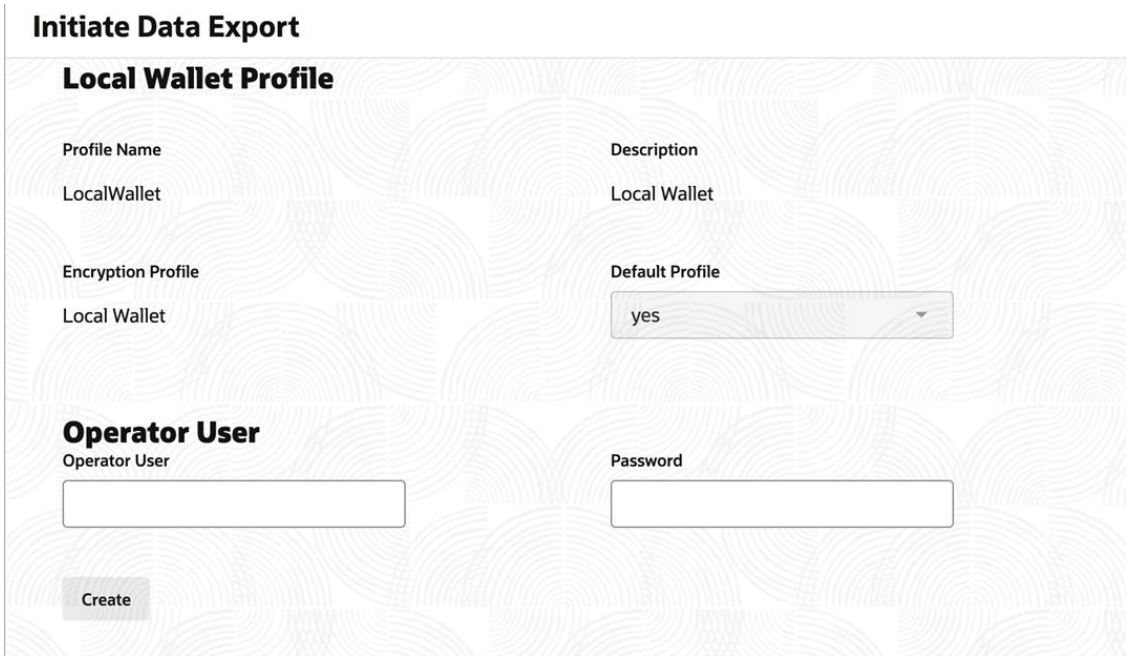
1.1.2 Operator User Creation

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.

Figure 1-4 Operator User Creation



Copyright © 2025, Oracle and/or its affiliates.

1.1.3 Initiate Export

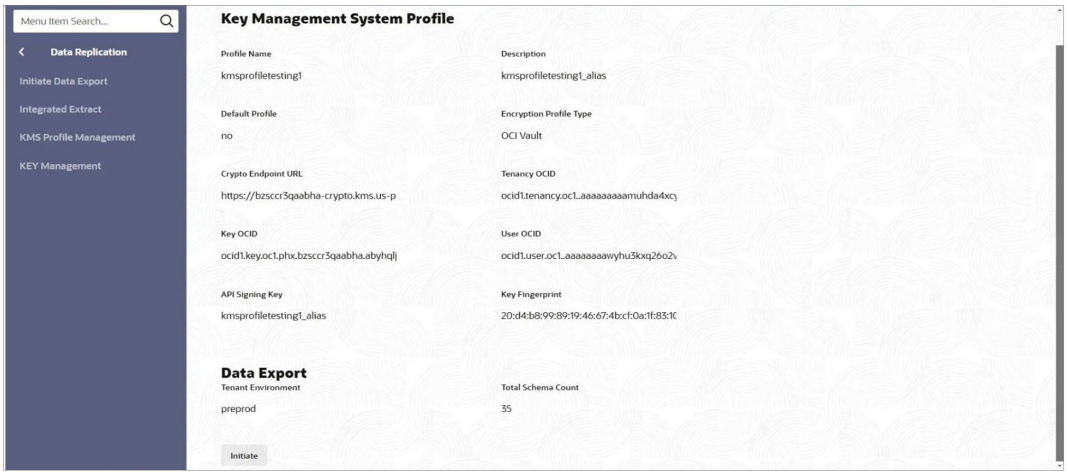
This topic describes the systematic instructions to initiate an export.

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

To initiate data export:

1. OCI Vault – available for BYOK customers.Local Wallet – the default option for other customers.
   - **OCI Vault**: Available for BYOK customers.
   - **Local Wallet**: Default option for other customers.
2. Start the export process.
3. Retrieve PAR URLs for:
   - Data dump files.
   - Encryption keys (ciphertext and AES-256 key).
4. Download the exported data using the provided PAR URLs.

Figure 1-5 Initiate Data Export



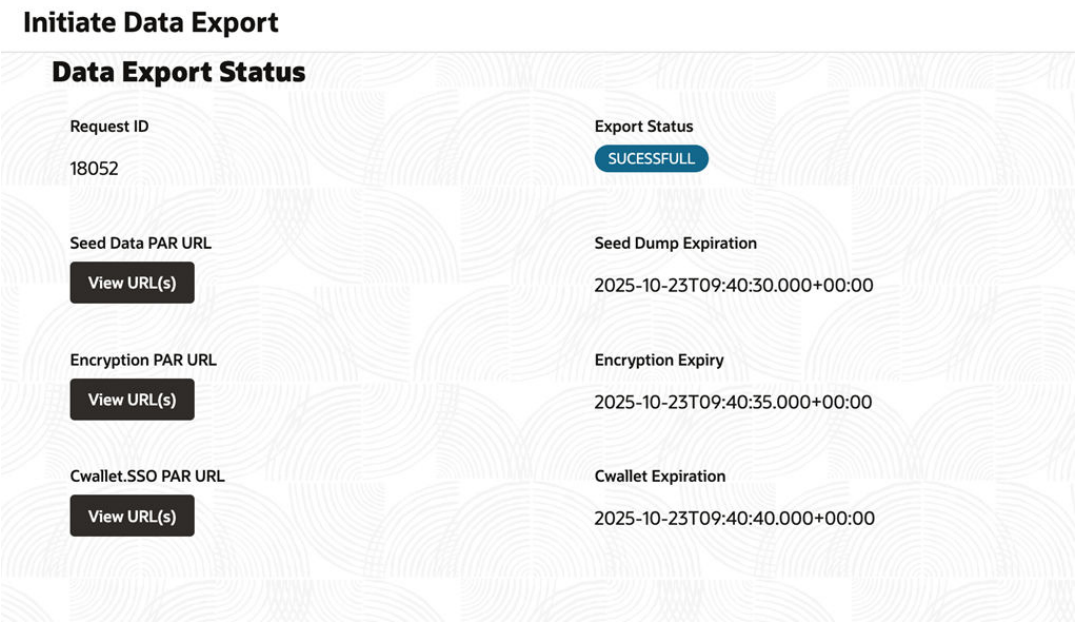
If this is the first time performing the export, the user will receive a **confirmation** that the export has been successfully initiated.

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**.

The UI prevents initiating a new export if the user has already completed an export within the recent period.

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-6 Initiate Data Export Status



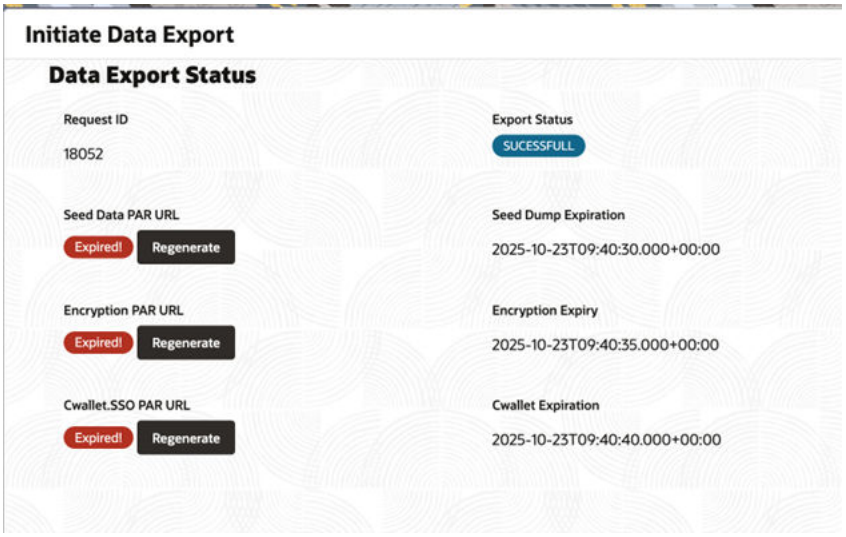
The PAR URLs for the dump files are **time-sensitive** and remain valid for approximately **two hours** from the time they are generated. If a PAR URL expires before the user downloads the file, a new URL can be generated by clicking the **Regenerate PAR URL** button on the **Data Export Status** page.

Additionally, the exported dump files remain available in **Object Storage** for **seven days**. After this period, the files are automatically removed or expired. If access to the initial dump is required after expiration, a **service request (SR)** must be raised with consulting to enable the export again.

> **Note**
>
> It is recommended to **download the dump files and import them into the target database** as soon as possible.

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-7 Regenerate PAR URL



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 intrgeated extracts.

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.

- 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 Create Extract

This topic describes the systematic instructions to create an extract.

Copyright © 2025, Oracle and/or its affiliates.

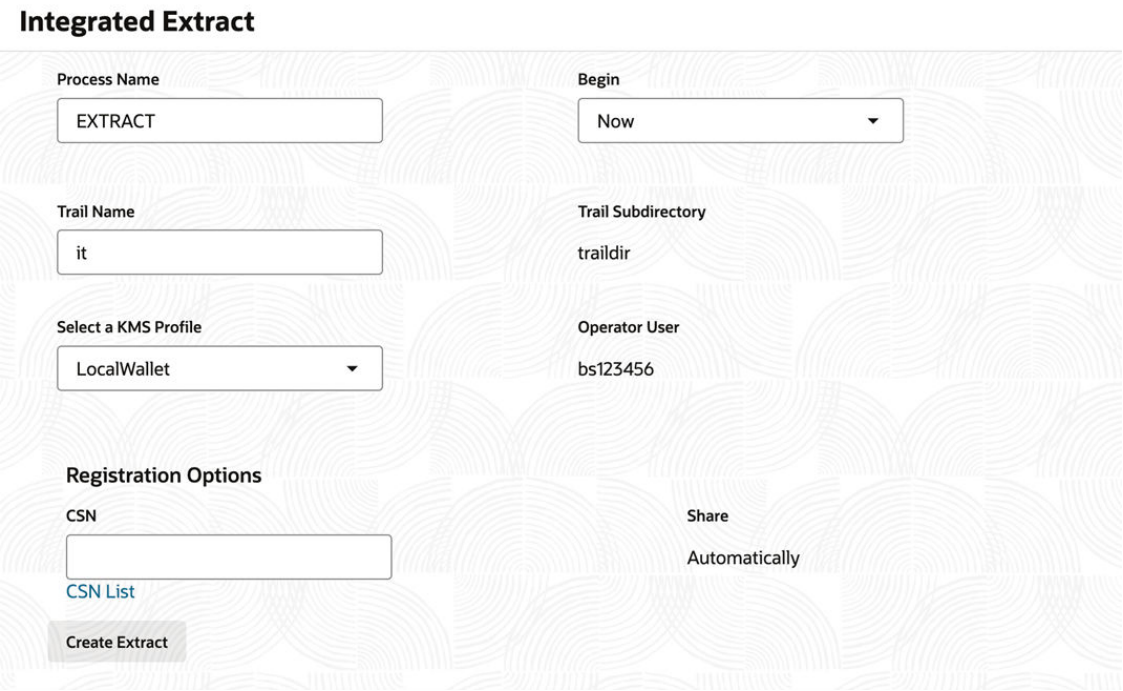
The user can create a new extract by selecting the **preferred start time** and **encryption profile**, then clicking **Create**.

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 1-8 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.

Copyright © 2025, Oracle and/or its affiliates.

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 **section2.2.3**

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 1-9 CSN Details

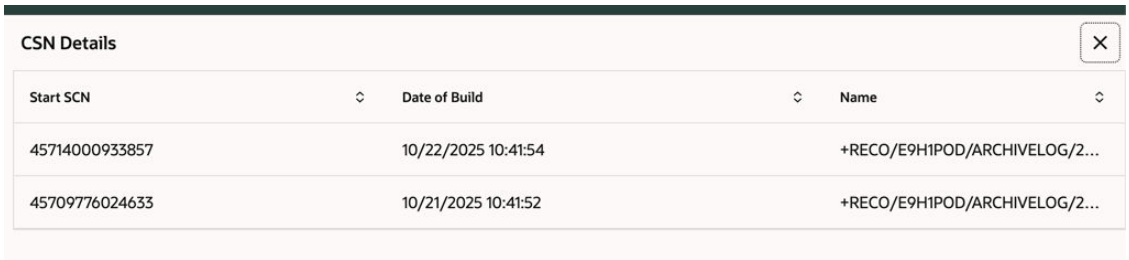
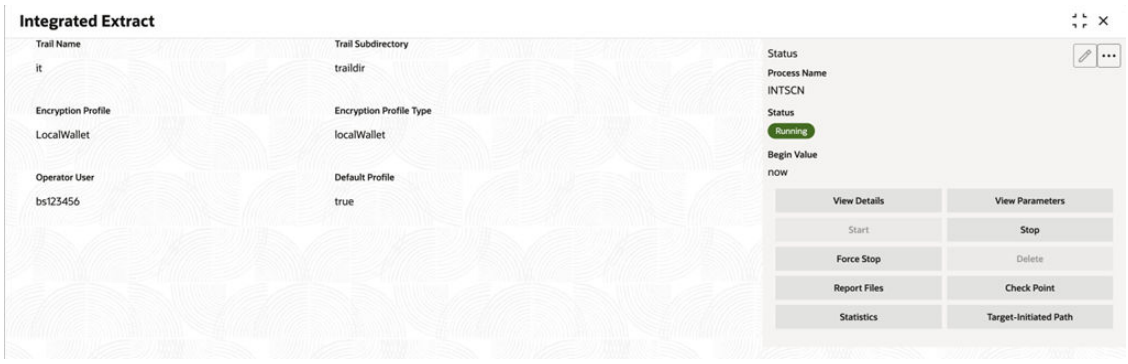


Figure 1-10 Extract Details Page



1.2.2 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**, **View Parameters**, **Report Files,Checkpoint,Statistics, Target-Initiated Path** 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 the **Now** option to start immediately or specifying a **CSN** to begin from a particular commit point in the source database. 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.

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-11 Start Extract with CSN from CSN List

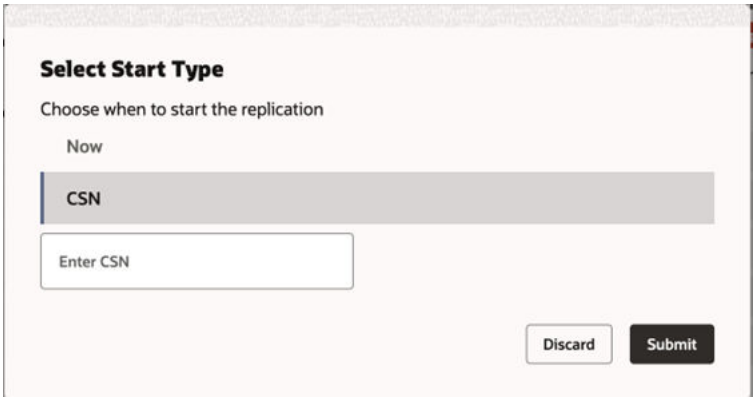
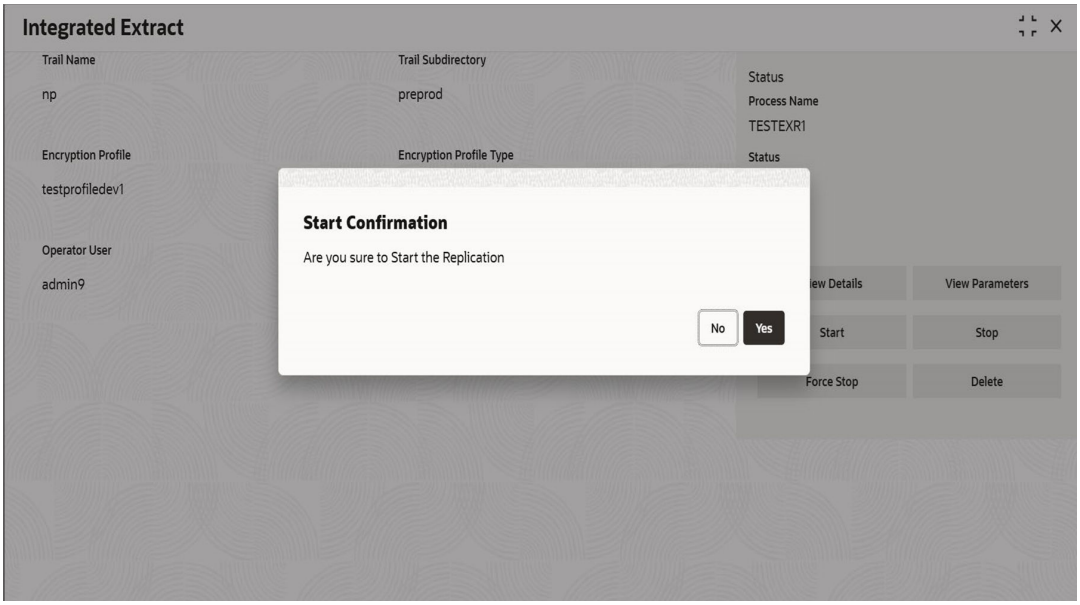


Figure 1-12 Start Extract with Now

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

Figure 1-13 Start Extract



Copyright © 2025, Oracle and/or its affiliates.

- **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 1-14 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 1-15 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 1-16 Force Stop Extract

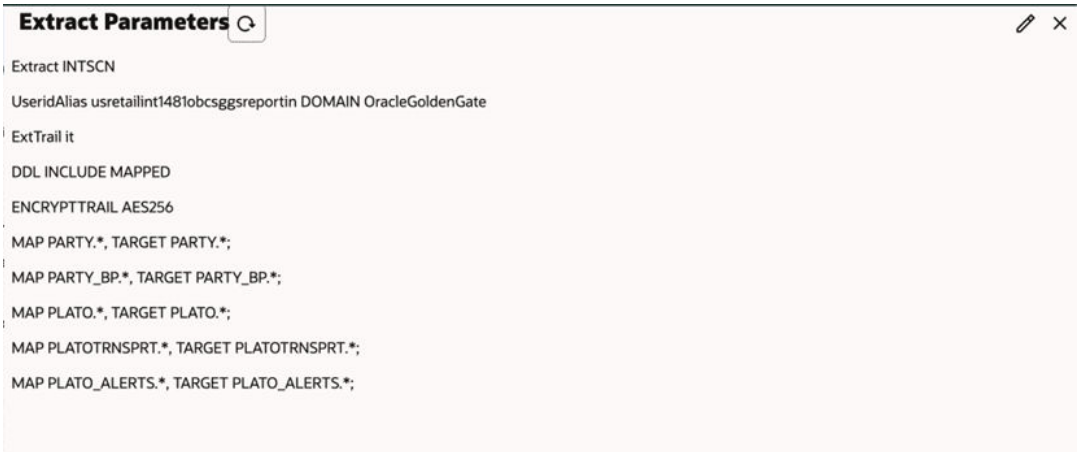
- **View Details**: This action displays detailed information about the extract, including the **trail name**, **lag details**, **trail sequence** and **trail size**.

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-17 View Details

- **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**.

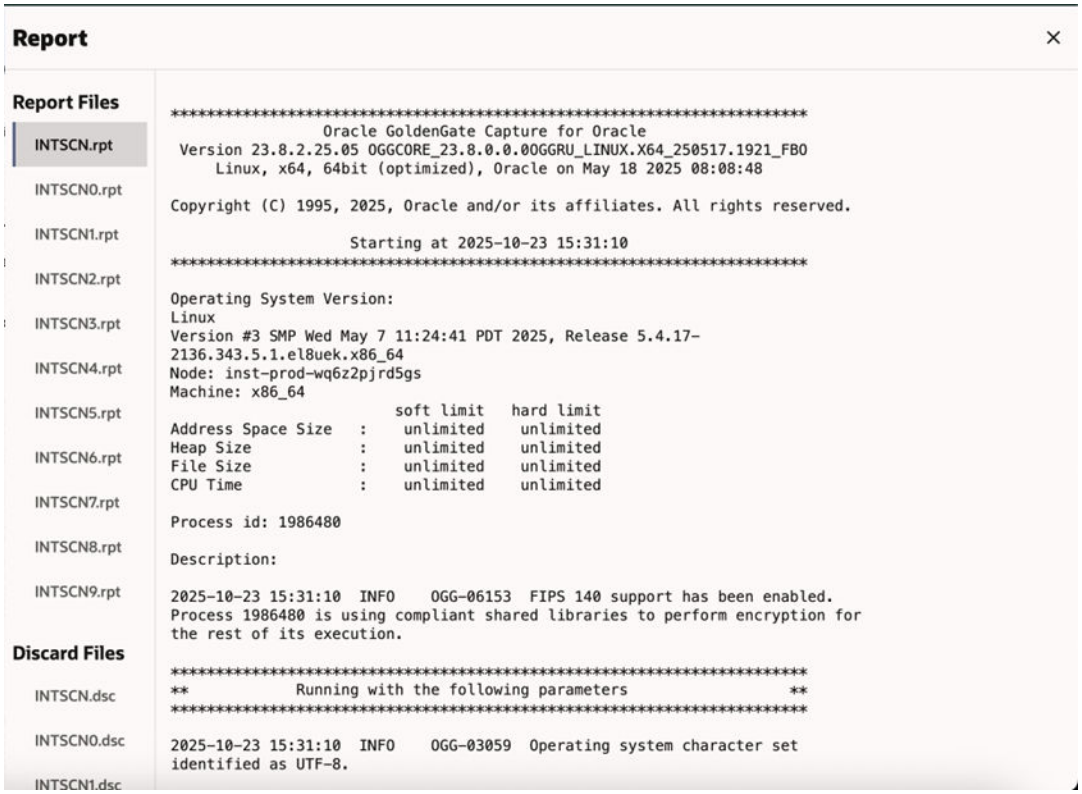
Figure 1-18 View/ Edit Parameter



- **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.

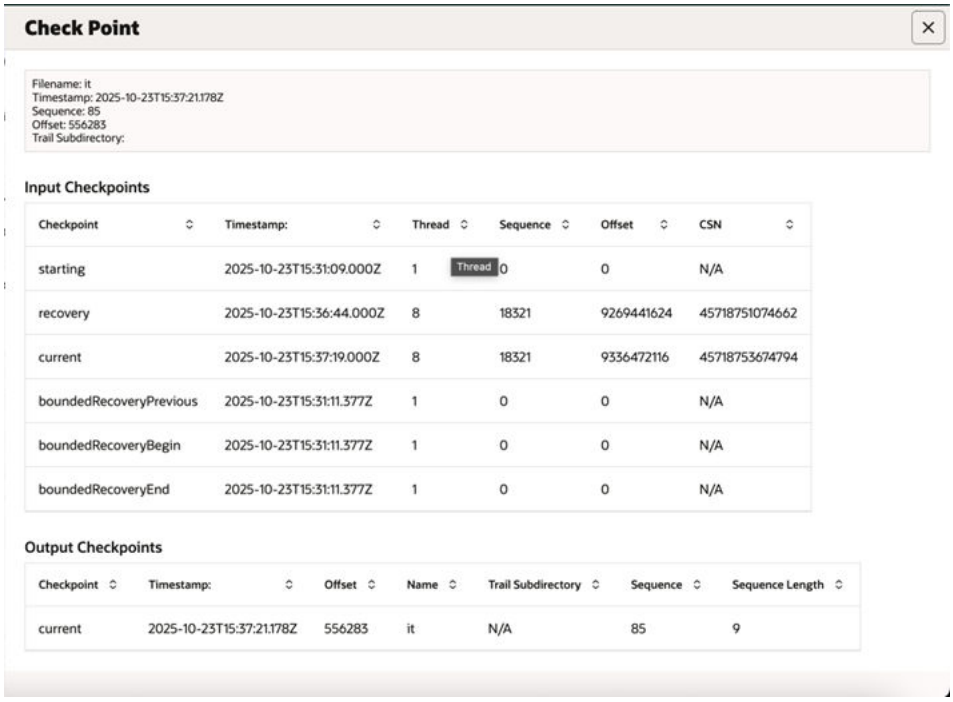
Copyright © 2025, Oracle and/or its affiliates.

Figure 1-19 Report Files



- **Check Point:** 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 Positionand Checkpoint Updates**.

Figure 1-20 Check Point



Copyright © 2025, Oracle and/or its affiliates.

- **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.

Figure 1-21 Statistics

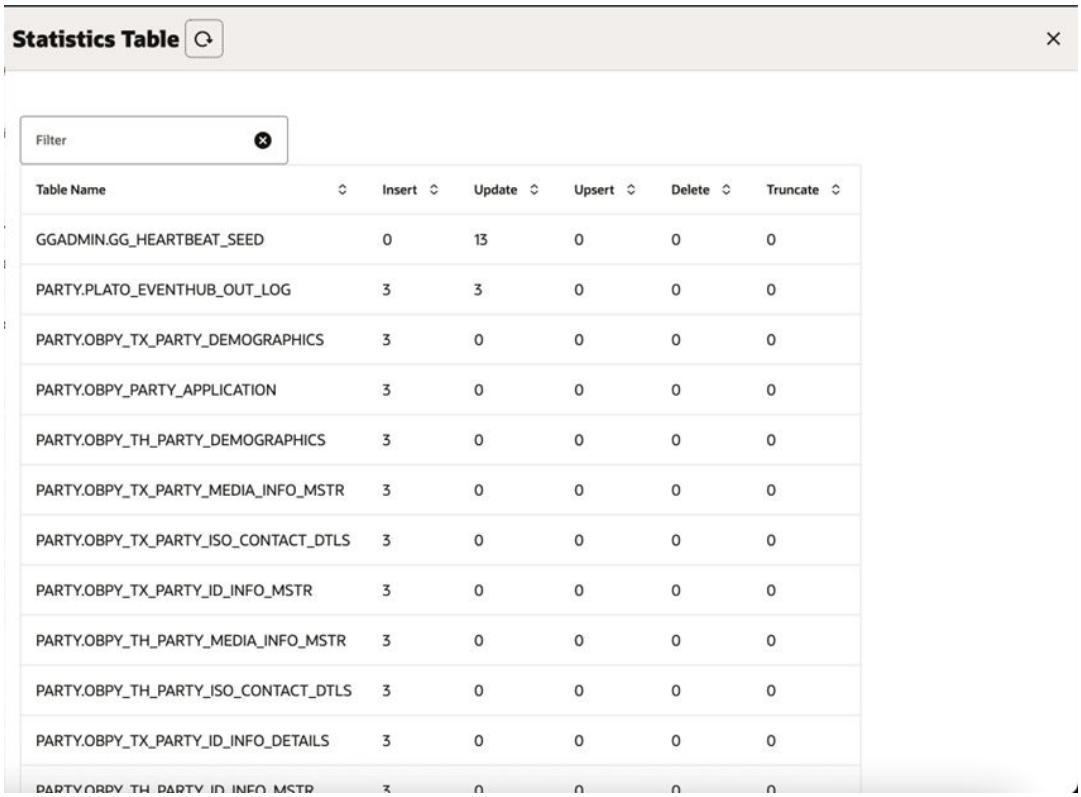


Table Name	Insert	Update	Upsert	Delete	Truncate
GGADMIN.GG_HEARTBEAT_SEED	0	13	0	0	0
PARTY.PLATO_EVENTHUB_OUT_LOG	3	3	0	0	0
PARTY.OBPY_TX_PARTY_DEMOGRAPHICS	3	0	0	0	0
PARTY.OBPY_PARTY_APPLICATION	3	0	0	0	0
PARTY.OBPY_TH_PARTY_DEMOGRAPHICS	3	0	0	0	0
PARTY.OBPY_TX_PARTY_MEDIA_INFO_MSTR	3	0	0	0	0
PARTY.OBPY_TX_PARTY_ISO_CONTACT_DTLS	3	0	0	0	0
PARTY.OBPY_TX_PARTY_ID_INFO_MSTR	3	0	0	0	0
PARTY.OBPY_TH_PARTY_MEDIA_INFO_MSTR	3	0	0	0	0
PARTY.OBPY_TH_PARTY_ISO_CONTACT_DTLS	3	0	0	0	0
PARTY.OBPY_TX_PARTY_ID_INFO_DETAILS	3	0	0	0	0
PARTY.OBPY_TH_PARTY_ID_INFO_MSTR	3	0	0	0	0

- **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 1-22 Mapping the Target Path

Copyright © 2025, Oracle and/or its affiliates.

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

Figure 1-23 Viewing Path Statistics and Information Post-Mapping

> **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.

1.2.3 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 to view valid SCNs
   - Select an **SCN** and create a new Extract

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-24 Status

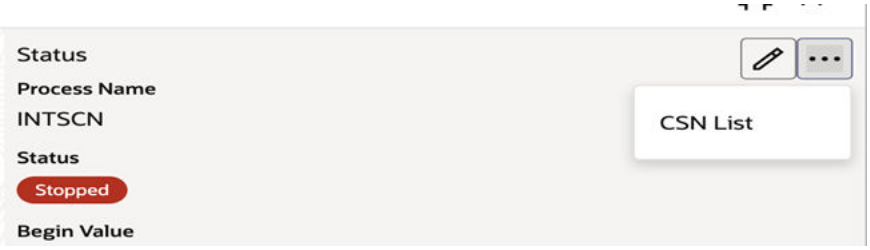
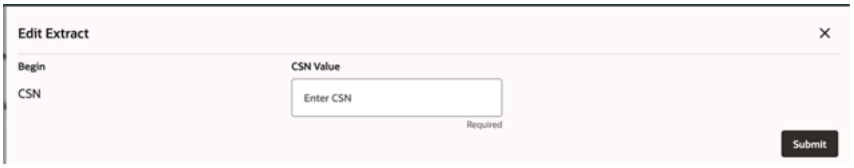


Figure 1-25 Edit Extract



- Register the **SCN** in **Registration Options** and Select **Begin as Now**
- **Start** and verify the Extract by checking the **Reports** in the Extract View.
- Wait for the extract to position to the **current timestamp**, then **Stop** the Extract.
- Use the **Edit Extract option** in top right corner the UI to reposition the Extract to the chosen **SCN**.
- Restart the Extract with **CSN option** by providing **CSN** Value and confirm repositioning via **Reports and Checkpoint lag**.
- 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

1.3 KMS Profile Management

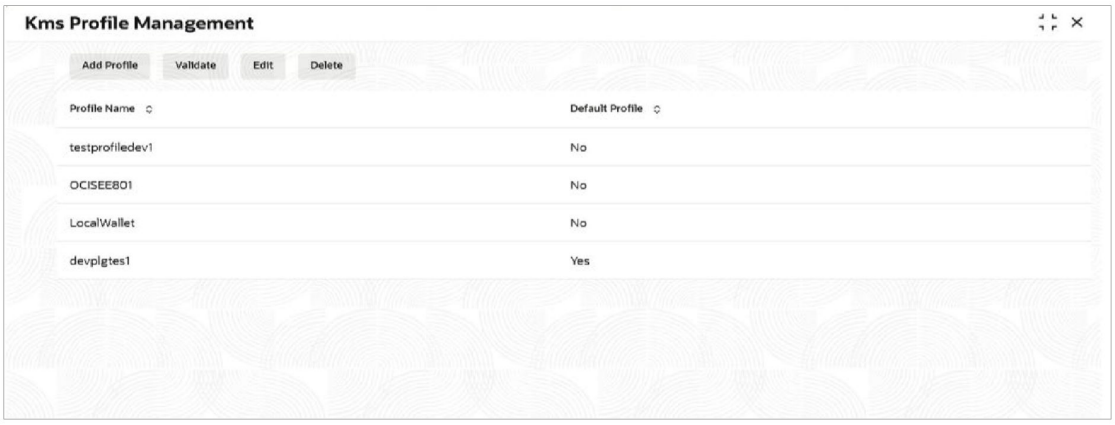
This topic provides information about KMS profile management.

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)**.

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-26 KMS Profile

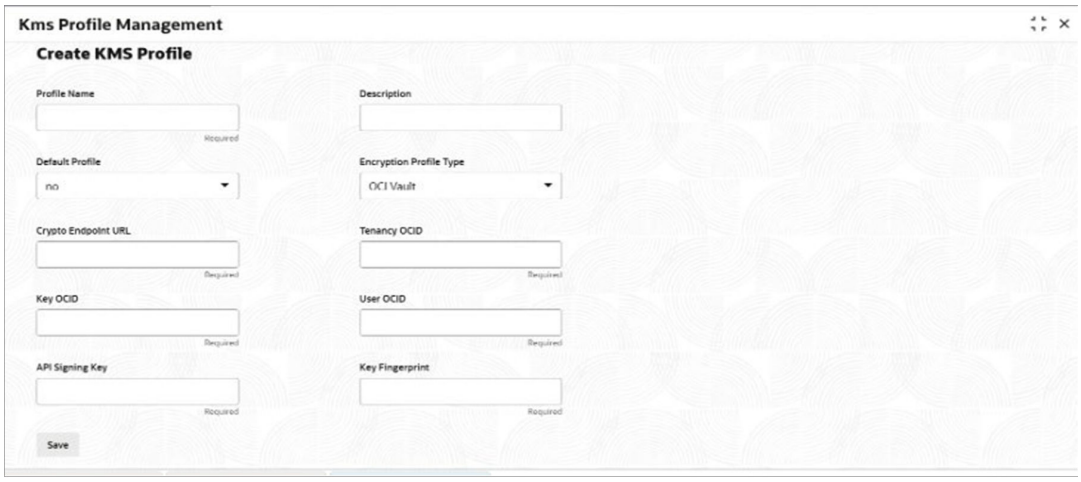
Figure 15: KMS Profile



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.

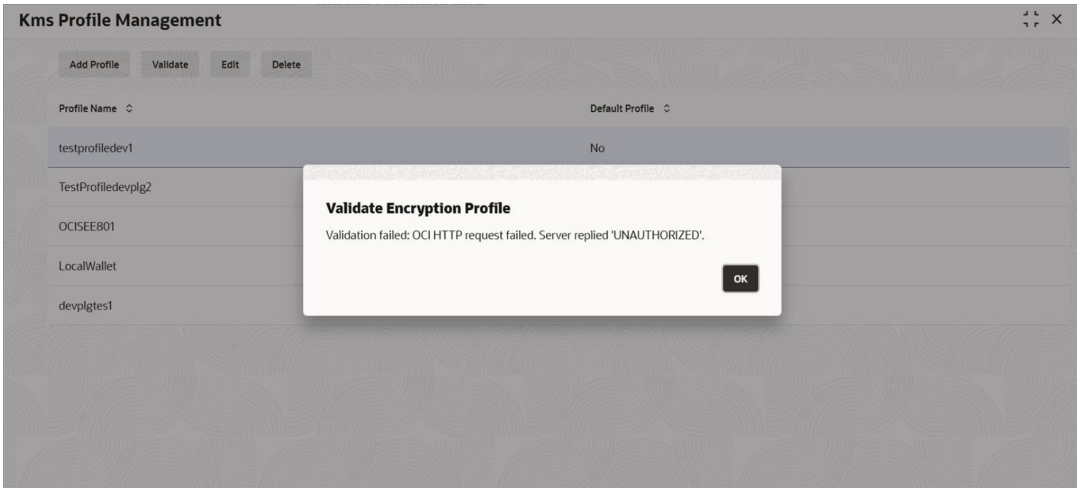
Figure 1-27 Create KMS Profile



- **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.

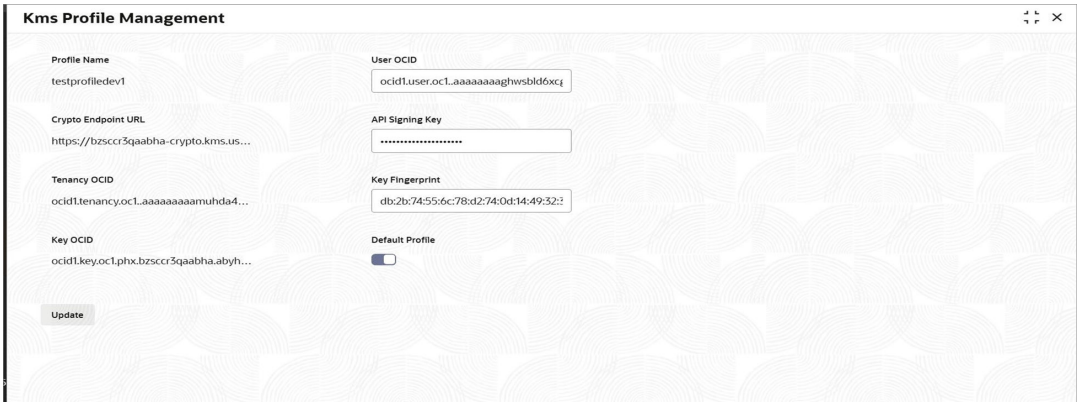
Copyright © 2025, Oracle and/or its affiliates.

Figure 1-28 Validate KMS Profile



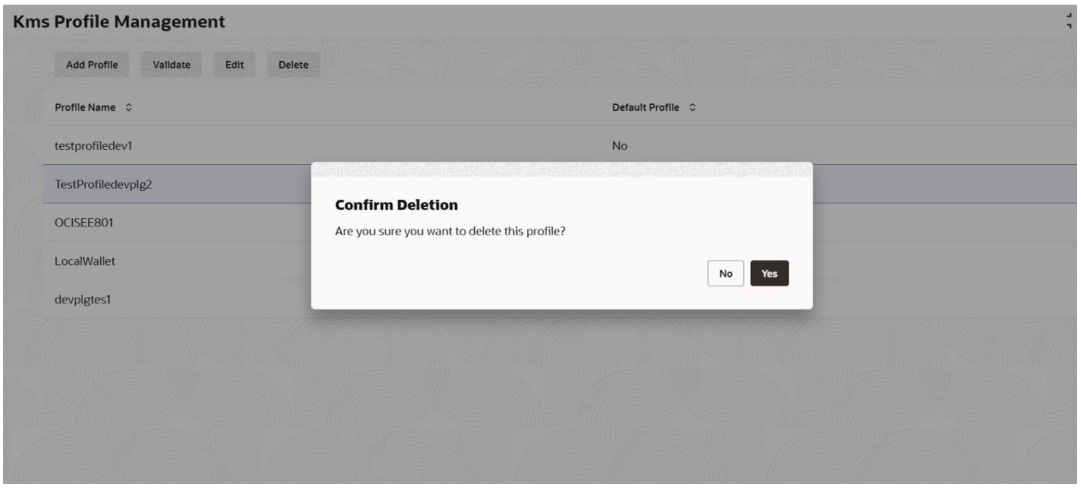
- **Edit**: This action allows the user to set or remove a profile as the default. Additionally, if any configuration issues were identified during the validation process, the user can modify the necessary fields and save the updated profile details.

Figure 1-29 Edit KMS Profile



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

Figure 1-30 Delete KMS Profile



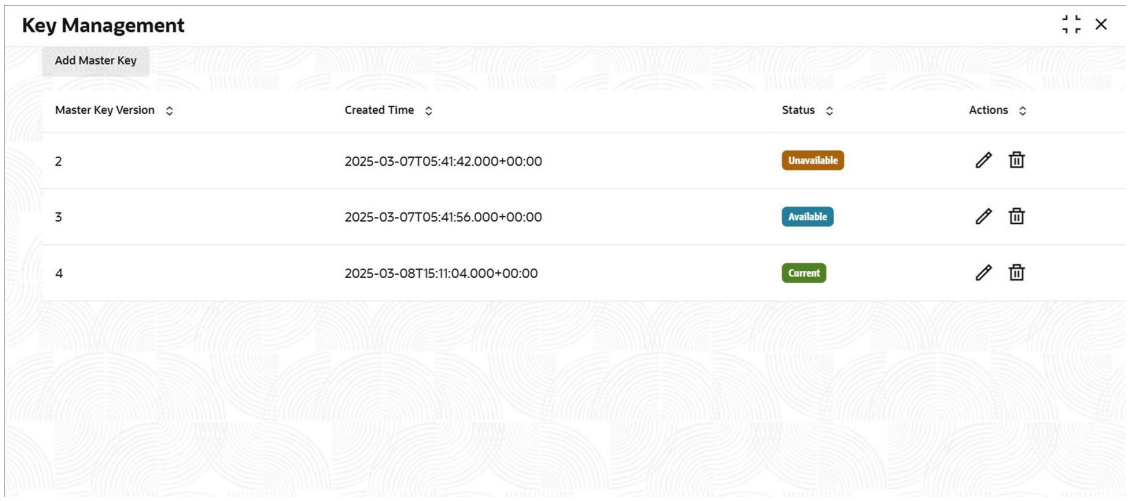
Copyright © 2025, Oracle and/or its affiliates.

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.

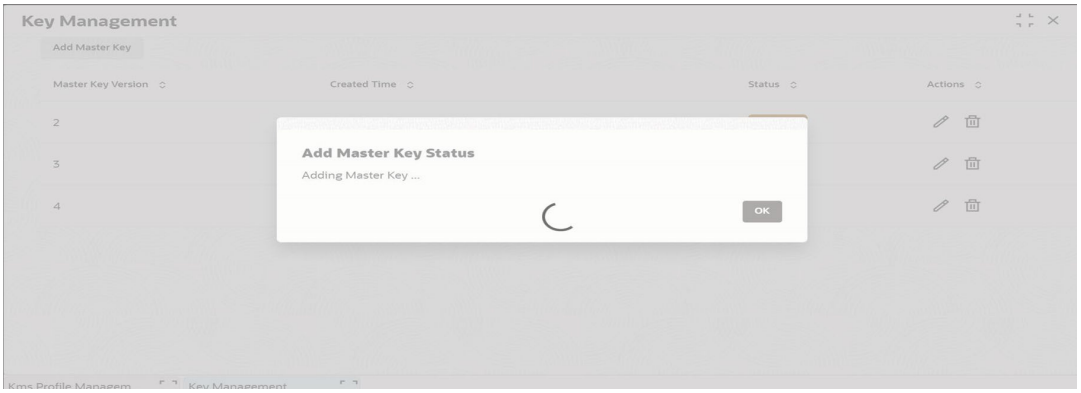
Figure 1-31 Master Keys



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 1-32 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.

Copyright © 2025, Oracle and/or its affiliates.

Figure 1-33 Update Master Key

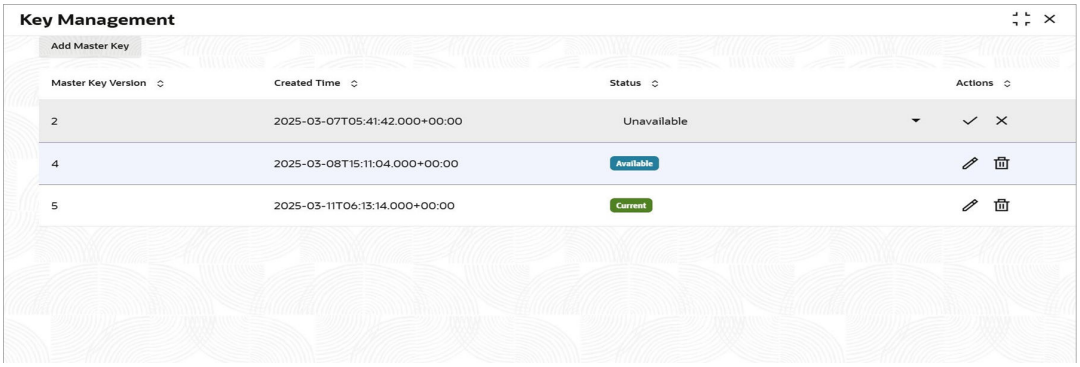
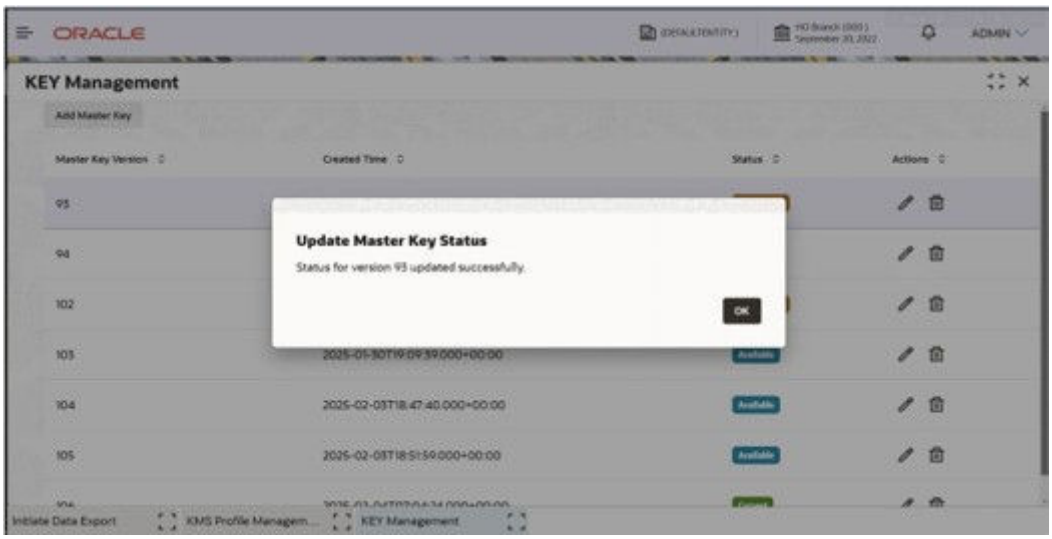
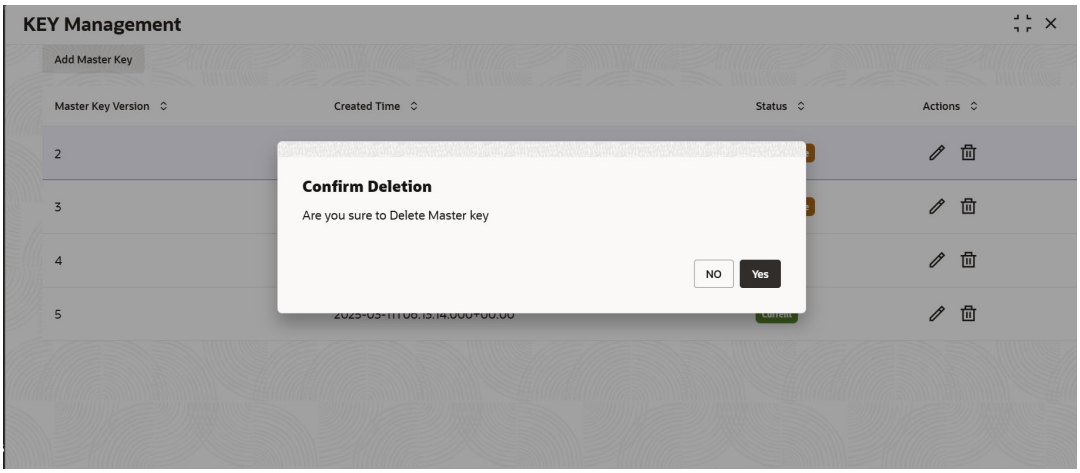


Figure 1-34 Update Confirmation



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

Figure 1-35 Delete Master Key



Copyright © 2025, Oracle and/or its affiliates.

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.

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 account
- An **ATP (Autonomous Transaction Processing) instance** in OCI for importing the initial data dump.
- A configured OCI Golden Gate instance in the SaaS tenancy

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.

Copyright © 2025, Oracle and/or its affiliates.

- 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.

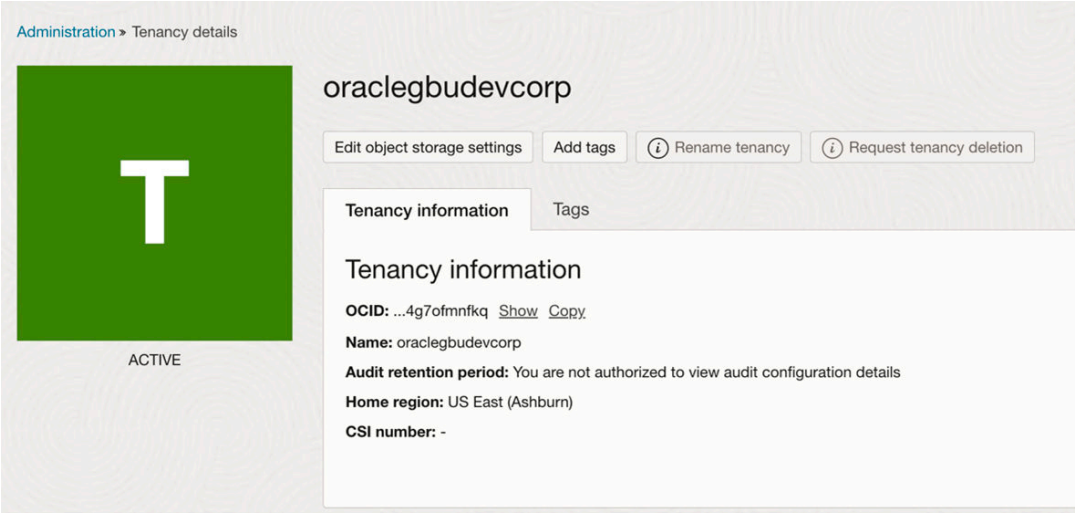
In this section, the user will learn how to **gather the Tenancy OCID**.

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



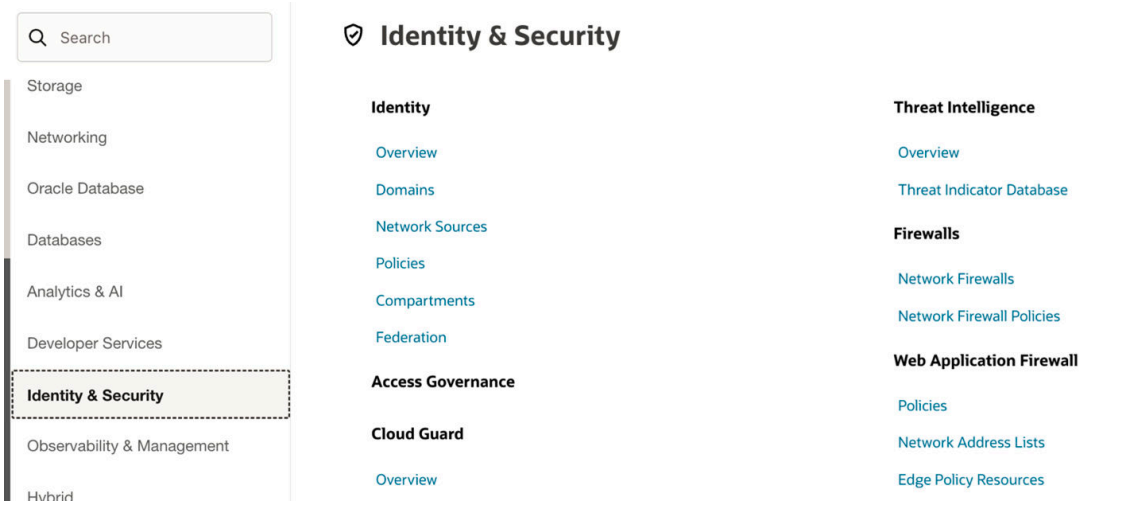
2.2.2 Identity and Security

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.

Copyright © 2025, Oracle and/or its affiliates.

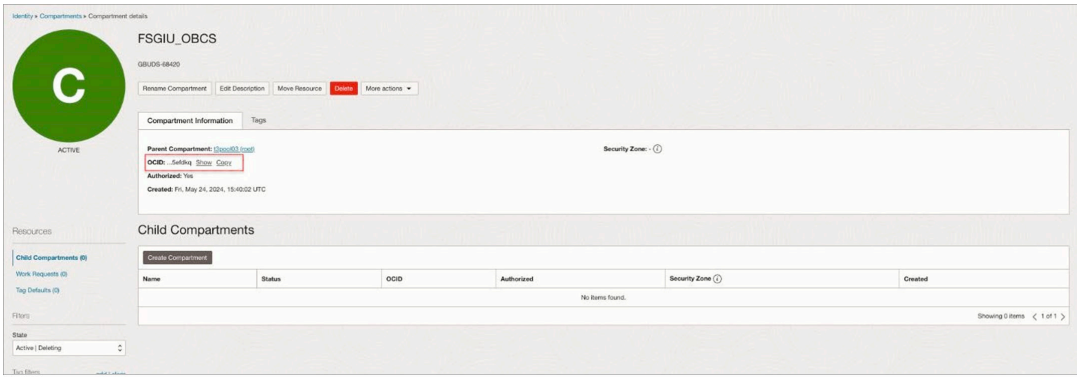
Figure 2-2 Identity and Security



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

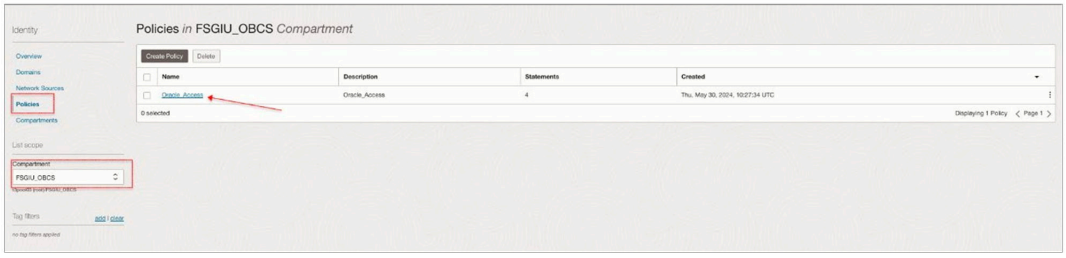


2. Create the security policies that will allow the Oracle to create the Public Endpoint in the compartment.

Copyright © 2025, Oracle and/or its affiliates.

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**
>
> a. **Policy names** must be unique across compartments.
>
> b. The **Policy Builder wizard** does not support all valid policy types; therefore, the user should use **Show Manual Editor** for full configuration.
>
> c. 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.

Copyright © 2025, Oracle and/or its affiliates.

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_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>
```

2.2.4 Network Setup

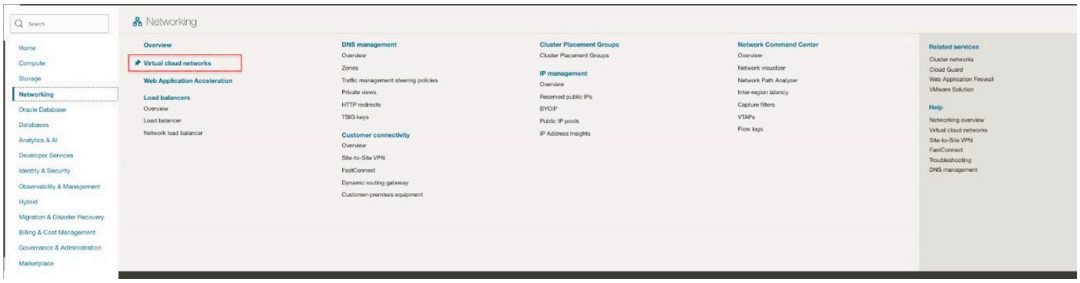
This topic describes the systematic instructions on network setup.

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:

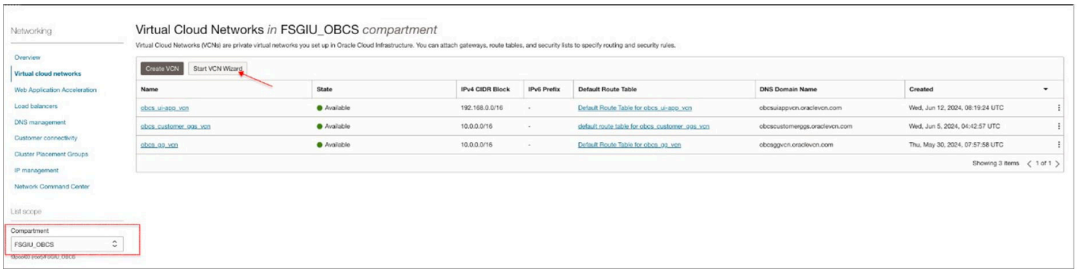
1. Ensure that the network configuration allows connectivity between the source and target environments.

Figure 2-6 Networking



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

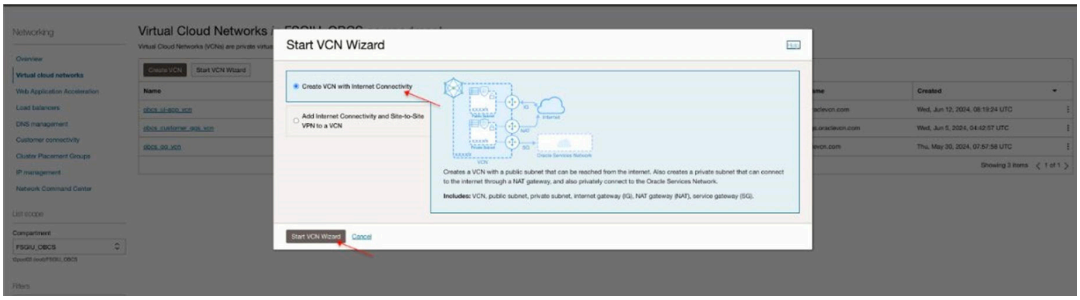
Figure 2-7 Virtual Cloud Network



Copyright © 2025, Oracle and/or its affiliates.

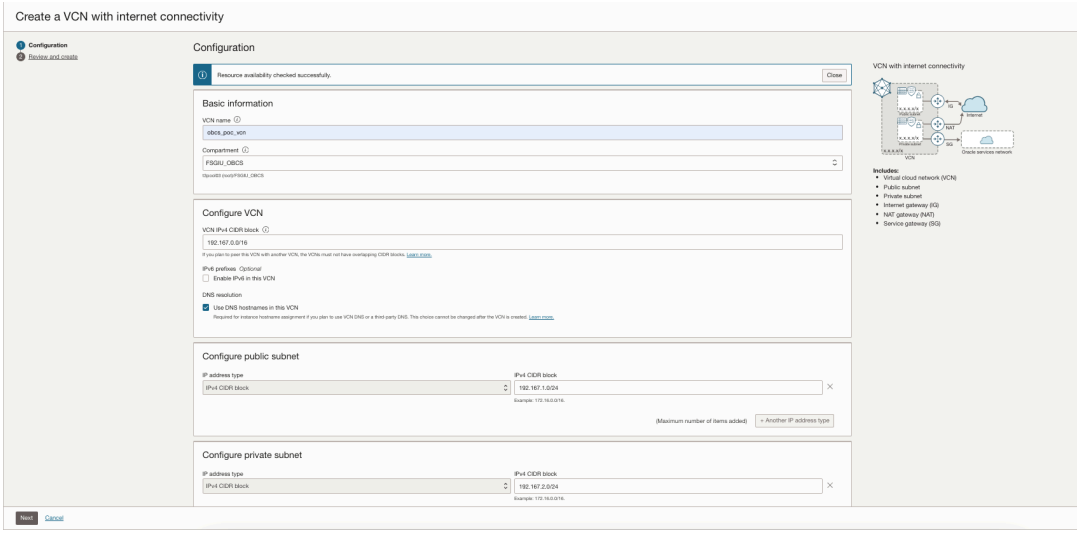
3. Select the **Create VCN with Internet Connectivity** option.

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

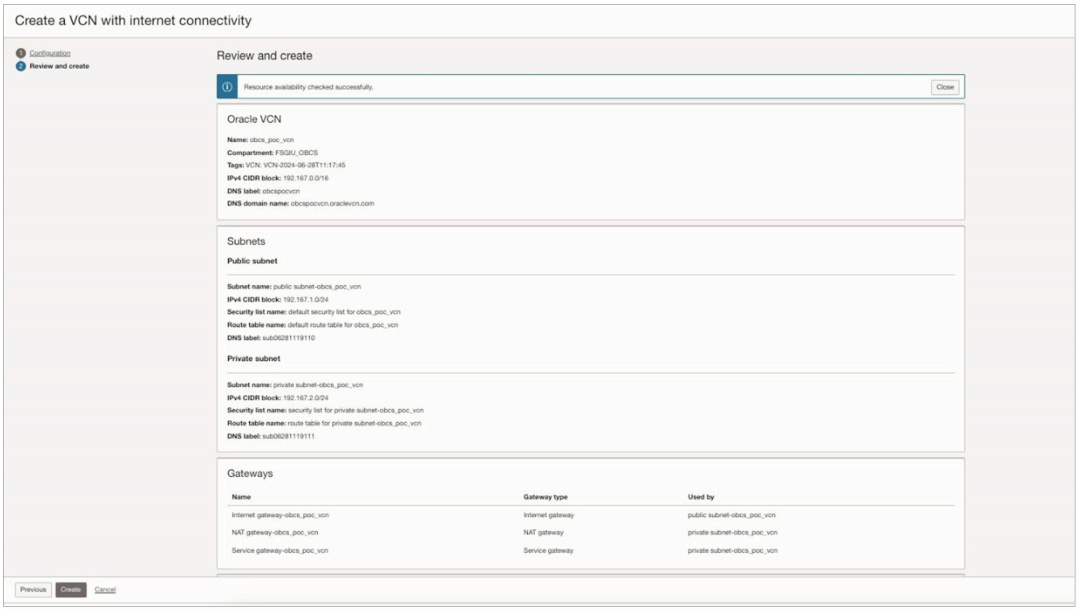


5. Review the resources and note the CIDR on the Subnet.

   User's Target environment resources will be associated with the subnet.

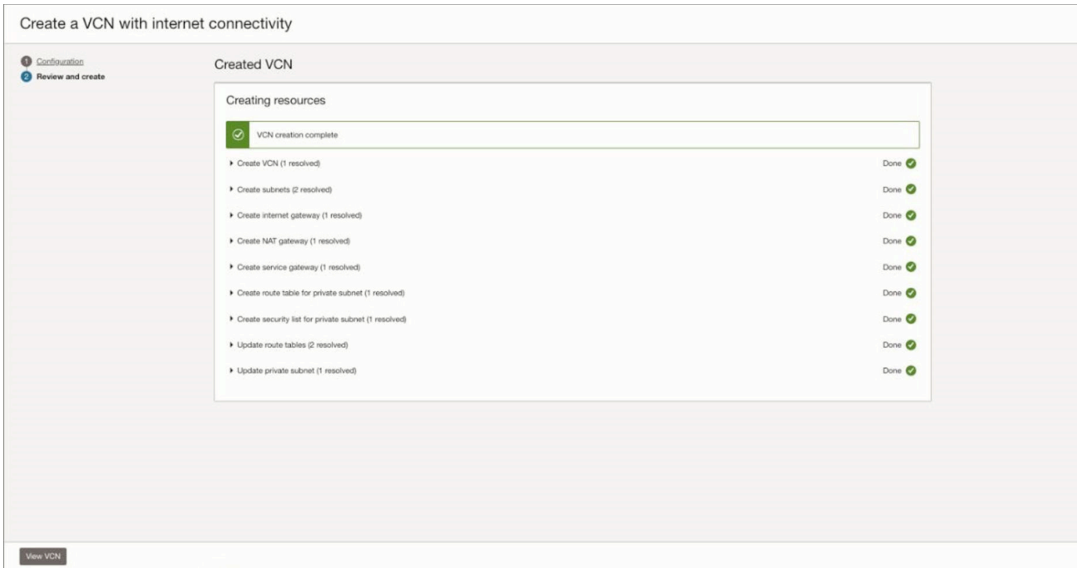
Copyright © 2025, Oracle and/or its affiliates.

Figure 2-10 Review and Create



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

Figure 2-11 Created VCN

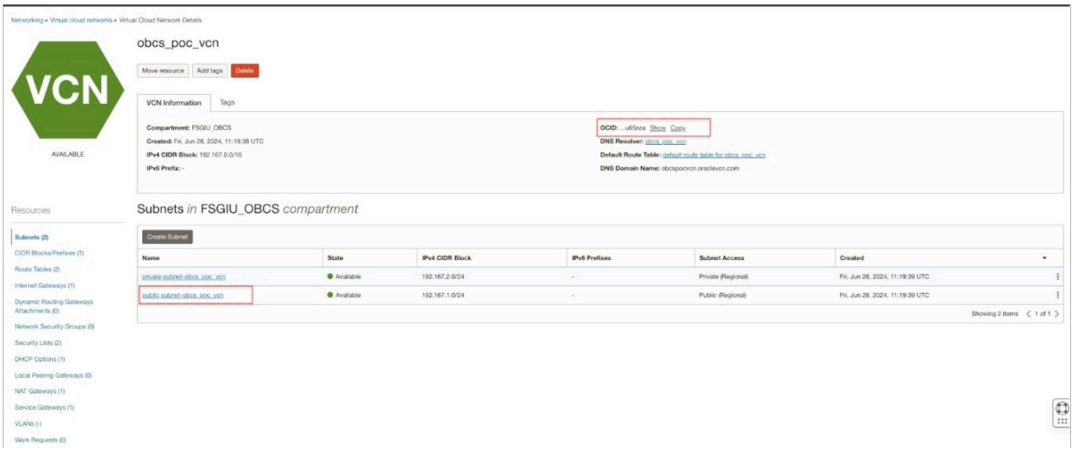


7. User can view the **Virtual Cloud Network** by following the process below:
   a. Copy and note the VCN's OCID and name. This information is required for the Network Path Creation.
   b. Select the subnet where the user would like the Target environment resources to be located.

Copyright © 2025, Oracle and/or its affiliates.

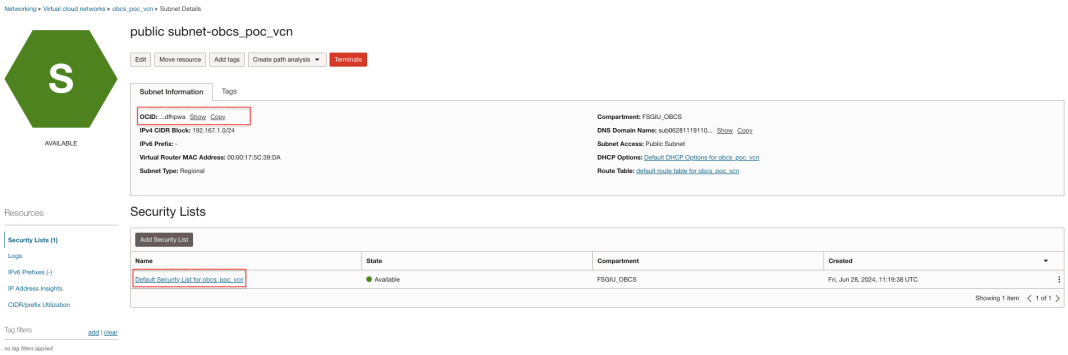
Figure 2-12 OBCS_POC_VCN

Figure 36: OBCS_POC_VCN



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

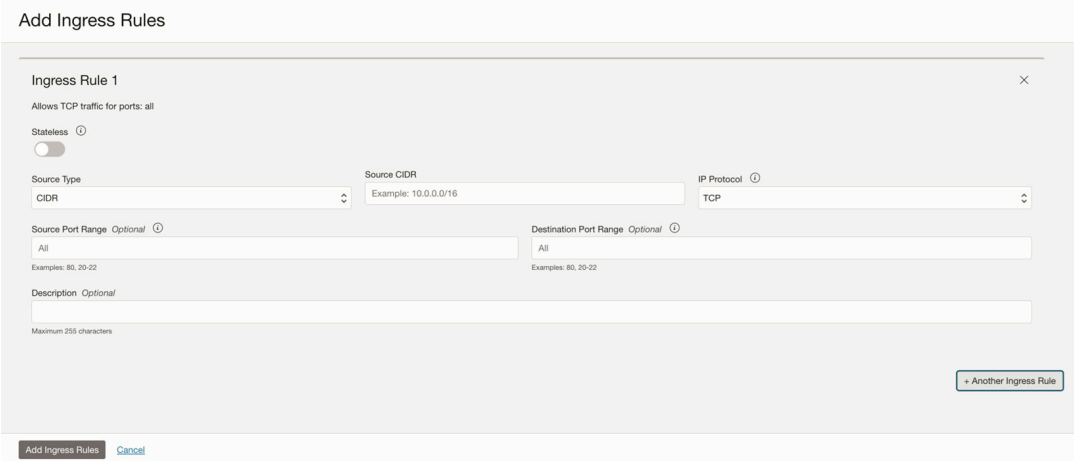


10. User can add an Ingress Rule to the default Security list, using the Subnet CIDR noted above in Step 5. The rule must allow ingress of TCP on 443.

> **Note**
>
> The Security Rule is prerequisite of the environment creation.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-14 Add Ingress Rule



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 creta a vault.
- Create Master Encryption Key
  This topic describes the systematic instructions to creta a master encryption key.

2.2.5.1 Create a Vault

This topic describes the systematic instructions to creta a vault.

User can create and configure the OCI Vault.

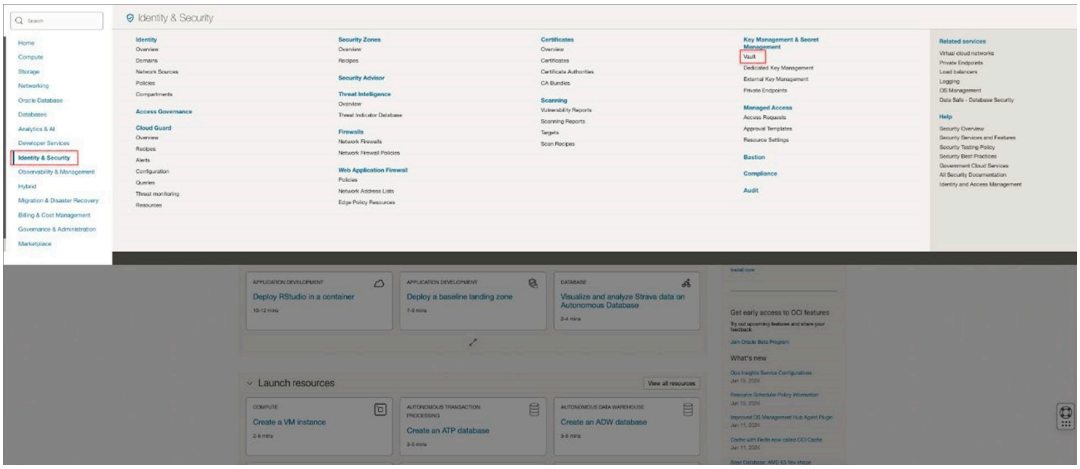
Follow the steps below to create and configure the OCI vault:

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**.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-15 Vault



a. To create a new vault:

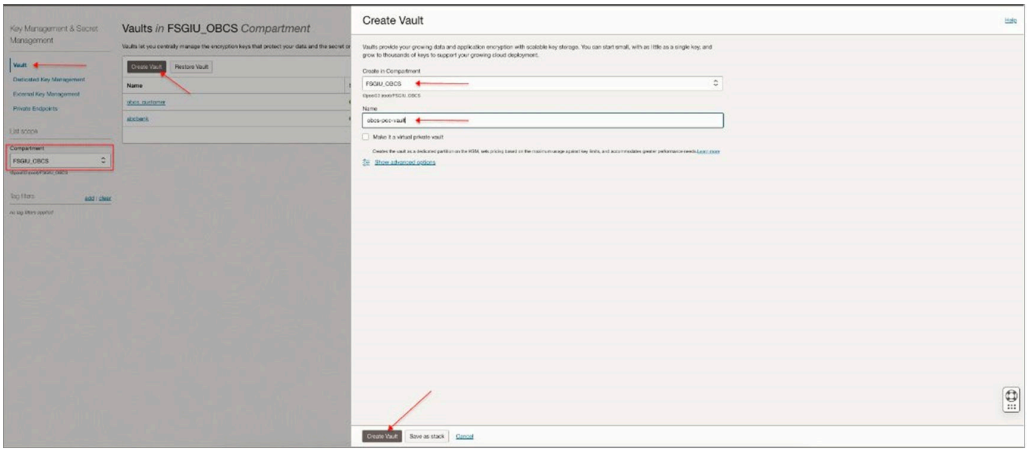
   i. Click **Create Vault**.

   ii. Provide a name for the vault.

   iii. Select the compartment where the vault is to be created.

   iv. Select the Vault type (Virtual Private Vault is commonly used)

Figure 2-16 Create Vault



b. To configure vault:

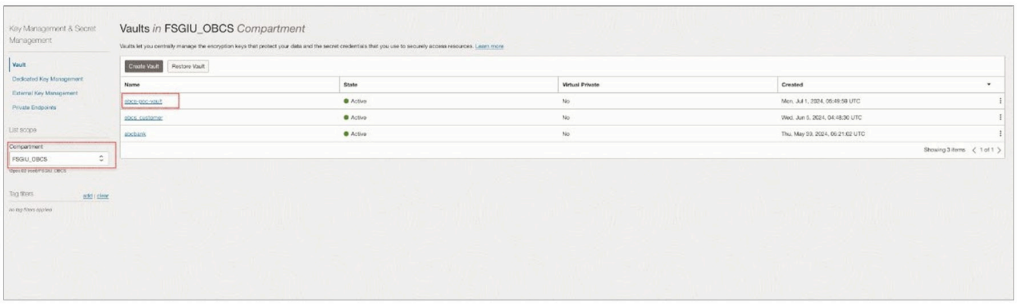
   i. Specify the Key Management and Recovery settings

   ii. Click **Create Vault**.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-17 Vaults in FSGIU_OBCS Compartment

Figure 41: Vaults in FSGIU_OBCS Compartment



2.2.5.2 Create Master Encryption Key

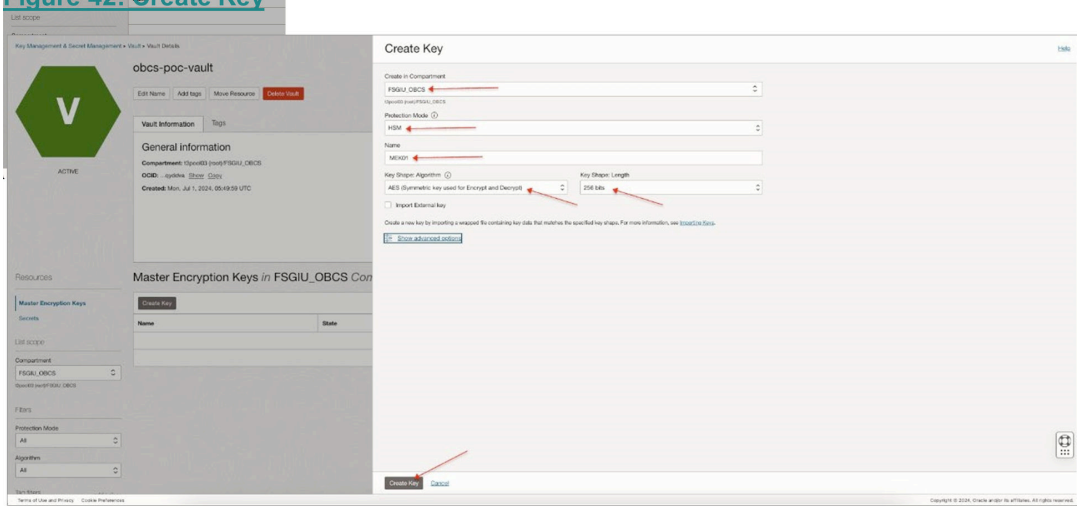
This topic describes the systematic instructions to creta a master encryption key.

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

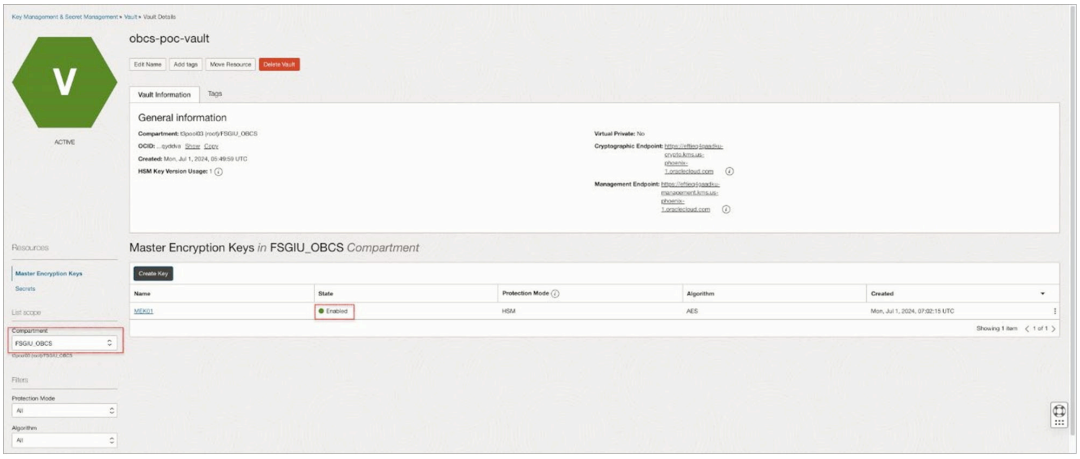
Figure 42: Create Key



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

Copyright © 2025, Oracle and/or its affiliates.

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:

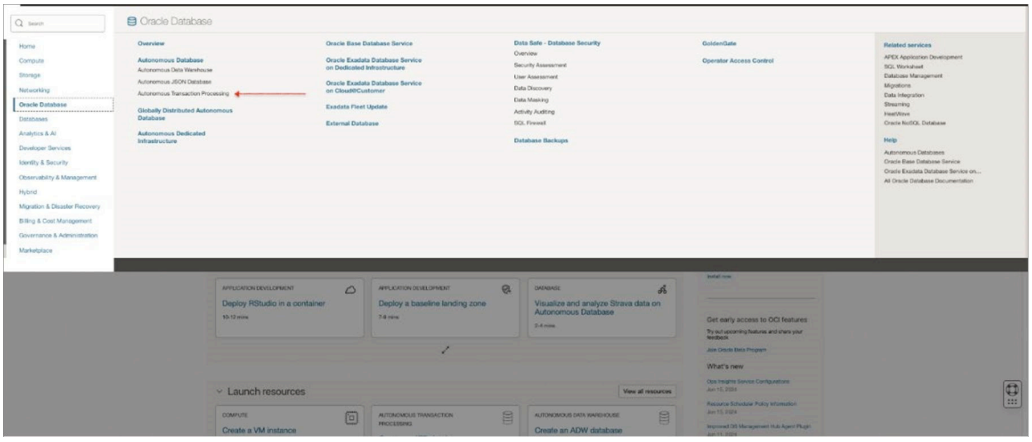
1. Create a **Virtual Cloud Network** (VCN) and **Subnet**.

> **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**.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-20 Oracle Database

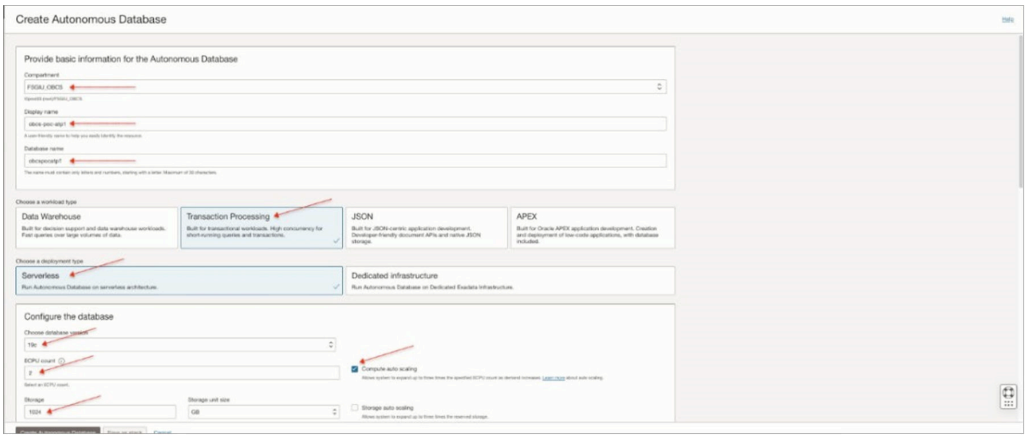


c. Create **Autonomous Database** by following the process below:

i. Click **Create Autonomous Database**.

ii. Select the **Autonomous Transaction Processing** option.

Figure 2-21 Create Autonomous Database



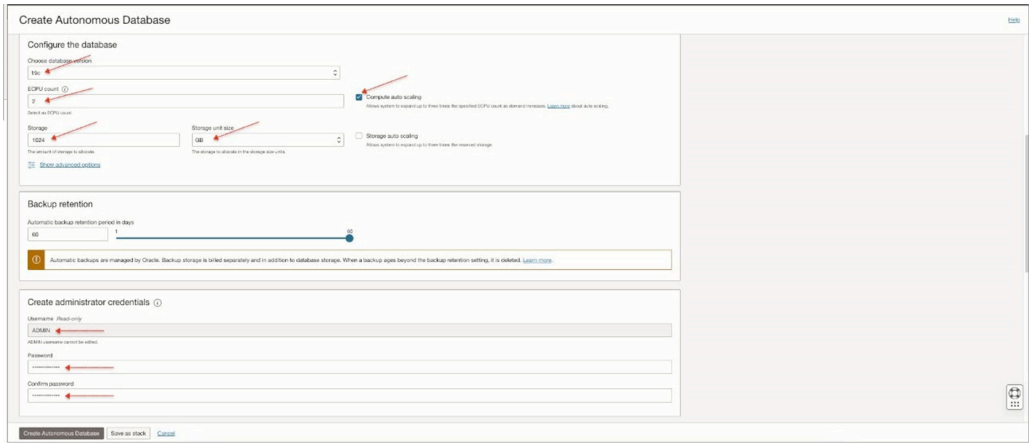
d. User should provide the following database details:

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.
OCPU Count	Specify the number of OCPU's.
Storage (TB)	Specify the storage size.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-22 Create Autonomous Database Details

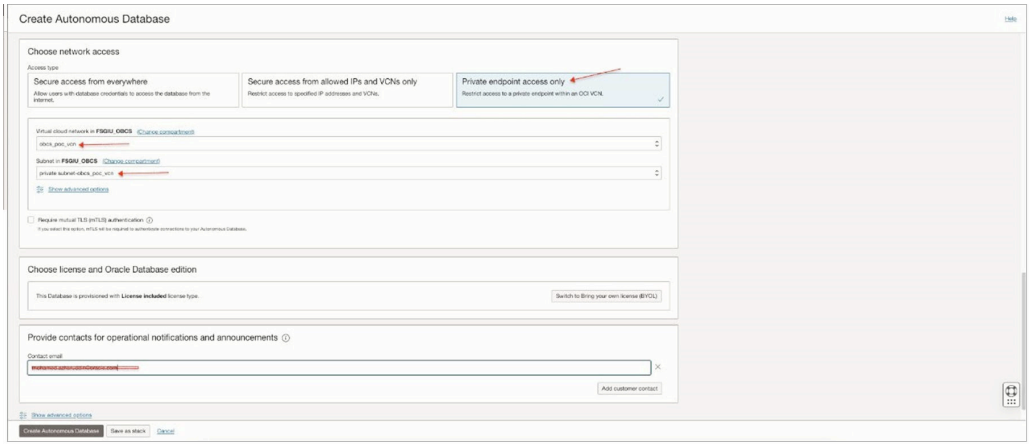


e. Configure the following network access:

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.

Copyright © 2025, Oracle and/or its affiliates.

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

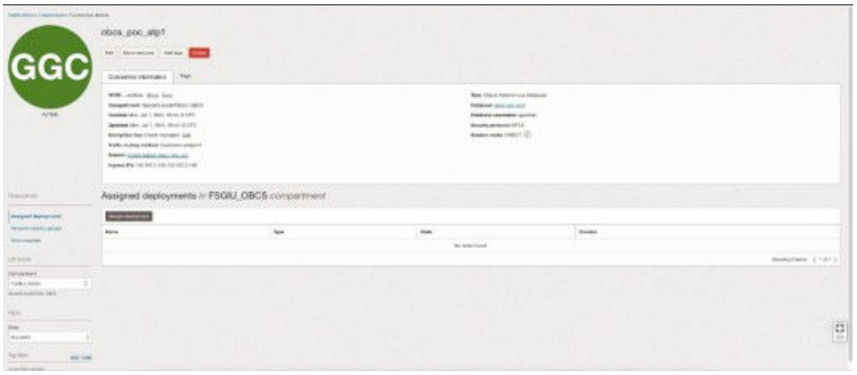
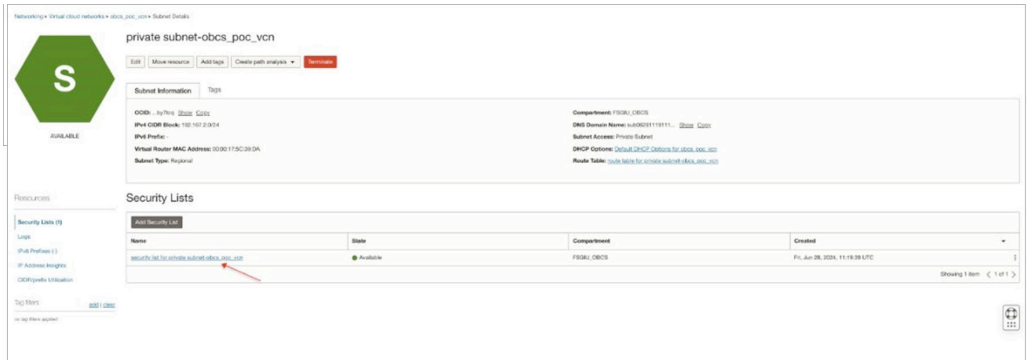


Figure 2-25 Private Subnet-OBCS_POC_VCN



   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.

Copyright © 2025, Oracle and/or its affiliates.

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

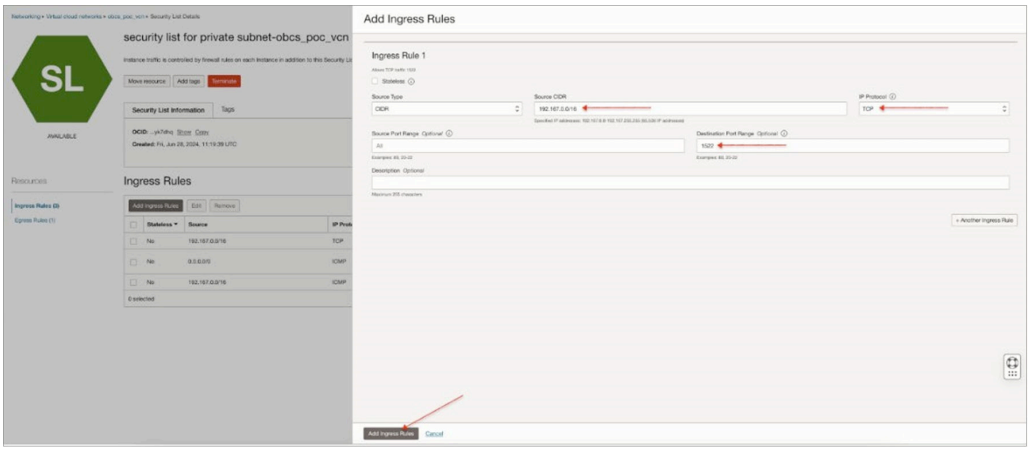
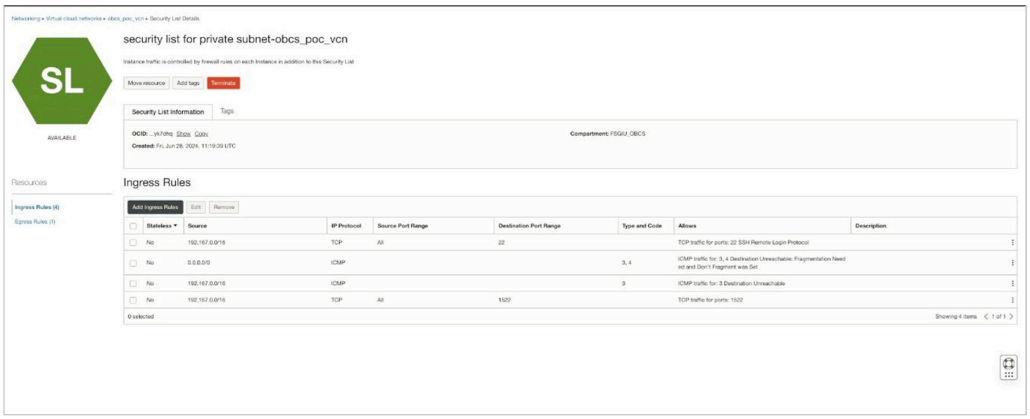


Figure 2-27 Security List for Private Subnet-OBCS_POC_VCN



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**.

Copyright © 2025, Oracle and/or its affiliates.

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
```


Copyright © 2025, Oracle and/or its affiliates.

```
        # 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.m
odels.DecryptDataDetai
ls(
     ciphertext="QZGCZ05MM9VlAOrKPXL9r<----readacted---
>lAC5NhEcQgeFslxpPBPI89WCIeJ1LcarYZlKJgAAAAA=", 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.

Copyright © 2025, Oracle and/or its affiliates.

> **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

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

Copyright © 2025, Oracle and/or its affiliates.

- 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:

Copyright © 2025, Oracle and/or its affiliates.

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

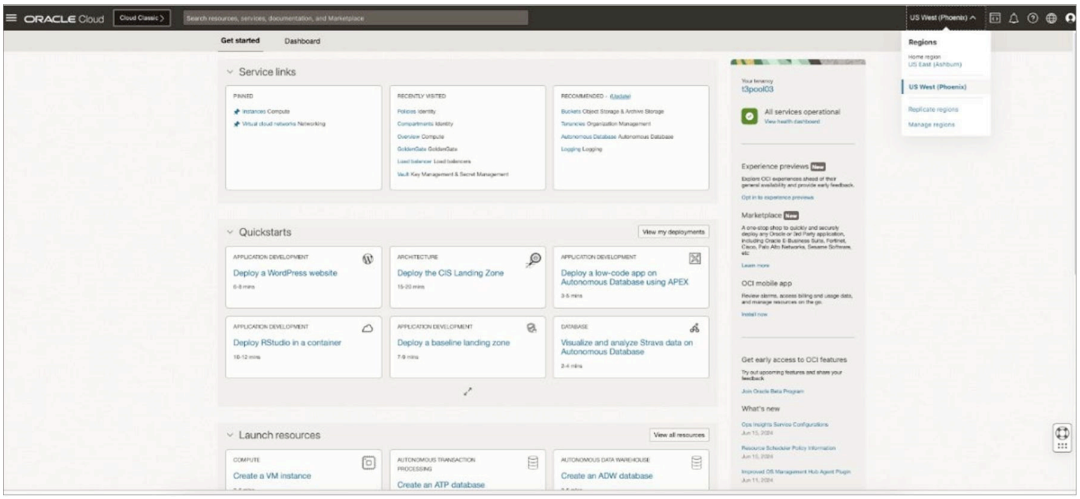
This topic describes the systematic instructions to create an OCI GoldenGate deployment.

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.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-29 Get Started - Regions



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

Figure 2-30 Create Deployment

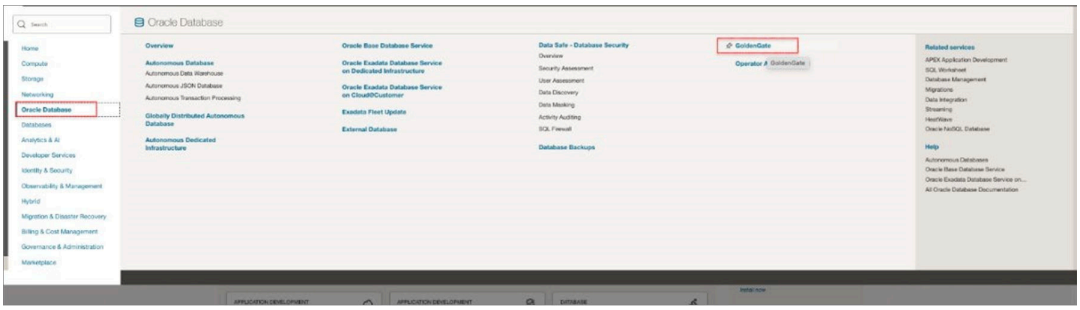
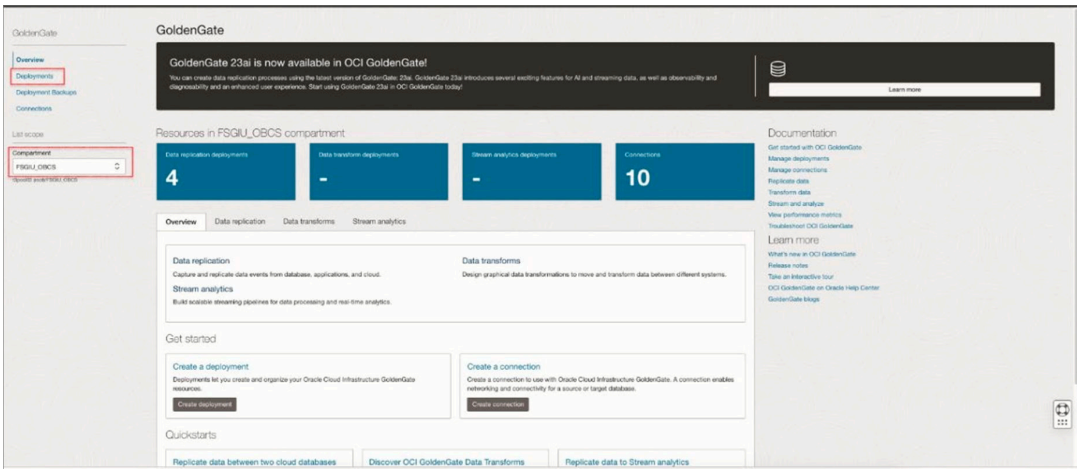
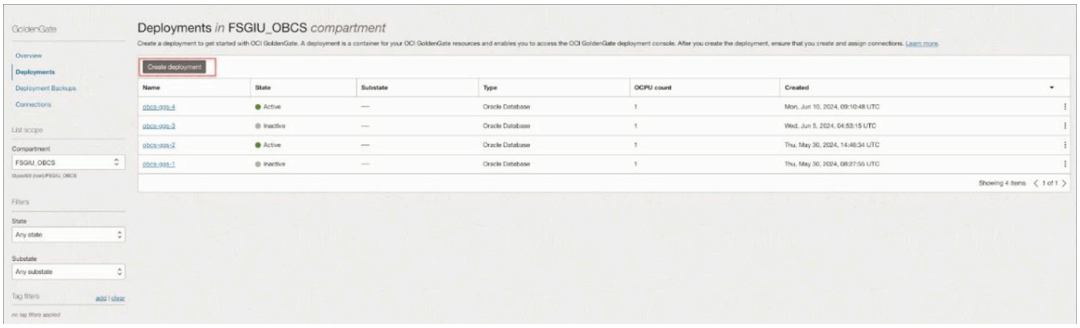


Figure 2-31 GoldenGate



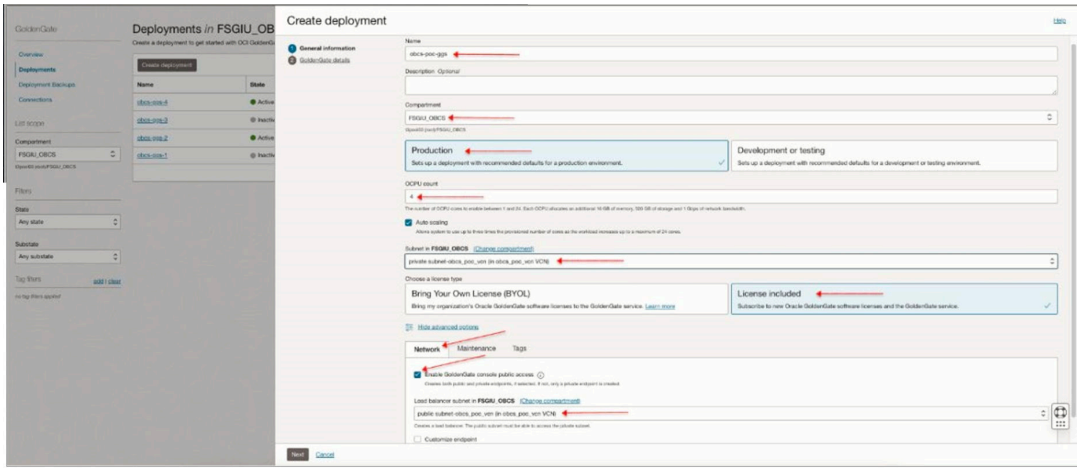
Copyright © 2025, Oracle and/or its affiliates.

Figure 2-32 Deployments in FSGIU_OBCS Compartment



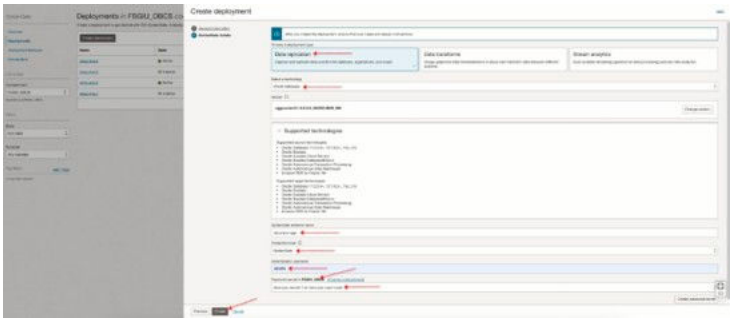
4. Select **Oracle GoldenGate** and provide necessary details like name, compartment, and network information.

Figure 2-33 Create Deployment



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

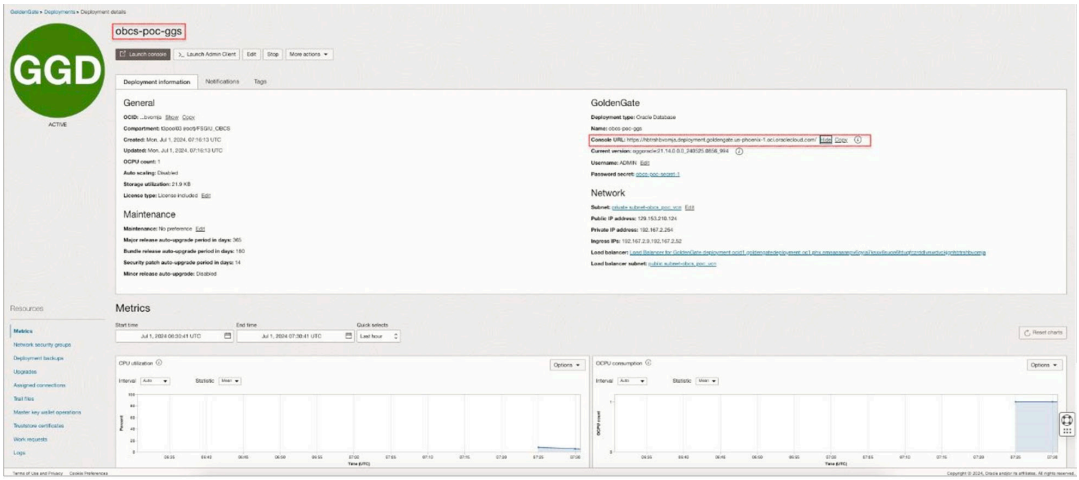
Figure 2-34 Create Deployment



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

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-35 OBCS_POC_GGS



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

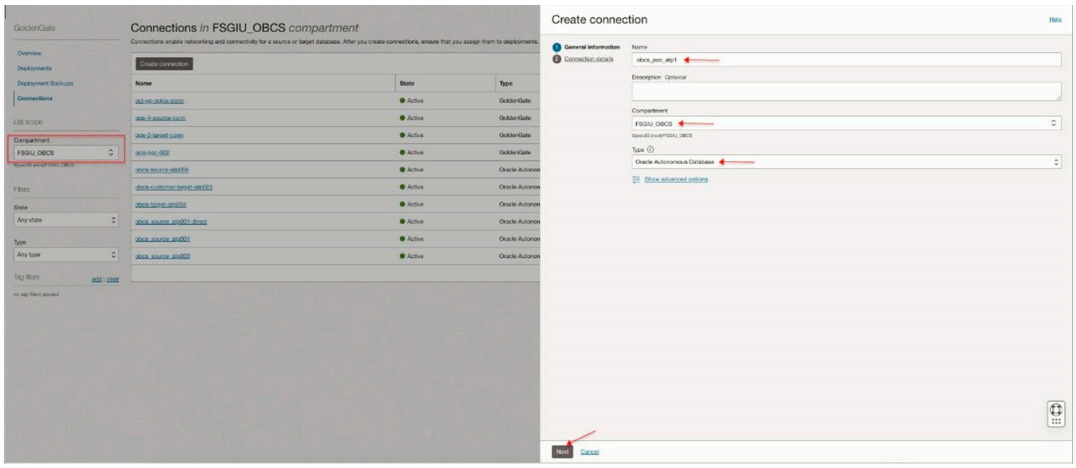
Field	Description
Name	Specify a name for the connection.
Description	Optional Specify a description that helps you distinguish this connection from others.
Compartment	Select the compartment in which to create the connection.
Type	From **Oracle**, select **Oracle Database**.
Show advances options	Optional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

Copyright © 2025, Oracle and/or its affiliates.

5. From **Tags**, add tags to organize the resources
6. Click **Next**.

Figure 2-36 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

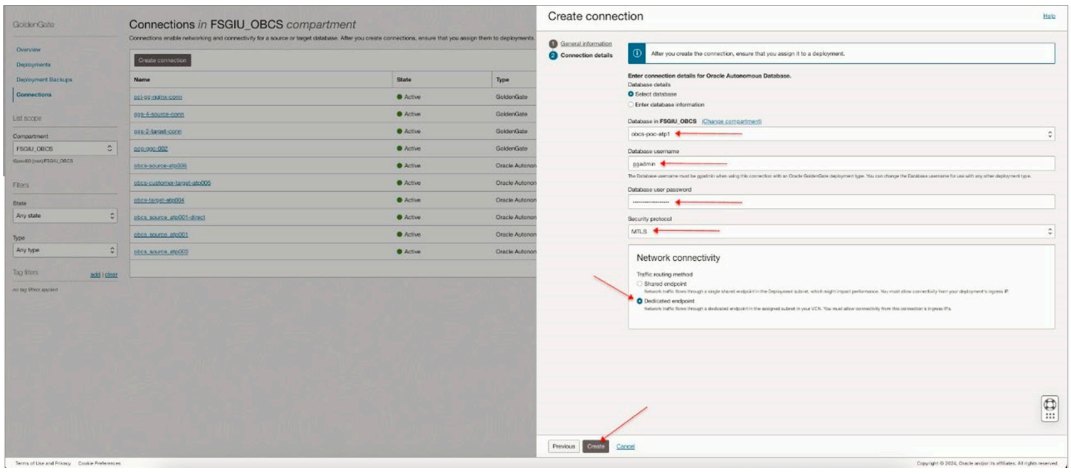
Field	Description
Database Information	Specify the database details.
Database Connection String	Optional Specify the database's connection string.
Database Username	Specify the username to connect to the database.
Database Password	Specify the password associated to the username provided in the previous 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.

Copyright © 2025, Oracle and/or its affiliates.

c. Click **Create**.

Figure 2-37 Create Connection



8. Assign the deployment details.

Figure 2-38 OBCS_POC_ATP1

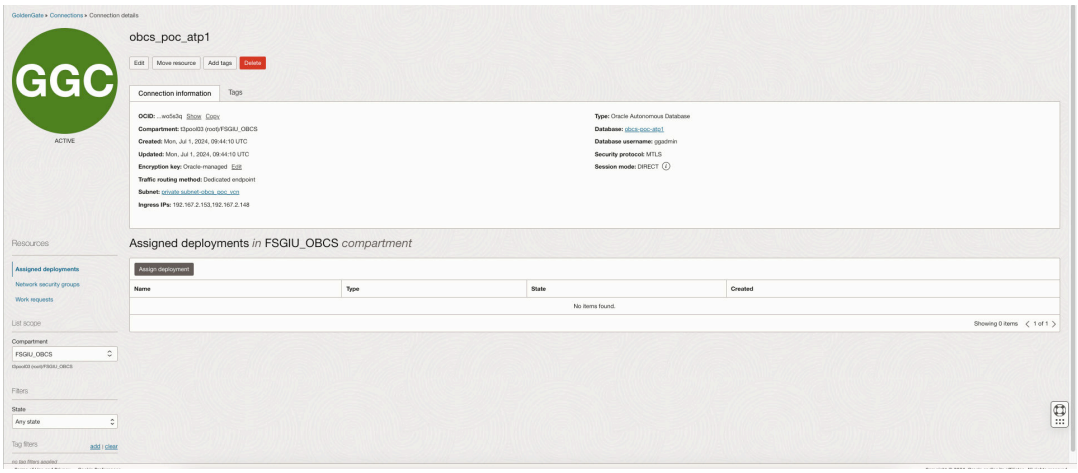
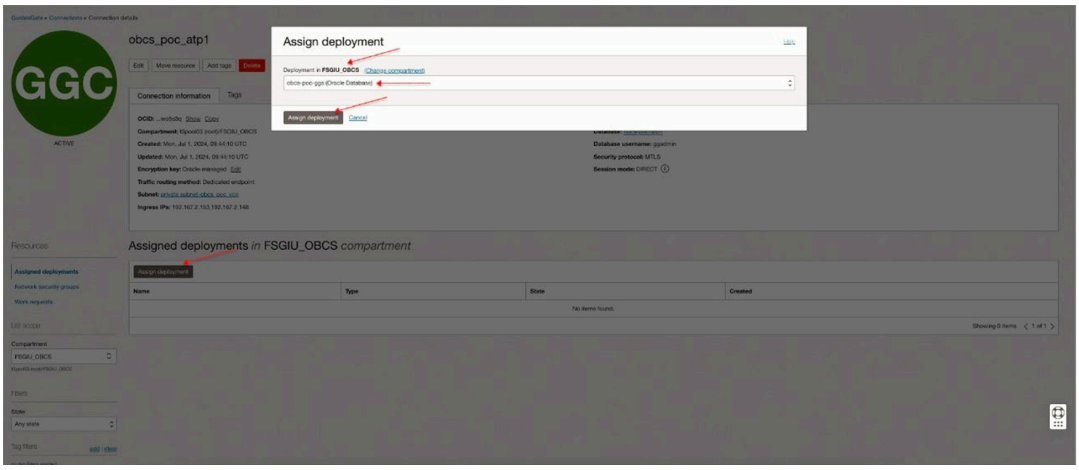


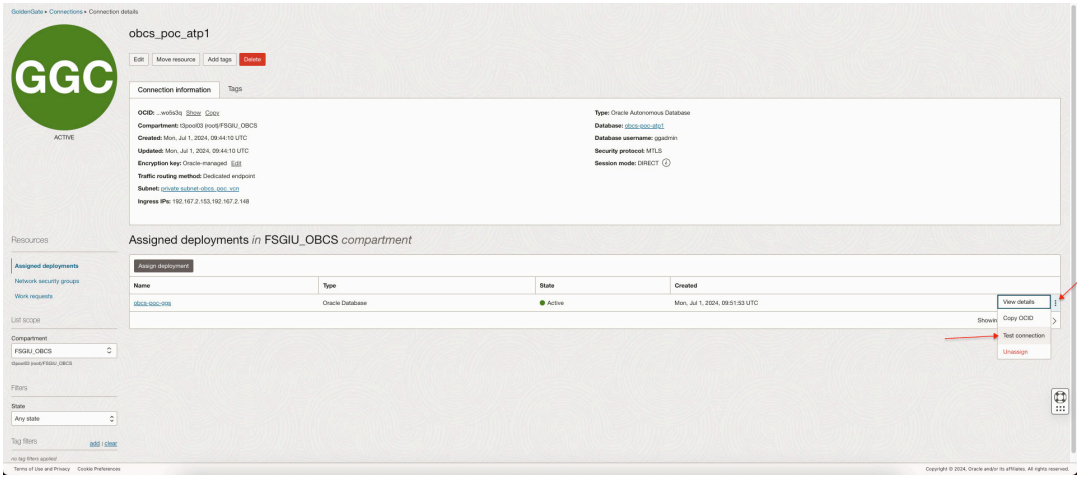
Figure 2-39 Assign Deployment



Copyright © 2025, Oracle and/or its affiliates.

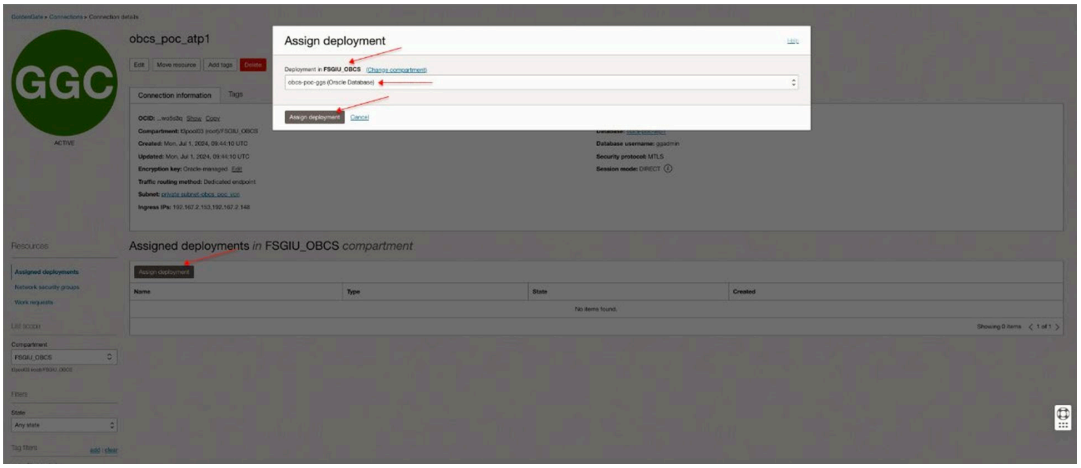
Click **Options** icon to the extreme right, for the assigned deployment and click **Test connection**.

Figure 2-40 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 2-41 Test Connection



2.4.3 Configure OCI GoldenGate

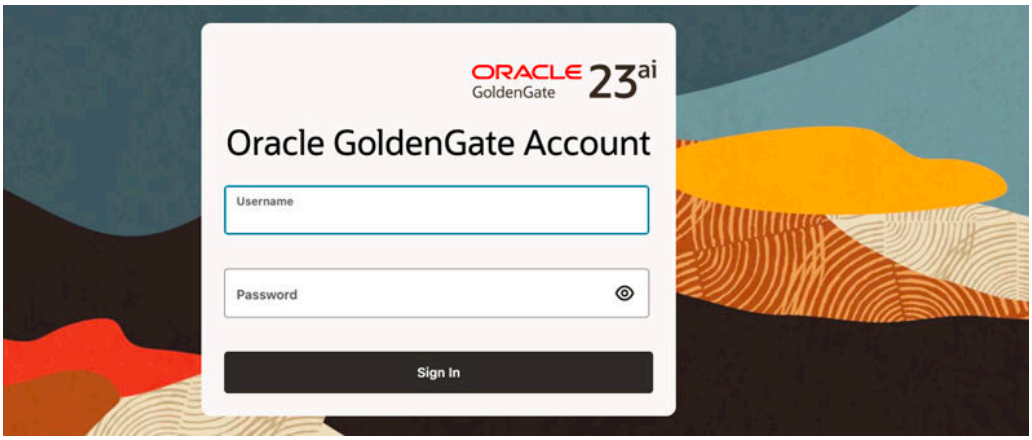
This topic describes the systematic instructions to configure OCI GoldenGate.

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

Copyright © 2025, Oracle and/or its affiliates.

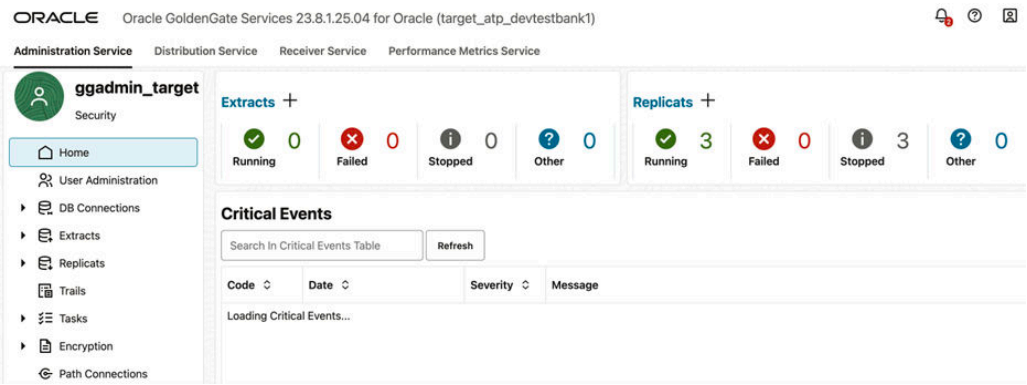
1. Access the GoldenGate Console by follows:
   a. Use the Admin URL to access the GoldenGate console.
   b. Login using the GGADMIN credentials.

Figure 2-42 Oracle GoldenGate Administration Service



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

Figure 2-43 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**.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-44 Connection to DB

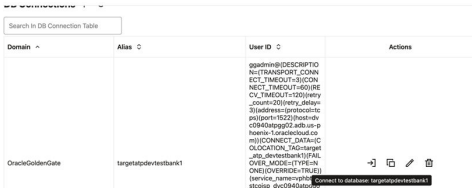


Figure 2-45 Checkpoint

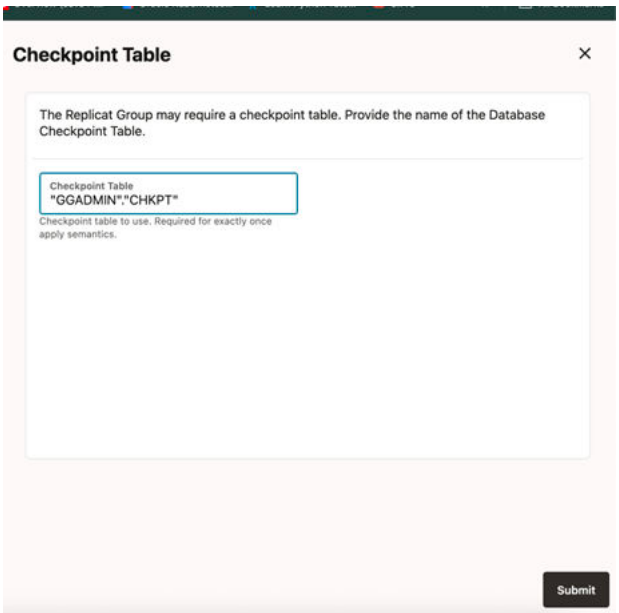
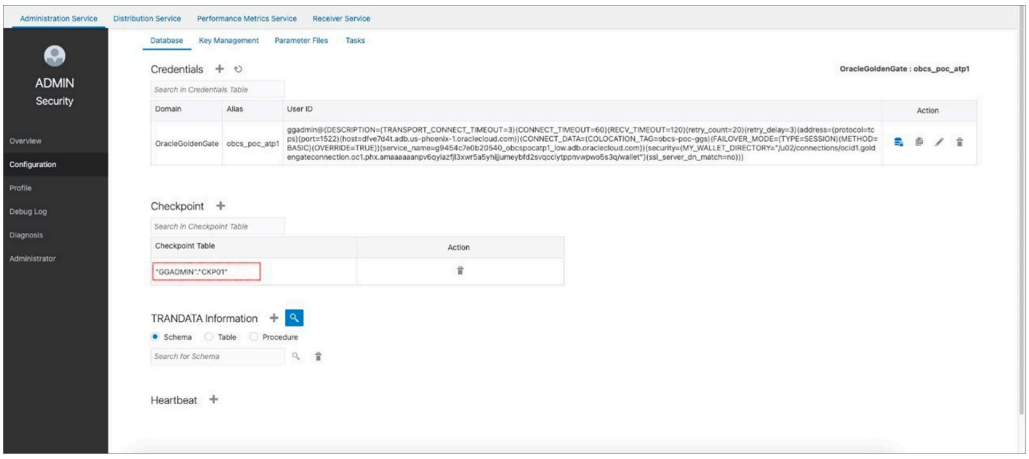


Figure 2-46 Checkpoint Details

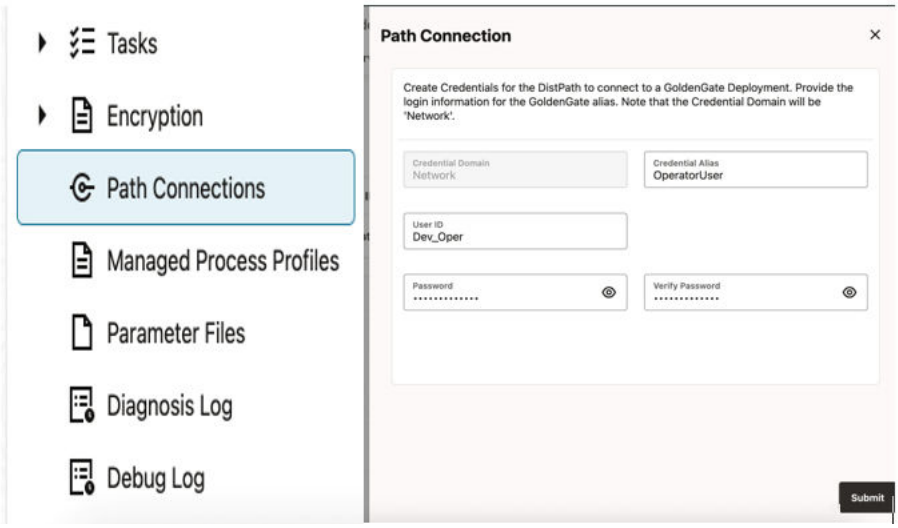


2. Add User for Path Connection:
   - Add the user for the path connection. This user should be the same as the Operator User that was created earlier in the SaaS Self-Service UI.
   - In the **Administration Service** on the Left Menu's scroll down to select **Path Connection** icon and Click on **"+"**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

Copyright © 2025, Oracle and/or its affiliates.

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

Figure 2-47 Path Connections



Things to Consider for Path Connection Creation:

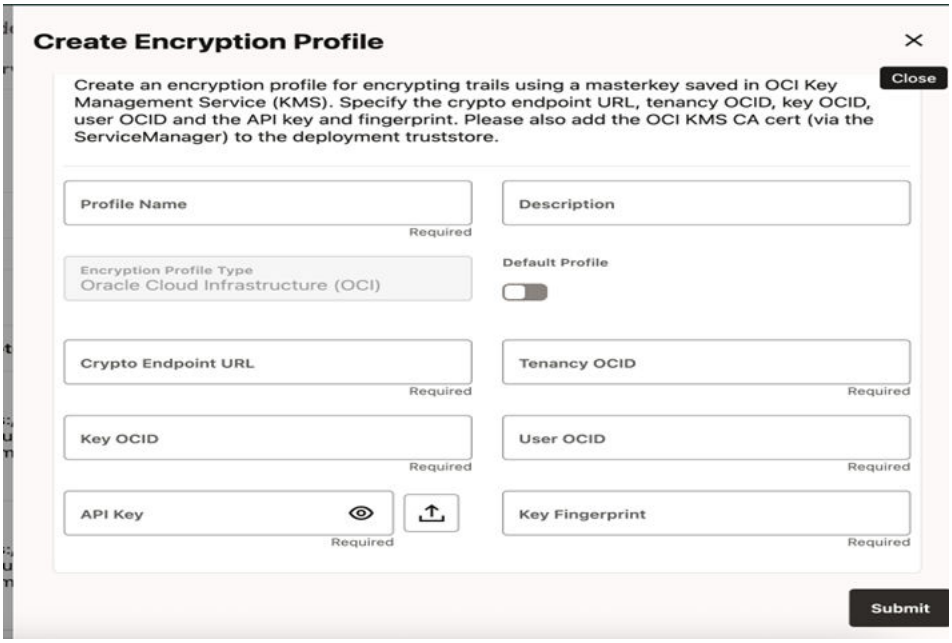
- **Credentials – `<tenantenv>_ggnet>`** – The user ID and password are defined by the **source OBCS SaaS replication configuration** and are used to authenticate the **credential alias**.
- This credential alias is **exclusively used** for the **target-initiated distribution path** between the **source 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** andselect **Profile.**
   b. In the Oracle Cloud Infrastructure section Click **"+"** to add a new profile.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-48 Create an Encryption Profile



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.

Copyright © 2025, Oracle and/or its affiliates.

Figure 2-49 Administration Service Home

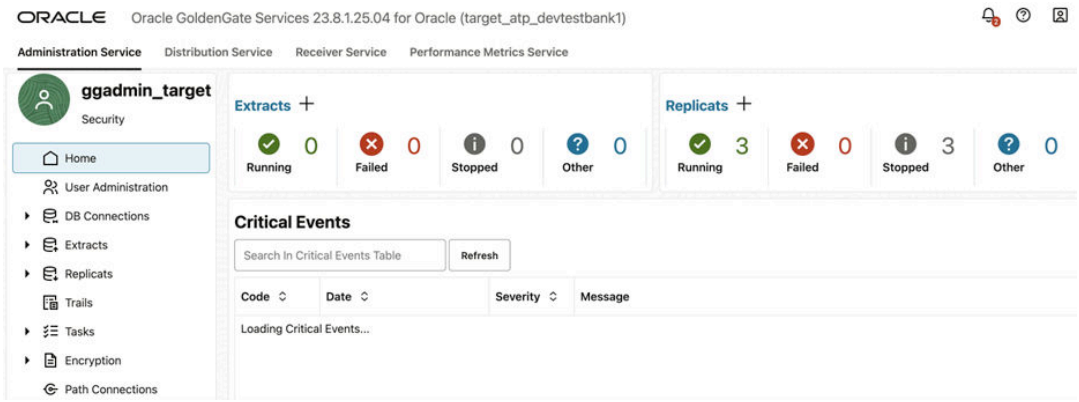
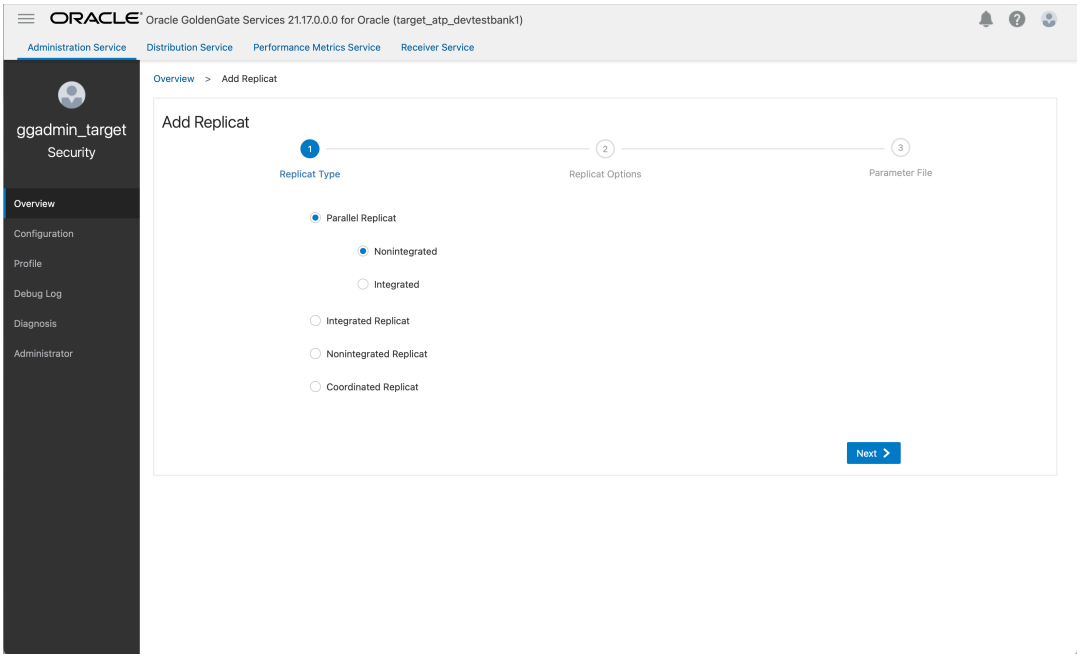
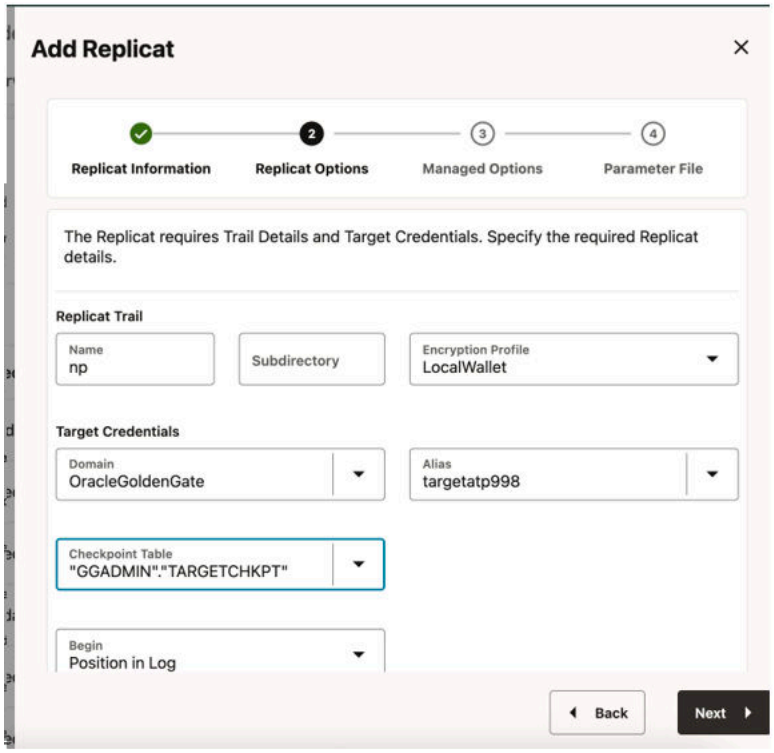


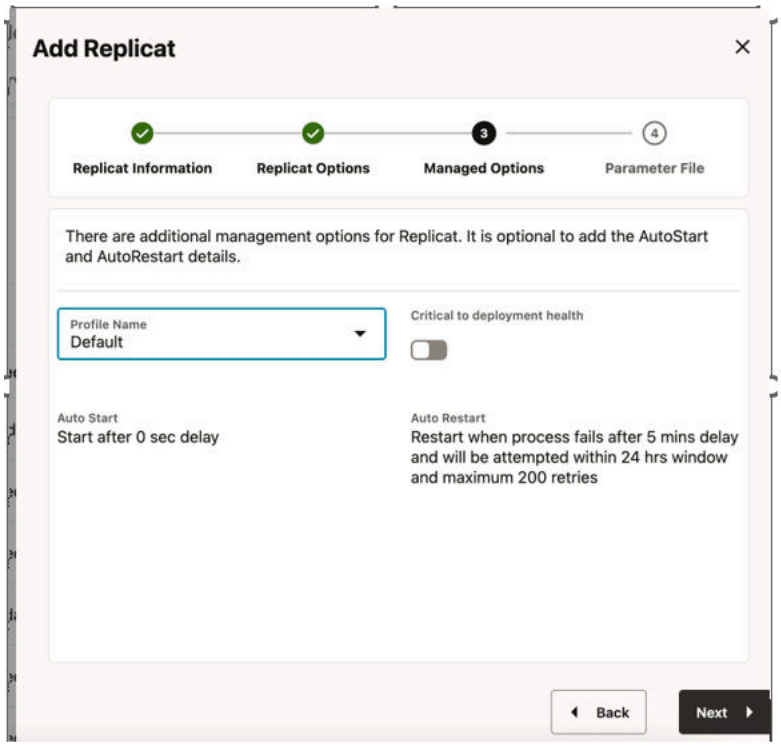
Figure 2-50 Replicat Type

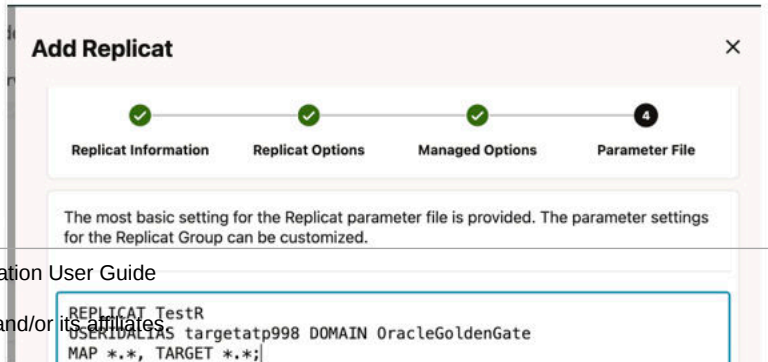


Copyright © 2025, Oracle and/or its affiliates.

Figure 2-51 Replicat Options







Copyright © 2025, Oracle and/or its affiliates.

5. To **Start** the Replicat, click on the **Play** button in the **Actions** column.

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.

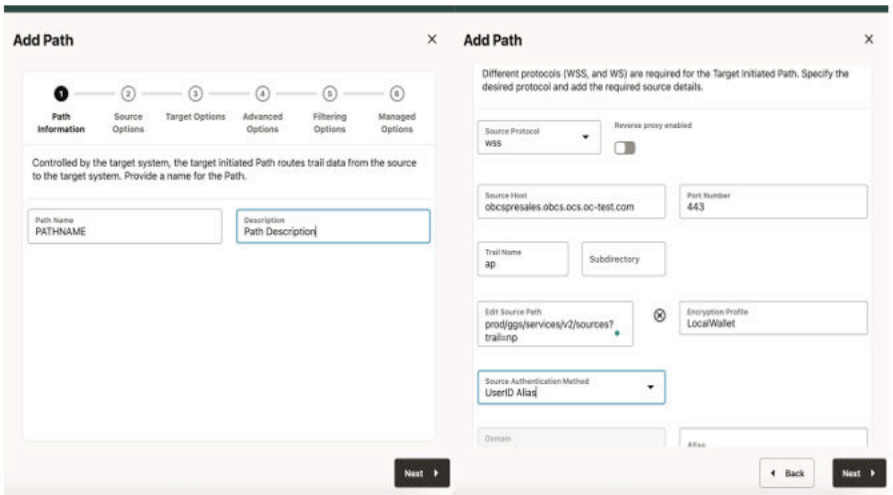
To create a Target-Initiated Distribution Path, follow the steps below:

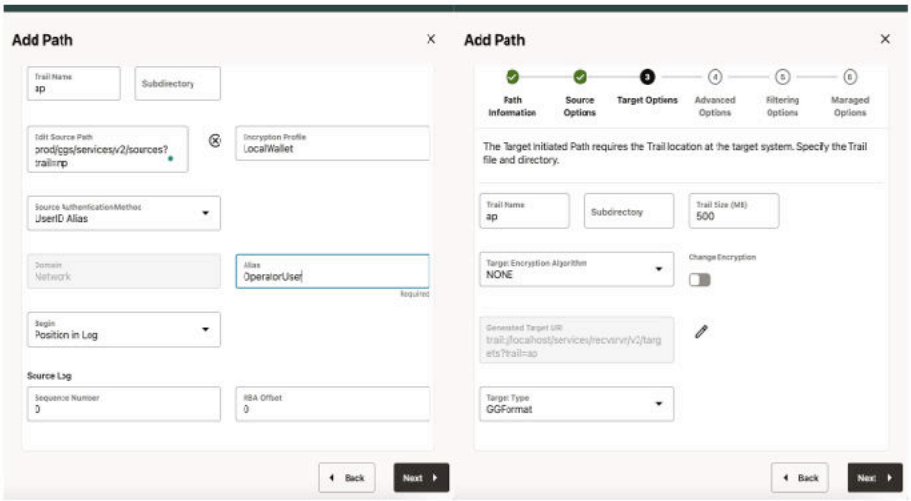
1. In the OCI GoldenGate self-service console, go to the **Receiver Service** section.
2. Under the Receiver Service page, locate and select the **Target-Initiated Path** option.
3. Click on the **"+"** symbol to create a new Target-Initiated Path.
4. **Enter the Path Details** as shown in the images 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).

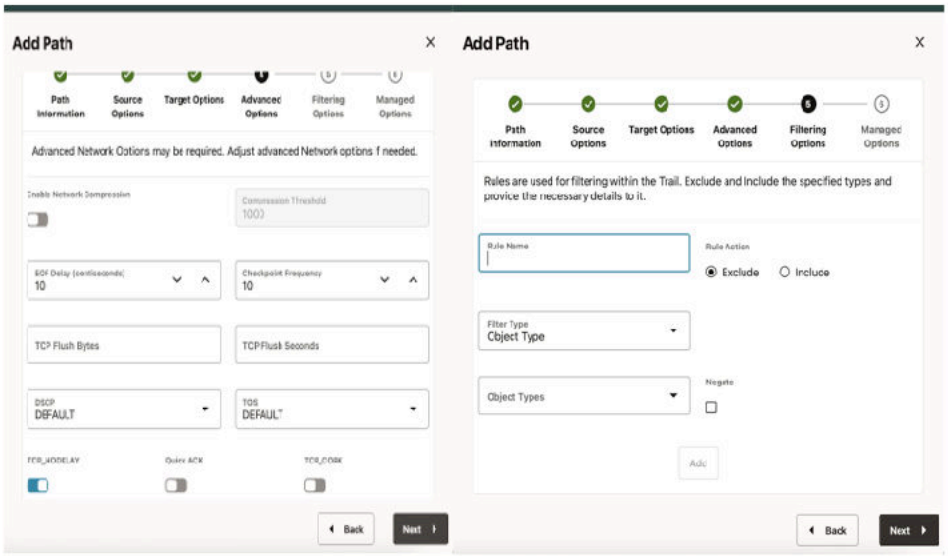
Figure 2-52 Add Receiver path

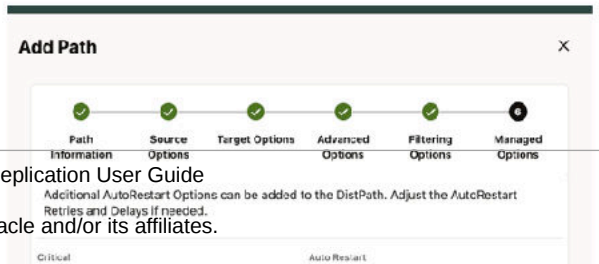
Copyright © 2025, Oracle and/or its affiliates.

Figure 2-53 Create Path









Copyright © 2025, Oracle and/or its affiliates.

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

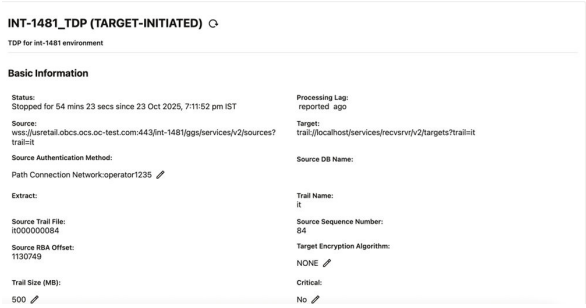
> **Note**
>
> Adding the OBCS App unique URI path in the source breaks the Generated Source URI.
> Hence, make sure the Generated Source URI is edited as shown below: wss://obcspresales.obcs.ocs.oc-test.com/nonprod/ggs:443/services/v2/sources?trail=np
>
> Change to
>
> wss://obcspresales.obcs.ocs.oc-test.com:443/non-prod/ggs/services/v2/sources?trail=np

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

Figure 2-54 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.

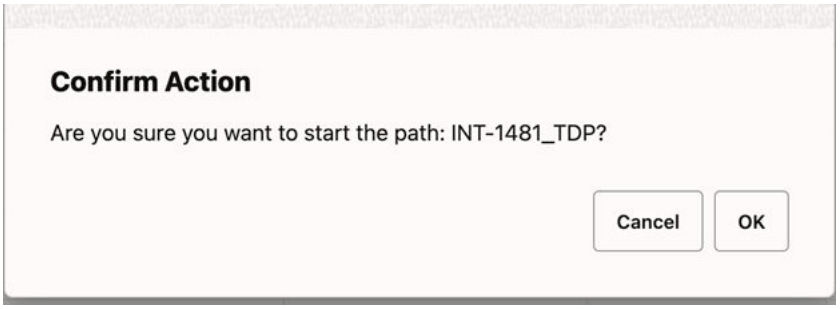
Figure 2-55 Receiver current Details



Copyright © 2025, Oracle and/or its affiliates.

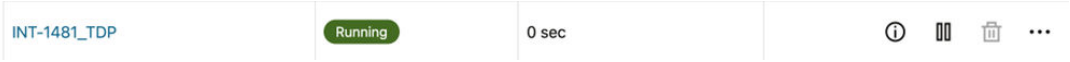
- Navigate back to Target Initiated Path and from the **Action** list for the Path, select **Start**.

Figure 2-56 Start Receiver Service



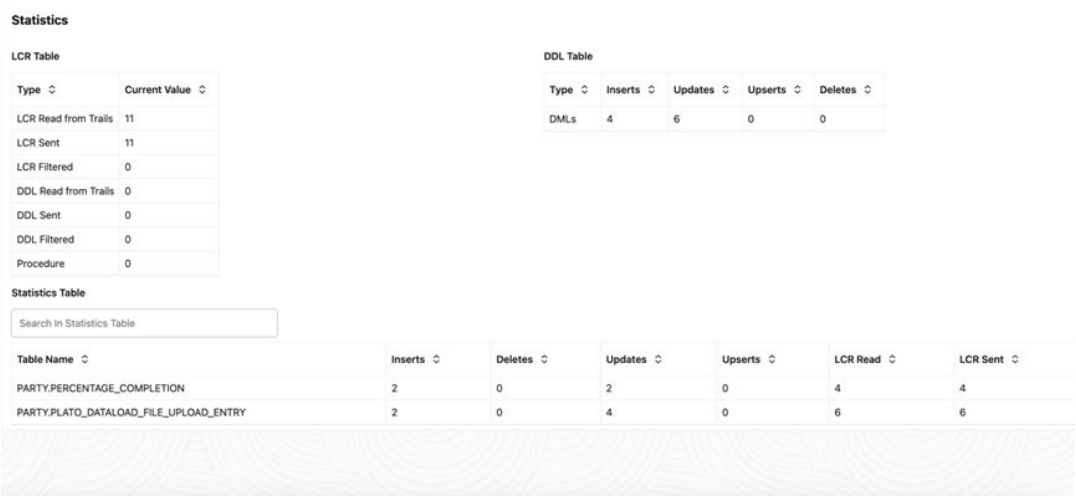
- Once the path is **up and running**, navigate to **Target-Initiated Path** from the left-hand menu and click on the **created path** to view its details.

Figure 2-57 Target-Initiated Path



- 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 Path statistics



- 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.

Copyright © 2025, Oracle and/or its affiliates.

2.4.4.1 Target OCI GoldenGate Deployment in devcorp

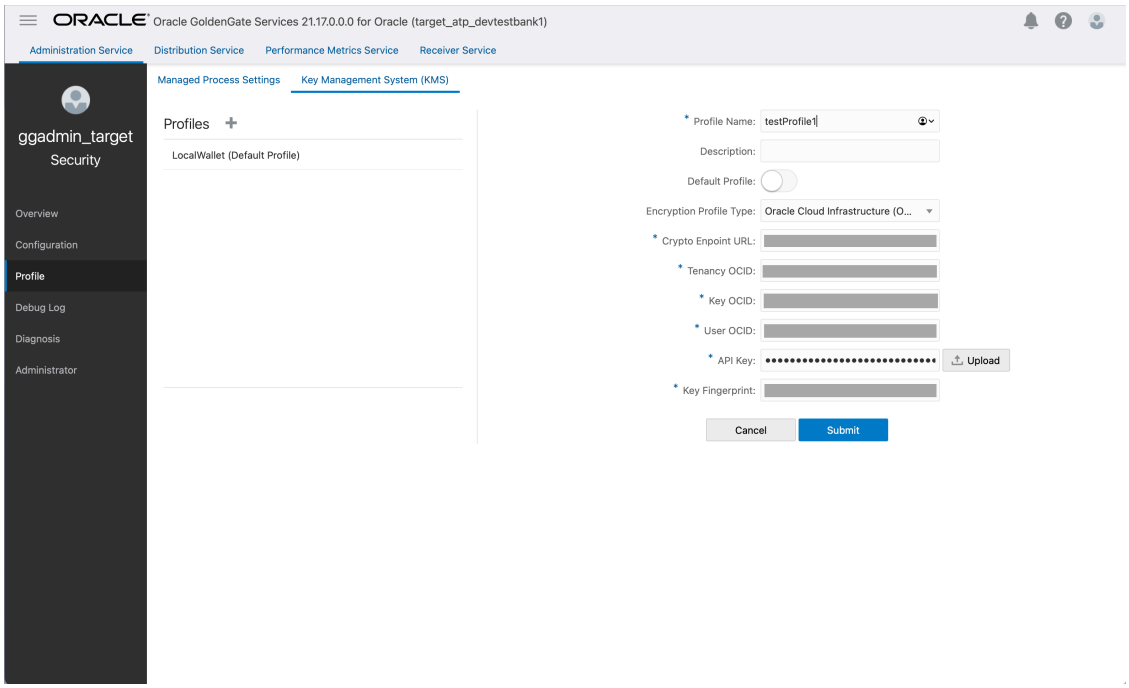
This topic provides information on target OCI goldengate deployment.

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.

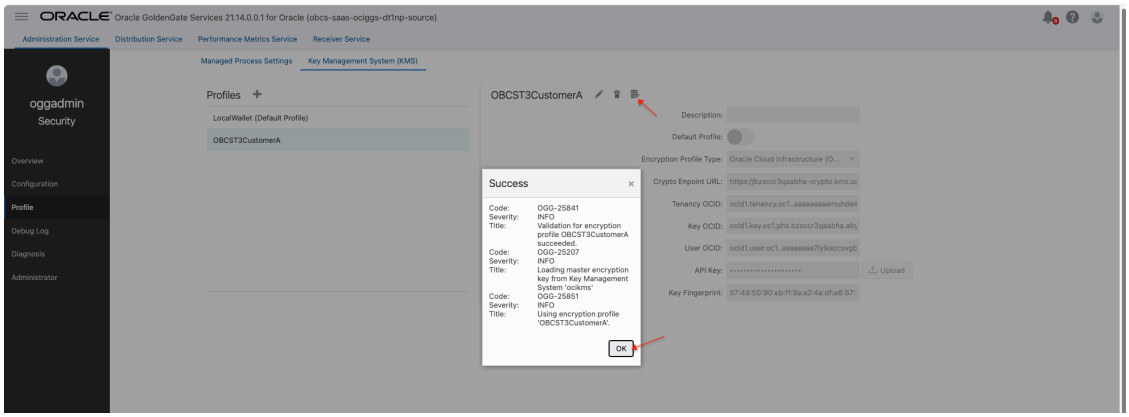
> **Note**
>
> Add a KMS Profile in Source OCI GoldenGate Deployment.

Figure 2-59 Key Management System Profile



Copyright © 2025, Oracle and/or its affiliates.

Figure 2-60 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.

Copyright © 2025, Oracle and/or its affiliates.

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.

Copyright © 2025, Oracle and/or its affiliates.

Index

Copyright © 2025, Oracle and/or its affiliates.