Oracle®OFS RR Cloud Service

US SAR User Guide

Release 25.03.01
G27776-02
March 2025

OracleOFS RR Cloud Service US SAR User Guide, Release 25.03.01

G27776-02

Contents

7 Acting on Reports

8 Filing Regulatory Reports

1 Preface

US-SAR User Guide guides you step-by-steps instruction to use Oracle Financial Crime and Compliance Management Regulatory Reporting cloud service.

1.1 Audience

This document is intended for users who are responsible for provisioning and activating Oracle FCCM Cloud services or for adding other users who would manage the services, or for users who want to develop Oracle Cloud applications.

1.2 Help

Use Help Icon 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 https://docs.oracle.com/en/ to find guides and videos.

1.3 Related Resources

For more information, see these Oracle resources:

- Oracle Public Cloud: http://cloud.oracle.com
- Community: Use https://community.oracle.com/customerconnect/ to get information from experts at Oracle, the partner community, and other users.
- Training: Take courses on Oracle Cloud from https://education.oracle.com/oracle-cloud-learning-subscriptions.

1.4 Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: https://support.oracle.com/portal/.

2 About US SAR

US SAR stands for the United States Suspicious Activity Report. As a part of regulations and compliances, a Financial Services Organization has to perform appropriate analysis and report any suspicious activities that may lead to fraud and money laundering to the regulatory authorities. These regulatory bodies are responsible for safeguarding financial institutions and consumers from abuse, providing transparency in the country's financial system, enhancing that country's security, and deterring and detecting criminal activity in the financial system.

Financial institutions must provide data regarding suspicious activities to their geographic region's regulatory authority. This data is delivered to the regulatory bodies through regulatory reports. These reports, depending on the regulatory, and geographic region, can be delivered in a paper format or in an electronic format. In the US, these reports are submitted in XML format to Financial Crimes Enforcement Network (FinCEN)

2.1 Oracle Financial Services Compliance Regulatory Reporting Cloud Service

The Oracle Financial Services Compliance Regulatory Reporting Cloud Service (OFS CRR CS) United States Suspicious Activity Report (USSAR) Cloud Service (hence, referred as USSR Cloud Service) is used to analyze the reports and take appropriate action on the report for a resolution.

Reports are generated in the USSAR Cloud Service as a result of the Generate USSAR action taken on a case or cases in the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Case Investigation Cloud Service (FCCM AML CM) Cloud Service. The business data (suspicious activity information, filing institution, and so on) and operational data (narratives, documents, and comments) related to the case, which led to the creation of a report are available in the USSAR Cloud Service. Using this information, authorized users analyze reports and report them to the regulator or close them by providing appropriate details.

The USSAR Cloud Service helps in generating e-file in a .xml format according to specifications described in FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Requirements. After successfully e-filing, you can download the acknowledgment (XML) file from the BSA E-Filing System and upload the acknowledgment into USSAR Cloud Service, thereby completing the SAR process.

2.1.1 Report LifeCycle

This section explains Report Life Cyle

- **Generate a USSAR Report**: After analyzing a suspicious case, if it is required to report to the regulator, you can take action to generate a report. For more information, see Case Investigation Cloud Service.
- **Create a Report**: A report is created in Case Investigation Cloud Service, and the related information is passed to the USSAR Cloud Service using web service. The newly created report is available in the USSAR Cloud Service, and it is assigned to a specific user with a due date to take appropriate action. These parameters are configurable. For more information, see Creating a Report.

- **Search and Open a Report**: To analyze the existing reports, you must open reports using basic, advanced, or views search criteria. For more information, see Opening a Report.
- **Analyze a Report**: To take any kind of action on a selected report, you must thoroughly analyze the details. You must verify the details of the report, such as the involved subject, account, branch, reporting entity details, related documents, narratives, and audit history. For more information, see Analyzing Reports.
- **Act on a Report**: Post analyses, you can take action on the selected report to close or generate an E-file based on your privileges. For more information, see Acting on Reports.
- **E-Filing**: If the report is approved, an e-file is generated for the report. The generated e-file is submitted with FinCEN's BSA E-Filing System. The E-file is validated, and an acknowledgment (XML file) is generated. The acknowledgment file is then uploaded into the USSAR Cloud Service, thereby completing the SAR process. The status of the report changes to Filed. The Filed status is the final status given to a SAR that has been submitted to and processed by FinCEN.

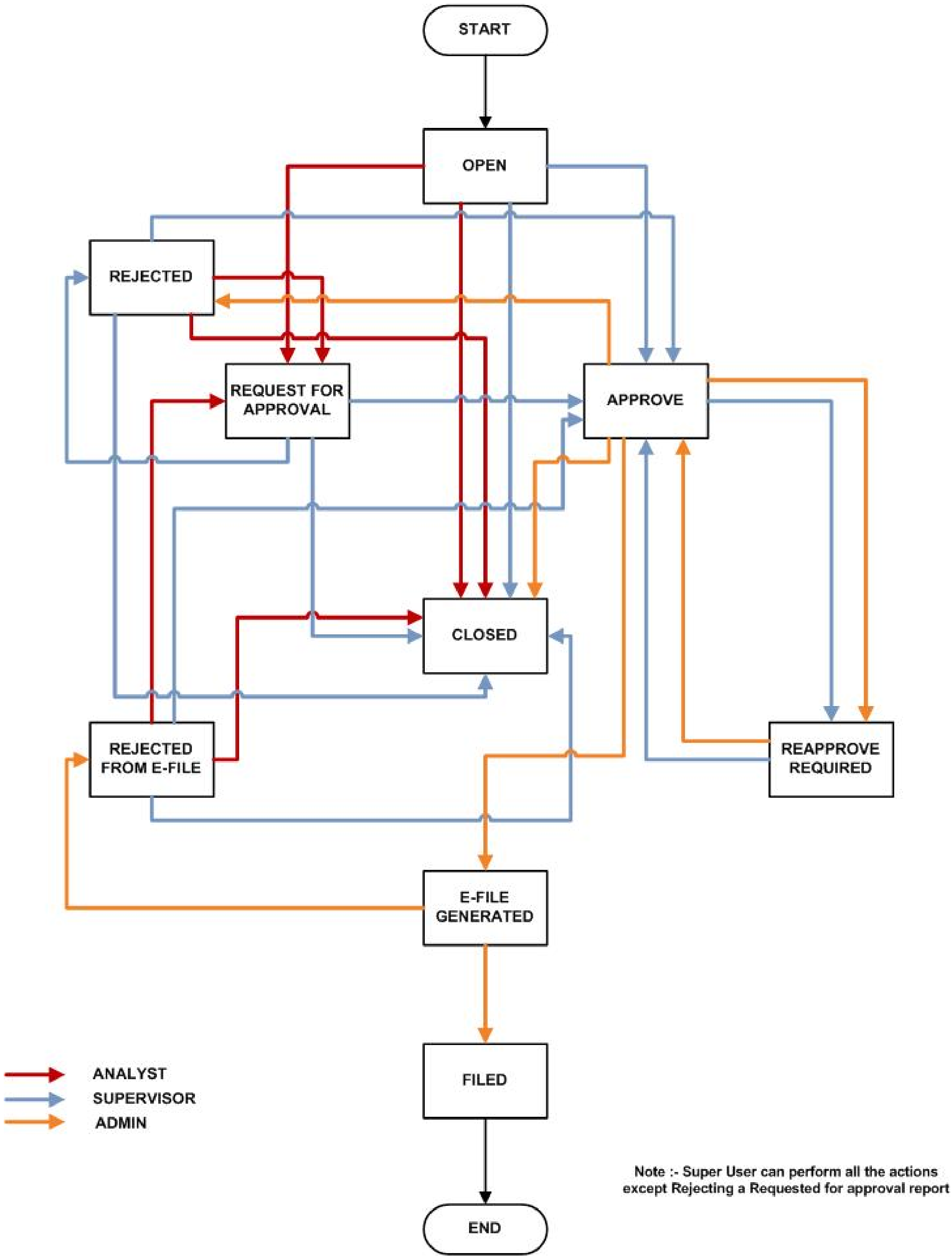
  If the report is rejected, then you must rework the report and submit the report for approval or you can close the report. If you close the report after being rejected, then the status of the report changes to closed. But if you choose to rework the report, then the status of the report changes to Request for Approval, which must be again validated and approved by authorized users. This process continues until the report is approved or closed. If there are any changes done to an approved report, the status of the report changes to Re- approve Required, which must be validated by authorized users.

  If you determine that a SAR report must not be filed, then you can close it. The Closed status removes it from the work queue and helps to distinguish it from those in a Filed status. If the report is closed, the report details cannot be edited, and the report is in View mode. For more information, see Filing Regulatory Reports.

2.2 User Workflow

The following figure illustrates the workflow of the OFS CRR CS USSAR Cloud Service:

Figure 2-1 OFS CRR CS USSAR Cloud Service Workflow



Every report generated in the USSAR Cloud Service can have various statuses.

The report has a life cycle, which begins with the Open status and ends when it is Closed/ Filed.

Table 2-1 Actions Performed by Various Users in Different Status

Status	Possible Action	Resulting Status	User Roles
Open	Request For Approval	Requested for Approval	Analyst or Super User
Open	Close	Closed	Analyst, Supervisor, or Super User
Open	Approve	Approved	Supervisor or Super User
Request for Approval	Approve	Approved	Supervisor or Super User
Request for Approval	Reject	Rejected	Supervisor
Request for Approval	Close	Closed	Supervisor or Super User
Approved	Re approve	Approved	Supervisor, Admin, or Super User
Approved	Reject	Rejected	Admin or Super User
Approved	Close	Closed	Admin or Super User
Approved	Generate E- File	E-File Generated	Admin or Super User
Rejected	Request For Approval	Requested for Approval	Analyst or Super User
Rejected	Close	Closed	Analyst, Supervisor, or Super User
Rejected	Approve	Approved	Supervisor or Super User
E-File Generated	File	Filed	Admin or Super User
E-File Generated	Reject	E-File Rejected	Admin or Super User
Rejected from E- File	Request For Approval	Requested for Approval	Analyst or Super User
Rejected from E- File	Approve	Approved	Supervisor or Super User
Rejected from E- File	Close	Closed	Analyst/Supervisor/ Super User
RE-Approve Required	Re-approve	Approved	Supervisor, Admin, or Super User

The report is in View mode in the following statuses:

- Closed
- E-file Generated
- Filed

You cannot edit report details when the report is in View mode. All action buttons are hidden in View mode.

Table 2-2 Status in Which Report Details are Editable by Different Users

Report Status	Analyst	Supervisor	Super User	Admin User
Open	X	X	X	
Request for Approval		X	X	
Approved		X	X	X

Table 2-2 (Cont.) Status in Which Report Details are Editable by Different Users

Report Status	Analyst	Supervisor	Super User	Admin User
Re-approve Required		X	X	X
Closed			X	X
Rejected	X	X	X	
E-file Generated				
Rejected from E-file	X	X	X	

To view report details, click the report name in the Regulatory Reports List Features. If the report is already opened by another user, the report-locked message displays.

3 Getting Started

This chapter explains the steps to log in to the OFS CRR CS US SAR application and provides a brief overview of the users and their roles.

3.1 User Access

This chapter provides different user roles in the OFS CRR CS US SAR Application.

Table 3-1 User Access

Actions	Analyst	Supervisor	Admin	Super User	Auditor
View Report	x	x			x
Edit Report	x	x		x	
Create New Report	x	x		x	
Request for Approval	x		x		
Approve Report		x		x	
Reject Report		x		x	
Close Report	x	x		x	
Edit Request for Approval Report		x		x	
Edit Approved Report		x	x	x	
Re-Approve Reports		x	x	x	
Reject Approved Reports			x	x	
Close Approved Reports			x	x	
Add Comments	x	x	x	x	x
Generate Draft PDF	x	x	x	x	
View Final PDF	x	x	x	x	
Reject E-File			x	x	
Generate E-File			x	x	
File E-File			x	x	
View / Edit Configuration					x

3.2 Accessing the OFS CRR RR US SAR Application

The OFS CRR US SAR application is qualified to run on Microsoft Edge Chromium or Google Chrome web browsers.

Your System Administrator provides the intranet address Uniform Resource Locator (URL), User ID, and Password to access the application. After your first login, you are prompted to change your password.

To access the OFS CRR CS US SAR application, follow these steps:

1. Enter the URL in the web browser using the following format:

   <Protocol>://<HostName>:<Port_Number >/crr/login <Enter a step example.>
2. The Transaction Monitoring Application login page is displayed.
3. Enter the login field details.

   Table 3-2 Login Fields

Fields	Description
User Name	Enter the unique identification of the user. You can enter up to twenty alphanumeric values.
Password	Enter the unique password of the user. You can enter up to twenty alphanumeric values.
4. Click **Sign in**. The **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service** landing page is displayed.
5. Click Compliance Regulatory Reporting in the Navigation List (LHS menu) and select USSAR. The United States Suspicious Activity Reporting Summary page is displayed.

3.3 Managing Preference

Thepreferences section enables you to set your OFS CRR default Home Page, time zone, and language.

To set the user preferences, follow thesesteps:

1. On the **Application** page, select Preferences from the **Application User** drop-down menu. The Preferences window is displayed.
2. Enter the required information in the **User Preference** fields.

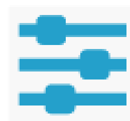
   Table 3-3 User Preference

Fields	Description
Start Page	Select the default page, which you want to display as your Home Page
Time Zone	Select the time zone you prefer from the Time Zone drop-down
Locale	Select the language you prefer from the Locale drop-down list. By default, it is US English
3. Click **Save** to update the preference.

4
Searching Reports

Use the Report Summary page to filter the list of reports that you want to open, view, analyze, and/or take action.

The types of search supported are Views, Basic Search, and Advanced Search. The Reports List pane displays the list of reports you have specified in the search parameters. Use the Summary page to perform the following search activities and view the results:

- **Basic Search**:This search is based on a limited set of search fields, such as Report Number and Report Name. This is the default search option. You can use either of them or both to narrow down the search.
- **Advanced Search**: This search is based on the ability to specify an additional set of fields to nar- row down your search results. Click Filter  to open the Advanced Search.
- **View**: This option helps you to quickly filter the reports based on pre-defined search queries. Select the search criteria from the View drop-down list and filter the list of reports.
- **Saving Views**: Use this option to save your search criteria as a View. The saved views are available in the View drop-down list.
- **Regulatory Reports List**: This is the list of reports that matches the search criteria provided.

4.1 Basic Search

The basic search is based on a limited set of search criteria and helps retrieve the required reports for your analysis. This search type is very useful if you know the report details such as report name and report number. Only those reports that match the criteria you specify are displayed.

To search for reports using basic search criteria, follow these steps:

1. Go to the **Report Summary** page. By default, the **Basic Search** option is displayed.
2. Enter the following information in the Basic Search pane as tabulated.

Table 4-1 Basic Search Fields

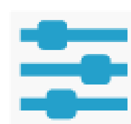
Fields	Description
Report ID	Enter one or more report IDs you want to search. For multiple report IDs, separate the report IDs with a comma (for example, 660, 671). Ensure that you do not enter a space after the comma. Report IDs are not case-sensitive. This overrides other filter criteria. For example, if you enter Report ID in search criteria, then this option overrides other details that you have entered previously in other search criteria such as Report Status, Jurisdiction, and so on.**NOTE**: You can enter a maximum of 50 numeric values in this field.
Report Name	Enter the report name you want to view. This field supports a wildcard search. You can use '%' and _ as wildcard indicators.NOTE: You can enter a maximum of 50 characters in this field

3. Click **Search** . Report or reports matching your search criteria are displayed.

4.2 Advanced Search

The advanced search offers an additional set of fields to the search report or reports provided with the Basic Search. This option helps you narrow down your search results. You can use combinations of these search criteria to quickly find the required reports.

To search for reports using advanced search criteria, follow these steps:

1. In the Summary Report page, click the **Advanced Search**  The Advanced Search window is displayed.

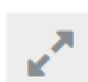
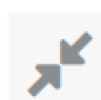
   Use the Expand  or Collapse  buttons to maximize or minimize the window.
2. Enter the following information in the Advanced Search window as tabulated. You can enter all the search fields or required fields. If you use more search fields, it will narrow down your search results.

Table 4-2 Advanced Search Fields

Fields	Description
Report ID	Enter one or more report IDs you want to search. For multiple report IDs, separate the report IDs with a comma (for example, 660, 671). Ensure that you do not enter a space after the comma. Report IDs are not case-sensitive. This overrides other filter criteria. For example, if you enter Report ID in search criteria, then this option overrides other details that you have entered previously in other search criteria such as Report Status, Jurisdiction, and so on.**NOTE**: You can enter a maximum of 50 numeric values in this field.
Report Name	Enter the report name you want to view. This field supports a wildcard search. You can use '%' and _ as wildcard indicators.NOTE: You can enter a maximum of 50 characters in this field
Report Status	Select one or more statuses from the drop-down list. For example, Approved, Reopened, and so on.
Reported Subject Name(s)	Enter the name of the subject(s) who reported. This field supports a wildcard search. You can use the '%' and '_' as wildcard indicators.
Case ID	Enter the Case ID to view reports associated with the specific Case ID. For multiple case IDs, separate them with a comma. Ensure you don't enter a space after the comma. For example, CA660, ca671. This overrides all other filter criteria. **NOTE**: This search is not case-sensitive. You can enter a maximum of 255 characters in this field. Case ID is the identifier that has triggered the creation of a report in the OFS CRR AUSMR application.
Types of Report	Select one or more types of reports from the drop-down list.
Last Modified By	Enter the customer or customer's name reported as subjects in the report. This field supports a wildcard search. You can use the '%' and '_' as wildcard indicators. Select the user who last modified the report. Use this criterion to view all the reports modified by the user. For example, Analyst1, Supervisor2, and so on.
Last Modified Date >=	Select the last modified date to view reports having a last modified date greater than or equal to the specified date. Using this criterion, you can view the reports modified during the date range. For example, reports modified on or after July 27, 2020 **NOTE**: You can either perform a range search using 'Last Modified Date >=' and 'Last Modified Date <=' or use them independently.

Table 4-2 (Cont.) Advanced Search Fields

Fields	Description
Last Modified Date <=	Select the Last Modified Date from the calendar to view reports having a last modified date lesser than or equal to the specified date. Using this criterion, you can view the reports modified during the date range. For example, reports were modified on or before July 27, 2020.
Approved By	Select the name of the approver to view reports approved by the selected user. For example, Supervisor1, Supervisor2, and so on.
Approved Date >=	Select the approved date to view reports having an approved date greater than or equal to the specified date. Using this criterion, you can view the reports approved during the date range. For example, reports approved on or after December 26, 2019.
Approved Date <=	Select the approved date from the calendar to view reports having an approved date lesser than or equal to the specified date. Using this criterion, you can view the reports that are approved during the date range. For example, reports are approved on or before December 26, 2019.
Submitted By	Select the name of the user or users to search for reports submitted by the selected user. For example, Analyst1, Analyst2, and so on.
Submitted Date >=	Select the submitted date to view reports having a submitted date greater than or equal to the specified date. For example, reports submitted on or after July 18, 2020.
Submitted Date <=	Select the submitted date to view reports having a submitted date lesser than or equal to the specified date. For example, reports submitted on or before July 18, 2020.
Created By	Select the user or users who have created the report.
Created Date >=	Select the created date to view reports having a created date greater than or equal to the specified date. Using this criterion, you can view the reports created during the date range. For example, reports were created on or after December 26, 2019. **NOTE**: You can either perform a range search using 'Created Date >=' and 'Created Date <=' or use them independently.
Created Date <=	Select the created date from the calendar to view reports having a created date lesser than or equal to the specified date. Using this criterion, you can view the reports created during the date range. For example, reports were created on or before December 26, 2019.

Table 4-2 (Cont.) Advanced Search Fields

Fields	Description
Jurisdiction	Select one or more jurisdictions to view reports mapped to the jurisdiction. **NOTE**: Jurisdictions are defined by your institution. Every report is associated with a jurisdiction. When a report is created from a case, the report inherits the jurisdiction that was associated with that case.
Due Date>=	Selectthe due date to view reports having a due date greater than or equal to the specified date. Using this criterion, you can view the reports that have a due date during the date range. For example, reports having a due date on or after December 26, 2019.
Due Date>=	Select the due date from the calendar to view reports having a due date lesser than or equal to the specified date. Using this criterion, you can view the reports that have a due date during the date range. For example, reports having a due date on or before December 26, 2019.
Account Number(s)	Enter the account or accounts involved in the STR. You can enter multiple account numbers by using a comma to separate the entries.

3. Click **Apply Filter**. The reports matching your search criteria are displayed on the Report Summary pageEnter the next step.

   To perform a different search, click the **Reset** button and enter your search criteria again
4. To save this search as Views, Click **Save As View**. The Save As View window is displayed
5. Enter View Name and Description
6. Click **Save** to add a new pre-defined view
7. Click **OK**. The view is saved and displayed in the *Views* drop-down list

> **Note:**
>
> The saved view is available only to the user who has created it, not to other users.

For example, if you regularly search for reports approved by Supervisor1 and reports approved on or before December 2019, you can pre-define a search as *SupDecember* under View. When you log in to the application next time, you need not enter all the search criteria again, select the pre-defined view as *SupDecember* and filter the reports.

4.3 View

Views search helps you quickly filter the reports based on pre-defined search queries. You can save your search criteria as Views. For more information on pre-defining the search as views, see Saving Views.

To search reports using the Views option, follow these steps:

1. On the **Summary** page, go to the View search option.
2. Select the pre-defined views from the View drop-down list. The Summary page refreshes to show the results matching the View search criteria.

> **Note:**
>
> The saved view is available only to the user who has created it, not to other users.

4.4 Regulatory Reports List

Use the Regulatory Reports section to view the list of reports based on your search criteria. Additional information on the reports is provided for analyses or take actions.

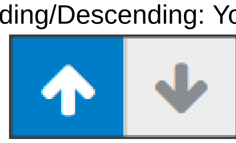
By default, all reports are displayed if you do not use any search criteria to filter the list.

4.4.1 Regulatory Reports List Features

The Reports List pane displays the list of all or specific reports you are looking for. You can select a report by clicking the corresponding Report ID link to view the details, investigate, and take action based on your role privileges.

> **Note:**
>
> If the report is already opened by another user, then that report is locked. You can only view that report.

The Reports List pane has the following User Interface (UI) controls.

- Sort Ascending/Descending: You can sort the Report List in ascending or descending order using  Ascending or Descending , respectively. By default, the Report List is in descend- ing order.
- Column Labels: The column labels provide you with the names of the columns. For example, Report Name, Report Type, and so on. This helps you to sort the information on the required report
- Tool Tip: A ToolTip that provides additional information is displayed when you position the cur- sor over a column label.
- Column Size: You can change the width of the column by dragging the column to right or left direction using the mouse or you can select the Resize Column option. To resize the column, right-click on the column. The Resize option is displayed.
- Click  arrow icons to decrease and  increase the size of the column or enter a number between 10 to 10,000 and click OK. The size of the column is updated based on your selection.

- Page Display: Use this option to modify the number of reports you want to view on a page (records per page) and also navigate back and forth between pages to view all reports in the Report List.
  To view a specific page, enter the page number, use arrow marks to go to the next or previous page, or click on the existing numbers such as 1, 2, 3, and so on to go directly to that page. The following table describes the column details.

Table 4-3 Column Name and Details

Column Name	Description
Report ID	The unique report identification number. This is a link to navigate to the Report Details page for further analysis.
Report Name	The name of the report.
Type of Report	The type of the report.
Case ID	The case ID associated with the report.
Created Date	The date when the report was created.
Subject Name	Name of the involved subject (person or entity).
Number of Subject	The count of the reported subject. It is the total number of subjects reported in the STR.
Count of Report Accounts	The count of the reported accounts. It is the total number of accounts involved in the STR. It will have both source and destination accounts.
Created By	The user who created the report.
Status	The status of the report. For example, Approved, Open, and so on. Based on the status you can open the Details page and take appropriate action on the report.
Jurisdiction	The jurisdiction to which the report is mapped. For example, AMEA, JAPAC, and so on. Jurisdiction over a territory relates to the geographic area over which the court has the authority to decide cases.
Draft Report	Click PDF to view the report details in PDF format.

5 Creating Reports

When a report is created in the OFS CRR CS US SAR application through the OFS Case Investigation application, the report details are auto-populated with information from the case, which triggered the action to generate the report. The newly created report is available in the OFS CRR CS US SAR application and it is assigned to a specific user with a due date to take appropriate action. These parameters are configurable.

When you identify a report of suspicious behavior that is not reported through the OFS Case Investigation application but want to report it to the regulator, you can manually create a new report using the Create New Report option in the OFS CRR CS US SAR application.

5.1 Update to OFS Case Investigation

When the OFS CRR CS US SAR application receives a report from the OFS Case Investigation application, it sends an acknowledgment to the OFS Case Investigation application when all the mandatory information is verified.

To send the acknowledgment, the OFS CRR CS US SAR Administrator must set the status to Y. If the status is set to N, the OFS CRR CS US SAR application does not send any status update to the OFS CRR Case Investigation application. By default, the AML STATUS UPDATE FLAG is set to Y. For more information on configuration, see the OFS CRR Case Investigation Administration Guide.

The following information is sent as a part of the acknowledgment:

- Case ID
- Acknowledgment Code – 0 (Meaning successful)
- Report ID (System Generated)
- Report Status
- In case of any error, the OFS CRR US SAR application sends a negative acknowledgment to the OFS CRR Case Investigation application. The error can be due to the following reasons:
  - User ID failure
  - Unsuccessful mandatory information verification
  - System or Application Error
  - The acknowledgment sent to the OFS Case Investigation application contains the following details:
  - Case ID
  - Acknowledgment Code: 1
  - Invalid User ID 2
  - Mandatory Information Missing 3
  - Format Failure System/Application Error
  - Error Description

> **Note:**
>
> If a case fails to complete the Generate Report action successfully, the failure is recorded in the Case Audit History.

5.2 Creating a Report Manually

When you identify a report of suspicious behavior that is not reported through the OFS Case Investigation application but want to report it to the regulator, you can manually create a new report using the Create New Report option in the OFS CRR CS US SAR application.

Only Analyst and Supervisor users can create a new report.

To create a new report from the OFS CRR US SAR application, follow these steps:

1. In the Report Summary page, click **Create Regulatory Report** . The Create Report window is displayed.
2. Enter the following information in the Create Report window as tabulated.

   Table 5-1 Creating a New Report fields

Fields	Description
Report Name	Enter the name for the new report.
Corrected Report	Select Yes or No from the drop-down to specify whether the report is corrected.
Internal Control/File Number	Enter the unique internal control or file number for the report to assign to FinCEN.
Report Type	Select the report type from the drop-down list. For example, AML_DD, AML_PAT, and so on.
Jurisdiction	Select the jurisdiction from the drop-down list.
Business Domain	Select the business domain from the drop-down list

3. Click **Save**. A confirmation message is displayed. The newly created report is available in the Report Summary List for further analysis and actions.

   A new report is created and the due date is set as per the number of days configured by your administrator in the static data table. The status of the new report is set to Open.

   > **Note:**
   >
   > The report details of a manually created report are not sent to the OFS Case Investigation application.

6 Analyzing Reports

To declare any report to be suspicious and report it to the FinCEN, you must view and assess the selected report and its details such as a filing institution, branches where the suspicious activity has occurred, the amount involved in the activity, type of suspicious activity (terrorist financing, fraud, and so on), subject (entity or person) associated with the suspicious activity. You must study narrations, documents, and audit history associated with the report before you take any type of action on the selected report. Use the Report Details page to view, analyze, and update the report information. You can add, delete, and modify the reports based on the status of the report and your user privileges. All the fields in the Regulatory Report Details tabs have numbers preceding the field labels. These numbers correspond to the numbers of the fields as they appear in the final FinCEN's SAR report that is used for discrete filing.

You must enter the report details in the tabs present in the Regulatory Report Details.

Topics:

- Accessing Report Details
- Filing Institution Information
- Financial Institution Where Activity Occurred
- Suspicious Activity Information
- Subject Information
- Documents
- Narrative
- Audit and Comments
- XSD Validation Details

6.1 Accessing Report Details

Use this section to access the Report Details page in the USSAR Cloud Service.

To access the Report Details page, follow these steps:

1. In the Report Summary page, click the required Report ID link. The Reports Details page is displayed. By default, the Reporting Information pane is displayed. To view the report details, click the More Details tab at the top of the page. The Reporting Context window is displayed. The Reporting Context window details Report Name, Report Status, Created By, and so on.
2. To collapse the Reporting Context window, click **Less Details**.

> **Note:**
>
> You must validate every tab before you move to the next tab. The tab color changes to green if the validation is successful else it will be yellow.

6.2 Filing Institution Information

Use the Filing Institution Information tab to view and update the report filing type, filing Institution information, financial institution identification type, and so on.

Topics:

- Reporting Information
- Filing Institution Information Details

6.2.1 Reporting Information

Use this pane to select the report filing type such as Initial Report, Correct/Amend Prior Report, Continuing Activity Report, and Joint Report.

To select the required report filing type, follow these steps:

1. On the Filing Institution Information tab. Go to the Reporting Information pane.
2. Select the report filing type.

Table 6-1 Report Filling Type fields and description

Fields	Description
Initial Report	Select Initial Report to submit the report to FinCEN for the first time.
Correct/ Amend Prior Report	Select Correct/Amend Prior Report to resubmit the report to FinCEN. This report was previously submitted, but after modification, it was resubmitted to correct the information provided earlier. **NOTE**: A corrected report must refer to the previously submitted report by the BSA ID of the previous report.

Table 6-1 (Cont.) Report Filling Type fields and description

Fields	Description
Continuing Activity Report	Select Continuing Activity Report to submit the report to FinCEN. This report is submitted to the regulator to report additional activities and to declare continuous behavior as related to one or more previously submitted reports on the same subject. A continuing report must be filed on suspicious activity that continues after an initial FinCEN SAR is filed. Financial institutions with SAR requirements may file SARs for continuing activity after a 90-day review, with the filing deadline being 120 days after the date of the previously related SAR filing. Financial institutions may also file SARs on continuing activity earlier than the 120-day deadline if the institution believes the activity warrants earlier review by law enforcement. Continuing reports must be completed in their entirety, including information about all subjects involved in the suspicious activity and all financial institutions where the activity occurred. The continuing report Part V narrative must include all details of the suspicious activity for the 90 days encompassed by the report, and only such data from prior reports as is necessary to understand the activity. Donot reproduce the narratives from prior reports in the continuing report. Provide both the dollar amount involved in the suspicious activity for the 90 days in Item 26 and the cumulative dollar amount for the current and all prior related reports in Item 28. If continuing losses are involved for any financial institution recorded in Part III, record the 90-day loss in Item 63 and the cumulative loss in Part V. **NOTE**: If a report is designated as a Continuing Activity report, then you must provide the BSA/DCN Number of the previously filed report along with the Total Cumulative Amount and Total Suspicious Amount. For example, • Total Cumulative Amount (Parent SAR Amount + Current CARamount) • Total Suspicious Amount is the Current CARAmount
Joint Report	Select Joint Report to submit the report to FinCEN. This report is filed by the current filing institution in collaboration with another financial institution.
Filing Institution Note to FinCEN	Enter the notes that you want to mention to FinCEN.

> **Note:**
>
> If you have selected the report as Joint Report and have not selected Initial Report or Correct/Amend Prior Report or Continuing Activity Report, then the system displays an error message.

6.2.2 Filing Institution Information Details

This pane provides details about the filing institution which is reporting the suspicious activity. There can be one or more filing institutions reporting the suspicious activity. Use this pane to view and update the filing institution associated with the report.

To view and update the filing institution information, follow these steps:

1. On the Filing Institution Information tab. Go to the Filing Institution Information pane.
2. Update the filing institution information.

Table 6-2 Filing Institution Information fields details.

Fields	Description
Filing Institution Name	Select the filing institution name from the drop-down list.
Filing Institution Name	NOTE: All the related fields are displayed based on the filing institution name selected. If details in the drop-down are not displayed, then you must contact your Administrator.
Primary Federal Regulator	The primary federal regulator of the financial institution where the activity occurred as well as the filing institution.
TIN Type	The TIN (Taxpayer Identification Number) type. For example, Social Security Number (SSN), Individual Taxpayer Identification Number (ITIN, and so on.
TIN	The TIN (Taxpayer Identification Number).
Type of Financial Institution	The type of financial institution. For example, Securities or Futures, loans or Finance Companies, Housing, and so on.
Other Description	Additional information about the type of financial institution.
Type of Securities and Futures Institution	The type of securities and futures institution. For example, Clearing broker, Futures commission merchant, Holding company, Introducing broker, and so on.
Other Description	Additional information about the type of securities and futures institution.
Financial Institution ID	The unique identification number of the financial institution involved in suspicious activity.
Financial Institution Identification Type	The financial institution identification type. For example, Central Registration Depository (CRD) number, Investment Adviser Registration Depository (IARD) number, National Futures Association (NFA) number, Research, Statistics, Supervision, and Discount (RSSD) number, and so on.
Alternate Name	The alternate name of the financial institution. AKA if an individual; doing business as (DBA) or trade name if entity.
Address	The address of the financial institution.

Table 6-2 (Cont.) Filing Institution Information fields details.

Fields	Description
City	The city where the financial institution is located.
State	The state where the financial institution is located.
Postal Code	The postal code of the financial institution.
Country	The country where the financial institution is located.
Filing Institute Contact Office	The filing institution's contact office name.
Filing Inst Contact Number	The filing institution's contact number.
Extension	Enter or modify the extension contact number of the filing institution.
Internal Control/File Number	Enter the internal control/file number. **NOTE**: This is the Case ID if the reports are auto-generated from Case Investigation Cloud Service. For manually created reports, you have the option to provide an internal control or file number to the new report.
Prior Report Doc Number	Enter the prior report document number. This number refers to the unique identifier assigned to a report that is submitted to FinCEN. This field is applicable when filing a continuing activity, corrected, or supplemental report on a previously submitted report. Select the unknown check box if the prior report document number is unknown. **NOTE**: • If the Prior Report Doc Number is not entered for Corrected, Supplemental, and Continuing Reports, nor if the Unknown check box field has been marked, the application displays an error message. • Ifyou have entered one or more prohibited words in the fields Filling Institution Contact Office and Prior Report Doc Number, then the application displays the following message: You are not allowed to enter prohibited words in Filling Institution Contact Office and Prior Report Doc Number. The following words are prohibited: AKA, COMPUTER GENERATED, CUSTOMER, DBA, NON CUSTOMER, NONE, NOT APPLICABLE, OTHER, SAME, SAME AS ABOVE, SEE ABOVE, SEE NARRATIVE, SIGNATURE CARD, T/A, UNKNOWN, VARIOUS, XX.

3. Click **Validate** to authenticate the information present in both the Reporting Information pane and the Filing Institution Information pane.

> **Note:**
>
> If you have not entered the correct information, an error message is displayed, and the color of the tab changes to Yellow. If your information is correct, then the color of the tab changes to Green.

4. Click **Save**. A confirmation message is displayed.

6.3 Financial Institution Where Activity Occurred

The Financial Institution Where Activity Occurred tab captures the details of the financial institution where the suspicious activity has occurred and also the associated branches of the financial institutions that are involved in the suspicious activity. This facilitates you to have more insight into the financial institution associated with the selected report and get more information such as the type of financial institution, the loss incurred due to suspicious activity, the role of the financial institution in suspicious activity, and so on.

Use this pane to view, add, edit, or delete the details of the financial institution where the activity occurred.

Topics:

- Managing Financial Institution Where Activity Occurred
- Adding a Financial Institution Where Activity Occurred

6.3.1 Managing Financial Institution Where Activity Occurred

Use this pane to view the list of the financial institution associated with the selected report. You can also use this pane to modify and delete financial institutions.

To view, modify, or delete a financial institution where the activity occurred, follow these steps:

1. (On the Reports Details page, click the Financial Institution Where Activity Occurred details tab. The list of Financial Institution Where Activity Occurred associated with the selected report is displayed.
2. To view or modify the required Financial Institution details, select the required Record Number, and click **Edit** . The Financial Institution Where Activity Occurred window is displayed.
3. Modify the required details.
4. Click **Validate** to authenticate the information and click Save. A confirmation message is displayed.
5. To remove the Financial Institution Where Activity Occurred associated with the report, select the required Record Number and click **Delete** . The Financial Institution Where Activity Occurred associated with the report is deleted from the list.

6.3.2 Adding a Financial Institution Where Activity Occurred

Use this pane to add a new financial institution where the activity occurred, along with the branch details.

To add a new financial institution where the activity occurred, follow these steps:

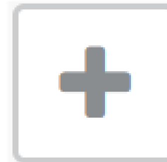
1. On the Financial Institution Where Activity Occurred list pane, click **Add**  .
   The Financial Institution Where Activity Occurred Details window is displayed.
2. Enter the following information in the Financial Institution Where Activity Occurred Details window.

Table 6-3 Financial Institutions Where Activity Occurred fields and description.

Fields	Description
Loss to Financial Institution	Enter the loss incurred due to the suspicious activity. This indicates the loss to the financial institution because of the suspicious activity. **NOTE**: The amount entered in this field cannot be zero and cannot be greater than the amount in the Amount involved in this report field.
Role	Enter the role of the financial institution in suspicious activity. These are values defined by FinCEN. Role refers to the role played by the institution in the suspicious activity when certain product types, instruments, or payment mechanisms were used in the activity. The Role is a drop-down list with the following options: • Paying Location: Select this option if the financial institution has played the role of Paying Location if the customer received payment from the institution for the products or instruments recorded on the SAR. • Selling Location: Select this option if the financial institution has played the role of Selling Location if the customer purchased products or instruments from the institution. • Both A and B: You must select Both A and B if the financial institution was both a paying and selling location for the products or instruments recorded on the SAR.
Legal name of the Financial Institution	Select the legal name of the financial institution from the drop-down list. NOTE: All the subsequent fields are displayed based on the name you select, and they are non-editable.
Alternate Name	The alternate name of the financial institution.
Type of Financial Institution	The type of financial institution. For example, Depository Institution, Insurance company, Securities or Futures, and so on.
Other Description	Additional information about the type of financial institution.
Financial Institution Code	The financial institution code. For example, Central Registration Depository (CRD) number, Investment Adviser Registration Depository (IARD) number, National Futures Association (NFA) number, and so on.

Table 6-3 (Cont.) Financial Institutions Where Activity Occurred fields and description.

Fields	Description
Primary Federal Regulator	The primary federal regulator. Typically, this is the state or federal regulatory agency that is the primary supervising entity of a financial institution.
Financial Institution ID Type	The financial institution's unique identification type.
Financial Institution ID Number	The financial institution ID number.
TIN	The TIN (Taxpayer Identification Number) number.
TIN Type	The TIN (Taxpayer Identification Number) type. For example, Social Security Number (SSN), Individual Taxpayer Identification Number (ITIN, and so on.
Type of Gaming Institute	The type of gaming institute. For example, Chip walking, Minimal gaming with large transactions, Suspicious use of counter checks or markers, and so on.
Other Description	Additional information about the type of gaming institute.
Type of Securities and Futures Institution	The type of securities and futures institution. For example, Investment adviser, Investment company, Retail foreign exchange dealer, and so on.
Other Description	Additional information about the type of securities and futures institution.
Address	The address of the financial institution where the suspicious activity occurred.
City	The city of the financial institution involved in the suspicious activity.
State	The state of the financial institution involved in the suspicious activity.
Postal Code	The postal code of the financial institution.
Country	The country of financial institution.

6.4 Branch Information

When there are one or more branches involved in suspicious activity for the selected financial institution, use this pane to manage existing branches or add new branches. But it is mandatory to mention the involvement of the branch in the suspicious activity for the selected financial institution. If no branch is involved, you have to specify.

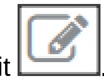
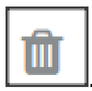
Topics:

- Managing Branch Details
- Adding a New Branch

6.4.1 Managing Branch Details

Use this pane to view the list of branches of the financial institution associated with the selected report. You can also use this pane to modify and delete branches of financial institutions.

To view, modify, or delete a branch information, follow these steps:

1. On the Financial Institution Where Activity Occurred Details pane, go to the Branch Information pane.
2. To modify the branch details, select the required Record Number and click Edit . The Branch Details pane is displayed.
3. Modify the required details.
4. Click Validate to authenticate the information and click Save. A confirmation message is displayed.
5. To remove the branch involved in suspicious activity, select the required Record Number, and click Delete . The Branch is deleted from the list.

6.4.2 Adding a New Branch

Use this pane to add a new branch to the selected financial institution involved in the suspicious activity.

> **Note:**
>
> If there is no branch involved in the suspicious activity, then select 'If no branch involved'. It is mandatory to either select the 'If no branch involved' check box or add a new branch to the report.

To add a new branch details, follow these steps:

1. On the Branch Information pane, click **Add** . The Branch Details window is displayed.
2. Enter the branch details.

Table 6-4 Branch Details fields and description

Fields	Description
Role	Select the role of the financial institution branch in suspicious activity. These are values as defined by FinCEN. Role refers to the role played by the institution in the suspicious activity when certain product types, instruments, or payment mechanisms were used in the activity. The Role is a drop-down list with the following options: • Paying Location: Select this option if the branch has played the role of Paying Location if the customer received payment from the institution for the products or instruments recorded on the SAR. • Selling Location: Select this option if the branch has played the role of Selling Location if the customer purchased products or instruments from the institution. • Both A and B: You must select Both A and B if the branch was both a paying and selling location for the products or instruments recorded on the SAR. **Note:** Based on the branch code and the role you select, the rest of the fields are displayed
Address	The address details of the branch.
City	The city where the branch is located.
State	The state where the branch is located.
Postal Code	The zip code where the branch is located.
Country	The country where the branch is located.
RSSD ID Number	The RSSD number of the branch. The RSSD ID number is a unique identifying number assigned by the Federal Reserve for all financial institutions, main offices, and branches. RSSD specifically refers to the assigned identifier for Research, Statistics, Supervision, and Discount identification numbers.

3. Click **Save**. A confirmation message is displayed, and a new branch is added to the report.

6.5 Suspicious Activity Information

The Suspicious Activity Information tab lists all the suspicious activities, such as activity classification, law enforcement agency details, and so on. Use this pane to view, modify, and add related details.

Topics:

- Suspicious Activity Details
- Suspicious Activity Classification
- Law Enforcement Agency Details
- Additional Information

6.5.1 Suspicious Activity Details

Use this pane to modify existing details of suspicious activity such as activity date, the amount involved, and so on for the selected report, or you can also add new suspicious activity. This is a default pane in the Suspicious Activity Information tab.

To modify or add suspicious activity details, follow these steps:

(Optional) <Describe the prerequisites.>

1. On the Regulatory Report Details page, click the Suspicious Activity Information tab. By default, the Suspicious Activity Details pane is displayed.
2. Enter the Suspicious Activity Details fields.

Table 6-5 Suspicious Activity Details

Fields	Description
Activity Date From	Enter the date on which the suspicious activity started. **Note:** You must enter a date later or equal to 1 January 1950.
To	Enter the date on which the suspicious activity ended. **Note:** NOTE: To Date must be greater than Activity Date From.
Amount	Enter the amount involved in the suspicious activity. **Note:** The amount entered in the Amount field must be less than the cumulative amount. The amount of value must be more than '0'.
Cumulative Amount	Enter the cumulative amount involved in suspicious activity. If the cumulative amount is unknown or there is no cumulative amount involved, then enter '0'. Cumulative Amount must be populated only if the report is a Continuing Activity Report. **Note:** The cumulative amount must not be blank.

Table 6-5 (Cont.) Suspicious Activity Details

Fields	Description
Amount Unknown/no Amount	Select the Amount unknown or no amount involved from the drop-down list. • Select Amount unknown if the amount involved in suspicious activity is unknown. • Select No amount involved if there is no amount involved in the suspicious activity. **Note:** You must enter the amount in the 'Amount' field or select 'Amount unknown' or 'No amount involved'.

3. Click the Validate button to verify the information on the current pane. Click the Validate Tab button to verify the information for all the panes on this tab.

> **Note:**
>
> If you click on Request for Approval and if the details are not valid, then the application displays an error message.

4. Click **Save**. A confirmation message is displayed.

6.5.2 Suspicious Activity Classification

Use this pane to specify the type of suspicious activity such as Fraud, Terrorist Financing, Insurance, and so on.

To specify the type of suspicious activity, follow these steps:

1. On the Suspicious Activity Information tab, select Suspicious Activity Classification. The Suspicious Activity Classification pane is displayed.

   The Activity Classification has the following classification categories:

   - Structuring
   - Terrorist Financing
   - Fraud (Type)
   - Gaming Activities
   - Money Laundering
   - Identification/Documentation
   - Other Suspicious Activities
   - Insurance
   - Securities/Futures/Options
   - Mortgage Fraud
   - Cyber Events

- Were any of the following product type(s) involved in the suspicious activity?
- Were any of the following instrument type(s)/payment mechanism(s) involved in the suspi- cious activity?
- Within each category, there are options such as Structuring, Terrorist Financing, and so on to select specific behavior to indicate suspicious activity.

2. Review these options within each category and select one or more activities to report.
3. Select Other from the activity classification list if above-mentioned activities are not relevant and enter the description of the activity classification.
4. Click **Save**. All the details in the Activity Classification pane are saved.

> **Note:**
>
> - If you click the Validate button and you have marked Other in any of the fields in the Activity Classification section without entering any description, then the application displays an error message.
> - If you have marked Other in Instrument Type/Payment Mechanism Involved, Product type, Mortgage fraud, Securities/futures/options, Insurance, Identification, Money laundering, Gaming Activity, Structuring, Cyber Events activity, and have not provided any description, then the application displays an error message.
> - If you click the Validate button and if the information in the Activity Classification section is not correct, then the application displays an error message.

6.5.3 Law Enforcement Agency Details

Financial Institutions contact the Law Enforcement (LE) agency to inform about suspicious activity. Use this pane to update the LE details.

To update the LE details, follow these steps:

1. On the Suspicious Activity Information tab, select Law Enforcement Agency Details. The Law Enforcement Agency Details pane is displayed.
2. Enter the Law Enforcement Agency fields.

Table 6-6 Law Enforcement Agency Details

Fields	Description
LE Contact Agency	Enter the name of the law enforcement contact agency.
LE Contact Name	Enter the law enforcement contact person's name. NOTE: Do not use prohibited words such as AKA, COMPUTER GENERATED, CUSTOMER, DBA, NON CUSTOMER, NONE, NOT APPLICABLE, OTHER, SAME, SAME AS ABOVE, SEE ABOVE, SEE NARRATIVE, SIGNATURE CARD, T/A, UNKNOWN, VARIOUS, XX. NOTE: Enter up to 150 characters.
Contact Number	Enter the phone number of the law enforcement agency.
Extension	Enter the phone extension number of the law enforcement agency.

Table 6-6 (Cont.) Law Enforcement Agency Details

Fields	Description
LE Contact date	Select the date on which the law enforcement agency was contacted.

3. Click the **Validate** button to verify the information.
4. Click **Save**. A confirmation message is displayed. . A confirmation message is displayed.

6.5.4 Additional Information

Use this pane to update additional information such as IP address, cyber event details, and so on used in this suspicious activity.

Topics:

- IP Address Details
- Cyber Event Details
- Additional Information Details

6.5.4.1 IP Address Details

Use this pane to update the existing IP address to the selected report.

To manage the IP address, follow these steps:

1. On the Additional Information pane, go to the IP Address Details pane.
2. To modify the required IP address details, select the required Record Number, and click **Edit** . The IP Address Details window is displayed.
3. Modify the IP address details.
4. Click **Save**. A confirmation message is displayed.
5. To remove the IP address associated with the report, select the required Record Number and click Delete . The IP address associated with the report is deleted from the list.
6. To add a new IP address, On the IP Address Details pane, click **Add** . The IP Address Details window is displayed.
7. Enter the IP address fields.

Table 6-7 IP Address Details

Fields	Description
IP Address	Enter the IP address details.
Activity Date	Enter the date of suspicious activity.

Table 6-7 (Cont.) IP Address Details

Fields	Description
Activity Time	Enter the time of suspicious activity.

8. Click **Save**. A confirmation message is displayed, and a new IP address is added to the list.

> **Note:**
>
> - If the IP address is IPv4, use a variation of the format nnn.nnn.nnn.nnn (n = number) with periods between the segments. The first set of numbers must be valued between 1-255 (inclusive). The second, third, and fourth sets of numbers must be valued between 0-255 (inclusive).
> - If the IP address is IPv6, use a variation of the format cccc:cccc:cccc:cccc:cccc:cccc:cccc:cccc (c = character, IPv6 is alphanumeric in some segments) with colons between the segments.

6.5.4.2 Cyber Event Details

Use this pane to provide the cyber event types used in this suspicious activity.

To manage Cyber Event Details , follow these steps:

1. On the Additional Information pane, go to the Cyber Event pane.
2. To modify the required cyber event details, select the required Record Number, and click Edit . The Cyber Event window is displayed.
3. Modify the cyber event details.
4. Click **Save**. A confirmation message is displayed.
5. To remove the cyber event associated with the report, select the required Record Number, and click **Delete** . The cyber event associated with the report is deleted from the list.
6. To add a new cyber event, On the Cyber Event pane, click **Add** . The Cyber Event Details window is displayed.
7. Enter the cyber event fields.

Table 6-8 Cyber event

Fields	Description
Cyber Event Type	Select the cyber event type from the drop-down list. For example, Command and Control, Suspicious IP Addresses, and so on.
Cyber Event Description	Enter the cyber event description.
Other Description	Enter the additional description.
Activity Date	Enter the date of suspicious activity.
Activity Time	Enter the time of suspicious activity.

8. Click **Save**. A confirmation message is displayed, and a new cyber event is added to the list.

Note:

- The value provided must adhere to the following requirements: 4000 characters or less; must be in the following format based on these specific types of cyber events:? Command and Control/Suspicious IP Addresses:
- If the IP address is IPv4, use a variation of the format nnn.nnn.nnn.nnn (n = number) with periods between the segments. The first set of numbers must be valued between 1-255 (inclusive); the second, third, and fourth set of numbers must be valued between 0-255 (inclusive).
- If the IP address is IPv6, use a variation of the format cccc:cccc:cccc:cccc:cccc:cccc:cccc:cccc (c = character, IPv6 is alphanumeric in some segments) with colons between the segments.
- URL/Domain names: Must contain at least one period, no spaces, cannot begin or end with a dash.
- Media Access Control (MAC) Addresses: Must be in the XX:XX:XX:XX:XX:XX format.
- Email Addresses: Must contain @ symbol and at least one period following the @ symbol

6.5.4.3 Additional Information Details

Use this pane to update the attributes of the assets (commodity, product, or instrument) that are involved in the suspicious activity.

To manage the additional information details, follow these steps:

1. On the Additional Information pane, go to the Additional Information sub- pane.
2. To modify the required additional information, select the required Record Number, and click **Edit** . The Additional Information window is displayed.
3. Modify the required additional information.
4. Click **Save**. A confirmation message is displayed.
5. To remove the additional information associated with the report, select the required Record Number, and click **Delete** . The additional information associated with the report is deleted from the list.
6. To add additional information, On the Additional Information pane, click **Add** . The Additional Information window is displayed.
7. Enter the additional information fields

Table 6-9 Additional Information

Fields	Description
Additional Information Type	Select the additional information type from the drop-down list. For example, commodity type, the market where it was traded, commodity, product or instrument, and so on.
Description	Enter the additional information type description.

8. Click **Save**. A confirmation message is displayed, and additional information is added to the list.

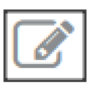
> **Note:**
>
> - You cannot edit the report details when the report is in View mode. Action buttons, such as Save and Reset, are hidden in the Activity Classification pane when the report is in View mode.
> - You cannot edit the report details when the report is in View mode. Action buttons, such as Save and Reset are hidden in the Law Enforcement Agency Details when the report is in View mode.
> - You cannot edit the report details when the report is in View mode. Action buttons, such as Add, Edit, and Delete are hidden in the Additional Information grid when the report is in View mode.

6.6 Alternate Name Details

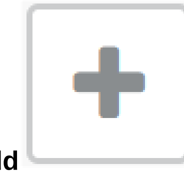
An alternative name facilitates identifying other names (alias) used by the subject (person or entity) in the involved suspicious activity. You can add up to 99 alternate names to the selected subject. Use this pane to view, modify, and delete the existing alternate names associated with the subject.

Use this pane to view the list of alternative names associated with the selected subject. You can modify the details of the alternative names and also delete them from the list.

To manage the alternative names, follow these steps:

1. On the Subject Information pane, go to the Alternate Name pane. The list of alternative names is displayed.
2. To modify the required alternate name, select the required Record Number, and click **Edit** . The Alternate Name window is displayed.
3. Modify the required alternative name details.
4. Click **Save**. A confirmation message is displayed.
5. To remove the alternative name associated with the subject, select the required Record Number and click **Delete** . The alternate name associated with the subject is deleted from the list.
6. Click **Validate** to authenticate the information that is present in the Alternate Name pane.

> **Note:**
>
> You are not allowed to add alternative names if you have selected 'Is critical information unknown?' in the Subject Information pane.

7. To add a new alternate name, on the Alternate Name pane, click **Add**  . The Alternate Name window is displayed.

> **Note:**
>
> You are not allowed to add alternative names if you have selected 'Is critical information unknown?' in the Subject Information pane.

8. Enter the alternate name.
9. Click **Save**. A confirmation message is displayed, and a new alternate name is added to the list.

> **Note:**
>
> - You can enter up to 150 characters for an alternate name.
> - You must not use prohibited words such as AKA, computer- generated, customer, DBA, Non-customer, none, not applicable, other, same, same as above, see above, see narrative, signature card, T/A, unknown, various, and so on.

6.7 Subject Information

A subject (individual or entity) can be a purchaser, sender, payee, or receiver. The Subject Information tab lists information related to the subject, accounts associated with the subject, and the subject's relationship with the financial institution. A maximum of 999 subject records can be added to one report or suspicious activity.

Use this pane to add a new subject to the selected report and modify or delete the existing subject from the report. **Topics**:

- Subject Details
- Address
- Subject Phone
- Form of Identification
- Alternate Name Details
- Email Address
- Website (URL) Address
- Account Information
- Relationship with Financial Institution

6.7.1 Subject Details

The Subject Details pane provides more information on the name, address, location of the person, or entity involved in the suspicious activity. Use this pane to view, modify, and delete the existing subject associated with the report. You can also add a new subject to the selected report.

Use this pane to view the list of subjects associated with the selected report. You can modify the subject details and also delete the subjects from the list.

To manage the subject, follow these steps:

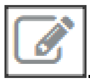
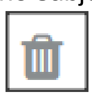
1. On the Reports Details page, click the **Subject Information** tab. The list of subject information associated with the selected report is displayed.
2. To modify the required subject details, select the required Record Number, and click **Edit** . The Subject Details pane is displayed.
3. Modify the required details.
4. To remove the subject associated with the report, select the required Record Number, and click **Delete** . The subject associated with the report is deleted from the list.
5. To add a subject, On the Subject Information tab, click **Add** . The Subject Details pane is displayed.
6. Enter the subject details fields

Table 6-10 subject details

Fields	Description
Is critical information unknown?	Select this check box if all the critical information about the subject is unavailable. Critical information is as follows: • Last Name or EntityName • FirstName • TIN • DOB (date of birth) • Address • Identification
Is subject an Entity	Select this check box if the subject is an entity (institution). **NOTE**: The fields such as first name, middle name, suffix, gender, date of birth, and so on are disabled on the selection of this check box.
Last Name/Entity Name	Enter the last name of the person or entity name or select the Unknown check box if you do not know the last name.
Middle Name	Enter the subject’s middle name.
First Name	Enter the subject’s first name or select the Unknown check box if you do not know the first name.

Table 6-10 (Cont.) subject details

Fields	Description
Suffix	Enter the subject suffix.
DOB	Enter the subject's date of birth or select the Unknown check box if you do not know the date of birth.
Gender	Enter the subject's gender.
TIN	Enter the subject TIN or select the Unknown check box if you do not know the TIN.
TIN Type	Enter the subject TIN type.
NAICS Code	Select the NAICS code from the drop-down list. The North American Industry Classification System (NAICS) is used by businesses and government to classify and measure economic activity in Canada, Mexico, and the United States. The NAICS numbering system is a six-digit code. The first five digits are generally the same in all three countries. The first two digits designate the largest business sector. The third digit designates the sub-sector, the fourth digit designates the industry group, the fifth digit designates particular industries and the last digit designates national industries.
Occupation/Type of Business	Enter the occupation or business type of the subject.
Corroborative Statement Received	Select whether the corroborative statement is received. As per FinCEN, a corroborative statement is where the subject has made a statement to the filing institution admitting to the involvement or otherwise substantiating the suspicious activity. If such a statement was made, you must select Yes. If not, select No. If you select Yes, then the nature of that statement must be captured in the report Narrative. **NOTE**: If you click Save without selecting any value in this field, then the application displays the following message: You have not selected any value for Corroborative Statement Received for Suspect ID- <Suspect ID>.
Subject role	Select the role of the subject in the suspicious activity from the drop-down list. • **Purchaser/Sender**:If the subject purchased, sent the instruments or products involved in the suspicious activity, then they are considered to have played the role of Purchaser/Sender. • **Payee/Receiver**: If the subject received the instruments or productsinvolved in suspicious activity, then they are considered to have played the role of the Payee/Receiver. • **Both A and B**: Select this option if the subject acted as both purchaser/Sender andPayee/Receiver.

7. Click **Validate** to authenticate the information present in the Subject Details pane.

> **Note:**
>
> - If Is critical information unknown? is unchecked and you have not entered information for at least one critical field or have not checked all of the subject information associated with Unknown check boxes, then an error message is displayed.
> - If you add or edit the subject details and select Is critical information unknown? Check box after entering information in one or more critical fields, then an error message is displayed.
> - If you select the Critical Information Unknown check box, you will not be able to add the subject address and identification details, and an error message is displayed.
> - In the Subject Information tab, if you click on the Validate button and if there are no records present in Address, Alternate Name, Phone, Email, Website, and Accounts grid, then the application displays an error message.

6.7.2 Address

The address helps identify the location of the subject (person or entity) involved in the suspicious activity. Use this section to view, modify, and delete the existing address associated with the report. You can also add a new address to the selected report. Use this pane to view the list of subject addresses associated with the selected report. You can modify the address details and also delete the address from the list.

To manage the subject's address, follow these steps:

1. On the Subject Information pane, go to the Address pane. The list of addresses associated with the subject is displayed.
2. To modify the required address details, select the required Record Number, and click **Edit** . The Address Details pane is displayed.
3. Modify the required details.
4. To remove the address associated with the report, select the required Record Number, and click **Delete** . The address associated with the report is deleted from the list.
5. Click **Validate** to authenticate the information that presents in the Address pane.
6. To add a new subject address, on the Address pane, click Add . The Subject Address Details window is displayed.

> **Note:**
>
> You are not allowed to add an Address if you have selected 'Is critical information unknown?' in the Subject Information pane

7. Enter the subject address details fields.

Table 6-11 Subject address details

Fields	Description
Address	Enter the address of the subject. **NOTE**: You can enter up to 100 characters.
City	Enter the city of the subject. **NOTE**: You can enter up to 50 characters.
Country	Select the country of the subject from the drop-down list.
State	Select the state of the subject from the drop-down list.
Zip/Postal Code	Enter the zip or postal code of the subject's location. **NOTE**: • For the US, the postal code must contain onlynumbers, either 5 or 9 in length. • For the US, the postal code must not end with 0000and 9999.

8. Click **Save**. A confirmation message is displayed, and a new address is added to the list.

6.7.3 Subject Phone

Phone details facilitate to identification numbers used by the subject (person or entity) in the suspicious activity. Use this section to view, modify, and delete the existing phone associated with the report. You can also add a new phone to the selected report.

Use this pane to view the list of subjects' phones associated with the selected report. You can modify the phone details and also delete them from the list.

To manage the subject's phone, follow these steps:

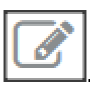
1. On the Subject Information pane, go to the Phone pane. The list of phone numbers is displayed.
2. To modify the required phone details, select the required Record Number, and click **Edit** . The Subject Phone Details window is displayed.
3. Modify the required details.
4. Click **Save**. A confirmation message is displayed.
5. To remove the phone associated with the report, select the required Record Number and click **Delete** . The phone associated with the report is deleted from the list.
6. Click **Validate** to authenticate the information present in the Phone pane.
7. To add a new subject phone , On the Address pane, click **Add** . The Subject Phone Details window is displayed.
8. Enter the subject phone fields.

Table 6-12 Subject Phone Details

Fields	Description
Phone Number	Enter the phone number of the subject. **NOTE**: You can enter up to 16 numeric values only.
Extension	Enter the extension of the subject's phone number, if any. **NOTE**: You can enter up to 6 numeric values only.
Type	Select the type of phone from the drop-down list. For example, mobile, home, office, and so on.

9. Click **Save**. A confirmation message is displayed, and a new phone is added to the list.

6.7.4 Form of Identification

The subject form of identification is the driving license, passport, and so on used in the suspicious activity by the subject. Use this pane to view, modify, and delete the existing form of identification associated with the report. You can also add a new identification to the selected report.

Use this pane to view the list of subject forms of identification associated with the selected report. You can modify the subject form of identification details and also delete them from the list.

To manage the subject form of identification, follow these steps:

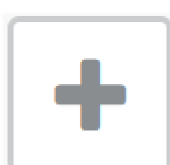
1. On the Subject Information pane, go to the Form Identification pane. The list of the subject forms of identification is displayed.
2. To modify the required subject form of identification details, select the required Record Number, and click **Edit** . The Subject Form of Identification window is displayed.
3. Modify the required details.
4. Click **Save**. A confirmation message is displayed.
5. To remove the subject form of identification associated with the report, select the required Record Number, and click **Delete** . The subject form of identification associated with the report is deleted from the list.
6. Click **Validate** to authenticate the information that is present in the Subject Form of Identification pane.
7. To add a new subject form of identification, On the Form Identification pane, click **Add** . The Subject Form of Identification Details window is displayed.
8. Enter the subject form of identification fields.

Table 6-13 Form of identification

Fields	Description
Identification Type	Select the identification type from the drop-down list. For example, Passport, Alien Registration, Driver's license, state ID, and so on.
Other	Enter another type of identification if you have not selected it in the previous field. **NOTE**: Enter up to 50 characters.
Identification Number	Enter a unique identification number. **NOTE**: Enter up to 24 alpha-numeric characters.
Country	Select the country to which the identification type belongs to.
State	Select the state to which the identification type belongs to.

9. Click **Save**. A confirmation message is displayed, and a new subject identification is added to the list.

Note:

- If you select the Unknown check box when a report already contains one or more identification details, the application displays an error message.
- If you try to add new identification details when you have already selected the Unknown check box, the application displays an error message.

6.7.5 Alternate Name Details

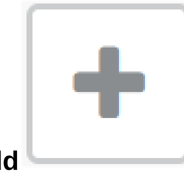
An alternative name facilitates identifying other names (alias) used by the subject (person or entity) in the involved suspicious activity. You can add up to 99 alternate names to the selected subject. Use this pane to view, modify, and delete the existing alternate names associated with the subject.

Use this pane to view the list of alternative names associated with the selected subject. You can modify the details of the alternative names and also delete them from the list.

To manage the alternative names, follow these steps:

1. On the Subject Information pane, go to the Alternate Name pane. The list of alternative names is displayed.
2. To modify the required alternate name, select the required Record Number, and click **Edit** . The Alternate Name window is displayed.
3. Modify the required alternative name details.
4. Click **Save**. A confirmation message is displayed.
5. To remove the alternative name associated with the subject, select the required Record Number and click **Delete** . The alternate name associated with the subject is deleted from the list.
6. Click **Validate** to authenticate the information that is present in the Alternate Name pane.

> **Note:**
>
> You are not allowed to add alternative names if you have selected 'Is critical information unknown?' in the Subject Information pane.

7. To add a new alternate name, on the Alternate Name pane, click **Add**  . The Alternate Name window is displayed.

> **Note:**
>
> You are not allowed to add alternative names if you have selected 'Is critical information unknown?' in the Subject Information pane.

8. Enter the alternate name.
9. Click **Save**. A confirmation message is displayed, and a new alternate name is added to the list.

> **Note:**
>
> - You can enter up to 150 characters for an alternate name.
> - You must not use prohibited words such as AKA, computer- generated, customer, DBA, Non-customer, none, not applicable, other, same, same as above, see above, see narrative, signature card, T/A, unknown, various, and so on.

6.7.6 Email Address

Email address facilitate the identification of electronic communication used by the subject (person or entity) in the suspicious activity. Use this pane to view, modify, and delete the existing email addresses of the subject associated with the report. You can also add one or more subject email addresses to the selected report.

Use this pane to view the list of email addresses associated with the selected report. You can modify the email addresses details and also delete them from the list.

To manage the email addresses, follow these steps:

1. On the Subject Information pane, go to the Email Address pane. The list of email addresses is displayed.
2. To modify the required email address, select the required Record Number, and click **Edit** . The Email Address window is displayed.
3. Modify the email address and click **Save**. A confirmation message is displayed.

4. To remove the email address associated with the report, select the required Record Number and click **Delete** . The email address associated with the report is deleted from the list.
5. Click **Validate** to authenticate the information present in the Email Address pane.
6. To add a new email address, On the Email Address pane, click **Add** . The Email Address window is displayed.
7. Enter the email address.
8. Click **Save**. A confirmation message is displayed, and a new email address is added to the list.

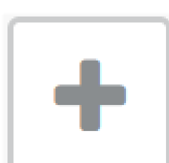
> **Note:**
>
> - You can enter up to 50 characters for an alternate name.
> - If you enter an invalid email address, the application displays an error message.

6.7.7 Website (URL) Address

A website (URL) address facilitates the identification of electronic communication used by the subject (person or entity) in the suspicious activity. Use this section to view, modify, and delete the existing website (URL) address associated with the report. You can also add one or more website (URL) addresses to the selected report.

Use this pane to view the list of website (URL) addresses used by the subject. You can modify the website (URL) address details and also delete them from the list.

To manage a website (URL) address, follow these steps:

1. On the Subject Information pane, go to the Website (URL) Address pane. The list of website (URL) addresses used by the subject is displayed.
2. To modify the required website (URL) address, select the required Record Number and click **Edit**. The Website (URL) Address window is displayed.
3. Modify the Website (URL) Address and click **Save**. A confirmation message is displayed.
4. To remove the website (URL) address associated with the report, select the required Record Number and click **Delete**. The website (URL) address associated with the report is deleted from the list.
5. Click **Validate** to authenticate the information that is present in the Website (URL) Address pane.
6. To add a new website (URL) address, On the Website (URL) Address pane, click **Add** . The Website (URL) Address window is displayed.

7. Enter the website (URL) address.
8. Click **Save**. A confirmation message is displayed and a new website (URL) address is added in the list.

> **Note:**
>
> - You can enter up to 517 characters for the website (URL) address.
> - The URL addresses must contain a dot (.) and must not include the "@" character.

6.7.8 Account Information

Account information facilitates the identification of accounts used by the subject (person or entity) in the suspicious activity. Use this section to view, modify, and delete the existing account associated with the subject. You can also add a new account to the selected report.

Use this pane to view the list of account information associated with the subject. You can modify the account details and also delete them from the list.

To manage the account information, follow these steps:

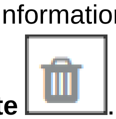
1. On the Subject Information pane, go to the Account Information pane. The list of accounts associated with the subject is displayed.
2. To modify the required account information, select the required Record Number, and click **Edit**. The Account Information window is displayed.
3. Modify the required details.
4. Click **Save**. A confirmation message is displayed.
5. To remove the account information associated with the subject, select the required Record Number, and click **Delete**. The Account Information associated with the report is deleted from the list.
6. Click **Validate** to authenticate the information that is present in the Account Information pane.
7. To add a new account, On the Account Information pane, click **Add**. The Subject Account Details window is displayed.
8. Enter the account information fields.

Table 6-14 Account Information

Fields	Description
Non-US Financial Institution	Select No if the financial institution associated with the account is a US- based financial institution. Select Yes if the financial institution associated with the account is a non-US institution.
Financial Institution TIN	Enter the financial institution's TIN.
Account Number	Enter the account number.
Is Account Closed	Select whether the account is closed or not. **NOTE**: If you have not selected any value in the field Is Account Closed, the system displays the error message.

9. Click **Save**. A confirmation message is displayed, and a new account is added to the list.

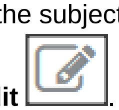
> **Note:**
>
> - If you click the check box If No Account Involved, check this box when the report already contains one or more account details, then an error message is displayed.
> - If there are no account details and No Account Involved, check this box is not checked, then an error message is displayed.
> - If you try to add a new account when If No Account Involved, check this box field is checked, then an error message is displayed.
> - While adding an account, you must specify either the TIN or the Account Number (at least one of them). In case you fail to mention both the TIN and the Account Number, then an error message is displayed.
> - If you enter TIN type as SSN/ITIN or EIN and if it is more than nine digits or if it contains any special characters, then an error message is displayed

6.7.9 Relationship with Financial Institution

The Relationship with Financial Institution pane provides details of the relationship of the subject with the financial institutions in the report. Use this pane to view, modify, and delete the existing relationship of the subject with the financial institution associated with the report. You can also add a new relationship of the subject with a financial institution.>

Use this pane to view the list of the relationship of the subject with a financial institution associated with the selected report. You can modify the relationship details and also delete them from the list.

To manage the relationship of the subject with the financial institution, follow these steps:

1. On the Subject Information pane, go to the Relationship with Financial Institution pane. The list of the Relationship with Financial Institution is displayed.
2. To modify the relationship of the subject with a financial institution, select the required Record Number, and click **Edit** . The Relationship with Financial Institution window is displayed.
3. Modify the required details.

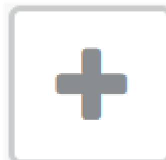
4. Click **Save**. A confirmation message is displayed.
5. To remove the relationship of the subject with a financial institution associated with the report, select the required Record Number and click **Delete** . The relationship of the subject with the financial institution associated with the report is deleted from the list.
6. Click **Validate** to authenticate the information that is present in the Relationship of the Subject with the Financial Institution pane. The Validate button in the Subject information tab checks for any missing mandatory information and identifies any disallowed combinations of Relationship types and the inclusion of an Action Date.
7. To add a new relationship of the subject with a financial institution, On the Relationship with Financial Institution pane, click **Add** . The Subject Relationship with Financial Institution window is displayed.
8. Enter the Subject Relationship with Financial Institution field details.

Table 6-15 Relationship with Financial Institution

Fields	Description
Financial Institution TIN	Enter the TIN number of the financial institution.
Relationship with Financial Institution	Select the relationship of the subject with the financial institution from the drop-down list. This field provides the following options in the drop-down list: • Accountant • Agent • Appraiser • Attorney • Borrower • Customer • Director • Employee • No relationship to the institution • Officer • Owner or Controlling shareholder • Other
Description (Relationship type “Other”)	Enter the relationship of the subject with the financial institution. If the relationship of the subject with the financial institution is anything other than the options provided in the Relationship with Financial Institution drop-down list, then you must select Other and describe the relationship.
Status	Select the status of the relationship of the subject with the financial institution from the drop-down list. This field provides the following options in the drop-down list: • Resigned • Suspended/Barred • Terminated Relationshipcontinues

Table 6-15 (Cont.) Relationship with Financial Institution

Fields	Description
Action Date	Select the date of termination of the subject related to the financial institution. **NOTE**: This field must be updated only if the relationship status is Terminated.

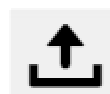
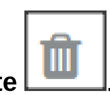
9. Click **Save**. A confirmation message is displayed, and a new account is added to the list.

6.8 Documents

While filing the report with regulatory authorities, you can also send additional documents. This additional information aids in making the correct decision on the report. When you attach a document to a report, the status of that report does not change. However, the attachment is added to the report's history. An Analyst or a Supervisor can attach, modify, or delete documents in all statuses except when the report is in View Only mode.

The Documents pane lists all the documents that are attached to the report. It also allows you to add additional documents. You can upload files of any format with a size of less than 1 MB. You can upload files of any format in the Documents tab. You can choose to include the attached document in the report. However, only one file of .csv format can be included in the report. You cannot include files of any other format other than .csv in the report. Use this pane to view and modify the documents, and you can also attach documents to the selected report.

To manage and attach documents to the selected report, follow these steps:

1. On the Regulatory Reports Details page, click the **Documents**  button. The Upload Documents window is displayed.
2. Go to the **Uploaded Details.**
3. To delete the uploaded file, select the required file and click **Delete** . The uploaded file is deleted from the list.
4. To modify the uploaded file, select the required file, and click **Edit**. Modify the uploaded file details and click Save.
5. To include (attach) the uploaded file in the report, select the file from the list and click **Upload**. The selected file is included in the report. Only one file of .csv format can be included in the report. You cannot include files in any other format.
6. To add the documents to the selected report, On the **Upload Documents** window, enter the file name of the document to be uploaded and Select **Yes or No** to specify whether to include the document in the report.
7. To upload the documents, click the **Click here to Upload** file button.
8. Select the file from your local system to upload. The uploaded document is displayed in the Uploaded list of documents.

6.9 Narrative

Use the Narrative to summarize suspicious activity and mention the action taken by the reporting entity.

To update the narrative, follow these steps:

1. On the Regulatory Reports Details page, click the **Narrative**  . The Narrative window is displayed.
2. Enter the information in the Narrative pane.

   > **Note:**
   >
   > You can enter up to 17000 characters in the narrative pane.

3. Click **Save**. A confirmation message is displayed.

   > **Note:**
   >
   > YCarriage returns (if any) and line breaks are removed when submitting an E- file to FinCEN. The Audit section tracks both actions and comments entered while performing the narrative.

   The Audit section tracks both actions and comments entered while performing the narrative.

6.10 Audit and Comments

Use the Audit window to view the audit history of a report. It provides details of actions performed on the report and comments provided by the users in the various statuses. You can also use the Audit window to provide comments on the selected report.

To view the audit history of the selected report, follow these steps:

1. On the Regulatory Reports Details page, click Audit . The Audit window is displayed.
2. Enter the comments in the Comments field and click **Save**. The comment is captured in the audit history of the report.

   Records in the Audit window are displayed when a user performs the following actions:

   - Filing Institution Information Modified
   - Added Financial Institution
   - Modified Financial Institution
   - Removed Financial Institution
   - Added Branch Information
   - Modified Branch Information
   - Delete Branch Information

- Added New Subject – Subject Record # (When you click Save)
- Removed Subject – Subject Record #
- Modified Subject Details – Subject Record #
- Modified Suspicious Activity Details Modified Suspicious Activity Classification
- Modified Law Enforcement Information
- Added Suspicious Activity Additional Information
- Modified Suspicious Activity Additional Information
- Removed Suspicious Activity Additional Information
- Added New Document – Name of the added document
- Removed Document – Name of the Removed document
- Added Relationship with Financial Institution
- Modified Relationship with Financial Institution
- Removed Relationship with Financial Institution
- Added New Account - Accounts Number
- Modified New Account - Account Number
- Removed New Account - Account Number
- Narrative Added
- Due Date Modified

6.11 XSD Validation Details

The XSD Validation Details tab allows to validate report formats/details against the XSD (XML Schema Definition) files. If there are any errors related to XSD, those errors will be listed in the XSD Validation Details tab. This feature helps avoid E-Files being rejected from the FinCEN E-File System due to errors during submission.

This allows Analysts to validate each detail before they request SAR approval and helps Super Users or Supervisor users validate errors and approve the report. If there are any errors related to XSD, it will not allow them to approve the report until the errors are rectified.

To view errors in SAR details, follow these steps:

1. Go to the Reports Details page.
2. Click the **XSD Validation Details** tab. The XSD Validation Details page is displayed with the list of errors present in the SAR.

Table 6-16 Upload Documents

Fields	Description
Date	Displays the date on which the XSD validation errors are recorded.
Section	Section Displays the name of the tab under which the errors are recorded. Displays the description of the record which has the error. Involved Record shows an individual record of sections. For example, if there is an error in the branch code in the Financial Institutions tab or Subject Record in the Subject Information tab, and so on
Error Description	Displays the description of the XSD error.

These error details will help you to go back to the respective tabs such as Filing Institution Information, Financial Institution Where Activity Occurred, Suspicious Activity Information, and so on to rectify the mistakes and take further actions.

7

Acting on Reports

After analyzing the reports using the Reports Details page, an authorized user can take action on reports to file it to FinCEN or close the report.

Topics:

- **Requesting the Report for Approval**
- **Approving/Rejecting/Closing Reports**
- Setting a Due Date

7.1 Requesting the Report for Approval

An Analyst requests the supervisor to approve the report for filing when it is in the Open, Reopened, Requested for Approval, or Rework status. A Supervisor evaluates and then approves, rejects, or closes the report.

To submit a report for approval, follow these steps:

1. On the Regulatory Report Details page, click **Request for Approval**. The Request for Approval Action window is displayed..

   > **Note:**
   >
   > If the mandatory information is missing or invalid, a warning message is displayed prompting you to correct the information before requesting approval.

2. Enter the comments in the Comments field.

   > **Note:**
   >
   > You can enter up to 255 characters.

3. Click **Save**. A confirmation message is displayed and on the Report Details page, the status of the report changes to Requested for Approval. The Audit page tracks both actions and comments entered while performing the Request for Approval action.

   If your requests are rejected by the Supervisor, you will receive a notification. Click the **Notification** icon to view the notification of rejected reports.

7.2 Approving/Rejecting/Closing Reports

As a Supervisor, you can assess the reports that are requested for approval and take the appropriate action on the selected report.

> **Note:**
>
> - – It is mandatory to add comments to perform thisaction.
>   – The comments added, and action taken on the selected report is recorded in the Audithistory.
>   – Notification of rejected reports is sent to only those users whohave sent the reports for approval

- **Approving a Report**: You can approve a report that is in Open, Re-open, Rejected, Rejected from E-file status, or Request for Approval status with all the mandatory fields updated. If the report is approved, an e-file is generated for the report. The generated e-file is submitted with the Fin- CENs BSA E-Filing System.
- **Rejecting a Report**: You can reject the report in Approved or Request for Approval status. If the report is rejected, then the Analyst must re-work the report and resubmit the report for approval or can close the report. If the Analyst closes the report after it is rejected, then the status of the report changes to Closed. But if the Analyst chooses to rework the report, then the status of the report changes to Request for Approval, which is again validated and approved by the Supervi- sor. This process continues until the report is approved or closed.
- **Closing a Report**: You can a close report without filing in Open, Re-open, Rejected, Rejected from E-file status, or Request for Approval status with all the mandatory fields updated. The Closed status removes it from the work queue and helps to distinguish it from those in the Filed status. After the report is closed, you cannot edit the report details, and the report is in View mode. The status of the report changes to Closed.

To approve, reject, or close a report, follow these steps:

1. On the Regulatory Report Details page, click **Approve**, **Reject**, or **Close**. The Report Actions window is displayed..

   > **Note:**
   >
   > If the mandatory information is missing or invalid, a warning message is displayed.

2. Enter the comments in the Report Actions window. You can enter up to 255 characters.
3. Click **Save**. A confirmation message is displayed. It is mandatory to add comments.

> **Note:**
>
> - It is mandatory to add comments to perform this action.
> - The comments added, and action taken on the selected report is recorded in the Audit history.

7.3 Setting a Due Date

The Set Due Date action enables you to set a due date or modify an existing due date of a report. The due date is set for a report when the Generate USSAR Report action is taken in the Case Investigation Cloud Service. This is the date by which the SAR must be filed with FinCEN. The Due date is configurable, and by default, it is set to 30 days from the date of report creation request is sent from the Case Investigation Cloud Service to USSAR Cloud Service. It includes only business days excluding holidays and weekends. This period is configurable.

There are two roles defined for the Set Due Date functionality.

- **Due Date with View and Edit**: Users mapped to this role can view, set, and edit the due date for reports.
- **Due Date with View**: Users mapped to this role can only view the due date for reports

> **Note:**
>
> The roles are mapped based on the configurations in the Application Parameters table.

Table 7-1 Set Due Date Functionality Configuration

Set Due Date Action	Take Set Due Date Action	View Dates
Open	X	X
Requested for Approval	X	X
Rejected	X	X
Rejected from E- File	X	X
Approved		X
Cancelled		X
E-File Generated		X
Filed		
Reapprove Required		X

To set a due date for a report, follow these steps:

1. On the Reports Details page, click **Set Due Date**. The Report Actions window is displayed.

> **Note:**
>
> If the mandatory information is missing or invalid, a warning message is displayed.

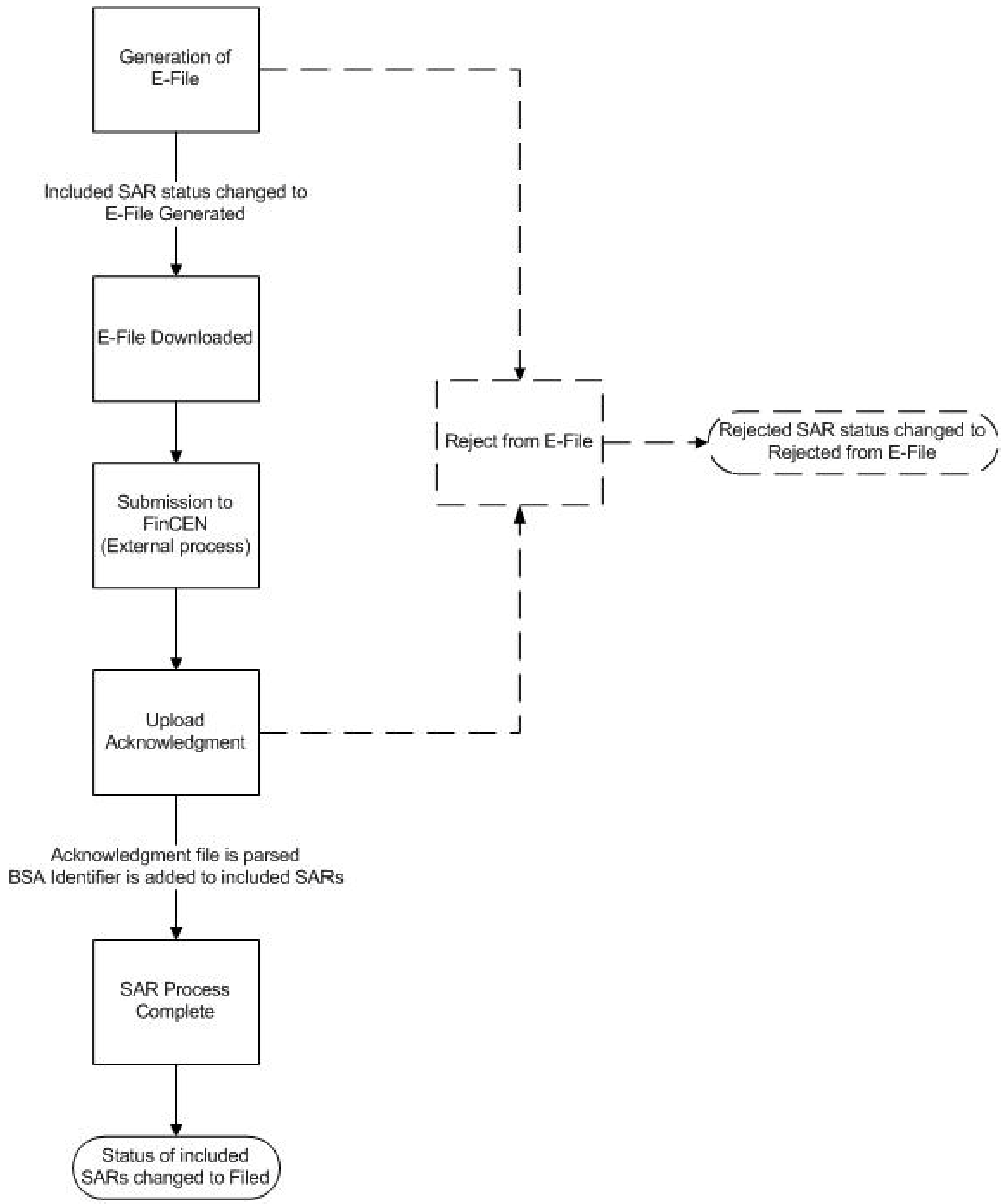
2. Enter the comments in the Report Actions window. You can enter up to 255 characters.
3. Click Save. A confirmation message is displayed. It is mandatory to add comments to perform the action.
4. Click **Save**. A confirmation message is displayed and the Report Details page is updated with a new due date. The Audit page tracks both actions and comments entered while performing the Set Due Date action.

8
Filing Regulatory Reports

How to file an approved report to the FinCEN's BSA E-Filing System, upload the acknowledgment into USSAR Cloud Service, and complete the SAR process is described here. Only users mapped to the role of Super User and Admin User can generate an E-file. When a report is created in the application, the report details are entered and then submitted for approval. After analysis, an Analyst submits the report for approval, Supervisor validates the report details, and either approves, rejects, or closes the report.

If the supervisor approves the report, then the report is available for E-file generation. The generated E- file is submitted to FinCEN's BSA E-Filing System. The E-file is validated by FinCEN, and an acknowledgment (XML file) is generated. Then the acknowledgment file is uploaded into the USSAR Cloud Service. The USSAR Cloud Service associates the FinCEN returned BSA Identifier to each SAR within the E-file. By this, the SAR process is marked as completed.

Figure 8-1 Workflow for Filing the Regulatory Report



Topics:

- Searching Approved Reports
- Generating E-File
- Downloading E-Files
- Submitting E-Files at FinCEN
- Downloading E-File Acknowledgments from FinCEN
- Uploading E-File Acknowledgments to USSAR Cloud Service

- Rejecting Reports from E-File
- Completing the SAR Process
- Generating Revised Reports

8.1 Searching Approved Reports

Use this pane to search the required approved reports using the search parameters. Super Users and Admin Users can search, file, reject, or close approved reports.

To search for approved reports, follow these steps:

1. On the Regulatory Report List page, click File Reports. The Approved Report Search page is displayed with the list of all approved reports.
2. If you want to search for the specific report in the list, then enter the search parameters.

Table 8-1 Approved Reports Search Bar

Fields	Description
Report Name	Enter the report name.
Jurisdiction	Select the jurisdiction from the drop-down list.
Case ID	Enter the Case ID for the report.
Approved By	Enter the name of the approver. Select the date from the calendar. Use this criterion to filter reports approved on or after this date. For example, reports approved on or after July 27, 2019.
Approved Date From	You can either perform a range search using Approved Date From' and Approved Date To or use them independently.
Approved Date To	Select the date from the calendar. Use this criterion to filter reports approved on or before this date. For example, reports approved on or before July 27, 2019.
Created By	Select the user role(s) from the drop-down list to search for reports created by.

3. Click **Go**. The relevant report list is displayed.

8.2 Generating E-File

After the status of a regulatory report changes to Approved, you can generate the E-file for those reports and upload the resultant .xml file into FinCEN's BSA E-Filing System.

When an E-file is generated, an attachment zip file is created for the E-file with a .csv file in it. This .zip file is only available if attachments were associated with any SAR within the E-file.

To generate an E-file, follow these steps:

1. On the Approved Report Search List page, select the required report or reports for which you want to generate an E-file.

> **Note:**
>
> If the size of E-File is more than 60 MB, the following message is displayed: "The efile is exceeding the size limit. To automatically split the efile, click on OK or else reduce the number of report selection before proceeding to generate an efile."

2. Click **Generate E-file** . A confirmation message is displayed. The status of the regulatory report changes to E-file Generated.

> **Note:**
>
> - The reports on which Generate E-file action is taken are moved from the Approved Reports list to the E-file list.
> - If you try to generate an E-file for the same report(s) which is already locked by another user, an error message is displayed.
> - If you try to E-file or reject a report which is already locked by another user, an error message is displayed. If you try to E-file a report which is already generated or rejected, an error message is displayed.

8.3 Downloading E-Files

After an E-file generated action is taken, the USSAR Cloud Service generates a .xml file with its content formatted according to FinCEN specifications for electronic filing. You must save this .xml file and submit to FinCEN's BSA E-Filing System.

Use the E-file Summary tab to manage the generated E-files for searching and downloading E-files to submit to the FinCEN.

To download the E-files, follow these steps:

1. On the E-file Summary tab, enter the search parameters.

Table 8-2 E-File search

Fields	Description
Report Name	Enter the report name.
Jurisdiction	Select the jurisdiction from the drop-down list.
Case ID	Enter the case ID for the report.
E-file Generated By	Enter the name of the E-file generator.Select the date from the calendar. Use this criterion to filter the E-file generated on or after this date. For example, E-file generated on or after July 27, 2020.
E-file Generated Date From	You can either perform a range search using E-file Generated Date From' and E- file Generated Date To or use them independently.
E-file Generated Date To	Select the date from the calendar. Use this criterion to filter the E-file generated on or before this date. For example, E-file generated on or before July 27, 2020.

2. Click **Go**. The relevant E-file list is displayed.
3. On the E-file list results page, select a record and click **E-file** in the E-file column. A File Download window prompts to Open or Save the E-file. Click **Save** to download the E-file.
4. To view the E-file details, select a record in the Details column and click **Details** . The E-file Details pane is displayed with the number of reports included in the selected E-file.

8.4 Submitting E-Files at FinCEN

After the E-file is generated, you must file them with the FinCEN's BSA E-Filing System, which in turn generates an acknowledgment or (XML) file.

To submit the E-file to BSA E-Filing System, follow these steps:

1. Log in to the BSA E-Filing System website.
2. From the left-hand side menu pane, click New Reports, and select File Batch FinCEN SAR. An Open an Existing Form window is displayed.
3. Click **Open New Form**. A BSA E-Filing SAR Batch Form is displayed.
4. Enter the BSA E-Filing SAR Batch Form fields.

Table 8-3 BSA E-Filing SAR Batch Form

Fields	Description
Filing Name	Enter the filing name. There is no specific requirement for the name of the filing. It is recommended that it must be a unique name as this can be used to identify the E-file on the BSA E- Filing system after submission.
Batch File	Click Add to attach the E-file that was downloaded from the USSAR Cloud Service. NOTE: The E-file must be in .xml format.
Attachments File	Add the E-file attachment .zip file that was downloaded from the USSAR Cloud Service along with the E-file.
Number of Forms in Batch	Enter the number of individual SAR reports in an E-file.

5. Click **Sign with PIN** and enter the title and date in the respective fields. The following message is added to the header and footer of the document: This form has been signed with a PIN and cannot be altered.

> **Note:**
>
> This is the unique identifier assigned by BSA and FinCEN to ensure that only authorized individuals are submitting SAR filings.

6. Click **Save**. The filled BSA E-Filing SAR Batch Form is saved. After you save the form, the Submit button is enabled.
7. Click **Submit**. A confirmation window displays the following message: We have received your submission. Please confirm the following information and retain it for your records. Please track the status of your submission using the 'Track Status' function in the BSA E-Filing system. The status of a submitted E-file can be one of the following:
   - Transmitted
   - Transmitted with Warnings
   - Rejected
8. Click the **Accepted with Warning or Rejected** status hyperlink in the Status column of Track Status page to view the submission errors on the E-file that are in Accepted with Warning or Rejected status.
9. Click **OK**. The E-file is successfully submitted at FinCEN.

8.5 Downloading E-File Acknowledgments from FinCEN

When the BSA E-Filing System Track Status page shows that the submitted file has been acknowledged, you can retrieve an acknowledgment file from the BSA E-Filing System Secure Messaging Center. You must save this acknowledgment .xml file and upload it into the USSAR Cloud Service.

To download the acknowledgment file from BSA E-Filing System, follow these steps:

1. Log in to the BSA E-Filing System website.
2. On Secure Messaging, select View Inbox to view the list of acknowledgments.
3. Click the **Subject of the required acknowledgment**. A BSA E-Filing Secure Message Reply Form is displayed.
4. Click **View/Save Attachment**. An Acknowledgment (XML) file window is displayed.
5. Click **View/Save** to download the XML file in your system.

8.6 Uploading E-File Acknowledgments to USSAR Cloud Service

After downloading the acknowledgments from BSA E-Filing System, you can upload the acknowledgments in the USSAR Cloud Service. After you upload the acknowledgment (XML) file, the file is then parsed to retrieve the BSA Identifier that is assigned by FinCEN to each report.

This BSA Identifier is then added to the report record.

To upload the acknowledgment, follow these steps:

1. On the E-file Summary page, go to the E-file List pane, and select the record for which you want to upload the acknowledgment.
2. Click **Upload Acknowledgment**. An Upload Acknowledgement window is displayed.
3. Enter the Upload Acknowledgement fields.

Table 8-4 SAR Acknowledgment Window

Fields	Desciption
E-file Name	The name of the E-file. **NOTE**: This field is auto-generated
Ack Updated By	The name of the user role who is updating the acknowledgment. NOTE: This field is auto-generated.
Ack Received On	Select the date from the calendar on which the acknowledgment was received.
Ack Number	Enter the acknowledgment number.
EFile Comments	Enter the required comments.
Logical File Name	Enter a logical file name for the acknowledgment.

4. Click the **Click here to upload a File** icon to upload the XML file downloaded from the BSA E- Filing System.
5. Click **Attach File** and click **Save**. A confirmation message is displayed.
6. Click **OK**. You are navigated back to the E-file List results.

Note:

- After you upload the acknowledgment file for an E-file, a BSA ID is associated with the respective report.
- After you upload the acknowledgment file successfully into the USSAR Cloud Service, the XML file can be viewed and saved from the E-file list results.
- When you try to upload an acknowledgment file for an E-file for which an XML file is already uploaded, a warning message is displayed.
- When an upload acknowledgment action doesn't pass the validation check, an error message is displayed.

8.7 Rejecting Reports from E-File

You can reject reports from an E-File at any point in time before completing the SAR process. After a SAR report is rejected from an E-File, it is removed from the reports list and the status of the rejected report changes to Rejected from E-File. For reports that are not rejected, a new E-File is regenerated. If the acknowledgment file is already uploaded, you can complete the SAR process of the regenerated E-File by clicking Complete SAR Process.

You can correct/amend a rejected report and submit it for Super User's approval. After the corrected report is approved, you can follow the workflow of filing a regulatory report all over again. Subsequently, while uploading the acknowledgment (XML) file received from FinCEN into the OFS CRR application, a new BSA Identifier overwrites the previously associated BSA Identifier of the rejected reports.

In the SDTM mode, when rejected Message XML is uploaded via batch while parsing the Message.xml if the value for attribute "Level" is as FATAL or WARN, the associated reports in the corresponding E-File will be automatically rejected. This will be captured in the Audit history for each report being rejected. It will also have associated rejected Message XML, which can be downloaded from the Attachment column in the Audit tab.

With the reports, left after the automatic rejection of reports, a new E-File will be regenerated.

After an E-File is uploaded and accepted by FinCEN, you cannot reject SARs from the E-File until the acknowledgment file is uploaded and parsed. If you reject a report after submission but before processing the acknowledgment files there will be a mismatch in the files referenced in the acknowledgment file and the current E-File. If a report is rejected prior to uploading the acknowledgment into the application, then you have to re-submit the E-File at FinCEN's BSA E-Filing System to get the latest acknowledgment file.

To reject the SARs from an E-file, follow these steps:

1. On the E-file Summary page, go to the E-file List pane, and select the E-file. The Report List for the selected E-files is displayed.
2. Select the report or reports you want to reject from the E-file and click reject . The rejected reports are removed from the E-file List results.

8.8 Completing the SAR Process

After uploading an acknowledgment into the USSAR Cloud Service, you can complete the suspicious activity reporting process by clicking the Complete SAR Process. The status of all regulatory reports included in the E-file then changes to Filed. After a report is moved to the Filed status it cannot be edited.

To complete the SAR process, follow these steps:

1. On the E-file Summary page, go to the E-file List pane, and select the E-file with acknowledgment.
2. Click **SAR Process Complete**. A confirmation message is displayed.

> **Note:**
>
> - If you try to take the Complete SAR Process action before performing the Upload Acknowledgment action, a warning message is displayed.
> - If you try to take the Upload Acknowledgment action on a file for which the SAR process is already complete, a warning message is displayed.

8.9 Generating Revised Reports

When you download an acknowledgment from FINCEN E-File System and identify there are errors or issues in the reports, but they are not rejected. You can update the report by selecting the Correct/ Amend Prior Report or Continuing Activity Report option for the report in the Filed status and resubmit an E-File with revised reports into FinCen E-File System again.

When you take the Generate Revised Report action on a report using the Correct/Amend Prior Report Type or Continuing Activity Report option, a new report is created with the same information, and the status of the report is Open with Correct/Amend Prior Report Type or Continuing Activity Report type. The report with Open status is available in the Regulatory Reports List. To submit the revised report into the FinCen E-File System again, follow the workflow. For example, if you have submitted report number 4458 into FinCen E-File System and received an acknowledgment with errors or issues. You have two options to revise the report and resubmit into FINCEN E-File System:

Corrected/Amend Prior Report Type: This option is used if any errors are to be corrected in the report. For example, Open Report Number 4458 in the Filed status and click Generate Revised Report. In the Generate Revised Report window, select the Correct/Amend Prior Report Type and save. A copy of Report Number 4458 was created with the new Report Number 2234 with the same information. The status of the report is Open, and the report type is Correct/Amend Prior Report Type. You can access the Correct /Amend Prior Report type in the Report Search and List page. Now follow the workflow and resubmit into FINCEN E-File System.

Continuing Activity Report Type: This option is used if you want to add additional information and continue the filed report. For example, open Report Number 4458 in the Filed status and click Generate Revised Report. In the Generate Revised Report window, select the Delete option and save. A copy of Report Number 4458 created with new Report Number 2234 with the same information. The status of the report is Open, and the report type is Continuing Activity Report. Now follow the workflow and resubmit into FINCEN E-File System.

To generate a revised report, follow these steps:

1. On the Regulatory Report List page, open the report with Filed status.
2. On the Details page, click **Revised Generate**. A Revised Generate window is displayed.
3. Select the Correct/Amend Prior Report Type or Continuing Activity Report from the Type of Filing drop-down list and enter the comments.

4. Click **Save**. A confirmation message is displayed, and a new report type is created as Correct/ Amend Prior Report Type or Continuing Activity Report with the same information. The status of the report is Open.
5. Go to Report List and open a newly created report. Make the required corrections to the report and get approved to resubmit into FINTRAC E-File System. The FINTRAC E-File System verifies the report and replaces this report in its system for correction.