Oracle FCCM Cloud Services

Case Investigation

User Guide

Release 23.11.1

November 2023

F36014-1

ORACLE®
Financial Services

Oracle FCCM Cloud Service Case Management User Guide

Document Control

Table 1 lists the document control.

Table 1: Revision History

Revision Number	Revision Date	Change Log
23.11.1	November 2023	Added Add to Exemption.
23.9.1	September 2023	- Added the following fields in Table 7 : - Message Type - Amount - Message Reference - Transaction Reference - Added note in the Access the Take Action Window section.
23.8.1	August 2023	Updated the Events List section.
23.5.1	May 2023	Updated the following sections/pages: - Fields in Customer Details Page and their Descriptions - The Account Details (Entities) page - Creating Cases
23.2.1	March 2023	Updated the Relationship and Creating Cases sections.
22.11.1	November 2022	Updated to include new features, such as in-app notifications, the US SAR Continuing Activity case type, enhanced filtering, and time zone support.
22.8.1	August 2022	Updated to include new functionality for case tags, primary entities, and updates to the Dashboard and Customer Details. A new section "Watchlist Match Disposition" was added to the Risk Assessment tab section.
22.5.1	May 2022	Updated to provide information about Primary Entities, describe the Dashboard and Entities tabs, and share updates made to Customer Details. It also describes updates made to the Risk Assessment tab for KYC Batch and KYC Onboarding cases.
22.2.1	February 2022	Updated to provide guidance on Entity Versioning, tell how to Export the Case Report, and provide additional guidance for KYC cases.

Table 1: Revision History

Revision Number	Revision Date	Change Log
21.11.1	November 2021	Updated to include instructions for manually creating cases and events, using Smart Case Search, working with Case Tags, and provide information about how to use the Case Network and Transaction graphs. There were also minor changes made to fields which display in various screens. Additional updates were made to describe changes made to the Risk Assessments and Prospect screens, and tell how to use the KYC Risk Score, Network Diagram and Customer/Interested Party sections, which are applicable to KYC cases only.
21.8.1	August 2021	Updated to include instructions for creating customized Case List views, and enhancements to how customer relationships and account details display.
21.6.1	June 2021	Updated to provide guidance on using the enhanced user interface, including Enhanced Entity Details, Case Audit History, and GDPR Compatibility.
21.2.1	February 2021	Updated to enhance batch processing information and to allow Analyst users to recommend that a Regulatory Report is filed for a case.
10.0.0.0 Second edition	December 2020	Updated to include screens added for Oracle FCCM Know Your Customer Cloud Service and Oracle FCCM Customer Screening Cloud Service.
10.0.0.0 First edition	October 2020	This is the first version of the Oracle Financial Crime and Compliance Management Cloud Service documents for Release 10.0.0.0.0.

Table of Contents

1   Preface

This preface introduces information sources that can help you use the application.

1.1   Using Oracle Applications

1.1.1   Help

Use help icons ❓ to access help in the application. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. Not all pages have help icons. You can also access the Oracle Help Center to find guides and videos.

1.1.2   Watch video

▶ Watch: This video tutorial shows you how to find and use help.

You can also read about it instead.

1.1.3   Additional Resources

- Community: Use Oracle Cloud Customer Connect to get information from experts at Oracle, the partner community, and other users.

- Training: Take courses on Oracle Cloud from Oracle University.

1.1.4   Conventions

Table 2 lists the conventions used in this document.

Table 2: Conventions Used in this Guide

Conventions	Meaning
Italics	● Names of books as references ● Emphasis ● Substitute input values
Bold	● Menu names, field names, options, button names ● Commands typed at a prompt ● User input
`Monospace`	● Directories and subdirectories ● File names and extensions ● Process names ● Code sample, including keywords and variables within the text and as separate paragraphs, and user-defined program elements within the text
Hyperlink	● Hyperlink type indicates links to the external websites and internal document links to sections
Asterisk (*)	● Mandatory fields in User Interface
<Variable>	● Substitute input value

1.2   Contacting Oracle

1.2.1   Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit My Oracle Support or visit Accessible Oracle Support if you are hearing impaired.

1.2.2   Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: My Oracle Support (MOS).

2   About Case Management

This application allows you to search, investigate, and take action on cases. After a case is created and appears in the application, your actions towards investigation and resolution change the status of a case from new (New) to closure (Closed as True Positive or Closed as False Positive). The application supports modifying case details and associated business data. Administrators can create unique and dynamic workflows through Process Modelling Framework. Access to types of cases and certain actions can be controlled based on a user's role and access permissions.

2.1   Key Features

The key features of the application include the following:

- Search and filter cases based on Case IDs, search criteria, and Views.
- Investigate cases by performing an in-depth analysis using detailed information provided for each case.
- Resolve cases by taking appropriate actions on cases.
- Record the audit history of the case, including narratives provided.
- Generate reports of cases you have access to.

2.2   User Roles and Privileges

You can perform activities associated with your user group throughout the functional areas in the application. For more information about which actions can be performed by your user role, see User Roles in Case Investigation.

2.2.1   Security within the Application

Security layers control how you interact with the application. Users may only access cases that are mapped to their user group. The following table describes the security layers. For more information about mapping users to user groups, see Application Security.

Table 3 describes the Security Details within the Application.

Table 3: Security Details within the Application

Security Layer Type	Controls	Description
Roles	Access to Features and Functions	User roles are used to identify which features and functions the user can access within the application. For example, Case Analysts can access and take action on cases.
Business Domains	Access to Case and Business Information	You can restrict access along operational business lines and practices, such as Retail Banking. Users can only see cases that are assigned to at least one of the business domains their user group is mapped to. For more information about Business Domains, see Configuring Business Domains.

Table 3: Security Details within the Application

Security Layer Type	Controls	Description
Jurisdictions	Access to Case Information	You can restrict access using geographic locations and legal boundaries. Users can only see cases that belong to the jurisdiction their user group is mapped to. For more information about Jurisdictions, see Configuring Jurisdictions.
Case Type	Access to Cases	You can restrict access to specific types of cases. To view a case, users must be mapped to a user group which has access to view the specific Case Type assigned to the case. For more information about case types, see Configuring Case Types.

3   Getting Started

This section provides step-by-step instructions to login to the application.

3.1   Accessing the Application

To access the application, follow these steps:

1. Enter the URL in the web browser.

   The **Oracle Cloud** login page is displayed.

2. Enter your **User ID** and **Password**.

3. Click **Sign In**. The **Applications** landing page is displayed.

4. The **Navigation List** displays the list of modules. Click **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service**. The menu options are displayed.

5. Click **Case Management** then click **Case Investigation**.

3.2   Oracle Cloud Service Home Page

The Cloud Service home page includes the following main menu icons. The following main menu items are displayed in the Home page.

Table 4: Main Menu Items

Icon	Description
☰	Displays the menu items in the home page.
⊞	Displays the list of applications that are accessible to the user based on the assigned roles and privileges.
👤⚙	Opens Admin Console Page.
⌂	Navigates to the Home page.
🔔 18	Displays the notification message alerts. The number in the icon represents the number of unread messages. For more information about notification messages, refer About Notifications.
👤	Displays user profile preferences and About the application pages. You can also sign out from the utility.
⚇	Displays Tenant details.

3.3　About Notifications

Notification services generates an alert message which displays on the Home page.

Click ![bell icon] (Notification Services), to view the message alerts.

- Click **More info**, to view the complete message.
- The message background is changed to white after the message is read.
- Click **Mark All as Read** to move the messages to Read status without opening the messages.
- Click **Dismiss** to delete an alert
- Read messages will be deleted automatically, after 7 days.

    The administrator can modify the auto delete duration in the Admin Console > Notification Configuration section. It can be set from 1 - 999. By default the duration is set to 7 days.

The messages are categorized based on the following priorities:

Table 5: Flag and its Priority

Flag Icon	Description
	Priority 1
	Priority 2
	Priority 3

4   Searching Cases

This section describes the multiple ways available to search cases and select one or multiple cases for investigation.

4.1   About Case Search and List

The Case Search and List page displays as a tab with a list of all open cases and a tab with a list of all open cases currently assigned to the logged in user. You can select a case by clicking the corresponding Case ID link to view the details, analyze, and resolve it, based on your role privileges.

Table 6 describes the columns which display in the Case Search and List page.

Table 6: Search Cases – Columns and Descriptions

Column	Description
Case Type	A logical grouping of cases. For example, AML_DD, AML_PAT.
Case ID	The unique case identification number. This is a link to navigate to the Case Details page for further analysis.
Assignee	The user this case is currently assigned to.
Priority	The priority which has been assigned to the case. Possible options are High, Medium, and Low.
Title	The title of the case. This will be generated automatically, based on the Case Type. You can also edit the Case Title in the Case Context page.
Status	Status the case is currently in. For example, New, Investigation, Pending Review, Closed.
Reason	The reason selected for the last resolution action performed.
Creation Date	The date and time when the case was created.
Due Date	Date and time by which action must be taken on the case.
Case Tags	Any Case tags associated with this case.
Due In	The number of days remaining before action must be taken on the case.
Events Count	The number of events associated with this case.
Jurisdiction	The jurisdiction, such as geographic locations and legal boundaries, to which this case belongs.
Watchlist Full Name*	The full name of the watchlist entries matched in the case.
Watchlist Aliases*	Aliases of the watchlist entries matched in the case.

* – Only applicable to CS cases

Click the Case ID link to view details of the selected case or select one or multiple cases to take action. When you return to the Case Search and List page after viewing a case or cases, any tabs you have opened, search criteria you have applied, or pagination settings are retained.

NOTE	If the selected case is locked, that is, another user has currently accessed the same case, a warning message is displayed. For more information, see Investigating Cases.

4.1.1 Notifications

Notifications alert you when specific actions are taken, either by the system or another user, and direct you to additional information.

- Notifications are generated in the following situations:

- When a case is assigned to you.

- When a case assigned to you is Overdue.

- When a case you are investigating has one or more customers, accounts, external entities, or transactions added by the system through correlation.

- If events are added through correlation, but no new customers, accounts, external entities, or transactions have been added, a notification is not generated.

To view your notifications, click the Notification icon in the Case Search and List page. Your notifications will display with the most recent notification at the top of the list.

- Click **More Info** to view the complete notification message.

- Click **Dismiss** to close the notification.

- Click the Case ID in the notification to navigate to the relevant case and view the complete details of the change.

Notifications that have been read will be deleted after 7 days by default. System administrators can configure the deletion period to meet your requirements.

4.1.2 Sorting Case Search and List

To sort the Case List, follow these steps:

1. On the Case Search and List page, select a column (for example, Case ID, Case Type, Priority, Status, and so on).

2. Sort in ascending or descending order by clicking the up arrow or down arrow buttons respectively.On the Search Results page, select an option (Created Date, Priority, Due Date, Case Type, Status) from the **Sort By** drop-down list.

NOTE	By default, the Search Results are sorted by **Due Date**, **Priority**, and **Case ID**.

4.1.3 Export Case Search and List

You can export the cases which display in the Case Search and List page to use outside of the system.

To export the Case List, follow these steps:

1. On the Case Search and List page, select the export format (XLSX, CSV) from the Export drop-down list.

2. The file downloads the list in the format you have specified.

   The exported file name is "CaseResults_YYYY_MM_DD_HH_MM" where the time stamp refers to your local system time. For example, CaseResults_2020_03_25_15_45.csv.

NOTE	By default, only 10,000 records may be exported. If your search results exceed 10,000 cases, a message displays. Click Yes to proceed with exporting the first 10,000 records. Click No to cancel the export.
	Administrators can use Case System Parameters to configure the number of records which can be exported.

4.2 Searching Cases

This section describes different ways to search cases and tells how to filter cases based on your search criteria.

You can filter cases by:

- Using Case List Views
- Using Smart Search
- Using Advanced Case Search

4.2.1 Using Case List Views

You can create and save one or more customized case lists, or views, to display only those cases which meet your defined criteria. This helps investigators save time by viewing only cases which meet specific criteria, such as closed cases, cases assigned to a specific assignee, and so on.

The custom case list view displays in the Case Search and List page. You can return to this view after you have accessed a case from it or logged out of the application, or you can select to view a different custom case list view. You can also choose which case list view should display as the default view of your Case Search and List page.

The following sections describe how to use case list views:

- Create Case List Views
- Manage Case List Views

4.2.1.1 Create Case List Views

To create a new case list view, follow these steps:

1. In the Case Search and List page, click **Create View** . The Create View pop-up window displays.

2. From the Available Columns list, select the columns you want to display for cases in this case list.

   Click **Select Column** to move these columns to the Selected Columns list.

3. Click **Nex**t.

4. Select the filter criteria you want the new case list view to consider.

Table 7 describes the filter criteria you can select.

Table 7: Case List View Columns and Descriptions

Field	Description
Case ID	Enter one or more unique case IDs you want to search. For multiple case IDs, separate them with a comma. Ensure that you do not enter a space after the comma. Case IDs are not case-sensitive. This overrides all other filter criteria. Example: CA660, ca671
Created From	Use the calendar to specify a date and time on or after which the case was created. For example: Select 08/15/19 to search for cases created on or after August 15, 2019. You can also use this along with the **Created To** filter to search for cases created within a date range.
Created To	Use the calendar to specify a date and time up to which case was created. For example: Select 12/06/19 to search for cases created up to and including December 6, 2019. You can also use this in conjunction with the **Created From** filter to search for cases created within a date range.
Age	Use this option to specify a case's age in number of days. For example, if you want to search a case not older than two days, use the "<" operator followed by 2 using the up/down arrows. A case's age is calculated as the number of calendar days between its date of creation and the current date. Cases stop aging when they are closed.
Case Class	A class is a grouping of case types. For example: AML is a class consisting of types AML_DD, AML_PAT, AML_SURV, and so on. Select the case class to narrow your search to include only cases associated with the selected class.
Case Type	A logical grouping of cases. For example: AML_DD, AML_PAT, and so on. Select the case type to narrow your search to include only cases of the selected type.
Case Tag	The case tags given to the case. Select case tags to narrow your search to include only cases with the selected case tag.
Status	The current status of the case. Select the case status to narrow your search to include only cases currently in the selected case status.
Reason	Search cases based on the reason selected for the last resolution action performed. For example: False positive, or Factual error.
Title	Search cases based on case title by enter a few letters of the case's title (case-sensitive). For example: if you type AML, you will find cases with titles AML, AML8, AML_Events_Processing_Rule, and so on in the Case Search and List.

Table 7: Case List View Columns and Descriptions

Field	Description
Jurisdiction	Search cases that belong to a certain business jurisdiction.
	The drop-down list contains only jurisdictions which you are authorized to view.
Business Domain	Search cases that belong to a certain business domain.
	For example: EMP, GEN, and INST.
	The drop-down list contains only business domains which you are authorized to view.
Entity Type	Search cases based on one or more entity type(s).
	When the entity type is specified, you must enter a value in the Entity ID or Entity Name field.
Entity ID	Used in conjunction with Entity Type.
	When the entity type is specified, you must enter a value in the Entity ID.
Entity Name	Search cases by the entity name associated with a case. When the Entity Type is specified, you must enter a value for Entity Name.
Case Action	Select one or more Case Actions to search for cases, which are marked for the specified action to be taken. This list is updated based on the Action Type you select.
Last Action	Used in conjunction with Case Action. Search for cases where the selected Case Action is the last action recorded on the case.
	For example: If you selected Clear Due Date as the Case Action and Yes as the Last Action, only cases for which the last Case Action was to clear the due date are listed.
Action From	Used in conjunction with Case Action. Search for cases on which the Case Action is recorded within the time range specified in the Action From and Action To filters.
	For example: If you select Case Accessed as the Case Action and 12/01/19 as the Action From date, all cases on which the action Case Accessed is recorded from and including December 1st are listed.
	You can use Action From and Action To date fields to specify a date and time range within which a selected action was taken.
Action To	Used in conjunction with Case Action. Search for cases on which the Case Action is recorded within the time range specified in the Action From and Action To filters.
	For example: If you selected Case Accessed as the Case Action and 12/01/19 as the Action To date, all cases accessed up to but not including December 1st are listed.
	You can use Action From and Action To date fields to specify a date and time range within which a selected action was taken.
	For example: If you selected Case Accessed and specify 12/01/19 and 12/06/19 as the Action From and To dates, respectively; all cases accessed between Dec 1st and Dec 6th are listed.
Priority	Select the priority of the case (High, Medium, or Low) from the drop-down to search based on the case's priority.
Due Date From	Select the date and time using the calendar to filter the Case List by the past date before the action should be taken on the case.
Due Date To	Select the date and time using the calendar to filter the Case List up to the date before the action should be taken on the case.

Table 7: Case List View Columns and Descriptions

Field	Description
Due In	The number of days remaining before action must be taken on the case.
	Select from Equals, Greater Than, or Less Than, and select the number of days using the arrows. The filter will display "Due in <operator> <number of days> Days". For example, "Due In Less Than 1 Day".
Closed From	Search cases closed on or after the specified date and time.
	You can also use this in conjunction with Closed To date filter to search cases closed within a date range.
Closed To	Search cases closed up to including the specified date and time.
	You can also use this in conjunction with Closed From date filter to search cases closed within a date range.
Event Type	Search cases based on the selected event type.
	For example: AML or CS_EDD.
Scenario	Use one or more scenario options to filter and narrow your search based on the selected scenarios associated with the case.
Assignee	Search cases by assigned user.
	For example: if you select CM Analyst as the Assignee, all cases assigned to the CM Analyst are listed.
	You can select multiple assignees to search using multiple-choice selections.
Comments	Search for cases based on comments provided on the case.
Report ID	Search cases by the Report ID for a report the case is associated with.
Report Name	Search cases by the name of the report the case is associated with.
Report Status	Search cases by the status of the report the case is associated with.
Watchlist Full Name*	The full name of the watchlist entries matched in the case.
Watchlist Aliases*	Aliases of the watchlist entries matched in the case.
Message Type	Transaction Message type code.
Amount	Amount in the transaction message.
Message	ReferenceMessage Reference in the transaction message.
Transaction Reference	Transaction Reference in the transaction message.

* - Only applicable to CS cases

5. Click **Next**.

6. Enter the following information into the appropriate fields:

   ▪ Enter a unique name for this view in the View Name field. This field is mandatory.

   ▪ Enter the number of records you wish to display for each page in the view. This field is mandatory.

   ▪ Enter a brief description for this view. This field is mandatory.

- Select whether or not you want this view to be the default view using the **Set as default** check box.

7. Click **Save**. The following message displays: *View saved successfully*. The case list view displays in the Case Search and List page with the appropriate search results.

NOTE	Only 10 unique custom case list views can be saved for a user. If you attempt to create a view and 10 views already exist, the following message displays: You have already saved 10 customized views. Please delete one or more existing views and try again.

4.2.1.2   Manage Case List Views

You can view and manage all custom case list views you have created through the View Manager.

- To select which custom case list view you wish to display, click All Views and select a view from the list.

- To manage all custom case list views, click All Views and then click View All. The View Manager displays, allowing you to take action on the custom views.

In the View Manager list, select the menu ⬡ associated with the view you want to manage.

- Select **Set as Default** to make this case list view the default which appears on your Case List and Search page.

- Select **Rename** to rename the case list view.

- Select **Delete** to delete the case list view.

Click **Save**. Your changes will not be made until you have clicked **Save** from the View Manager.

4.2.2   Using Smart Search

Smart Search is the quickest way to locate cases based on criteria you define. You can use a combination search criteria to quickly find the case(s).

To search cases using Smart Search, follow these steps:

1. Click the **Search...** field. The list of available search filters displays.

2. Select a search filter criteria, such as Case ID or Priority, from the list. If needed, you can further define the filters using the options that display.

3. Enter the value you want to search by in the Value field.

4. Click **OK** ☑ to accept the search filter criteria as entered. The criteria displays in the **Search...** field.

    - You can edit the filter by clicking it in the **Search...** field.

    - You can remove the filter by clicking **Remove** ⊠ in the **Search...** field.

5. Continue adding search filter criteria until you have defined your search.

6. Click **Search** 🔍 or press the Enter key on the keyboard. The **Search Results** tab displays the list of Cases.

7. Click **Reset** 🔘 to reset all search filters.

4.2.3 Using Advanced Case Search

Advanced Case Search is a powerful option to search and narrow down the Case Search and List based on a host of search criteria. You can use a combination of these search criteria to quickly find the case(s). If you don't enter any value in any search field, it is equivalent to selecting all the criteria.

To search cases using Advanced Case Search, follow these steps:

1. In the Case Search and List page, click **Advanced Case Search** . The Advanced Search page opens and displays the search criteria.

2. Enter one or multiple search criteria as described in Table 8 .

Table 8: Advanced Case Search – Fields and Descriptions

Field	Description
Case ID	Enter one or more unique case IDs you want to search. For multiple case IDs, separate them with a comma. Ensure that you do not enter a space after the comma. Case IDs are not case-sensitive. This overrides all other filter criteria. Example: CA660, ca671
Created From	Use calendar to specify a date and time on or after which the case was created. For example: Select 08/15/19 to search for cases created on or after August 15, 2019. You can also use this along with the **Created To** filter to search for cases created within a date range.
Created To	Use calendar to specify a date and time up to which case was created. For example: Select 12/06/19 to search for cases created up to and including December 6, 2019. You can also use this in conjunction with the **Created From** filter to search for cases created within a date range.
Age	Use this option to specify a case's age in number of days. For example, if you want to search a case not older than two days, use the "<" operator followed by 2 using the up/down arrows. A case's age is calculated as the number of calendar days between its date of creation and the current date. Cases stop aging when they are closed.
Case Class	A class is a grouping of case types. For example: AML is a class consisting of types AML_DD, AML_PAT, AML_SURV, and so on. Select the case class to narrow your search to include only cases associated with the selected class.
Case Type	A logical grouping of cases. For example: AML_DD, AML_PAT, and so on. Select the case type to narrow your search to include only cases of the selected type.

Table 8: Advanced Case Search – Fields and Descriptions

Field	Description
Status	The current status of the case. Select the case status to narrow your search to include only cases currently in the selected case status.
Reason	Search cases based on the reason selected for the last resolution action performed. For example: False positive, or Factual error.
Title	Search cases based on case title by enter a few letters of the case's title (case-sensitive). For example: if you type AML, you will find cases with titles AML, AML8, AML_Events_Processing_Rule, and so on in the Case Search and List.
Jurisdiction	Search cases that belong to a certain business jurisdiction. The drop-down list contains only jurisdictions which you are authorized to view.
Business Domain	Search cases that belong to a certain business domain. For example: EMP, GEN, and INST. The drop-down list contains only business domains which you are authorized to view.
Entity Type	Search cases based on one or more entity type(s). When the entity type is specified, you must enter a value in the Entity ID or Entity Name field.
Entity ID	Used in conjunction with Entity Type. When the entity type is specified, you must enter a value in the Entity ID.
Entity Name	Search cases by the entity name associated with a case. When the Entity Type is specified, you must enter a value for Entity Name.
Case Action	Select one or more Case Actions to search for cases, which are marked for the specified action to be taken. This list is updated based on the Action Type you select.
Last Action	Used in conjunction with Case Action. Search for cases where the selected Case Action is the last action recorded on the case. For example: If you selected Clear Due Date as the Case Action and Yes as the Last Action, only cases for which the last Case Action was to clear the due date are listed.
Action From	Used in conjunction with Case Action. Search for cases on which the Case Action is recorded within the time range specified in the Action From and Action To filters. For example: If you select Case Accessed as the Case Action and 12/01/19 as the Action From date, all cases on which the action Case Accessed is recorded from and including December 1st are listed. You can use Action From and Action To date fields to specify a date and time range within which a selected action was taken.

Table 8: Advanced Case Search – Fields and Descriptions

Field	Description
Action To	Used in conjunction with Case Action. Search for cases on which the Case Action is recorded within the time range specified in the Action From and Action To filters. For example: If you selected Case Accessed as the Case Action and 12/01/19 as the Action To date, all cases accessed up to but not including December 1st are listed. You can use Action From and Action To date fields to specify a date and time range within which a selected action was taken. For example: If you selected Case Accessed and specify 12/01/19 and 12/06/19 as the Action From and To dates, respectively; all cases accessed between Dec 1st and Dec 6th are listed.
Priority	Select the priority of the case (High, Medium, or Low) from the drop-down to search based on the case's priority.
Due Date From	Select the date and time using the calendar to filter the Case List by the past date before the action should be taken on the case.
Due Date To	Select the date and time using the calendar to filter the Case List up to the date before the action should be taken on the case.
Due In	The number of days remaining before action must be taken on the case.
Closed From	Search cases closed on or after the specified date and time. You can also use this in conjunction with Closed To date filter to search cases closed within a date range.
Closed To	Search cases closed up to including the specified date and time. You can also use this in conjunction with Closed From date filter to search cases closed within a date range.
Event Type	Search cases based on the selected event type. For example: AML or CS_EDD.
Scenario	Use one or more scenario options to filter and narrow your search based on the selected scenarios associated with the case.
Assignee	Search cases by assigned user. For example: if you select CM Analyst as the Assignee, all cases assigned to the CM Analyst are listed. You can select multiple assignees to search using multiple-choice selections.
Comments	Search for cases based on comments provided on the case.
Report ID	Search cases by the Report ID for a report the case is associated with.
Report Name	Search cases by the name of the report the case is associated with.
Report Status	Search cases by the status of the report the case is associated with.

3. Click **Search**. The cases matching your search criteria display in a new **Search Results** tab**.**

4. To carry out a new search, click **Reset Filter** and add or remove search criteria as desired.

5   Investigating Cases

This section explains how to investigate cases and determine the actions to resolve them.

Topics:

- About Investigating Cases
- Case Details
- Dashboard
- Events
- Entities
- Transactions
- Relationship
- Attachment
- Risk Assessment
- Prospect

5.1   About Investigating Cases

A case investigation is carried out using the Case Details page. This page provides complete details of the selected case and allows you to take appropriate actions.

5.2   Case Details

The Case Details section provides detailed information about the case. The sections which display will be based on the type of case you are viewing, for example, AML, CS, or KYC.

You can view high-level case information in the Case Information section at the top of the page. Depending on your role, you can also modify case-related information.

You have options to view and filter the required information.

Topics:

- Access Case Details
- Case Information
- Export Case Report
- Primary Entity
- Case Summary

5.2.1   Access Case Details

To access the Case Details, follow these steps:

On the Case Search and List page, click a Case ID link to open the Case Details in a new tab. Clicking more than one Case ID will open multiple Case Details tabs.

If the case is in New status and is not assigned to any owner, the following message displays: *Do you want to assign the case to yourself? Click YES to assign the case. Click NO to proceed in Read-Only mode without assigning the case.*

The Case Details include the Case Information and Case Summary sections, as well as the following tabs:

- Dashboard
- Events
- Entities
    - Account
    - Customer
    - External Entity
- Transactions
- Relationship
- Attachment
- Risk Assessment
- Prospect

| NOTE | If your firm has enabled General Data Protection Regulation (GDPR) redaction, Personal Identifying Information (PII) will display in AML cases as XXXX in the fields listed in the following table. If your user role has been mapped to the Unredacted data function code, you may view this PII unredacted. |

Table 9 describes the Redacted PII Fields in AML Cases.

Table 9: Redacted PII Fields in AML Cases

Page	Fields Redacted
Customer List	- Customer ID - Customer Name - Customer Name - Customer ID

Table 9: Redacted PII Fields in AML Cases

Page	Fields Redacted
Customer Details	• Primary Address • Primary Contact Number • Primary Email • First Name • Middle Name • Last Name • Marital Status • Date of Birth • Credit Rating • Credit Source • Employer • Employment Status • Gender • Other Address • Other Contact Numbers • Other Emails
Customer Account Details	• Account Name • Account ID
Account List	• Account Name • Account ID
Account Details	• Account Name • Account ID • Owner ID • Primary Address • Primary Contact Number • Primary Email • Other Address • Other Contact Numbers • Other Email

5.2.2   Case Information

Use the Case Information section to view important details of the selected case.

Table 10 describes the fields which display in the Case Information section.

Table 10: Fields in Case Details and their Descriptions

Field	Description
Priority Indicator	This icon displays the case priority, as L (Low), M (Medium), and H (High). This is used to quickly determine which cases to work first.

Table 10: Fields in Case Details and their Descriptions

Field	Description
Title	The title for the case. This can be automatically generated or manually entered.
Type	The type of case, such as AML, KYC, and so on.
Priority	The case priority level.
Creation Date	The date and time on which this case was created.
Due Date	The deadline to complete resolution action on this case.
Assignee	The current owner of this case. If the case is currently not assigned and you would like to assume ownership of the case, you can click **Assign to me.** The following message displays: *Assignee updated successfully.*
Status	The current status of this case.
Comment	The narrative comments provided for the last resolution action performed. This helps you to understand why that action was taken.
Reason	The reason selected for the last resolution action performed.
Case Summary	A brief description of the case that gives high-level insight on the subject matter of the case.
Case Tags	Any Case tags associated with this case
Primary Entity Type	The entity type of the primary entity of the case, such as Customer or External Entity.
ID	The ID of the primary entity of the case.
Name	The name of the primary entity of the case.
Jurisdiction	The jurisdiction to which the case belongs.
Business Domain	The business domain to which the case belongs.
Batch Type	The type of batch associated with the risk assessment. The following options may display: ● Deployment Initiation (DI) ● Periodic Review ● New Account Review ● Accelerated Review (ARR) This field displays only for KYC Batch Cases.
KYC Risk Score	The KYC Risk Score originally associated with this case. This field displays only for KYC Batch Cases.
Overridden KYC Risk Score	The KYC Risk Score most recently associated with this case. This field displays only for KYC Batch Cases.
Next Review Date	The date on which this customer should next be considered for risk assessment review This field displays only for KYC Batch Cases.

Table 10: Fields in Case Details and their Descriptions

Field	Description
Overridden Next Review Date	The date on which this customer was previously scheduled to be considered for risk assessment review. This field displays only for KYC Batch Cases.
Focus Applicant	The name of the focus prospect. This field displays only for KYC Onboarding Cases.
Application ID	Displays the unique ID for the application which is a part of the onboarding JSON. This field displays only for KYC Onboarding Cases.
Risk Category	Displays the category of the risk assessment. For example, Low, Medium, High. This field displays for both KYC Onboarding and KYC Batch Cases.
Overridden Risk Category	Displays the category of the risk assessment which is calculated based on Overriden Risk Score. This field displays for both KYC Onboarding and KYC Batch Cases.
Risk Assessment Score	Displays the risk assessment score for this prospect. This field displays only for KYC Onboarding Cases.

5.2.2.1 Update Case Information

Based on your role, you can also update information in some fields.

To update the case information, follow these steps:

1. In the Case Information section of a selected case, click the Case Details icon ⌄. The case details display.

2. Update the case information as required. You can only modify the case's **Priority, Title, Due Date, Assignee**, and **Case Summary**. For KYC Cases, you can only modify the case's **Priority, Title, Due Date, Assignee**, **Override KYC Risk Score**, and **Override Next Review Date**. The remaining details are view-only.

> **NOTE**   If you are not the Assignee of the case, you can only edit the Assignee field.

- Update the **Case Priority** by selecting the new priority from the drop-down list.

- Update the **Case Title** by entering text into the text box. If the case title contains more than 150 characters, an ellipsis **(...)** will display in the Case Information section.

- Update the **Due Date** by entering a date into the text box or by selecting a date from the calendar.

- Update the **Case Assignee** by selecting a user from the drop-down list.

- Update the **Case Tags** associated with this case by selecting an existing case tag from the lists.

  — The Recommended Tags list shows tags which are recommended based on case attributes, in order of confidence score.

  — The Available Tags list shows all created tags available.

- — You can also create a new case tag by entering the name of the case tag you wish to create in the Case Tags field. You can enter up to 20 characters.

    - — You can add up to 5 case tags per case.

    - — You can remove a case tag by clicking **Remove** ⊠.

  - Update the **Primary Entity** as required.

  - Update the **Case Summary** by entering text into the text box. You can enter up to 4000 characters.

  - Update the **Overriden KYC Risk Score** as required. Click the help icon 🛈 for the score ranges of the risk categories configured for that particular customer.

  - Update the **Overriden Next Review Date** as required.

3. Click **Save** to save your updates. The updated information displays in the Case Information section.

  - Click **Cancel** to close the Case Details without your updates. The following message displays: *Unsaved data will be lost. Do you want to continue?*

5.2.3 Export Case Report

You can export the basic information of a case as a PDF report. This allows you to share initial query information to others, such as regulators and auditors, without requiring system access.

To export case information, follow these steps:

1. In the Case Search and List page, select the check box associated with the case you want to export the report of.

2. Click Export Case Report 📄. The report generates as a PDF and downloads to your machine.

5.2.4 Primary Entity

The Primary Entity section provides details about the primary subject of the investigation (customer, prospect, or external entity). For any case created by the system, the Primary Entity will be automatically provided based on the events associated with the case. You can manually specify the Primary Entity as needed.

To update the Primary Entity, follow these steps:

1. In the Case Information section of a selected case, click the Case Details icon 🔽. The case details display.

2. Select the **Primary Entity Type**, such as Customer, Prospect, Candidate, or External Entity, from the drop-down list.

3. Select either the **Entity ID** or **Name** from the drop-down list.

  - Select the **Entity ID** for the primary entity from the ID drop-down list. This list contains the IDs of entities associated with the case. Selecting the Entity ID automatically populates the Name.

- Select the **Name** of the primary entity from the drop-down list. This list contains the names of entities associated with the case. Selecting the Name automatically populates the Entity ID.

4. The Jurisdiction and Business Domain the entity is associated with will be automatically populated based on the selections above.

5. Click **Save** to save your updates. The updated information displays in the Primary Entity section.

- Click **Cancel** to close the Case Details without your updates. The following message displays: *Unsaved data will be lost. Do you want to continue?*

5.2.5 Case Summary

The Case Summary section provides a brief description of the case that gives a high-level insight on the subject matter of the case. You can update the Case Summary by entering text into the text box. You can enter up to 4000 characters.

5.3 Dashboard

The Dashboard tab provides a summary of information about the case.

For AML cases, this tab contains the following sections:

5.3.1 Smart Search

The Smart Search bar allows you to filter the transaction data which displays in the dashboard. This helps investigators to quickly find the suspicious transactions they are investigating.

To filter transactions in the Dashboard using Smart Search, follow these steps:

1. Click the **Search** field. The list of available search filters displays.

2. Select a search filter criteria, such as Case ID or Priority, from the list. If needed, you can further define the filters using the options that display.

3. Enter the value you want to search by in the Value field.

4. Click **OK** ☑ to accept the search filter criteria as entered. The criteria displays in the **Search...** field.

   - You can edit the filter by clicking it in the **Search...** field.

   - You can remove the filter by clicking **Remove** ☒ in the **Search...** field.

5. Continue adding search filter criteria until you have defined your search.

6. Click **Search** 🔍 or press the Enter key on the keyboard. The **Search Results** tab displays the list of Cases.

7. Click **Reset** ↻ to reset all search filters.

- Smart Search
- Case Network
- Transactions

- Smart Search

For KYC cases, this tab contains the following sections:

- KYC Risk Score
- Network Diagram
- Customer/Interested Party

Additional case information is provided under the appropriate tabs.

- Events
- Entities
- Transactions
- Relationship
- Attachment
- Risk Assessment
- Prospect

5.3.2   Smart Search

The Smart Search bar allows you to filter the transaction data which displays in the dashboard. This helps investigators to quickly find the suspicious transactions they are investigating.

To filter transactions in the Dashboard using Smart Search, follow these steps:

1. Click the **Search** field. The list of available search filters displays.

2. Select a search filter criteria, such as Case ID or Priority, from the list. If needed, you can further define the filters using the options that display.

3. Enter the value you want to search by in the Value field.

4. Click **OK** ☑ to accept the search filter criteria as entered. The criteria displays in the **Search...** field.

   - You can edit the filter by clicking it in the **Search...** field.

   - You can remove the filter by clicking **Remove** ☒ in the **Search...** field.

5. Continue adding search filter criteria until you have defined your search.

6. Click **Search** 🔍 or press the Enter key on the keyboard. The **Search Results** tab displays the list of Cases.

7. Click **Reset** ⟳ to reset all search filters.

5.3.3   Transactions List

This section provides information about the transactions and scenarios associated with the case.

If the Primary Entity of the case is a customer, you can view all transactions associated with the case which have occurred within the last 90 days, or you can select to view only the evented transactions.

If the Primary Entity of the case is an external entity, you can view only the evented transactions between the customers associated with the case and the primary entity of the case.

The scenarios which triggered the case and the number of transactions associated with each scenario are highlighted above the Transactions list. Evented transactions can be filtered by clicking the scenario which triggered the event. Click the scenario name again to remove the filter. Only one scenario can be selected.

Click a Transaction ID to view the details of the transaction.

5.3.4   Case Network

This section displays a graphical representation of the network consisting of customers, accounts, and external entities involved in the selected case.

- Customers, Accounts and External Entities are displayed as nodes.
- The relationships which occur between these nodes display as links.
- Movement of funds between these nodes display as dotted links.
- Backoffice transactions are not displayed in this graph.

You can view the relationship between customers, external entities and accounts using the following steps:

1. In the **Dashboard** of a selected case, navigate to the **Case Network** graph.

2. The Case Network graph displays the relation between customers and external entities. Click the graphical line between the required customer and their external entity to view the **Transactions Details** window. The details, such as **Total Amount**, **Number of Transactions**, **Type of Transactions**, and **Transaction Dates** are displayed.

3. The graph displays the relation between transactions and customers and external entities, with the total value for each day's transactions displayed. Hover over the transaction to view transaction details, such as the Transaction ID, Transaction Type, Date on which the transaction occurred, and so on.

   - Scroll or zoom out to view fewer details. The network will display at the scale selected.
   - Scroll or zoom in to view more details. The network will display at the scale selected.
   - Click and drag to move to other sections of the graph.

> **NOTE**
>
> - Click Reset ⟳ to clear the filters
>
> - Click **Expand** 🖉 to open the graph in a new window.

5.3.5   Transactions Chart

This section displays a graphical representation of all the transactions for all the counterparties involved in the selected case within the defined time period. This helps investigators identify patterns of expected customer activity.

You can view the transactions using the following steps:

1. In the **Dashboard** of a selected case, navigate to the **Transactions** diagram by selecting **Transactions** from the **Case Network** drop-down list.

2. You can filter which transactions display in the chart.

- Select the types of **Transactions** you want to view in the graph. All Transaction Types are selected by default.

- Select the **Scenario** associated with the evented transactions from the drop-down list.

- Select the **Customer** you want to view the Transactions of from the drop-down list. The graph will display transactions from all accounts of the customer.

- Select the **Accounts** you want to view Transactions for from the drop-down list. All Accounts are selected by default.

- Select the date range for these transactions using the Date To and Date From calendar options. A date range of greater than 36 months is not allowed. The default date range is 36 months from the current date.

3. You can navigate the chart in the following ways:

- Scroll or zoom out to view a longer date range. You can also resize the window in the overview bar. The chart will display at the scale selected.

- Scroll or zoom in to view a shorter date range. You can also resize the window in the overview bar. The chart will display at the scale selected.

- Click and drag to move to other sections of the graph.

- The overview bar provides the trend of the transactions over the defined time period. Resizing the window in this bar displays the Transactions chart in the time range selected.

4. The graph displays the relation between transactions and customers and external entities, with the total value for each day's transactions displayed. Hover over the transaction to view transaction details, such as the Transaction ID, Value of the transaction, Transaction Type, Date on which the transaction occurred, and so on.

> **NOTE**
>
> - Click Reset [icon] to clear the filters
>
> - Click **Expand** [icon] to open the graph in a new window.

5.3.6 KYC Risk Score

> **ATTENTION**   This section will only display for KYC Batch Case Types.

This section displays a graphical representation of the risk scores for the risk assessments which have been conducted for customers involved in the selected KYC case within the defined time period.

You can view the risk scores using the following steps:

1. In the **Dashboard** of a selected case, navigate to the **KYC Risk Score** diagram by selecting **KYC Risk Score** from the drop-down list.

2. You can filter which risk assessments will display in the chart.

- Select the **Customer** or external entities you want to view in the graph from the drop-down list.

- Select the **Review** you want to view the risk assessments of from the drop-down list. You can choose from the following options:

— 1 Year Review

— 3 Years Review

— 5 Years Review

- Scroll or zoom out to view a longer date range. You can also resize the window in the over-view bar. The chart will display at the scale selected.

- Scroll or zoom in to view a shorter date range. You can also resize the window in the overview bar. The chart will display at the scale selected.

- Click and drag to move to other sections of the graph.

3. The graph displays the risk assessments which have been conducted for the customer or external entity, with the risk score for each risk assessment displayed. Hover over the risk assessment to view details, such as the type of risk assessment, the risk score and the date the risk assessment was performed.

> **NOTE**
>
> - Click Reset [⟳] to clear the filters
>
> - Click **Expand** [✎] to open the graph in a new window.

5.3.7   Network Diagram

> **ATTENTION**   This section will only display for KYC Batch Case Types.

This section displays a graphical representation of the network consisting of customers and interested parties involved in the selected KYC case.

- Customers and Interested Parties are displayed as nodes.

- The relationships which occur between these nodes display as links.

You can view the relationship between customers and interested parties using the following steps:

1. In the **Dashboard** of a selected KYC case, navigate to the **Network Diagram** graph by selecting Network Diagram from the drop-down list.

2. The Network Diagram graph displays the relation between customers and interested parties. Click the link between the customer and the interested party to view the **Relationship Type** details. Click and drag to move to other sections of the graph.

5.3.8   Customer/Interested Party

> **ATTENTION**   This section will only display for KYC Batch Case Types.

This section displays the details of customers and interested parties involved in this case and their relationship.

Click on a Customer/Party's ID to view the details about the selected party.

5.4   Events

Use the Events tab to view complete details of events associated with the selected case.

Topics:

- Events List
- Event Details

5.4.1   Events List

The Event list section allows you to view the list of events which were the basis for creating the case. You can sort the list of events by selecting the name of the column you wish to sort by. You can also export the list of events to Excel or CSV format.

Click an Event ID in the Event List to view more details about the event.

Table 11 describes the fields which display at the top of the Event Details page.

Table 11: Fields in Event List Page and their Descriptions

Field	Description
Event ID	Displays the ID for the event.
Event Type	Displays the event type. For example, AML, KYC, and so on.
Focus Name	Displays the name of the focused customer or account for the event, such as the name of the customer or external entity.
Focus Type	Displays what the focus type is for this event.
Scenario Name	Displays the name of the scenario used to create the event.
Threshold Details	Displays the threshold details. Under this column, click the View button to view threshold names and their values. **NOTE:** This column is shown only for Transaction Monitoring (TM) Events. By default, This can only be viewed by the CM Supervisor role users. However, the Admin can grant permission to the other user roles if required via Roles-Function Mapping.
Jurisdiction	Displays the jurisdiction to which the event belongs.
Business Domain	Displays the business domain to which the event belongs.
Source System	Displays the source system of the event.
Score	Displays the score of the event.
Created Date	Displays the date this event was created.
Promotion Date	Displays the date this event was promoted.

5.4.2　Event Details

The Event Details page displays a complete description of the events associated with the selected case. Events can be focused on customers, accounts, or external entities. This section also displays the details of the scenario which triggered this event.

Click an Event ID in the Event List to view more details about the event.

Click on the Export icon in the Event Details page to export the event details in PDF format (Only applicable to CS cases).

For the re-alerts, the changed attributes are highlighted inside a red box.

Table 12 describes the fields which display at the top of the Event Details page.

Table 12:　Fields in Event Details Page and their Descriptions

Field	Description
Event ID	Displays the ID for the event.
Event Type	Displays the event type. For example, AML, KYC, and so on.
Focus Name	Displays the name of the focused customer or account for the event, such as the name of the customer or external entity.
Focus ID	Displays the ID for the focus of the event.
Focus Type	Displays what the focus type is for this event.
Scenario Name	Displays the name of the scenario used to create the event.
Scenario Highlights	Displays the detection criteria for the behavior which triggered the event.
Created Date	Displays the date this event was created.
Jurisdiction	Displays the jurisdiction to which the event belongs.
Business Domain	Displays the business domain to which the event belongs.

The Event Details page also contains the following sections:

- Transactions List
- Event Decisions

5.4.2.1　Transactions List

The Event Details page provides a list of all transactions associated with this event. The Transactions details are displayed under multiple tabs.

- **All Transactions:** Use this tab to view details of all transactions associated with this event.
- **Funds Transfer:** Use this tab to view details of funds transfers.
- **Monetary Instrument Transaction:** Use this tab to view details of monetary instrument transactions.
- **Cash Transactions:** Use this section to view cash transactions associated with the selected transaction.
- **Backoffice Transaction:** Use this tab to view back-office transactions for the selected transaction.

   For more information about transactions, see Transactions.

5.4.2.2 Event Decisions

After reviewing the events associated with a case, you can decide whether or not the events are relevant to this case.

To set an event decision, follow these steps:

1. In the **Events** list of the **Case Details** page, select one or more check boxes associated with events and click **Set Decision.**

2. Or, you can click the **Event ID** link for the event you are setting the decision for. The Event Details page displays.

3. Select a Decision from the **Event Decision** drop-down list.

4. Enter comments to explain why you have reached this decision.

5. Click **Save** to save your decision or **Cancel** to close the window.

5.4.2.3 Add to Exemption

After reviewing the events associated with a case, you can add the case to the exemption.

To add to exemption, follow these steps:

1. In the **Events** list of the **Case Details** page, select one or more check boxes associated with events and click **Add to Exemption.** The Add to exemption configuration page is displayed.

2. Select the part of text to be added in exemption list click move ≫ icon.

3. Click **Clear** to delete the selected part of the name.

4. Select the **Expiry Date**.

5. Click **Submit for Approval** to submit the allow list name for approval or Click **Cancel** to close the window.

The exemption record is then sent to the Supervisor for approval.

5.5 Entities

The Entities tab displays information about the Involved Parties and Accounts associated with the case.

Topics:

- Involved Parties
- Customer
- External Entity
- Account

5.5.1 Involved Parties

This section displays the list of parties involved and their description in this case. This section contains the following tabs:

- Customer
- External Entity

Click on a party's name or ID to view the details about the selected party.

5.5.1.1 Specify Involvement Type

You can indicate the involvement type for a customer or external entity associated with the case based on the results of your investigation. If a regulatory report is filed for this case, having involvement types specified will reduce the amount of effort required during the reporting process.

To specify the involvement type, follow these steps:

1. Navigate to the **Dashboard** tab of the Case Details page, under **Involved Parties.**

2. In the **Customers** tab, select the check box associated with one or more customers. In the **External Entitie**s tab, select the check box associated with one or more external entities.

NOTE	Selecting multiple check boxes can be used to apply the same involvement type to all selected customers or entities.

3. Click **Specify Involvement Type**.

4. Select the **Involvement Type** from the drop-down list and enter a comment in the **Comments** box. You can choose from the following types:

   - Unknown
   - Conductor
   - Suspect
   - Victim
   - Witness
   - Other
   - Not Involved

5. Enter the reason you have selected this involvement type in the **Comments** box. This step is mandatory.

6. Click **Save**. A message *Involvement Type Set Successfully* displays. The system records the Involvement Type change in the Involvement tab of the Customer Details or Entity Details page.

   Repeat these steps to change the involvement type as needed. If you change the Involvement Type, the system updates the Involvement Type change in the Involvement tab of the Customer Details or Entity Details page.

5.5.2 Customer

Use this section to view a complete list and description of customers associated with the selected case.

Topics:

- Customer Details
- Add Customers
- Remove Customers
- Sort Customers

5.5.2.1 Customer Details

To view details about the customer associated with this case, follow these steps:

In the **Case Details** page for a selected case, click the **Customer ID** link corresponding to a customer whose details you want to view. The details of the selected customer are displayed. The Latest information for this customer displays by default. To view customer details at the time of case creation, select Cased from the drop-down list. For cases in Closed status, you can view customer details at the time of case closure by selecting Closed from the drop-down list.

Table 13 describes the fields which display at the top of the Customer Details page.

Table 13: Fields in Customer Details Page and their Descriptions

Field	Description
Customer Name	Name of the customer on whom the case is created.
Customer ID	ID for the customer on whom the case is created.
Customer Type	Customer type for this customer. The customer type can be Organization, Financial Institution, or Individual.
Last Risk- Assessment Date	Last time when Risk Assessment was done.
KYC Risk- Assessment Score	KYC Risk Assessment score when Risk Assessment was done.
Next Risk- Assessment Date	Date when the next Risk Assessment will be done.
Effective Risk	Level of effective risk associated with this customer.
Total Cases	Total number of cases associated with this customer.
SARed Cases	Number of SARed cases associated with this customer.
Open Cases	Number of open cases associated with this customer.
Date Added	Date and time the customer was added to the case.
Jurisdiction	Displays the jurisdiction to which the customer belongs.
Business Domain	Displays the business domain to which the customer belongs.
Tax ID	This customer's Tax ID.

The Customer Details page also contains the following sections:

- **Basic Detail**: This tab provides basic information pertaining to the selected customer such as name, contact information, employment status, credit rating, personal information like Date of Birth, and so on. The fields which display in this section may be different based on the customer type.

- **Risk List Membership**: This tab displays watch lists associated with the selected customer. You can view details such as the source of the data, when the customer was added or removed from the Type, List Name, Risk Score, and List Description.

- **Anticipatory Profile**: The anticipatory profile of all customers is collected at the inception of customer relationships in order to understand the sources of funds and the expected transactions for these entities. This tab displays the list of all anticipatory profiles associated with the selected customer.

- **Customer Accounts**: This tab displays the list of all accounts that are associated with the customer. This provides the details of the accounts, such as the account name, type, account open and closed date, and so on.

- **Involvement**: This tab lists the cases for which this customer is considered an Involved Party, such as a Victim, Suspect, or Witness, and provides details about the customer's involvement in the case.

- **Relationship**: This tab displays the actual graphical representation of the customer's relationship network, such as any accounts held by this customer, any other customers who share these accounts, the customer's address, and any banks or external entities considered related to this customer. The information displayed in this network is determined by your user role. Hovering over a node displays additional information.

- **Quantifind Data**: This tab displays Quantifind information which allows users to retrieve and view Quanitifind Risk Cards. Only users mapped to the QUANTIFIND_ACCESS user role have access to Quantifind results. Quantifind is a third party company and a contract with Quantifind is required to use this feature.

- **IDV Documents**: This tab displays identification and verification documents and attachments previously added to this customer.

5.5.2.2 Add Customers

Use this section to add a customer with the selected case. This is useful when an Investigator wants to add a customer or customers to a case to reflect the relationship of that customer with the selected case.

To add a new customer, follow these steps:

1. In the **Case Details** page of a selected case, navigate to the Customers tab in the Involved Parties section.

2. Click **Add Customer** [+] . The **Add Customer** window is displayed.

3. **Enter the Customer ID, Customer Type** or **Customer Name**.

   The **Customer Name** field supports wildcard and case-insensitive search.

   Customer Type drop-down list is enabled only when **Customer Name** is entered. The supported **Customer Types** are:

   - Financial Institution
   - Individual
   - Other Organization

4. Click **Search**. The list of Customers is displayed.

   Reset discards the customer data entered by you and resets the contents to their original state.

5. Select the customer (or customers) and click **Add**.

   A confirmation message is displayed. *Customer Added Successfully.* The system saves the new customer details and associates it to the current case.

   The newly added records display in the Customer list. Corresponding audit entries are also recorded in **Audit History** on the case. For more information, see Audit History.

5.5.2.3   Remove Customers

Use this section to remove an existing customer from the selected case.

To remove a customer, follow these steps:

1. In the **Case Details** page of a selected case, navigate to the Customers tab in the Involved Parties section.

2. Select the required Customer (or Customers) and click **Remove Customer** ▬.

3. Provide a reason for why you are removing the selected customer from the case.

4. Click **Yes**. A confirmation message is displayed. *Customer Removed Successfully.* The window closes and navigates you to the refreshed list of **Customers**. Corresponding audit entries are also recorded in **Audit History** on the case. For more information, see Audit History.

5.5.2.4   Sort Customers

To sort the list of customers, follow these steps:

1. In the **Customer** page, select a column (for example, Customer ID, Customer Type, and so on).

2. Sort in ascending or descending order by clicking the up arrow or down arrow buttons respectively.

5.5.3   External Entity

Use this section to view a complete list and description of external entities associated with the selected case.

Topics:

- External Entity Details

- Involvement

- Add External Entities

- Remove External Entities

- Sort External Entities

5.5.3.1   External Entity Details

To view the list of all external entities associated with this case, follow these steps:

1. In the Involved Parties section of the **Case Details** page for a selected case, select the **External Entity** tab.

2. Click either the **Entity ID** or **Entity Name** link corresponding to the external entity whose details you want to view. The details of the selected entity are displayed.

Table 14 describes the fields which display at the top of the External Entity Details page.

Table 14: Fields in External Entity Details Page and their Descriptions

Field	Description
Entity Name	Name of the external entity on whom the case is created.
Entity ID	ID for the external entity on whom the case is created. If no ID has been presented, this will remain blank.

Table 14: Fields in External Entity Details Page and their Descriptions

Field	Description
Entity Type	Entity type of this external entity.
Risk Rating	Level of risk associated with this external entity.
Date Added	Date and time the external entity was added to the case.
Addresses	Displays address information for this external entity.

5.5.3.2   Involvement

This section lists the cases for which this external entity is considered an Involved Party, such as a Victim, Suspect, or Witness, and provides details about the entity's involvement in the case.

5.5.3.3   Add External Entities

Use this section to add a new external entity to the selected case. Adding a new External Entity allows you to perform the detailed analysis of external entities associated with the case to determine case resolution.

To add a new external entity, follow these steps:

1. In the Involved Parties section of the **Case Details** page for a selected case, select the **External Entity** tab.

2. Click **Add External Entity** . The **Add External Entity** page is displayed.

3. Enter the **Entity ID, Entity Type** or **Entity Name**.

    The **Entity Name** field supports wildcard and case-insensitive search.

    Select an external entity type from the drop-down list. For example, credit card, driver license, corporate identifier, and so on.. The **Entity Type** drop-down list is enabled only when **Customer Name** is entered.

4. Click **Search**. The list of external entities is displayed.

    Reset discards the external entity data entered by you and resets the contents to their original state.

5. Select one or more entities from the search results.

6. Click **Add**. A confirmation message is displayed: *External Entity Added Successfully*. The system saves the new external entity details and associates it to the current case.

    The newly added records display in the External Entity list. Corresponding audit entries are also recorded in the **Audit History** on the case.

5.5.3.4   Remove External Entities

Use this section to remove an existing external entity from the selected case.

To remove an external entity, follow these steps:

1. In the Involved Parties section of the **Case Details** page for a selected case, select the **External Entity** tab.

2. Select the external entities you wish to remove from the case and click **Remove External Entity** .

3. Provide a reason for why you are removing the selected entity from the case.

4. Click **Yes**. A confirmation message is displayed: *External Entity Removed Successfully*. The window closes and navigates you to the refreshed list of external entities. Corresponding audit entries are also recorded in the **Audit History** on the case.

5.5.3.5 Sort External Entities

To sort external entities in the list, follow these steps:

1. On the **External Entity** page, select a column (for example, Entity ID, Entity Type, and so on).

2. Sort in ascending or descending order by clicking the up arrow or down arrow buttons respectively.

5.5.4 Account

Use this section to view the details of accounts associated with the selected case.

Topics:

- Account Details
- Add Accounts
- Remove Accounts
- Sort Accounts

5.5.4.1 Account Details

To view details of accounts, follow these steps:

In the Accounts list on the **Case Details** page for a selected case, click the **Account ID** link corresponding to the account details you want to view. The details of the selected account are displayed.

Table 15 describes the fields which display at the top of the Account Details page. The number of accounts associated with this customer displays. The Latest information for this account displays by default. To view account details at the time of case creation, select Cased from the drop-down list. For cases in Closed status, you can view account details at the time of case closure by selecting Closed from the drop-down list.

Table 15: Fields in Account Details Page and their Descriptions

Field	Description
Account Name	Displays the name for this account
Account ID	Displays the unique ID for this account.
Primary Type	Displays the primary account type for this account (for example, Savings, Retirement, and so on).
Secondary Type	Displays the secondary account type for this account.
Status	Displays the status of this account (for example, active, inactive, or closed).
Open Date	Displays the date and time on which the account was opened.
Owner ID	Displays the unique ID for the owner of the account.

Table 15: Fields in Account Details Page and their Descriptions

Field	Description
Registration	Displays the registration type. This is a client-specified form of legal ownership for the account (for example, joint tenant, individual, custodial, or corporate).
Last Activity	Displays the date and time of the last trading or transaction activity in this account.
Tenure	Displays the length of time this account has been opened.
Jurisdiction	Displays the jurisdiction to which the account belongs.
Updated On	Displays the date and time this account information was last updated.
Date Added	Date and time the account was added to the case.
Effective Risk	Level of effective risk associated with this account.
Business Risk	Level of business risk associated with this account.
List Risk	Level of risk associated with this account as determined by membership on one or more Watch Lists.
Geography Risk	Level of risk associated with this account as determined by geography.

The Account Details page also contains the following sections:

- **Basic Detail**: This tab provides basic information pertaining to the selected account such as address information, financial institution information, Tax information, and so on.

  Table 16 provides some examples of commonly displayed information:

Table 16: Commonly Displayed Fields in the Basic Details Tab

Field	Description
Primary Address	Displays the address your firm has designated as primary for this account, based on the data your firm has loaded. Other addresses linked to this account display in the Other Information area.
Primary Email	Displays the email address your firm has designated as primary for this account, based on the data your firm has loaded. Other email addresses linked to this account display in the Other Information area.
Primary Phone Number	Displays the phone number your firm has designated as primary for this account, based on the data your firm has loaded. By default, if the account owner is an Individual, this will be the Mobile Phone Number. If the account is a Financial Institution or Other Organization, then this will be the Business Phone Number. Other phone numbers linked to this account display in the Other Information area.
Owner Type	Displays the type of owner for this account, for example Individual or Financial Institution.

- **Account Authority:** This tab provides details for all entities that are considered as having authority for this account, including the type of authority each customer has for this account.
- **Risk List Membership**: This tab displays watch lists associated with the selected account. You can view details such as the source of the data, when the customer was added or removed from the watch list, the list name, and the risk rating.

- **Anticipatory Profile**: The anticipatory profile of all customers is collected at the inception of customer relationships in order to understand the sources of funds and the expected transactions for these entities. This tab displays the list of all anticipatory profiles associated with the selected account.

- **Transaction:** This tab displays details pertaining to the account transactions associated with this case.

- **Account Summary:** This tab displays a monthly summary of the activity occurring in this account. This information helps investigators understand the data that led to generation of events associated with this case.

- **Loan Summary**: This tab displays a monthly summary of the activity occurring in the Loan account, up to the previous 13 months. If the account business type is LOAN, then that account will be a loan account and existing tab name of Account Summary will be changed to Loan Summary dynamically.

> **NOTE**   At any given point, Account Summary or Loan Summary will be shown and not both.

5.5.4.2   Add Accounts

Use this section to add an account with the selected case. During the investigation of a case, you can add an account or accounts to a case to reflect the relationship of the accounts with the selected case.

To add a new account, follow these steps:

1. Navigate to the Accounts list on the **Case Details** page for a selected case.

2. Click **Add Account** ⊞ . The **Add Account** window is displayed.

3. Enter the **Account ID** or **Account Name**.

   - The **Account Name** field supports wildcard and case-insensitive search.

   - The **Account ID** field supports search for multiple IDs with a comma (,) separator.

   - The **Account Type** drop-down list is enabled only when an **Account Name** is entered.

4. Click **Search**. The list of Accounts is displayed.

   Reset discards the data entered by you and resets the contents to their original state.

5. Select the account (or accounts) and click **Add**.

   A confirmation message is displayed: *Account Added Successfully.*

   The system saves the new account details and associates it to the current case. Corresponding audit entries are also recorded in **Audit History** on the case. For more information, see Audit History.

5.5.4.3   Remove Accounts

Use this section to remove an existing account from the selected case.

To remove an account, follow these steps:

1. Navigate to the Accounts list on the **Case Details** page for a selected case.

2. Select the required account (or accounts) and click **Remove Account** ⊟.

3. Provide a reason for why you are removing the selected account from the case.

4. Click **Yes**. A confirmation message is displayed: *Account Removed Successfully*. The window closes and navigates you to the refreshed list of the **Accounts** dashboard. Corresponding audit entries are also recorded in the **Audit History** on the case.

5.5.4.4 Sort Accounts

To sort accounts in the list, follow these steps:

1. In the Accounts list on the **Case Details** page, select a column (for example, Account ID, AccountType, and so on).

2. Sort in ascending or descending order by clicking the up arrow or down arrow buttons respectively.

5.6 Transactions

Use this section to view a complete list and description of the transactions when the event was created associated with the selected case.

Topics:

- Transaction Details
- Add Transactions
- Remove Transactions
- Sort Transactions

To view the transactions associated with a selected case, follow the step:

1. Click the **Transactions** tab in the **Case Details** page for a selected case. The **Transactions** tab is displayed with the list of transactions associated with this case.

   Transactions are displayed under multiple tabs. Each tab label provides the number of transactions of this type.

   - **All Transactions:** Use this tab to view details of all transactions associated with this event.
   - **Funds Transfer:** Use this tab to view details of funds transfers.
   - **Monetary Instrument Transaction:** Use this tab to view details of monetary instrument transactions.
   - **Cash Transactions:** Use this section to view cash transactions associated with the selected transaction.
   - **Back Office Transaction:** Use this tab to view back-office transactions for the selected transaction.

5.6.1   Transaction Details

To view the details of a transaction associated with a selected case, follow these steps:

1. In the **Transactions** tab of the **Case Details** page for a selected case, click the **Transaction ID** for the transaction you want to view details for. The Transactions Details page opens.

   The Transaction Details pop-up window provides information about the transaction included with this case when the case was created. The information which displays depends on the transaction type of the selected transaction.

   Table 17 describes these fields and the transaction types for which they display:

Table 17: Fields in Transaction Details and their Descriptions

Field	Description	Funds Transfer Transactions	Monetary Instrument Transactions	Cash Transactions	Back Office Transactions
Transaction ID	The unique identification number of the transaction.	X		X	X
Transaction Date	The date and time on which this transaction was conducted.	X			X
Source	Source system from which the transaction data was extracted, such as your firm's core banking system.	X		X	X
Amount	Monetary value of the funds transferred via this transaction.	X		X	X
Bank - to - Bank Instructions	Instructions that the sending bank provides to the receiving bank for processing this transaction.	X			
Originator- to - Beneficiary Instructions	Instructions that the transaction's originator provides to be conveyed to the beneficiary upon receipt of this transaction.	X			

Table 17: Fields in Transaction Details and their Descriptions

Field	Description	Funds Transfer Transactions	Monetary Instrument Transactions	Cash Transactions	Back Office Transactions
Jurisdiction	Jurisdiction of the transaction.	X			
Issue Date	For monetary instruments and checks, the date and time on which the monetary instrument associated with this transaction was issued or purchased.			X	
Deposit Date	For monetary instruments and checks, the date and time on which the monetary instrument associated with this transaction was deposited at the depositing institution.			X	
Clearing Date	For monetary instruments and checks, the date and time on which the clearing institution cleared the monetary instrument associated with this transaction.			X	
Post Date	Date and time this transaction was posted.			X	
Serial#/ Check	The serial or check number.			X	
Foreign	Whether the transaction originated or terminated in a different country.			X	

Table 17: Fields in Transaction Details and their Descriptions

Field	Description	Funds Transfer Transactions	Monetary Instrument Transactions	Cash Transactions	Back Office Transactions
Third-Party Passthrough	Whether the originator or beneficiary on this transaction is not the ultimate originator or beneficiary of the funds (for example, a wire transfer with instructions for further credit to a third party).	X		X	
Transaction Date	The date and time on which this transaction was conducted.	X			X
Debit/Credit	Whether assets are being transferred into (credit) or out of (debit) this account by this transaction.				X
Account ID	The ID number for the account from which this transaction was conducted.				X
Offset Account ID	The principal offset account unique identification number in which this transaction was conducted.				
Account Risk	The level of risk associated with the account.				X
Conductor Name	The name of the conductor who has done this transaction.				X

Table 17: Fields in Transaction Details and their Descriptions

Field	Description	Funds Transfer Transactions	Monetary Instrument Transactions	Cash Transactions	Back Office Transactions
Conductor Account	The account of the conductor who has done this transaction.				X
Location ID	The ID of the location where this transaction was conducted (for example, ATM terminal).			X	
Location Name	The name of the location where this transaction was conducted (for example, the merchant name).			X	
Location Address	The address of the location where this transaction was conducted.			X	
User ID	The ID of the user who conducted this back office transaction.				X
Remitter	Details of the party who is the remitter on the transaction.		X		
Originator	Details of the party who is the originator on the transaction.	X			
Third-party Originator	Details of the third- party originator on the transaction.	X			
Beneficiary	Details of the party who is the beneficiary on the transaction.	X	X		

Table 17: Fields in Transaction Details and their Descriptions

Field	Description	Funds Transfer Transactions	Monetary Instrument Transactions	Cash Transactions	Back Office Transactions
2nd Beneficiary	Details of the party who is the 2nd beneficiary on the transaction.		X		
Third-party Beneficiary	Details of the third- party beneficiary on the transaction.	X			
Sending FI	Details of the Financial Institution which sent this transaction.	X			
Receiving FI	Details of the Financial Institution which received this transaction.	X			
Issuing FI	Details of the Financial Institution which issued this transaction.		X		
Clearing FI	Details of the Financial Institution which cleared this transaction.		X		
Deposit FI	Details of the Financial Institution which deposited this transaction.		X		
Description	Any comments pertaining to this transaction.				X
Information	Additional information about this back office transaction.				X

Table 17: Fields in Transaction Details and their Descriptions

Field	Description	Funds Transfer Transactions	Monetary Instrument Transactions	Cash Transactions	Back Office Transactions
Risk Information	Information about the risk associated with the offset account involved in this transaction.				X

5.6.2 Add Transactions

Use this section to add a transaction to the selected case. This is useful when an Investigator wants to perform the comprehensive analysis of transactions associated with the selected case.

To add a new transaction, follow these steps:

1. In the **Case Details** page of a selected case, click the **Transactions** tab. The **Transaction** tab displays a list of transactions associated with the event when the event was generated.

2. Click **Add Transaction** [+] . The **Add Transaction** window is displayed.

3. Enter the details as described in Table 18 .

Table 18: Fields in Add Transaction Window and their Descriptions

Field	Description
Transaction ID	Enter the unique identification number of the transaction.
Transaction Type	Select the type of transaction, such as cash or funds transfer from the drop-down list.
Transaction Date From Transaction Date To	Enter the date range on which this transaction was conducted. This date range is in MM/DD/YYYY format.
Party Name	Enter the name of party (for example, account and customer).

4. Click **Search**. The list of transactions is displayed.

   Reset discards the transaction data entered by you and resets the contents to their original state.

5. Select one or more transactions and click **Add**. A confirmation message is displayed: *Transaction Added Successfully*.

   The system saves the new transaction details and associates them to the current case. The newly added records display in the list of transactions. Corresponding audit entries are also recorded in **Audit History** on the case. For more information, see Audit History.

5.6.3   Remove Transactions

Use this section to remove an existing transaction from the selected case.

To remove a transaction, follow these steps:

1. In the **Case Details** page of a selected case, click the **Transactions** tab.

2. Select one or more transactions and click **Remove Transaction** ▬.

3. Provide a reason for why you are removing the selected transaction from the case.

4. Click **Yes**. A confirmation message is displayed: *Transaction Removed Successfully.* The window closes and navigates you to the refreshed list of the **Transactions.** Corresponding audit entries are also recorded in the **Audit History** on the case.

5.6.4   Sort Transactions

To sort transactions in the list, follow these steps:

1. In the Transactions list of the **Transactions tab,** select a column (for example, Transaction ID,, and so on).

2. Sort in ascending or descending order by clicking the up arrow or down arrow buttons respectively.

5.7   Relationship

This section provides details about cases and events related to the selected case.

To view cases and events related to a selected case, follow the step:

1. On the **Case Details** page of a selected case, click the **Relationship** tab. The Related Cases and Related Events display.

   - Related Cases: Cases are considered Related in the following situations:

      — When the same Applicant is part of multiple KYC Onboarding cases.

      — When the same Applicant is part of both a KYC Onboarding case and a CS RT case.

      — When a KYC OB Prospect (for example, P1) is on-boarded as a Customer (for example, C1), the relationship between prospect P1 and customer C1 is provided through stage data. If a KYC Onboarding case (C100) is created for P1 and a KYC Batch case is created for C1 (C101), the KYC Batch case (C101) and KYC Onboarding case (C100) will display as Related.

      — When CS batch cases and CS Real-time cases are created with the same Source Request Id, the cases are considered related and are displayed under each other's relationship tab.

   - Related Events: Cases are considered Related in the following situations:

      — Events which have the same Application ID (Case Type: KYC Onboarding and CS RT).

      — When CS batch events and CS Real-time events are created with the same Source Request Id, the events are considered related and are displayed under each other's relationship tab.

5.8   Attachment

This section provides details about documents attached to the selected case.

Investigators can view evidence that has been attached to a case and assess whether it is relevant to their investigation. The Attachments tab in the Case Details page displays a list of evidence that is associated with this case, as well as who uploaded the document and any comments provided.

To view attachments related to a selected case, follow these steps:

1. On the **Case Details** page of a selected case, select the **Attachment** tab. The list of documents and attachments display.

2. Click the attachment name to download the attachment.

5.8.1   Add Documents in the Attachments Tab

You can add evidence to cases in order to provide more insight on the case being investigated.

To add documents from the Attachments tab in the Case Details page, follow these steps:

1. In the Case Details page, under the **Attachments** tab, click **Add Document** +.

2. Drag and drop files or click to upload files as attachments. When you upload the files, the file name, size, and file type are displayed. You can also delete the uploaded files using **Delete** ×.

3. Enter a description for these documents, if you choose to.

4. Enter comments to explain why you are attaching these documents.

5. Click **Upload**. The documents are saved and display in the Attachments tab.

5.8.2   Remove Documents from the Attachments Tab

If you determine that a document is no longer relevant to your investigation, you can remove it from the case.

To remove documents from the Attachments tab in the Case Details page, follow these steps:

1. In the **Attachments** tab, select the document or documents that you want to remove from the case.

2. Click **Remove** Docu**ment** +. A message displays, *Are you sure you want to remove the selected document(s) from the case?*

3. Enter comments to explain why you are removing these documents.

4. Click **Yes**. The documents are removed from the Attachments tab.

5.9   Risk Assessment

This section provides details about the events and risk assessments associated with this case.

> **ATTENTION**   This section will only display for KYC Onboarding and KYC Batch.

To view risk assessments and events related to a selected case, click the **Risk Assessment** tab from the **Case Details** page of a selected KYC case. The Risk Assessments tab displays the event details along with the list of the Risk Assessments associated with this event.

5.9.1   Event Details

The Event Details section displays a complete list and description of the events linked to prospects associated with the selected case.

Table 19 describes the fields in Event Details List.

Table 19: Fields in Event Details List and their Descriptions

Field	Description
Event ID	Displays the event ID and the batch type of the risk assessment. The valid values for the batch type include New Account Review, Periodic Review, Accelerated Re-review, and Deployment Initiation. Click **Accelerated Re-review** to view the evidence details, including Change Log evidence, Case evidence and Regulatory report evidence.
Focus Name	Displays the name of the focused prospect customer or account for the event, such as the name of the customer or external entity.
Focus Type	Displays the focus type for this event. For example, RISK_ASSESSMENT.
Jurisdiction	Displays the jurisdiction to which the event belongs.
Business Domain	Displays the business domain to which the event belongs.
Created By	Displays whether the case is promoted Manually or by the System. To view the Reason for the case creation, click the hyperlinked value. • If the case is promoted manually, the Reason for the case displays with any Comments. • If the case is automatically promoted by the system due to the Risk Assessement Score being greater than or equal to the threshold score set in the evaluator widget, the Reason displays with the Current KYC Risk Score and Defined Threshold Score. This is applicable for KYC Onboarding and KYC Batch cases. • If the case is automatically promoted by the system due to a change in the current risk category compared to the last risk category set in the Evaluator widget, the Reason displays with the Current KYC Risk Category, Current KYC Risk Priority, Last KYC Risk Category, Last KYC Risk Priority, Last Risk Assessment ID, and Last Risk Assessed On date. This is applicable only for KYC Batch cases.
Source System	Displays the source system name for which the event is received. For example, CRM, Core Banking, Account Onboarding, and so on.
Score	Displays the matching score value for the event.
Created Date	Displays the date and time this event was created.

5.9.2   Risk Assessments List

To access the Risk Assessment details, follow these steps:

1. Navigate to the **Risk Assessments** list below the Event ID section. The system displays the list of Risk Assessments for primary and secondary prospects for KYC Onboarding cases, and the risk assessments for Primary Customers and Interested Parties for KYC Batch cases.

- For KYC Batch cases: Each risk assessment record displays as the Customer/Interested Party name and KYC Risk Score.

- For KYC Onboarding cases: Each risk assessment record displays as the Risk Assessment ID, Primary/Secondary Prospect name, and KYC Risk Category. Secondary Prospects who only undergo Watchlist Screening will not have a KYC Risk Category. The Assessment Type in the Risk Assessment Details will either be Full KYC or Watch List Screening.

NOTE	• For KYC Onboarding cases, a unique risk assessment ID is assigned for each prospect in the application.
	• For KYC Batch cases, a unique Risk Assessment ID is assigned only at the Primary Customer level, and all Interested Parties are linked to the same Risk Assessment ID.

2. Use the Search bar to filter the risk assessment details.

- For KYC Batch cases: Use the Search bar below the Risk Assessment ID and Risk Category to filter the Risk Assessments with Customer or Interested Party details. Customer and Interested Party names will display in different font colors, as follows:

  — Primary Customers #AE562C( )

  — Interested Parties #000000 ( )

Click the Customer, Interested Party, or Risk Score link to view the risk assessment details. By default, the risk assessment details for Primary Customer display.

- For KYC Onboarding cases: use the Search bar under the Event details on the left to filter the Risk Assessments with Primary and Secondary Prospects. Primary and Secondary Prospect's names display in different font colors, as follows:

  — Primary Prospect #AE562C( )

  — Secondary Prospect #000000 ( )

  — Focus Party #000CD ( )

  — Primary Prospect and Focus Party (If the primary prospect is also a focus party)

    #AE562C( )

Click the Primary Prospect, Secondary Prospect, or Risk Category detail to view the risk assessment details. By default, the risk assessment details for Focus prospect display.

- Algorithmic Score: Provides the complete list of risk attributes (also called rule names) considered for this risk assessment. Each row contains the rule name (such as, Occupation risk), contributing risk score (on a scale of 0 to 100), and the value (such as, occupation code or description).

- Business Check Score: Provides the complete breakdown of business check score attributes considered for this risk assessment.

- Matches: Provides the details of watch list entities this prospect/customer matches with across various watch list types, namely Sanctions list, PEP list & EDD list.

The Risk Assessment List opens and displays the Prospect or Customer Name and the respective KYC risk score. Other risk assessment details which display depend on the case type of the selected KYC Case, as described in Table 20 .

Table 20: Fields in Risk Assessment Details List and their Descriptions

Field	Description	Case Type
Customer/Party ID	Displays the unique ID for the customer or interested party associated with this risk assessment.	KYC Batch
Focus Risk Assessment	Displays whether or not the risk assessment was created for this particular prospect. Valid values are Yes or No. If the value is Yes, it indicates the case was created because of this particular prospect.	KYC Onboarding
Jurisdiction	Displays the jurisdiction to which the risk assessment belongs.	Both KYC Onboarding and KYC Batch
Prospect Type	Displays the Prospect Type of the prospect who is the focus of the risk assessment. For example, Individual.	KYC Onboarding
Batch Type	Displays the type of batch associated with this risk assessment. For example, Deployment Initiation (DI), Periodic Review, New Account Review, and Accelerated Review (ARR).	KYC Batch
Entity Type	Displays the type of customer who is the focus of the risk assessment. For example, Organization or Individual.	Both KYC Onboarding and KYC Batch
SSN/TIN	Displays the Social Security Number (SSN) or Tax Identification Number (TIN) of the prospect who is the focus of the risk assessment.	KYC Onboarding
CIP Status	Displays whether or not this risk assessment has been verified through CIP.	KYC Onboarding
Assessment Type	Displays the assessment type based on the relationship of the Prospect or Interested Party with the Primary Prospect or Customer. For example, Full KYC Assessment, and Watchlist Screening.	Both KYC Onboarding and KYC Batch
Primary Prospect	Displays whether or not the prospect who is the focus of the risk assessment is the Primary Prospect.	KYC Onboarding
Primary Customer	Displays whether or not the customer who is the focus of the risk assessment is the Primary Customer.	KYC Batch
Application ID	Displays the unique ID for the application which triggered the risk assessment.	KYC Onboarding

Table 20: Fields in Risk Assessment Details List and their Descriptions

Field	Description	Case Type
Next Review Date	Displays the date and time on which this customer should next be considered for risk assessment review.	KYC Batch

5.9.3   Split Cases

If, during your investigation, you decide that separate cases should be created for entities that are linked to the same case, you can split the case for each Prospect as desired, and work these cases through to closure.

For example, you can decide to investigate both a company and an individual (UBO) who are listed as Prospects on this case in separate cases.

> **ATTENTION**   This feature is only applicable for KYC Onboarding Case Types.

To split a case, follow these steps:

1. In the Events list of the Risk Assessment tab, click the Event ID to open the Risk Assessment Details.

2. Select the appropriate Risk Assessment record.

3. Click **Split Case** . A new event and a new case are created. The new case is considered a Child to this Parent case.

5.9.3.1   Set Decision

This option allows you to set the decision status for events associated with this case.

> **ATTENTION**   This feature is only applicable for KYC Onboarding Case Types.

5.9.3.2   Sorting Events in the List

You can sort the list of events by selecting the name of the column you wish to sort by from the drop-down list.

5.9.4   Watchlist Match Disposition

As part of KYC Onboarding Case Investigation, Watchlist Match Disposition allows you to dispose the watchlist matches for primary and secondary prospects and recompute the KYC Score. Configuring the watchlist rule as a part of an Algorithmic Score, Business Check Score, or both is mandatory for match disposition.

> **NOTE**   Watchlist match disposition and KYC risk score recomputation are not mandatory for case closure.

You can dispose the watchlist matches as **True Positive** or **False Positive**. After disposing all the watchlist matches, if necessary, you may recompute the KYC risk score.

> **NOTE**   Recompute KYC Score is enabled only for Prospects with the "Full KYC Assessment."

- As a part of risk inheritance, all the matches of primary and related non-primary prospects with Watchlist Screening are considered.
- Watchlist Rule score for Business Check & Algorithmic Scoring is recomputed based on earlier configuration when the initial risk scoring was performed.
- The KYC Risk Score is recomputed based on the new Algorithmic and Business Check Scores. The Risk Category is again derived based on the current risk category configuration for the respective jurisdiction.
- Case Management Audit captures the Watchlist Disposition and KYC Score recomputation actions.

To dispose the watchlist matches, follow these steps:

1. In the **Matches** section, select one or more match records.

2. Click **Dispose Match Records** . The **Dispose Watchlist Matches** pop-up window opens.

3. Determine whether the match is a **True Positive** or **False Positive** and enter any **Comments**.

4. Click **Save** to save the match dispositions.

> **NOTE**   You can dispose matches multiple times before KYC risk score recomputation or case closure. Once the case is closed, the Disposition and Recomputation actions are disabled.

To recompute the KYC risk score, follow these steps:

1. Dispose all the watchlist matches of primary/secondary prospect(s).

2. Click **Re-compute KYC Score** .

The Case Management UI displays the recomputed Risk Assessment Score and Risk Category along with the old Risk Assessment Score and Risk Category as KYC Score (Undisposed) and Risk Category (Undisposed).

5.10   Prospect

This section provides details about any potential prospect when the event was created.

> **ATTENTION**   This section will only display for KYC Onboarding Case Types.

To view prospect details related to a selected case, follow these steps:

1. On the **Case Details** page of a selected KYC case, open the **Prospect** tab. The Prospect Network diagram shows the visual connection between the primary and secondary prospects based on their relationship.

2. Click any Prospect Name. A pop-up window opens and displays the relationship between the primary prospect to the secondary prospect.

5.10.1 Prospect Details

To access the Prospect details, click an Applicant ID. The Prospect Details opens and displays the following tabs.

- Prospect Details: Provides the essentials details for this Prospect, such as Date of Birth, ID Type, Occupation, and so on.
    - Occupation
    - Marital Status
    - Primary Citizenship
    - Secondary Citizenship
    - Jurisdiction
    - Employer
    - Employer Status
    - Estimated Annual Income
    - SSN/Tax ID
    - Gender
    - Date of Birth
    - CIP Status
    - Risk Category
    - Risk Assessment Score
    - Algorithmic Score
    - Business Score
- Basic Information: Provides the following essential demographic attributes pertaining to the selected prospect:
    - Primary Address
    - Primary Contact Number
    - Primary Email
    - Entity Name
    - Jurisdiction
    - Date of Incorporation
    - Market Served
    - Legal Structure and Ownership
    - Other information section provides all provided contact details of the selected prospect, such as addresses, phone numbers, and email addresses.
- IDV Documents: Provides the following Identification and Verification (IDV) Document attributes to identify and verify the documents:

- Document Purpose
- Document Number
- Document Name
- Issuing District
- Issuing Province
- Issuing City
- Issuing State
- Issuing Country
- Issuing Date
- Expiry Date
- Issuing Authority

6   Acting on Cases

This section explains how to take actions on a selected case or cases.

> **NOTE**   To take actions on multiple cases simultaneously, use the Case Search and List page to select the cases and take necessary actions. To take action on a single case, select the case from the Case Search and List page or navigate to the Case Details page of the case and perform the required actions.

6.1   Access the Take Action Window

The Take Action window has several options that you can take on a selected case. The options that you see in this window are based on the case type, case status, and the user role for the selected case or cases.

This section explains how to take resolution action on the selected case or cases. Supervisor approval provides a dual control or approval process that requires an authorized user (for example, a Supervisor) to approve actions of other users, prior to those actions taking full effect on the case (for example, closing the case). This process also enables users of specified roles to acknowledge approved or rejected changes proposed and to annotate an acknowledgment with comments.

To take action on one or multiple cases, follow these steps:

1. Navigate to the **Case Search and List** page. Select one or more cases you want to take action on.

> **NOTE**
> - In order to take action on multiple cases, all cases must be in the same status.
> - If one or more cases you have selected are currently locked by another user, you can apply the actions to all unlocked cases.

2. Click **Take Action** ⌘. The **Take Action** window is displayed.

3. Or, if you are taking action on a single case, you can also click **Take Action** ⌘ on the **Case Details** page. The **Take Action** window is displayed.

> **NOTE**   If you click on Take Action for new Cases, you will receive a popup message and can do the following actions in the popup screen:
> - Click **Yes**: The case will be assigned to you, and you can release or block the case on the Take Action page.
> - Click **No**: The Case will not be assigned to you, and you can only set the case assignee on the Take Action page.

6.2   Assign Cases

You can assign a case to reassign ownership of a case to a different user in multiple ways.

- From the Case Search and List page
- From the Case Details page and the Case Information section of the Case Details page

- From the Set Case Assignee drop-down list in the Take Action window

If the initial analysis of the case reveals an issue that should be reviewed by another user, reassign the case to the most appropriate user.

6.2.1   From Case Search and List

To assign a case or cases from the Case Search and List page, follow these steps:

1. In the Case Search and List page, hover over a Case ID or select one or more cases.

2. Click **Assign** to view the Assign options.

   - Click **Assign to me** to assign the case or cases to yourself. The confirmation message displays: *Assignee Successfully Updated*

   - Click **Assign To** to assign the case to another user. The Assign To window opens.

   a. Select the user you want to assign the case or cases to from the Assign selected cases drop-down list.

   b. Click **Apply.** The confirmation message displays: *Assignee Successfully Updated.*

6.2.2   From Case Details

To assign a case or cases from the Case Information section of the Case Details page, follow these steps:

1. In the Case Search and List page, click a Case ID. The case opens in a new tab.

2. Click **Assign to me** in the Case Information to assign the case to yourself.

3. To assign the case to another user, click the **Case Details** icon . The Case Detail window displays.

4. Select the user you want to assign the case to from the **Assignee** drop-down list.

5. Click **Save**. The case is updated with the new assignee.

6.2.3   From Take Action

To assign a case or cases from the Take Action page, follow these steps:

1. Navigate to the **Case Search and List** page. Select one or more cases you want to take action on.

2. Click **Take Action** . The **Take Action** window is displayed.

   Or, if you are taking action on a single case, you can also click **Take Action** on the **Case Details** page. The **Take Action** window is displayed.

3. Select the user you want to assign the case to from the **Set Case Assignee** drop-down list.

4. Click **Save**. A confirmation message displays: *Case Actions Taken Successfully.* The case is updated with the new assignee.

6.3   Set Due Date

To set a due date, follow these steps:

1. On the **Take Action** window, select a due date using the calendar in **Set Due Date**. Use the clock to set the time.

2. Click **Save**. The new due date is set for the case.

   ■ Due Date must be set to a current or future date.

   ■ It is mandatory to enter comments when you are clearing or setting a due date.

   ■ The Due Date will display in the time zone you set in Preferences.

6.4 Submit Cases for Review

If a case's initial analysis reveals an issue that should be reviewed by another user, you can reassign the case to the most appropriate user and submit the case for review.

To submit a case for review, follow these steps:

1. Select a case in Investigation status and click **Take Action** ⌘,The Take Action window displays.

2. Set a new **Due Date**, if desired, by either using the calendar or entering the new due date in the text box.

3. Select a Case Assignee using the **Set Case Assignee** drop-down list. You cannot assign a case to yourself for review.

4. Under the **Resolution** option, select **Submit for Review.**

5. Select the reason this case requires review from the **Reason** drop-down list. This field is mandatory.

6. Enter your comments in the **Comments** field. This field is mandatory.

7. Click **Save**. The case is updated and moves to Pending Review status.

6.5 Review Cases

Supervisors can review cases when the case's initial analysis reveals an issue requires further review.

> **NOTE**   You must be the case assignee to review this case. If you wish to review a case that is not currently assigned to you, click the **Assign to Me** link.

To review a case, follow these steps:

1. Select a case in Pending Review status. The case is updated and moves to Pending Review status.

2. You can now take action on the case, including attaching evidence or documents, adding to the Narrative, resolving the case, and so on.

6.6 Close Cases

When you have completed your investigation, you can close the case. To close a case, follow these steps:

1. In the Case Search and List page, select a case in either Investigation or Review in Progress status.

2. Click **Take Action** ⌘,The Take Action window displays.

3. Under the **Resolution** option, select **Close Case.**

4. Select the reason this case should be closed from the **Reason** drop-down list. This field is mandatory.

   The following reasons are available by default. Your Administrator may add additional reasons for closure:

   - False positive

   - SAR required

   - STR required

5. Enter your comments in the **Comments** field. This field is mandatory.

6. Click **Save**. The case is updated and moves to Closed status.

6.7   Reopen Closed Cases

After you have closed a case, you may discover that you need to provide additional information to this case. For example, if a case is missing key information you may need to add a comment or attachment.

To reopen a case, follow these steps:

1. In the Case Search and List page, select a case in Closed status.

2. Click **Take Action** ⌘,The Take Action window displays.

3. Under the **Resolution** option, select **Reopen Case.**

4. Select the reason this case should be reopened from the **Reason** drop-down list. This field is mandatory.

   The following reasons are available by default. Your Administrator may add additional reasons for reopening:

   - Factual Error

   - Failed QA

   - Missing Key Information

5. Enter your comments in the **Comments** field. This field is mandatory.

6. Click **Save**. The case is updated and moves to Investigation status.

6.8   Track Regulatory Reports

If you have closed a case with a recommendation to file a regulatory report, such as STR or SAR, you can track the status of the report.

To view regulatory report status, follow these steps:

1. In the Case Search and List page, select a case in Closed status with a Reason of either SAR required or STR required.

2. Click **Regulatory Report** ,The Regulatory Report window displays, showing the report details.

If your firm has implemented Oracle FCCM Regulatory Reporting Cloud Service, you can click the Report ID to view and manage this report in the Regulatory Reporting Cloud Service user interface.

6.9   Continuing Activity Investigations

If you have closed a case with a recommendation to file a US SAR regulatory report, a supplemental review is required to determine whether or not a continuing SAR is necessary. When you close an AML case which meets your firm's requirements for supplemental review, a new Continuing Activity (AML_CA) case is created.

The Continuing Activity case allows investigators to review activities which occurred after the time the previous case was closed. This case must be investigated and concluded within your firm's review period, typically between 90-120 days. During this period, the continuing SAR must be filed, if necessary.

When investigating the Continuing Activity case (AML_CA) you can view selected information from the original case. If your firm has implemented Oracle FCCM Regulatory Reporting Cloud Service, you can view a summary of SARs filed as a result of the original case to assist in your investigation.

6.9.1   Creating a Continuing Activity Case

To create a Continuing Activity case, follow these steps:

1. In the Case Search and List page, select an AML case (for example, AML_SURV) in either Investigation or Review in Progress status.

2. Click **Take Action** ⌘. The Take Action window displays.

3. Under the **Resolution** option, select **Close Case.**

4. Select **SAR Required** from the **Reason** drop-down list and enter comments.

5. Click **Continue**. The Subjects for Supplemental Case window displays.

6. Select any Customers, External Entities, or Accounts which should be included in the supplemental case from the appropriate section.

7. Click **Save & Create Supplemental Case**. The supplemental case is created according to your firm's requirements. By default, the Due Date for the case is 120 days from case creation.

6.10   Audit History

When an action is taken on a case that leads to a change of status or value, such as a transaction is added, the Case Assignee is updated, and so on, the change is recorded in the Audit History. This allows you to understand who performed an action, why it was taken, when the action occurred, and what the value was before the change was made.

To access the Audit History, follow these steps:

1. Navigate to the **Case Details** page by selecting a case from the **Case Search and List** page.

2. Click **Audit History** 🕐. The **Audit History** window opens and displays a record of all actions taken on a case with the following types of details:

   - **ID**: The ID assigned to this action based on the order the action occurred. By default, actions display in descending order by ID so you can view the most recent action first.

   - **Action Taken**: The specific action which was taken, for example, Case Status Updated.

- **Before**: The value or status prior to this action being taken, for example, Pending Review. If the action was to add a value, such as adding a transaction to the case, N/A will display.

- **After**: The updated value or status after this action was taken, for example, Review In Progress. If the action was to remove a value, such as removing a transaction from the case, N/A will display.

- **Who**: The user who took the action.

- **Date and Time**: When the action was taken.

- **Why**: Reason or comments given by the user when the action was taken. If the action was taken by the system, such as an automated status update, this field will be blank.

6.10.1   Filter Audit History

You can also filter the Audit History to display only specific actions, actions which were performed by a specific user, or changes which occurred within a specific time frame.

To filter the Audit History, follow these steps:

1. Navigate to the **Case Details** page by selecting a case from the **Case Search and List** page.

2. Click **Audit History** . The **Audit History** window opens and displays a record of all actions taken on a case.

3. Select one or more filter criteria from the following options:

   - **Action Taken**: Select an action from the drop-down list. This list displays only unique actions which have been taken on this case.

   - **Who**: Select a user from the drop-down list. This list displays only users who have taken action on this case.

   - **Date From** and **Date To:** Select the date range during which the actions were taken.

4. Click **Apply** to filter the results. The Audit History displays only the records which meet the filter criteria.

6.11   Narrative

Use the Narrative option to capture any narrative surrounding the analysis of a case that has helped you decide how to dispose the case. The narrative exists as a single data element on a case, which allows you to add and maintain that narrative. The case narrative supports Rich Text Formatting (RTF).

6.11.1   Create or Edit a Narrative

To create or edit a narrative, follow these steps:

1. Navigate to the **Case Details** page.

2. Click **Narrative** . The **Narrative** page is displayed with a blank text area.

3. Enter your analysis and format as required.

4. Click **Save**. A confirmation message is displayed: *Narrative Added Successfully.*

   The system saves your changes, adds the current date to the **Last Updated** field, and your name to the **Last Updated By** field in the **Narrative** pane header.

7   Creating Cases

> **ATTENTION**   This section is applicable for Transaction Monotoring (TM) Cases.

Cases are created for investigating business entities involved in potentially suspicious events. If there is a need for investigation on an entity for which there are no open cases, then you can create a case manually and proceed with the investigation.

> **NOTE**
> - Only users with relevant case-creation permissions can create a case.
> - Cases are created by users by entering new case information manually.
> - Case types are displayed based on the logged-in user.
> - Cases are created based on the case type. For example, AML Surveillance.

To create a case, follow these steps:

1. Click **Create Case** to open the case creation pop-up window.

2. Before you can manually create a case, you must create the event or events which will be associated with this case. To create an event, set the event attributes:

   - Event Type: Select an Event Type for this event from the drop-down list. **For example**, Anti Money Laundering.

   - Scenario: Select the scenario you want this event to be associated with from the drop-down list. For example, High Risk Geography-Customer Focused.

   - Scenario Highlights: Enter the behavior of interest which caused you to create this event, if desired.

   - Label: Enter the risk indicator associated with the behavior of interest for this event. For example, High Risk Percentage.

   - Value: Enter the value associated with the behavior of interest for this event. For example, 20.

3. Click **Next**.

4. Select an entity who will be the focal entity of this case.

   - Select an Entity Type from the drop-down list.

> **ATTENTION**
> - You must select a Customer who has an associated Account.
> - You must select an Account that has an associated Customer.

   - Either search for an entity by Entity ID or Entity Name. Select the entity you want to be the focus of this case.

5. Click **Next**.

6. Select one or more transactions to be linked to this case. This step is optional.

7. Click **Next**.

8. Enter the following attributes for the new case. These fields are mandatory:

    ■ Enter a Title for the new case.

    ■ Select the Case Type for the new case from the drop-down list.

    ■ Set the Case Priority using the drop-down list.

    ■ Select the Business Domain and Jurisdiction for the new case from the drop-down lists.

    ■ Select a Due Date for this case using the calendar option.

    ■ Select the Case Assignee from the drop-down list.

    ■ Provide a Case Summary, explaining why you have created this case, in the **Case Summary** box.

9. Click **Create Case**. The case is created and added to the Case List.

8   Case Reports

The application enhances data visualization and analyses by providing the ability to generate operational reports of cases. Use the filter mechanism to narrow down the cases of your interest, select the row and column data, and generate the report for cases you have access to view. These reports are available in tabular and graphical formats. You can save, update, or delete the search criteria of generated report.

8.1   Generate Report

To generate a report, follow these steps:

1. From the Navigation List, click **Case Reports**.

2. Expand the **Case Filters** pane, if it's not already expanded, by clicking **Expand** ▶ or **Collapse** ◢ .

3. Provide your filter criteria. See Using Advanced Case Search for more information on using filters.

4. Collapse the **Case Filters** pane by clicking **Expand** ▶ or **Collaps**e ◢ .

5. Select one of the following options from the **Columns** list.

   Table 21 describes the Fields in Case Filter Window.

Table 21: Fields in Case Filter Window and their Descriptions

Field	Description
Case ID	Enter one or more unique case IDs you want to search. For multiple case IDs, separate them with a comma. Ensure that you do not enter a space after the comma. Case IDs are not case-sensitive. This overrides all other filter criteria. Example: CA660, ca671
Created From	Use calendar to specify a date and time on or after which the case was created. For example: Select 08/15/19 to search for cases created on or after August 15, 2019. You can also use this along with the **Created To** filter to search for cases created within a date range.
Age	Use this option to specify a case's age in number of days. For example, if you want to search a case not older than two days, use the "<" operator followed by 2 using the up/down arrows. A case's age is calculated as the number of calendar days between its date of creation and the current date. Cases stop aging when they are closed.
Case Class	A class is a grouping of case types. For example: AML is a class consisting of types AML_DD, AML_PAT, AML_SURV, and so on. Select the case class to narrow your search to include only cases associated with the selected class.

Table 21: Fields in Case Filter Window and their Descriptions

Field	Description
Case Type	A logical grouping of cases. For example: AML_DD, AML_PAT, and so on. Select the case type to narrow your search to include only cases of the selected type.
Status	The current status of the case. Select the case status to narrow your search to include only cases currently in the selected case status.
Reason	Search cases based on the reason selected for the last resolution action performed. For example: False positive, or Factual error.
Title	Search cases based on case title by enter a few letters of the case's title (case-sensitive). For example: if you type AML, you will find cases with titles AML, AML8, AML_Events_Processing_Rule, and so on in the Case Search and List.
Jurisdiction	Search cases that belong to a certain business jurisdiction. The drop-down list contains only jurisdictions which you are authorized to view.
Business Domain	Search cases that belong to a certain business domain. For example: EMP, GEN, and INST. The drop-down list contains only business domains which you are authorized to view.
Entity Type	Search cases based on one or more entity type(s). When the entity type is specified, you must enter a value in the Entity ID or Entity Name field.
Entity ID	Used in conjunction with Entity Type. When the entity type is specified, you must enter a value in the Entity ID.
Entity Name	Search cases by the entity name associated with a case. When the Entity Type is specified, you must enter a value for Entity Name.
Case Action	Select one or more Case Actions to search for cases, which are marked for the specified action to be taken. This list is updated based on the Action Type you select.
Last Action	Used in conjunction with Case Action. Search for cases where the selected Case Action is the last action recorded on the case. For example: If you selected Clear Due Date as the Case Action and Yes as the Last Action, only cases for which the last Case Action was to clear the due date are listed.
Action From	Used in conjunction with Case Action. Search for cases on which the Case Action is recorded within the time range specified in the Action From and Action To filters. For example: If you select Case Accessed as the Case Action and 12/01/19 as the Action From date, all cases on which the action Case Accessed is recorded from and including December 1st are listed. You can use Action From and Action To date fields to specify a date range within which a selected action was taken.

Table 21: Fields in Case Filter Window and their Descriptions

Field	Description
Action To	Used in conjunction with Case Action. Search for cases on which the Case Action is recorded within the time range specified in the Action From and Action To filters. For example: If you selected Case Accessed as the Case Action and 12/01/19 as the Action To date, all cases accessed up to but not including December 1st are listed. You can use Action From and Action To date fields to specify a date range within which a selected action was taken. For example: If you selected Case Accessed and specify 12/01/19 and 12/06/19 as the Action From and To dates, respectively; all cases accessed between Dec 1st and Dec 6th are listed.
Priority	Select the priority of the case (High, Medium, or Low) from the drop-down to search based on the case's priority.
Due Date From	Select the date and time using the calendar to filter the Case List by the past date before the action should be taken on the case.
Due Date To	Select the date and time using the calendar to filter the Case List up to the date before the action should be taken on the case.
Closed From	Search cases closed on or after the specified date and time. You can also use this in conjunction with Closed To date filter to search cases closed within a date range.
Closed To	Search cases closed up to including the specified date and time. You can also use this in conjunction with Closed From date filter to search cases closed within a date range.
Event Type	Search cases based on the selected event type. For example: AML or CS_EDD.
Scenario	Use one or more scenario options to filter and narrow your search based on the selected scenarios associated with the case.
Assignee	Search cases by assigned user. For example: if you select CM Analyst as the Assignee, all cases assigned to the CM Analyst are listed. You can select multiple assignees to search using multiple-choice selections.
Comments	Search for cases based on comments provided on the case.

6. From the **Rows** list, select a different option from the one you chose from the **Columns** list. Note that the options available in the **Rows** list are the same as those available in the **Columns** List. If you select Case Age, you must select one of the Row Aggregation options: Weekly, Daily, Monthly, Quarterly, or Yearly.

Use the Case Aggregation option to specify how the cases meeting your criteria must be displayed, that is, on a daily, weekly, monthly, quarterly, or yearly basis.
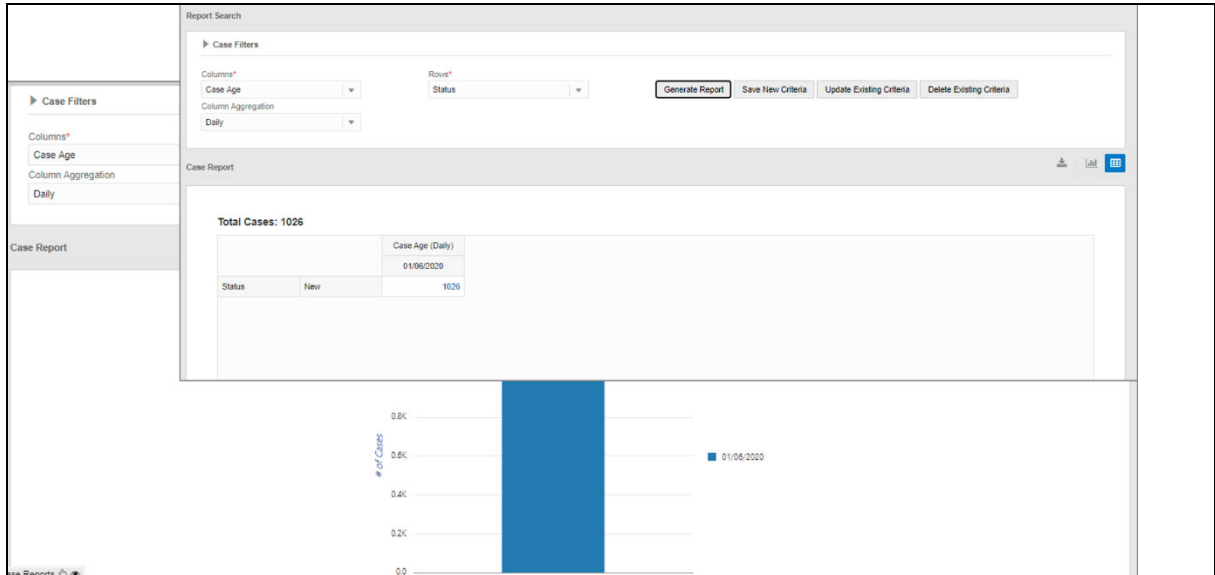
> **NOTE**   The selected Column and Row options should not be the same.

7. Click **Generate Report**. The report is generated and displayed in the **Case Report** pane.
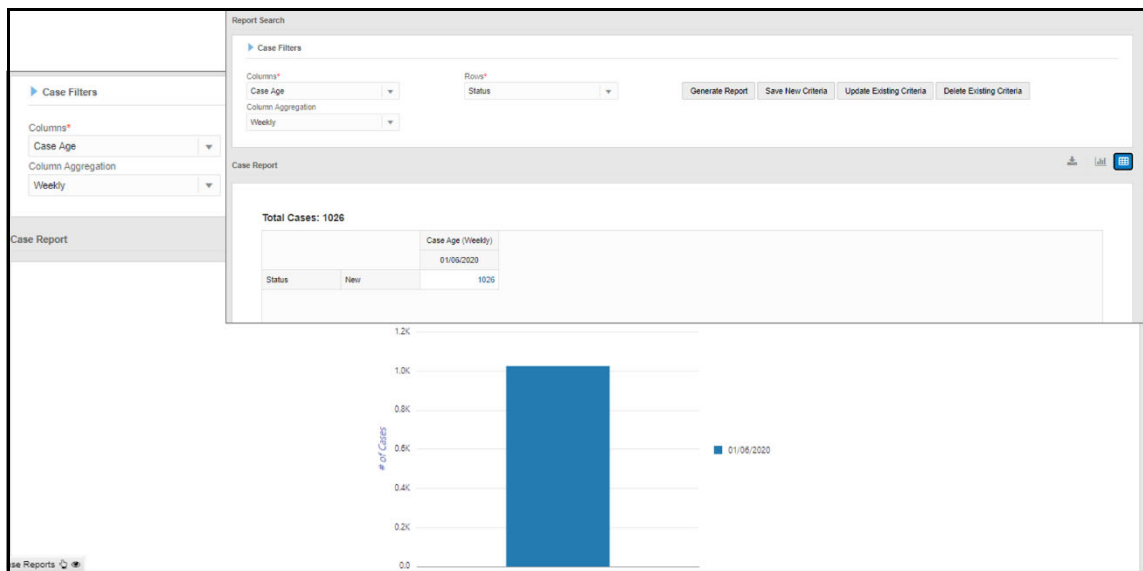
8.1.1 Samples

Sample report showing cases aggregated in tabular and graphical formats:

Figure 1: Sample report showing cases aggregated Daily in tabular and graphical formats


Figure 2: Sample report showing the same cases aggregated Weekly in tabular and graphical formats

Description of the Sample reports follows:

In the graphical view, the **Columns** values form the y-axis and the **Rows** values form the x-axis of the chart.

8. Click the **Graphical View** or **Tabular View** on the top-right corner of this pane to view the report as a chart or a table, respectively.

8.2 View Report

You can view and analyze the generated report. The search criteria of the report are also displayed in the **Report Search** pane.

To view a report, follow these steps:

1. Navigate to **Case Reports page.**

2. Click the Report from the **Report List** pane. The report is displayed in the **Case Report** pane.

The following tasks can be performed on an existing report:

- Generate Report
- Save Search Criteria of Report
- Update Search Criteria of Report
- Delete Search Criteria of Report
- Export the Report

8.2.1 Save Search Criteria of Report

The **Save New Criteria** option allows you to create and manage personal search criteria for your future uses.

To save the search criteria, follow these steps:

1. Navigate to the **Case Reports page.**

2. Generate Report or view the existing report and click Save New Criteria**.** See the Generate Report section for information on generating the report. See the View Report section for information on viewing the existing report. The **Save New Criteria** window is displayed.

3. Enter the name and description of new criteria. Click **Save**. A confirmation message is displayed: *Criteria Added Successfully*. The newly added search criteria are updated in **Report List** section.

8.2.2 Update Search Criteria of Report

The **Update Existing Criteria** option allows you to update the search criteria of selected report.

To update the search criteria, follow these steps:

1. Navigate to the **Case Reports page.**

2. Select the existing report from the **Report List** section and update the Columns and Rows of the report. Provide your filter criteria, if required. See *Step 2* in Using Advanced Case Search for more information on providing the filter criteria.

3. Click **Update Existing Criteria.** The **Update Existing Criteria** window is displayed.

4. Enter the **Selected Criteria's** description and click **Update Existing Criteria.** A confirmation message is displayed: *Criteria Updated Successfully*. Click **OK.**

8.2.3 Delete Search Criteria of Report

The **Delete Existing Criteria** option allows you to delete the search criteria.

To delete the search criteria, follow these steps:

1. Navigate to the **Case Reports page.**

2. Select the existing report from the **Report List** section and click **Delete Existing Criteria**. The **Delete Existing Criteria** window is displayed. Click **Delete.** A confirmation message is displayed: *Criteria Deleted Successfully*.

8.2.4 Export the Report

The *Export as Excel* option allows you to export reports available in the application to your local machine. Reports are exported in the Excel (*.xlsx) file format, which can be saved.

To export a report, follow these steps:

1. Navigate to the **Case Reports page.**

2. Generate a new report or view the existing report and click **Save New Criteria.** See the Generate Report section for information on generating the report.

3. Click **Export as Excel** .

4. Browse the path you want to save the Excel file and click **Save**.

   The Report is downloaded to the selected path in .xlsx format

OFSAA Support Contact Details

Raise a Service Request (SR) in My Oracle Support (MOS) for queries related to OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.