SAS Anti-Money Laundering Online Help

Version: 2.2.1 (221AML01)

About this Document

Usage information for the SAS Anti-Money Laundering Investigation User Interface is provided in the online Help. When users click **Help**, they see the following two options:

- **Help Contents**: Topic-based Help. Describes concepts and features in a linear fashion, similar to how a user's guide would be organized.

- **Help On This Page**: Context-sensitive Help. Describes the active window in detail.

This document is provided for customers who need to provide a hard copy of the topic-based online Help to regulators. The online Help was designed to take advantage of Web browsing capabilities - such as linking to files that contain related information - that printed documents cannot accommodate.

What is SAS Anti-Money Laundering?

SAS Anti-Money Laundering is a powerful solution that financial institutions use to detect suspected criminal financial activities quickly and accurately, thus reducing risk, meeting government regulations, and protecting shareholder and consumer confidence.

This solution processes data from disparate sources and multiple lines of business, transforms it into useable knowledge, identifies potential money laundering activity, and reports on the results.

SAS Anti-Money Laundering provides

users with intelligence that increases their accuracy in pinpointing suspicious activity while decreasing the rate of identifying false positives. The solution also weighs the severity of scenario violations and ranks suspicious behavior. All this means company resources are better utilized and more effective.

Copyright

About Alerts

About Alerts

What is an alert?

An *alert* is a report of a situation that may be indicative of money laundering. Alerts are displayed on alert list windows, which provide tools and information to aid users as they determine whether alerts represent suspicious activity that should be reported to authorities. Once this determination is made, users close the alerts.

Alerts come from two sources:

1. **SAS Anti-Money Laundering generates them.** The alert generation process runs scenarios and risk factors across data to detect suspicious behavior. There are two kinds of system-generated alerts:
    1. **Scenario alerts** are the most common. When a *subject* (an account, customer, household, or transaction) matches a scenario, an alert is generated. Each alert of this type is based on **one** scenario. The same subject may match one or more risk factors. These matched risk factors raise the alert's risk score and provide users additional information about the subject's suspicious behavior.

    3. **Risk-factor-only alerts** are based entirely on risk factors. If a subject does not match a scenario, but matches risk factors that give the subject a combined a risk score that exceeds a threshold for either terror financing risk or money laundering risk, then a risk-factor-only alert is created. Risk-factor-only alerts can be identified by the contents of the Scenario and Triggering Values columns on an alert list window. The Scenario column will display ML_Risk or TF_Risk, and the Triggering Values column will say "Click risk rank for details."
2. **Users create them.** Users manually create alerts when they observe suspicious behavior that may not be detected by the scenarios and risk factors.

💡 Understanding the differences between owned and checked out alerts is critical to understanding SAS Anti-Money Laundering.

About Alerts

How do users get alerts?

You get an alert when:

- SAS Anti-Money Laundering assigns it to you based on how the solution is configured at your site. You will own alerts that you receive this way.
- You create it, in which case you own it.
- Another user routes it to you, in which case you own it.
- You activate it after it was suppressed or closed. In this case as well, you own it.
- You check it out. If it is not already checked out by another user, you do not own it. If it is checked out by another user, you own it.

See also: Understanding owned and checked out alerts.

About Alerts

Understanding owned and checked out alerts

	Alert You Own	**Alert You Check Out**
How you get it	- The solution assigns it to you, or - You create it, or - Another user routes it to you, or - You activate it after it was suppressed or closed, or - You take ownership by checking it out when another user already has it checked out.	Click **Check Out** in that alert's **Availability** column on the Available Alerts window. The alert cannot already be checked out by another user.
Who can see it	- You see it in My Alerts. - Your manager sees it in Available Alerts, with your name in the Availability column. - Other users cannot see it.	- You see it in My Alerts. - Your manager and others in your group see it in Available Alerts, with your name in the Availability column.
How you can move it	- You cannot check it in. - You can route it.	- You can check it in. - You can route it.
What other users can do	Your manager can take ownership if he/she has "take alert ownership" privilege.	Your manager and others in your group can take ownership if they have "take alert ownership" privilege.

About Risk Assessments

About Risk Assessments

What is a risk assessment?

Risk assessments are an optional component of SAS Anti-Money Laundering. If System Administrators at your site have enabled the risk classification process, users with the View Risk Assessments privilege can access My Risk Assessments and Available Risk Assessments - two windows referred to collectively as *risk assessment list* windows.

A *risk assessment* is a proposal to change a customer's risk classification. Each risk assessment has a current risk classification and a proposed risk classification. The objective is to use the tools and information that SAS Anti-Money Laundering provides to determine whether the proposed risk classification should be accepted and closed, or rejected and closed.

Risk assessments come from two sources:

1. **SAS Anti-Money Laundering generates them.** The risk classification process runs risk classifiers across customer data.
2. **Users create them.** Users manually create risk assessments when they observe suspicious behavior that may not be detected by the risk classifiers.

Understanding the differences between owned and checked out risk assessments is critical to understanding SAS Anti-Money Laundering.

About Risk Assessments

How do users get risk assessments?

You get a risk assessment when:

- SAS Anti-Money Laundering assigns it to you based on how the solution is configured at your site. You will own risk assessments that you receive this way.
- You create it, in which case you own it.
- Another user routes it to you, in which case you own it.
- You check it out. If it is not already checked out by another user, you do not own it. If it is checked out by another user, you own it.

See also: Understanding owned and checked out risk assessments.

About Risk Assessments

Understanding owned and checked out risk assessments

	Risk Assessment You Own	Risk Assessment You Check Out
How you get it	• The solution assigns it to you, or • You create it, or • Another user routes it to you, or • You take ownership by checking it out when another user already has it checked out.	Click **Check Out** in that risk assessment's **Availability** column on the Available Risk Assessments window. The risk assessment cannot already be checked out by another user.
Who can see it	• You see it in My Risk Assessments. • Your manager sees it in Available Risk Assessments, with your name in the Availability column. • Other users cannot see it.	• You see it in My Risk Assessments. • Your manager and others in your group see it in Available Risk Assessments, with your name in the Availability column.
How you can move it	• You cannot check it in. • You can route it.	• You can check it in. • You can route it.
What other users can do	Your manager can take ownership if he/she has "take risk assessment ownership" privilege.	Your manager and others in your group can take ownership if they have "take risk assessment ownership" privilege.

List Windows

List Windows

How to select your starting tab

The starting tab is the tab that is active after you log on. By default, the Alerts tab is the starting tab.

To select a starting tab

1. Open the Preferences window by clicking **Preferences**, which is to the left of your user ID at the top of most windows.
2. Open the drop-down menu next to **Starting tab**.
3. Select the name of the tab you would like use as your starting tab.
4. Click **Modify**.
5. Click **Close**.

The next time you log on, the tab you selected will be active.

List Windows

How to specify the number of rows to display

You can specify *temporary* and *persistent* numbers of rows to display on certain windows. A temporary setting is one that expires when you log off. A persistent setting is one that is retained from session to session.

The windows for which you can specify temporary and persistent rows per page are:

- Alert list windows: My Alerts, Available Alerts, Suppressed Alerts, and Closed Alerts
- Query results windows
- Risk assessment list windows: My Risk Assessments and Available Risk Assessments
- Customer Transactions window

To specify a temporary number of rows to display on certain windows

1. Enter a value in the **Rows per page** box on that window.
2. Press ENTER.

To specify a persistent number of rows to display on certain windows

1. Open the Preferences window by clicking **Preferences**, which is to the left of your user ID at the top of most windows.
2. Click in a **rows per page** field that you want to change. This activates the field.
3. Delete the existing value and enter a new one. Any integer between one and 9,999 is allowed; however, a very large value will make the page take longer to display and could cause your browser to time out.
4. Change all the additional fields that you want to change.
5. Click **Modify**. If all the values you entered are valid, the window will display a "modification successful" message.
6. Click **Close**.
7. If you are viewing one of the windows for which you entered a new number of rows, refresh the browser to see the new number of rows.

List Windows

Sort by a single column

To sort a list window by a single column

1. Click on the column heading.
2. To reverse the sort order, click on the column heading again.

The sort arrow appears in the column that you sorted by, and its direction indicates whether the columns are sorted in ascending or descending order.

Sort by multiple columns

To sort a list window by multiple columns

1. Click the sort icon to open the Sort window.
2. In the **Sort by** box, select the first column that you want to sort by.
3. Select either **Ascending** or **Descending**.
4. Follow steps 2 and 3 for the following three **Then by** boxes.
5. When you are done, click **OK**.

The results of a multiple-column sort are:

- The list window will be refreshed and sorted as you specified.
- The sort specifications will appear at the top of the list.
- The sort arrow will appear in the columns that you sorted by, and its direction will indicate whether that column is in ascending or descending order.

Other Actions

Export data to CSV

Users with the Export to CSV privilege can export data from the following windows to a comma-separated value file that can be opened in spreadsheet software such as Microsoft Excel.

- Alert Details
- Alert List
- Customer Transactions
- Query Results
- Risk Assessment List

Users with the User and Group Administration privilege (but not the Export to CSV privilege) can export the data from the Privileges Assigned to Users window, which is on the System Administration tab.

System Administrators at your site configure a system-wide setting that specifies the format for all CSV files exported from SAS Anti-Money Laundering. The default format is a standard RFC 4180 Comma-Separated Values file. The other option is a CSV file that has a 'value' format applied to long numeric strings, such as account numbers, to prevent spreadsheet applications from converting them to scientific notation with the resulting loss of precision.

System administrators can also specify which delimiter to use (default is comma) and the maximum number of rows to export (default is 1,000). Contact your System Administrators to find out how SAS Anti-Money Laundering has been configured for your site.

To export data to CSV

1. Navigate to the window that displays the data that you would like to export. If you are not sure how to do this, please refer to the help topics on the left side of this window.
2. Click either the Export icon or the **Export to CSV** link, depending on which window you are working with.

List Windows

My Alerts

Which alerts are displayed here?

The alerts listed on this window are the alerts you own and the alerts you have checked out.

- The alerts you own have five asterisks (*****) in the **Availability** column.
- The alerts you have checked out say "Check In" in the **Availability** column.

By default, alerts are sorted by money laundering risk rank, with the highest risk alerts listed first. You can specify any order that suits your needs by performing a single- or multiple-column sort.

Working with My Alerts

- What the column headings mean

- What the icons mean

- How to select alerts

- How to check in an alert

- How to select your starting tab

- How to specify the number of rows to display

List Windows

What the Column Headings Mean

This is a description of column headings on the alert list windows.

Alert ID: The solution assigns each alert a unique identification number. Click the value for Alert ID to see the Alert Details window.

Subject: The type of entity that exhibited the behavior that caused the alert. The values you will see in this column are account, customer, household, and transaction.

Subject Number: For an account alert, this will be the account number. For a customer alert, this will be the customer number. For a household alert, this will be the household number. For a transaction alert, this will be the transaction number. Click the value for Subject Number to view details about the subject.

Name: For an account alert, this will be the primary name on the account. For a customer alert, this will be the name of the customer. For a household alert, this will be the name of the head of the household. For a transaction alert, this will describe the transaction.

Create Date: Date the alert was created. This is usually different from the date on which the suspicious activity occurred.

Money Laundering Risk and **Terror Financing Risk:** Each alert's risk is expressed as a numerical rank between one and 999 in two categories: Money Laundering Risk and Terror Financing Risk. The risk rank indicates the level of risk exhibited by a customer for engaging in suspicious activity that may be indicative of either money laundering or terror financing, and therefore the priority of the alert. If the alert was created manually, both risk ranks were assigned by the user who created the alert. For all other alerts, both risk ranks are assigned by the solution, which uses conditional probabilities to determine ranking. A risk of 250 represents a lower priority than a risk of 850.

Scenario: The scenario that triggered the alert. Click the scenario name to view the Scenario Details window. If the scenario name is ML_RISK or TF_RISK, the alert is a risk-factor-only alert.

Description: This is a description of the scenario that triggered the alert. If an alert was manually created, then the description was selected by the user who created the alert. If the description is "Money Laundering Risk" or "Terror Financing Risk," the alert is a risk-factor-only alert.

Triggering Values: Triggering values provide a brief summary of the activity responsible for the generation of a scenario-based alert.

- If the alert was created manually, the triggering values will be **None**.

- If the alert is a risk-factor-only alert, the triggering values will say "Click risk rank for details" because risk-factor-only alerts do not involve scenarios. Clicking the risk rank for these alerts is the best way to find out what behavior caused the alert to be generated.

Risk factors also have triggering values. They are displayed on the Risk Factor Details window.

Availability: The contents of the Availability column vary based on which alert list is displayed. See also: Understanding owned and checked out alerts.

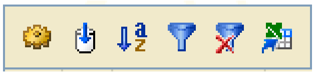
- On Available Alerts, the Availability column may say "Check Out" or it may display another user's name. If an alert's Availability cell says "Check Out" then no other user is currently investigating that alert, and you can move it to My Alerts by checking it out. If the cell displays another user's name, then that user has checked out the alert. If you have Take Alert Ownership privilege, you can take ownership of the alert by clicking on the other user's name.
- On My Alerts, the Availability column may say "Check In" or it may display five asterisks (*****). If an alert's Availability cell says "Check In" then you can click that cell to move the alert to Available Alerts. If the cell displays five asterisks, then you own the alert and cannot check it in, but you can route it.
- On Suppressed Alerts, you can click "Activate" in the Availability column to unsuppress the alert. You will be the owner of any alerts that you unsuppress. The date on which the investigation started will not be the date you unsuppressed the alert; instead it will be the first date on which a user performed an action that started the investigation. You must have Activate Suppressed Alerts privilege to access the Suppressed Alerts window.
- On Closed Alerts, you can click "Activate" in the Availability column to reactivate the alert. You will be the owner of any alerts that you reactivate. The date on which the investigation started will not be the date you reactivated the alert; instead it will be the first date on which a user performed an action that started the investigation. You must have Activate Closed Alerts privilege to access the Suppressed Alerts window.

List Windows

Icons on the My Alerts Window

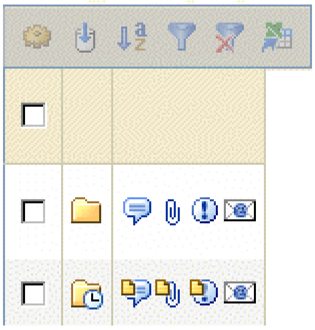
This online help describes all the icons that could appear on the My Alerts window. If your screen does not display an icon that appears in the images below, or if the icon appears but it is "dimmed" (unavailable), this is because either you do not have the associated privilege, or a System Administrator has disabled the associated function.

Toolbar icons



⚙	Go to the Actions window, where you can route, suppress, or close the selected alert(s), or set an e-mail reminder.
☝	Check in the selected alert(s).
↓az	Open the Sort window, where you can perform multiple-column sort. You can perform single-column sort by using the sort arrow (described under "Other Icons" below).
▼	Open the Filter window, where you can make selections to display only alerts that have certain characteristics.
▼✗	Remove filter (if one has been applied).
▦	Export the alert list to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.

Other Icons



☐ ☐ ☐	To select all the alerts currently displayed, click the check box in the same row as the column headings. To select one or several alerts, click the check box for each alert.
▲	The sort arrow appears in the column that alerts are sorted by, and its direction indicates whether alerts are sorted in ascending or descending order. The sort icon on the toolbar (described above) opens a window where you can perform multiple-column sort.

📁	Click the folder icon to open the Alert History window. The clock on the folder 📁 indicates that investigation on the corresponding alert has been started.
💬 💬	Add or view alert comments. The yellow box on this icon indicates that a comment has been entered for that alert.
📎 📎	Add or view an attached alert document. The yellow box on this icon indicates that a document has been attached to that alert.
❗ ❗	View an existing regulatory report or create a new one. This icon will not appear if your institution does not support regulatory reporting for the subject of the alert. The yellow box on this icon indicates that a regulatory report has been attached to that alert.
✉	Send the alert details in an e-mail.

List Windows

How to select alerts on an alert list window

- To select one or several alerts, click the checkbox for each alert in the far left column.
- To select all the alerts currently displayed, click the checkbox in the same row as the column headings.

List Windows

Filter alerts

Use the Filter window when you would like an alert list to display only alerts that have certain characteristics.

To filter an alert list

1. Click the filter icon to open the Filter window.
2. Enter information in the fields to specify which alerts you want to see.
    1. The fields are case-sensitive. In other words, **Stevens** is not the same as **stevens**.
    2. Enter numerals without commas or symbols (such as $).
    3. Fields that have **(contains)** in the label will look for records that contain, instead of exactly match, the characters that you enter.
3. When you are done, click **OK**.

The results of a filter are:

- The alert list will be refreshed and filtered as you specified.
- The filter specifications will appear at the top of the alert list.

To remove a filter

Click the Remove Filter icon . The alert list will be refreshed without the filter.

Alert Actions

Check in & out

To understand this help page, you must understand owned and checked out alerts.

Check in alerts

When you check in one or more checked-out alerts, the alerts move from My Alerts to Available Alerts.

If the Availability column displays ***** instead of **Check In**, then you own that alert and cannot check it in. If you want another user or group to investigate an alert that you own, you should route the alert.

To check in alerts

1. On My Alerts, select the checkboxes for the alerts that you want to check in. To select all the alerts currently displayed, click the checkbox in the same row as the column headings.
2. Click the Check In icon .

You can also check in an alert by clicking **Check In** in the Availability column for that alert.

Check out alerts

When you check out one or more alerts, the alerts move from Available Alerts to My Alerts.

If an alert displays another user's name in the Availability column, then that user has already checked the alert out. If you have the Take Alert Ownership privilege, you can take ownership by clicking on that user's name. The alert will move to My Alerts, and you will own it.

To check out alerts

1. On Available Alerts, select the checkboxes for the alerts that you want to check out. To select all the alerts currently displayed, click the checkbox in the same row as the column headings.

3. Click the Check Out icon .

You can also check out an alert by clicking **Check Out** in the Availability column for that alert.

List Windows

The Alert Actions Window

To open the Alert Actions window, first select one or more alerts. Then click the Actions icon ⚙. On the Alert Actions window you can:

- Route the selected alerts to another user or group
- Suppress the selected alerts
- Set a date on which you would like to receive an e-mail reminder about the selected alerts
- Close the selected alerts

Actions that you are not authorized to perform and that are not activated for your site will not appear on your screen.

To route the selected alerts

1. Click **Route To**.
2. Select another user or group.
3. Click **OK**.

When you route alerts:

- If you route an alert to a user, that user becomes the owner of that alert.
- If you route an alert to a group, that alert becomes available for check-out by members of that group.

To suppress the selected alerts

1. Click **Suppress**.
2. Enter how long you would like to suppress the alert:
    1. If you want to suppress the alert permanently, select **Permanently Suppress**.
    2. If you want to suppress it for a specific period of time, select **Suppress Until**. Enter a date or click the calendar icon to select one.
3. Enter the reason you are suppressing the alert. This will be attached to the alert in the form of a comment.
4. Click **OK**.

When you suppress alerts:

- Only users with Activate Suppressed Alerts privilege can access the Suppressed Alerts window and "unsuppress" an alert.
- Suppressed alerts are not displayed on My Alerts or Available Alerts, and alerts for that scenario are not displayed for that subject for the duration that you specify.
- The status code for alerts that you suppress here will change from **Active** to **Suppressed (UI)**.

To set an e-mail reminder

1. Click **Set E-mail Reminder**

2. Enter a date or click the Calendar icon to select a date.
3. Click **OK**.

When you set an e-mail reminder:

- You will receive one e-mail message for each selected alert on the day that you specify.
- You cannot cancel the reminder.
- If another user takes ownership of an alert that you have set a reminder for, you will still get the reminder.

To close the selected alerts

1. Click **Close Alert**.
2. Select a reason for closing the alert in the drop-down menu.
3. Click **OK**.

When you close alerts:

- Only users with Activate Closed Alerts privilege can access the Closed Alerts window and activate closed alerts.
- Closed alerts are not displayed on My Alerts or Available Alerts. Administrators at your site control the list of possible reasons for closing alerts.

List Windows

Available Alerts

Which alerts are displayed here?

This window displays all the alerts that you are eligible to check out or take ownership of. This means you will see:

- Alerts that belong to your group and that are not owned by any user. These alerts say **Check Out** in the **Availability** column.
- Alerts that belong to your group and that are checked out by another user. These alerts display the user's name in the **Availability** column. If you have Take Alert Ownership privilege, you can click on the user's name to remove the alert from that user's My Alerts list and place it in yours.
- If you are a manager, in addition to the above, you will see alerts owned and checked out by your subordinates. If your subordinates are members of groups that you are not in, you will still see the alerts that they own and have checked out from those groups. When viewing these alerts you will see the user's name in the **Availability** column. If you have Take Alert Ownership privilege, you can click on the user's name to remove the alert from that user's My Alerts list and place it in yours.

Unless you are a manager, this window does not display alerts owned by other users in your group.

By default, alerts are sorted by money laundering risk rank, with the highest risk alerts listed first. You can specify any order that suits your needs by performing a single-column or multiple-column sort.

Working with Available Alerts

- What the column headings mean

- What the icons mean

- How to select alerts

- How to check out an alert

- How to select your starting tab

- How to specify the number of rows to display

List Windows

Icons on the Available Alerts window

	Check out the selected alert(s).
↓az	Open the Sort window, where you can perform multiple-column sort. You can perform single-column sort by using the sort arrow (described below).
	Open the Filter window, where you can make selections to display only alerts that have certain characteristics.
	Remove filter (if one has been applied).
	Export the alert list to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.
☐ ☐ ☐	To select all the alerts currently displayed, click the check box in the same row as the column headings. To select one or several alerts, click the check box for each alert.
	The sort arrow appears in the column that alerts are sorted by, and its direction indicates whether alerts are sorted in ascending or descending order. The sort icon on the toolbar (described above) opens a window where you can perform multiple-column sort.
📁	Click the folder icon to open the Alert History window. The clock on the folder 📁 indicates that investigation on the corresponding alert has been started.

List Windows

Suppressed Alerts

You must have the Activate Suppressed Alerts privilege to access this window and to activate suppressed alerts.

Which alerts are displayed here?

- Alerts that you owned and suppressed. When other members of your group view this window, they will not see these alerts, but your manager will.
- Alerts that you and other members of your group checked out and suppressed.
- If you are a manager you will see:
  - Alerts that you suppressed,
  - All alerts suppressed by your subordinates, and
  - All suppressed alerts for your group(s) and your subordinates' group(s).

By default:

- Alerts that have been suppressed for more than 90 days will no longer be displayed here.
- Alerts are sorted by money laundering risk rank, with the highest risk alerts listed first. You can specify any order that suits your needs by performing a single- or multiple-column sort.

Working with Suppressed Alerts

- What the column headings mean
- What the icons mean
- How to select alerts
- How to activate a suppressed alert
- How to select your starting tab
- How to specify the number of rows to display

List Windows

Closed Alerts

You must have the Activate Closed Alerts privilege to access this window and to activate closed alerts.

Which alerts are displayed here?

- Alerts that you owned and closed. When other members of your group view this window, they will not see these alerts, but your manager will.
- Alerts that you and other members of your group checked out and closed.
- If you are a manager you will see:
    - Alerts that you closed,
    - Alerts closed by your subordinates, and
    - Closed alerts for your group(s) and your subordinates' group(s).

By default:

- Alerts that have been closed for more than 90 days will no longer be displayed here.
- Alerts are sorted by money laundering risk rank, with the highest risk alerts listed first. You can specify any order that suits your needs by performing a single- or multiple-column sort.

Working with Closed Alerts

- What the column headings mean
- What the icons mean
- How to select alerts
- How to activate a closed alert
- How to select your starting tab
- How to specify the number of rows to display

List Windows

Icons on the Suppressed Alerts and Closed Alerts Windows

🚦	Activate the selected alert(s).
↓az	Open the Sort window, where you can perform multiple-column sort. You can perform single-column sort by using the sort arrow (described below).
▼	Open the Filter window, where you can make selections to display only alerts that have certain characteristics.
▼✗	Remove filter (if one has been applied).
▦	Export the alert list to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.
☐ ☐ ☐	To select all the alerts currently displayed, click the check box in the same row as the column headings. To select one or several alerts, click the check box for each alert.
▲	The sort arrow appears in the column that alerts are sorted by, and its direction indicates whether alerts are sorted in ascending or descending order. The sort icon on the toolbar (described above) opens a window where you can perform multiple-column sort.

You will be the owner of any alerts you activate.

Alert Actions

Activate a closed or suppressed alert

You will be the owner of any alerts that you activate.

You must have the Activate Suppressed Alerts privilege to access the Suppressed Alerts window, and you must have the Activate Closed Alerts privilege to access the Closed Alerts window.

To activate a suppressed or closed alert

1. On the Suppressed Alerts or Closed Alerts window, select the alert(s) to activate.
2. Click the Activate icon 🟩.

When you activate alerts

- You will be the owner of alerts that you activate.
- The date on which the investigation started will not be the date you unsuppressed the alert; instead it will be the first date on which a user performed an action that started the investigation. The Alert History window displays the date on which the investigation was started, as well as the user who performed the action that started the investigation.

💡 You can also activate an alert by clicking **Activate** in the **Availability** column for that alert.

List Windows

My Risk Assessments

Risk assessments are an optional component of SAS Anti-Money Laundering. If you do not see the Risk Assessments tab, then System Administrators at your site have disabled risk assessment processing.

Which risk assessments are displayed here?

The risk assessments listed on this window are the risk assessments you own and the risk assessments you have checked out.

- The risk assessments you own have five asterisks (*****) in the **Availability** column.
- The risk assessments you have checked out say "Check In" in the **Availability** column.

By default, risk assessments are sorted by proposed risk classification. You can specify any order that suits your needs by performing a single-column or multiple-column sort.

Working with My Risk Assessments

- What the column headings mean
- What the icons mean
- How to select risk assessments
- How to check in a risk assessment
- How to select your starting tab
- How to specify the number of rows to display

List Windows

What the Column Headings Mean

This is a description of column headings on My Risk Assessments and Available Risk Assessments.

Assessment ID: The solution assigns each risk assessment a unique identification number. Click the value for Assessment ID to open the Risk Assessment Details window.

Customer Number: The unique identification number that your institution assigned to the customer who is the subject of the risk assessment. Click the value for Customer Number to open the Customer Details window.

Customer Name: The name of the customer who is the subject of the risk assessment. There cannot be more than one open risk assessment for a customer at any time.

Current Risk Classification: The most recent risk classification assigned to the customer. **H** means high; **M** means medium; **L** means low. The current risk classification may have been set through a previous risk assessment.

Proposed Risk Classification: The risk classification that is being suggested for the customer. **H** means high; **M** means medium; **L** means low. If the risk assessment was created manually, the proposed risk classification was assigned by the user who created the risk assessment. For all other risk assessments, the proposed risk classification was assigned by the solution, which uses risk classifiers to determine risk classification.

Risk Classifiers: The risk classifier(s) that the customer matched, ordered by weight, from highest to lowest. System Administrators at your site set the maximum number of risk classifiers that can be displayed in this column. The default is four. To see a complete list of all the risk classifiers associated with a risk assessment, click the value in the Assessment ID column for that risk assessment to open the Risk Assessment Details window. From there you can click a risk classifier name to open the Risk Classifier Details window.

Create Date: Date the risk assessment was created.

Availability: The contents of the Availability column vary based on whether you are viewing My Risk Assessments or Available Risk Assessments. See also: Understanding owned and checked out risk assessments.

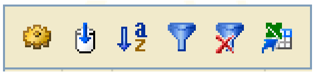
- On Available Risk Assessments, the Availability column may say "Check Out" or it may display another user's name. If a risk assessment's Availability cell says "Check Out" then no other user is currently working with that risk assessment, and you can move it to My Risk Assessments by checking it out. If the cell displays another user's name, then that user has checked out the risk assessment. If you have Take Risk Assessment Ownership privilege, you can take ownership of the risk assessment by clicking on the other user's name.
- On My Risk Assessments, the Availability column may say "Check In" or it may display five asterisks (*****). If a risk assessment's Availability cell says "Check In" then you can click that cell to move the risk assessment to Available Risk Assessments. If the cell displays five asterisks, then you own the risk assessment and cannot check it in, but you can route it.

List Windows

Icons on the My Risk Assessments Window

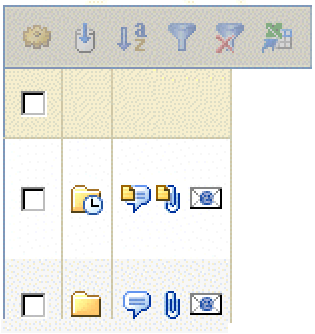
This online help describes all the icons that could appear on the My Risk Assessments window. If your screen does not display an icon that appears below, or if the icon appears but it is "dimmed" (unavailable), this is because either you do not have the associated privilege, or an Administrator has disabled the associated function.

Toolbar icons



⚙	Go to the Actions window, where you can close or route the selected risk assessment(s).
⬇	Check in the selected risk assessment(s).
↓ a z	Open the Sort window, where you can perform multiple-column sort. You can perform single-column sort by using the sort arrow (described below).
▽	Open the Filter window, where you can make selections to display only risk assessments that have certain characteristics.
☒	Remove filter (if one has been applied).
▦	Export the risk assessment list to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.

Other Icons



☐ ☐ ☐	To select all the risk assessments currently displayed, click the check box in the same row as the column headings. To select one or several risk assessments, click the check box for each risk assessment.
↑	The sort arrow appears in the column that risk assessments are sorted by, and its direction indicates whether risk assessments are sorted in ascending or descending order. The sort icon on the toolbar (described above) opens a window where you can perform multiple-column sort.

📁	Click the folder icon to open the Risk Assessment History window. The clock on the folder 📁 indicates that investigation on the corresponding risk assessment has been started.
💬 💬	Add or view risk assessment comments. The yellow box on this icon indicates that a comment has been entered for that risk assessment.
📎 📎	Add or view an attached risk assessment document. The yellow box on this icon indicates that a document has been attached to that risk assessment.
✉	Send the risk assessment details in an e-mail.

List Windows

How to select risk assessments

- To select one or several risk assessments, click the checkbox for each risk assessment in the far left column.
- To select all the risk assessments currently displayed, click the checkbox in the same row as the column headings.

List Windows

Filter risk assessments

Use the Filter window when you would like a risk assessment list to display only risk assessments that have certain characteristics.

To filter a risk assessment list

1. Click the filter icon to open the Filter window.
2. Enter information in the fields to specify which risk assessments you want to see.

    1. The fields are case-sensitive. In other words, **Stevens** is not the same as **stevens**.
    2. Enter numerals without commas or symbols (such as $).
    3. Fields that have **(contains)** in the label will look for records that contain, instead of exactly match, the characters that you enter.
3. When you are done, click **OK**.

The results of a filter are:

- The risk assessment list will be refreshed and filtered as you specified.
- The filter specifications will appear at the top of the risk assessment list.

To remove a filter

Click the Remove Filter icon. The risk assessment list will be refreshed without the filter.

Risk Assessment Actions

Check in & out

To understand this help page, you must understand owned and checked out risk assessments.

Check in risk assessments

When you check in one or more checked-out risk assessments, the risk assessments move from My Risk Assessments to Available Risk Assessments.

If the Availability column displays ***** instead of **Check In**, then you own that risk assessment and cannot check it in. If you want another user or group to investigate a risk assessment that you own, you should route the risk assessment.

To check in risk assessments

1. On My Risk Assessments, select the checkboxes for the risk assessments that you want to check in. To select all the risk assessments currently displayed, click the checkbox in the same row as the column headings.
2. Click the Check In icon .

You can also check in a risk assessment by clicking **Check In** in the Availability column for that risk assessment.

Check out risk assessments

When you check out one or more risk assessments, the risk assessments move from Available Risk Assessments to My Risk Assessments.

If a risk assessment displays another user's name in the Availability column, then that user has already checked the risk assessment out. If you have the Take Risk Assessment Ownership privilege, you can take ownership by clicking on that user's name. The risk assessment will move to My Risk Assessments, and you will own it.

To check out risk assessments

1. On Available Risk Assessments, select the checkboxes for the risk assessments that you want to check out. To select all the risk assessments currently displayed, click the checkbox in the same row as the column headings.

3. Click the Check Out icon .

You can also check out risk assessment by clicking **Check Out** in the Availability column for that risk assessment.

List Windows

The Risk Assessment Actions Window

To open the Risk Assessment Actions window, first select one or more risk assessments. Then click the Actions icon ⚙. On the Risk Assessment Actions window you can:

- Accept the proposed risk classification(s) and close the selected risk assessment(s)
- Reject the proposed risk classification(s) and close the selected risk assessment(s)
- Route the selected risk assessment(s) to another user or group

📝 Actions that you are not authorized to perform or that are not activated for your site will not appear on your screen.

To accept the proposed risk classification(s) and close the selected risk assessment(s)

top

1. Click **Close Risk Assessment - Accept**.
2. Select a reason for accepting and closing the risk assessment in the drop-down menu.
3. Click **OK**.

When you accept and close risk assessments:

- The customer's risk classification is changed immediately.
- The closed risk assessments cannot be re-activated.
- Users with Risk Assessment Query privilege can access closed risk assessments through the Risk Assessment Query window (available from the **Query** tab).

To reject the proposed risk classification(s) and close the selected risk assessment(s)

top

1. Click **Close Risk Assessment - Reject**.
2. Select a reason for rejecting and closing the risk assessment in the drop-down menu.
3. Click **OK**.

When you reject and close risk assessments:

- The customer's risk classification stays the same.
- The closed risk assessments cannot be re-activated.
- Users with Risk Assessment Query privilege can access closed risk assessments through the Risk Assessment Query window (available from the **Query** tab).

To route the selected risk assessment(s)

top

1. Click **Route To**.
2. Select another user or group.
3. Click **OK**.

When you route risk assessments:

- If you route to a user, that user becomes the owner of the risk assessment(s).
- If you route to a group, that risk assessment becomes available for check-out by members of that group.

List Windows

Available Risk Assessments

Risk assessments are an optional component of SAS Anti-Money Laundering. If you do not see the Risk Assessments tab, then System Administrators at your site have disabled risk assessment processing.

Which risk assessments are displayed here?

This window displays all the risk assessments that you are eligible to check out or take ownership of. In other words, this window displays:

- Risk assessments that belong to your group and that are not owned by any user. These risk assessments say **Check Out** in the **Availability** column.
- Risk assessments that belong to your group and that are checked out by another user. These risk assessments display the user's name in the **Availability** column. If you have Take Risk Assessment Ownership privilege, you can click on the user's name to remove the risk assessment from that user's My Risk Assessments list and place it in yours.
- If you are a manager, in addition to the above, you will see risk assessments owned and checked out by your subordinates. If your subordinates are members of groups that you are not in, you will still see the risk assessments that they own and have checked out from those groups. When viewing these risk assessments you will see the user's name in the **Availability** column. If you have Take Risk Assessment Ownership privilege, you can click on the user's name to remove the risk assessment from that user's My Risk Assessments list and place it in yours.

Unless you are a manager, this window does not display risk assessments owned by other users in your group.

By default, risk assessments are sorted by proposed risk classification. You can specify any order that suits your needs by performing a single- or multiple-column sort.

Working with Available Risk Assessments

- What the column headings mean
- What the icons mean
- How to select risk assessments
- How to check out a risk assessment
- How to select your starting tab
- How to specify the number of rows to display

List Windows

Icons on the Available Risk Assessments window

	Check out the selected risk assessment(s).
	Open the Sort window, where you can perform multiple-column sort. You can perform single-column sort by using the sort arrow (described below).
	Open the Filter window, where you can make selections to display only risk assessments that have certain characteristics.
	Remove filter (if one has been applied).
	Export the risk assessment list to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.
☐ ☐ ☐	To select all the risk assessments currently displayed, click the check box in the same row as the column headings. To select one or several risk assessments, click the check box for each risk assessment.
	The sort arrow appears in the column that risk assessments are sorted by, and its direction indicates whether risk assessments are sorted in ascending or descending order. The sort icon on the toolbar (described above) opens a window where you can perform multiple-column sort.
	Click the folder icon to open the Risk Assessment History window. The clock on the folder indicates that investigation on the corresponding risk assessment has been started.

Detail Windows

Detail Windows

Account Details

To open the Account Details window, click an account number on an alert list window, risk assessment list window, detail window, or query results window.

The **General Information** section displays basic information about the account.

Account Customers displays the name, role, and customer number of each customer on this account. Click a customer number to open the Customer Details window.

Account Households displays the household number and head-of-household name for all households that the primary owner of this account belongs to. Click a household number to open the Household Details window.

Account Attachments indicates how many comments and documents are attached to this account. Click **Comments** to open the Account Comments window. Users with the Add and View Subject Documents privilege can click **Documents** to open the Account Documents window.

All alerts for...

- **...this account** displays the number of *account* alerts associated with this account. Click the link to view these alerts.

- **...all customers on this account** displays the number of *customer* alerts associated with customers who have a role on this account. Click the link to view these alerts.

- **...all accounts related to the customers on this account** displays the number of *account* alerts associated with accounts on which customers on this account have a role. Click the link to view these alerts.

The **Account Summary** section shows the latest month's account summary detail.

Account summaries for previous months can be accessed by performing an Account Query or an Advanced Query.

System Administrators at your site determine whether a **Detail Information** section is displayed. If it is, they determine which data elements are displayed there.

If the Account Details window title ends with **At Alert Generation**, then the information here was current when the alert was generated. Click **Current account details** (in the **More Information** box) to see the most recent information. System Administrators at your site determine what changes are tracked in the system.

Also in the **More Information** box, click **More information on this account** to explore related information in the SAS Anti-Money Laundering database. System Administrators at your site determine what information is accessible here.

Detail Windows

Alert Details

To open the Alert Details window from an alert list window, click an alert's ID number.

The Alert Details window describes how and why the alert was generated, and displays (and links to) information about the alert's subject. The actions you can perform on this window are determined by your privileges and whether you own or have checked out the alert.

If you open the Alert Details window from the My Alerts window, based on the privileges you have been assigned, you will see buttons at the bottom of the window that you can use to:

- Perform actions on this alert (route, suppress, set an e-mail reminder, or close).
- View an existing regulatory report for this alert, or create a new one. This button appears when System Administrators at your site activate SAS Anti-Money Laundering's regulatory reporting facility.
- Send these details in an e-mail.

The More Information Box

The **More Information** box is one of the customizable componenets of SAS Anti-Money Laundering. System Administrators at your site determine whether the **More Information** box is displayed, and if so, what it contains.

With the default settings for the **More Information** box, you can:

- Click **Alert history** to open the Alert History window.
- Click **More alert information** to explore related information in the SAS Anti-Money Laundering database. The information presented is controlled by administrators at your site.
- Click **Near neighbors information** to open the Near Neighbors window.

Monthly Transaction History Graphs

System Administrators at your site determine whether the Account Alert Details and Customer Alert Details windows include two graphs: **Monthly Transaction Counts** and **Monthly Transaction Amounts**.

Only the Account Alert Details and Customer Alert Details windows can display the transaction history graphs.

These graphs provide the ability to perform multivariate time-series analysis on accounts and customers that have alerts. In other words, these visual representations of summarized transaction history can help you quickly detect unusual transaction activity that occurred during the last six months.

When analyzing the graphs, move the pointer over a marker to see the numbers or amounts that were plotted for the corresponding month, and click **Advanced** to open Monthly Transaction Counts/Monthly Transaction Amounts, where you can control the display of additional analysis variables and their underlying data.

By default, wire and cash transactions are plotted. System Administrators can activate other types of transactions, as well as specify whether the graphs have legends, titles, line markers, and axis labels.

The graphs will be displayed if the AML database contains at least one month of summarized transaction history for the account or customer that you are investigating. There will be no markers for months that have no data.

SAS Anti-Money Laundering will display an error message if the AML database does not contain summarized transaction history for this account or customer for any of the last six months.

Alert Transactions Table

The alert transactions table has three tabs:

1. **Triggering** - Transactions that contributed to the alert. For example, if the alert was generated by a scenario that looks for deposits made via high-risk instruments, the triggering transactions will be the deposits made via high-risk instruments. Some alerts may have no triggering transactions.
2. **Alert Associated** - Transactions that are associated with the subject of an alert. You will see the triggering transactions (denoted with a red dot ●) as well as other transactions that occurred in the time period specified by the matched scenario.
3. **All Available** - All transactions in the entire AML database for the subject of the alert, whether they contributed to the alert or not. For performance reasons, administrators at your site may set a limit on the number of transactions displayed here. Unlike the other two tabs, the All Available tab does not denote triggering transactions with a red dot ●.

Transactions are expressed in the base currency.

The maximum number of rows that can be displayed on all three tabs is set by your system administrator.

If you have the Export to CSV privilege, you will see an **Export to CSV** option. Click this link to export the data in the current tab to a comma-separated values file that can be opened in spreadsheet software such as Microsoft Excel.

The maximum number of rows that can be exported to a CSV file is set by your System Administrator. This setting could allow you to export more rows than you see on the user interface.

Detail Windows

Alert History

To open the Alert History window, open the Alert Details window and click View Alert History.

You can also click the folder icon 📁 on My Alerts or Available Alerts to open the Alert History window.

The Alert History window displays activities that have been performed on the alert you are working on, as well as who performed each action and on what date.

- The **Activity** column displays activities that have been performed on the alert.
- The **User** column indicates who performed the activity.
- The **Date - Time** column displays when the activity was performed.
- The **Details** column varies based on the activity. If the activity is a route or check-out, this column will indicate to whom the alert was routed or checked out. If the activity involves attaching a comment or document, sending e-mail, or creating a regulatory report, this column will display a system-assigned ID number for that activity.

Detail Windows

Associate Details

To open the Associate Details window, open the Transaction Details window and click the value for Associate.

The Associate Details window displays information about the associate who performed the transaction you are interested in.

System Administrators at your site determine whether a **Detail Information** section is displayed. If it is, they determine which data elements are displayed there.

If the window title indicates **at alert generation**, then the information here was current when the alert was generated. Click **View current associate details** to see the most recent information on that associate.

If the window title indicates **current**, then the information here is the most recent. If the "at alert generation" window is just like the "current" window, then the information has not changed since the alert was generated. Administrators at your site determine what changes are tracked in the system.

Detail Windows

Branch Details

To open the Branch Details window, open the Transaction Details window and click the value for Branch.

The Branch Details window displays information about the location where the transaction you are interested in occurred.

System Administrators at your site determine whether a **Detail Information** section is displayed. If it is, they determine which data elements are displayed there.

If the window title indicates **at alert generation**, then the information here was current when the alert was generated. Click **View current branch details** to see the most recent information on that branch.

If the window title indicates **current**, then the information here is the most recent. If the "at alert generation" window is just like the "current" window, then the information has not changed since the alert was generated. Administrators at your site determine what changes are tracked in the system.

The **Type** field indicates whether the transaction was conducted in a branch, at a point-of-sale (POS), or by ATM. Administrators at your site may add additional location types for your institution.

Detail Windows

Comprehensive Customer Information

The Comprehensive Customer Information window displays information about a customer, followed by information about each account related to the customer.

The customer information is comprised of:

- A link to a World Wide Web search for the customer name
- Links to Comprehensive Customer Information windows for all customers in the same household
- Lists of all comments, documents, regulatory reports, and alerts for the customer

The account information contains lists of comments, documents, regulatory reports, and alerts for each account related to the customer.

The minimize and maximize icons

Click the minimize icon to hide a table.

Click the maximize icon to display a table.

More about the customer information sections

World Wide Web Search - Click the World Wide Web search link to open a new browser window containing the results of exact matches on the customer name as it appears in the link. System Administrators at your site specify which search engine is used.

Related Customers - The Related Customers box displays all customers in the same household as the selected customer. Click a customer name to open a Comprehensive Customer Information window about that customer.

Customer Attachments - If there are comments, documents, regulatory reports, or alerts for the customer, they are displayed on this window. Click a document name to open the document. Click an alert ID to open the Alert Details window. Click a scenario name to open the Scenario Details window. Click a money laundering risk rank (ML Risk) or terror financing risk rank (TF Risk) to open the Risk Factors window.

More about the account information sections

The account information sections display information about each account related to the customer. Each related account appears under a **Related Account Information** heading.

After the account general information you will see lists of comments, documents, regulatory reports and alerts for the respective account. These lists are identical to the lists for the customer, except that the lists relate directly to the account, and not the customer. In other words, the comments and documents are account comments and documents, the regulatory reports are on account level alerts and the alerts list is of account level alerts for that account.

Detail Windows

Customer Details

To open the Customer Details window, click a customer number on an alert list window, detail window, or query results window.

The **General Information** section displays the customer's name and customer number, the customer's risk classification, and other basic information about the customer.

Customer Accounts displays the account number and primary owner of each account associated with this customer. Click an account number to open the Account Details window.

Customer Households displays the household number and head-of-household name for all households that this customer belongs to. Click a household number to open the Household Details window.

Customer Attachments indicates how many comments and documents are attached to this customer. Click **Comments** to open the Customer Comments window. Users with the Add and View Subject Documents privilege can click **Documents** to open the Customer Documents window.

All alerts for...

- **...this customer** displays the number of *customer* alerts associated with this customer. Click the link to view these alerts.

- **...all accounts related to this customer** displays the number of *account* alerts associated with accounts on which this customer has any role. Click the link to view these alerts.

The **Customer Summary**, **Employment**, and **Contact Information** sections provide more details about the customer.

System Administrators at your site determine whether a **Detail Information** section is displayed. If it is, they determine which data elements are displayed there.

If the Customer Details window title ends with **At Alert Generation**, then the information here was current when the alert was generated. Click **Current customer details** (in the **More Information** box) to see the most recent information. System Administrators at your site determine what changes are tracked in the system.

Also in the **More Information** box:

- Click **Customer Transactions** to see all the transactions that are available for this customer.

- Click **Comprehensive customer information** to see all available data about this customer.

- Click **Related entities** to see customers, accounts, and households with the same tax ID, address, phone, employer, or name as the selected customer's.

- Click **More information on this account** to explore related information in the SAS Anti-Money Laundering database. System Administrators at your site determine what information is accessible here.

Detail Windows

Customer Transactions

To open the Customer Transactions window, open the Customer Details window and in the More Information box, click Customer transactions.

The Customer Transactions window displays all the transactions that are in the database for the selected customer.

What the icons mean

↓az	Open the Sort window, where you can perform multiple-column sort. You can perform single-column sort by using the sort arrow (described below).
▼	Open the Filter window, where you can make selections to display only transactions that have certain characteristics.
▼✗	Remove filter (if one has been applied).
⊞	Export the transaction list to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.
▲	The sort arrow appears in the column that transactions are sorted by, and its direction indicates whether transactions are sorted in ascending or descending order. The sort icon on the toolbar (described above) opens a window where you can perform multiple-column sort.

💡 You can specify *temporary* and *persistent* numbers of rows to display on the Customer Transactions window. Entering a very large value will make the page take longer to display and may cause your browser to time out.

What the column headings mean

Transaction Number: Your institution assigns each transaction a unique identification number. Click a transaction number to open the Transaction Details window.

Account Number: The unique identification number for the account associated with the transaction. Click an account number to open the Account Details window.

Role: The person executing the transaction may be the primary owner, secondary owner, signer, beneficiary, or insured. System Administrators at your site may add other roles.

Date: The date on which the transaction was executed.

Amount: The amount of the transaction expressed in the base currency.

Currency: The original transaction currency.

C/D/I: Denotes whether the transaction was a debit, credit, or event.

Primary Medium: The primary meduim for executing the transaction. Possible values are cash and check.

Secondary Medium: The secondary description of the meduim used in the transaction. Possible values are US, non_USD, personal, cashiers, and counter.

Mechanism: How the transaction was executed. Possible values include teller, ATM, and online.

Country: The country where the transaction occurred.

Second Account Number: If the transaction was an internal transfer, this column will contain the secondary account number. Otherwise, this column will be blank.

Related: Y indicates that the transaction took place between related accounts. N indicates that it did not.

Third Party: Y indicates that a third party is associated with the transaction. N indicates that no third party is associated with the transaction.

Remitter: The extermal party that initiated the transaction.

Beneficiary: The extermal party that received the transaction.

Branch: The branch where the transaction took place.

Associate: The associate is a person from the financial institution and the name represents either the person who executed the transaction or the name of the person assigned to the account.

Transaction Description: This typically provides a more detailed description of the transaction than the C/D/I column.

Status Description: The state of the transaction. Possible values include success and denied.

Detail Windows

External Party Details

To open the External Party Details window, open the Transaction Details window. If there is an external party on the transaction, Transaction Details will include rows for Remitter and Beneficiary. Click these values to open the External Party Details window.

The External Party Details window displays information about an external remitter or beneficiary on a transaction.

System Administrators at your site determine whether a **Detail Information** section is displayed. If it is, they determine which data elements are displayed there.

Click **View more information on this external party** to explore related information in the SAS Anti-Money Laundering database. The information presented is controlled by administrators at your site.

Detail Windows

Funds Tracker Network

To open the Funds Tracker Network window from an alert list window, open the Account Details window by clicking the value for Subject Number on an account-based alert. If Funds Tracker data is available for this account, the More Information box will include an option to View Funds Tracker network.

The Funds Tracker network shows movement of funds between accounts. When you are investigating accounts with wires or unusual internal transfers, the Funds Tracker network for that account will shed light on where the funds are coming from and where they are going.

When your financial institution acts as an intermediary on a wire, the transaction will not be displayed on the Funds Tracker network.

Understanding the chart

- The chart is a visual representation of the data in the table.
- The circles represent nodes, or accounts.
- The arrows represent edges, or relationships. The direction of the arrows indicates the direction of the flow of funds. The width of the arrows increases with the amount of money involved in the transfer(s). The chart legend defines the meaning of the colors.
- A "related" journal, or internal transfer, is one that takes place between accounts that have some sort of relationship. For example, when a customer transfers funds from his savings account to his wife's checking account, this is a related journal. Your implementation team determines what characteristics define "related" and flag it in the data model.

If the number of relationships exceeds a threshold established by administrators at your site, the chart will not be displayed.

Understanding the table

The modify icon is visible to users with Modify Funds Tracker Network privilege. Click this icon to remove legitimate relationships from the network and to change an unrelated relationship to related, or vice-versa. Specifically you can:

- **Exclude beneficiary/remitter combination** - Use this option to prevent the display of two accounts that frequently conduct legitimate exchanges.
- **Exclude remitter from being the source** - Use this option to prevent the display of a legitimate disbursement account as a remitter. For example, a disbursement account for a 401(k) program is a frequent remitter in many relationships.
- **Exclude beneficiary from being the destination** - Use this option to prevent the display of a legitimate collection account as a beneficiary. For example, an account into which consumers of a service transfer money to pay their bills is a frequent beneficiary in many relationships.
- **Mark unrelated as related, or mark related as unrelated** - If two accounts considered unrelated are found to be related, or vice-versa, you can change the nature of the relationship within the network.

Modifications made here are reflected on the user interface upon the next execution of the alert generation process.

The numbers in the **Relationship** column are not used in the analysis. They are just a simple way to refer to a relationship.

For accounts belonging to clients of your financial institution, the **Remitter** and **Beneficiary** columns display the account numbers, and you can click an account number to open the Account Details window. For external accounts, the contents of the **Remitter** and **Beneficiary** columns is determined by your implementation team. The suggested value is "bank number;account number."

The **First Transaction Date** is the date of the earliest transaction considered in building the network.

The **Number of Transactions** tells how many transactions are considered in this analysis and displayed on the chart.

The **Amount** column is the sum of all the transactions in the relationship within the interval considered in building the network.

Detail Windows

Household Details

To open the Household Details window, click a household number on an alert list window, detail window, or query results window.

The **General Information** and **Street Address** sections display basic information about the household.

Household Customers displays the name and customer number of each customer in this household. Click a customer number to open the Customer Details window.

Household Accounts displays account number and primary owner of each account associated with this household. Click an account number to open the Account Details window.

Household Attachments indicates how many comments and documents are attached to this household. Click **Comments** to open the Household Comments window. Users with the Add and View Subject Documents privilege can click **Documents** to open the Household Documents window.

All alerts for...

- **...this household** displays the number of *household* alerts associated with this household. Click the link to view these alerts.
- **...all customers in this household** displays the number of *customer* alerts for all members of this household. Click the link to view these alerts.
- **...all accounts in this household** displays the number of *account* alerts related to this household. Click the link to view these alerts.

If the Household Details window title ends with **At Alert Generation**, then the information here was current when the alert was generated. Click **Current customer details** (in the **More Information** box) to see the most recent information. System Administrators at your site determine what changes are tracked in the system.

Also in the **More Information** box, click **More information on this household** to explore related information in the SAS Anti-Money Laundering database. System Administrators at your site determine what information is accessible here.

Detail Windows

Near Neighbors

To open the Near Neighbors window, open the Alert Details window and click View Near Neighbors information in the **More Information** box.

The Near Neighbors window displays accounts that have similar behavior to any account potentially associated with the selected alert (which on this window is called the "target account"). You can use this information to identify potentially suspicious behavior that may not have matched the particular requirements of a scenario.

To generate this information, SAS Anti-Money Laundering analyzes the transaction history of all accounts that are related to alerts, and identifies all accounts showing a similar transaction history over the past six months.

- The **General Information** section describes the alert for which the analysis was done.
- The next section displays the target account number and name, and then lists the near neighbor accounts in rank order, with the most similar account listed first.

  The far-right column gives the "distance," which is a description of how similar this account is to the target. If the distance is 0, the account is exactly the same as the target. The larger the number, the less similar the account is to the target.

💡 Another way your institution may choose to use near neighbor analysis is to save a particularly suspicious account history and compare accounts to it on an ongoing basis. The resulting near neighbor analyses are displayed on the Reports tab. Instructions for how to do this are in the **System Administrator's Guide**.

Detail Windows

Related Entities

To open the Related Entities window from an alert list window, open the Customer Details window by clicking the value for Subject Number on an customer-based alert. Click Related entities investigation for this customer.

Administrators at your site determine how many related entities can be displayed.

The Related Entities window displays customers, accounts, and households with the same tax ID, address, phone, employer, or name as the selected customer's.

The **Customer Information** box displays the name and customer number of the selected customer.

The **Tax ID** box displays the selected customer's tax ID in the shaded field, and if any other customers, accounts, or households have the same tax ID, they is displayed on subsequent rows. Click a customer number to open the Customer Details window, click an account number to open the Account Details window, or click a household number to open the Household Details window.

The **Address**, **Phone**, **Employer**, and **Name** fields follow the same format as the **Tax ID** box.

Detail Windows

Risk Assessment Details

To open the Risk Assessment Details window from a risk assessment list window, click a risk assessment's ID number.

In general, the left side of the Risk Assessment Details window displays information about the risk assessment, the right side displays information about the customer whose risk classification is being assessed, and the bottom displays information about the risk classifiers.

In the **Risk Assessment Attachments** section, click **Comments** to open the Risk Assessment Comments window and click **Documents** to open the Risk Assessment Documents window.

In the **Customer Information** section, click **Customer Number** to open the Customer Details window. Click **Customer Comments** to open the Customer Comments window and click **Customer Documents** to open the Customer Documents window.

System Administrators at your site determine whether a **Detail Information** section is displayed. If it is, they determine which data elements are displayed there.

In the **More Information** box, click **Risk assessment history** to open the Risk Assessment History window.

The risk classifiers table at the bottom of this window has two tabs.

1. **Risk Classifiers** - Risk classifiers that contributed to the risk assessment.

3. **All Risk Classifiers** - All active risk classifiers.

The following is a description of the column headings in the risk classifiers table:

Name - The name of the risk classifier. Click the value for name to open the Risk Classifier Details window.

Date - The date on which the risk classifier was created.

Description - A brief description of the risk classifier.

Threshold - The limit that defines when the risk classifier contributes to the classification score. Not all risk classifiers have thresholds.

Detail Windows

Risk Assessment History

Click the folder icon 📁 to open the Risk Assessment History window from a risk assessment list window.

The Risk Assessment History window displays activities that have been performed on the risk assessment you are working on, as well as who performed each action and on what date.

- The **Activity** column displays activities that have been performed on the risk assessment.
- The **User** column indicates who performed the activity.
- The **Date - Time** column displays when the activity was performed.
- The **Details** column varies based on the activity. If the activity is a route or check-out, this column will indicate to whom the risk assessment was routed or checked out. If the activity involves attaching a comment or document, or sending e-mail, this column will display a system-assigned ID number for that activity.

Detail Windows

Risk Classifier Details

To open the Risk Classifier Details window, click a risk classifier name on the Risk Assessment Details window.s

The Risk Classifier Details window gives information about a single risk classifier.

Classifier Name - The name of the risk classifier can contain up to 35 characters. SAS-shipped risk classifiers use the following naming convention: SASRC#####.

Long Description - The user who added the risk assessment may have entered a long description. This optional field can contain up to 255 characters.

Short Description - The user who added the risk assessment may have entered a short description. This optional field can contain up to 35 characters.

Type - There are five types of risk classifiers.

1. Account or Customer Numbers
2. Account or Customer - Other
3. Customer Monthly Profile
4. Account or Customer Indicators
5. Custom

Active - Y means the risk classifier is being used by the risk classification process; N means it is not being used.

Weight - A number that tells the risk classification process how significantly this risk classifier should affect the overall score for the customer, relative to other risk classifiers. For example, a risk classifier with a weight of **10** contributes to the overall customer score five times as much as a risk classifier with a weight of **2**. Each financial institution determines the range of values to use (for example, 1 through 10 or 1 through 100). Elsewhere in the system, the ranges for high, medium, and low risk classifications are set.

Source Table - FSC_ACCOUNT_DIM, FSC_PARTY_DIM or FSC_PARTY_PROFILE_FACT.

Source Column - The column in the source table that this risk classifier analyzes during the risk classification process.

Indicator Value - This field is used by risk classifiers that examine indicator columns in the data. This is the value that the risk classifier looks for.

Classifier Fact Column - This column is where the risk classification process will store the results of this risk classifier.

Operator - If this risk classifier looks for counts, an operator and threshold value will be displayed. For example, a risk classifier might look for a wire count *greater than* (displayed as GT) 20. The possible values operator are less than (LT), greater than (GT), or equals (EQ).

Threshold - For risk classifiers looking for counts, the threshold is the numeric limit for analysis conditions. In the operator example above, the threshold is 20.

Category - Risk classifiers are organized in categories. Compliance Administrators at your site can create, modify, and delete categories.

List - Two types of risk classifiers use lists: Account or Customer Numbers and Account or Customer - Other. This field displays the name of the list that stores the values that this risk classifier uses.

Create Date - Date the risk classifier was created.

Detail Windows

Risk Factors

To open the Risk Factors window from an alert list window, click the value for money laundering risk or for terror financing risk.

The Risk Factors window displays the risk factors that matched the alert. Risk factor matches provide additional information that may be indicative of suspicious activity, and they elevate the risk score.

The table on top of the Risk Factors window displays some basic information about the alert. If the scenario name is ML_RISK or TF_RISK, the alert is a risk-factor-only alert.

The table below describes the risk factors that were present when the alert was created. Click the value for **Risk Factor** to view details about that risk factor.

Detail Windows

Risk Factor Details

To open the Risk Factor Details window from an alert list window, click the value for money laundering risk or for terror financing risk. Then, on the Risk Factors window, click a risk factor name.

The Risk Factor Details window gives information about the selected risk factor.

Risk Factor Type will be "AML" for SAS Anti-Money Laundering risk factors.

Risk Factor Status indicates whether the risk factor is active or inactive. A risk factor is active when it is included in the alert generation process, and inactive when it is not. System Administrators at your site control status of risk factors.

Create Date displays the date on which the risk factor was created.

If the risk factor is inactive, **End Date** displays the date on which it became inactive. If the risk factor is active, this value will be Jan 1, 5999.

The **Parameters** section describes how the parameters were set when the alert was generated.

Detail Windows

Scenario Details

To open the Scenario Details window, click the value for Scenario on an alert list window.

The Scenario Details window gives information about the scenario that triggered an alert.

Scenario Type will be "AML" for SAS Anti-Money Laundering scenarios.

Scenario Status indicates whether the scenario is active or inactive. A scenario is active when it is included in the alert generation process, and inactive when it is not. Administrators at your site control status of scenarios.

Create Date displays the date on which the scenario was created.

If the scenario is inactive, **End Date** displays the date on which it became inactive. If the scenario is active, this value will be Jan 1, 5999.

The **Parameters** section describes how the parameters were set when the alert was generated. If the alert was created manually, or if it is a risk-factor-only alert, it will not have scenario parameter values.

Detail Windows

Transaction Details

To open the Transaction Details window...

- **For a transaction-based alert that appears on an alert list window, click the value for Subject Number.**

- **For all alert types, open the Alert Details window and click a value for Reference Number in the Alert Transactions table.**

- **On the Customer Transactions window, click a value in the Transaction Number column.**

The Transaction Details window displays information related to a single transaction.

- Click the value for Account Number to view Account Details for that account.
- Click the value for Branch to view the Branch Details window.
- Click the value for Associate to view the Associate Details window.
- Click the value for Executing Party to view Customer Details for that customer.

If one or more external parties were involved with the transaction, you will see a row for Remitter, for Beneficiary, or for both, depending on the external party's role(s). Click these values to open the External Party Details window.

System Administrators at your site determine whether a **Detail Information** section is displayed. If it is, they determine which data elements are displayed there.

Click **View more information on this transaction** to explore related information in the SAS Anti-Money Laundering database. The information presented is controlled by administrators at your site.

Alert Actions

Alert Actions

Activate a closed or suppressed alert

You will be the owner of any alerts that you activate.

You must have the Activate Suppressed Alerts privilege to access the Suppressed Alerts window, and you must have the Activate Closed Alerts privilege to access the Closed Alerts window.

To activate a suppressed or closed alert

1. On the Suppressed Alerts or Closed Alerts window, select the alert(s) to activate.
2. Click the Activate icon 🚦.

When you activate alerts

- You will be the owner of alerts that you activate.
- The date on which the investigation started will not be the date you unsuppressed the alert; instead it will be the first date on which a user performed an action that started the investigation. The Alert History window displays the date on which the investigation was started, as well as the user who performed the action that started the investigation.

💡 You can also activate an alert by clicking **Activate** in the **Availability** column for that alert.

Alert Actions

Alert comments

An alert comment is a comment that is attached to an alert.

- You can view comments for alerts that are on Available Alerts.
- You can add and view comments for alerts that are on My Alerts. In other words, you can perform these actions on alerts that you own or have checked out.
- If you have the Delete Alert Comments privilege, you can delete comments that you added to alerts that are on My Alerts. If you are a manager and you have the Delete Alert Comments privilege, you can also delete alert comments added by your subordinates.
- Users with the associated privileges can also enter comments for accounts, customers, and households, as well as for risk assessments.

A yellow box over the Comments icon on My Alerts indicates that a comment has been added to that alert. Although you cannot edit existing comments, you can add as many additional comments as you need to.

To open the Alert Comments window

- If you are viewing My Alerts, click the Comments icon.
- If you are viewing Available Alerts, click the **Alert ID** to open the Alert Details window. Under **Alert Attachments**, click **Comments**.

To add or view an alert comment

1. Open the Alert Comments window as described above.
2. **View:** If there are attached comments, the window will display them in the order they were added.
   Comments that users enter when creating and suppressing alerts appear on the Alert Comments window.
3. **Add:** Enter your comment in the **Add New Comment** box. You can enter up to 2,000 characters. When your comment is complete, click **Save Comment**.

To delete an alert comment

The Delete Comment icon is displayed for comments that you can delete. If you have the Delete Alert Comments privilege, you can delete comments that you added. If you are a manager and you have the Delete Alert Comments privilege, you can also delete comments added by your subordinates.

1. Open the Alert Comments window as described above.
2. Click the Delete Comment icon.

Alert Actions

Alert documents

An alert document is a document that is attached to an alert.

- If you have the Add and View Alert Documents privilege, you can view documents for alerts that are on Available Alerts.
- If you have the Add and View Alert Documents privilege, you can add and view documents for alerts that are on My Alerts. In other words, you can perform these actions on alerts that you own or have checked out.
- If you have the Delete Alert Documents privilege, you can delete documents that you added to alerts that are on My Alerts. If you are a manager and you have the Delete Alert Documents privilege, you can also delete alert documents added by your subordinates.
- Your client and browser settings determine which document types can be displayed and whether the **File** download dialog appears.
- Users with the associated privileges can also enter documents for accounts, customers, and households, as well as for risk assessments.

A yellow box over the Documents icon on My Alerts indicates that a document has been added to that alert. Although you cannot edit existing documents, you can add as many additional documents as you need to.

To open the Alert Documents window

- If you are viewing My Alerts, click the Documents icon .
- If you are viewing Available Alerts, click the **Alert ID** to open the Alert Details window. Under **Alert Attachments**, click **Documents**.

To view an existing alert document

1. Open the Alert Documents window as described above. If there are attached documents, they are displayed in the order they were added.
2. Click on the document name.

To add an alert document

1. Open the Alert Documents window as described above.
2. Click **Browse** to select the document from your local directory structure.
3. Optionally, enter a description of the document in the **Description** field. The description is displayed along with the document name in the **Document Name** column.
4. Click **Attach Document**.

To delete an alert document

The Delete Document icon is displayed for documents that you can delete. If you have the Delete Alert Documents privilege, you can delete documents that you added. If you are a manager and you have the Delete Alert Documents privilege, you can also delete documents added by your subordinates.

1. Open the Alert Documents window as described above.
2. Click the Delete Document icon .

Alert Actions

Check in & out

To understand this help page, you must understand owned and checked out alerts.

Check in alerts

When you check in one or more checked-out alerts, the alerts move from My Alerts to Available Alerts.

If the Availability column displays ***** instead of **Check In**, then you own that alert and cannot check it in. If you want another user or group to investigate an alert that you own, you should route the alert.

To check in alerts

1. On My Alerts, select the checkboxes for the alerts that you want to check in. To select all the alerts currently displayed, click the checkbox in the same row as the column headings.
2. Click the Check In icon .

You can also check in an alert by clicking **Check In** in the Availability column for that alert.

Check out alerts

When you check out one or more alerts, the alerts move from Available Alerts to My Alerts.

If an alert displays another user's name in the Availability column, then that user has already checked the alert out. If you have the Take Alert Ownership privilege, you can take ownership by clicking on that user's name. The alert will move to My Alerts, and you will own it.

To check out alerts

1. On Available Alerts, select the checkboxes for the alerts that you want to check out. To select all the alerts currently displayed, click the checkbox in the same row as the column headings.

3. Click the Check Out icon .

You can also check out an alert by clicking **Check Out** in the Availability column for that alert.

Alert Actions

Close an alert

You can close alerts that appear on My Alerts.

To close an alert

1. On My Alerts, select the alert(s) that you want to close.
2. Click the **Actions** icon ⚙.
3. On the Alert Actions window, select **Close Alert**.
4. Select a reason for closing the alert(s) in the drop-down menu. System Administrators at your site control the list of possible reasons for closing alerts.
5. Click **OK**.

When you close alerts:

- Only users with the Activate Closed Alerts privilege can access the Closed Alerts window and activate closed alerts.

- Closed alerts are not displayed on My Alerts or Available Alerts.

Alert Actions

Create an alert

- You will be the owner of any alerts that you create.
- All fields except the **Comment** are required.

To create an alert:

1. Select a subject. The subject is the account, customer, household, or transaction that exhibited the behavior that caused the alert.
2. In the **Number** field, enter the subject number. (In other words, for an account alert, enter the account number; for a customer alert, enter the customer number; and so on.)
3. From the **Reason** menu, select the reason you are creating this alert. The reason will appear as the **Description** on the alert list windows and various detail windows. Administrators at your site control the list of possible reasons for closing alerts.
   the list of possible reasons for creating alerts.
5. Use the **Run Date** field to specify the date on which the suspicious activity took place. You can click in the field and enter a date, or click the calendar icon to select one. The **Run Date** that you enter and the **Create Date** is displayed on the Alert Details window, while the alert list windows will display only the **Create Date**.

   💡 In the **Comment** field, you might want to explain the basis of your **Run Date**.
6. Enter values for **Money Laundering Risk** and **Terror Financing Risk**.

   💡 When assigning a risk rank, any integer between one and 999 is allowed. Since you discovered activity suspicious enough to create an alert, the risk should presumably be on the high end.
7. Enter a **Comment** about the suspicious activity. The text you enter will be attached to the alert as a comment. This field is optional.
8. Click **Save**. The system will create the alert. The ID of the new alert will appear on the Create Alert window, and the new alert will appear in My Alerts.

Alert Actions

Route an alert

Users with the Route Alerts privilege can route alerts that appear on My Alerts to other users and groups.

To route an alert

1. On My Alerts, select the alert(s) that you want to route.
2. Click the Actions Icon ⚙.
3. On the Alert Actions window, click **Route To**.
4. Select a user or group.
5. Click **Submit**.

When you route alerts:

- If you route an alert to a user, that user becomes the owner of that alert.
- If you route an alert to a group, that alert becomes available for check-out by members of that group.

Alert Actions

Send alert e-mail

You can send an e-mail message that has the Alert Details window, as well as associated comments and documents, included as attached files. You can send the message to anyone with an e-mail address, at any domain.

- E-mail functionality is only available for alerts listed in My Alerts.
- The alert details file attached to the message will be exactly like the Alert Details window, except the e-mail message will not include hyperlinks to further information.
- You cannot prevent any of the attachments from being sent. Although you can delete the **Attachment(s)** text in the message body, all listed files will still be attached.
- The e-mail message will be from "SAS AML Alert Service."
- Recipients cannot reply to e-mail messages sent from the solution.

To send the alert details in an e-mail

1. Open the Alert E-mail window by either:
    Clicking the **E-mail** icon ✉ on the My Alerts window.
    Clicking the **E-mail** button on the Alert Details window.
3. Enter recipient(s) address(es) in the **To** field.

    💡 By default, SAS Anti-Money Laundering will automatically send a copy of this message to the e-mail address associated with your user profile.
4. Edit the **Subject** if you want to. The default subject will be "SAS Anti-Money Laundering Alert: ID# (system-assigned ID number)."
5. Edit the **Message** if you want to. By default it will include the alert description, the account holder's name, a list of attachments (the alert details and any existing comments and documents), and your name.
6. Click **Send Message**.

Alert Actions

Set an e-mail reminder

You can use this feature to send yourself reminder e-mails about alerts that are in My Alerts.

To set an e-mail reminder

1. On My Alerts, select the alert(s) for which you would like to receive e-mail reminders.
2. Click the Actions icon ⚙.
3. On the Actions window, click **Set E-mail Reminder**.
4. Enter the date on which you would like to receive the reminder, or click the Calendar icon to select one.
5. Click **Submit**.

When you set an e-mail reminder:

- You will receive one e-mail message for each selected alert on the day that you specify.
- You cannot delete or remove the reminder.
- If another user takes ownership of an alert that you have set a reminder for, you will still get the reminder.

Alert Actions

Suppress an alert

If you have Suppress Alerts privilege, you can suppress alerts that are on My Alerts. When you suppress an alert, that alert is not displayed on My Alerts or Available Alerts, and alerts for that scenario are not displayed for that subject for the duration that you specify.

To suppress an alert

1. On My Alerts, select the alert(s) that you want to suppress.
2. Click the Actions icon ⚙.
3. On the Actions window, click **Suppress**.
4. Enter how long you would like to suppress the alert:
    1. If you want to suppress the alert permanently, select **Permanently Suppress**.
    2. If you want to suppress it for a specific period of time, select **Suppress Until**. Enter a date or click the calendar icon to select one.
5. Enter the reason you are suppressing the alert. This will be attached to the alert in the form of an alert comment.
6. Click **Submit**.

When you suppress alerts:

- Only users with Activate Suppressed Alerts privilege can access the Suppressed Alerts window and "unsuppress" and alert.
- Suppressed alerts are not displayed on My Alerts or Available Alerts, and alerts for that scenario are not displayed for that subject for the duration that you specify.
- The status code for alerts that you suppress here will change from **Active** to **Suppressed (UI)**.

Risk Assessment Actions

Risk Assessment Actions

Check in & out

To understand this help page, you must understand owned and checked out risk assessments.

Check in risk assessments

When you check in one or more checked-out risk assessments, the risk assessments move from My Risk Assessments to Available Risk Assessments.

If the Availability column displays ***** instead of **Check In**, then you own that risk assessment and cannot check it in. If you want another user or group to investigate a risk assessment that you own, you should route the risk assessment.

To check in risk assessments

1. On My Risk Assessments, select the checkboxes for the risk assessments that you want to check in. To select all the risk assessments currently displayed, click the checkbox in the same row as the column headings.
2. Click the Check In icon .

You can also check in a risk assessment by clicking **Check In** in the Availability column for that risk assessment.

Check out risk assessments

When you check out one or more risk assessments, the risk assessments move from Available Risk Assessments to My Risk Assessments.

If a risk assessment displays another user's name in the Availability column, then that user has already checked the risk assessment out. If you have the Take Risk Assessment Ownership privilege, you can take ownership by clicking on that user's name. The risk assessment will move to My Risk Assessments, and you will own it.

To check out risk assessments

1. On Available Risk Assessments, select the checkboxes for the risk assessments that you want to check out. To select all the risk assessments currently displayed, click the checkbox in the same row as the column headings.

3. Click the Check Out icon .

You can also check out risk assessment by clicking **Check Out** in the Availability column for that risk assessment.

Performing Actions

Close a risk assessment

You can close risk assessments that appear on My Risk Assessments.

To close a risk assessment

1. On My Risk Assessments, select the risk assessment(s) that you want to close.
2. Click the **Actions** icon ⚙.
3. On the Risk Assessment Actions window, click the appropriate button:
    1. Click **Close Risk Assessment - Accept** to accept the proposed risk classification(s).

    3. Click **Close Risk Assessment - Reject** to reject the proposed risk classification(s).
4. Select a reason for accepting or rejecting the proposed risk classification(s) in the corresponding drop-down menu. System Administrators at your site control the list of possible reasons for closing risk assessments.
5. Click **OK**.

When you close risk assessments:

- If you accept the proposed risk classification, the change takes effect immediately. If you reject the proposed risk classification, the risk assessment is closed but no other change occurs.
- Closed risk assessments cannot be re-activated.
- Closed risk assessments are not displayed on My Risk Assessments or Available Risk Assessments.
- Users with the Risk Assessment Query privilege can access closed risk assessments through the Risk Assessment Query window (available from the **Query** tab).

Risk Assessment Actions

Create a risk assessment

- You will be the owner of any risk assessments that you create.
- All fields except the **Comment** are required.
- You cannot create a risk assessment for a customer who already has an active risk assessment.

To create a risk assessment:

1. In the **Customer Number** field, enter the number of the customer whose risk you want to assess.
2. From the **Reason** menu, select the reason you are creating this risk assessment. The reason is displayed on the Risk Assessment History window. System Administrators at your site control the list of possible reasons for creating risk assessments.
3. Use the **Create Date** field to specify an appropriate date. You can click in the field and enter a date, or click the calendar icon to select one. The create date is displayed on all risk assessment windows.

   💡 In the **Comment** field, you might want to explain the basis of your create date.
4. Enter the **Risk Classification** that you are proposing for the customer.
5. Optionally, enter a **Comment**. The text you enter will be attached to the risk assessment as a risk assessment comment.
6. Click **Save**. The system will create the risk assessment. The ID of the new risk assessment will appear on the Create Risk Assessment window, and the new risk assessment will appear in My Risk Assessments.

Risk Assessment Actions

Risk assessment comments

A risk assessment comment is a comment that is attached to a risk assessment.

- You can view comments for risk assessments that are on Available Risk Assessments.
- You can add and view comments for risk assessments that are on My Risk Assessments. In other words, you can perform these actions on risk assessments that you own or have checked out.
- If you have the Delete Risk Assessment Comments privilege, you can delete comments that you added to risk assessments that are on My Risk Assessments. If you are a manager and you have the Delete Risk Assessment Comments privilege, you can also delete risk assessment comments added by your subordinates.
- Users with the associated privileges can also enter comments for accounts, customers, and households, as well as for alerts.

A yellow box over the Comments icon on My Risk Assessments indicates that a comment has been added to that risk assessment. Although you cannot edit existing comments, you can add as many additional comments as you need to.

To open the Risk Assessment Comments window

- If you are viewing My Risk Assessments, click the Comments icon .
- If you are viewing Available Risk Assessments, click the **Risk Assessment ID** to open the Risk Assessment Details window. Under **Risk Assessment Attachments**, click **Comments**.

To add or view a risk assessment comment

1. Open the Risk Assessment Comments window as described above.
2. **View:** If there are attached comments, the window will display them in the order they were added.

   Comments that users enter when creating risk assessments appear on the Risk Assessment Comments window.

3. **Add:** Enter your comment in the **Add New Comment** box. You can enter up to 2,000 characters. When your comment is complete, click **Save Comment**.

To delete a risk assessment comment

The Delete Comment icon is displayed for comments that you can delete. If you have the Delete Risk Assessment Comments privilege, you can delete comments that you added. If you are a manager and you have the Delete Risk Assessment Comments privilege, you can also delete comments added by your subordinates.

1. Open the Risk Assessment Comments window as described above.
2. Click the Delete Comment icon .

Risk Assessment Actions

Risk assessment documents

A risk assessment document is a document that is attached to a risk assessment.

- If you have the Add and View Risk Assessment Documents privilege, you can view documents for risk assessments that are on Available Risk Assessments.
- If you have the Add and View Risk Assessment Documents privilege, you can add and view documents for risk assessments that are on My Risk Assessments. In other words, you can perform these actions on risk assessments that you own or have checked out.
- If you have the Delete Risk Assessment Documents privilege, you can delete documents that you added to risk assessments that are on My Risk Assessments. If you are a manager and you have the Delete Risk Assessment Documents privilege, you can also delete risk assessment documents added by your subordinates.
- Your client and browser settings determine which document types can be displayed and whether the **File** download dialog appears.
- Users with the associated privileges can also enter documents for accounts, customers, and households, as well as for alerts.

A yellow box over the Documents icon on My Risk Assessments indicates that a document has been added to that risk assessment. Although you cannot edit existing documents, you can add as many additional documents as you need to.

To open the Risk Assessment Documents window

- If you are viewing My Risk Assessments, click the Documents icon .
- If you are viewing Available Risk Assessments, click the **Risk Assessment ID** to open the Risk Assessment Details window. Under **Risk Assessment Attachments**, click **Documents**.

To view an existing risk assessment document

1. Open the Risk Assessment Documents window as described above. If there are attached documents, they are displayed in the order they were added.
2. Click on the document name.

To add a risk assessment document

1. Open the Risk Assessment Documents window as described above.
2. Click **Browse** to select the document from your local directory structure.
3. Optionally, enter a description of the document in the **Description** field. The description is displayed along with the document name in the **Document Name** column.
4. Click **Attach Document**.

To delete a risk assessment document

The Delete Document icon is displayed for documents that you can delete. If you have the Delete Risk Assessment Documents privilege, you can delete documents that you added. If you are a manager and you have the Delete Risk Assessment Documents privilege, you can also delete documents added by your subordinates.

1. Open the Risk Assessment Documents window as described above.
2. Click the Delete Document icon .

Risk Assessment Actions

Route a risk assessment

Users with the Route Risk Assessments privilege can route risk assessments that appear on My Risk Assessmets to other users and groups.

To route a risk assessment

1. On My Risk Assessments, select the risk assessment(s) that you want to route.
2. Click the Actions Icon ⚙.
3. On the Risk Assessment Actions window, click **Route To**.
4. Select a user or group.
5. Click **Submit**.

When you route risk assessments:

- If you route a risk assessment to a user, that user becomes the owner of that risk assessment.
- If you route a risk assessment to a group, that risk assessment becomes available for check-out by members of that group.

Risk Assessment Actions

Send risk assessment e-mail

You can send an e-mail message that has the Risk Assessment Details window, as well as associated comments and documents, included as attached files. You can send the message to anyone with an e-mail address, at any domain.

- E-mail functionality is only available for risk assessments listed in My Risk Assessments.
- The risk assessment details file attached to the message will be exactly like the Risk Assessment Details window, except the e-mail message will not include hyperlinks to further information.
- You cannot prevent any of the attachments from being sent. Although you can delete the **Attachment(s)** text in the message body, all listed files will still be attached.
- The e-mail message will be from "SAS AML Risk Assessment Service."
- Recipients cannot reply to e-mail messages sent from the solution.

To send the risk assessment details in an e-mail

1. Open the Risk Assessment E-mail window by either:
    Clicking the **E-mail** icon ✉ on the My Risk Assessments window.
    Clicking the **E-mail** button on the Risk Assessment Details window.
3. Enter recipient(s) address(es) in the **To** field.

    💡 By default, SAS Anti-Money Laundering will automatically send a copy of this message to the e-mail address associated with your user profile.
4. Edit the **Subject** if you want to. The default subject will be "SAS Anti-Money Laundering Risk Assessment: ID# (system-assigned ID number)."
5. Edit the **Message** if you want to. By default it will include the risk assessment description, the account holder's name, a list of attachments (the risk assessment details and any existing comments and documents), and your name.
6. Click **Send Message**.

Other Actions

Other Actions

Account, customer, and household comments

Subject comments are comments attached to accounts, customers, and households. Although transactions can also be subjects of alerts, you cannot attach comments to transactions.

- You can view and add comments for accounts, customers, and households that appear on any of the alert list or risk assessment list windows that you have access to.
- If you have the Delete Subject Comments privilege, you can delete comments that you added to accounts, customers, and households. If you are a manager and you have the Delete Subject Comments privilege, you can also delete subject comments added by your subordinates.
- Users with the associated privileges can also enter comments for alerts and risk assessments.

To open the Subject Comments window

To Open	Do This
Account Comments window	From the Account Details window, click **Comments** in the **Account Attachments** section.
Customer Comments window	From the Customer Details window, click **Comments** in the **Customer Attachments** section.
Household Comments window	From the Household Details window, click **Comments** in the **Household Attachments** section.

To view an existing subject comment

1. Open the subject comments window as described in the table above.
2. Existing comments are displayed in the order they were entered.

To add a comment to a subject

1. Open the subject comments window as described in the table above.
2. Enter your comment in the **Add New Comment** field.
3. Click **Save Comment**.

To delete a subject comment

If you have the Delete Subject Comments privilege, you can delete subject comments that you added. If you are a manager and you have Delete Subject Comments privilege, you can also delete subject comments added by your subordinates.

1. Open the subject comments window as described in the table above.
2. Click the Delete Comment icon .

Other Actions

Account, customer, and household documents

Subject documents are documents attached to accounts, customers, and households. Although transactions can also be subjects of alerts, you cannot attach documents to transactions.

- If you have the Add and View Subject Documents privilege, you can view and adddocuments for accounts, customers, and households that appear on any of the alert list or risk assessment list windows that you have access to.
- If you have the Delete Subject Documents privilege, you can delete documents that you added to accounts, customers, and households. If you are a manager and you have the Delete Subject Documents privilege, you can also delete subject documents added by your subordinates.
- Your client and browser settings determine which document types can be displayed and whether the **File** download dialog appears.
- Users with the associated privileges can also enter documents for alerts and risk assessments.

To open the Subject Documents window

Once a document is added, you cannot edit it, but you can add as many additional documents as you need to.

To Open	Do This
Account Documents window	From the Account Details window, click **Documents** in the **Account Attachments** section.
Customer Documents window	From the Customer Details window, click **Documents** in the **Customer Attachments** section.
Household Documents window	From the Household Details window, click **Documents** in the **Household Attachments** section.

To view an existing subject document

1. Open the Subject Documents window as described above. If there are attached documents, they are displayed in the order they were added.
2. Click on the document name.

To add a subject document

1. Open the Subject Documents window as described above.
2. Click **Browse** to select the document from your local directory structure.
3. Optionally, enter a description of the document in the **Description** field. The description is displayed along with the document name in the **Document Name** column.
4. Click **Attach Document**.

To delete a subject document

The Delete Document icon is displayed for documents that you can delete. If you have the Delete Subject Documents privilege, you can delete documents that you added. If you are a manager and you have the Delete Subject Documents privilege, you can also delete documents added by your subordinates.

1. Open the Subject Documents window as described above.
2. Click the Delete Document icon.

Other Actions

Export data to CSV

Users with the Export to CSV privilege can export data from the following windows to a comma-separated value file that can be opened in spreadsheet software such as Microsoft Excel.

- Alert Details
- Alert List
- Customer Transactions
- Query Results
- Risk Assessment List

Users with the User and Group Administration privilege (but not the Export to CSV privilege) can export the data from the Privileges Assigned to Users window, which is on the System Administration tab.

System Administrators at your site configure a system-wide setting that specifies the format for all CSV files exported from SAS Anti-Money Laundering. The default format is a standard RFC 4180 Comma-Separated Values file. The other option is a CSV file that has a 'value' format applied to long numeric strings, such as account numbers, to prevent spreadsheet applications from converting them to scientific notation with the resulting loss of precision.

System administrators can also specify which delimiter to use (default is comma) and the maximum number of rows to export (default is 1,000). Contact your System Administrators to find out how SAS Anti-Money Laundering has been configured for your site.

To export data to CSV

1. Navigate to the window that displays the data that you would like to export. If you are not sure how to do this, please refer to the help topics on the left side of this window.
2. Click either the Export icon or the **Export to CSV** link, depending on which window you are working with.

Queries

Performing Queries

Alert, Account, Customer, External Party, Household, Transaction, and Risk Assessment Queries

On each query window, the fields represent query criteria. Query criteria help you restrict your query so that you get only the information that you want. The more criteria you can enter, the better your results will be. Leave a field blank if you want to see all associated records or if the field is not relevant to the query.

When you are entering query criteria, keep the following points in mind:

- An Alert Query on a given subject will only return alerts related directly to that subject. So, when querying alerts where subject=account, only account alerts will be returned. All customer and household alerts will be ignored. The same is true when querying where subject=customer (ignores account and household alerts) or subject=household (ignores customer and account alerts).

  💡 See Examples of Alert Queries by Subject Name.
- Fields that have a **Contains** checkbox can be used in two different ways:
  - If you do not check the **Contains** checkbox, the query will look for records that *exactly match* the characters that you enter.

  - If you check the **Contains** checkbox, the query will look for records that *contain* the sequence of characters that you enter. In other words, when entering an account number in a "contains" field, you can enter a full or partial number.

    Caution: Depending on the amount and type of data at your site, a **Contains** query may be so resource-intensive that the system could slow down or even stop operating.

- Enter numerals without commas or symbols (such as $). Exclude leading and trailing spaces.

- Avoid unrestricted queries.

- When you have an option for **Scope**, select **Query only current account information** if you only want to see the latest information. Select **Query Account History** if you want to see all the information ever stored on that account.

- You cannot cancel a query once you start it. Even if you close SAS Anti-Money Laundering, the query will run until it finishes.
- The Customer Query has two options for entering a name. You can use the **Name** field, or the **First**, **Middle**, and/or **Last** fields. Some pointers for working with these fields:

- The **Name** field is populated for individuals and organizations.
- The **First**, **Middle**, and **Last** fields are only populated for individuals. Therfore, if you use these fields your results will not include organizations.
- For individuals, the **Name** field is a concatenation of the **First**, **Middle**, and **Last** fields.
- The **First**, **Middle**, and **Last** fields are treated as "exact match" fields.

What are the differences and similarities between the Customer Names Query and the Customer Query?

Customer Names Query	Customer Query
You can only search by customer name.	There are several ways to restrict the query.
Query results are a list of accounts that the customer has a role on.	Query results are a list of customers that match the criteria you entered.
Returns individuals and organizations.	Returns individuals and organizations.
Returns all all the information ever stored on that account.	You can specify whether to see only current customer information or all information ever stored on that customer.

Performing Queries

Examples of Alert Queries by Subject Name

- Alert Query on Customer - using the customer name will return customer-level alerts only for customers where the customer name matches the name search criteria.
- Alert Query on Account - using the account name will return account-level alerts only for accounts where the account name matches the name search criteria.
- Alert Query on Household - using the household name will return household-level alerts only for households where the head of household name (in the household table) matches the name search criteria.

Attempting to find all account-level alerts for a specific customer's name using the Alert Query on Account will not be successful for the reason illustrated in the following example:

Suppose John Smith, the customer, has two accounts with names "College Savings" and "Retirement Fund." Looking for the string "John Smith" in the account name field won't return any results. (This will only work if the account names happen to include John Smith's name, as in "John Smith's College Savings.")

To be certain of finding all of John Smith's account alerts, search for John Smith using the Name field of Customer Query. Then, from the query results select the number of the appropriate customer and use the All Alerts section of the Customer Detail screen to navigate to all of the customer's alerts.

Detail Windows

How to use the Account Query to access an account summary

💡 Before you begin, if possible, copy the account number so you don't have to type it in step 2.

To access an account summary

1. On the Query tab, select **Account**.
2. In the **Number** field, paste or type the account number.
3. Click **Show Matching**.
4. On the Account Results window, select the ✥ icon.
5. On the Account Details window, select **More.**
6. Under **Related Information** select the value for **Profiles List**.

Users with "Issue Advanced Queries" permission can also access this window by defining an Advanced Query on the Account table.

Performing Queries

Alert, Account, Customer, External Party, Household, Transaction, Risk Assessment, and Advanced Query Results

Because administrators at your site control the exact contents of this window, this online help describes how to interact with this window in general terms.

- The window title reflects the table you queried.
- Click **Fewer** or **More** to see fewer or more columns in each row.
- If you have the Export to CSV privilege, click **Export to CSV** to export the query results to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.
- The query criteria selected to build the query are displayed below the window title. The window uses symbols for comparison operators.

Symbol	Meaning
=	Equals
!	Not equals
?	Contains
:	Not contains
<</td>	Less than
>	Greater than
(	Less than or equal
)	Greater than or equal
%	Like

- You can specify *temporary* and *persistent* numbers of rows to display on query results windows. Entering a very large value will make the page take longer to display and may cause your browser to time out.
- You can sort query results by any column. The down-pointing triangle in a column heading indicates that alerts are sorted by that column, in descending order (from highest to lowest). To reverse the order, click on the column heading, and the alerts will be re-sorted in ascending order.
- Use icons on the window to access or remove additional information. Not all versions of this window display all the icons described below.

Icon	Function
✥	• Drill to get more information related to a **row** if the icon occupies its own cell in an untitled column on the far left side of the table. • Drill to get more information related to a **cell** if the icon appears within a titled column.
⤓	Expand the cell in place, displaying more information about the cell contents.
⤒	Collapse the cell. In other words, reverse the expansion.

Performing Queries

Watch List Query

About watch lists

A watch list is a database of individuals and organizations that have been identified as being at risk for money laundering or terrorist financing activity. Your financial institution may choose to obtain watch lists from vendors such as World-Check, or it may create its own watch lists.

SAS Anti-Money Laundering provides scenarios that, when activated for your site, generate alerts when a name in your customer database matches a name on a watch list.

You can use the Watch List Query to explore the watch lists in place at your site.

If your site has not populated the watch list tables, the Watch List Query will not run.

Performing a watch list query

When you are entering query criteria, keep the following points in mind:

- On each query window, the fields represent query criteria. Query criteria help you restrict your query so that you get only the information that you want. The more criteria you can enter, the better your results will be. Leave a field blank if you want to see all associated records or if the field is not relevant to the query.
- All of the data entry fields on the Watch List Query window accept a full or partial value. For example, entering "ste" in the **Last Name** field will return all last names that contain "ste."
- Avoid unrestricted queries.
- You cannot cancel a query once you start it. Even if you close SAS Anti-Money Laundering, the query will run until it finishes.

Performing Queries

Watch List Query Results

Because administrators at your site control the exact contents of this window, this online help describes how to interact with this window in general terms.

- The window title reflects that you performed a Watch List Query.
- Click **Fewer** or **More** to see fewer or more columns in each row.
- If you have the Export to CSV privilege, click **Export to CSV** to export the query results to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.
- The query criteria selected to build the query are displayed below the window title. The question mark indicates that a "contains" operator was used.
- To specify the number of rows you would like to see, enter a value in the **Rows per page** box and press ENTER. A large value may make the page take longer to display and could cause your browser to time out.
- Click the ✥ icon to get more information related to a row.

Performing Queries

Customer Names Query

The Customer Names Query is provided in response to legislation requiring financial institutions to perform periodic customer name searches. In the United States, the USA PATRIOT Act specifies this requirement in section 314(a). Other countries have similar requirements.

The Customer Names Query returns all accounts associated with the names you enter, regardless of whether they are associated with alerts or not, and regardless of the role the customer has on the account (in other words, you will see accounts where the customer is primary owner, secondary owner, beneficiary, etc.).

- If you do not check the **Contains** checkbox, the query will look for records that *exactly match* the characters that you enter.

- If you check the **Contains** checkbox, the query will look for records that contain the sequence of characters that you enter. Use the **Contains** checkbox if you need to search for a partial name.

  Caution: Depending on the amount and type of data at your site, a **Contains** query may be so resource-intensive that the system could slow down or even stop operating.

When entering names:

- Enter one customer name per line.
- When searching for individuals, enter the name in the following order: first, middle, last, suffix (without the commas). For example:

  ```
  John Albert Doe Jr.
  ```

- Do not enter commas.
- Enter other punctuation (such as periods after middle initials) as it appears in your database.

What are the differences and similarities between the Customer Names Query and the Customer Query?

Customer Names Query	**Customer Query**
You can only search by customer name.	There are several ways to restrict the query.
Query results are a list of accounts that the customer has a role on.	Query results are a list of customers that match the criteria you entered.
Returns individuals and organizations.	Returns individuals and organizations.
Returns all all the information ever stored on that account.	You can specify whether to see only current customer information or all information ever stored on that customer.

Performing Queries

Customer Names Query Results

The Customer Names Query returns all accounts associated with the names you enter, regardless of whether they are associated with alerts or not, and regardless of the role the customer has on the account (in other words, you will see accounts where the customer is primary owner, secondary owner, beneficiary, etc.).

The **Name** column displays the names you entered that matched customers in your database. If some of the names you entered were not in your database, they will not be displayed here.

The **Role** column displays the role that the customer has on the account.

Click the value for **Account Number** to open the Account Details window.

The **Average Balance** and **Number of Transactions** are based on the most recent account profile. Account profiles are updated every month.

If the account is inactive, **Closing Date** displays the date on which it became inactive. If the account is active, the value for **Closing Date** will be Jan 1, 5999.

Performing Queries

Advanced Query

Use the Advanced Query window to issue queries against the SAS Anti-Money Laundering database.

To define an advanced query

1. Select a table to query. Initially, the drop-down menu lists the most commonly used tables. Click **More Selections** to add more tables (these are not commonly used tables). Click **More Selections** again to see all the available tables. At this point you may find tables with missing or irrelevant data. Click **Fewer Selections** once to return to the less commonly used tables, or twice to return to the initial list.
2. If you want to specify multiple criteria in step 4:
    1. Select **Match** all of the following to display all records that match the values you specify.
    2. Select **Match** any of the following to display records that match some or any of the values you specify.

       If you are only specifying one criterion, the **Match** any/all of the following selection will not affect the query.
3. For each parameter, select (or enter) a **Column**, an **Operator**, and a **Value**. Some pointers on working with the **Value** field:

    1. The **Contains** operator matches the specified characters in any position in the string. In other words, when entering an account number in a "contains" field, you can enter a full or partial number.

       Caution: Depending on the amount and type of data at your site, a **Contains** query may be so resource-intensive that the system could slow down or even stop operating.

    3. For date comparisons, enter a date or click the calendar icon to select a date.

    5. Strings that can have only a limited list of values (for example, Yes/No indicators) appear as drop-down menus displaying valid values.

    7. To compare a field to a missing (or NULL) value, use either "Equal" or "Not Equal" as the comparison operator and delete all characters from the value side of the comparison expression (in this context, blanks are not the same as no characters).

4. Use the **More Parameters** link to add up to eight rows for entering criteria.
5. Click **Show Matching** to issue the query.

Regulatory Reporting

Regulatory Reporting

Create a regulatory report

SAS Anti-Money Laundering compliments your organization's regulatory report filing procedures by facilitating the preparation of regulatory report forms. It is assumed that users with regulatory reporting privileges have knowledge of and experience with their government's reporting requirements.

You cannot create a regulatory report for a household alert or a transaction alert. You can, however, create a manual alert for an account or customer from the household or transaction, and then create a regulatory report for that alert.

To create a regulatory report

1. Open the Alert Regulatory Report window by either:
    1. Clicking the **Regulatory Report** icon on My Alerts.

    3. Clicking the **Regulatory Report** button on the Alert Details window.

2. Review the Alert Regulatory Report window to make sure you don't duplicate an existing report. To proceed, click **Create New Report.**
3. On the Create New Regulatory Report: Select Report Type window, use the drop-down menu to select the type of report you want to file, and select a radio button for either **Money Laundering** or **Terror Financing**. This helps the solution pre-populate the regulatory report form. Once you have made your selections, click **Next**.

   For some countries, the next window will be the regulatory report. Other countries should proceed to the next step.
4. On the Create New Regulatory Report: Select Institution/Branch window, use the drop-down menus to select the institution and branch where the suspicious activity took place. Once you have selected the options, click **Create**. This will create a regulatory report.
5. Fill in the form, referring to online Help for that window if you have questions about working with the fields, adding or editing additional names, or the difference between **Batch File** and **Hardcopy File**.

   U.S. customers can find complete instructions about the U.S. report forms at www.fincen.gov.

Regulatory Reporting

Edit or delete a regulatory report

Users with regulatory reporting privileges can open and edit or delete a regulatory report that is in progress, as long as the associated alert appears in My Alerts and the report's status is **open**.

Not all regulatory report types can be edited and deleted. If an action is not available, the icon will not be displayed.

To edit or delete a regulatory report

1. Open the Alert Regulatory Report window by either:
    1. Clicking the **Regulatory Report** icon on My Alerts.

    3. Clicking the **Regulatory Report** button on the Alert Details window.

2. Click the icon that corresponds to the action you want to take:
    1. Click the **Edit** icon to open and edit the report.
    2. Click the **Delete** icon to delete the report.

When a user determines that the report is complete and selects either the batch file or print file option, the report is no longer open and it cannot be edited or deleted. You can, however, open a copy of that report to use as a correction of the previous report.

Regulatory Reporting

Correct a regulatory report

When a user with regulatory reporting privileges determines that a report is complete and selects either the batch file or print file option, the report is no longer open and it cannot be edited or deleted. You can, however, open a copy of that report to use as a correction of the previous report.

Not all regulatory report types allow for corrections. If the correct option is not available, the wrench icon 🔧 will not be displayed.

If the report is still open, you can simply open and edit it.

To correct a regulatory report

1. Open the Alert Regulatory Report window by either:
    1. Clicking the **Regulatory Report** icon ❗ on My Alerts.

    3. Clicking the **Regulatory Report** button on the Alert Details window.

2. Click the wrench icon 🔧 for the report you want to correct. This will open a new report based on the report that you want to correct. On the Alert Regulatory Report window, this new report will have its own Report ID, and the Report ID of the report you are correcting will be displayed in the Related Report ID column.

The Reports Tab

The Reports Tab

Introduction

Administrators at your site determine what information appears on the Reports tab. Any file that can be accessed from your browser - including Internet and intranet pages, SAS report output in HTML format, internal reports, Microsoft Word documents, and Microsoft Excel spreadsheets - can be included here.

The Reports Tab

Viewing and printing reports

To view a report

1. On the left side of the Reports tab, open the folders to find the name of the report that you are interested in.
2. Click either:
    1. The report name (the report will either display on the right side of the Reports tab, or open in a new window).
    2. The report icon (the report will open in a new window).

To print a report

1. Right-click within the report you wish to print.
2. From the pop-up menu, select **Print**.

- To print only a chart, right-click on the chart and select the **Print Picture** option from the pop-up menu.
- To print a target without opening it, right-click on the link, such as a bar in a chart, and select the **Print Target** option from the pop-up menu.

The Reports Tab

Understanding the SAS-supplied batch reports

This online Help describes the report samples that were shipped with SAS Anti-Money Laundering. The report samples are based on dummy data - they do not reflect how the system is operating at your site. Your implementation team may activate these reports by running them against your data, and they may change them and add new reports.

Some reports present information that can change frequently. Your system administrator determines how often the reports are refreshed with new data.

Investigation reports

- Active Alert Ownership and Activity
- Age of Active Alerts
- Duration of All Alerts
- Near Neighbors of Saved Targets
- Alert Status by Scenario Category
- Total Alerts by Month
- Total Alerts by Week

Scenario Administration Reports

- Active Headers
- Scenarios and Risk Factors
- Scenario Audit
- Weights and Execution Probabilities

Risk Classifier and List Reports

- Risk Classifiers by Category
- Lists by Category

System Administration Reports

- Batch Execution Statistics
- Users By Group
- Lookup Table Values

The Reports Tab

Active Alert Ownership and Activity

This report shows statistics on active alert ownership and activity by user.

- The Alerts Owned column shows how many active alerts are owned by each user. Because a user can check out an alert without owning it, when interpreting this column, it is important to understand the characteristics of owned and checked out alerts.
- The Alerts Created column shows the number of active alerts manually created by each user. The NO OWNER cell displays the number of active alerts created by the alert generation process.
- The Alerts Last to Update column shows the number of active alerts that each user was the last user to update. The NO OWNER cell displays the number of active alerts that were created by the alert generation process, and not yet updated by a user.

Click on a value in the Owner column to see details on all the active alerts that a user owns.

The Reports Tab

Age of Active Alerts

This report shows how old all the active alerts are. An administrator at your site determines how many time periods to show, and the system divides the number of days since the oldest active alert was created by the number of time periods.

An administrator also determines whether this report is presented as a bar chart, a table, or both.

- To see the number of alerts associated with a bar, hover the mouse over that bar.
- To see a detailed list of alerts associated with a time period, click on the bar in the bar chart, or on the value for Age in Days on the table.

The Reports Tab

Duration of All Alerts

This report shows:

- How many days all active alerts have been active.
- How many days all closed alerts were active.
- How many days all suppressed alerts were active.

In the Days Active row, the Average section shows the average number of days that all active alerts have been open. The Maximum section shows how many days the oldest active alert has been open.

In the Days to Close row, the Average section shows the average number of days that all closed alerts were active. In other words, this is the average time it has taken to close an alert. The Maximum section shows the maximum number of days that a closed alert was active.

In the Days to Suppress row, the Average section shows the average number of days that all suppressed alerts were active. In other words, this is the average time it has taken to suppress an alert. The Maximum section shows the maximum number of days that a suppressed alert was active.

To see a detailed list of alerts associated with a status, click on Average or Maximum for that status. Administrators at your site may restrict the number of alerts displayed to avoid exceeding the capabilities of your browser.

The Reports Tab

Near Neighbors of Saved Targets

This report displays accounts that have similar behavior to one or more target accounts. The target accounts are identified and saved for this report by administrators at your site. (Instructions for how to do this are in the **System Administrator's Guide**.) You will see a different table for each target account.

- The near neighbor accounts are displayed in rank order, as indicated in the Rank column, with the most similar account listed first.
- The Target column reflects which of the targets this account is similar to.
- The Distance column describes how similar this account is to the target. If the distance is 0, the account is exactly the same as the target. The larger the number, the less similar the account is to the target.
- The Neighbor Account Number column displays the account numbers of the similar accounts.

The Reports Tab

Alert Status by Scenario Category

This report shows the number of active, closed, and suppressed alerts by scenario category.

- Alerts suppressed in the Investigation user interface are displayed under the heading **Suppressed (UI)**.
- Alerts suppressed in the alert generation process are displayed under the heading **Suppressed (Batch)**.

If you do not see a column for active, closed, or suppressed under Alert Status, that means there are no alerts with that status.

- A large proportion of active alerts for a scenario may indicate that Investigation Users are having trouble processing those alerts.
- If the number of alerts for a scenario is higher or lower than expected, the parameters that trigger the alerts may need adjustments.

Click a status (such as **Active**) to see a pie chart showing distributions of alerts with that status by scenario category.

The Reports Tab

Total Alerts by Month

This report shows the number of alerts created each month over a time period specified by your administrator. A change in the number of alerts created per month may be due to seasonality, new products, new procedures, or a change in scenario processing, such as a different trigger limit, a new scenario, or activation/deactivation of an existing scenario.

An administrator at your site determines whether this report is presented as a bar chart, a table, or both.

To see the number of alerts associated with a bar, hover the mouse over that bar.

The Reports Tab

Total Alerts by Week

This report shows the number of alerts created each week during a time period specified by your administrator. A change in the number of alerts created per week may be due to seasonality, new products, new procedures, or a change in scenario processing, such as a different trigger limit, a new scenario, or activation/deactivation of an existing scenario.

An administrator at your site determines whether this report is presented as a bar chart, a table, or both.

To see the number of alerts associated with a bar, hover the mouse over that bar.

The Reports Tab

Active Headers

Scenario administration reports are intended for Administrators and members of IT staff. For information on administering headers, scenarios, and risk factors, refer to the online help for the Scenario Administrator user interface. For information on the alert generation process, refer to the **System Administrator's Guide.**

This report describes all the active headers, and the value for Number of Header Elements links to a description of the elements in each header. The following table defines the terms used on this report.

Term	**Description**
Header Name	The header name is displayed on the Scenario Administrator's Header Main window, and the scenario code generation module uses this as the file name for the header code that it generates.
Short Description	The header description is displayed on the Scenario Administrator's Header Main window.
Number of Header Elements	Click on the number to view a description of the elements in the header.
Subject	The term used in the Investigation UI to describe the entity that exhibited the behavior that caused the alert. The possible values are Account, Customer, Household, and Transaction. In the back end, the term "entity" is used instead of subject.
Prep Data Set	A prep data set contains the subset of the data in the Core Data Model required to execute the scenarios and risk factors registered to it.
Alert Table Name	This is the name of the alert table that this header generates.
Header Autogen Indicator	If **Y**, then the scenario code generation module creates the SAS program code required to execute the scenarios during the alert generation process.
Header Type	Three types of headers are supported: • DATA Step (Auto-Generated) • DATA Step (Non Auto-Generated) • Custom
Created By	The user name of the person who registered the header.
Date	The date on which the header was registered.
Last Updated By	The user name of the person who last updated the header.
Last	

Updated	The date on which the header was last updated.
Header Host Description	Host where the header is executed. "Localhost" is the host where the Scenario Administrator is deployed.
Header Source Location	Location of the header source code.

The Reports Tab

Scenarios and Risk Factors

Scenario administration reports are intended for Administrators and members of IT staff. For information on administering headers, scenarios, and risk factors, refer to the online help for the Scenario Administrator user interface. For information on the alert generation process, refer to the **System Administrator's Guide.**

This report shows the properties for all scenarios and risk factors. Active scenarios and risk factors are at the top, and inactive ones are at the bottom.

Administrators can use the Scenario Administrator user interface to activate and de-activate scenarios and risk factors, as well as to edit properties and adjust parameter values.

The following table defines the terms used on this report.

Term	Description
Name	Production scenarios and risk factors are named using the convention SAS100XX. Custom scenarios and risk factors can be named at the discretion of the implementation team. A character prefix followed by a numeric identification number is recommended. Once assigned, this value cannot be changed.
Status	The status can be either **Active** or **Inactive**. Active scenarios are scheduled for execution in the alert generation process; inactive scenarios are not.
Number of Parameters	This shows the number of parameters in the scenario or risk factor code. Click on either the text or the number to view a list of the parameters and their settings.
Category	The type of behavior that the scenario or risk factor checks for.
Short Description	The short description is used as the label in the **Available Scenarios** box on the Scenario Administrator's Scenario Main window.
Long Description	The long description is displayed on the Scenario Administrator's Scenario Main window as well as in the Investigation UI.
Code Location	The path to the scenario or risk factor code.
Header Name	The name of the header that this scenario or risk factor uses.
Frequency	The frequency at which this scenario or risk factor will be executed. Valid values are **Daily**, **Weekly**, and **Monthly**.
Initial Route ID	ID of the user or group that alerts from this scenario or risk factor are initially routed to. Investigation Users can subsequently route alerts within the Investigation user interface.
Route Type Code	This value indicates whether alerts from this scenario or risk factor are initially routed to a user or to a group.
Suppression (Days)	The default suppression duration for this scenario. Each alert generated from this scenario will be suppressed for the number of calendar (not business) days entered.

	Because suppression applies to alerts, and risk factors do not generate alerts, suppression duration does not affect risk factors.
Scenario Duration (Days)	The number of business days of transactions that will be replicated to the Knowledge Center. By default this is set to the same value as the num_days parameter.
Money Laundering and Terrorist Financing Bayes Weight	The relative number of known money launderers that would engage in the behavior described by the scenario or risk factor. If they all do it, the value should be **10**. If it is a rare money laundering scheme, the value should be **1**. To remove a scenario or risk factor from the scoring process, assign a value of **0**. Valid values are 0 <= Bayes Weight <= 10. The default setting for scenarios and risk factors is **5**. See the **Scenario Administration Guide** for details on Bayes Weight.
Execution Probability	The probability that a scenario or risk factor will be matched with respect to the other scenarios and risk factors. Valid values are 0 < Execution Probability < 1. The default setting is **.0050000**. See the **Scenario Administration Guide** for details on Bayes Execution Probability.
Risk Factor	**Y** indicates that this is a risk factor. Risk factors are used in the risk ranking process and do not generate alerts. **N** indicates that this is a scenario.
Effective Date	Date on which the scenario or risk factor was activated.
Owner	The user name of the person who registered or edited the scenario.
Version Number	The Scenario Administrator increments the version when the scenario or risk factor is modified.

The Reports Tab

Scenario Audit

Scenario administration reports are intended for Administrators and members of IT staff. For information on administering headers, scenarios, and risk factors, refer to the online help for the Scenario Administrator user interface. For information on the alert generation process, refer to the **System Administrator's Guide.**

This report shows the history of changes made to all active scenarios and risk factors.

The following table defines the terms used on this report.

Term	Description
Version	If your site used the Scenario Administrator to activate scenarios and risk factors, then the activation process incremented the version number, and this report will begin with version 2. If your site activated scenarios and risk factors in batch, then the activation process did not increment the version number, and this report will begin with version 1.
Last Updated	Date and time of the most recent update.
Last Updated By	User name of the person who performed the last update.
Name	Name of the property or parameter that was updated.
Original Value	The value that was in place before the update.
Updated Value	The value that was in place after the update.
Type	Possible values are change, deletion, and addition.
Attribute	Possible values are value, description, and format.

The Reports Tab

Weights and Execution Probabilities

Scenario administration reports are intended for Administrators and members of IT staff. For information on administering headers, scenarios, and risk factors, refer to the online help for the Scenario Administrator user interface. For information on the alert generation process, refer to the **System Administrator's Guide.**

This report shows the Money Laundering Bayes Weight, Terrorist Financing Bayes Weight, and Execution Probability for each active scenario and risk factor.

Bayes Weight is the relative number of known money launderers that would engage in the behavior described by the scenario or risk factor. If they all do it, the value should be **10**. If it is a rare money laundering scheme, the value should be **1**. To remove a scenario or risk factor from the scoring process, assign a value of **0**. Valid values are 0 <= Bayes Weight <= 10. The default setting for scenarios and risk factors is **5**.

Execution Probability is the probability that a scenario or risk factor will be matched with respect to the other scenarios and risk factors. Valid values are 0 < Execution Probability < 1. The default setting is **.0050000**.

See the **Scenario Administration Guide** for details on Bayes Weight and Execution Probability.

Working With Reports

Risk Classifiers by Category

This report shows all risk classifiers by risk classifier category.

Values in the Type Code column
RC1 = Account or customer numbers
RC2 = Account or customer - other
RC3 = Customer monthly profile
RC4 = Account or customer indicators
RC5 = Custom

Values in the Source Table column
PTY = FSC_PARTY_DIM
ACC = FSC_ACCOUNT_DIM
PPF = FSC_PARTY_PROFILE_FACT

Values in the Operator column
GT = Greater than
LT = Less than
EQ = Equals

The User ID column shows the ID of the user who created the risk classifier.

The Reports Tab

Lists by Category

This report shows all lists by category. It does not show list values.

The Subject column is the validation type. If the subject is Account, then all values must be valid account numbers. If the subject is Customer, then all values must be valid party numbers. If the subject is None, then values are strings that are not validated.

The User ID column shows the ID of the user who created the list.

The Reports Tab

Batch Execution Statistics

The system report is intended for Administrators and members of IT staff. For information on administering headers, scenarios, and risk factors, refer to the online help for the Scenario Administrator user interface. For information on the alert generation process, refer to the **System Administrator's Guide.**

The Batch Execution Statistics report summarizes performance statistics for most modules over the life of the system. These summary statistics may be used during the initial investigation into performance bottlenecks.

For a complete listing of all gathered statistics, refer to the JOB_STATISTICS table.

This report does not eliminate the need to use system tools to monitor OS-level performance. As volumes increase, so will the values of these statistics.

Additional performance statistics are available to the SAS System. For information on these options, please refer to the documentation for the SAS System or contact SAS Technical Support.

The Reports Tab

Users By Group

The Users By Group report lists all the groups in alphabetical order, and lists the members of the groups in alphabetical order.

Each user must be a member of at least one group. Some of the alerts and risk assessments that users see depends on which groups the users belong to.

The Reports Tab

Lookup Table Values

The Lookup Table Values report displays the FSK_LOV table, which is also referred to as the "list of values" table.

This is a generic lookup table that is used mostly for labels and menu options in the user interface. For example, the FSK_LOV table contains the reasons a user could select when closing alerts and risk assessments.

The Investigation UI code expects certain FSK_LOV values to be present. Although adding custom entries may be necessary, updating or removing entries should be undertaken with caution.

Administering Users and Groups

Administering Users and Groups

Introduction to administering users and groups

The user administration features are available only to users with user administration privileges. Administrators use the User Administration and Group Administration windows to create, modify, duplicate, and delete user and group profiles.

- When SAS Anti-Money Laundering is installed, the System Administrator uses the "sasamladmin" user profile to log on and create user and group profiles. To ensure that there is always a valid user profile, this profile cannot be deleted.
- The "sasamladmin" profile is a member of the "Default Group" and cannot be a member of any other group.
- The "sasamladmin" profile should only be used for creating other users and groups.
- The "Default Group" is a template that facilitates adding new groups to the system. The "Default Group" can be modified and duplicated, but it cannot be deleted.
- Administrators at your site control how alerts are initially routed to users and groups. Therefore the groups that a user is a member of determine which alerts that user can see.

Administering Users and Groups

Administering users

Users with the User and Group Administration privilege use the User Administration window to create, modify, duplicate, and delete user profiles.

When specifying which groups a user is a member of and assigning privileges, remember:

- Some of the alerts and risk assessments that users see depends on which groups the users belong to.
- Each user must be a member of at least one group.
- A description of the user privileges is provided for your reference.

To make User A the manager of User B, modify User B's profile. In the **Manager** drop-down menu, select User A.

When SAS Anti-Money Laundering is installed, the System Administrator uses the "AML Administrator (sasamladmin)" user profile to log on and create user profiles. To ensure that there is always a valid user profile, this profile cannot be deleted. The "sasamladmin" profile is a member of the "Default Group."

Rules associated with administering users

- The "AML Administrator (sasamladmin)" user profile cannot be deleted.

- A user cannot be deleted if he or she:
  - Owns or has checked out one or more alerts or risk assessments
  - Is a manager
  - Is designated as "initial route" on a scenario or risk assessment routing rule
  - Is the last user in a group that is designated as "initial route" on a scenario or risk assessment routing rule
  - Is the last user in a group that has one or more alerts or risk assessments

- When a user is removed from a group, all the alerts and risk assessments that the user had checked out from that group will be automatically checked back in.

To create a user profile

1. Select **Create**.
2. Enter information in the user profile fields as appropriate. Be sure to select at least one group for this user to be a member of.
3. Click **Validate** to make sure the values you entered are acceptable. If any values are not acceptable, descriptions of the problems will appear at the top of the page. Examples of unacceptable values are users that do not belong to at least one group, duplicate user IDs, and missing values.
4. Once the **Validate** button returns no errors, click **Save**.

To modify an existing user profile

1. Select **Modify**.
2. From the **User** drop-down menu, select the profile that you would like to modify.
3. Edit the user profile fields as appropriate.
4. Click **Validate** to make sure the values you entered are acceptable. If any values are not acceptable, descriptions of the problems will appear at the top of the page. Examples of unacceptable values are users that do not belong to at least one group, duplicate user IDs, and missing values.
5. Once the **Validate** button returns no errors, click **Save**. The changes will take effect the next time the user logs on.

To duplicate an existing user profile

1. Select **Duplicate**.
2. From the **User** drop-down menu, select the profile that you would like to duplicate.
3. Edit the user profile fields as appropriate.
4. Click **Validate** to make sure the values you entered are acceptable. If any values are not acceptable, descriptions of the problems will appear at the top of the page. Examples of unacceptable values are users that do not belong to at least one group, duplicate user IDs, and missing values.
5. Once the **Validate** button returns no errors, click **Save**.

To delete a user profile

1. Select **Delete**.
2. From the **User** drop-down menu, select the profile that you would like to remove.
3. Click **Validate** to make sure the user profile can be deleted. Rules associated with administering users are at the top of this page.
4. Click **Delete**.

Administering Users and Groups

User Privileges

The following tables describe the user privileges in SAS Anti-Money Laundering. Privileges are listed alphabetically under the following categories: Administration, Alert Actions, Analysis Actions, Regulatory Reporting, Risk Assessment Actions, Special Tab Access, and Subject (Account, Customer, and Household) Actions.

Administration (System and Compliance Administration)

Privilege	**Description**
Manage Lists	A user with this privilege can access the Compliance Administration tab and configure lists.
Manage Risk Assessment Routing Rules	A user with this privilege can access the Compliance Administration tab and configure risk assessment routing rules.
Manage Risk Classifiers	A user with this privilege can access the Compliance Administration tab and configure risk classifiers.
Report Administration	A user with this privilege can access the Report Administration window and configure the contents of the Reports tab.
User and Group Administration	A user with this privilege can access the User Administration and Group Administration windows and create, modify, duplicate, and delete users and groups. A user with this privilege can also access the Privileges Assigned to Users window.

Alert Actions

Privilege	**Description**
Activate Closed Alerts	A user with this privilege can access the Closed Alerts window and activate the displayed closed alerts.
Activate Suppressed Alerts	A user with this privilege can access the Suppressed Alerts window and activate the displayed suppressed alerts.
Add and View Alert Documents	A user with this privilege can add and view documents for alerts that appear in My Alerts.
Close Alerts	A user with this privilege can close alerts that are in My Alerts.
Create Manual Alerts	A user with this privilege can access the Create Alert window and create an alert.
Delete Alert Comments	A user with this privilege can delete alert comments that he or she added. A manager with this privilege can also delete alert comments added by subordinates.

Delete Alert Documents	A user with this privilege can delete alert documents that he or she added. A manager with this privilege can also delete alert documents added by subordinates.
Route Alerts	A user with this privilege can route alerts that he or she owns or has checked out.
Send Alert E-mail	A user with this privilege can send details about an alert in a system-generated e-mail.
Suppress Alerts	A user with this privilege can suppress alerts that he or she owns or has checked out.
Take Alert Ownership	A user with this privilege can take a checked-out alert away from another user. Managers with this privilege can take owned or checked-out alerts away from their subordinates.

Analysis Actions

Privilege	Description
Export to CSV	A user with this privilege can export data from the following windows to a comma-separated value file that can be opened in spreadsheet software such as Microsoft Excel. • Alert Details • Alert List • Customer Transactions • Query Results • Risk Assessment List
Issue Advanced Queries	A user with this privilege can access the Advanced Query window and issue complex queries.
Modify Funds Tracker Networks	A user with this privilege can modify Funds Tracker network data.

Regulatory Reporting

A user with one of these regulatory reporting privileges and the Access Summary Tab privilege can view the Regulatory Reports window on the Summary tab.

Privilege	Description
Regulatory Reports - Create	A user with this privilege can access the Regulatory Reporting windows and view, create, delete, and correct regulatory reports.
Regulatory Reports - File	A user with this privilege can access the Regulatory Reporting windows and view, create, delete, correct, and file regulatory reports.

Regulatory Reports - View	A user with this privilege can access the Regulatory Reporting windows and view existing regulatory reports.

Risk Assessment Actions

Privilege	**Description**
Add and View Risk Assessment Documents	A user with this privilege can add and view documents for risk assessments that appear in My Risk Assessments.
Close Risk Assessments	A user with this privilege can close risk assessments that are in My Risk Assessments.
Create Manual Risk Assessments	A user with this privilege can access the Create Risk Assessment window and create a risk assessment.
Delete Risk Assessment Comments	A user with this privilege can delete risk assessment comments that he or she added. A manager with this privilege can also delete risk assessment comments added by subordinates.
Delete Risk Assessment Documents	A user with this privilege can delete risk assessment documents that he or she added. A manager with this privilege can also delete risk assessment documents added by subordinates.
Risk Assessment Query	A user with this privilege can access the Risk Assessment Query window and issue risk assessment queries.
Route Risk Assessments	A user with this privilege can route alerts that he or she owns or has checked out.
Send Risk Assessment E-mail	A user with this privilege can send details about a risk assessment in a system-generated e-mail.
Take Risk Assessment Ownership	A user with this privilege can take a checked-out risk assessment away from another user. Managers with this privilege can take owned or checked-out risk assessments away from their subordinates.

Special Tab Access

Privilege	**Description**
Access Custom Tab	If your site has added a customized application that is accessed through the custom tab, a user with this privilege can access that custom tab.
Access Query Tab	A user with this privilege can access the Query tab.

Access Summary Tab	A user with this privilege can access the Summary tab. In order to see the Regulatory Reports window on the Summary tab, a user must have the Access Summary Tab privilege and one of the regulatory reporting privileges.
View Risk Assessments	A user with this privilege can access the Risk Assessments tab.

Subject (Account, Customer, and Household) Actions

Privilege	**Description**
Add and View Subject Documents	A user with this privilege can add documents to accounts, customers and households that appear on any of the windows that he or she has access to.
Delete Subject Comments	A user with this privilege can delete account, customer, and household comments that he or she added. A manager with this privilege can also delete account, customer, and household comments added by subordinates.
Delete Subject Documents	A user with this privilege can delete account, customer, and household documents that he or she added. A manager with this privilege can also delete account, customer, and household documents added by subordinates.

Administering Users and Groups

User Profile Fields

The following table defines the fields available when you are creating or modifying user profiles.

For more information about User Profile fields, see the column descriptions for FSK_USER and FSK_GROUP_USER in the Knowledge Center Data Model.

Field	**Description**
User Name	You must enter a user name when you are creating or duplicating a user. This name cannot be changed once the user is created. The user name can be up to 35 characters, and it must be unique within the population of existing user and group names. The user name is the name the user should enter on the Log On window. If you are using external security, this value is used to match user profile information with the user name authenticated at log-on time through an authentication process (such as Lightweight Directory Access Protocol).
Display Name	This required value is displayed for this user profile in the UI. This identifier must be unique within the population of existing display names.
E-mail	This required value is the e-mail address for the user. It must not be blank but is not validated otherwise. If your site has configured SAS Anti-Money Laundering to automatically cc users when they send e-mail messages from the solution, this is the e-mail address that will be used.
Manager	This drop-down menu can be used to select another user who can manipulate the alerts of this user.
Available Groups	This list displays the groups that this user could belong to, but does not. Each user must belong to at least one group.
Member Of	This list specifies which groups this user belongs to, an association used to determine which alerts and risk assessments are presented to the user.
Available Privileges	This list displays the privileges that this user could have, but does not. The various privileges enable a user to perform various actions.
User Privileges	This list specifies which privileges this user has.

Administering Users and Groups

Administering groups

Users with the User and Group Administration privilege use the Group Administration window to create, modify, duplicate, and delete group profiles.

When specifying which users belong to groups and assigning privileges, remember that some of the alerts and risk assessments that users see depends on which groups the users belong to.

Rules associated with administering groups

- The Default Group cannot be deleted.
- When a user is removed from a group, all the alerts and risk assessments that the user had checked out from that group will be automatically checked back in.
- A group with one or more alerts or risk assessments cannot be deleted.
- A group with one or more users cannot be deleted.
- A group that is designated as "initial route" on a scenario or risk assessment routing rule cannot be deleted.
- A group that is designated as "initial route" on a scenario or risk assessment routing rule must have at least one member.
- The last user in a group that has one or more alerts or risk assessments cannot be removed from the group.

To create a group profile

1. Select **Create**.
2. Edit the group profile fields as appropriate.
3. Click **Validate** to make sure the values you entered are acceptable. If any values are not acceptable, you will get an error message. Examples of unacceptable values are duplicate group names and too many characters for a field.
4. Click **Save**.

To modify an existing group profile

1. Select **Modify**.
2. From the **Group** drop-down menu, select the profile that you would like to edit.
3. Edit the group profile fields as appropriate.
4. Click **Validate** to make sure the values you entered are acceptable. If any values are not acceptable, you will get an error message. Examples of unacceptable values are duplicate group names and too many characters for a field.
5. Click **Save**.

To duplicate an existing group profile

1. Select **Duplicate**.
2. From the **Group** drop-down menu, select the profile that you would like to duplicate.
3. Edit the group profile fields as appropriate.
4. Click **Validate** to make sure the values you entered are acceptable. If any values are not acceptable, you will get an error message. Examples of unacceptable values are duplicate group names and too many characters for a field.
5. Click **Save**.

To delete a group profile

1. Select **Delete**.
2. From the **Group** drop-down menu, select the profile that you would like to remove.
3. Click **Validate** to make sure the group profile can be deleted. Rules associated with administering groups are at the top of this page.
4. Click **Delete**.

Administering Users and Groups

Group Profile Fields

The following table defines the fields available when you are creating or modifying group profiles.

For more information about Group Profile fields, see the column descriptions for FSK_GROUP in the Knowledge Center Data Model.

Field	**Description**
Group	This field appears only when you are modifying, duplicating, or deleting a group. It displays the group description followed by the group name in parentheses to facilitate selecting a group.
Group Name	You must enter a group name when you are creating or duplicating a group. This name cannot be changed once the group is created. The group name can be up to 35 characters, and it must be unique within the population of existing user and group names.
Group Description	You must enter a group description when you are creating or duplicating a group. This description can be changed after the group is created. The group description can be up to 35 characters, and it must be unique within the population of existing group descriptions.
Available Users	Users who are not members of this group.
Members	Users who are members of this group.

Administering Users and Groups

Privileges assigned to users

The Privileges Assigned to Users window displays a table with all SAS Anti-Money Laundering users on the vertical axis and all privileges on the horizontal axis. Check marks where user names intersect with privileges indicate which privileges have been assigned to users.

Users with the User and Group Administration privilege can access this window.

Click **Export to CSV** export the data to a CSV file that can be opened in spreadsheet software such as Microsoft Excel.

A description of the user privileges is provided for your reference.

Administering Reports

Administering Reports

Adding a link to a file

The report administration features are available only to users with report administration privileges.

In this example, you will add a link to the report tree display. The link will be to the SAS Canada home page, and it will appear in the **SAS Links** folder.

1. From the Administration tab, select **Report Administration**.
2. Select **Duplicate**.
3. From the **Report/Link** drop-down menu, select **2430 SAS Home Page**, because this entry is similar to the entry you are adding.
4. Modify the report fields to correspond to the values that your link uses. For this example, the values would be as follows:
    1. Set **Name** to **SASCanadaHomePage**.
    2. Click **Active** so that the link will appear on the Reports tab.
    3. Set **Position/ID** to **2440**.
    4. Set **Parent** to **2400 SASLinksFolder**.
    5. Set **Link Text** to **SAS Canada Home Page**.
    6. Set **Tooltip Text** to **Link to SAS Canada's Home Page**.
    7. Set **Link URL** to **http://www.sas.com/offices/NA/canada/**.
    8. Set **Show in New Window** to Yes.
5. Click **Validate** to make sure all the values are acceptable. Examples of unacceptable values are those that attempt to make a report a parent of itself, that attempt to delete a report with children, and missing values.
6. Once the **Validate** button returns no errors, click **Save**. To verify, go to the Reports tab, open the **Links** folder, then open the **SAS Links** folder, and the link to SAS Canada Home Page will be the last link in the list.

后退

Descriptions of Report Fields

The following tables describe the fields available when you are working with reports.

Field	**Description**
Report/Link	This is a drop-down menu used to select a report.
Report/Link Name	A unique name for the report. Once are report has been saved, this value cannot be edited.
Active/Inactive	Indicates whether the link is displayed in the tree display of reports.
Position/ID	A unique positive integer that positions the link in the tree display of reports. Reports that share the same parent appear in order of increasing values of this number.
Parent	The parent (containing) node of this report link. All report definitions that share the same parent appear in order of increasing values of their Position/ID number under the link when the tree is expanded.
Link Text	This text will appear as the link to the report output on the Reports tab. Clicking on the link text causes the report output to appear in the frame to the right. Hovering over the link text causes the tooltip text to appear. Clicking on the report listing icon causes the report to appear in a separate window.
Tooltip Text	This text appears as a tool tip when the mouse hovers over the link text.
Link URL	The URL of the report output. The Link URL can be any URL that your browser can display.
Show in New Window	Yes or No based on whether the link should open a new browser window.

Administering Reports

Adding a new folder

The report administration features are available only to users with report administration privileges.

In this example, you will add a new folder to the report tree display. The folder will be called My Custom Links, and it will appear at the bottom of the report tree display.

Folders only have the folder icon when they are the parent of another file.

1. From the Administration tab, select **Report Administration**.
2. Select **Duplicate**.
3. From the **Report/Link** drop-down list, select **2500 USGovernmentLinksFolder**, because this entry is similar to the entry you are adding.
4. Modify the report fields to correspond to the values that your folder uses. For this example, the values would be as follows:
    1. Set **Report/Link Name** to **MyCustom**.
    2. Click **Active** so that the folder will appear on the Reports tab.
    3. Set **Position/ID** to **3000**.
    4. Set **Parent** to **2000 LinksFolder**.
    5. Set **Link Text** to **My Custom Links**.
    6. Set **Tooltip Text** to **Links that I need**.
    7. Verify that **Link URL** is blank.
5. Click **Validate** to make sure all the values are acceptable. Examples of unacceptable values are those that attempt to make a report a parent of itself, that attempt to delete a report with children, and missing values.
6. Once the **Validate** button returns no errors, click **Save**. To verify, go to the Reports tab and open the **Links** folder. **My custom links** will be the last entry in the list. It will not have a folder icon until it is made a parent of another file.

Compliance Administration

Compliance Administration

Introduction

Users with compliance administration privileges should be familiar with the data model, particularly tables related to accounts, customers, lists, and risk classification.

Compliance administration within SAS Anti-Money Laundering involves managing lists, risk classifiers, and risk assessment routing rules.

- Users with the Manage Lists privilege can access the List Management window. Lists can be used to collect values for general internal use, as input values for risk classifiers, and in risk assessment routing rules.
- Users with the Manage Risk Classifiers privilege can access the Risk Classifier Management window and add, edit, and delete risk classifiers. When the underlying table structures associated with the risk assessment process are modified, the involvement of a Database Administrator is required.
- Users with the Manage Risk Assessment Routing Rules privilege can access the Risk Assessment Routing window and configure rules that determine how risk assessments are routed to users and groups.

For complete technical documentation on compliance administration topics, please refer to the **Solution Planning Guide** and the **System Administrator's Guide**.

Compliance Administration

Managing lists

To open the List Management window, from the Compliance Administration tab, select List Management.

Users with the Manage Lists privilege use the List Management window to:

- Add, edit, and delete list categories
- Add, edit, and delete lists
- Add, edit, and delete list values

The List Management window displays lists organized in categories. A list is a collection of account numbers, party numbers, or text values. Lists can be used:

- To collect values for general internal use
- As input values for risk classifiers
- In risk assessment routing rules

To add a category

top

1. Click the category menu icon and select **New Category**.
2. Enter a value for **Name** and, optionally, enter a value for **Description**. The name can contain up to 35 characters and the description can contain up to 255 characters.
3. Click **Save**.

To edit a category

top

1. Select the category.
2. Click the category menu icon and select **Edit Category**.
3. Change the values for **Name** and **Description** as needed. The name can contain up to 35 characters and the description can contain up to 255 characters.
4. Click **Save**.

To delete a category

top

1. Select the category.
2. Click the category menu icon and select **Delete Category**.

You cannot delete a category that contains lists.

To add a list

top

1. Select the category for the new list.
2. Click the list menu icon and select **New List**.
3. Enter a value for **Name** and, optionally, enter a value for **Description**. The name can contain up to 35 characters and the description can contain up to 255 characters.
4. Select a validation type.

    If you select **None**, the entries in the list are not validated against any values in the database.
    If you select **Account Number**, the values in the list must be valid account numbers.
    If you select **Customer Number**, the values in the list must be valid customer numbers.

6. Click **Save**.

To edit a list

top

1. Select the list.
2. Click the list menu icon and select **Edit List**.
3. Change the values for **Name**, **Description**, and **Validation** as needed.

    You cannot change the validation type of a list that contains values.

4. Click **Save**.

To delete a list

top

1. Select the list.
2. Click the list menu icon and select **Delete List**.

If you delete a list, all values in the list are also deleted.

To add values to a list

top

1. Select the list.
2. Click the value menu icon and select **New Entry**.
3. Enter up to 75 characters in the **Value** field and, optionally, enter up to 35 characters in the **Description** field.
4. If you need to add additional values to the list, enter the number of additional values in the **Add Rows** field and click **Go**.
5. Enter data in the additional **Value** and **Description** fields.

    You may want to enter the account or customer name as the description for account number or customer number values.

7. Click **Save**.

The values will be verified if the list's validation type is account or customer number.

To edit a list value

top

1. Select the list value.
2. Click the value menu icon and select **Edit Entry**.
3. Change the values for **Value** and **Description** as needed.
4. Click **Save**.

The values will be verified if the list's validation type is account or customer number.

To delete a list value

top

1. Select the list value.
2. Click the value menu icon and select **Delete Entry**.

Compliance Administration

Managing risk classifiers

To open the Risk Classifier Management window, from the Compliance Administration tab, select Risk Classifier Management.

Users with the Manage Risk Classifiers privilege use the Risk Classifier Management window to:

- Add, edit, and delete risk classifier categories
- Add, edit, and delete risk classifiers

The Risk Classifier Management window displays risk classifiers organized in categories.

To add a category

top

1. Click the category menu icon and select **New Category**.
2. Enter a value for **Name** and, optionally, enter a value for **Description**. The name can contain up to 35 characters and the description can contain up to 255 characters.
3. Click **Save**.

To edit a category

top

1. Select the category you wish to edit.
2. Click the category menu icon and select **Edit Category**.
3. Change the values for **Name** and **Description** as needed. The name can contain up to 35 characters and the description can contain up to 255 characters.
4. Click **Save**.

To delete a category

top

1. Select the category you wish to delete.
2. Click the category menu icon and select **Delete Category**.

You cannot delete a category that contains risk classifiers.

To add a risk classifier

top

1. Select the category for the new risk classifier.
2. Click the risk classifier menu icon and select **New Classifier**.
3. Enter up to 35 characters for **Name**. Optionally, enter up to 35 characters for **Short Description** and up to 255 characters for **Long Description**.
4. Select a risk classifier **Type**. This selection determines which of the fields below are required.

Risk Classifier Type	Required Fields

All risk classifiers	Name, Type, Classifier Fact Column, Weight, Active
Account or Customer Numbers	List, Source Table, Source Column
Account or Customer - Other	List, Source Table, Source Column
Customer Monthly Profile	Source Table, Source Column, Operator, Threshold
Account or Customer Indicators	Source Table, Source Column, Threshold, Indicator
Custom	Operator, and Threshold or Indicator

5. If required, select a **List**. The list provides the values that determine whether the risk classifier contributes to a customer's risk classification. The **List Category** menu facilitates locating lists.
6. If required, select a **Source Table** and a **Source Column**. These fields tell the risk classification process which data this risk classifier will analyze.

   For Account or Customer Number classifiers, if you select FSC_ACCOUNT_DIM as the source table, the source column will be account_number, and if you select FSC_PARTY_DIM as the source table, the source column will be party_number.
7. Select a value for **Classifier Fact Column**. This column is where the risk classification process will store the results of this risk classifier.

   You cannot add a new risk classifier if all the columns in the FSC_CLASSIFIER_FACT table are assigned to other risk classifiers. This includes risk classifiers that are inactive or have been deleted as described below in **To delete a risk classifier**.

   Only one risk classifier can be defined to each column in the FSC_CLASSIFIER_FACT table because the results of the risk classification process are stored in this table.

   If you must add a new risk classifier, your Database Administrator can do one of two things:

   1. *Physically* delete one or more existing risk classifiers from the FSK_RISK_CLASSIFIER table. Although the Risk Classifier Management window provides a way to delete risk classifiers, this is a logical delete, which means they are still in the database.

      CAUTION: Physically deleted risk classifiers cannot be restored.

   3. Add new columns to FSC_CLASSIFIER_FACT.
8. If required, select a value for **Operator**. The operator is used to create analysis conditions for the risk classification process.

   The operator defaults to EQUALS for account and customer indicator classifiers and cannot be changed.
9. If required, enter a value for **Threshold**. The threshold is the numeric limit for analysis conditions.
10. If required, select an **Indicator Value**. The indicator value is used for comparison to indicator columns in the database.
11. Enter a value for **Weight**. This value determines how much this risk classifier contributes to the risk classification for each customer.
12. Select a value for **Active**. Only active risk classifiers are used by the risk classification process.
13. Click **Save**.

To edit a risk classifier

top

1. Select the category and the risk classifier.

3. Click the risk classifier menu icon and select **Edit Classifier**.

    For risk classifiers shipped by SAS, the following fields **can** be modified: short description, long description, operator, threshold, indicator value, weight, active.

    For all other risk classifiers, the following fields **cannot** be modified: name, type, classifier fact column.

5. Modify the enabled fields as needed. If you change the category value, the risk classifier will be organized under the selected category.
6. Click **Save**.

To delete a risk classifier

top

1. Select the category and the risk classifier.

3. Click the risk classifier menu icon and select **Delete Classifier**.

When you delete a risk classifier using the Risk Classifier Management window, the record remains in the database, but the LOGICAL_DELETE_IND column is set to **Y**. This enables the database to store historical information about the risk classifier and provides a way for your Database Administrator to reinstate it in the future, if necessary and desired. Contact your Database Administrator if you want the risk classifier to be physically deleted (in other words, removed from the database).

You cannot delete risk classifiers shipped by SAS.

Compliance Administration

Risk Assessment Routing

To open the Risk Assessment Routing window, from the Compliance Administration tab, select Risk Assessment Routing.

Users with the Manage Risk Assessment Routing Rules privilege use the Risk Assessment Routing window to configure rules for routing risk assessments to users or groups.

The risk classification process routes risk assessments to the selected user or group if the values in the selected list match values in the selected column in the risk assessment table.

Investigation Users can subsequently route risk assessments that they own or have checked out by using the Actions window.

To add a routing rule

top

Enter the following values in a blank routing rule:

1. Enter a value for **Priority**. Rules with higher priority are used first.
2. Select a **List**. The list contains the values used for comparing against data in the risk assessment table. Click the list details icon ▦ to see more information about the selected list.
3. Select a value for **Column**. The column in the risk assessment table contains the data used for matching with the list values.
4. Select a value for **Route To**. Risk assessments that match this rule will be routed to the selected user or group.
5. Click **Save**.

If you need to create more than 10 routing rules, save any changes you made, enter the number of additional rules you need in the **Add Rules** field, and click **Go**.

To edit a routing rule

top

Modify any of the values for a previously saved rule and click **Save**.

- To change the order of the rules, change the priority value.
- If you enter the same priority value for two or more rules, the rule that is currently lower in priority will move to that priority position in the list of rules. All other rules will decrease in priority.

To delete one or more routing rules

top

1. Click the checkbox in the **Delete** column for each rule you wish to delete.
2. Click **Save**. The selected rules will be deleted, and the priority of the remaining routing rules may be adjusted so that they are sequential.

The Summary Tab

The Summary Tab

Introduction

Users with the Access Summary Tab privilege can view the Summary tab. Each Summary window contains three graphs that represent alerts or regulatory reports grouped by user, scenario, and customer. (Alert Aging is the one exception - these three graphs are all grouped by user.)

If System Administrators have enabled regulatory reporting at your site, users with the Access Summary Tab privilege **and** one of the Regulatory Reporting privileges can view the Regulatory Reports window on the Summary tab.

To print a graph

1. Right-click within the graph you wish to print.

3. From the pop-up menu, select **Print Picture**.

The Summary Tab

Alert Aging

The Alert Aging window displays three graphs:

1. Age of Active Alerts, by User

3. Alerts Closed in the Last 30 Days, by User

5. Age of Alerts at Closing, by User

These graphs are generated dynamically when you open the Active Alerts window. This is different from the Reports tab, where all data is updated at once on a schedule that is determined by System Administrators at your site (often this is nightly).

Move the pointer over a bar to see the number of alerts associated with that bar. Click on a bar to open a window that shows the data used to generate that bar.

If there are alerts that are not owned or checked out, they will be displayed in a bar labeled **Unassigned**.

Age of Active Alerts shows the number of active alerts owned or checked out by each user grouped into four date ranges representing the length of time since the alert was generated. The four date ranges are: 0-10 days, 11-20 days, 21-30 days, and over 30 days.

Alerts Closed in the Last 30 Days shows how many alerts each user closed in the last 30 days. The three date ranges are: 0-10 days, 11-20 days, and 21-30 days.

Age of Alerts at Closing shows the length of time that alerts were open before they were closed by users. The four date ranges are: 0-10 days, 11-20 days, 21-30 days and over 30 days.

The Summary Tab

Active Alerts

The Active Alerts window displays three graphs:

1. Active Alerts by User

3. Active Alerts by Scenario

5. Active Alerts by Customer

These graphs are generated dynamically when you open the Active Alerts window. This is different from the Reports tab, where all data is updated at once on a schedule that is determined by System Administrators at your site (often this is nightly).

Move the pointer over a bar to see the number of alerts associated with that bar. Click on a bar to open a window that shows the data used to generate that bar.

Active Alerts by User shows the number of active alerts that each user owns or has checked out. If there are alerts that are not owned or checked out, they will be displayed in a bar labeled **Unassigned**.

Active Alerts by Scenario shows the number of active alerts generated by each scenario.

Active Alerts by Customer shows the number of active alerts for each customer.

The Summary Tab

Closed Alerts

The Closed Alerts window displays three graphs:

1. Closed Alerts by User

3. Closed Alerts by Scenario

5. Closed Alerts by Customer

These graphs are generated dynamically when you open the Closed Alerts window. This is different from the Reports tab, where all data is updated at once on a schedule that is determined by System Administrators at your site (often this is nightly).

Move the pointer over a bar to see the number of alerts associated with that bar. Click on a bar to open a window that shows the data used to generate that bar.

Closed Alerts by User shows the number of alerts that each user closed.

Closed Alerts by Scenario shows the number of alerts that have been closed for each scenario.

Closed Alerts by Customer shows the number of closed alerts for each customer.

The Summary Tab

Suppressed Alerts

The Suppressed Alerts window displays three graphs:

1. Suppressed Alerts by User

3. Suppressed Alerts by Scenario

5. Suppressed Alerts by Customer

These graphs are generated dynamically when you open the Suppressed Alerts window. This is different from the Reports tab, where all data is updated at once on a schedule that is determined by System Administrators at your site (often this is nightly).

Move the pointer over a bar to see the number of alerts associated with that bar. Click on a bar to open a window that shows the data used to generate that bar.

Suppressed Alerts by User shows the number of alerts suppressed by each user.

Suppressed Alerts by Scenario shows the number of alerts that have been suppressed for each scenario.

Suppressed Alerts by Customer shows the number of suppressed alerts for each customer.

The Summary Tab

High-Risk Alerts

The High-Risk Alerts window displays the number of active high-risk alerts by user, by scenario, and by customer.

System Administrators at your site configure a threshold value for money laundering and terror financing risk scores that is considered high risk. Any alert with a money laundering or terror financing risk rank that exceeds the threshold will be included in these graphs.

These graphs are generated dynamically when you open the High-Risk Alerts window. This is different from the Reports tab, where all data is updated at once on a schedule that is determined by System Administrators at your site (often this is nightly).

Move the pointer over a bar to see the number of alerts associated with that bar. Click on a bar to open a window that shows the data used to generate that bar.

If there are alerts that are not owned or checked out, they will be displayed in a bar labeled **Unassigned**.

The Summary Tab

High-Risk Customers

The High-Risk Customers window displays the number of active alerts for high-risk customers by user, by scenario, and by customer.

High-risk customers are defined as those whose risk classification is high. If the subject of an alert is a high-risk customer, the alert will be included in these graphs.

These graphs are generated dynamically when you open the High-Risk Customers window. This is different from the Reports tab, where all data is updated at once on a schedule that is determined by System Administrators at your site (often this is nightly).

Move the pointer over a bar to see the number of customers associated with that bar. Click on a bar to open a window that shows the data used to generate that bar.

If there are alerts that are not owned or checked out, they will be displayed in a bar labeled **Unassigned**.

The Summary Tab

Regulatory Reports

The Regulatory Reports window displays three graphs:

1. Regulatory Reports by User

3. Regulatory Reports by Scenario

5. Regulatory Reports by Customer

These graphs are generated dynamically when you open the Regulatory Reports window. This is different from the Reports tab, where all data is updated at once on a schedule that is determined by System Administrators at your site (often this is nightly).

Move the pointer over a bar to see the number of alerts associated with that bar. Click on a bar to open a window that shows the data used to generate that bar.

If your site contains household- and/or transaction-based alerts, the total of all regulatory reports for a user or scenario may not equal the total of all regulatory reports for a customer.

Regulatory Reports by User shows the number of regulatory reports by user.

Regulatory Reports by Scenario shows the number of regulatory reports by the scenario associated with the alert on which the regulatory report was created.

Regulatory Reports by Customer shows the number of regulatory reports for each customer, defined as all party alerts for the customer and all account alerts where this customer is the primary owner.

Reference

Reference

FAQs

What are the differences between alerts and risk assessments?

What is the difference between a risk rank and a risk classification?

How are risk ranks assigned?

Why can't I reply to an e-mail sent from SAS Anti-Money Laundering?

What is a scenario?

Why do different users see different tabs and icons?

Why do some of my alerts have ***** instead of Check In?

Why do some available alerts have another user's name instead of Check Out?

Answers

What are the differences between alerts and risk assessments?

Alerts	Risk Assessments
Are generated nightly. Are a result of an account, customer, household, or transaction matching one scenario and/or one or more risk factors.	Are generated quarterly or less often. Are a result of the risk classification process.

What is the difference between a risk rank and a risk classification?
Risk ranks are assigned to alerts, while risk classifications are assigned to all customers.

How are risk ranks assigned?
If the alert was created manually, the risk rank was assigned by the user who created the alert. For all other alerts, risk rank is assigned by the solution, which uses conditional probabilities to determine a ranking based on a combination of the severity of the scenario causing the alert, other alerts generated during the same run, recent alert history, risk factors, and the subject's deviation from normal behavior. An alert with a risk of 250 has a lower priority than one with a risk of 850.

Why can't I reply to an e-mail sent from SAS Anti-Money Laundering?
When you request that an e-mail be sent from SAS Anti-Money Laundering, the e-mail originates from the solution and not from your e-mail account.

What is a scenario?
In the context of this solution, a scenario is a program that represents a situation that may be indicative of money laundering. A scenario checks relevant data to see whether that situation has occurred, and if it has, the solution reports this in the form of an alert.

Scenarios were written with parameters that can be changed. This allows scenarios to be fine-tuned so an organization can strike a balance between catching the most likely suspicious activity and reducing the number of false positives. An example of a simple scenario description, with parameters in parentheses, is:

An account's aggregated withdrawal amount exceeds (a certain number of dollars) over (a certain period of time).

An organization may choose to set the parameters for this scenario with the following values:

An account's aggregated withdrawal amount exceeds $10,000 over seven days.

In this case, if the scenario detects that an account holder has withdrawn $20,000 in seven days, then the scenario is said to be *matched* because its parameter values were exceeded, and an alert is generated and routed to the appropriate user or group.

Why do different users see different tabs and icons?

You will see different tabs and icons based on the privileges that your Administrator has given you. Actions that you are not authorized to perform will not appear on your screen.

Why do some of my alerts have ***** instead of Check In?

If you see ***** instead of **Check In**, then you own that alert and cannot check it in. If you want another user or group to investigate an alert that you own, you should Route the alert.

Why do some available alerts have another user's name instead of Check Out?

If an alert's Availability cell gives another user's name, then that user has checked out the alert. If you have Take Alert Ownership privilege, you can take ownership of the alert by clicking on the other user's name.

When you take ownership of an alert, you become the only user who can perform actions on that alert. You cannot check in alerts that you have taken ownership of. If you decide another user or group should investigate the alert, you should route the alert.

Reference

Glossary

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

A top

Alert - A report of a situation that may be indicative of money laundering. Alerts are displayed on alert list windows, which provide tools and information to aid users as they determine whether alerts represent suspicious activity that should be reported to authorities. Once this determination is made, users close the alerts.

Alert Generation Process - The alert generation process analyzes customers and transactions, detects suspicious activities, and makes results available to the Investigation user interface. It usually runs each night, but it is scheduled by administrators at your site. For more information about the alert generation process, see the System Administrator's Guide.

Alert List Windows - Four windows are referred to as alert list windows:

1. My Alerts
2. Available Alerts
3. Suppressed Alerts
4. Closed Alerts

Access to the Suppressed Alerts and Closed Alerts windows is restricted by user privileges.

B top

Batch SAR Collection Process - A process that collects all SARs that have a status of Prepared for Batch SAR Collection and formats them according to FinCEN's specifications for batch filing. The batch SAR collection process is scheduled and managed by System Administrators at your site.

C top

Category - The type of behavior that caused the alert. An alert's category label comes from the scenario that triggered the alert. SAS Anti-Money Laundering has many scenarios, and these are organized into categories by the type of behavior that they check for. For example, there are several scenarios that detect Structuring And Obfuscation, so this is one of the categories. Other categories are Unexpected Deposits, Cash Activity, and Wire Activity. Administrators at your site determine which categories are appropriate for your organization. Manual alerts, which are created by users, are categorized as **Manual**.

Compliance Administrator - A user with compliance administration privileges and responsibilities. Compliance administration within SAS Anti-Money Laundering involves managing lists, risk classifiers, and risk assessment routing rules. Compliance Administrators should be familiar with the data model, particularly tables related to accounts, customers, lists, and risk classification.

Core - A large database that contains all of the customer data necessary to support the alert generation process. Once alerts have been created, transactions related to each alert are replicated from the Core to the Knowledge Center.

Create Date - The system-assigned date on which the alert was created, whether it was created by the alert generation process or by a user. The alert list windows display the **Create Date**. The **Create Date** is not necessarily the date on which the suspicious activity occurred. See also Run Date.

F

top

Format for CSV export files - System administrators at your site can select between two formats for the CSV files exported from alert list, risk assessment, query results, Customer Transactions, and Alert Details windows. The default format is a standard RFC 4180 Comma-Separated Values file. The other option is a CSV file that has a 'value' format applied to long numeric strings, such as account numbers, to prevent spreadsheet applications from converting them to dates. System administrators can also specify which delimiter to use (default is comma) and the maximum number of rows to export (default is 1,000).

I

top

Investigation Started/Investigation Not Started - In environments where alerts and risk assessments must be processed within a certain amount of time, it can be helpful to know whether investigation has begun on an alert or risk assessment. The following windows use folder icons to indicate whether investigations have started: My Alerts, Available Alerts, My Risk Assessments, and Available Risk Assessments.

Click the folder icon to open the Alert History or Risk Assessment History window, which displays the date on which the investigation was started, as well as the user who performed the action that started the investigation.

<table>
<tr><td colspan="2">A plain folder 📁 indicates that investigation has not started.</td></tr>
<tr><th>Actions that <i>do not</i> start an alert</th><th>Actions that <i>do not</i> start a risk assessment</th></tr>
<tr><td>• Checking an alert in or out
• Routing an alert
• Sending alert details in an e-mail
• Setting an e-mail reminder
• Viewing the Scenario Details window</td><td>• Checking a risk assessment in or out
• Routing a risk assessment
• Sending risk assessment details in an e-mail</td></tr>
</table>

<table>
<tr><td colspan="2">A folder with a clock 📁🕒 indicates that investigation has started.</td></tr>
<tr><th>Actions that start an alert</th><th>Actions that start a risk assessment</th></tr>
<tr><td>• Viewing detail windows specific to that alert
• Adding comments
• Attaching documents
• Creating a regulatory report</td><td>• Viewing detail windows specific to that risk assessment
• Adding comments
• Attaching documents
• Closing the risk assessment</td></tr>
</table>

• Suppressing or closing the alert • Creating the alert, in the case of manual alerts	• Creating the risk assessment, in the case of manual risk assessments

Investigation UI - A secure Web-based user interface (UI) for managing and investigating alerts and risk assessments. Investigation Users can view various customer, account, transaction, scenario, and risk assessment details, as well as add comments and electronic attachments, and take other actions to change the status of an alert or risk assessment.

Investigation Users - Users who use the Investigation UI to investigate alerts and risk assessments. Other roles in relation to the Investigation UI are System Administrators and Compliance Administrators. Some individuals may have more than one role.

K top

Knowledge Center - A database that contains definitions of scenarios, risk factors, administration items, alerts, and copies of all transactions related to each alert.

M top

Money Laundering Risk Rank - Each alert's money laundering risk is expressed as a numerical rank between one and 999. The risk rank indicates the level of risk exhibited by a customer for engaging in suspicious activity that may be indicative of money laundering, and therefore the priority of the alert. If the alert was created manually, the risk rank was assigned by the user who created the alert. For all other alerts, risk rank is assigned by the solution, which uses conditional probabilities to determine a ranking based on a combination of the likelihood of money laundering and the subject's deviation from normal behavior. An alert with a risk of 250 has a lower priority than one with a risk of 850.

O top

Owner - The owner of an alert is the only person who can view and perform actions on it. More.

P top

Parameter - A variable factor or characteristic. In information technology, a parameter is an item of information - such as a name, a number, or a selected option - that is passed to a program by a user or another program. Parameters affect the operation of the program receiving them. The Scenario Details window describes how a scenario's parameters were set when the alert was generated.

Q top

Query - A set of instructions that requests particular information from one or more data sources.

R top

Risk Assessment - A proposal to change a customer's risk classification. Risk assessments are displayed on My Risk Assessments and Available Risk Assessments. Each risk assessment has a current risk classification and a proposed risk classification. The objective is to determine whether the proposed risk classification should be accepted and closed, or rejected and closed.

Risk Assessment List Windows - Two windows are referred to as risk assessment list windows:

1. My Risk Assessments
2. Available Risk Assessments

Risk assessments are an optional component of SAS Anti-Money Laundering. If enabled, users with the View Risk Assessments privilege can see the Risk Assessments tab and risk assessment list windows.

Risk Classification - Designates which of three levels best describes a customer's risk of money laundering. Each customer is assigned a risk classification expressed as **H** (high or 3), **M** (medium or 2), or **L** (low or 1). Risk classifications are displayed on the risk assessment list windows and the related detail windows.

Risk Classifier - A rule that the risk classification process uses as input to determine a customer's risk classification. The Risk Assessment Details window, which can be accessed by clicking the value for Assessment ID on a risk assessment list window, displays each risk classifier that contributed to a customer's total risk classification score - a value that is used to determine the customer's risk classification. The Risk Assessment Details window also displays all active risk classifiers. Some sample risk classifiers are shipped with SAS Anti-Money Laundering; others are created and managed by Compliance Administrators at your site.

Risk Classification Process - The risk classification process (RCP) determines each customer's risk classification (high, medium, or low). If a customer's risk classification changes, the RCP surfaces a risk assessment and associated information in the Investigation user interface. The RCP may run quarterly or less often, and is scheduled by administrators at your site. For more information about the RCP, see the **System Administrator's Guide**.

Risk Factor - In the context of this solution, a risk factor is a program that represents a situation that may be indicative of money laundering, but is more common than a scenario. A risk factor checks relevant data to see whether that situation has occurred.

- If a risk factor is matched for a subject that also matches a scenario (thereby generating an alert), then the risk factor is attached to the alert to provide a description of the behavior and to raise the alert's risk score.
- If a subject does not match a scenario, but matches risk factors that give the subject a combined risk factor score that exceeds a threshold for either terror financing risk or money laundering risk, then a risk-factor-only alert is created.

Risk-Factor-Only Alert - A system-generated alert that is based entirely on risk factors, instead of a scenario. If a subject does not match a scenario, but matches risk factors that give the subject a combined risk score that exceeds a threshold for either terror financing risk or money laundering risk, then a risk-factor-only alert is created. Risk-factor-only alerts can be identified by the contents of the Scenario and Triggering Values columns on an alert list window. The Scenario column will display ML_Risk or TF_Risk, and the Triggering Values column will say "Click risk rank for details." Click the corresponding value for either Money Laundering Risk or Terror Financing Risk to open the Risk Factors window, which displays a list of the risk factors that contributed to the alert, and links to the Risk Factor Details window. Administrators at your site set the thresholds for risk-factor-only alerts.

Risk Rank - Each alert's risk is expressed as a numerical rank between one and 999 in two categories: Money Laundering Risk and Terror Financing Risk. The risk rank indicates the level of risk exhibited by a customer for engaging in suspicious activity that may be indicative of either money laundering or terror financing, and therefore the priority of the alert. If the alert was created manually, both risk ranks were assigned by the user who created the alert. For all other alerts, both risk ranks are assigned by the solution, which uses conditional probabilities to determine ranking. A risk of 250 represents a lower priority than a risk of 850.

Run Date - If the alert was created by the alert generation process, the run date is the date of the data being processed. If the alert was manually created, the run date was assigned by the user who created the alert. The **Run Date** is displayed on the Alert Details window. See also Create Date.

S top

SAS Anti-Money Laundering Resource Center - A Web site that facilitates communication between the development team and licensed customers. Use the Resource Center to:

- Download product documentation and supplemental files.
- Check for documentation updates - Documents may be updated to accommodate Hot Fixes or to correct errors. The latest version will always be available on the Resource Center. To determine whether you have the most recent version, compare the edition number on your document cover with the edition number displayed on the Resource Center.
- Submit comments and suggestions about the software and documentation - Fill out the feedback form on the Resource Center.
- Read about the SAS Anti-Money Laundering User Forum - The purpose of User Forum is to facilitate the sharing of information among developers, users, and implementation partners.

To access the Resource Center, contact SAS Technical Support.

Scenario - In the context of this solution, a scenario is a program that represents a situation that may be indicative of money laundering. A scenario checks relevant data to see whether that situation has occurred, and if it has, an alert is generated. The alert list windows display the name of the scenario that triggered each alert, and provide a link to the Scenario Details window.

Scenarios were written with parameters that can be changed. This allows scenarios to be fine-tuned so an organization can strike a balance between catching the most likely suspicious activity and reducing the number of false positives. An example of a simple scenario description, with parameters in parentheses, is:

An account's aggregated withdrawal amount exceeds (a certain number of dollars) over (a certain period of time).

An organization may choose to set the parameters for this scenario with the following values:

An account's aggregated withdrawal amount exceeds $10,000 over seven days.

In this case, if the scenario detects that an account holder has withdrawn $20,000 in seven days, then the scenario is said to be *matched* because its parameter values were exceeded, and an alert is generated and routed to the appropriate user or group.

Scenario Administrator - A separate user interface to SAS Anti-Money Laundering. The Scenario Administrator UI is used to manage headers, scenarios, risk factors, and alert routing.

Subject - The subject of an alert is the account, customer, household, or transaction that exhibited the behavior that caused the alert. Each scenario and risk factor focuses on a single subject. Account scenarios and risk factors check for suspicious account activity, such as high turnover or periods of dormancy. Customer scenarios and risk factors check for suspicious customer activity, such as depositing numerous small amounts into multiple accounts. Likewise, the household and transaction scenarios check for suspicious household and transaction activity.

Suppressed (Batch) - Status code for an alert that an administrator suppressed during the alert generation process. When applicable, this status code is displayed in the Alert History window.

Suppressed (UI) - Status code for an alert that a user suppressed by using the Actions window of the user interface. When applicable, this status code is displayed in the Alert History window.

System Administrator - System Administrators at your site configure and maintain SAS Anti-Money Laundering. During the installation process, they define system-wide properties that determine, for example, which format will be used when downloading data to CSV files, the maximum number of rows to be returned by each query component, whether user names are case-sensitive, whether users who send e-mail from the system are automatically copied on those e-mails, whether certain tabs and features are enabled, and how long suppressed and closed alerts can be accessed via user interface windows and query results. They administer options displayed in the user interface, such as lists of possible reasons for creating and closing alerts and risk assessments. They use the Scenario Administrator user interface to activate and de-activate scenarios and risk factors, as well as to edit properties, adjust parameter values, and determine how new alerts are routed to users and groups.

T

top

Take Alert Ownership - Users with Take Alert Ownership privilege can move alerts from another user's My Alerts window to theirs. If you take an alert from another user, you will own the alert. This is called "taking ownership." If you **own** an alert, your manager can take ownership if he/she has Take Alert Ownership privilege. If you have **checked out** an alert, your manager and others in your group can take ownership if they have Take Alert Ownership privilege. For more details, see Understanding owned and checked out alerts.

Take Risk Assessment Ownership - Users with this privilege can move risk assessments from another user's My Risk Assessments window to theirs. If you take a risk assessment from another user, you will own the risk assessment. This is called "taking ownership." If you **own** a risk assessment, your manager can take ownership if he/she has Take Risk Assessment Ownership privilege. If you have **checked out** a risk assessment, your manager and others in your group can take ownership if they have Take Risk Assessment Ownership privilege. For more details, see Understanding owned and checked out risk assessments.

Target - In Web browser terminology, the target is the page you see after you click on a link.

Terror Financing Risk Rank - Each alert's terror financing risk is expressed as a numerical rank between one and 999. The terror financing risk rank indicates the level of risk exhibited by a customer for engaging in suspicious activity that may be indicative of terror financing, and therefore the priority of the alert. If the alert was created manually, the risk rank was assigned by the user who created the alert. For all other alerts, risk rank is assigned by the solution, which uses conditional probabilities to determine a ranking. An alert with a risk of 250 has a lower priority than one with a risk of 850.

Time Out - If a SAS Anti-Money Laundering user interface is inactive for a predefined time period, it expires, and you must log back on to continue working. In Web browser terminology, this expiration is referred to as timing out.

Triggering Values - This is one of the columns on alert list windows. Triggering values provide a brief summary of the activity responsible for the generation of a scenario-based alert.

- If the alert was created manually, the triggering values will be **None**.

- If the alert is a risk-factor-only alert, the triggering values will say "Click risk rank for details" because risk-factor-only alerts do not involve scenarios. Clicking the risk rank for these alerts is the best way to find out what behavior caused the alert to be generated.

Risk factors also have triggering values. They are displayed on the Risk Factor Details window.

U

top

Unrestricted Query - A query with no criteria. For example, if you opened the Alert Query window and clicked **Show Matching** without restricting by any of the criteria, SAS Anti-Money Laundering would interpret this unrestricted query as a request to view every alert in the system. A request to view every alert, account, customer, household, or transaction in the system will be so resource-intensive that the system could slow down or even stop operating.

UI - User interface.

V

top

Velocity Factor - A measure of how quickly money flows through an account, regardless of how much is normally in that account. The velocity factor is expressed as a decimal where the closer the value is to 1, the faster funds that were deposited were withdrawn. This term only appears on the Risk Factors window for alerts that are associated with the risk factor that measures velocity factor.