Oracle® FLEXCUBE Investor Servicing

Privacy by Design User Guide

Release 14.7.6.0.0
G30485-01
April 2025

ORACLE

Oracle FLEXCUBE Investor Servicing Privacy by Design User Guide, Release 14.7.6.0.0

G30485-01

Contents

Preface

Oracle FLEXCUBE Investor Servicing is a comprehensive mutual funds automation software from Oracle® Financial Servicing Software Ltd.©.

You can use the system to achieve optimum automation of all your mutual fund investor servicing processes, as it provides guidelines for specific tasks, descriptions of various features and processes, and general information.

This topic contains the following sub-topics:

Purpose

You are intended to become familiar with the **Oracle Flexcube Investor Servicing** application through this guide. This guide offers responses to particular features and procedures that are necessary for the module to operate effectively.

Audience

This user guide is intended for the Fund Administrator users and System operators in the AMC.

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.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

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.
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

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

Acronyms and Abbreviations

The list of the acronyms and abbreviations used are as follows:

Table Acronyms and Abbreviations

Abbreviation	Description
CIF	Customer Information File
EOD	End of Day
EPU	Earnings per unit
FCIS	Oracle FLEXCUBE Investor Servicing

Table (Cont.) Acronyms and Abbreviations

Abbreviation	Description
FMG	The Fund Manager component of the system
FPADMIN	Oracle FLEXCUBE Administrator
GTA	Global Transfer Agency
ID	Identification
IHPP	Inflation Hedged Pension Plan
IPO	Initial Public Offering
LEP	Life and Endowment Products
LOI	Letter of Intent
NAV	Net Asset Value
REG	The Registrar component of the system
ROA	Rights of Accumulation
ROI	Return on Investment
SI	Standing Instructions
SMS	Security Management System
URL	Uniform Resource Locator
VAT	Value Added Tax
WAUC	Weighted Average Unit Cost

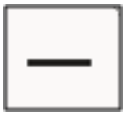
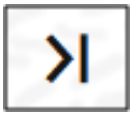
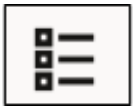
Symbols and Icons

This guide may refer to all or some of the following symbols and icons:

Table Symbols and Icons

Symbol/Icon	Function
	Lists all records maintained
	Minimize
	Maximize
	Close
	Perform Search

Table (Cont.) Symbols and Icons

Symbol/Icon	Function
	Open a list
	Select a Date
	Add a new row to enter details in a record.
	Delete a row, which is already added.
	Navigate to the first record
	Navigate to the last record
	Navigate to the previous record
	Navigate to the next record
	View a single record
	Sort the values in ascending or descending order
	Sort the values in ascending
	Sort the values in ascending

Basic Actions

Following are the basic actions of the screens that an user may require to perform on new or existing records in a screen.

Table Basic Actions

Action	Description
New	Used to add a new record. When the user click **New**, the system displays a new record enabling to specify the required data. **Note**: The fields, which are marked with an asterisk, are mandatory.
Copy	Used to copy the details of a record.
Close	Used to close a record. This action is available only when a record is created.
Unlock	Used to update the details of an existing record. System displays an existing record in editable mode.
Print	Used to print a record. This action is available only when a record is created.
Enter Query	Used to give details of a saved record in a detail screen. When the user click **Enter Query**, the system displays a saved record enabling to specify only the required or primary data.
Execute Query	User need to perform this after entering query. Click **Execute Query** after specifying the details of the record to be fetched, the system retrieves all the information of that particular record.
Audit	Used to view the maker details, checker details and report status.
Cancel	Used to cancel the performed action.
Save	Used to save the details entered or selected in the screen.
Refresh	Used to refresh the details selected in the screen.
Reset	Used to reset the fields to enter a new criteria.
Clear All	Used to clear all the data entered for search criteria.
Details	Used to navigate to Detail screen.
Search	Used to search either the details of a particular record or a list of records by querying particular field.
Advanced Search	Used to search details more precisely.
Approve	Used to approve the initiated report. This button is displayed, once the user click **Authorize**.
Authorize	Used to authorize the report created. A maker of the screen is not allowed to authorize the report. Only a checker can authorize a report, created by a maker.
Confirm	Used to confirm the performed action.
OK	Used to confirm the details in the screen.
Reject	Used to reject the report created. A maker of the screen is not allowed to authorize the report. Only a checker can reject a report, created by a maker.

Table (Cont.) Basic Actions

Action	Description
View	Used to view the report details in a particular modification stage. This button is displayed, once the user click **Authorize**.

Getting Help

Online help is available for all tasks. You can get help for any function or fields by clicking the help icon provided or by pressing **F1**.

Prerequisite

Specify **User ID** and **Password**, and log in to **Home Screen**.

1

Privacy By Design

This topic provides information on Privacy by Design.

Privacy by Design is to include functionality and options that allow customers to configure many privacy-related controls, such as logging, log retention and secure personally identifiable information.

In **Oracle FLEXCUBE Investor Servicing** privacy by design is achieved by the following features:

- Multi Factor Authentication
- Pseudonymization Data Masking
- Anonymization Data Masking
- Consent Recording
- Transparent Data Encryption (TDE)
- General Logging & Audit Logging
- Data Minimization / Data Deletion at Contract Term or Termination
- Data Portability
- End-user Access and Other Requests
- Separation of Duties

The topic contains the following sub-topics:

- Multi Factor Authentication - Access Control
  This topic provides an overview on Multi Factor Authentication.
- Implement Multi Factor Authentication
  This topic provides instructions to implement any third party MFA provider.
- Enable Multi Factor Authentication for User
  This topic provides the systematic instructions to enable Multi Factor Authentication for user.
- Log in Multi Factor Authentication Screen
  This topic provides the systematic instructions to log in Multi Factor Authentication Screen.
- Pseudonymization
  This topic provides an overview on Pseudonymization.
- Pseudonymization - User Classification
  This topic provides instructions to allow or restrict user to view PII data
- Anonymization
  This topic provides an overview on Anonymization.
- Process PII Access Policy Maintenance
  This topic provides the systematic instructions to maintain access to Personal Identifiable Information(PII).

1.1 Multi Factor Authentication - Access Control

This topic provides an overview on Multi Factor Authentication.

Multi Factor Authentication (MFA) is a method of confirming user access after multiple level of user access validation.

It includes:

- Authenticating the application **User ID** and **Password**.
- Additional authentication via third party multi-factor authentication provider.

Oracle FLEXCUBE Investor Servicing provides framework to enable **Multi Factor Authentication (MFA)** using third party MFA provider. MFA can be enabled at user level. If MFA is applicable for a user, user will be allowed to log in only after successful additional authentication implemented using MFA.

Oracle FLEXCUBE Investor Servicing is not shipped with any inbuilt third party MFA. IMFAAuthenticatePassword interface needs to be extended to implement MFA validation.

1.2 Implement Multi Factor Authentication

This topic provides instructions to implement any third party MFA provider.

In **Oracle FLEXCUBE Investor Servicing**, framework support is provided to implement any third party MFA provider.

Implement third party MFA authentication

1. Create new class `MFAAuthenticatePassword` by extending IMFAAuthenticatePassword interface.

The class file `MFAAuthenticatePassword.class` is created.

2. Place the class file `MFAAuthenticatePassword.class` in the file path `\FCJNeoWeb\Javasource\com\ofss\fcc\mfa` before building application EAR.
3. In `MFAAuthenticatePassword.process` method, enter parameter `dataMap` is of `HashMap` data type with Key values `UserId`, `MFAId`, and `MFAPin`.
4. The `MFAAuthenticatePassword.process` method should return xml with tag `msgStatus` as **SUCCESS** or **FAILURE**.

   The MFA Login will be considered as successful if `msgStatus` tag value is **SUCCESS**.

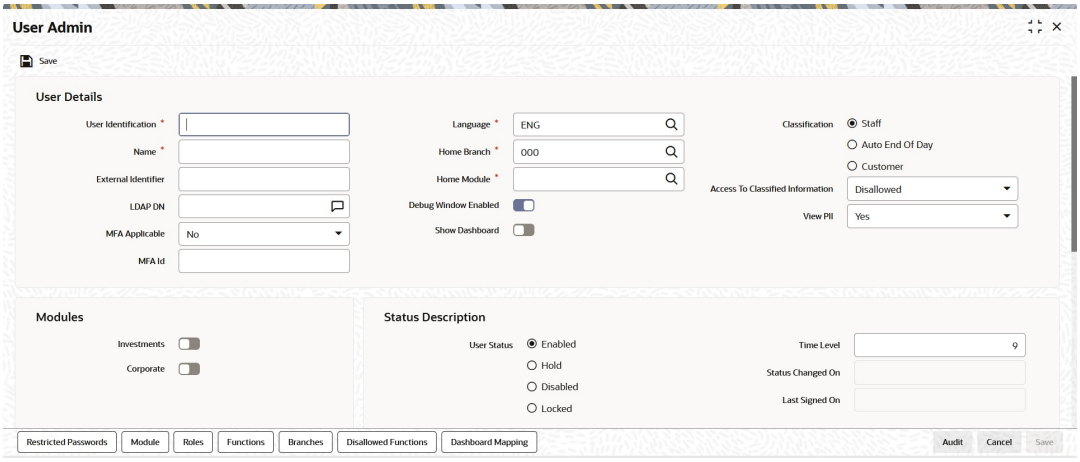
1.3 Enable Multi Factor Authentication for User

This topic provides the systematic instructions to enable Multi Factor Authentication for user.

1. On **Home** screen, type **SMDUSRDF** in the text box, and click **Next**.

   The **User Admin_Multi Factor Authentication** screen is displayed.

Figure 1-1 User Admin_Multi Factor Authentication



2. On **User Admin** screen, click **New** to enter the details.
3. Capture **MFA applicable** and **MFA ID** for a user in **User Details** section of **User Admin** screen to enable Multi Factor Authentication.
4. Select if MFA applicability is applicable or not from the drop-down list.

   If MFA applicable is selected as **Yes**, then **MFA ID** is mandatory.
5. Map one **MFA ID** to one user in the system.

   The **MFA ID** should be unique.
6. Consider even closed user for unique **MFA ID** validation.

   The **MFA ID** is an amendable field.

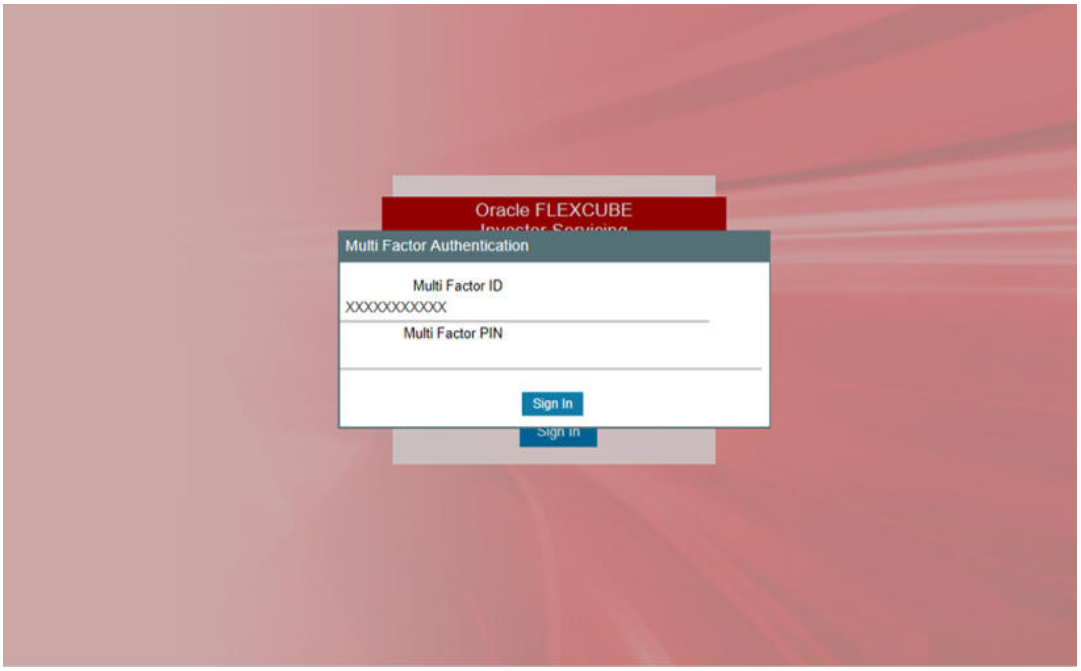
1.4 Log in Multi Factor Authentication Screen

This topic provides the systematic instructions to log in Multi Factor Authentication Screen.

1. Enter **Multi Factor PIN** and **Multi Factor ID** that the user will be prompted if the user is enabled for **Multi Factor Authentication (MFA)**, after successful application user authentication.

   The **Multi Factor Authentication** login page is displayed.

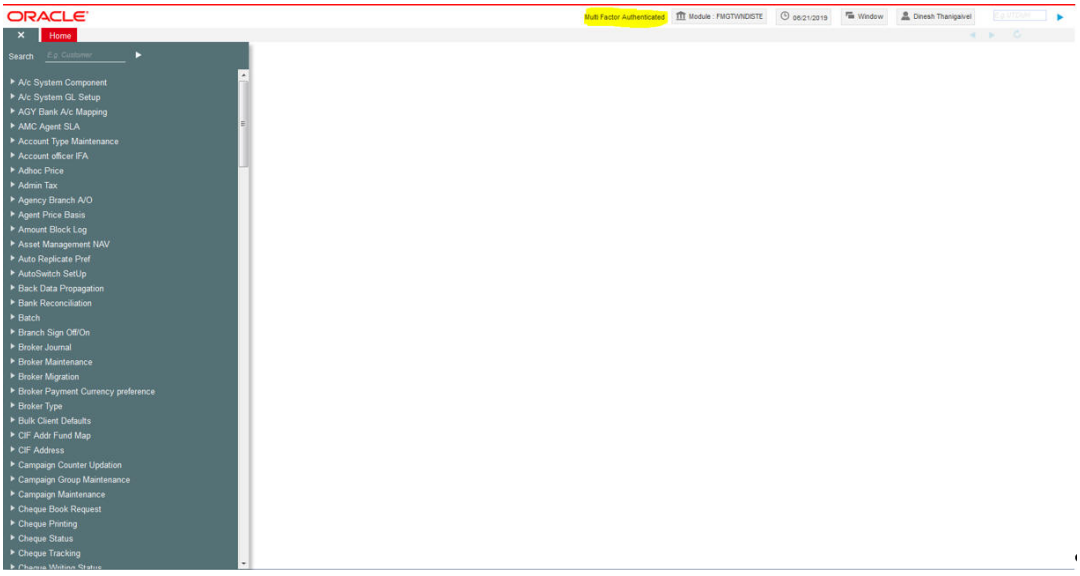
Figure 1-2 Multi Factor Authentication Login



2. Provide **Multi Factor PIN** to authenticate.

   On successful authentication, the system will log in to the application.

Figure 1-3 Multi Factor Authentication Screen



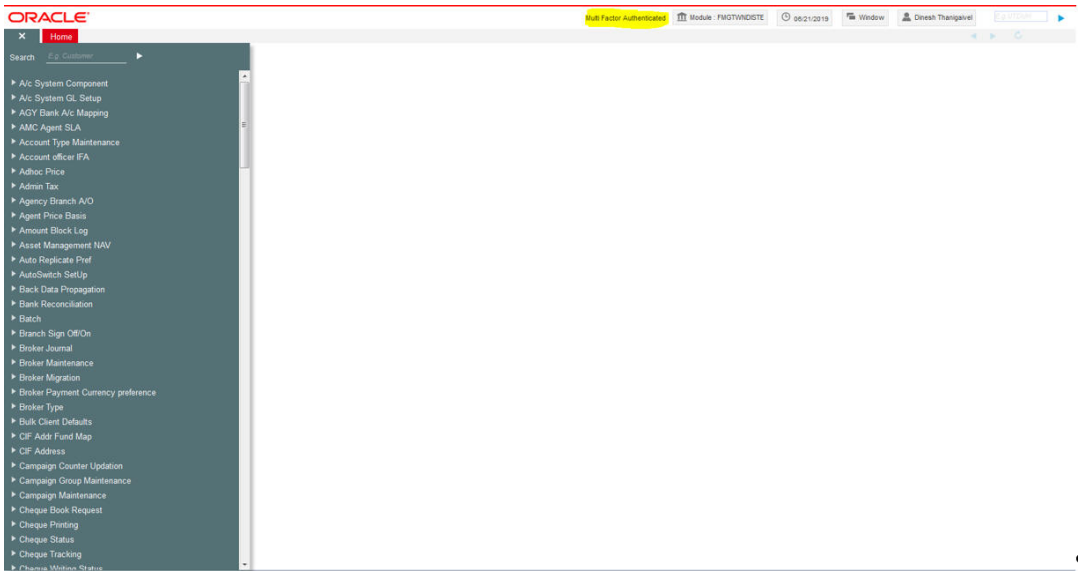
3. Log in to the application after successful authentication using MFA.

The system will validate MFA PIN for the MFA ID using implemented MFA class.

4. If user is MFA authenticated, then the system will show the MFA authentication status in the home page.

   The MFA authentication status is displayed in **Multi Factor Authentication** home page.

Figure 1-4 Multi Factor Authentication Screen



1.5 Pseudonymization

This topic provides an overview on Pseudonymization.

Pseudonymization is a procedure by which personally identifiable information within a data set is replaced by one or more artificial identifiers during view.

- Application users are allowed to view personal identifiable information as masked or clear text based on user classification.
- User with access to all personal information can view/modify all details as applicable in the roles mapped.
- User with no access to personal information will be restricted to access limited functions with only view option.

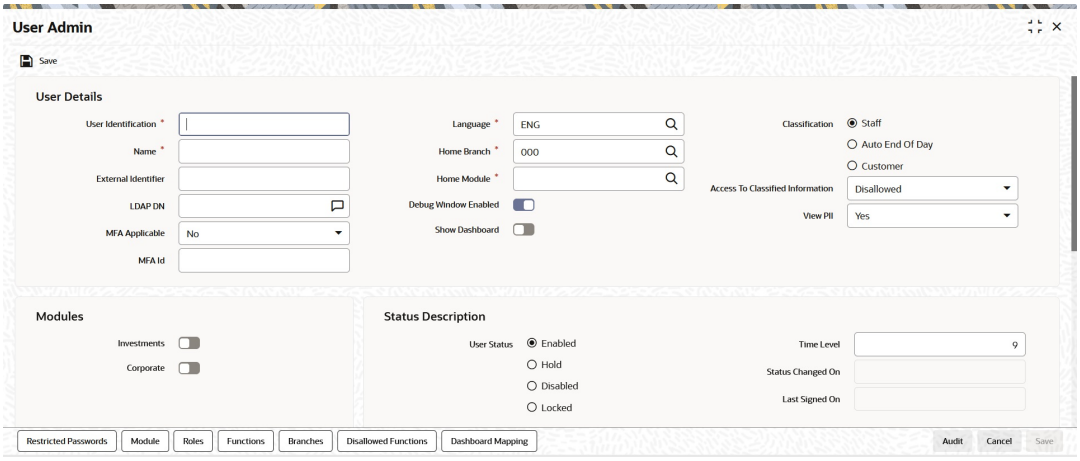
1.6 Pseudonymization - User Classification

This topic provides instructions to allow or restrict user to view PII data

1. On **Home** screen, type **SMDUSRDF** in the text box, and click **Next**.

   The **User Admin_View PII** screen is displayed.

Figure 1-5 User Admin_View PII



2. On **User Admin** screen, click **New** to enter the details.
3. Capture **View PII** for a user in the **User Details** section of **User Admin** screen to enable Pseudonymization.
4. Select if **View PII** is applicable or not from the drop-down list. User maintenance screen is enhanced to allow /disallow user to view PII data.

   If **View PII** is selected as **No**, you will be restricted to map only PIIVIEWROLE, PIIVIEWROLE_PAS roles. You cannot modify factory shipped PIIVIEWROLE, PIIVIEWROLE_PA to add other function IDs or other actions.

   There will not be any validation for amending these roles.

1.7 Anonymization

This topic provides an overview on Anonymization.

Anonymization process is either encrypting or partially removing personally identifiable information permanently in the database. Anonymization used when moving database from production server to other environment.

1.8 Process PII Access Policy Maintenance

This topic provides the systematic instructions to maintain access to Personal Identifiable Information(PII).

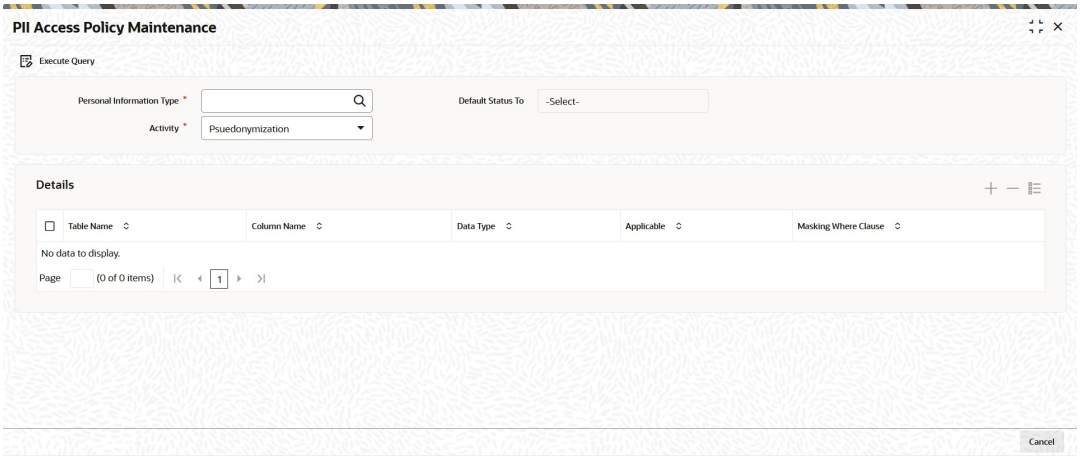
Personal Identifiable Information(PII) Access Policy Maintenance screen is used to maintain **Pseudonymization** table column mapping as needed. This maintenance allows enabling table column applicable for implementing Pseudonymization.

This screen is also used to maintain **Anonymization** table column mapping. This maintenance allows enabling table column applicable for implementing Anonymization. Application user cannot add any data in the screen.

1. On **Home** screen, type **UTDPIIMT** from UT Module or **PADPIIMT**from Pension Administration module in the text box, and click **Next**.

   The **PII Access Policy Maintenance** screen is displayed.

Figure 1-6 PII Access Policy Maintenance



2. On **PII Access Policy Maintenance** screen, click **Enter Query** to enter the details.

   For more information on fields, refer to the field description table.

Table 1-1 PII Access Policy Maintenance - Field Description

Field	Description
Personal Information Type	*Alphanumeric; 200 Characters; Mandatory* Specify the personal information type to be restricted. Alternatively, you can select personal information type from the option list. The list displays all valid personal information type maintained in the system.
Activity	*Mandatory* Select the activity status from the drop-down list. The list displays the following values: • **Pseudonymization** • **Anonymization** Click **Execute Query** option after specifying **Personal Information Type** and **Activity**. The system displays the following values pertaining to the personal information type details: • **Table Name** • **Column Name** • **Data Type** • **Applicable** • **Anonymization Where Clause** Click **Unlock** option to edit the above values.
Personal Information Type	*Display* The system displays the personal information type details provided before executing the query.
Default Status to	*Optional* Select the status that needs to be defaulted from the drop-down list. The list displays the following values: • **Yes** • **No** If you select **Yes** then the system resets **Applicable** field to **Yes** for all the records. Same is the case if you select **No**.
Details	The section displays the following fields.

Table 1-1 (Cont.) PII Access Policy Maintenance - Field Description

Field	Description
Table Name	*Display* The system displays the table name based on the **Personal Information Type** value selected.
Column Name	*Display* The system displays the column name based on the **Personal Information Type** value selected.
Data Type	*Display* The system displays the data type based on the **Personal Information Type** value selected.
Applicable	*Mandatory* The system default the status based on the **Default Status to** value selected. However, you can amend this value by selecting **Yes** or **No** from the from the drop-down list. • For Pseudonymization, if you select **Applicable** field as **Yes**, then system will mask data as the format maintained. Else, the system will not mask the data. • For Anonymization, if you select **Applicable** field as **Yes**, the system will update data with hashed value. Else, the system will not update the data.
Anonymization Where Clause	*Display* The system displays the Anonymization where clause for the table column. **Note:** Anonymization where clause is applicable only for Anonymization batch.

3. Click **Save** after providing the necessary details.

- PII Access Policy Maintenance - Pseudonymization
  This topic provides the instructions to maintain **Pseudonymization** table column mapping.
- PII Access Policy Maintenance - Anonymization
  This topic provides the instructions to maintain **Anonymization** table column mapping.

1.8.1 PII Access Policy Maintenance - Pseudonymization

This topic provides the instructions to maintain **Pseudonymization** table column mapping.

1. Select **Pseudonymization** in the **Activity** field of the **PII Access Policy Maintenance** screen.

   If Pseudonymization Applicable field is changed, then the system will mark the same for regeneration of policy.

> **Note:**
>
> You can add or modify the service provider related table masking only in default FMG as maintained. All the Redact related details will be factory shipped. For any new maintenance the predefined data needs to be maintained operationally.

2. The factory shipped data will show only first 3 characters and rest will be masked for the remaining length of the data. The system will mask the data whose length is less than 3.

   Note the following:

   - The system defaults Marital status, Sex to predetermined values.
   - Schema user with DBA Role or Grants, PII protection will not be applicable.
   - Data Masking of Tanked data is not applicable.
   - Redact Policy creation on particular table makes all the objected references invalid.
   - Redact Policy needs to be done during non-business hours.

1.8.2 PII Access Policy Maintenance - Anonymization

This topic provides the instructions to maintain **Anonymization** table column mapping.

1. Select **Anonymization** in the **Activity** field.
2. Edit Anonymization table column mapping in the **PII Access Policy Maintenance** screen.
3. Perform **View** and **Modify** operations in this screen.

   User will not be allowed to add additional details through screen.

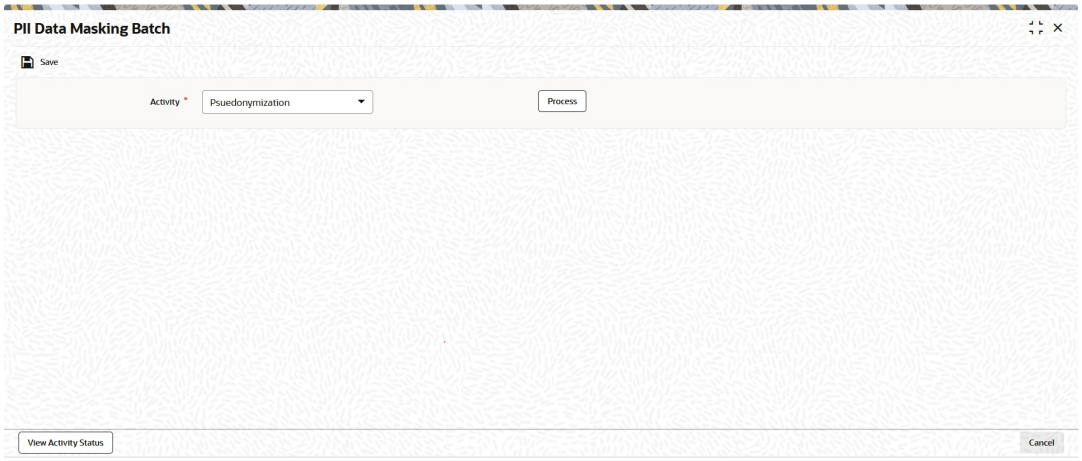
1.9 Process PII Data Masking Batch

This topic provides the systematic instructions to start the Pseudonymization or Anonymization process.

1. On **Home** screen, type **UTDPIIBT** from UT Module or **PADPIIBT** from Pension Administration module in the text box, and click **Next**.

   The **PII Data Masking Batch** screen is displayed.

Figure 1-7 PII Data Masking Batch



2. On **PII Data Masking Batch** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 1-2 PII Data Masking Batch - Field Description

Field	Description
Activity	*Mandatory* Select the activity from the drop-down list. The list displays the following values: • **Pseudonymization** • **Anonymization**

3. Click **Process** to process the batch.

- PII Data Masking Batch - Pseudonymization
  This topic provides the instructions to process Pseudonymization.
- PII Data Masking Batch - Anonymization
  This topic provides the instructions to process Anonymization.
- View Activity Status
  This topic provides the systematic instructions to view the activity status once the batch is processed.

1.9.1 PII Data Masking Batch - Pseudonymization

This topic provides the instructions to process Pseudonymization.

1. Select **Pseudonymization** in the **Activity** field to process Pseudonymization policy creation and click **Process**.

   The system submits the job to create/alter redact policy for which changes are done.

2. Specify Keystring details and click **View Activity Status** to view the status of the Pseudonymization process.

   The system displays the following values:

   - **Tables**
   - **Column Name**
   - **Status**
   - **Error Code**
   - **Error Description**

1.9.2 PII Data Masking Batch - Anonymization

This topic provides the instructions to process Anonymization.

1. Select **Anonymization** in the **Activity** field and click **Process** to process Anonymization.
2. Anonymization Personal Information Batch is to permanently anonymize PII data after execution of this batch.

   For every execution a **Batch Number** will be generated. The **Batch Number** is used to view the activity status.

3. Click **View Activity Status** button to view the list of activities in each status by selecting current status and batch number.

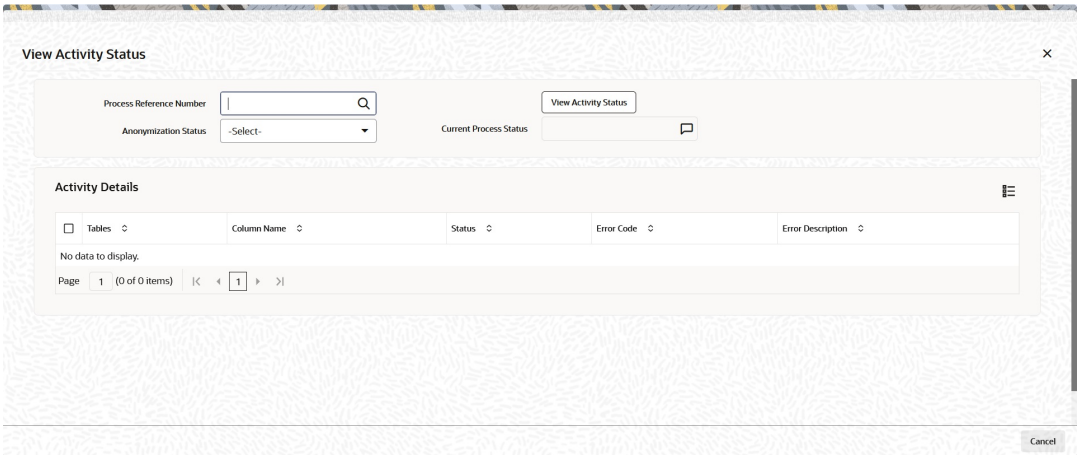
1.9.3 View Activity Status

This topic provides the systematic instructions to view the activity status once the batch is processed.

1. On the **PII Data Masking Batch** screen, click **View Activity Status** button to view the status of the Anonymization process.

   The **View Activity Status** screen is displayed.

Figure 1-8 PII Data Masking Batch_View Activity Status Button



2. On **View Activity Status** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-3 View Activity Status - Field Description

Field	Description
Process Reference Number	*Alphanumeric; 50 Characters; Optional* The system displays the process reference number to query the status. However you can amend this value by selecting the values from the option list. The list displays all valid key string maintained in the system.
Anonymization Status	*Optional* Select the anonymization status from the drop-down list. The list displays the following values: • **Not Started** • **Running** • **Failed** • **Completed**

Table 1-3 (Cont.) View Activity Status - Field Description

Field	Description
Current Process Status	*Optional* Select the current status from the drop-down list. The list displays the following values: • **Not Started** • **Running** • **Failed** • **Completed**

3. Click **View Activity Status** button after specifying the necessary details.

   The system displays the following values:

   - **Tables**
   - **Column Name**
   - **Status**
   - **Error Code**
   - **Error Description**

4. Start the process once all the Anonymization static data is verified.
5. Once the process is running, you cannot run another process.

   If you click **Process** button while Anonymization job is running, the system will display an error message.

6. Restart the failed Anonymization process after correcting the necessary data process.
7. Update the status to restart on abort.
8. Click **Process** button if the job is completed with an error.

   The system restarts the masking process for the failed tables.

9. Mask the data by giving Seed value in **SEEDDATA** Param code in **Parameter Setup Detail** screen.

   This can be changed before each process of Anonymization. Specifically, one seed data for one complete process for all fund managers.

   All the policy related Pseudonymization and row level security should be disabled or dropped.

1.10 Transparent Data Encryption

This topic provides information on Transparent Data Encryption.

Introduction

Transparent Data Encryption (TDE) enables to encrypt sensitive data, such as Personally Identifiable Information stored in tables and tablespaces.

After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access this data.

TDE helps protect data stored on media (also called data at rest) in the event that the storage media or data file is stolen.

Oracle Database uses authentication, authorization, and auditing mechanisms to secure data in the database, but not in the operating system data files where data is stored. To protect these data files, Oracle Database provides **Transparent Data Encryption (TDE)**.

TDE encrypts sensitive data stored in data files. To prevent unauthorized decryption, TDE stores the encryption keys in a security module external to the database, called a **keystore**.

Enable TDE for Database

Refer *Installation manual database* to enable TDE for a database.

1.11 Process Consent Maintenance Detail

This topic provides the systematic instructions to capture the consent details.

Customer options for providing consent on data usage and sharing at point and time where the end-user data is collected.

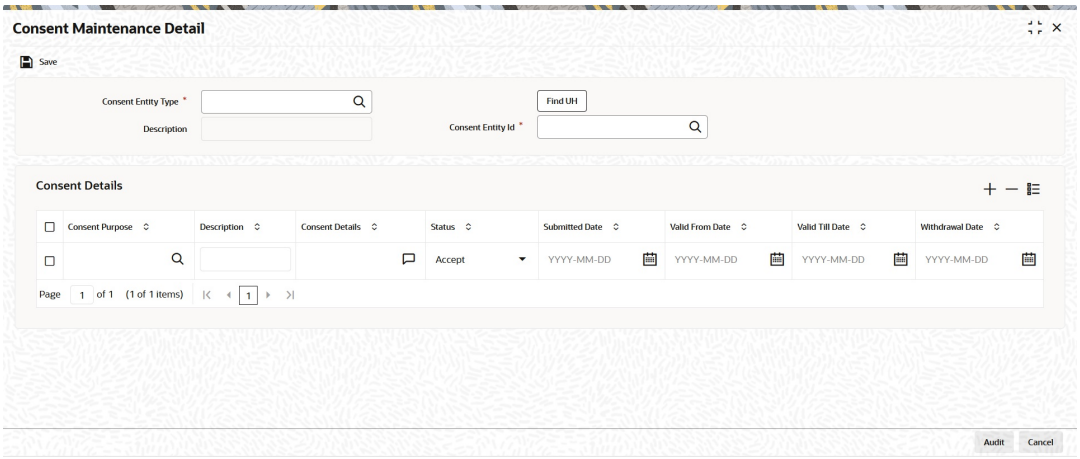
This screen allows to capture consent/opt-in for service offering. Also for customer to configure list of data captured, stored, shared and for what business purpose. It also allows customer to opt-out of the service provided or accept and opt-out request from the process.

If consent is provided for the same purpose, existing consent details will be overridden. Only new consent details for the same purpose will be stored in the system. History of consent details available only in audit logs.

1. On **Home** screen, **UTDCONMT** from **agency branch module** and **PADCONMT** from **Pension module** in the text box, and click **Next**.

   The **Consent Maintenance Detail** screen is displayed.

Figure 1-9 Consent Maintenance Detail



2. On **Consent Maintenance Detail** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 1-4 Consent Maintenance Detail - Field Description

Field	Description
Consent Entity Type	*Alphanumeric; 1 Character; Mandatory* Specify the consent entity type. Alternatively, you can select consent entity type from adjoining option list. The list displays all valid consent entity type maintained in **CONSENTENTITY** Param code.
Description	*Display* The system displays the description for the selected consent entity type.
Consent Entity ID	*Alphanumeric; 12 Characters; Mandatory* Specify the consent entity ID. Alternatively, you can select consent entity ID from adjoining option list. The list displays all valid consent entity ID maintained in the system. • If you select **U - Unit Holder ID** in **Consent Entity Type** field, then **Find UH** button will return unit holder details. • If you select **P - PAS Party ID**, then **Find UH** is not applicable.
Consent Details	The section displays the following fields.
Consent Purpose	*Alphanumeric; 100 Characters; Mandatory* Specify the purpose of consent. Alternatively, you can select consent purpose from adjoining option list. The list displays all valid consent purpose maintained in the **CONSENTPURS** param code. Consent purpose cannot be deleted but can be withdrawn.
Consent Details	*Alphanumeric; 255 Characters; Optional* Specify the details of the consent.
Status	*Optional* Select the status of consent from the drop-down list. The list displays the following values: • **Accept** • **Withdraw**
Submitted Date	*Date Format; Mandatory* Select the date on when the consent request is received from the adjoining calendar.
Valid From Date	*Date Format; Mandatory* Select the validity period from the adjoining calendar. This field is applicable only if you have selected **Status** field as **Active**.
Valid Till Date	*Date Format; Mandatory* Select the validity period from the adjoining calendar. This field is applicable only if you have selected **Status** field as **Active**.
Withdrawal Date	*Date Format; Optional* Select the date of withdrawal from the adjoining calendar. This field is applicable only if you have selected **Status** field as **Withdraw**. The Record modified date will be considered as Withdrawal date.

1.12 Consent Maintenance Summary

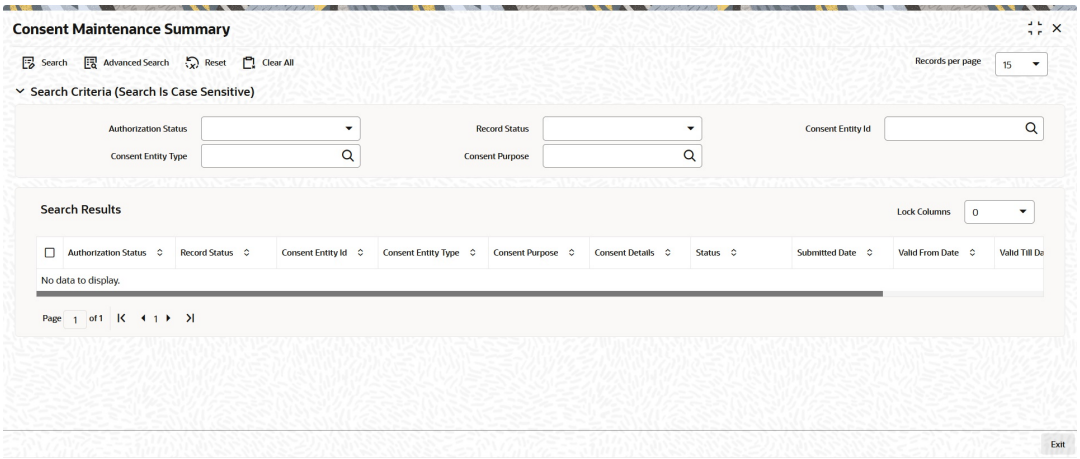
This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve Consent Maintenance Record

1. On **Home** screen, type **UTSCONMT** in the text box, and click **Next**.

   The **Consent Maintenance Summary** screen is displayed.

Figure 1-10 Consent Maintenance Summary



2. On **Consent Maintenance Summary** screen, specify any or all of the following details in the corresponding fields.
   - **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.
   - **Record Status**
   - **Consent Entity ID**
   - **Consent Purpose**
   - **Consent Entity Type**
3. Click **Search** to view the records.

   All the records with the specified details are retrieved, and displayed in the screen.

> **Note:**
>
> You can also retrieve the individual record detail from the detail screen by querying in the following manner:
>
> - Press F7
> - Input the Consent Entity ID/Type
> - Press F8

4. Perform **Edit**, **Amend**, and **Authorize** operations by selecting the desired operation from the Action list. You can also search a record by using a combination of % and alphanumeric value.

- Edit Consent Maintenance Record
  This topic provides the systematic instructions to edit Consent Maintenance Record.

- View Consent Maintenance Record
  This topic provides the systematic instructions to view Consent Maintenance Record.
- Authorize Consent Maintenance Record
  This topic provides the systematic instructions to authorize Consent Maintenance Record.
- Amend Consent Maintenance Record
  This topic provides the systematic instructions to amend Consent Maintenance Record.
- Authorize Amended Consent Maintenance Record
  This topic provides the systematic instructions to authorize amended Consent Maintenance Record.

1.12.1 Edit Consent Maintenance Record

This topic provides the systematic instructions to edit Consent Maintenance Record.

Modify the details of Consent Maintenance record that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **Consent Maintenance Summary** screen from the Browser.
2. Select the status of the record that you want to retrieve for modification in the **Authorization Status** field.

   You can only modify records that are unauthorized. Accordingly, choose the **Unauthorized** option.
3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.
4. Click **Search** button.

   All unauthorized records with the specified details are retrieved and displayed in the screen.
5. Double-click the record that you want to modify in the list of displayed records.

   The **Consent Maintenance** screen is displayed.
6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.
7. Click **Save** to save your changes.

   The **Consent Maintenance Detail** screen is closed and the changes made are reflected in the **Consent Maintenance Summary** screen.

1.12.2 View Consent Maintenance Record

This topic provides the systematic instructions to view Consent Maintenance Record.

View a record that you have previously input by retrieving the same in the **Consent Maintenance Summary** screen. Perform this operation as follows:

1. Start the **Consent Maintenance Summary** screen from the Browser.
2. Select the status of the record that you want to retrieve for viewing in the **Authorization Status** field.

   You can also view all records that are either unauthorized or authorized only, by choosing the Unauthorized/Authorized option.
3. Specify any or all of the details of the record in the corresponding fields on the screen and click **Search** button.

All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to view in the list of displayed records.

   The **Consent Maintenance Detail** screen is displayed.

1.12.3 Authorize Consent Maintenance Record

This topic provides the systematic instructions to authorize Consent Maintenance Record.

Authorize an unauthorized Consent Maintenance record in the system for it to be processed as follows:

1. Start the **Consent Maintenance Summary** screen from the Browser.
2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.
3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.
4. Double-click the record that you wish to authorize.

   The **Consent Maintenance Detail** screen is displayed.
5. Select **Authorize** operation from the Action List.

   When a checker authorizes a record, details of validation, if any, that were overridden by the maker of the record during the **Save** operation are displayed. If any of these overrides results in an error, the checker must reject the record.

1.12.4 Amend Consent Maintenance Record

This topic provides the systematic instructions to amend Consent Maintenance Record.

Modify the details of an authorized record using the **Unlock** operation from the Action List. To make changes to a record after authorization:

1. Start the **Consent Maintenance Summary** screen from the Browser.
2. Select the status of the record that you want to retrieve for amendment.

   You can only amend authorized records.
3. Specify any or all of the details and click **Search** button.

   All records with the specified details are retrieved and displayed in the screen.
4. Double-click the record that you wish to amend.

   The **Consent Maintenance Detail** screen is displayed.
5. Select **Unlock** operation from the Action List to amend the record.
6. Amend the necessary information and click **Save** to save the changes.

1.12.5 Authorize Amended Consent Maintenance Record

This topic provides the systematic instructions to authorize amended Consent Maintenance Record.

Authorize an amended Consent Maintenance record for the amendment to be made effective in the system. The authorization of amended records can be done only from Fund Manager Module and Agency Branch module.

The process of subsequent authorization is the same as that for normal transactions.

1.13 Data Minimization/ Data Deletion

This topic provides information on Data Minimization/ Data Deletion.

Introduction

Data minimization is the process of deleting the data on expiry of the holding period.

End-User Access and Other Requests

The following are the end-user access and other requests that helps in data minimization:

- Use Purge/Archival process to minimize the data set.
- Specify Purge/Archival process at functionality level or at table level.
- Specify the table and the set of records to be deleted by maintaining valid join conditions among the tables.
- Data minimization can also be scheduled to run on specific time intervals.

Refer *Purge Frequency Maintenance* for further details in *Admin* user manual.

1.14 Data Portability

This topic provides information on Data Portability.

Introduction

Customers may be required to provide end-users with copies of their data in a structured, commonly used electronically readable format. Support a configuration that lets customers enable their end-users to perform the export themselves or provide means for end-users to request that customer perform it.

Import/Export of Data

The following are the points that support data portability:

- User can export or import data set with Data Interface maintenance.
- User can specify the set of tables, columns that need to be exported or imported.
- User can also specify the format in which export/import file need to be generated.

Refer *Setting up and Maintaining Interfaces* for further details in *Interface* user manual.

1.15 Separation of Duties

This topic provides information on Separation of Duties.

Row Level Security

Application users are classified to allow/disallow to access sensitive information. Customers will be classified as protected and unprotected.

Users with full access are allowed to see all customers. Users with limited access are allowed to view unprotected customer.

Refer to the topic *Row Level Security Maintenance* for further details in *Security* User Manual.

Refer to the topic *Process Customer Maintenance Detail* for further details in *Entities* User Manual.

Access Control on Function IDs

Role based access to the User with appropriate module will be able to perform his duties.

With grouping of Function ids into roles users can be mapped to particular roles as per their requirements. Also user's access across module to specific function ID can be restricted.

Refer to the topics *Ensuring Security for Fund Manager* and *Ensuring Security for Agency Branch* for further details in *Security* User Manual.

1.16 General Logs and Audit Controls

This topic provides information on general logs and audit controls.

Log in PII Data Access

FCIS supports storing PII data accessed by the business user. The data access audit log covers the following data:

- Unit Holder Account Information and change of information(amendment)
- Customer Information and change of information
- Transactions
- Unit holder balance
- Consolidated inquiry
- Unit holder income distribution setup
- Balance view through various transaction screen (through hyperlinks)
- Audit of personnel accessing the above data will stored/ logged and the details are as following:
  - User Identification
  - Access date and Time(Application date and system date)
  - Operation
  - function id accessed
  - Unit holder account/Entity ID/Auth rep ID
  - Customer account
  - To unit holder account (in case of transfers)
  - To Customer account (in case of transfers)

Refer *Personal Data Protection Act document* for further details.

General Logging
FCIS supports logging data captured or modified by the business user. The audit log stores the user name, data captured date time and the captured data for audit purposes.

Enabling/ Disabling Application Logs
Application logs can be enabled at application level to identify any failures. By default, application logs are disabled. Administrators or support team only can enable application logs.

1.17 Backup and Recovery

This topic provides information on Backup and Recovery.

Backup and Recovery

Take backup of all database related files such as, data files, control files, redologs, archived files, init.ora, config.ora, etc., periodically to reduce the data loss.

Secure Backup
Security Guide provides detailed information on securing database, backup controls and securing database backups.

Index