ACCUITY

Compliance Link
Administrator Guide

February, 2018 / Version 3.4

© 2018 ACCUITY

TABLE OF CONTENTS

1. INTRODUCTION

Accuity's Compliance Link is an enterprise-wide, modular solution for screening prospect, customer, vendor and employee information, plus financial transaction data against lists mandated by governments and AML regulatory organizations. Compliance Link was designed around Accuity's unrivaled compliance data and industry-leading filter engine to facilitate compliance with requirements of programs such as the Bank Secrecy Act (BSA) and the USA PATRIOT Act, as well as the U.S. Treasury's Office of Foreign Assets Control (OFAC) and requirements to screen cross-border ACH transactions (IATs). Compliance Link's ability to cast a wide net while minimizing the operational burden makes it best in class.

Compliance Link is interdiction screening software developed as a comprehensive solution that enables organizations to holistically manage AML screening and compliance programs enterprise-wide. Compliance Link is capable of screening a wide variety of data from numerous sources ranging from financial transactions to customer and vendor information. It includes a Case Management module that can immediately streamline your workflow and false positive reduction tools to increase screening efficiencies.

This Administrator Guide will provide detailed instructions on how to use the application to create the best practices within Compliance Link to fit within individual institution's processes. It will also serve as a useful reference tool for those individuals familiar with the application. For further questions regarding the application or this manual please contact our Technical Support staff at Support@Accuity.com.

2. USER ROLES

Compliance Link allows for the creation of customizable User Roles which group different sets of features that determine what functions a user can access within the application. Compliance Link comes with six standard User Roles (Administrator, Application User, Lookup Supervisor, Lookup User, Review Only, and Supervisor). This section describes how to add/edit custom User Roles.

> ➢ **NOTE:** A prerequisite to creating/modifying User Roles is to have the Institution Management feature set. By default, users with the Administrator User Role have the Institution Management feature set.

2.1. Feature Sets

This section includes a comprehensive listing of all feature sets including descriptions.

> ➢ **NOTE:** Depending on your implementation of Compliance Link, this listing may include feature sets that are unavailable to your Institution. For more information, please contact ComplianceLinkInfo@Accuity.com.

2.1.1. Application Features

- **Automated Screening Lookup** – Ability to access the Automated Screening Lookup tool which allows for real-time import and screening of records into an Automated Screening dataset.

- **Batch Maintenance** – Ability to access the Batch Maintenance screen, which allows for search, review, and deletion of previously screened files.

- **Good File Preload** – Ability to perform a Good File Preload. For more information please review the Good File Preload section of this User Manual.

- **ILS Activity History** – Ability to search on previously performed lookups.

- **ILS Custom Lookup** – Ability to perform Custom Lookups.

- **ILS Lookup** – Ability to perform Interactive Lookups.

- **Manage File Specifications** – Ability to add new and modify current File Specifications.

- **Review/Search Matches** – Ability to perform Match, Transaction, and Case Review searches. Also includes access to Match Inbox and provides the ability to change the status of accessible matches.

- **Screen a File** – Ability to perform Simple and Custom Screenings of batch files.

- **Search Good File** – Ability to search on and inactivate Good File records.

- **Search Matches (Read-only)** – Ability to perform Match, Transaction, and Case Review searches. Also includes access to Match Inbox, but this feature set does not allow for the changing of match statuses. This is for Compliance Link matches only, not Automated Screening Manager.

2.1.2. Application Configuration

- **Automated Screening Case Admin** – Ability to access all Automated Screening cases, including cases in final status and cases with no matches.

- ➢ **NOTE:** If a user has multiple roles that are mapped to feature sets that include Case Search, it should only be seen once. Having this feature set will mean that the user should see the "admin" version of the case search screen in Automated Screening Manager.

- **Commodity List Manager** – Ability to access the Commodity List Manager tool to add/edit MLCWLXML files. For more information please refer to the **Commodity List Manager User Guide**.

- **Controlled Goods Manager Admin** – Ability to access Controlled Goods Manager to add/edit Controlled Goods Policies for screening against Dual-use Goods lists. For more information please refer to the Controlled Goods Manager documentation.

- **ILS Configuration** – Ability to configure Fields and Screening Profiles in the Interactive Lookup System.

- **Institution Management** – Ability to access Institution Summary and Search Institution pages. This is a prerequisite to User Management, Manage GWL Subscriptions and User Activity Audit Trail reports.

- **Manage Dictionaries and Char. Map** – Ability to upload Synonym Dictionaries and Character Mapping files.

- **Manage GWL Subscriptions** – Ability to add/remove Global WatchList lists from an Institution's subscription. (Must have Institution Management feature set).

- **Manage Private Lists** – Ability to upload Private Watch Lists (PWL) into Compliance Link from Private File Creator.

- **Private List Manager** – Ability to access the Private List Manager tool to add/edit private UPIDGWL data files. For more information please refer to the **Private List Manager User Guide**.

- **User Activity Audit Trail** – Ability to access and export User Security Audit and User Application Audit reports. (Must have Institution Management feature set).

- **User Management** – Ability to create/modify User Roles, add/edit/delete Users, and add/edit User Groups. (Must have Institution Management feature set).

2.1.3. Workflow Management

- **Automated Screening Workflow** – Ability to configure Automated Screening Manager workflow including Assign Hierarchy and Dataset Workflow stages.

- **Case Management Configuration** – Ability to create folders, Assignment Rules, Forwarding Rules, and general Case Management workflow.

- **False Positive Reduction Rules Management** – Ability to add, edit, and/or inactivate False Positive Reduction Rules.

- **Manage Review Notes** – Ability to add, edit, and/or inactivate standard Review Notes.

- **Match Status Management** – Ability to create and/or inactivate Custom Match Statuses. (Must have Case Management Configuration feature set).

- **Risk Scorecard Management** – Ability to add and inactivate Risk Scorecards.

- **Screening Profile Management** – Ability to add, edit, inactivate Screening Profiles for batch screening.

- **View Dashboard** – Ability to view the Dashboard screen.

2.2. Adding User Roles

Add a New User Role

1. Click on the **Institution Summary** link in the sidebar. If your Institution is running in Service Bureau mode, this link will say **Search Institutions**. Click on the Institution in which you would like to create a new User Role.

2. Click on the **Add User Role** button on the right side of the screen.

3. Enter a name for the User Role.

4. Choose the feature sets to add to the new custom User Role.

5. Click on **Save** to create the new User Role. Clicking **Cancel** will return to the **Institution Summary** screen and clicking **Reset** will reset the screen.

Add Custom User Role

• = Required Field

Name: [   ] •   Status: Active

User Role Features •

Application Features	Application Configuration	Workflow Management
☐ Batch Maintenance	☐ Commodity List Manager	☐ Case Management Configuration
☐ Good File Preload	☐ ILS Configuration	☐ False Positive Reduction Rules Management
☐ ILS Activity History	☐ Institution Management	☐ Manage Review Notes
☐ ILS Custom Lookup	☐ Manage Dictionaries and Char. Map	☐ Match Status Management
☐ ILS Lookup	☐ Manage GWL Subscriptions	☐ Risk Scorecard Management
☐ Manage File Specifications	☐ Manage Private Lists	☐ Screening Profile Management
☐ Review/Search Matches	☐ User Activity Audit Trail	☐ View Dashboard
☐ Screen a File	☐ User Management	
☐ Search Good File		
☐ Search Matches (Read-only)		

[Save] [Cancel] [Reset]

Edit a User Role

1. Click on the **Institution Summary** link in the sidebar. If your Institution is running in Service Bureau mode, this link will say **Search Institutions**. Click on the Institution in which you would like to create a new User Role.

2. Click on the User Role to edit.

3. Enter a **Name** for the User Role.

4. Choose the feature sets to add to the new custom User Role.

5. Click on **Save** to create the new User Role. Clicking **Cancel** will return to the **Institution Summary** screen and clicking **Reset** will reset the screen.

Add Custom User Role

• = Required Field

Name: [   ] •   Status: Active

User Role Features •

Application Features	Application Configuration	Workflow Management
☐ Batch Maintenance	☐ Commodity List Manager	☐ Case Management Configuration
☐ Good File Preload	☐ ILS Configuration	☐ False Positive Reduction Rules Management
☐ ILS Activity History	☐ Institution Management	☐ Manage Review Notes
☐ ILS Custom Lookup	☐ Manage Dictionaries and Char. Map	☐ Match Status Management
☐ ILS Lookup	☐ Manage GWL Subscriptions	☐ Risk Scorecard Management
☐ Manage File Specifications	☐ Manage Private Lists	☐ Screening Profile Management
☐ Review/Search Matches	☐ User Activity Audit Trail	☐ View Dashboard
☐ Screen a File	☐ User Management	
☐ Search Good File		
☐ Search Matches (Read-only)		

[Save] [Cancel] [Reset]

3. ADDING & EDITING USERS

Only users with the User Management feature set can add or edit users.

Add a New User Using Compliance Link Authentication (User ID and Password)

1. Click on the **Add User** link in the sidebar.

2. Fill out the information fields relating to the new user. All mandatory fields are marked by a red dot "•".

3. Choose the Roles for this user. For more information about User Roles please refer to the **User Roles** section of this **Administration Guide**.

   ➢ **NOTE:** No two users can have the same User ID.

4. Click on **Save** to create the new user. A new screen should appear displaying that the new user was created successfully.

Add a New User Using External Authentication (Not available on Accuity-Hosted)

1. Click on the Add User link in the sidebar.

2. Fill out the information fields relating to the new user. All mandatory fields are marked by a red dot "•".

   ➢ **NOTE:** If External Authentication is chosen, Compliance Link will authenticate the user using the External Authentication Identifier (LDAP User Name) and the Password fields will be un-used. For more information please refer to the **Compliance Link Installation Guide** or contact Technical Support.

   ➢ **NOTE:** Click on the **Search** button to look-up External Authentication users from the LDAP server configured in Compliance Link. For more information please refer to the **Compliance Link Installation Guide** or contact Technical Support.

3. Choose the Roles for this user. For more information about User Roles please refer to the **User Roles** section of this **Administrator Guide**.

4. Click on **Save** to create the new user. A new screen should appear displaying that the new user was created successfully.

⊚ User Information

• The user NewUser was created successfully.

Continue

Edit an Existing User

1. Click on the Search Users link in the sidebar.

2. Enter the search criteria:

    a. **First Name**

    b. **Last Name**

    c. **User ID**

    d. **Email**

    e. **Status** (Active/Inactive)

⊚ Search For User

First Name:

Last Name:

User ID:

E-Mail:

Status: -- Select --

Search   Cancel   Reset

➢ **NOTE:** To search for all users leave all fields blank.

1. Click on **Search**.

2. Click on a User ID that you would like to edit.

3. Make necessary changes to the User's information. All mandatory fields are marked by a red dot "•".

4. Click on **Save** to save.

If the user's status is Inactive, he/she will be unable to sign into the application.

If a user is locked out (reported by an error message), the User Management user will be able to restore the login by clicking on the Unlock User button on the User Information screen for that user. The User Management user may need to change the user's password if it has been lost/forgotten before the user can sign in again.

Change a User's Password

1. Click on the **Change Password** button from the User Information screen.

2. Enter the New Password.

3. Re-enter the New Password.

4. Enter the **Password Hint**.

5. Click **Save**.

   ➢ **NOTE:**   Always change the password first. Then, go to main user screen and make changes. Making changes on the main screen without saving and then clicking **Change Password** resets any changes made to the user information.

   ➢ **NOTE:**   If External Authentication is being used, User Management users will not be able to change passwords within Compliance Link. They must be changed on the LDAP server configured in Compliance Link. For more information please refer to the **Compliance Link Installation Guide** or contact Technical Support.

3.1. Setting Web Service credentials for WS-Security

Currently only applicable for Automated Screening Manager (ASM) Web Services (Import and Screening Service and Case Management Service). There is further details in this guide explaining the features and functionality of ASM.

An Access ID and Password will need to be created on the Institution Summary Page (**Web Service Access Credentials)** to use the ASM web services. Please see the programmers guides and installations guides for these services.
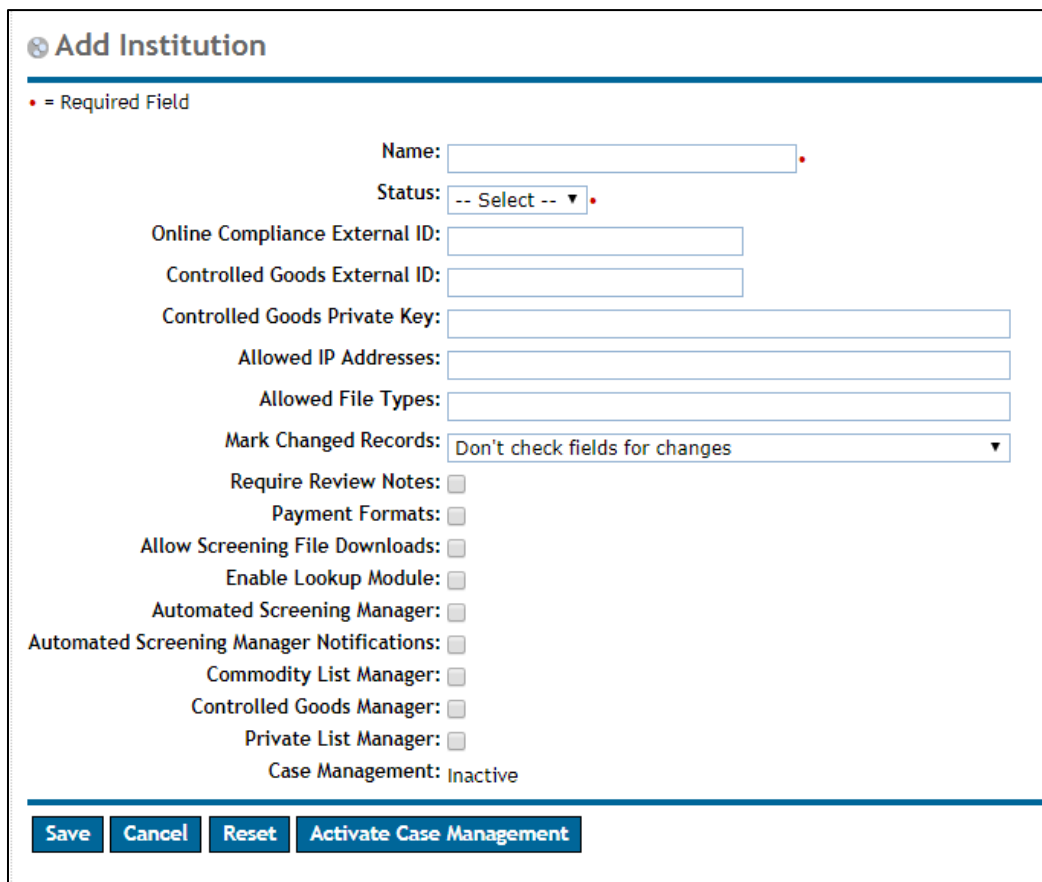
3.2. Adding & Editing Institutions

Only users with the Institution Management feature set can add or edit institutions and institutions can only be added in Service Bureau Mode accounts.

> ➢ **NOTE:** For more information regarding Service Bureau Mode accounts please contact your Account Manager or email Support@Accuity.com.

3.3. Adding Institutions

Add a New Institution

1. Click on the **Add Institution** link in the sidebar.

2. Enter the **Name** of the institution.

3. Change the **Status** to Active.

4. Enter the **Online Compliance External ID.** This is an authentication code for direct access to external websites. Accuity provides this code for access to Online Compliance, Accuity's

online enhanced due diligence research tool. For more information regarding Online Compliance please email Support@Accuity.com.

5. Enter the **Controlled Goods External ID.** This is an authentication code for direct access to Controlled Goods Manager. For more information regarding Controlled Goods Manager please email Support@Accuity.com.

6. Enter the **Controlled Goods Private Key.** This is an authentication code for direct access to Controlled Goods Manager. For more information regarding Controlled Goods Manager please email Support@Accuity.com.

7. Enter the **Allowed IP Addresses** for user logins for this institution. If left empty, no IP Address validation will occur. All IP Addresses entered will have a default wild card. Please note the limit of 100 characters.

8. Add or remove applicable **Allowed File types** for the institution. These extensions will be enforced during file uploads if added. Extensions should be comma separated. Ex: (.TXT, .ZIP, .PDF)

9. Choose the **Mark Changed Records** options.

   a. **Don't check fields for changes** – Compliance Link will mark records as Changed only when the field causing the match has changed.

   b. **Check all fields for changes** – Compliance Link will mark records as Changed when any input field has changed.

   c. **Check only Screening Fields and Match Field for changes** – Compliance Link will mark records as Changed when any of the Screening Fields or Match Field changes.

10. Check the **Require Review Notes** box to require users to enter Review Notes when making status changes in Compliance Link and Automated Screening Manager.

11. Check the **Payment Formats** box to enable the Payments File Specifications in the dropdown lists when screening a file, Good File Pre-Load, and Auto File Transfer.
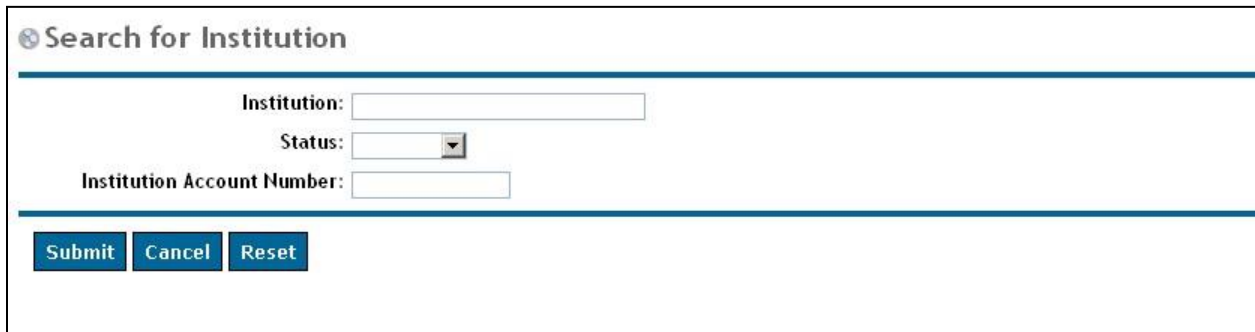
   ➢ **NOTE:** You must purchase the Payments module from Accuity in order to have access to the Payment File Specifications.

12. Check the **Allow Screening File Downloads** to allow users to download the original file screened from the Batch Detail screen.

13. Check **Enable Lookup Module** to allow for use of the Interactive Lookup System. For more information please refer to the **Interactive Lookup System** section of this **Administrator Guide** or contact Support@Accuity.com.

14. Check **Automated Screening Manager** to allow for use of the Automated Screening Manager module. For more information please refer to the **Automated Screening Manager** section of this Administrator Guide or contact Support@Accuity.com.

15. Check **Commodity List Manager** to allow for use of the Commodity List Manager application. For more information please refer to the **Commodity List Manager Administrator Guide** or contact Support@Accuity.com.

16. Check **Controlled Goods Manager** to allow for use of the Controlled Goods Manager application. For more information please contact Support@Accuity.com.

17. Check **Private List Manager** to allow for use of the Private List Manager application. For more information please refer to the **Private List Manager Administrator Guide** or contact Support@Accuity.com.

18. Click **Save**.

3.4. Editing Institutions

Review an Institution's Settings

1. Click on the **Search Institutions** link in the sidebar.

2. Enter the **Institution Name**, **Status**, and/or **Institution Account Number**. If these are left blank all Institutions will show on the search results screen.

3. Click on **Search**.

Search for Institution Results

Search Criteria:
Bank/Account Name: Product

Bank/Account Name	Status
Product Demo	Active

4. Click on the Bank/Account Name you wish to review. You will then get the Institution Summary Information page. Bank/Account Name and Institution are interchangeable.

Institution Summary Information

Inactive items are marked with an *****

Account: Sample		Edit Institution
Account Numbers: 12345		Edit Account Numbers

User Roles: Administrator
Application User
Lookup Supervisor
Lookup User
Review Only
Supervisor

Add User Role

User Groups: Default Group
New Sample

Add User Group

Users: Mike Vaughn (New Sample)
* Mike1 vaughn1 (Default Group)

Add User
User Security Audit
User Application Audit

Subscribed Lists: Accuity's OFAC List
Accuity OFAC Enhancements
US PEP List powered by WorldCompliance
PEP List powered by WorldCompliance

AutoPFC import
somethingMORE

Edit List Subscriptions

3.4.1. Edit Institution

Edit an Institution

1. Click on the **Edit Institution** button.

2. Change the necessary fields and click **Save**.

3. To deactivate Case Management, click on the **Deactivate Case Management** button.

> ➤ **NOTE:** If an institution has **Inactive** or **Pending** for its status, no users will be able to log in at that institution, and any screenings done by the multi-processor for account numbers assigned to that institution will cause errors.
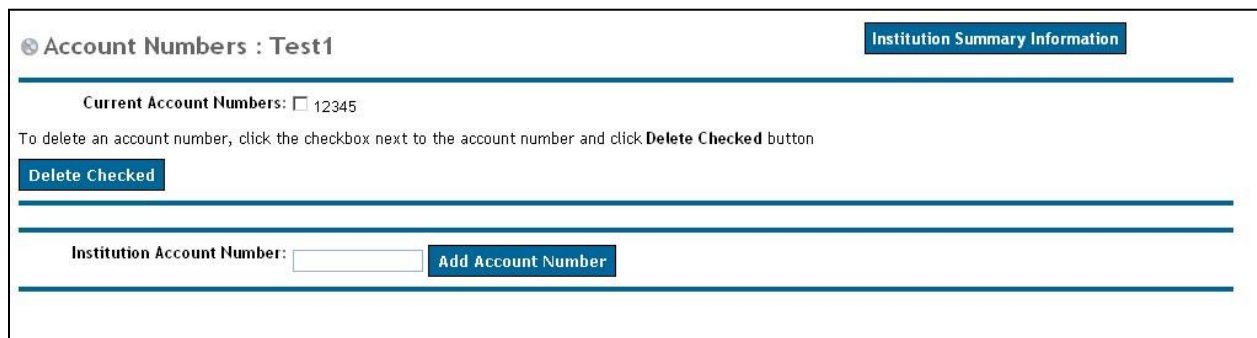
3.4.2. Edit Account Numbers

If you choose to use Compliance Link in Service Bureau mode you may add or edit account numbers. Account Numbers are used to identify which child institution a match is sent. For instance, if a parent institution is screening a file consisting of records from 3 separate child institutions, each record would reference an Account Number and be routed accordingly.

Add or Edit Account Numbers

1. Click on the **Edit Account Numbers** button to update or delete current account numbers.

2. To add a new account number, enter the number in the Institution Account Number field and click on **Add Account Number**.

3. Click on **Institution Summary Information** to return to the Institution Summary page. The Institution Summary page gives you a high-level overview of the Institution, including Users, User Groups, and Global WatchList subscriptions.

> ➤ **NOTE:**   No two institutions can have the same account number. If you try to add an account number that already exists at another institution within your group, you will get the following error: Duplicate Institution Account Numbers are not allowed.

3.5. User Groups

User Groups are important to understand when using the Interactive Lookup System and Automated Screening Manager. You can add users to specific User Groups and these User Groups define whether an ILS user will have the ability to review matches from ILS. Additionally, workflow and case assignment in Automated Screening Manager is based on the user group.

3.5.1. Add/Edit User Groups

Add a New User Group

1. Click on **Add User Group**.
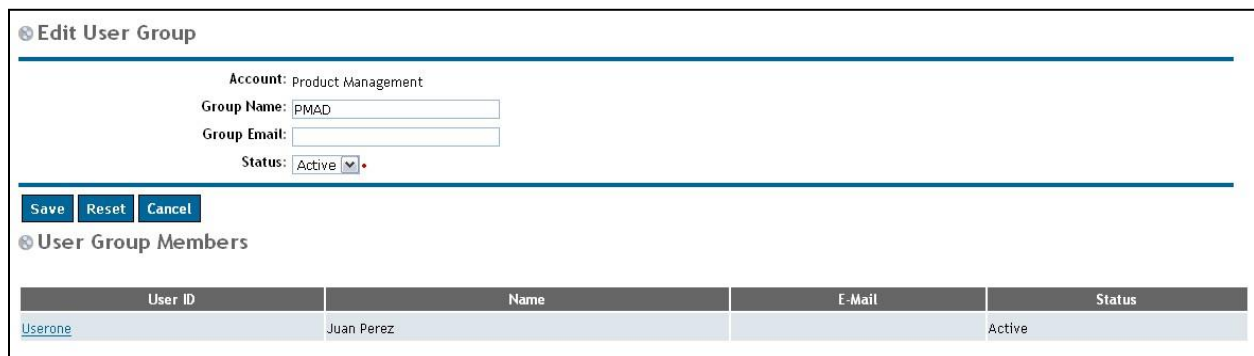
2. Enter the **Group Name**.

3. Click on **Save**. This User Group can now be assigned to new or existing users.

Edit an Existing User Group

1. Click on the existing User Group name.

2. Make necessary changes to **Group Name**, **Group Email**, and/or **Status**.

3. Click on **Save** to save changes made to the User Group. Click on **Reset** to eliminate all changes made or click on **Cancel** to go back to the Institution Summary Information screen.

Edit an Institution's Users

1. Click on a current user to update or delete the record, or **Add User** to add new users. Specific instructions dealing with adding and editing users can be found in the **Adding & Editing Users** section.

   a. If a user is locked out, an Administrator will see an **Unlock User** button on the User Information screen for that user. Click on the **Unlock User** button and the user will be able to try again. You may need to change the user password, if the user has forgotten it.

   b. To edit a current user, click on the name of the user. You will get the User Information screen. Make any necessary changes and click on **Save** to save.
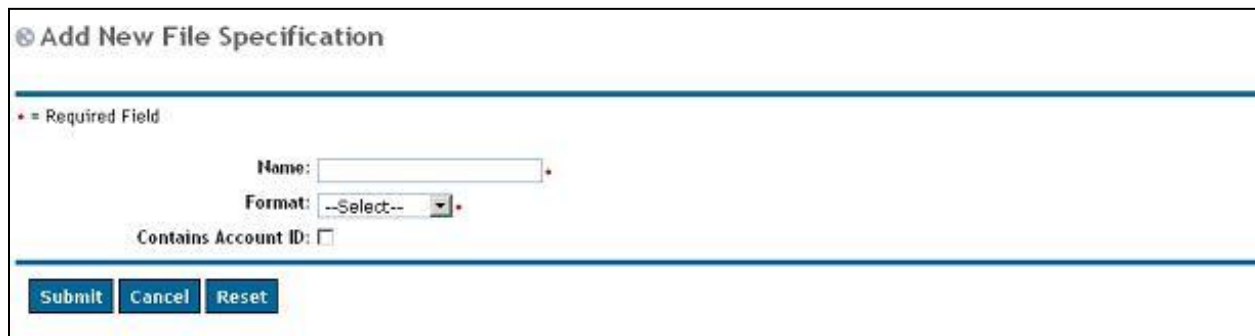
➢ **NOTE:** The users added on this screen are specific users to the child institution, not a user at the parent institution. Enter the institution and users through these screens if you are screening for multiple institutions. If you are only screening for a single institution, use the Add User/Search Users links in the main menu.

4. FILE SPECIFICATIONS

File Specifications can be considered the structure, or file format, of the file to be screened. These can be customized for proprietary data or the standard payment format File Specifications for ACH (and ACH-IAT), Fedwire, and SWIFT can be purchased from Accuity. For more information contact your Account Manager or ComplianceLinkInfo@Accuity.com.
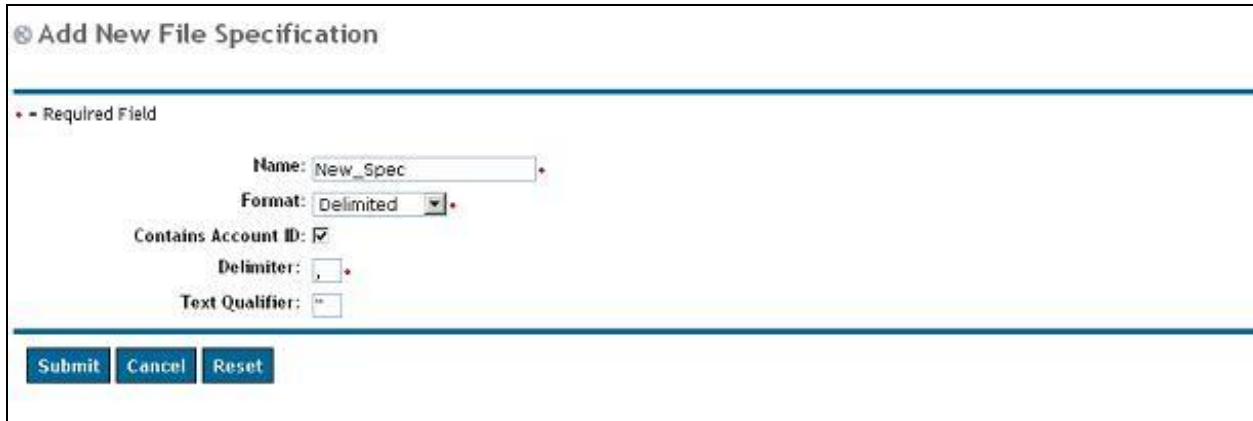
Create a New File Specification

1. Click on the **Add Specification** link in the Compliance Link sidebar.

2. Enter the **Name** of the File Specification.

3. Select the **Format** of your file (e.g. **Fixed Width**, **Delimited**).

   ➢ **NOTE:** If you are attempting to screen standard formatted transaction files consisting of ACH (including IATs), Fedwire, or SWIFT transactions, a File Specification for such file formats in embedded within Compliance Link. If the standard payment format File Specifications do not appear in the File Specification drop-down, your version of Compliance Link does not have the payments module activated. To enable transaction screening, please contact your account representative or email Support@Accuity.com.

4. If your file is delimited, enter the **Delimiter** and **Text Qualifier** for your file in the boxes provided.

5. Click on the **Save** button to create a new File Specification. To reset the data and begin the process with blank fields, without saving, click on **Reset**. To cancel what you have entered without saving, click on **Cancel**.

   ➢ **NOTE:** If your file includes records for multiple institutions and you have included the account IDs/numbers in your file, click on the **Contains Account ID** field. You cannot add or remove the Account ID field once you have created a new File Specification. If you need to add the Account ID field, create a new File Specification and click the **Contains Account ID** field before submitting the File Specification. On the next screen, you will need to indicate which field you have

added that contains the account number. If you need to delete the Account ID field, you must delete the specification, restart the process and deselect the **Contains Account ID** field before creating the File Specification.

1. Enter the field **Name**.

2. Enter a **Sort Order** to indicate the order in which the fields appear in your input file.

3. Choose whether the field is a **Screening Field**.

4. Choose whether the field is a **Unique Field**.

5. Choose the **Data Type** from the dropdown list. If no data types match the expected input data, choose **Unspecified**.

➢ NOTE: For Commodity Screening, use the Commodity Name, Commodity Routing and Commodity Country fields. Commodity Name is used for fields that will contain commodity information or descriptions. Commodity Routing is used for fields that will contain station or routing codes (i.e. ORD → US) that are mapped to ISO Country Codes using the routing mapping file. Commodity Country is used when the field contains country information instead of station codes (i.e. DE, Germany, and Deutschland). Whenever any fields in a File Specification are marked as Commodity Type data, the Commodity Screening Engine will be invoked during screening. Normal GWL/PEP Screening and Commodity Screening can be used simultaneously.

6. Click **Save**.

7. Repeat Steps 1–6 for all of the fields in your input file.

A single field must be selected as the Unique ID. A Unique ID is a value unique to that record and not duplicated elsewhere in the file. The Unique ID is used in the Good File to identify a record that has been previously screened.

Multiple fields can be selected (at least one must be selected) as Screening Fields.

These fields are used with the Screening Fields Only screening option. When the option is selected only "screening fields" will be filtered against the Global WatchList but all fields will be written to the match database. This feature can be very useful if your screening file contains data that does not need to be matched against the Global WatchList (i.e. department names, addresses, postal codes).

If Compliance Link is running in Multiprocessor Mode (Service Bureau), you must have at least one field that is indicated as an Account ID (if Account ID Field = Yes). The Account ID is used to distribute matches to more than one Compliance Link account from a single batch.

Field Name and Sort Order are required for each field. You cannot use the same Field Name or Sort Order for multiple fields. If you need to make a change to a field after clicking on Save, click on the Edit button at the top of the page and you will be able to choose a field to update.

To remove an existing specification click on the Delete button at the top of the page and the entire specification will be deleted. File Specifications can only be deleted if no batches are associated with the File Specification.

> **NOTE:** You must not assign the same field as Unique ID <u>AND</u> Account ID. They must be two separate fields in your file with different data.

Modify Field List for Demo

					Edit	Delete

Format: Delimited   **Delimiter:** ,
Text Qualifier: "   **Account ID Field:** No

• = Required Field
One Unique Field and at least one Screening Field is required.

Field Name	Sort Order	Screening Field	Unique Field	Data Type	
ID	1	X	X	Customer Unique ID	Edit
Name	2	X		Name - People	Edit
Company	3	X		Name - General	Edit
Address	4	X		Unspecified	Edit
City	5			Unspecified	Edit
State	6	X		Unspecified	Edit
Country	7	X		Country Name	Edit
Filler	8			Unspecified	Edit
Code	9			Unspecified	Edit
_____ •	10 •	☐	☐	Unspecified ▾	Save Reset

Example:
" ID " , " Name " , " Company " , " Address " , " City " , " State " , " Country " , " Filler " , " Code " , " "

If your file is fixed width, you will not be asked for the Delimiter and Text Qualifier but will be taken directly to the following screen to enter the specifics about the fields. You will need to enter the Field Name, the Start Position, the Field Length and Data Type for each field. You cannot use the same Field Name for multiple fields. Indicate one field as the unique identifier and any other fields that are "screening fields".

> ➢ **NOTE:** Fields are truncated after 4,000 bytes.

Modify an Existing File Specification

1. Click on the **Modify File Specification** link in the sidebar.

2. Choose the file you wish to modify from the drop down list of existing File Specifications.

3. Click on **Submit**.

4. Click on the **Edit** link next to the field you wish to update.

   ➢ **NOTE:**   You can see the format type and, if delimited, the delimiter and text qualifier for each File Specification. If you wish to change the delimiter and/or text qualifier, click on the **Edit** button at the top of the page. Remember that you cannot change the option "Contains Account ID". If you wish to delete the entire File Specification, click on the **Delete** button at the top of the page.

   ➢ **NOTE:**   If a File Specification was used for an existing batch, you will not be able to delete it until all batches for the File Specification have been deleted first.

Once you click on **Edit** next to an existing field, in addition to being able to update the data for that field, you can also click on the **Delete** button to the right of the field to delete the field entirely.

5. BATCH QUEUE

You can check the status of all batches on the Batch Filter Process Log/Queue screen. Only users with the Batch Maintenance feature set have this option. Click on the Batch Queue link. You will see the last completed batch, and then any batches that are currently running, failed (within the last week), ran successfully on the current day, or in line to be run. You will see Not Displayed for the File Name and User ID if the batch was submitted by a user at another account. You will also see a note at the bottom of the screen that tells you when the last batch was run, and when the next one is scheduled to start.

If a batch fails, you will see a status of "Error", and you will receive a failure email. Possible causes of an error could be that the File Specification does not match the uploaded file's format, or the file name is too long, or the file was improperly compressed (zipped), or too many error records exist. Another possible cause, though rare, of a batch failure is a server issue. Please try again and if it still fails, email Support@Accuity.com.

⊗ Batch Filter Process Log/Queue

Batch ID	User ID	File Name	Screen Date	Status
7036	ProductDemo	IATfile.txt		Waiting
7035	ProductDemo	OFAC.csv		Waiting

Last batch ran at 2008-11-04 09:59:56.0
Next batch scheduled to run at 2008-11-04 10:00:56.0

6. MANAGE LISTS

Compliance Link is driven by Accuity's Global WatchList (GWL) data which provides Compliance Link users the most comprehensive sanctions and enhanced due diligence database. Updates to specific lists within GWL are often random and frequent, making it ever important to be confident that screening is being performed against the most up-to-date lists. Compliance Link provides the ability to show a full history of all updates to all lists by using the Search Global WatchList History page.

Additionally, there may be a need for screening against lists that are not a part of Accuity's GWL database. These may be lists that are internal and specific to each and every customer. The Manage Lists screen is used for uploading these types of private watch lists created using Accuity's Private File Creator (PFC) or Private List Manager (PLM), or commodity watch lists (CWL) created by the Commodity List Manager (CLM). For more information regarding Private List Screening please contact ComplianceLinkInfo@Accuity.com. For more information regarding Commodity Screening please contact ComplianceLinkInfo@Accuity.com.

6.1. Global WatchList History

The Global WatchList History screen shows all historical updates to all of the lists within the institution or the account. This includes when the update occurred and how many additions, changes, and deletes were a part of the update. This is useful to ensure that the lists are being updated in a timely manner and screening is being performed against the most up-to-date lists.

Search Global WatchList History

1. Click on the **Manage Lists** link in the sidebar.

2. Click on **Search Global WatchList History**.

3. Choose the search criteria.

   a. **List Name** – All Global WatchList and private watch lists assigned to the account.

   b. **Uploaded To/From** – Date when the watch list was uploaded to Compliance Link.

4. Click on **Search**.

5. Click on **Export CSV** to export an electronic report of watch list updates. (Optional)

6.2. Manage Private Watch Lists

Private watch lists are created using Accuity's Private File Creator, Accuity's Private List Manager, or Accuity's Commodity List Manager and should be in MLGWLXML.zip, MLUPIDGWL.zip or MLCWLXML.zip format when being loaded into Compliance Link. Once uploaded, these lists are automatically assigned to your account and can be used for screening immediately.

Watch lists uploaded to the account can be updated or inactivated at any time.

6.2.1. Upload/Update Private or Commodity Watch Lists

Upload/Update Private Watch List Data

1. Click on the **Manage Lists** link in the sidebar.

2. Click on **Update Private List Data**.

3. Browse for the **MLGWLXML.zip**, **MLUPIDGWL.zip** or **MLCWLXML.zip** file.

4. Click **Save** to upload/update the private watch list.

Clicking on the **Reset** button will clear all fields. Clicking on the **Cancel** button returns you to the Manage Lists screen without editing the folder.

6.2.2. Inactivate Private or Commodity Watch Lists

Inactivate a Private Watch List

1. Click on the **Manage Lists** link in the sidebar.

2. Click on the List Name.

3. Change the **Status** dropdown.

4. Click **Save** to change the status.

7. MANAGE SCREENING OPTIONS

The Manage Screening Options screen is the screen from which you can manage Screening Profiles, Risk Scorecards, Character Mapping files and Synonym Dictionaries.

7.1. Screening Profiles

Screening Profiles are used to simplify the day-to-day job of screening batches in Compliance Link. They determine the settings/configurations that are used during the screening process which include but are not limited to screening algorithms, Risk Scorecard used, and Global WatchList files. Once you have set up and save a screening profile you, or your users, can reuse it in subsequent screenings.

Add a New Screening Profile

1. Click on **Manage Screening Options** from the sidebar.

2. Click on **Manage Screening Profiles**.

3. Click on **Add New Screening Profile**.

ACCUITY

1. Enter the **Screening Profile Name**.

2. Choose which of the **Screening Algorithms** to use.

   a. **Accuity Token** – Accuity Token is the standard matching algorithm built around Stop Descriptors, Accuity's Synonym Table, and Token-based matching. Accuity Token is used for every screening and cannot be deselected.

b. **Fuzzy Logic** – Fuzzy Logic is based on the Edit Distance algorithm (or Levenshtein Distance algorithm) which, using Stop Descriptors, can address many common misspellings and typos such as insertion, deletion, transposition and substitution.

c. **Soundex** – A phonetic algorithm that indexes names by sound and matches them against Soundex encoded Stop Descriptors. (Only used for Latin-based screening)

d. **Metaphone** – A phonetic algorithm that encodes input names with varying lengths by their English pronunciation. These encodings are compared to encoded Stop Descriptors. (Only used for Latin-based screening)

e. **Double Metaphone** – Second generation of Metaphone phonetic algorithm. (Only used for Latin-based screening)

3. Choose a **Risk Scorecard**. For more information about Risk Scorecards please refer to the **Risk Scorecard** section of this **Administrator Guide**. If no Risk Scorecard is selected then no Risk Scoring will be performed.

4. Choose a **False Positive Reduction Rules Pack**.

5. Choose a **Controlled Goods Policy**. This option requires the Controlled Goods Manager application.

6. Select or deselect the use of **Good File**.

7. Check **Screen against Add/Change Lists only** to perform Delta Screening.

➢ **NOTE:** Delta Screening will only screen against the most recent update of the watch lists selected. It is important to understand the implications of Delta Screening as they fit within your Compliance procedures. Generally, Delta Screening is performed against a master data file each time the watch lists are updated. For more information regarding Delta Screening please contact ComplianceLinkInfo@Accuity.com.

8. Select from the following **Screening Options**:

a. **Match on Screening Fields Only** – This option will only filter fields that have been identified as screening fields in the File Specification. All fields (screening fields and "non" screening fields) in a matched record will be written to the Compliance Link match database.

b. **Remove Middle-Initial** – This option will remove the middle initial before filtering to reduce false positive matches. Only screening fields will be affected. The text must be in the format of Firstname [middle initial] Lastname or Lastname, Firstname [middle initial].

c. **Ignore Vessels** – This option will ignore any match where the entity type is Vessel.

9. Choose a **Character Mapping File**.

10. Choose a **Custom Dictionary**.

11. Pick at least one Global WatchList against which the file should be screened.

12. Click on **Save** to save the new Screening Profile.

Edit an Existing Screening Profile

1. Click on **Manage Screening Options** from the sidebar.

2. Click on the Screening Profile name to edit.

3. Make necessary changes to the Screening Profile.

4. Click on **Update**.

Delete an Existing Screening Profile

1. Click on **Manage Screening Options** from the sidebar.

2. Click on **Manage Screening Profiles** button.

3. Click on **Delete** to delete a specific Screening Profile.

7.2. Risk Scorecards

Compliance Link can produce a Risk Score for each match generated through the screening process. Risk Scores are based on Risk Scorecards which evaluate and risk rate additional data elements involved in a match. Compliance Link compares additional data elements involved with the match and based on those elements' similarities/differences produces a highly-tunable score that represents the likelihood of a match being either "true" or "false positive".

Compliance Link's Screening Engine uses Stop Descriptors to determine matches and there are instances where a single Stop Descriptor will have many entities associated with it. Once a "match" is found using the Screening Engine, each entity associated with the match is run through the Risk Scoring Engine, using Risk Scorecards.

Compliance Link is delivered with three default, or standard, Scoring Components.

- **Full Name Comparison** – Compares the Input Record's name to each name associated with the matched GWL entity (i.e. Entity Name, Alias, AKA) using language-specific rules.

    - Uses the Edit Distance, or Levenshtein, algorithm to calculate a score on the similarities for all name parts. For example, an input name "Robert John Duffy" compared to "Robert David Duffy" would return a score of $11/16 = 0.6875$.

◆ This scoring component will compare all tokens (words) from both the input record marked as a Name field and all tokens in the entity name fields on Accuity's Global WatchList. When the amount of tokens differ between Input Record Name and GWL Entity Name, the scoring component will always produce a score based on the element with the least amount of tokens. In the below example the first two rows produce a score of 100% because all of the Input Record Name's tokens appear in the GWL Entity Name's tokens.

INPUT RECORD NAME	GWL ENTITY NAME	RISK SCORE
Robert Duffy	Robert John Duffy	1.0 (100%)
Robert Duffy	Robert John D. Duffy	1.0 (100%)
Mr. Robert John Duffy	Robert John Duffy	1.0 (100%)
Mr. Robert David Duffy	Robert John Duffy	0.6875 (~69%)

- **Year of Birth Comparison** – Compares the Input Record's Year of Birth (YOB) to each YOB associated with the matched GWL entity (i.e. DOB, alternate DOB).

  ◆ Default values are:

    ▪ Exact match = 1.0 (100%)

    ▪ +/- 1 year = 0.75 (75%)

    ▪ +/- 2 years = 0.5 (50%)

    ▪ Over 2 years = 0.0 (0%)

- **Associated Country Comparison** – Compares the Input Record's Associated Country (ISO Country Code or Country Name) to each country associated with the matched GWL entity (i.e. Country, Nationality, Citizenship)

Additional Scoring Components can be customized by Accuity's Professional Services Group (PSG). For more information please contact your Account Manager or Support@Accuity.com.

Create a New Risk Scorecard

1. Click on **Manage Screening Options** from the sidebar.

2. Click on **Manage Risk Scorecards**.

ACCUITY

3. Click on **Add New Risk Scorecard**.

4. Enter the name for the Risk Scorecard.

5. Choose which Scoring Components to use for this Risk Scorecard by checking the boxes in the Select column.

6. Assign a Weight (1-9) for each Scoring Component selected.

➢ **NOTE:** These weights are relative to the highest weight assigned to a scoring component: If the highest value for any component is "4", a weight of "2" for another component will be 50% as impactful and "1" will be 25% as impactful. If the highest value for any component is "10", a weight of "2" for another component will be 20% as impactful and "1" will be 10% as impactful.

7. Click on **Save**.

➢ **NOTE:** For audit trail purposes, Risk Scorecards cannot be deleted or modified after they have been created. Risk Scorecards can be inactivated from the Manage Risk Scorecards screen.

7.3. Character Mapping Files

Character Mapping is an advanced feature of Compliance Link that allows users to screen certain characters that normally do not appear in watch lists. Most watch lists do not include "high ASCII characters" or letters with diacritical marks (such as #, %, ü). If your input data contains these characters you may need to use a Character Mapping file.

Compliance Link will make certain that (if activated on screening instructions) Character mapping takes place when the input data is uploaded. The Character Mapping take place before Screening, before False Positive Rules and before Risk Scoring.

The character mapping file must be in .XML format with the following schema:

```
<charmap>
  <asciiset>
    <ascii id="1" filtermap=" "/)
    <ascii id="2" filtermap=" "/)
  </asciiset>
</charmap>
```

Accuity provides a standard character mapping file as part of the download package, but you are able to upload as many additional character mapping files as necessary.

> ➢ **NOTE:** The character mapping file is only used when screening against Latin-based data. Any input data that is identified as Cyrillic, Chinese, and/or Japanese will not be mapped and will be screened against the Cyrillic, Chinese, and/or Japanese watch list data when available.

> ➢ **NOTE:** The default Character Mapping file considers 255 control, printable and extended ASCII characters. The extended ASCII characters are mapped mainly to spaces in the default file. Please ensure that you know what types of characters you have in your input data and to make any applicable changes in the Character Mapping file.

Upload a New Character Mapping File

1. Click on **Manage Screening Options** from the sidebar.

2. Click on **Manage Character Mapping Files**.

3. Choose a file, in proper XML format, by clicking on **Browse**.

4. Name the Character Mapping File.

5. Click on **Upload New File**.

Inactivate a Character Mapping File
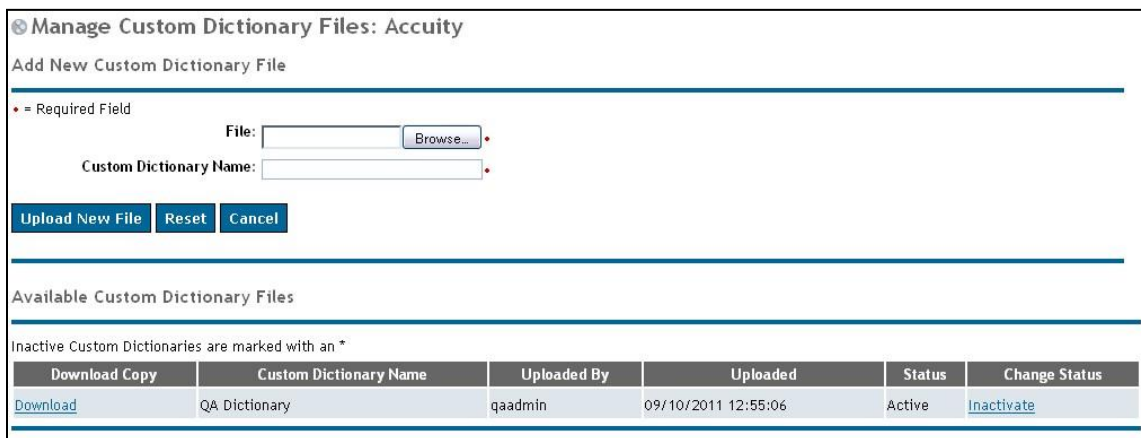
1. Click on **Manage Screening Options** from the sidebar.

2. Click on **Manage Character Mapping Files**.

3. Click on **Inactivate** from the **Change Status** column. The page will reload and the Status will be updated.

7.4. Custom Dictionaries

Custom Dictionaries, or Synonyms tables, are used to accommodate and match on different spellings or transliterations of common words. Accuity manages a synonyms table that accounts for misspellings, transliterations, nicknames, etc. Compliance Link will always use the Accuity Dictionaries as these are built into the Accuity Global WatchList data files. However, each customer can also upload and use their own dictionaries in conjunction with the Accuity synonyms.

Upload a New Custom Dictionary

1. Click on **Manage Screening Options** from the sidebar.

2. Click on **Manage Custom Dictionaries**.

3. Choose a file, in proper tab-delimited format, by clicking on **Browse**.

   ➢ **NOTE:** The format of the uploaded file should be two columns, tab-delimited, text files. The first column contains the original word and can contain duplicates, while the second column contains the synonym and should not have any duplicates in the file. If Unicode data exists in the Custom Dictionary file, then a header record should be added.

4. Name the Custom Dictionary.

5. Click on **Upload New File**.

Inactivate a Custom Dictionary

1. Click on **Manage Screening Options** from the sidebar.

2. Click on **Manage Custom Dictionaries**.

3. Click on **Inactivate** from the **Change Status** column. The page will reload and the Status will be updated.

8. BATCH MAINTENANCE

A common administrative task is maintaining the batches of records from your screened files. You can view whether a batch screening has completed by clicking the Batch Maintenance link in the sidebar.

The Batch Maintenance screen can be used to search for specific batches, review batch details, delete batches, and link to Open/Changed records. When the Batch Maintenance screen is opened it will display the last 25 batches by default.

8.1. Searching For Batches

The Batch Maintenance screen allows users with the Batch Maintenance feature set to search through historical screenings for specific batches to analyze.

Search for Batches

1. Click on the **Batch Maintenance** link in the sidebar.

2. Enter the search criteria.

   a. **User ID** – User that performed the screening

   b. **Bank/Account Name** – The Institution Name the batch was screened in (only applies for Service Bureau Mode)

    c. **Batch ID To/From** – Range of Batch IDs

    d. **Screen Date To/From** – Range of dates the batch was screened on

    e. **Most Recent Batches** – Enter a number to view the last "x" batches

    f. **File Specification** – Only return batches screened using a particular File Specification

    g. **Screening Algorithms** – Returns batches where specific screening algorithms (Accuity Token, Fuzzy, Soundex, Metaphone, and Double Metaphone) have been used

    h. **Risk Scorecard** – Returns batches where specific Risk Scorecards have been used.

3. Click on **Search**.

The search results will appear in the same screen.

8.2. Batch Information

Batch Information is displayed on the Batch Maintenance screen in a table format with the following fields:

- **Batch ID** – the identification number for that batch

- **User ID** – the user that performed the screening

- **Dept Name** – the screening user's user group

- **Screen Date** – the date/timestamp the file was screened

- **File Spec: Source** – the File Specification and file name

- **Total Records** – total number of records within the batch

- **Total Matched** – total number of records containing at least one match, click this link to view all records with matches

- **Matched %** – percentage of records containing at least one match

- **Open/Changed** – total number of records containing at least one Open or Changed match

- **Status** – the current status of the batch

- **Bad File** – a downloadable file containing all invalid records

All possible statuses are:

- **Finished** – The batch has screened correctly.

- **Error** – The batch failed for other reasons than listed below. Resubmit the batch, if it still fails, contact your administrator.

- **Processing** – The batch is currently being processed.

- **Starting** – Batch information is compiling before the screening of records starts.

- **Unzipping** – The file you submitted was a compressed zip file, and the system is in process of unzipping it in order to begin screening.

- **Waiting** – The batch is waiting **1)** for the system to begin screening your file or **2)** for the system to finish screening a different batch (See Batch Queue if you receive this status).

8.3. Deleting Batches

You can delete a batch by clicking on the ✖ next to the Batch ID.

➢ **NOTE:** Deleting the batch will also remove it from the dropdown lists from Match Review Search and Case Review Search. Remain on the Batch Maintenance screen until the deletion is complete. Leaving the Batch Maintenance screen may cause the batch to not be deleted.

8.4. View Batch Detail

From the Batch Maintenance screen, you can click on the **Batch ID** to see the details of the original screening, such as the file that was screened, the File Specification used, the number of records in the file, when the batch completed, and the number of hits.

⊛ **Batch Details**

Batch ID:	1001
User ID:	test
Department:	Temporary Master User
Uploaded:	2011-09-09 13:07:54.0
Screen Date:	2011-09-09 13:10:08.0
File Specification:	Test
Original Filename:	Test1.txt
Screening Algorithms:	Accuity Token
Risk Scorecard:	None
Compliance Link Options:	Use False Positive Reduction Rules: Yes
	Use Good File: Yes
Screening Options:	Match on Screening Fields only: Yes
	Ignore Vessels: No
	Remove Middle Initial: No
Custom Dictionary:	None
Character Mapping File:	Default
Filter Versions:	Accuity's OFAC List: 20110908134212
	Accuity OFAC Enhancements: 20110830131302
Filter Results:	Total Records in File: 7
	Records with Matches: 4
	Records Marked As True Match (Blocked):0
	Records Marked as CHANGED: 0
	Records Marked As False Positive (Good): 0
	Records Marked As OPEN: 4
	Total Invalid Records: 0

Back to Batch Maintenance

If your institution allows Screening File downloads then a link to download the original file will be provided.

You can return to the Batch Maintenance screen by clicking on the **Back to Batch Maintenance** button. If there were any failed records, you will see a "Download" link. Click on the link to download the file of invalid records and examine the file to detect the cause of the error(s).

On occasion, a file does not match the File Specification under which it was processed. This can happen **1)** if the input file was created manually, **2)** if there is something unusual about the data in the input file such as embedded control characters, **3)** if the number of fields does not match the File Specification, or 4) an incorrect File Specification was chosen.

Before Compliance Link processes a record in an input file or "Batch", the record is verified against the file structure, and the unique ID and name fields are identified. If there is an error in this verification process, Compliance Link will remove the record and place it into a "bad file" which is associated with the batch. An administrator can download the bad file either from the Batch Maintenance by clicking on the Download link, or from the Batch Details screen by clicking on the Download link. Once downloaded the file should be examined and compared to the File Specification. In some cases, the rejected records can be repaired and resubmitted, in others the entire file may need to be rescreened.

> ➢ **NOTE:**   If the delimiter used in your File Specification differs from the delimiter used in your Input File, all records will be considered "bad" and will not be screened.

8.5. Batch Reporting

At any time administrators can report on historical batches by clicking on the **Export CSV** button. This will download a comma-separated values file containing the batch information.

9. FALSE POSITIVE REDUCTION RULES

9.1. Introduction

The matching engine used in Compliance Link is designed to find matches between two sets of data and as a result may find "close" or "false positive" matches. A false positive is a match generated by the Filter that, after further review, is determined to not be the entity on the Global WatchList. The goal in watch list matching should be to keep the rate of false positives low without unduly increasing the risk of missing a true match.

Some recurring false positives contain recognizable patterns. Once identified these patterns can help to eliminate or reduce false positive rates. For example, the Albanian National Army was added to the OFAC list, as an organization, in 2001. It is also referred to by the aliases ANA and AKSH. "ANA" causes false positive matches when phrases like the city "Santa Ana" or the name "Ana Maria" are screened. In these cases a rule could be created that ignores matches on ANA when one of these patterns is present.

In addition, data within the match itself can be used to remove false positives. For example, a rule could be created to exclude any matches that occur in the field "Name" against a Shipping Vessel (like 'Laura' or 'Huntsville'). Or, a rule could exclude matches in the "City" field when the match is from the EU list or the UN list.

9.2. Manage Rules

To manage False Positive Reduction Rules click the Manage Rules link from the sidebar. The system will then display the Manage False Positive Reduction Rules screen. Initially, it will show the first 20 active rules. An example of the Manage False Positive Reduction Rules screen is shown below.

Along with Rule ID, which is automatically assigned by Compliance Link each time a rule is added, the following fields are displayed:

- **Stop Descriptor** – The phrase that caused the match; an asterisk "*****" signifies that the rule will be applied to matches on any stop descriptor.

- **Match Parameters** – This includes the Matched Field, the Match Type (GWL/PEP), and Match Score (or Stop Descriptor score).

- **Rule Clause** – A summary of all the clauses that make up the rule.

ACCUITY

Manage False Positive Reduction Rules

ID	Stop Descriptor	Match Parameters	Rule Clause
1	SANCHEZ LAURA	Matched Field: ANY	When "Name" Contains "Laura M Sanchez"

Rules 1 to 1 of 1 Total Rules

Add Rule | **View All Rules** | **Export Rules** | **Import Rules** | **Search Rules**

9.3. Add a False Positive Reduction Rule

Add a new False Positive Reduction Rule

1. Click on the **Manage Rules** link in the sidebar.

2. Click on the **Add Rule** button.

Add False Positive Reduction Rule

Cancel

• = Required Field

Stop Descriptor: [*] • (* = any Stop Descriptor)

Matched Field: [ANY]   **Match Type:** [ANY ▾]

Match Score is less than or equal to: [   ] % (Max 99%)

Update This Clause   **Reset**

Select one of the following clauses. Required fields within the selected clause are marked with •

Clauses Based on Entity Data

⦿ Entity Type [Is ▾] [-- Select -- ▾] •

◯ Source Code [Is ▾] [   ] •

◯ Risk Score is less than or equal to: [   ] • % (Max 99%)

◯ Entity Field [Entity Name ▾] [Contains ▾] [   ] •

Clauses Based on Customer Data

◯ Input Record Field [   ] • [Contains ▾] [   ] •

◯ [   ] • [Occurs ▾] in Field [   ] •

◯ [   ] • [Occurs ▾] [Within ▾] [   ] • words of [   ] • in Field [   ] •

◯ [   ] • [Occurs ▾] [▾] [   ] words of [   ] in Instance [   ] of Field
[   ] •

Add Selected Clause   **Reset**

3. In the **Stop Descriptor** field, enter the Stop Descriptor to which the False Positive Reduction Rule will apply. An asterisk "*****" will cause the rule to apply to any and all Stop Descriptors.

4. In the **Matched Field** field, enter the name of the field in which the Stop Descriptor must be found in order for the rule to apply. Entering the word "ANY" will cause the rule to apply to all data fields.

5. In the **Match Type** field, choose GWL, PEP, CWL or ANY. The False Positive Reduction Rule will only apply to those types of matches.

6. In the **Match Score** field, set the threshold for the Match Score for the rule to apply to. This is the fuzzy score calculated by the filter.

   ➢ **NOTE:** All rules fields are case sensitive; therefore the False Positive Reduction Rule will only apply if these values match exactly ("Name" and "name" are not the same because of the capital "N").

7. Click on the **Update This Clause** button.

You have just created the base for your False Positive Reduction Rule, but your new rule will have no effect, and cannot be saved, until you add a clause to your rule. There are 8 different types of clauses that you can add to your rule and every rule can have up to ten different clauses.

Clauses Based on Entity Data

- Entity Type Clause

- Source Code Clause

- Risk Score Clause

- Entity Field Clause

Clauses Based on Customer Data
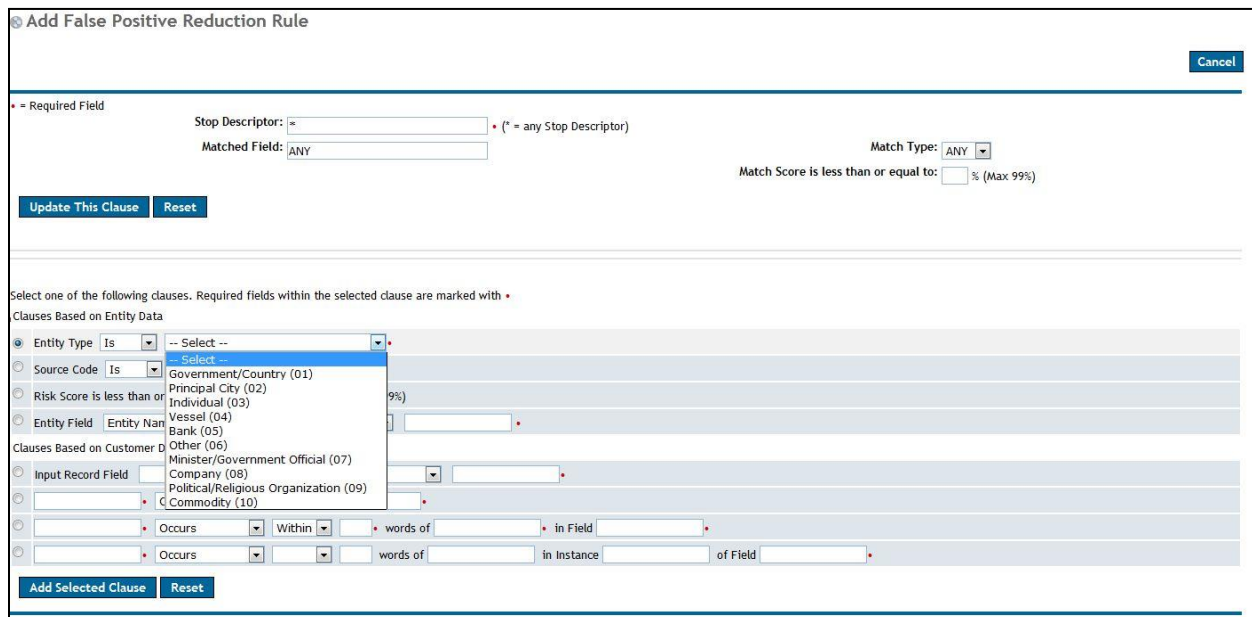
- Input String Clause

- Basic Text Clause

- Intermediate Text Clause

- Complex Text Clause

9.3.1. Entity Type Clause

Entity types are the categories that describe the people, places and organizations on the Global WatchList. They include: Governments, Cities, Individuals, Shipping Vessels, Companies, Banks, Government Officials, Political and Religious Organizations.
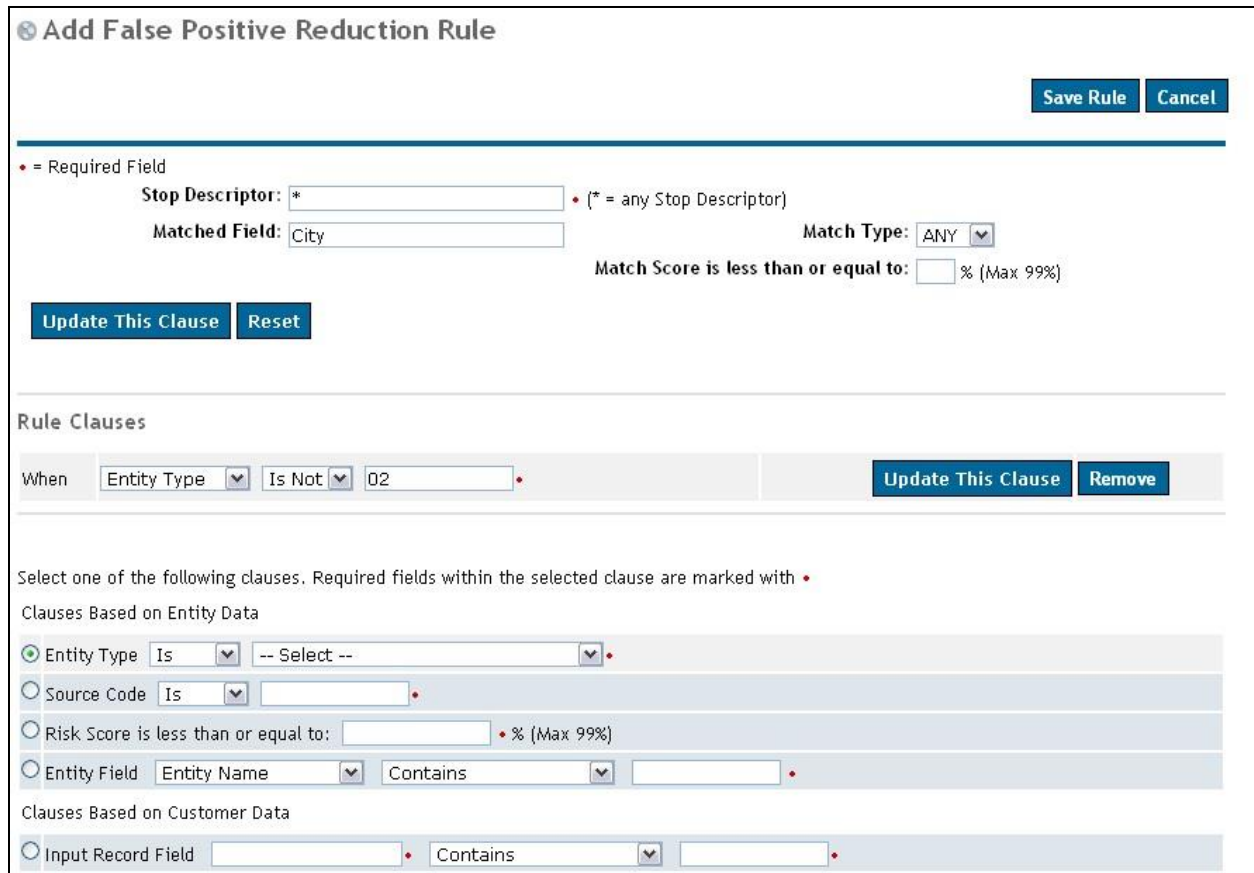
Add an Entity Type Clause

1. Select the button ⦿ next to the **Entity Type** clause.

2. Choose **Is** or **Is Not** from the first dropdown list.

3. Choose an **Entity Type** from the final dropdown list.

4. Click on **Add Selected Clause** button to save the clause.

5. Click on **Save Rule** to save the rule.

Only click the **Reset** button, before clicking **Add Selected Clause**, if you wish to clear all fields and start again.

ACCUITY

As we can see in the image above, this rule will ignore the all matches in the City field when the matched entity is not of type "02" or Principle City.

Also take note that after you have added your first rule clause, you now have the ability to save your rule. Click on the **Save Rule** button at the top of the page. Clicking the **Cancel** button before clicking the **Save Rule** button will remove the rule and return you to the Manage Rules screen. Once a Rule has been saved it cannot be removed but it can be inactivated.

9.3.2. Source Code Clause

Source Codes identify the watch list or sublist from which the match originated. The Accuity OFAC and OFAC Enhancement files include the following sources: UST (U.S. Treasury), OGO (Government Officials), RBL (Restricted or Blocked Locations), TFP (Accuity Research) and WBD (World Bank Directory). If you receive multiple watch lists within your Global WatchList file, each watch list will be referenced by its own source code.

Create a Source Code Clause

1. Select the button ⦿ next to **Source Code**.

2. Choose **Is** or **Is Not** from the dropdown list.

ACCUITY

3. Enter the proper **Source Code** in the input field.

> **NOTE:** The Source Code for a Global WatchList can be found in the Entities field from the Match Review screen. It is the 2-5 alphanumeric code found after the Entity ID Number.

4. Click on **Add Selected Clause** to add this clause to your rule.

5. Click on **Save Rule** to save your rule.

Only click the **Reset** button, before clicking **Add Selected Clause**, if you wish to clear all fields and start again.

9.3.3. Risk Score Clause

Risk Score Clauses are used to pass matches that are below an established Risk Score threshold. The Risk Score is calculated based on the Risk Scorecard used for screening and looks at each entity associated with a Stop Descriptor match.

Create a Risk Score Clause

1. Select the button ⊙ next to **Risk Score**.

2. Enter the **Risk Score** threshold (Max 99%).

3. Click on **Add Selected Clause**.

4. Click on **Save Rule** to save your rule.

Only click the **Reset** button, before clicking **Add Selected Clause**, if you wish to clear all fields and start again.

9.3.4. Entity Field Clause

Entity Field Clauses allow you to create False Positive Reduction Rules based on specific fields within Accuity's Global WatchList data. Additionally, these clauses allow for the use of a number of different operators and conditions.

Entity Field Clauses use the entire data string that is entered and can contain more than a single token, which is different from Simple, Intermediate, and Complex Text Clauses. For more information on these clauses please refer to later segments in this section.

Entity Field Clause rules can be used to eliminate matches that are considered low priority by using PEP Level (International, National, State, Local) and PEP SubCategory. This is sometimes referred to as Micro-categorization.

<u>Create an Entity Field Clause</u>

1. Select the button ⊙ next to **Entity Field**.

2. Choose the **Entity Field** from the dropdown.

    a. **Entity Name**

    b. **Associated Country**

    c. **Entity DOB**

    d. **PEP Level**

    e. **PEP SubCategory**

3. Choose the operator.

    ➢ **NOTE:**   The operators, "Contains Any of (IN)" and "Contains None of (IN)", compare multiple words separated by a comma.

4. Enter the text that is used with the operator in the chosen Entity Field.

> **NOTE:** The above False Positive Reduction Rule will eliminate all matches that are caused by Local-level Politically Exposed Persons from the United States. This is only one example of a False Positive Reduction Rule using Entity Field clauses.

9.3.5. Input String Clause

Input String Clauses allow you to create False Positive Reduction Rules based on specific fields within your proprietary data. Additionally, these clauses allow for the use of a number of different operators and conditions.

Input String Clauses use the entire data string that is entered and can contain more than a single token, different than Simple, Intermediate, and Complex Text Clauses. For more information on these clauses please refer to later segments in this section.

Create an Input String Clause

1. Select the button ⊙ next to Input Record Field.

2. Enter the **Input Record Field**.

   > **NOTE:** Input Record Field entries are case-sensitive. Use "ANY" to indicate any field within the input record.

3. Choose the operator.

> ➢ **NOTE:** The operators, "Contains Any of (IN)" and "Contains None of (IN)", compare multiple words separated by a comma.

4. Enter the text that is used with the operator in the chosen Entity Field.

9.3.6. Simple Text Clause

Simple Text Clauses follow a basic "If-statement". If "Text" occurs (or does not occur) in "X" field. For example, "CUBA" is a Stop Descriptor because the country is on the OFAC Watch List, but Cuba, New York is a city within the United States. The following rule with a simple text clause would prevent false positive matches on "CUBA": Ignore "CUBA" in the "City" field if "New York" occurs in the "State" field.

Create a Simple Text Clause

1. Click on the sixth button ⊙.

2. Enter the text that must occur (or not occur) within the input data.

3. Select **Occurs** or **Does Not Occur**.

4. Enter the name of the field where the text must occur (or not occur).

5. Click on **Add Clause** to add this clause to your rule.

6. Click on **Save Rule** to save your rule.

Only click the **Reset** button, before clicking **Add Selected Clause**, if you wish to clear all fields and start again.

9.3.7. Intermediate Text Clause

The Intermediate Text Clause allows you to search for words in relation to other words. For instance, the "ANA" Stop Descriptor is found on the OFAC list to represent the Albanian National Army. Because of this, any input data containing the Californian city "Santa Ana" will match "ANA". An Intermediate Text Clause could be used to ignore matches to the Stop Descriptor "ANA" when the word "SANTA" occurs within one word of "ANA" in the field "City".

Create an Intermediate Text Clause

ACCUITY

1. Click on the seventh button ⊙.

2. Enter a word in the first text box. In the below case this would be "SANTA".

3. Select **Occurs** or **Does Not Occur**.

4. Choose whether the word must occur (or not occur) Before, After, or Within x amount of words.

5. Enter a number for the amount of words that can separate the two selected words.

6. Enter the second word, in the below case this would be "ANA".

7. Enter the name of the field where the two words must occur (or not occur).

   ➢ **NOTE:** Input Record Field entries are case-sensitive. Use "ANY" to indicate any field within the input record.

8. Click on **Add Clause** to add this clause to your rule.

9. Click on **Save Rule** to save your rule.

Only click the **Reset** button, before clicking **Add Selected Clause**, if you wish to clear all fields and start again.

9.3.8. Complex Text Clause

The Complex Text Clause exists for input records that may contain multiple fields with the same Field Name. Although Compliance Link will not allow the creation of File Specifications with duplicate field names, certain payment messages, like SWIFT messages, permit the use of duplicate field names. The Complex Text Clause allows you to specify which of the multiple instances of a field name you would like added to your rules clause.

Create a Complex Text Clause

1. Click on the last button ⊙.

2. Enter a word in the first text box.

3. Select **Occurs** or **Does Not Occur**.

4. Choose whether the word must occur (or not occur) Before, After, or Within x amount of words. (Optional)

5. Enter a number for the amount of words that can separate the two selected words. (Optional)

6. Enter the second word. (Optional)

7. Enter the instance of the field. For example, if you have three data fields named "{54A}" and you would like this rule to apply to the second instance of "{54A}" you would enter "2". (Optional)

8. Enter the name of the field.

➢ **NOTE:** Input Record Field entries are case-sensitive. Use "ANY" to indicate any field within the input record.

9. Click on **Add Clause** to add this clause to your rule.

10. Click on **Save Rule** to save your rule.

Only click the **Reset** button, before clicking **Add Selected Clause**, if you wish to clear all fields and start again.

9.4. Edit a False Positive Reduction Rule

Edit a False Positive Reduction Rule

1. Click on the **Manage Rules** button in the sidebar.

2. Click on the Rule ID link that you would like to edit.

From the Edit False Positive Reduction Rule screen you can:

- Edit the Stop Descriptor pertaining to the rule.

- Change the Matched Field(s).

- Inactivate the Rule.

- Update Current Clauses.

- Remove Current Clauses.

- Add New Clauses.

9.4.1. Edit the Stop Descriptor

Edit the Input Field Named Stop Descriptor

1. Click on **Update This Clause**.

2. Click on **Save Rule**.

 ➢ NOTE: Entering an asterisk "*****" in this field will allow this rule to apply to all Stop Descriptors.

9.4.2. Change the Matched Field

Edit the Input Field Named Matched Field

1. Click on **Update This Clause**.

2. Click on **Save Rule**.

 ➢ NOTE: Entering "ANY" in this field will allow this rule to apply to all data fields.

9.4.3. Inactivate the Rule

Click on the **Inactivate Rule** button. Inactive rules are not applied during the screening process. If you wish to re-activate an inactive rule, search for and select the rule. (You must search for Inactive records.) Click on the **Reactivate Rule** button.

9.4.4. Update a Clause

Only one clause can be edited at one time. The available clause has an **Update This Clause** button on the same line and to the right. You can change the clause and then click the button to preserve the changes. To select a different clause, click on the **Edit** button to the right of that clause.

9.4.5. Entity/Source Type

1. In the left dropdown, select whether you want a Source Type Clause or Entity Type Clause.

2. Select **Is** or **Is Not** from the second dropdown list.

3. Enter the Entity Type or Source Code text.

4. Click on **Update This Clause**.

5. Click on **Save Rule**.

9.4.6. Text Clause

> **NOTE:** Once a text clause is added to your False Positive Reduction Rule it is formatted into the Complex Text Clause syntax.

You can modify any of the following:

- The word in the first text box.

- OCCURS or DOES NOT OCCUR.

- Before, After, or Within X words of. (Optional).

- The number for how many words can separate the two words. (Optional)

- The second word. (Optional)

- The instance of the field. For example, if you have three data fields named "Name" and you would like this rule to apply to the second instance you would enter "2". (Optional)

- The name of the field.

When you have finished making changes:

1. Click on **Add Clause** to add this clause to your rule.

2. Click on **Save Rule** to save your rule.

9.5. Exporting & Importing Rules

Often times False Positive Reduction Rules may be run through test systems to ensure they work as intended. Therefore Compliance Link offers the ability to Export/Import False Positive Reduction Rules.

9.5.1. Exporting Rules

Compliance Link allows you to export your rules in .xml format.

Export a List of Your Rules

1. Click on the **Manage Rules** button in the sidebar.

ID	Stop Descriptor	Matched Field	Rule Text
20	ANA	City	When "SANTA" occurs within 1 words of "ANA" in field "City"

Rules 1 to 1 of 1 Total Rules

Add Rule | View All Rules | Export Rules | Import Rules | Search Rules

2. Click on the **Export Rules** button.

Your browser's download dialog box will open. You will have the option to **Open** or **Save** the file or to **Cancel** the export.

9.5.2. Importing Rules

Only rules in a properly formatted file with an extension of '.xml' or '.dat' can be imported. All rules must have the correct syntax for the import to be successful. The first rule with an improper syntax will generate an error message that identifies the line in which the error occurred. No rules will be imported if syntax errors exist.

Import a List of Already Created Rules

1. Click on the **Manage Rules** button in the sidebar.

2. Click on the **Import Rules** button.

3. Browse for the .xml or .dat file that you would like to import, by either clicking within the input field or clicking on the Browse button.

4. Choose the proper format, either .xml or .dat, from the dropdown list.

5. If you would like to inactivate all current rules check the box titled **Inactivate All Current Rules**.

6. Click on the **Import** button. If you would like to clear all fields click on the **Reset** button.

   ➢ **NOTE:**   If Inactivate All Current Rules is not selected then the imported rules will be appended to the current rule set. If this option is selected, all existing rules will be made inactive and only the imported rules will be active. If the Import fails, for any reason, the existing rules will not be made inactive regardless if this option is selected or unselected.

9.6. Searching For Rules

Search for False Positive Reduction Rules

1. Access the Search False Positive Reduction Rules screen by clicking on the **Search Rules** button from the sidebar or from the Manage Rules screen.

2. Enter the **Rule ID** that you would like to locate in the Rule ID input field. Leave this input field blank if you would like to search all Rule IDs.

3. Enter the **Stop Descriptor** to which the False Positive Reduction Rule pertains in the Stop Descriptor input field. Leave this input field blank if you would like to search all Stop Descriptors.

4. Enter the **Matched Field** to which the False Positive Reduction Rule pertains in the Matched Field input field. Leave this input field blank if you would like to search any Matched Field.

5. Choose **Active**, **Inactive**, or **All** from the dropdown list.

6. Click on **Search Rules** to search using the given criteria. To go back to the Manage Rules screen without searching click on **Cancel**. To clear all input fields click on **Reset**.

After you execute your search, the Search Results screen will be displayed. If you would like to go back and edit your search criteria click on the link next to Search Criteria. This screen also allows you to create a new False Positive Reduction Rule, to do so click on Add Rule. More detailed instructions on creating new False Positive Reduction Rules are in the **Add a False Positive Reduction Rule** section.
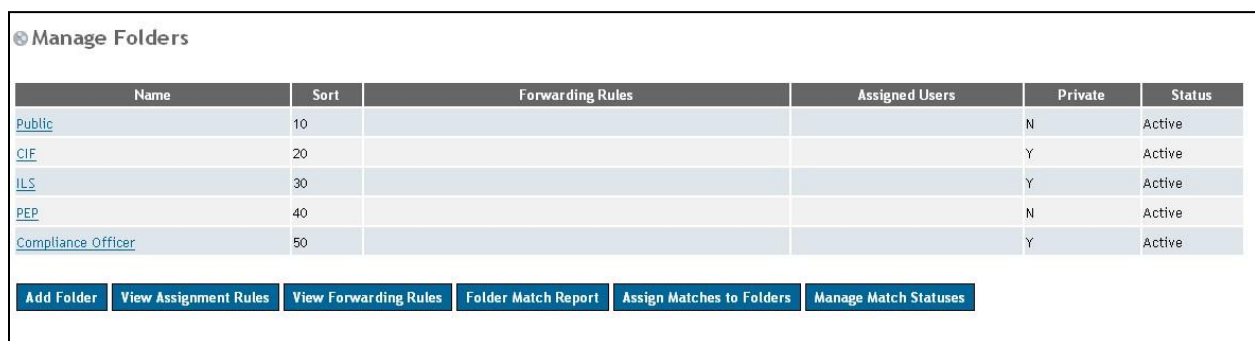
10. CASE MANAGEMENT

10.1. Introduction

Case Management allows users with the Case Management Configuration feature set to create an organizational structure or workflow for their screening processes. It also allows for the creation of Service Level Agreements, SLAs, to ensure that matches are worked in an expeditious manner.

Folders are a means of organizing Matches to help improve a user's ability to efficiently review and assign statuses to matches. Compliance Link is delivered with a default "Public" folder. Other folders can be created and managed only by users who have been assigned the Case Management Configuration feature set.

All of the Folder Management tasks are accessed through the Manage Folders screen. To gain access click on the Manage Folders link from the sidebar. An example of a Manage Folders screen is displayed below. This is the gateway to many of the Folder Management features.

⊛ Manage Folders

Name	Sort	Forwarding Rules	Assigned Users	Private	Status
Public	10			N	Active
CIF	20			Y	Active
ILS	30			Y	Active
PEP	40			N	Active
Compliance Officer	50			Y	Active

| Add Folder | View Assignment Rules | View Forwarding Rules | Folder Match Report | Assign Matches to Folders | Manage Match Statuses |

10.2. Adding New Folders

From the Manage Folders screen you are able to add a new folder. To add a new folder click on the Add Folder button at the bottom of the Manage Folders screen. The Add Folder screen displays, as shown below.

ACCUITY

Add a New Folder

1. Enter the name of the folder in the **Name** field.

2. Enter its **Sort** value. This designates the order in which it will appear on screen. This must be a numeric value.

3. Check the **Private** check box if the folder will be "Private" and only visible to users assigned to it.

4. Enter due the folder's SLA and choose either, Minutes, Hours, or Days. (Optional)

   ➢ **NOTE:** The SLA is the amount of time a match can remain un-worked in the folder before being considered overdue. If it is left blank, matches in the folder will never be considered overdue.

5. Click on the **Save** button to return to the Manage Folders screen. The folder you just created should now be visible.

   ➢ **NOTE:** Clicking on the **Cancel** button returns you to the Manage Folders screen without creating a new folder. Clicking on the **Reset** button clears all fields.

10.3. Editing Folders
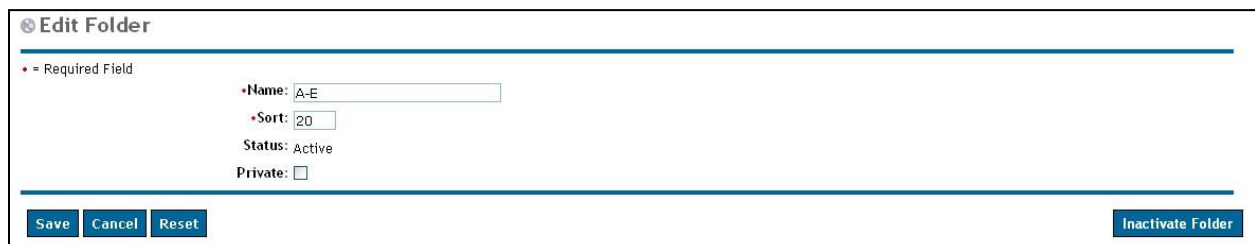
Edit an Existing Folder

1. Click on the **Manage Folders** button on the sidebar.

2. Click on the Folder Name that you would like to edit.

---

3. The Edit Folder screen is divided into four sections separated by a row of four buttons (**Save**, **Cancel**, **Reset**, **Activate Folder** (**Inactivate Folder**)).

   a. Folder Properties section

   b. Forwarding Rules section

   c. Assign Users section

   d. Notification Settings

   ➤ NOTE: The Edit Folder screen contains three sets of the four buttons (**Save**, **Cancel**, **Reset**, **Activate Folder** (**Inactivate Folder**)). All buttons located on this page affect all fields within the page. Clicking on the **Save** button in the top section saves all changes made to all other sections as well. Clicking on the **Reset** button in the top section resets all changes made to all other sections as well. Clicking on the **Cancel** button in any section returns you to the Manage Folders screen without editing the folder.

10.3.1.   Edit Folder Properties

The top section of the Edit Folder screen looks similar to the Add Folder screen containing input fields for Name, Sort, and Private/Public Status, but also displays whether the folder you are currently editing is Active or Inactive. A screenshot of this section is shown below.
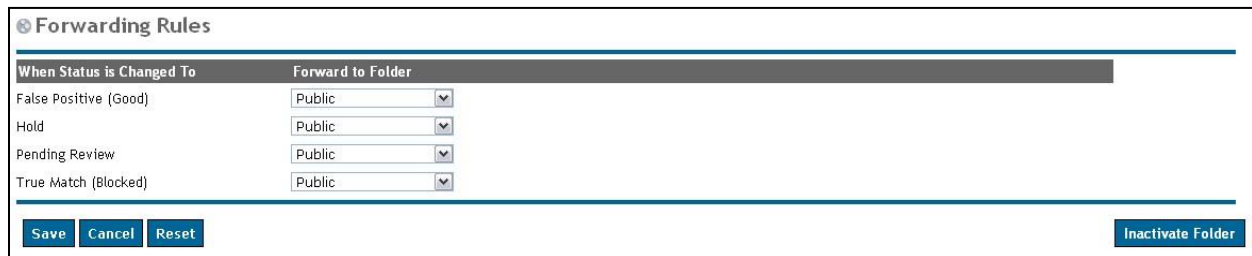
- To alter the name of the folder, change the text within the **Name** field.

- To change the Sort value, edit the value within the **Sort** field.

- Check/Uncheck the **Status** box to declare the folder Private or Public.

- Inactivate the folder by clicking on the **Inactivate Folder** button. A more detailed description of this button can be found later in this section.

Clicking on the **Save** button saves your changes. Clicking on the **Reset** button will clear all fields. Clicking on the **Cancel** button returns you to the Manage Folders screen without editing the folder.

10.3.2.　Edit Forwarding Rules

The second section on the Edit Folder screen is the Forwarding Rules section. Forwarding Rules are useful for moving matches from one folder to another. When a match status is changed by a user, the Forwarding Rules automatically routes the match to a different folder. This section displays all standard user-assignable Match Statuses {False Positive (Good), Hold, Pending Review, and True Match (Blocked)} and any customized Match Statuses along with corresponding Forwarding Rules located on the right side of the screen.

This section allows you to:

- Manage Matches that have not been automatically assigned a Match Status.

- Automatically route matches depending on assigned Match Status.

Select a folder from the "Forward to Folder" dropdown list to choose where the matches with specific Match Statuses are sent.
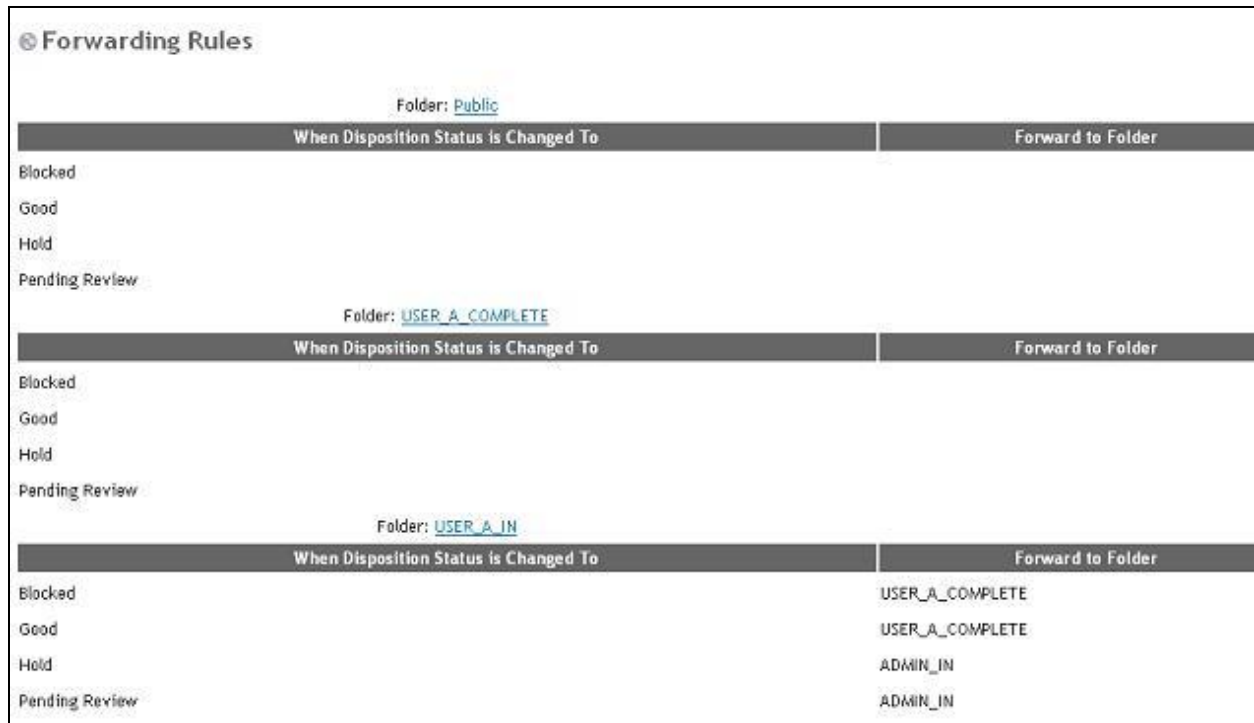
Click the **Save** button to save your selections and return to the Manage Folders screen. Click the **Reset** button to undo the changes to the Edit Folder screen. To return to the Manage Folders screen without editing the folder click the **Cancel** button.

10.3.3.　View Forwarding Rules

View Forwarding Rules

1. Click on the **Manage Folders** button in the sidebar.

2. Click on the **View Forwarding Rules** button.

This leads you to the Forwarding Rules screen shown below.

To edit the Forwarding Rules for a folder, click on any of the folder Names shown. The process by which you edit Forwarding Rules is discussed in the **Editing Forwarding Rules** section.

10.3.4.　　Assign/Un-Assign Users

The third section of the Edit Folder screen is the Assign Users section. The Assign Users section allows the users with the Case Management Configuration feature set to select the users that will be assigned to the selected folder. Two select boxes are located within this section, Available Users and Assigned Users. The Available Users select box displays all users within the system that do not have access to the selected folder. The Assigned Users select box displays all users that have access to the selected folder.

> ➢ **NOTE:**　　If a user has been inactivated they will have an asterisk "*****" in front of their user ID.

Add a Single New User

1. Click on the user ID in the **Available Users** box to be added.

2. Click on the arrow right "**>**" button.

Add Multiple Users

1. Click on multiple user IDs in the **Available Users** box while holding the Ctrl key.

2. Click on the arrow right "**>**" button.

Add All Available Users

1. Click on the double arrow right "**>>**" button.

Remove a Single User

1. Click on the user ID in the **Assigned Users** box.

2. Click on the arrow left "**<**" button.

Remove Multiple Users

1. Click on multiple user IDs in the **Assigned Users** box while holding the Ctrl key.

2. Click on the arrow left "**<**" button.

Remove All Assigned Users

1. Click on the double arrow left "**<<**" button.

Click the **Save** button to save your selections and return to the Manage Folders screen. Click the **Reset** button to undo the changes to the Edit Folder screen. To return to the Manage Folders screen without editing the folder click the **Cancel** button.

10.4. Activating & Inactivating Folders

Inactivate a Folder

1. Click on the **Manage Folders** link in the sidebar.

2. Click on the Folder Name that you wish to inactivate.

    ➢ **NOTE:** Inactivating a folder has implications for many related items such as Forwarding Rules and users for the inactivated folder, Forwarding Rules from

other folders to the inactivated folder, Folder Assignment Rules which reference the folder, and Matches in the inactivated folder.

The Edit Folder screen is divided into four sections separated by a row of four buttons [**Save**, **Cancel**, **Reset**, **Inactivate Folder**]. The button aligned to the right is the **Inactivate Folder** button; if the folder is active this button will display **Inactivate Folder**. You should note that this button appears on the Edit Folder screen three times. All three instances of this button function in the same way.

3. Click on the **Inactivate Folder** button. This takes you to the Inactivate Folder screen.

There are three reasons that the system may prevent a folder from being inactivated:

- Forwarding Rules reference this folder

- Folder Assignment Rules reference this folder

- Matches are contained within the folder

10.4.1.   Forwarding Rules Reference This Folder
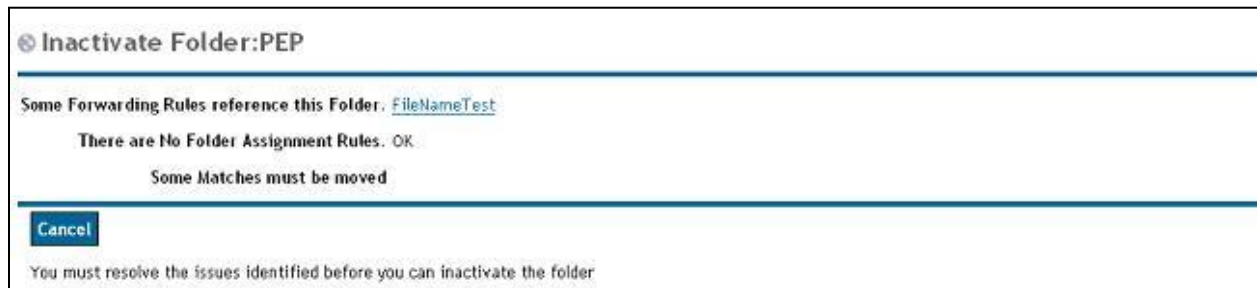
In the example above, the user is attempting to inactivate a folder named "PEP." Forwarding Rules that reference the PEP folder must be removed before the folder can be inactivated.

Edit the Forwarding Rules

1. Click on the link provided to reach the Edit Folder screen.

2. Edit the Forwarding Rules so they do not reference the folder you are trying to inactivate. Specific instructions are in the **Edit Forwarding Rules** section.

3. Attempt to inactivate the folder again.

Once there are no Forwarding Rules referring to the folder the Inactivate Folder screen will display "No Forwarding Rules reference this folder" followed by "OK".

10.4.2. Folder Assignment Rules Reference This Folder

If the folder that you are trying to inactivate is the Destination Folder for any Folder Assignment Rules then you must edit those rules.

Edit the Folder Assignment Rules

1. Click on the link to the rule provided on the Inactivate Folder screen.

2. Edit the Folder Assignment Rules. Specific instructions are in the **Editing Assignment Rules** section.

3. Attempt to inactivate the folder again.

Once there are no Forward Assignment Rules referring to the folder the Inactivate Folder screen will display "There are no Folder Assignment Rules" followed by "OK".

10.4.3. Matches are Contained in Folder

A folder that has Matches within it cannot be inactivated without moving these Matches to another folder.

Move the Matches

1. Click on the **Manage Folders** link in the sidebar.

2. Click on the **Assign Matches to Folder** button.

3. Select the folder you are trying to inactivate from the dropdown.

4. Click **Search**.

5. Select a folder from the dropdown list, at the bottom of the screen, to which you will move the Matches.

6. Click on **Move All Results**.

7. Attempt to inactivate the folder again.

Once there are no Matches within the folder you are inactivating, the Inactivate Folder screen will display "No Matches must be moved" followed by "OK".

If all three parameters are met, an Inactivate Folder screen like the one below is shown.

1. Click on the **Inactivate Folder** button to complete the inactivation process and return to the Edit Folder screen.

Clicking on the **Cancel** button will return you to the Edit Folder screen without inactivating the folder.

Inactivate Folder:PEP

No Forwarding Rules reference this Folder. OK
There are No Folder Assignment Rules. OK
No Matched must be moved. OK

Inactivate Folder | Cancel
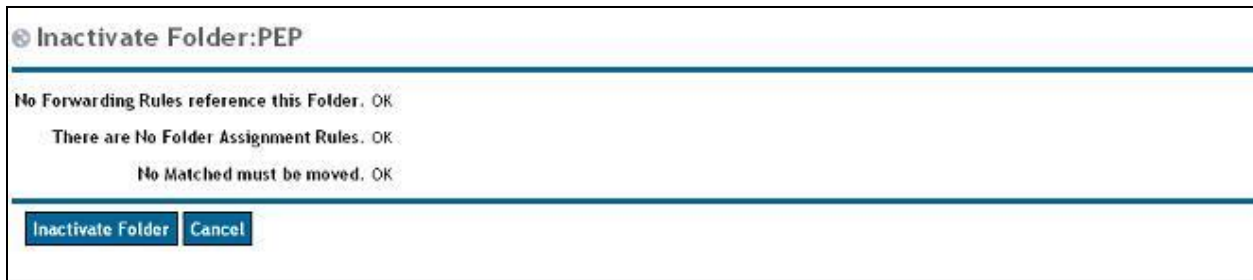
Reactivate a Folder

1. Click on the **Manage Folders** button in the sidebar.

2. Click on the Folder Name that you want to activate.

3. Click on one of the Activate buttons.

10.4.4.   Edit Notification Settings

Notification Settings are only useful for customers using the Notification API. These settings determine when a notification is sent from the Compliance Link Application. For more information about Notification Settings please contact your Account Manager or Support@Accuity.com.

To edit the Notification Settings:

1. Click on **Manage Folders**.

2. Click on the Folder Name that you want to edit.

Notification Settings

Notifications are enabled for New Match Notification, Review Match Notification

When Match Enter the Folder with Status	Send Notification
Changed	☐
False Positive (Good)	☐
Hold	☐
Open	☐
Passed by Good File	☐
Passed by Rules	☐
True Match (Blocked)	☐

Besides enabling notification on Match Statuses, actual delivery of notification also depends on Notification Handlers integrated with Compliance Link for this Institution.

3. Check the checkbox associated with each Match Status that should generate a notification. Whenever a match enters the folder with a checked Match Status an email will be generated and sent to a pre-configured email address.

4. Un-check any checkboxes for Match Statuses that should not create automatic email notifications.

5. Click the **Save** button to save your selections and return to the Manage Folders screen. Click the **Reset** button to undo the changes to the Edit Folder screen. To return to the Manage Folders screen without editing the folder click the **Cancel** button.

10.5. Assignment Rules

Assignment Rules automatically route initial matches to specific folders. This facilitates user match review, tracking, and work prioritization. Until Assignment Rules are established, all initial matches are routed to the default "Public" folder.

Begin Using Assignment Rules

1. Click the **Manage Folders** link located in the sidebar.

2. Click the **View Assignment Rules** button to access the Assignment Rules screen.

10.5.1.   Adding an Assignment Rule

To add a new Assignment Rule click on the Add Assignment Rule button, this brings you to the Add Assignment Rule screen shown below.

Add an Assignment Rule

1. Enter a name for the Rule in the **Name** field.

2. Enter a Sort Value in the **Sort** field.

   ➢ **NOTE:** The Sort value for a particular Rule determines the order in which Matches are compared to Assignment Rules. If a match meets the requirements of two Assignment Rules, the Assignment Rule with a lower Sort value would take precedence.

3. Choose the folder in which the matches that fit this rule will be placed from the **Destination Folder** dropdown (which includes all active folders sorted in alphabetical order).

4. Select a data element from the dropdown box that contains the set of Accuity standard fields and fields from your proprietary File Specifications.

5. Select the comparison operator from the dropdown box populated with: equal to "**=**", less than or equal to "**<=**", and greater than or equal to "**>=**".

6. Enter the Rule Text in the input field to the right of the comparison operator.

An example of an Assignment Rule can be viewed as such:

	Data Element	**Comparison Operator**	**Rule Text**
When	Source Code	=	UST

7. Check the **Numeric Comparison** checkbox if the Rule is comparing the selected data element to a number.

For instance, if you use the criteria in the example above and select the folder named "OFAC" as the Destination Folder, this would cause any match caused by the UST, or OFAC list, be assigned to the "OFAC" Folder.

8. Click on **Add** to add another Assignment Rule clause to the rule.

9. Click the **Save** button to store the Rule that you created and return to the Assignment Rules screen displaying the newly created Rule. Clicking the **Reset** button clears the input fields. Clicking on the **Cancel** button returns you to the Assignment Rules screen without creating a Rule.

   ➢ **NOTE:** Clicking **Delete** next to any Assignment Rule clause will remove that clause from the rule.
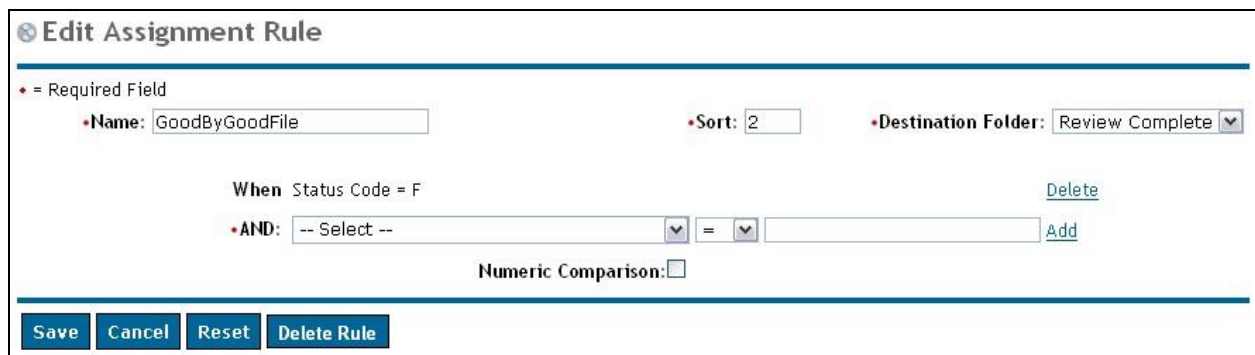
10.5.2. Editing Assignment Rules

Edit an Assignment Rule

1. Click on the **Manage Folders** button in the sidebar.

2. Click on the **View Assignment Rules** button located beneath the folder listing.

3. Click on the name of the Rule that you would like to edit.

This leads you to the Edit Assignment Rules screen. An example is shown below.

- To change the Name of the Assignment Rule, edit the **Name** input field.

- Edit the **Sort** input field to change the Sort value.

  ➢ **NOTE:** The Sort value for a particular Rule determines the order in which Matches are compared to Assignment Rules. If a match meets the requirements of two Assignment Rules, the Assignment Rule with a lower Sort value takes precedence.

To change the data element of the Assignment Rule, select a new data element from the dropdown list populated by the set of Accuity standard fields (Status Code, Entity Type, File Name, Matched Field, Screening User ID, Source Code, Stop Descriptor, Web Service Profile Name, and Web Service Profile ID) as well as fields from user-defined File Specifications.

- Select a different comparison operator from the dropdown list to change the comparison operator.

- Change the Rule Text by editing the Rule Text input field to the right of the comparison operator.

- Check the **Numeric Comparison** checkbox if the Rule Text consists of a number.

- To change the folder to which the Matches are sent, select the proper folder from the **Destination Folder** dropdown list. This dropdown list consists of all active folders within the account.

- To delete a specific Assignment Rule clause, click **Delete** next to that clause.
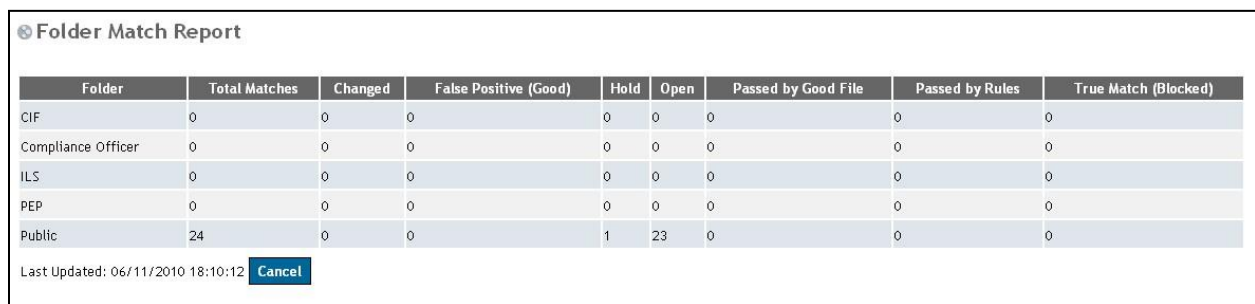
Click the **Save** button to store your changes and return to the Assignment Rules screen. Click on the **Cancel** button to return to the Assignment Rules screen without saving. Click on the **Reset** button to change all the input fields back to their original state. Clicking on the **Delete Rule** button removes the Rule entirely. Deleting an Assignment Rule returns you to the Assignment Rules screen where the deleted Rule will not appear.

10.6. Folder Match Report

Compliance Link's Case Management module allows users with the Case Management Configuration feature set to view counts of matches in each folder with each assigned Match Status.

View the Folder Match Report

1. Click on **Manage Folders** from the sidebar.

2. Click on **Folder Match Report**.

⊗ Folder Match Report

Folder	Total Matches	Changed	False Positive (Good)	Hold	Open	Passed by Good File	Passed by Rules	True Match (Blocked)
CIF	0	0	0	0	0	0	0	0
Compliance Officer	0	0	0	0	0	0	0	0
ILS	0	0	0	0	0	0	0	0
PEP	0	0	0	0	0	0	0	0
Public	24	0	0	1	23	0	0	0

Last Updated: 06/11/2010 18:10:12 Cancel

3. Click on **Cancel** to return to the Manage Folders screen.

10.7. Assign Matches to Folders

Manually Move Matches to Folders

1. Click on **Manage Folders** from the sidebar.

2. Click on **Assign Matches to Folders**.

3. Select search criteria from the following options:

    a. **Batch ID** (dropdown list)

    b. **Folder** (dropdown list)

    c. **Range of Batch IDs** (mm/dd/yyyy)

    d. **Range of Match IDs** (mm/dd/yyyy)

    e. **Unique ID** (numerical only)

    f. **Case ID** (numerical only)

    g. **Status Code** (checkbox)

4. Click on **Search**.

5. Choose a folder to move the matches to from the dropdown list.

6. Either select matches individually and click on **Move Selected Results** or click on **Move All Results** to move all matches to the designated folder.
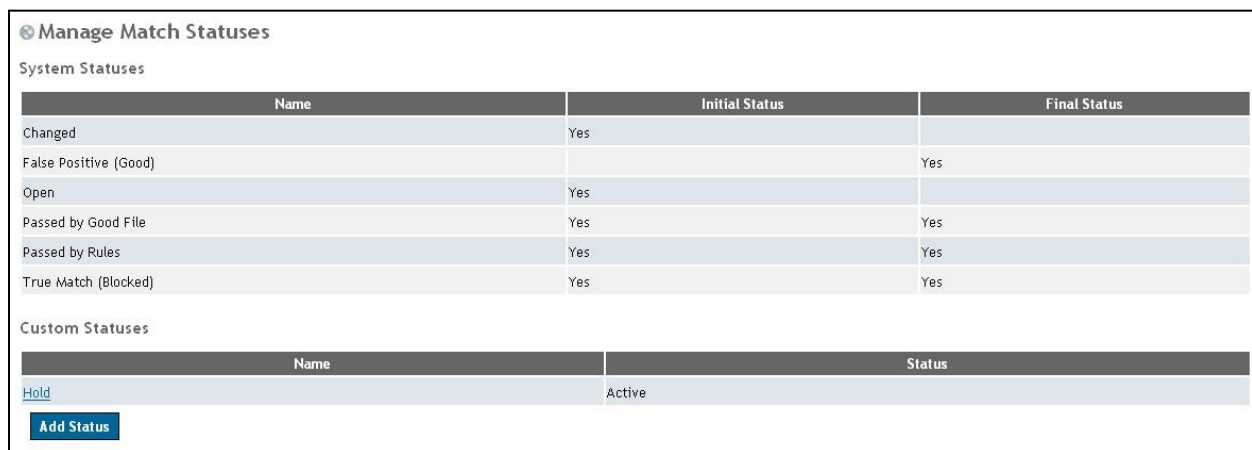
10.7.1. Manage Match Statuses

Compliance Link offers the ability for users with the Match Status Management feature set to customize Match Statuses to further enhance their workflow. The standard System Statuses (Changed, False Positive, Open, Passed by Good File, Passed by Rules, and True Match) cannot be customized.

10.7.2. Add a Match Status

Add a New Match Status

1. Click on **Manage Folders** from the sidebar.

2. Click on **Manage Match Statuses**.

3. Click on **Add Status**.

4. Enter the **Name** of the New Match Status.

5. Click on **Save**.

10.7.3. Delete / Inactivate a Match Status

Custom Match Statuses can only be deleted if they have not been used previously. If a Match Status has been used, users can inactivate the Match Status, removing it from all search and review screens.

Delete / Inactivate a Match Status

1. Click on **Manage Folders** from the sidebar.

2. Click on **Manage Match Statuses**.

3. Click on the Match Status to be deleted.

4. Click on **Delete Match Status**.

5. If there are Forwarding Rules that reference the Match Status or Matches that currently have the Match Status it cannot be inactivated. These issues must be resolved before the Match Status can be inactivated.

11. GOOD FILE

Good File is a database of information from matched records that have been reviewed and been marked as False Positive. This information is retained for use in subsequent screenings. When a file is screened, records that contain a match are compared to the Good File. The Good File eliminates the burden of reviewing repeated matches in customer file screenings. Good File records are "persistent" - deleting batches from the Batch Maintenance screen will not affect the records in the Good File.

Users with the feature sets, Good File Preload and Search Good File, have the option of viewing the current Good File and/or removing records from the Good File.

11.1.Good File Preload

Good File Preload is a mechanism by which records can be automatically assigned the match review codes of False Positive (or True Match depending on which type of files you wish to load). When Good File Preload is used, a file is screened and if matches are found, all matches will be placed into the Compliance Link Good File as if a user had manually assigned the Match Status of False Positive to each record. Good File Preload can be very beneficial for users who are upgrading to Compliance Link from other screening software applications that contain "good file" or "white list" entries.

Records in the Good File Preload file that do not generate matches during the screening process will not be loaded into the Good File.

Preload a Good File

1. Click on **Good File Preload** from the sidebar.

2. Select whether the file you are uploading is populated with False Positive records or True Match records only.

3. Choose a File Specification for your file.

4. Browse to and select the file.

5. Screen the file by clicking **Submit**.

This process will place all matches found in that file in the Good File as either False Positive or True Match.

Search the Good File

1. Click on **Search Good File** from the sidebar. Here you can enter a wide variety of search criteria:

    a. **Record Type** (False Positive, False Positive or All)

    b. **Unique Field**

    c. **Stop Descriptor Text**

    d. **Matched Field**

    e. **Match Type** (CWL, GWL or PEP)

    f. **Date Created Range**

    g. **Last Update Date Range**

    h. **Data Field Name**

    i. **Data Field Value**

    j. **Active/Inactive Records**

2. Enter the search criteria. (Leave these fields blank to view all records in the Good File.)

3. Click on **Search**.

Good Records Search Results						
Search Criteria:						
Stop Descriptor Text	**Unique ID**	**Matched Field**	**Record Type**	**Original Creation Date**	**Last Update Date**	**Status**
FELIX ALBERTO	564782139	Name	Good	10/30/2008 15:24:17	10/30/2008 15:24:17	Active

Records 1 to 1 of 1 Total Records

Download Good File

The comma delimited file downloaded includes all search results

The results include:

- **Stop Descriptor**

- **Unique ID**

- **Matched Field**

- **Record Type**

- **Original Creation Date**

- **Last Update Date**

- **Status**

    ➢ **NOTE:** You can click on the STOP DESCRIPTOR TEXT to view the full details on the good file record, and to inactivate the record.

You can download a comma-delimited file of all active good file records by clicking on the **Download Good File** button. You will be prompted to open or save the file.

The Good File Download will consist of the following fields:

- **Stop Descriptor Text**

- **Unique ID**

- **Matched Field**

- **Match Type**

- **Record Type**

- **Original Creation Date**

- **Last Update Date**

- **Status**

  - ➢ **NOTE:** Inactivated good file records will not be treated as good records during screening, and will not appear in the search results or the downloaded file.

12. CHANGING PASSWORDS

You can change your password by clicking on the Change Password link in the sidebar.

To change your password:

1. Enter your Old Password

2. Enter your desired New Password

3. Re-enter your New Password

> ➢ **NOTE:**   There are password policy rules that are set at the Compliance Link instance-level by your System Operator.

If you wish to cancel changing the password, just click on the Cancel button.

Sometimes, users are required to change their passwords during their first login or after a set period of inactivity. In these cases, the Change Password screen will automatically appear after signing in.
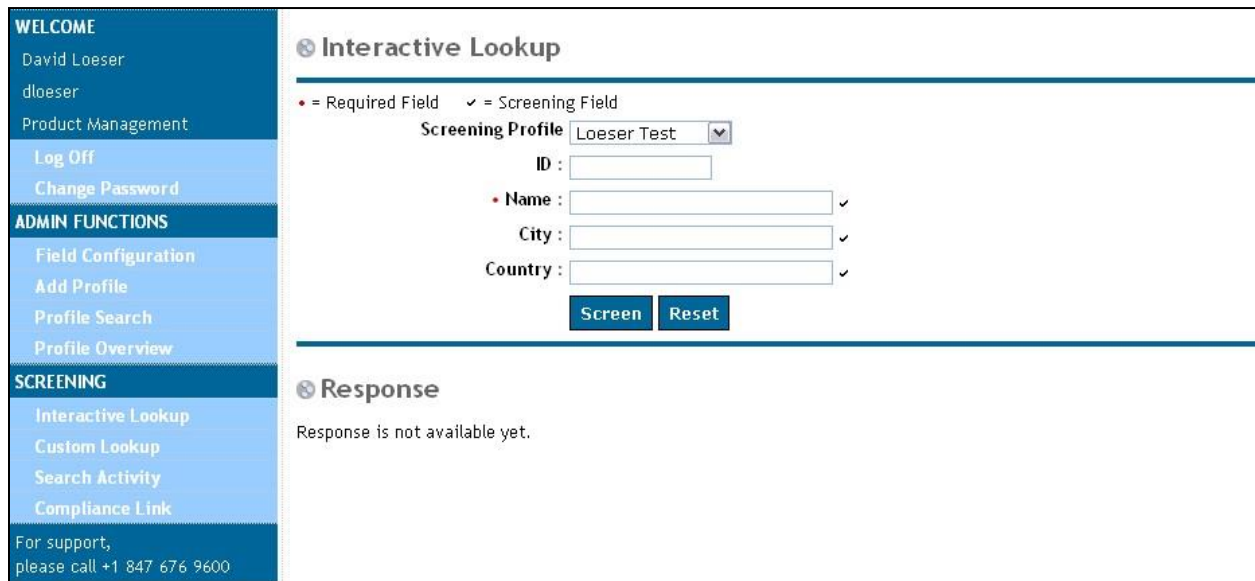
13. INTERACTIVE LOOKUP SYSTEM (ILS)

Compliance Link includes the Interactive Lookup System (ILS) which allows for customizable ad hoc lookups. ILS is a separate module that can be reached by clicking on the Interactive Lookup System link at the bottom of the sidebar.

Users with the Lookup Role of Lookup Supervisor have the ability to:

- Edit Field Configuration

- Add/Edit Screening Profiles

- Perform Interactive Lookups

- Perform Custom Lookups

- Query Search Activity/Download Activity File

Before any Interactive Lookups can be performed, a user with the Lookup Supervisor role or feature set, ILS Configuration, must configure the data fields for the lookups.

13.1. Edit Field Configuration

Edit the Field Configuration

1. Click on the **Interactive Lookup System** link at the bottom of the sidebar.

2. Click on **Field Configuration** link on the sidebar.

ACCUITY

Manage Field Configuration

Field Name	Screening Field	Unique Field	Required Field	Display Order	Max Allowed Data Length	Display Size	Data Type
ID	☐	☑	☐	1	50	30	Customer Unique ID ▼
Name	☑	☐	☑	2	50	30	Name - General ▼
Address	☐	☐	☐	3	50	30	Unspecified ▼
Country	☐	☐	☐	4	50	30	Country Name ▼
DOB	☐	☐	☐	5	50	30	DOB ▼
	☐	☐	☐				Unspecified ▼
	☐	☐	☐				Unspecified ▼

Save Reset Cancel   Add More Lines

3. Enter the **Field Name**.

4. Choose whether the field will be a **Screening Field**, **Unique Field**, and/or **Required Field**

A single field must be selected as the Unique ID. A Unique ID is a value unique to that record and not duplicated elsewhere in the file. The Unique ID is used in the Good File to identify a record that has been previously screened.

Multiple fields can be selected (at least one must be selected) as Screening Fields.

These fields are used with the Screening Fields Only screening option. When the option is selected only "screening fields" will be filtered against the Global WatchList but all fields will be written to the match database. This feature can be very useful if your screening file contains data that does not need to be matched against the Global WatchList (i.e. department names, addresses, postal codes). This option is set for each Screening Profile.

Required fields must be filled out to perform an Interactive Lookup.

5. Enter the **Display Order**. This determines in which order the fields are shown on the Interactive Lookup screen.

6. Enter a **Max Allowed Data Length**.

7. Enter a **Display Size**. This determines the length of each input field on the Interactive Lookup screen.

8. Choose the **Data Type** from the dropdown list. If no data types match the expected input data, choose **Unspecified**.

➢ NOTE: For Commodity Screening, use the Commodity Name, Commodity Routing and Commodity Country fields. Commodity Name is used for fields that will contain commodity information or descriptions. Commodity Routing is used for fields that will contain station or routing codes (i.e. ORD → US) that are mapped to ISO Country Codes using the routing mapping file. Commodity Country is used when the field contains country information instead of station codes (i.e. DE, Germany, Deutschland). Whenever any fields in field configuration are marked as Commodity Type data, the Commodity Screening Engine will be invoked during screening. Normal GWL/PEP Screening and Commodity Screening can be used simultaneously.

If more fields are necessary, click on **Add More Lines**.

9. Click the **Save** button to save your selections and return to the Interactive Lookup screen. Click the **Reset** button to undo the changes to the Field Configuration. To return to the Interactive lookup screen without editing the Field Configuration click the **Cancel** button.

13.2. Add Screening Profiles

Screening Profiles are managed by Lookup Supervisors and/or users with the ILS Configuration feature set. These Screening Profiles configure the manner in which the lookup is performed. This includes the Profile Name, User Group, Screening Options, Screening Algorithms, Compliance Link User Name, False Positive Reduction tools, Response Type, and watch lists screened against.

<u>Add a New Screening Profile</u>

1. Click on the **Interactive Lookup System** link in the sidebar.

2. Click on **Add Profile** from the sidebar.

ACCUITY

3. A **Profile ID** will be automatically assigned to the Profile. Enter the desired **Profile Name**.

4. Assign the new profile to a **User Group**. More information about User Groups is in the **User Group** section of this **Administrator Guide**.

5. Mark the **Status** as **Active**.

6. Choose which of the **Screening Algorithms** to use

    a. **Accuity Token** – Accuity Token is the standard matching algorithm built around Stop Descriptors, Accuity's Synonym Table, and Token-based matching. Accuity Token is used for every screening and cannot be deselected.

    b. **Fuzzy Logic** – Fuzzy Logic is based on the Edit Distance algorithm (or Levenshtein Distance algorithm) which, using Stop Descriptors, can address many common misspellings and typos such as insertion, deletion, transposition and substitution.

    c. **Soundex** – A phonetic algorithm that indexes names by sound and matches them against Soundex encoded Stop Descriptors. (Only used in Latin-based screening)

    d. **Metaphone** – A phonetic algorithm that encodes input names with varying lengths by their English pronunciation. These encodings are compared to encoded Stop Descriptors. (Only used in Latin-based screening)

    e. **Double Metaphone** – Second generation of Metaphone phonetic algorithm. (Only used in Latin-based screening)

7. Choose an associated **Compliance Link User**. When matches are written to the Review History, this will be the Screening User.

8. Choose a **Risk Scorecard**. For more information about Risk Scorecards please refer to the **Risk Scorecard** section of this **Administrator Guide**. If no Risk Scorecard is selected then no Risk Scoring will be performed.

9. Choose whether to use the Compliance Link **Good File** associated with the institution or not.

10. Each profile can use customizable False Positive Reduction **Rules** sets. Choose to use the uploaded rules file or not. You can upload the rules file while editing the Screening Profile. More information about editing the Screening Profile is in the **Editing Screening Profile** section of this **Administrator Guide**.

11. Choose whether to **Write Hits** to the Compliance Link database or not.

    ➢ **NOTE:** If this option is set to "Do not write hits" then ILS users will not be able to review matches within ILS.

12. Configure the **Response Type**.

    a. **Return Full Response** – Matches will display the full Entity Information from the watch lists.

    b. **Return Full Response and List Versions** – Matches will display the full Entity Information from the watch lists as well as the list versions screened against.

c. Return Pass/Fail Response – Lookup response will include Hit/No Hit, but the Entity Information will not be shown.
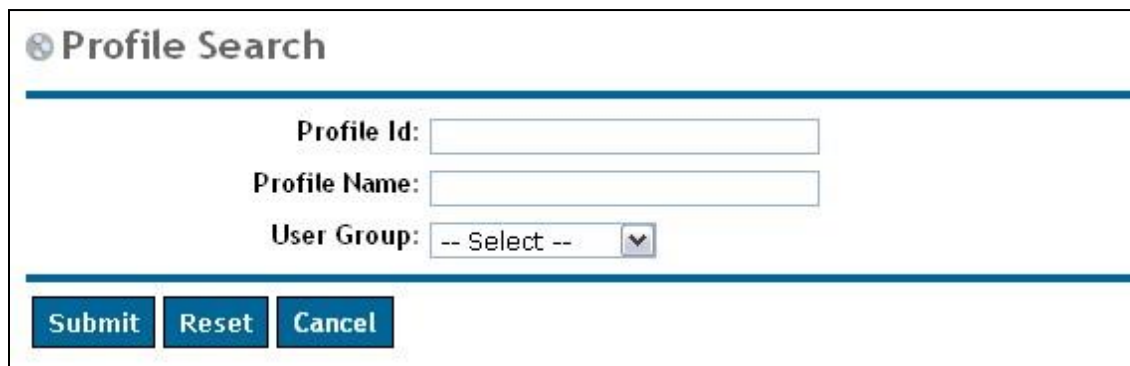
13. Select which watch **Lists to Filter Against**.

14. Click on **Submit** to save the new Screening Profile. Clicking on **Reset** will undo all changes made to the new Screening Profile. Click **Cancel** to return to the Interactive Lookup screen.

> **NOTE:** If a False Positive Reduction Rules file and/or Character Mapping File are to be used for this Screening Profile they must be uploaded at this time. More information about these changes is in the **Upload New Rules File** section and **Upload Char Map File** section.

13.3. Edit Screening Profiles

Screening Profiles can be edited by performing a Profile Search or linking through the Profile Overview screen.

Perform Profile Search

1. Click on the **Interactive Lookup System** link from the sidebar.

2. Click on the **Profile Search** link from the sidebar.

3. Enter the search criteria:

    a. Profile ID

    b. Profile Name

    c. User Group

4. Click on **Submit** to perform the Profile Search. Click **Reset** to clear all information from the input fields. Click **Cancel** to return to the Interactive Lookup screen.

Edit a Screening Profile from Profile Search Results

1. Click on the Profile Name.

2. Click on **Edit Profile**. Clicking **Cancel** will return you to the Interactive Lookup screen.

   ➢ **NOTE:** Users can also upload False Positive Reduction Rules files by clicking on **Upload New Rules File** or upload Character Mapping files by clicking on **Upload Char Map File**. More information about these changes is in the **Upload New Rules File** section and **Upload Char Map File** section.

3. Make necessary changes and click on **Submit** to save the changes. Click **Reset** to clear all changes to the Screening Profile. Click **Cancel** to return to the Interactive Lookup screen.

Edit a Screening Profile from Profile Overview

1. Click on **Interactive Lookup System** from the sidebar.

2. Click on **Profile Overview** from the sidebar.
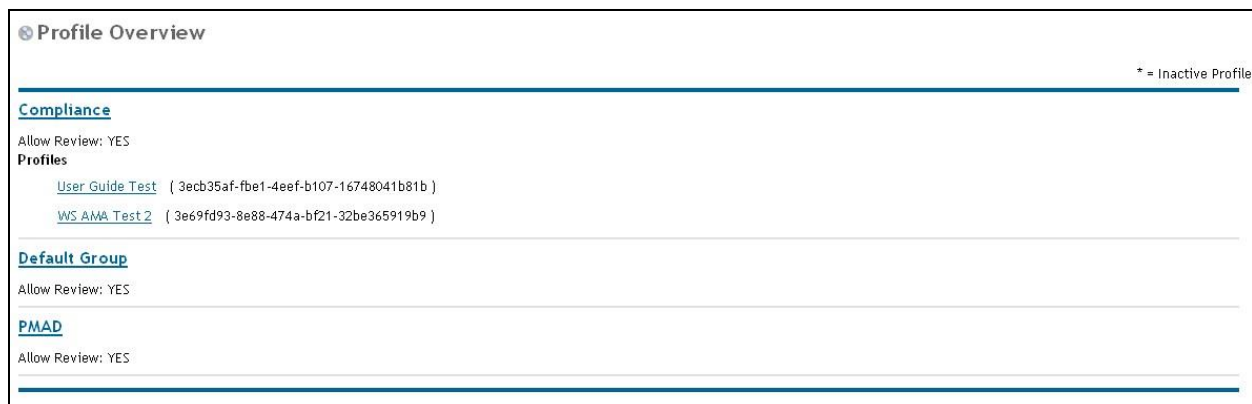
3. Click on the Profile Name to be changed.

4. Click on **Edit Profile**. Clicking **Cancel** will return you to the Interactive Lookup screen.

   ➢ NOTE: Users can also upload False Positive Reduction Rules files by clicking on **Upload New Rules File** or upload Character Mapping files by clicking on **Upload Char Map File**.

5. Make necessary changes and click on **Submit** to save the changes. Click **Reset** to clear all changes to the Screening Profile. Click **Cancel** to return to the Interactive Lookup screen.

13.4. Upload a Rules File

Every Screening Profile has the ability to apply specific sets of False Positive Reduction Rules. These rules must be uploaded to the Screening Profile.

Upload a Rules File

1. Click on the **Interactive Lookup System** button in the sidebar.

2. Click on **Profile Overview**.

3. Click on the Profile Name to be edited.

```
◉ View Profile
                    Profile Id: 0c3b01f1-21a4-4d9b-8fc8-703dc2ce6c3c
                  Profile Name: OFAC
                    User Group: Default Group
                        Status: Active

              Screening Options: Screening Fields Only: YES
                                 Remove Middle Initial: YES
                                 Ignore Vessels: YES
                                 Use Advanced Matching Algorithm: NO
                    AMA Setting: 75 (Range: 50-99)

          Compliance Link User: Lookup User [Lookup]

                     Good File: Use Compliance Link Good File
                         Rules: Use uploaded Rules.xml File
                     Write Hits: Write hits to Compliance Link Database
                  Response Type: Return Full Response and List Versions

            • Lists to Filter Against:
                                 Accuity OFAC Enhancements
                                 Accuity's OFAC List

   [Edit Profile]  [Cancel]

◉ Rules Upload

This profile is using Uploaded Rules.
Last Uploaded Rules: 06/25/2010 17:33:07
   [Upload New Rules File]  [Download Rules File]
```

4. Click on **Upload New Rules File**.

```
◉ Rules Upload
                    Profile Id: 0c3b01f1-21a4-4d9b-8fc8-703dc2ce6c3c
                  Profile Name: OFAC
               Rules File Type: [RULES.DAT Format ▼]
                          File: [              ] [Browse...] •
   [Upload]  [Cancel]
```

5. Choose the **Rules File Type** from the dropdown (RULES.DAT Format/RULES.XML Format)

6. **Browse** for the rules file.

7. Click **Upload** to upload the rules file to the Screening Profile. Clicking **Cancel** will bring up the Screening Profile page without uploading a rules file.
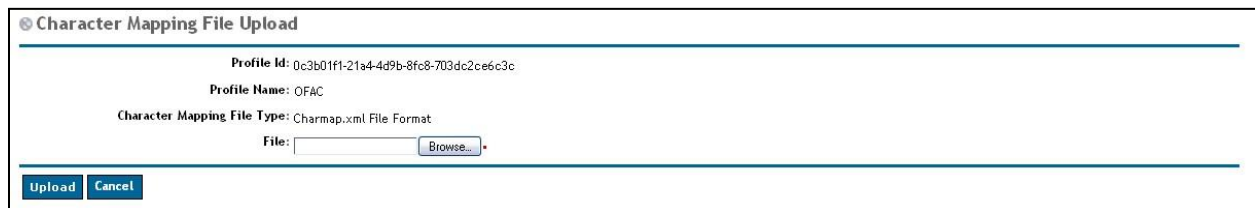
13.5. Upload a Character Mapping File

Each Screening Profile can utilize a character mapping file that will associate specific alphanumeric characters with other standard characters. This is useful when screening information that may have tildes, umlauts, etc.

Upload a Character Mapping File

1. Click on the **Interactive Lookup System** button in the sidebar.

2. Click on **Profile Overview**.

3. Click on the Profile Name to be edited.

4. Click on **Upload Char Map File** at the bottom of the screen.

5. **Browse** for a charmap.xml file to be uploaded.

6. Click **Upload** to upload the character mapping file to the Screening Profile. Clicking **Cancel** will bring up the Screening Profile page without uploading a character mapping file.

13.6. Search Activity / Download Activity File

For auditing and reporting purposes, ILS will log every lookup performed. Lookup Supervisors or users with the ILS Activity History can search, review, and download this activity.

> ➢ **NOTE:** The Activity log in ILS will also maintain any calls made to the FilterActivityService Web Service.

Search Lookup Activity

1. Click on **Interactive Lookup System** from the sidebar.

2. Click on **Search Activity** from the sidebar.

3. Enter at least one of the following search criteria:

    a. Screen Date Range (mm/dd/yyyy)

    b. Check **Limit** results from current session only – This will only return the Interactive Lookups that have been performed since you have logged in last.

    c. User Name

    d. Match Result (ALL, Contains Matches, or No Matches)

4. Click **Search** to view the Search Activity Results screen. Click **Reset** to clear all search criteria. Clicking **Cancel** will take you back to the Interactive Lookup Screen.

5. Click on **Download Activity File** to download a comma-separated values file containing the following fields:

    a. Account ID

ACCUITY

   b. **Account Name**

   c. **Search Date**

   d. **User ID**

   e. **Profile Name**

   f. **Profile ID**

   g. **Number of Results**

   ➢ **NOTE:** These are then followed by every field in the Interactive Lookup.

13.7. Interactive Lookups

Perform an Interactive Lookup

  1. Click on **Interactive Lookup System** from the sidebar.

  1. If there are multiple Screening Profiles associated with the User Group, a dropdown list will be seen. Choose the **Screening Profile** to be used.

  2. Fill out the input fields as necessary. All required fields will be marked. Failure to enter information in these fields will cause an error.

  3. Click on **Screen**.

Depending on Screening Profile settings, the Response may vary. At a minimum the response will return whether the Interactive Lookup caused a match or not.

13.8. Custom Lookups

Users with the ILS Custom Lookup feature set can perform customized lookups with configurable screening options.

Perform a Custom Lookup

1. Click on **Interactive Lookup System** from the sidebar.

2. Click on **Custom Lookup** from the sidebar.

3. Fill out the input fields as necessary. All required fields will be marked. Failure to enter information in these fields will cause an error.

4. Choose which of the **Screening Algorithms** to use.

   a. **Accuity Token** – Accuity Token is the standard matching algorithm built around Stop Descriptors, Accuity's Synonym Table, and Token-based matching. Accuity Token is used for every screening and cannot be deselected.

   b. **Fuzzy Logic** – Fuzzy Logic is based on the Edit Distance algorithm (or Levenshtein Distance algorithm) which, using Stop Descriptors, can address many common misspellings and typos such as insertion, deletion, transposition and substitution.

   c. **Soundex** – A phonetic algorithm that indexes names by sound and matches them against Soundex encoded Stop Descriptors. (Only used in Latin-based screening)

   d. **Metaphone** – A phonetic algorithm that encodes input names with varying lengths by their English pronunciation. These encodings are compared to encoded Stop Descriptors. (Only used in Latin-based screening)

   e. **Double Metaphone** – Second generation of Metaphone phonetic algorithm. (Only used in Latin-based screening)

5. Select **Screening Options** to use for the custom screening.

6. Choose which watch **Lists to Filter Against**.

7. Click **Screen**.

Depending on Screening Profile settings, the Response may vary. At a minimum the response will return whether the Interactive Lookup caused a match or not.

14. AUDIT TRAIL REPORTS

Compliance Link provides the ability to create Audit Trail reports that house information regarding changes to the Application in the User Application Audit report and logs regarding user security in the User Security Audit report. Access to these reports is limited to users with Institution Management and User Activity Audit Trail feature sets. Access to the User Application Audit and User Security Audit report is available through the Institution Summary link in the sidebar (for standalone institutions) or the Search Institutions screen (for service bureau/multiprocessor institutions).

14.1. User Security Audit

The User Security Audit report contains details about changes to user access and entitlement. These can be system-generated changes (e.g. User Lock-out) or administrator-generated changes (e.g. New User Role created). The following is a list of activities logged in the User Security Audit report:

Activity/Event	Change Type
User was automatically locked due to inactivity	LOCKED_NO_ACTIVITY
Administrator unlocked the user	USER_UNLOCKED
User was automatically locked due to too many invalid login attempts	LOCKED_INVALID_PASSWORD
Administrator created new user	NEW_USER
Administrator created new user role	NEW_USER_ROLE
Administrator activated new role for user	USER_ROLE_ACTIVATED
Administrator changed user information	USER_INFO_CHANGED
Administrator inactivated user	USER_DELETED
Administrator removed user role from user	USER_ROLE_INACTIVATED
Administrator created new child institution	NEW_INST
Administrator changed roles for user	USER_ROLES_CHANGED

14.2. User Application Audit

The User Application Audit report contains details about changes to application configuration including changes to case management, screening profiles, etc. The following is a list of activities logged in the User Application Audit report:

Activity/Event	Change Type
Application Parameters were updated	APP_PARAMETER_SAVED
User deleted a batch	BATCH_DELETED
Batch was restarted	BATCH_RESTARTED
User revived a batch thread	BATCH_THREAD_REVIVE
Batch Thread was suspended	BATCH_THREAD_SUSPEND
Good File Preload for True Matches was performed	BLOCKED_FILE_PRELOAD
External ID for Controlled Goods Manager was updated	CGM_EXTID_UPD
Access to Controlled Goods Manager was removed	CGM_INACTIVATED
Controlled Goods Manager Key was updated	CGM_KEY_UPD
Character Map file was activated	CHARMAP_ACTIVATED
Character Map file was inactivated	CHARMAP_INACTIVATED
New Character Map file was uploaded	CHARMAP_UPLOADED
Access to Controlled Goods Manager was activated	CM_ACTIVATED
A Custom Dictionary was activated	DICTIONARY_ACTIVATED
User inactivated a Custom Dictionary	DICTIONARY_INACTIVATED
User uploaded a new Custom Dictionary	DICTIONARY_UPLOADED
Online Compliance External ID was created	EID_CREATED
Online Compliance External ID was updated	EID_UPDATED
User created a new folder assignment rule	FAR_CREATED
User deleted a Folder Assignment Rule	FAR_DELETED
User updated a Folder Assignment Rule	FAR_UPDATED
A Folder was activated	FOLDER_ACTIVATED
New Folder was created	FOLDER_CREATED
A Folder was marked as inactivate	FOLDER_INACTIVATED
User updated information about a Folder	FOLDER_UPDATED
User created a new False Positive Rule	FPR_ADDED
False Positive Rule was inactivated	FPR_INACTIVATED
False Positive Rule was reactivated	FPR_REACTIVATED
User updated a False Positive Rule	FPR_UPDATED
Good File Preload for False Positives was performed	GOOD_FILE_PRELOAD
Access to ILS was removed	ILS_INACTIVATED
Institution Status was marked as active	INST_STATUS_ACTIVATED

Institution status was marked as inactive	INST_STATUS_INACTIVATED
Institution information was updated	INST_UPDATED
List subscription for an institution was updated	LIST_SUBSCRIPTION_UPDATED
A match was moved to a new folder manually	MATCH_MOVED
User created a new Match Status	MATCH_STATUS_CREATED
User deleted a custom Match Status	MATCH_STATUS_DELETED
User inactivated Match Status	MATCH_STATUS_INACTIVATED
New SFTP User was created	NEW_SFTP_USER
New User Group was created	NEW_USER_GROUP
Report Profile was deleted	REPORT_PROFILE_DELETED
Report Profile was saved	REPORT_PROFILE_SAVED
Risk Scorecard was activated	SCORECARD_ACTIVATED
Risk Scorecard was created	SCORECARD_CREATED
Risk Scorecard was deleted	SCORECARD_DELETED
Risk Scorecard was inactivated	SCORECARD_INACTIVATED
Screening Profile was created	SCR_PROFILE_CREATED
Screening Profile was deleted	SCR_PROFILE_DELETED
Screening Profile was updated	SCR_PROFILE_UPDATED
Screening Profile was deleted	SCREENNING_PROFILE_DELETED*
Screening Profile was saved	SCREENNING_PROFILE_SAVED*
User Group was activated	USER_GROUP_ACTIVATED
User Group was inactivated	USER_GROUP_INACTIVATED
User Group was updated	USER_GROUP_UPDATED
User changed his/her password	USER_PASSWORD_CHANGED
SFTP User Profile was changed	USER_SFTP_CHANGED

* indicates Change Types that are no longer used

15. AUTOMATED SCREENING MANAGER

Compliance Link's Automated Screening Manager provides for automated, intelligent screening that results in increased screening efficiency, consolidated match information, and a clear and complete audit trail.

The Automated Screening Manager allows users to create a Master Dataset that will be screened automatically based on the user's preferences. Compliance Link will perform true "delta" screening by understanding which of the Watch List Entities have been added or changed, as well as which input records have changed over time, notifying users only when they have work to do reducing overall processing times and manual intervention. This ensures that all of your screenings are up to date, reducing regulatory and reputational risks. Once an action has been taken, the comprehensive audit trail is updated showing auditors each and every step in the compliance process for every record, even ones that did not produce matches.

The Automated Screening Manager User Manual will provide detailed instructions on how to use the application to create the best practices within Compliance Link to fit within individual institution's processes. It will also serve as a useful reference tool for those individuals familiar with the application. For further questions regarding the application or this manual please contact our Technical Support staff at Support@Accuity.com. To begin to use the module click on the "Automated Screening Manager" tab in Compliance Link.
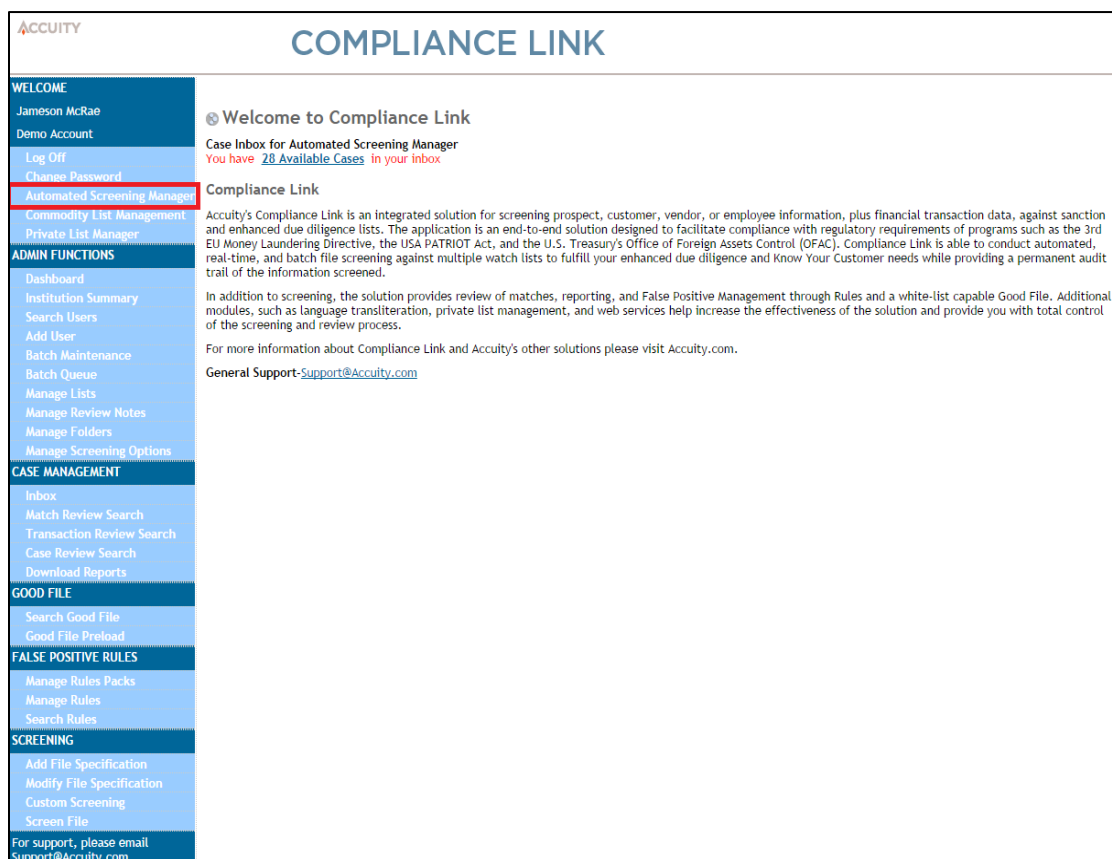
15.1.Manage Datasets

Datasets are used to store sets of input records to be screened on an ongoing basis. Datasets are configured to accept certain types of input record files and screen using specific parameters using screening instructions. Data can be added to the dataset either through file import or through the Automated Screening Lookup screen.

15.1.1.   Adding/Editing Datasets

To begin this process click Manage Datasets within the Automated Screening Manager module:

1. Click Add Dataset

2. Name the Dataset

3. Make sure the Status is marked as "Active"

4. Select a Region for this dataset. If no region is needed, choose "All Regions." For more information about Regions, please refer to the Regions section of this Administrator Guide

15.1.2.   Adding/Editing a Dataset's File Specification:

File Specifications are used to format the expected input record data being imported into the dataset. This also determines the fields available for users with access to Automated Screening Lookup for this particular dataset.

1. Click on the Manage Datasets link in the sidebar

2. Click on the dataset name

3. Click "Add File Specification"

ACCUITY

4.   If you have already created a File Specification from Compliance Link that you would like to use for this particular Dataset you can chose that to copy that File Specification from the "Copy From" dropdown box. Select the name of the pre-existing File Specifications and the fields will be automatically be populated with the information. If not, follow the steps below:

5.   Select the format of your file (e.g. **Fixed Width**, **Delimited**)

6.   If your file is delimited, enter the **Delimiter** and **Text Qualifier** for your file in the boxes provided.

7.   If your file is fixed width, you will not be asked for the **Delimiter** and **Text Qualifier.** You will need to enter the **Field Name**, the **Start Position**, the **Field Length** and **Data Type** for each field. You cannot use the same **Field Name** for multiple fields. Indicate one field as the Unique Field.

➢ **NOTE:** Fields longer than 4,000 bytes will be truncated.

Follow the steps below to properly complete your File Specification:

1.   Enter the **Field Name**.

2.   Enter a **Sort Order** to indicate the order in which the fields appear in your input file.

3.   If the file is Fixed Width, enter a Start Position and Field Length.

4.   A single field must be selected as the Unique ID. A Unique ID is a value unique to that record (i.e. account number) and not duplicated elsewhere in the dataset.

5. Choose the **Data Type** from the dropdown list. If no data types match the expected input data, choose **Unspecified**.

➢ **NOTE:** For Commodity Screening, use the Commodity Name, Commodity Routing and Commodity Country fields. Commodity Name is used for fields that will contain commodity information or descriptions. Commodity Routing is used for fields that will contain station or routing codes (i.e. ORD → US) that are mapped to ISO Country Codes using the routing mapping file. Commodity Country is used when the field contains country information instead of station codes (i.e. DE, Germany, and Deutschland). Whenever any fields in a File Specification are marked as Commodity Type data, the Commodity Screening Engine will be invoked during screening. Normal GWL/PEP Screening and Commodity Screening can be used simultaneously.

6. **Repeat** Steps 1-5 for all of the Field Names in your input file.

7. Once you populated all necessary fields, click **Save**.

15.1.3. Adding/Editing a Dataset's Screening Instructions:

Screening Instructions determine how the records will be screened when they are first added to the dataset, through file import, Automated Screening Lookup, and Automated Screening Web Service call.

1. Click on "Add Instructions" on the Edit Dataset page.

2. Add the **Screening Instruction** Name.

Screening Fields:

1. Select which fields from your data will be **Screening Fields** and then select the **Fuzzy Logic** threshold for each field selected as a Screening Field.

➢ **NOTE:** Multiple fields can be selected (at least one must be selected) as Screening Fields. Only "screening fields" will be screened against the watch lists.

➢ **NOTE:** Fuzzy Logic is based on the Edit Distance algorithm, or Levenshtein Distance, which calculates the number of changes made to get the individual text strings from the Input Record to equal the text strings from the Stop Descriptor.

Screening Parameters:

Screening Parameters
- Risk Scorecard: Demo Scorecard ▼
- Rules Pack: DEFAULT ▼
- Screening Options: ☑ Remove Middle Initial
- ☐ Ignore Vessels
- Character Mapping File: DEFAULT ▼
- Custom Dictionary: --NONE-- ▼

Lists to Filter Against: *(Must select at least one of the following lists)* •
Select: All None ☑ Accuity's OFAC List
☑ Accuity OFAC Enhancements

☐ AU
☐ BofE

☐ Dave Test

Save **Cancel**

3. If applicable, choose a **Risk Scorecard** for your Screening Instructions. Risk Scorecards are created within Compliance Link under the Manage Screening Options tab.

4. Choose the (False Positive Reduction) **Rules Pack** for your Screening Instructions. Rules Packs can be created and are editable under the False Positive Rules heading in Compliance Link.

5. Select a **Controlled Goods Policy**. This requires the Controlled Goods Manager application and may not be available in your account. Please contact Support@Accuity.com for more information.

➢ **NOTE:** If a Controlled Goods Policy is selected, then the field that contains the Good Description must be selected as a Screening Field.

6. **Remove Middle-Initial** – This option will remove the middle initial before filtering to reduce false positive matches. Only screening fields will be affected. The text must be in the format of Firstname [middle initial] Lastname or Lastname, Firstname [middle initial].

7. **Ignore Vessels** – This option will ignore any match where the entity type is Vessel.

8. Choose a **Character Mapping File** if applicable.

ACCUITY

9.   Choose a **Customer Dictionary** if applicable.

10. Choose the **Lists** you would like to filter against.

11. Click **Save**

Once you have completed the File Specification and Screening Instructions click **Save** in the bottom left corner of the Edit Dataset screen.

➢   **NOTE**: From the Manage Datasets page, you can click on any Dataset you have created and edit any of the options in either the File Specification or Screening Instructions. To edit the File Specification click the Edit File Specification button, and to edit the Screening Instructions click on the name of the Screening Instruction.

➢   **NOTE:** If you add a second Screening Instruction to a Dataset it will screen against all available instructions. Each watch list can only be on one Screening Instruction.

15.1.4.   Configure Web Service Profile ID

Each dataset is automatically assigned a Web Service Profile ID that allows for either external Web Service calls or Automated Screening Lookups to import and screen new, and existing, data into the dataset. By default, the Web Service Profile ID is set to inactive.

ACCUITY

Activate or Deactivate a Web Service Profile ID

1. Click on Manage Datasets from the sidebar

2. Click on the dataset name

3. Click on the Web Service Profile ID hyperlink

4. Change the **Status** to Active or Inactive

5. Click on **Save**

Configure Allowed IP Addresses

Each Dataset Web Service Profile ID can limit which IP addresses are allowed to make calls to that particular datasets. For users that are importing and screening using the Automated Screening Lookup tool, the Allowed IP Addresses field should be left empty.

1. Click on Manage Datasets from the sidebar

2. Click on the dataset name

3. Click on the Web Service Profile ID hyperlink

4. Enter the IP Address in the free text field

5. Click on **Add** (Click on **Delete** to remove the IP Address from the allowed list)

6. Repeat steps 4 and 5 until all IP Addresses have been added

7. Click on **Save**

Configure Assigned User Groups

User Groups are used to determine which users can import and screen this dataset through the Automated Screening Lookup screen. Only users within groups assigned to the dataset and with the Automated Screening Lookup feature set will be able to import and screen.

To add User Groups:

1. Click on Manage Datasets from the sidebar

2. Click on the dataset name

3. Click on the Web Service Profile ID hyperlink

4. Select one, or multiple, user groups from the Available User Groups section

5. Click the single arrow, ">", to move the selected user groups to the Assigned User Groups section

6. Click the double arrow, ">>", to move all user groups to the Assigned User Groups section.

7. Click on **Save**

To remove User Groups:

1. Click on Manage Datasets from the sidebar

2. Click on the dataset name

3. Click on the Web Service Profile ID hyperlink

4. Select one, or multiple, user groups from the Assigned User Groups section

5. Click the single arrow, "<", to move the selected user groups to the Available User Groups section

6. Click the double arrow, "<<", to move all user groups to the Available User Groups section

7. Click on **Save**

ACCUITY

15.1.5.   Manual Full Dataset Screening

⊗ Edit Dataset

• = Required Field
Name: New Dataset Lookup •
Status: Active ▼ •   Last Updated: 08/10/2015 12:35:44 • DemoAdmin
☐ Retain Match Status when Input Record changes

Data Specifications: **Edit File Specification**

Format: Delimited   Delimiter: ,   Text Qualifier: "

Field Name	Sort Order	Unique Field	Data Type
Acct Number	1	Y	Customer Unique ID
Name	2	N	Name - General
DOB	3	N	DOB
Address	4	N	Unspecified
City	5	N	Unspecified
Country	6	N	Country Name

Screening Instructions: **Add Instructions**

All
Screening Fields: City (100), Name (100), Country (100)
Lists to Filter Against: US PEP List powered by WorldCompliance, PEP List powered by WorldCompliance, 314a, PLM Test List
Rules Pack: None   Custom Dictionary: None   Character Mapping File: Default   Risk Scorecard: None
Screening Options: None

Webservice Profile ID: eec9f16c-e88c-4043-ae4c-b93e8d1422ec (Active)

Save **Cancel**   ☐ Good File Migration **Screen**

If you would like to manually screen a full dataset against the full set of watch lists you can do so in the Edit Dataset screen. In the bottom right hand corner of the Edit Dataset screen click **Screen** run the full versus full screen.

Manual Full Dataset Screening can be a good way to get caught up on screening if any delta files have not been loaded correctly or if there have been any errors in the screening process. During the Manual Full Dataset Screening, Compliance Link will compare the matches against existing matches in the database, if the match already exists, a duplicate will not be written.

15.1.6.   Good File Migration

For users migrating their processes from Compliance Link's batch processing model to Automated Screening Manager, Good File Migration utilizes the existing Compliance Link Good File when performing a full versus full dataset screening.

When the Good File Migration checkbox is checked, Compliance Link will compare all matches occurring in Automated Screening Manager to the existing Compliance Link Good File. If the following elements are identical, then the match will be assigned the status of "Passed by Good File" and the Review Note of "Good File Migration" added to the record.

- Unique ID
- Entity ID
- Entity Version

Good File Migration should only be performed once for each dataset/file being moved from Compliance Link Batch to Automated Screening Manager, however it can be run multiple times if needed.

15.2. Import Datasets

1. Click Import Master Dataset under the Admin Functions heading in the Automated Screening Manager Module.

2. Choose a pre-existing Dataset from the dropdown box.

3. Choose the File you are screening against the Dataset.

➢ **NOTE:** The file name must be 50 characters or less.

4. Click Import

    ➢ **NOTE:** The Inactivate All Records in this File will allow you to inactivate records for a specific Dataset. For example, if you had customers who no longer you use your service, you could upload a batch of their names to the Dataset in which they appear and those records would become inactive.

5. After you click Import, your file will appear in the Import History with the Dataset used to screen against, the file name screened, the upload and processing time, the user who uploaded the file, and the adds, changes, and deletes to a particular file.

6. The Invalid heading shows any files that may have invalid records. Clicking on the number will produce a downloadable file containing all invalid records, also known as the bad file. Examine the downloaded file to detect the cause of the errors.

On occasion, a file does not match the File Specification under which it was processed. This can happen **1)** if the input file was created manually, **2)** if there is something unusual about the data in the input file such as embedded control characters, **3)** if the number of fields does not match the File Specification, or 4) an incorrect File Specification was chosen.

15.3. Notification Settings

Notification Settings allow you to configure email notifications when certain actions in Automated Screening Manager take place.

1. Click "Notification Settings" in the Automated Screening Manager Module. There are four types of Notification Settings that can be modified:

    a. Import Notifications: sends an email when every time an import file has finished.

    b. Watch List Update Notification: sends an email every time a Watch List has been updated.

    c. Screening Notifications: sends an email every time a screening against any list has occurred.

    d. Work Assignment Notifications: sends an email to each user when they have Assigned or Available Cases to review

ACCUITY

2. Select when you want email notifications sent:

   a. Import Notifications: Immediate or Once per Day

   b. Watch List Update Notifications: Immediate or Once per Day

   c. Screening Notifications: Immediate or Once per Day

   d. Work Assignment Notifications: Every (1, 2, 4, 8, 12, 24, 48, 72) hours

3. Enter the recipient email addresses for Import Notification, Watch List Update Notification, and/or Screening Notifications.

4. Click **Save** to save the changes or click **Cancel** to return to the previous screen.

15.4. Screening History

Screening History shows the full history of screening within your institution. It documents when screenings have occurred based on updates to datasets, watch lists, as well as manual screenings.

> ➢ **NOTE:** The Automated Screening Manager module is capable of having multiple threads run simultaneously and is dependent on your environment. Please refer to the Installation manual for more details.

Screening History

Search   * Good File Migration

ID	Dataset	Instruction	List Name	GWL Data	Input Data	Scheduled Date	Completion Date	Screened Version	Status
29470	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	F	F	08/14/2015 15:17:43	08/17/2015 11:57:14	20150805124409	Finished
28576	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	F	D	08/10/2015 11:44:38	08/10/2015 11:52:27	20150805124409	Finished
27593	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	08/05/2015 16:20:31	08/05/2015 16:23:04	20150805124409	Finished
27019	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	08/03/2015 21:20:09	08/03/2015 21:21:08	20150803181115	Finished
26826	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	07/31/2015 10:20:09	07/31/2015 10:20:31	20150731071145	Finished
25654	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	07/23/2015 21:20:59	07/23/2015 21:21:06	20150723175416	Finished
24917	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	07/21/2015 20:20:37	07/21/2015 20:21:05	20150721163551	Finished
21731	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	07/02/2015 17:21:17	07/02/2015 17:21:59	20150702123802	Finished
20239	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	06/24/2015 20:20:42	06/24/2015 20:21:51	20150624170915	Finished
18705	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	F	F	06/11/2015 19:39:28	06/11/2015 19:39:49	20150611100341	Finished
18615	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	06/11/2015 13:20:35	06/11/2015 13:21:40	20150611100341	Finished
18057	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	06/10/2015 17:21:11	06/10/2015 17:21:36	20150610141303	Finished
16858	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	06/04/2015 18:21:11	06/04/2015 18:21:58	20150604113648	Finished
16652	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	F	F	06/03/2015 10:47:18	06/03/2015 10:48:33	20150601114112	Finished
16600	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	F	D	06/03/2015 10:41:10	06/03/2015 10:41:37	20150601114112	Finished
16453	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	06/01/2015 14:20:37	06/01/2015 14:21:57	20150601114112	Finished
15123	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	05/22/2015 17:20:19	05/22/2015 17:20:47	20150522142519	Finished
15018	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	F	D	05/22/2015 11:29:32	05/22/2015 11:29:39	20150521140156	Finished
14498	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	05/21/2015 17:20:27	05/21/2015 17:20:51	20150521140156	Finished
12184	Demo Dataset	GWL Fuzzy	Accuity's OFAC List	D	F	04/28/2015 16:20:20	04/28/2015 16:21:20	20150428120859	Finished

Records 1-20 of 69 Total Records
1 2 3 4 ≥ >>

1. A unique **ID** will be automatically assigned to each time a screen is done against any list.

2. **Dataset** provides the name of the Dataset screened against.

3. **Instructions** provide the name of the Dataset that was screened against.

> ➢ **NOTE:** The Dataset in the Instructions is a hyperlink that will provide the Instructions from the Dataset at the time of the screening. If a Dataset is edited the hyperlink in the Instructions will not update. This will allow the User to know exactly how something was screened at the time of the screening, since Datasets will likely change over time.

4. **List** provides the name of the Global WatchList, Private List, or Commodity List screened against.

5. The **GWL Data** and **Cust Data** heading tell you whether it was a Full (F) or Delta (D) file that was screened.

6. Schedule Date provides the time that the screening began to process.

7. Completion Date provides the time that the screening completed.

8. **Screened Version** provides the version of the List that was screened. The number in the Screened Version correlates to the time in which the list was updated in the following format: year, month, day, hour, minute, second.

9. The following **Statuses** are available:
   - **New**: when a batch is created either because they manually submitted screening from the dataset, an update to the dataset occurred causing an automated batch screening, or an update to a list occurred causing an automated batch screening.

   - **Start**: when the batch is picked up by the thread and the screening parameters are read/checked that the batch is ready to go.

   - **Processing**: when the batch is being run.

   - **Failed/Error/Restart**: when Compliance Link is unable to complete the screening process the failed error message will appear. Jobs can be restarted by clicking the "restart" button. Some examples include, if the file specification changed and doesn't match the fields from the file or if a configuration issue exists for the system/database (intranet).

   - **Finished**: when the batch is done running, and results can be reviewed.

15.5. Workflow Configuration

15.5.1. Region Management

Automated Screening Manager allows for datasets and User Groups to be assigned to specific Regions. This limits what data users, even Automated Screening Case Admins, can see within Automated Screening Manager. User Groups assigned to a specific region will only be able to search for Input Records from datasets within region. If a User Group is assigned to All Regions, then they are able to see all data within all datasets.

To add Regions:

1. Click on Region Management from the sidebar

2. Click on **Add Region**

3. Enter the Name of the Region

4. Click on **Save**

To assign User Groups to Regions:

1. Click on Region Management from the sidebar

2. Select a Region from the dropdown for each User Group

3. Click on **Save**

16. ASM SUB-CASE TYPES

Master Datasets are used to store sets of input records to be screened on an ongoing basis. A Dataset is imported into ASM, screening instructions are set-up, a workflow is created and data is then screened. Cases are generated for input records after screening whether or not matches are produced. For the cases that have generated a potential match or matches, ASM will distribute those matches into Sub-case Types on the Case Review Screen. Currently, there are five default Sub-case Types added to every dataset (when created) that are used to organize case level matches.

Sub-case Type	Description
Commodity	The Commodity Sub-case Type or CWL will contain matches that are relevant to Dual use goods and commodity screening. **Example:** Match types CWL.
GWL	The GWL Sub-case Type will contain matches from all Accuity Sanctions or Global WatchLists. **Example:** Accuity OFAC Enhancements, HMT, etc.
Other	This Sub-case Type is maintained for all datasets as a catch-all. If a dataset has been set up in a way where matches do not have a sub-case Type to be placed in, those matches will be grouped here. **Example:** A dataset is configured with the PEP/EDD Sub-case Type only, but the screening instruction has the Accuity OFAC Enhancements list marked, any matches off that list will go into the "Other" Sub-case Type, until a GWL sub-case is configured to a Dataset by an Administrator.
PEP/EDD	The PEP/EDD Sub-case Type will contain matches from all Accuity PEP (Politically Exposed Person or Enhanced Due Diligence Lists). **Example:** US PEP List powered by WorldCompliance)
Private	The Private Sub-case Type will contain matches from all customer loaded private lists. **Example:** 314(a) List or any private list loaded.

Below is a look at an ASM Case (with matches) on the Case Review screen. Applicable matches are organized into the various Sub-case Type tabs.

A list of all Sub-case Types can be found on the Dataset Workflow Configuration screen. Sub-case Types are listed alphabetically by name and a description of each is displayed. Additionally, the table will only include the first ten Sub-case Types and a "**View All**" button is available to view all Sub-case Types (not pictured below).

17. CREATING NEW SUB-CASE TYPES

Sub-case Types can be created at an account level. Since Sub-case Types can be configured with any Dataset and Datasets can be restricted to certain user groups or regions, the adding and editing of Sub-case Types are limited to Administrators. Sub-case Type creation and editing is completed in the **Workflow Configuration** screen under the Admin Functions in the Automated Screening Manager.

17.1. Sub-case Type Creation:

1. Click the **Workflow Configuration** link from the sidebar (image above).

2. On the Workflow Configuration screen, select the **Add Sub-case** button located at the top of the Sub-case types table.

3. Clicking this will take you to the **Add Sub-case** screen.

4. Enter a name value. The **Name** field is a required field, that identifies the Sub-case Type. This field is limited to ten characters.

5. Enter a Sub-case Type description. The **Description** field is a required field that describes the Sub-case Type criteria. This field is limited to fifty characters.

6. Enter the **Sub-case Type Criteria**. This criteria will determine what type of matches a Sub-case Type will hold. The table below displays the three selection types available.

Criteria Type	Description
Match Type	Click the ✏ icon on the screen to open up the available match types. There are four standard Match Types: Commodity, GWL, PEP/EDD and Private. Selecting one or all of these will drive matches from all applicable WatchLists. **Example**: Selecting GWL and PEP/EDD will drive all matches from the GWL and PEP/EDD lists.
List Type	Click the ✏ icon to open the available lists for selection. You may select one or multiple lists. **Example:** Selecting the 314(a) list will drive all 314(a) matches into the Sub-case.
Source Code	Type a source code into the source code field. Source codes must be typed exactly like they are found in the list. Click the ✚ symbol to add more source codes to the criteria.
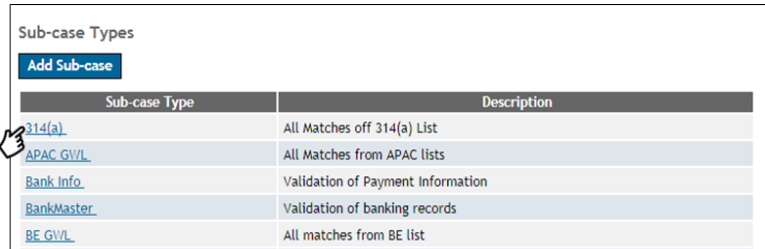
Note: The five default Sub-case Types <u>will not</u> be editable. However, the GWL, PEP/EDD, Private and Commodity Sub-case Types can be removed from any Dataset. The only Sub-case Type that cannot be removed from a dataset is "Other". Section 18 will describe how to configure (add or remove) a Sub-case Type to a Dataset.

Note: There is also a list of all of the Datasets that a Sub-case Type is assigned to (Assigned Datasets). It will only display once a Sub-case Type is configured to a Dataset.

7. Click the **Save** button when finished

17.2. Editing an Existing Sub-case Type

To edit an existing Sub-case Type, click the **Sub-case Type Name** highlighted in blue font. This will open up the **Edit** screen for the selected Sub-case Type where the user can modify the existing criteria. If changes are made to a Sub-case Type, Dataset re-calculation is required to successfully drive matches into the Sub-case Type.

Sub-case Type	Description
314(a)	All Matches off 314(a) List
APAC GWL	All Matches from APAC lists
Bank Info	Validation of Payment Information
BankMaster	Validation of banking records
BE GWL	All matches from BE list

Section 21 will describe how to re-calculate or re-assign a dataset.

18. CONFIGURING A DATASET'S SUB-CASE TYPES

All Dataset's (once created) will include the five default Sub-case Types (GWL, PEP/EDD, Private, Commodities and Other). Additional Sub-case Types that are created can be configured to any dataset. There is currently a configuration limitation of ten Sub-case Types per Dataset. Configuration is completed in the **Workflow Configuration** screen under the Admin Functions in Automated Screening Manager.

18.1. Sub-Case Configuration

To configure Sub-case Types for a Dataset

1. Click the **View/Edit** link under the **Sub-Case Configuration** column.

   Note: This is a necessary step to ensure that Cases in your Dataset have potential matches organized correctly.

2. This will bring you to the **Sub-case configuration** screen. The image below describes the features found on this screen.

ACCUITY

3. Click the **Configure Sub-case** link to add, remove and prioritize Sub-case Types for the dataset. Every Dataset will automatically be configured with the five default Sub-Case Types.

4. Select a new or existing Sub-case Types on the left (in the available Sub-case list) and click the [>] button to move it into the Dataset.

   Note: There is a limit of ten Sub-case Types allowed per Dataset. The "Other" Sub-case Type, cannot be removed from any dataset as it acts as a catch-all for all unsynchronized matches.
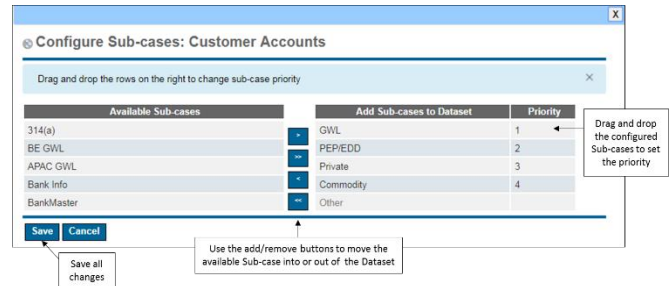
5. After the applicable Sub-case Types are added (or removed) to a Dataset, the Sub-case Type will need to be prioritized according to the needs of the user.

   Note: It is important to understand how Sub-case priority works. We always recommend that the five default Sub-case Types are left configured to all Datasets.
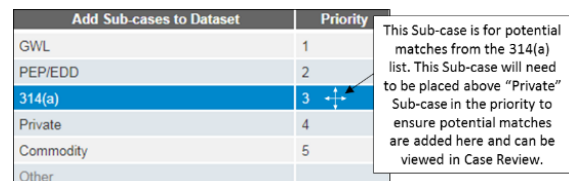
   Note: If custom Sub-case Types are created and added into a Dataset, they should be prioritized over the default Sub-case Types to ensure potential matches are organized correctly.

6. Click the **save** button when finished.

7. Once a Sub-case Type is added, prioritized and saved to a Dataset, it will display on the Sub-case Configuration screen. Ensure that all desired Sub-cases are present and in the correct order (left to right). If they are not, please re-configure any missing Sub-cases and ensure the **save** button is clicked.

8. The final step is to assign the Status Hierarchy for each Sub-case. Click the Sub-case Type tab at the top of the table to view and/or change the Status Hierarchy. There are six Sub-case Types in the example to the right. The 314(a) Sub-case Type is currently highlighted.
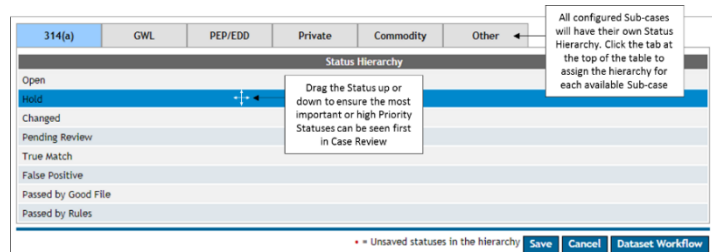
   Note: The "Other" Sub-case Type will always be prioritized last as a catch-all.

9. Drag and Drop the Status rows to set the hierarchy.

   Note: The "Sub-case Status Hierarchy" will determine the order in which the different types of Case Statuses, Match Types and Match Statuses (in particular) will be reviewed. Each Dataset will have its own unique Hierarchy to help prioritize the most important statuses for a particular Match Type to ensure the high-priority matches are reviewed first.

10. Click the **save** button.

19.   CONFIGURE A DATASET'S WORKFLOW

Each Dataset will have its own workflow custom tailored to the organization's needs. The workflow will allow the assignment of specific Sub-case Types to different User Groups in order to better separate the workload amongst the different groups reviewing a case.
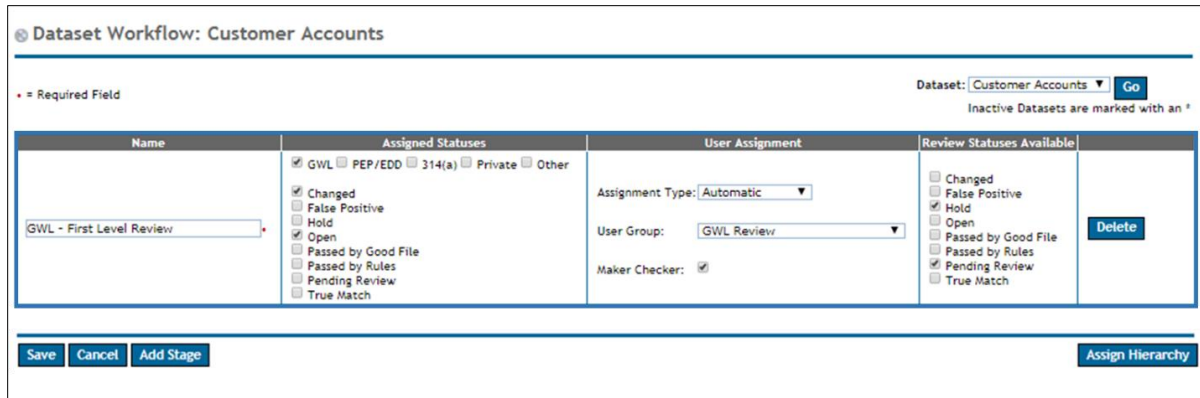
1. Click **Workflow Configuration** under the Admin Functions in Automated Screening Manager.

2. Click on the **View/Edit** link under Dataset Workflow for the Dataset you would like to configure. This will bring you to the Dataset Workflow screen. The following steps outline how to create a workflow in the Automated Screening Manager.
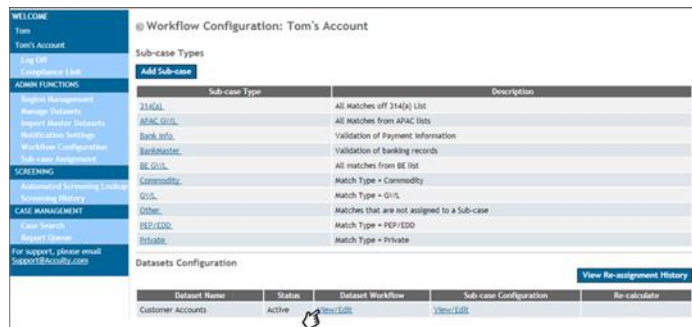
There are four values that are available for Workflow configuration.

Column Name	Description
Name	This represents the Name of the stage. It is currently limited to 30 characters.
Assigned Statuses	This column will include two values, the Sub-case Types that are configured to the Dataset (which are found horizontally at the top) and the assignment match statuses (listed vertically underneath the Sub-case Type values).
User Assignment	This column will include three values: Assignment Types, User Groups and Maker Checker. **Assignment Types:** 1. No Assignment: Any user within the institution with the proper review capabilities can view these cases. 2. Final: These cases have reached a final state and can only be accessed by Automated Screening Manager Case Administrators. 3. Automatic: Automatically assigns an even amount of Cases to each User within a User Group. 4. Sign Out: Once a User accesses a Case it becomes assigned to them and all others non-admin users will be locked out. **Note:** Only the assigned User and Administrators will be able to access cases that are assigned to a user. **User Group:** All of the available User Groups will be found here in a drop down. The same group can be used for different Sub-cases and different stages. **Maker/Checker:** This option allows the user that last reviewed/created the Sub-case to not review the match again. This is commonly referred to as a "four-eyed" review and can be used to have multiple users within the same User Group validate each other's work.
Review Statuses Available	This column will include all of the available review statuses that the assigned user group are limited to for disposition (at a paticular stage).

ACCUITY

3. **Name** the Stage

4. Check the **Sub-case Type(s)** (GWL, PEP/EDD, etc.) relevant to the Stage.

5. Check the **Assigned Status(es)** of the Stage.

   Note: The User Group selected to review this Stage of the Workflow will only be required to review Cases with the Assigned Statuses chosen.

6. Choose the **Assignment Type** and **User Group** assigned to the Stage.

7. Check **Maker/Checker** if this option should be used when Sub-case Types enter this workflow stage.

8. Select the **User Group** that will review the Cases in this Stage of the Workflow (for Automatic and Sign Out only).

9. Select the **Review Statuses Available** for this Stage. These Review Statuses determine what status a user can mark a match in this stage. In the above example, any case with the status of GWL-Open or Changed will only be able to be changed to Hold and Pending Review. None of the other match statuses will be available to the reviewing user (during disposition in Case Review).

10. Click **Add Stage** in the bottom left corner of the Configure Workflow screen to add another Stage to the Workflow.

11. If you would like to create or change the Hierarchy for a Dataset click the Assign Hierarchy button in the bottom right corner.

    Note: More information on Assigning Hierarchies can be found in the Sub-Case Type Configuration portion of this manual.

12. After you have configured all Stages of a Dataset's Workflow, click **Save.**

    Note: If you edit your Workflow for a particular Dataset the changes will apply for all screenings going forward, but will not retroactively reassign all matches that may still be outstanding from previous screens. You will have to Re-calculate the Dataset to ensure that historical matches are re-assigned. Section five will describe how to re-calculate or re-assign a dataset.

20. DATASET WORKFLOW RE-ASSIGNMENT

In order to ensure that the application is accurately assigning potential matches or hits to the correct Sub-case Type and following the Dataset workflow correctly, the Dataset Re-assignment feature will allow Admins to re-calculate a Dataset due to any adhoc changes (without rescreening).

This Re-assignment should be completed after the following scenarios:

1. A new sub-case Type is created and configured to a Dataset.

2. A Sub-case Type is re-prioritized in a Dataset.

3. A change to the status hierarchy for a Sub-case Type is made.

4. Any Dataset workflow changes are made.

20.1. Re-calculating a Dataset

The following steps must be completed for dataset re-assignment:

1. Click **Workflow Configuration** under the Admin Functions in Automated Screening Manager.

2. A note on the screen will appear if a Dataset needs to be re-assigned.

3. You may choose to click the **Re-assign All** link, which will re-assign all datasets applicable, or you can re-assign single Datasets by clicking the **Submit** link in the re-calculate column.

4. A pop-up modal will appear for the admin to confirm the re-assignment action.

5. When submitting a Dataset for re-assignment, the Dataset Re-assignment history table will display the re-assignment processes and their stage. Dataset re-assignment processes can be canceled on the history screen, if further changes are required or the action needs to be canceled.

   Note: Inactive datasets cannot be re-calculated.

20.2. Dataset Re-assignment error scenarios

Please review the following section that describes error scenarios and more context into Dataset re-assignment.

20.2.1.   Re-assignment due to Workflow changes

If there are any changes to the Dataset workflow (new Stage, new User Group, new Sub-case Type, etc.), those changes will be reflected for ongoing screening and new screening only. If the Admin would like to re-assign all cases (specifically the Sub-case Types) to reflect the current or updated workflow, the admin will need to re-calculate the dataset. Upon re-assignment, Sub-case Types that are currently assigned to users may be assigned to a different user in that group.

For example, if a new user is added to a group and the admin would like to distribute Sub-case Types automatically to that user, upon dataset re-assignment all Sub-case Types at any given stage will be re-assigned to any users in a group based on workflow configuration settings.

Note: When a dataset is being re-calculated, the editing of the workflow configuration will be locked. A message indicating this will be displayed on the Dataset Workflow page and the save buttons will be removed.

20.2.2.   Re-assignment due to Sub-case Type changes

If a new Sub-case Type is added to a dataset or if a Sub-case Type is re-prioritized in a dataset, the Admin will have to re-calculate the Dataset to ensure that matches are driven into the Sub-case successfully. Before doing this, The Sub-case Type should be prioritized and the Dataset Workflow should be set up accordingly first.

For example: If a new Sub-case Type is created for 314(a) screening, the 314(a) Sub-case Type must be added to the dataset in the Sub-case Configuration screen and prioritized above the "Private" Sub-case Type. Upon Dataset Re-assignment, all matches applicable to 314(a) will be moved out of the Private Sub-case Type and pushed into the new 314(a) Sub-case Type.

Note: When a Dataset is being re-calculated, the editing of a Sub-case Type (applicable to the Dataset) will be locked for editing. A message indicating this will be displayed on the Add/Edit Sub-case page and the save buttons will be removed.

20.2.3. Unsynchronized Cases/ Sub-case Types

Cases (specifically Sub-case Types in a case) can become unsynchronized when the two following scenarios occur:

1. A case in inactive and,
2. An applicable Sub-case Type for the inactive case was removed from the Dataset's configuration
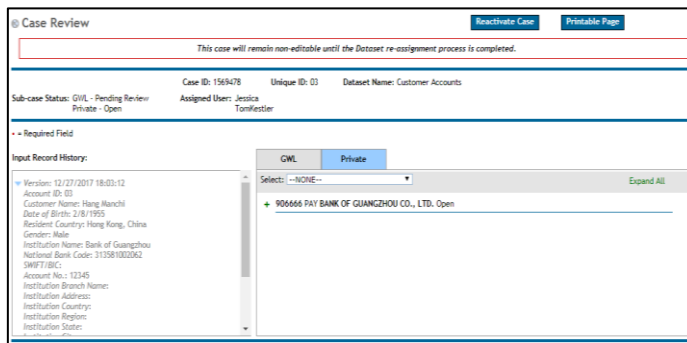
21. REVIEWING AND ASSIGNING CASE STATUSES

21.1.1. Case Review
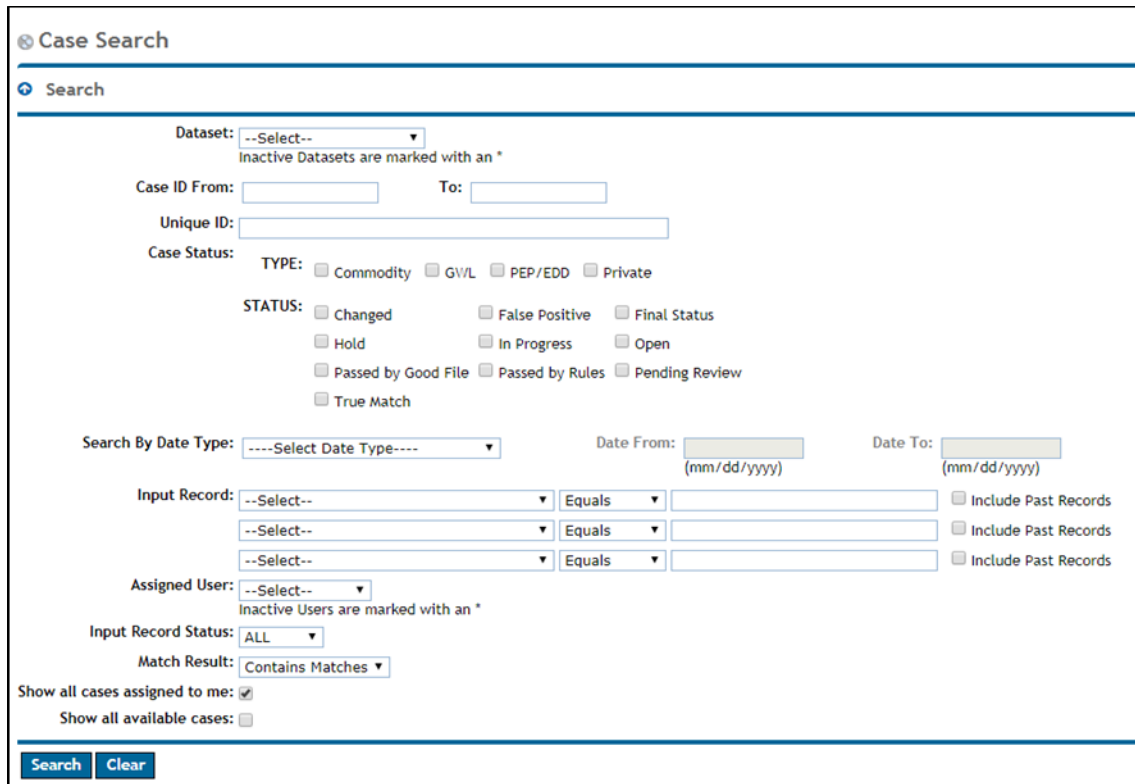
There are two ways to review your Cases within Automated Screening Manager:

1. Click Case Search under the Case Management heading in Automated Screening Manager

2. Click the hyperlink of the amount of Cases you have available for review in your Inbox from the Compliance Link home screen. This will take you directly to you inbox where you can review assigned or available Cases.
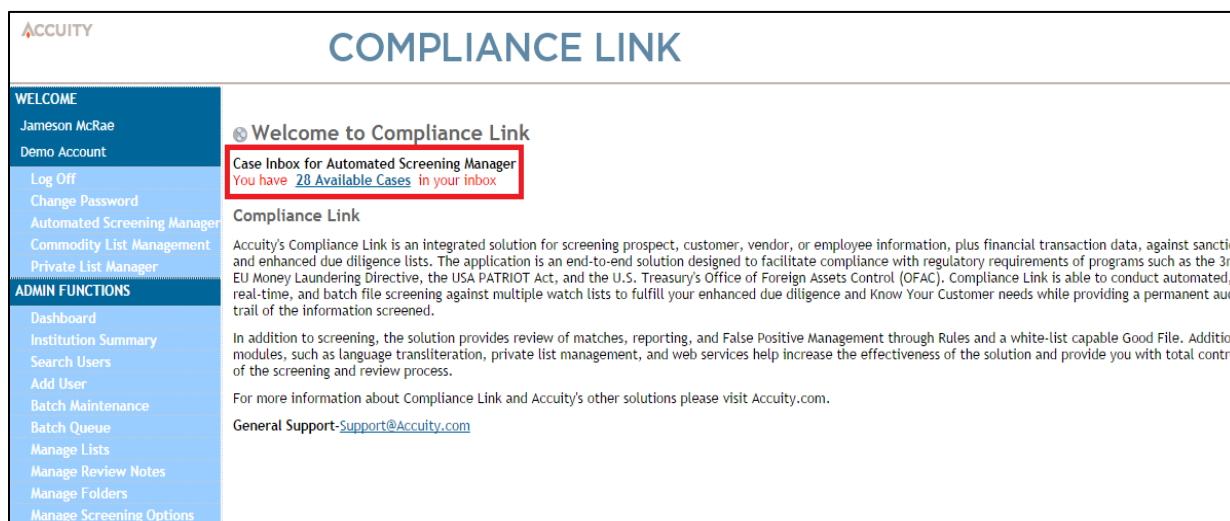
21.1.2. Case Review Search

1. Click the **Case Review** link in the sidebar under Case Management.

2. Search for Matches by one or more of the following criteria:

    a. A specific **Dataset** (from the dropdown list)

    b. A specific Case or a range of Cases (Case ID)

    c. Unique **ID** (from the Input Record)

    d. Case Type (Commodity, GWL, PEP/EDD, Private)

    e. **Case Status** {Changed, False Positive (Good), Hold, Open, Passed by Good File, Passed by Rules, Pending Review, True Match (Blocked), as well as any custom match statuses}

    f. Input Record created or updated date (by providing a date range and record type)

    g. Up to 3 **Input Record Fields**

    h. Check "Include Past Records" to search for inactive Input Record versions. If left unchecked, only the most recent versions will be searched

i. Assigned User (User ID)

j. Customer Status (Active or Inactive)

k. **Match Results** (ALL, Contains Matches, or Contains No Matches)

l. **Show all Cases assigned to you**

m. **Show all available Cases**

3. After you have chosen your Case Search criteria click Search. The results of your search will appear with the following:

a. The **Dataset** in which your Case appeared

b. The **Unique ID** from your Input Record to help identify a specific Case

c. Whether the customer is Active or Inactive via the **Customer Status**

d. A **Record Sample** that shows the Unique ID and screening fields up to 50 characters of the Input Record.

e. **Case Status** shows the aggregated status of all of the matches against an Input Record based on status hierarchy.

f. **Assigned User** is displayed with their User ID present.

g. Input Record version (Date)

21.2. Sub-case Re-assignment

Users with the ASM Case Admin feature set are able to re-assign Sub-cases from user to user.

To assign Sub-cases:

1. Click on Sub-case Assignment in the sidebar

2. Search for Sub-cases using the available criteria

3. At the bottom of the Case Search screen you can Assign Selected Results or Assign All Results from a specific Case Search to a certain User via the dropdown list.

   ➢ **NOTE:** To Assign Selected Results to Users select the checkbox next to a particular Case, choose the User from the dropdown list, and click Assign Selected Results.

21.3. Review a Case

1. Click the **Unique ID** associated with the Case you would like to review.

2. High level information will be provided at the top of the screen. This includes the Dataset Name, Case ID, Unique ID (of the input record), Sub-case Status(es) and the assigned user.

3. If a specific Case has matches against multiple Types of Lists then multiple tabs will occur (called sub-cases). Click on tab with the List name that you would like to review. The List names are as follows:

    a. Global WatchList (GWL)
    b. Politically Exposed Persons (PEP)/ Enhanced Due Diligence (EDD)
    c. Commodity (CWL)
    d. Private

4. The input record and input record history will be provided on the left side of the screen. This displays all fields available for this record and a view of previous version (based on changes made to the record)

5. Assign a **Match Status** from the dropdown list.

6. Review all the potential matches within the Case and click the checkbox(s) on the particular Entity(ies) that you would like to make a Status decision on. When a checkbox is selected, drop downs will be provided to change the status and provide review notes.

7. Entities/matches will be sorted based on their Case Hierarchy status and then their Risk Score. Cases with a green arrow are considered to be "Passed by Rule."

8. Click the **green (+) sign** to unwrap more Entity Information in the Case Review Screen.

9. You can expand all matches in a case by clicking the "expand all" button. You can then collapse all matches by clicking the "collapse all" button.

10. There is a selection box provided to select similar match statuses for bulk dispositioning.

11. Each match will highlight what was matched between the input record and the entity. By clicking the highlighted portion in the match review, you can see more information. This functionality may be limited when "expand all" is clicked.

12. Matches are grouped by entity. If an entity is on multiple WatchLists, sources will be referenced together.

13. There is also a reference of the Entity history (within the match information) that details a history of any changes that were made.

14. You can make attachments to a Case by clicking Choose File at the bottom of a Case. You are able to attach a Word document, Excel spreadsheet, JPEG, and many other file formats. The attachment will be stored in the Audit Trail and attached to the match after it is saved.

15. You can add a pre-configured **Review Note** from a dropdown list or enter a custom Review Note in the text box. (Optional)

16. After reviewing and updating the match the following options are available:

    a. Click on **Save** to save the updated status(es) and reload the case.

    b. Click on **Cancel** in the bottom right hand corner of the Case Review screen to return to the Case Search results screen without saving your changes.

    c. Click **Next** in the bottom right hand corner of the Case Review screen to move to the next Case Review.

➢ **NOTE**: If you do not **Save** the changes made on your Case before clicking **Next** then they will not be saved.

ACCUITY

Case Review Screen

21.4. Printable Page

At the top right corner of the Case Review screen, a user can format the case for printing. This will open a new tab, or browser, with the formatted case information.

21.5. Audit Trail

At the bottom of each Case Review a full Audit Trail for your Screening History will appear The Audit Trail have a record for each time this input record was screened and/or changed by data import. The Audit Trail contains the following information:

1. The **Date** in which the Audit Trail changed.

2. The **Activity** for the change in the Audit Trail, options include: Screening (Input Record Change), Screening (Watch List Change), and Input Record Change.

3. The specific **List Name** that the Case appeared on or the List that changed.

4. **Full/Delta** shows whether the screen was performed against a delta (add/change) or full watch list.

5. **Instructions** provide the name of the Dataset that was screened against.

   ➢ **NOTE:** The Dataset in the Instructions is a hyperlink that will provide the Instructions from the Dataset at the time of the screening. If a Dataset is edited the hyperlink in the Instructions will not update. This will allow the User to know exactly how something was screened at the time of the screening, since Datasets will likely change over time.

6. The **Version** of the list screened against. The number listed under Version provide the date of the List from the Version was updated, it appears in the following format: year, month, day, hour, minute, second.

Screening History:

Date	Reason	List	Full/Delta	Instruction	Version
09/29/2014 10:28:22	Watch List Change	Dave Test	Delta	PWL Screening	20140929090310
09/29/2014 10:24:20	Customer Data Change	Dave Test	Full	PWL Screening	20140908092344
09/29/2014 10:24:19	Customer Data Change	Accuity OFAC Enhancements	Full	Sanctions Only	20140902191929
09/29/2014 10:24:18	Customer Data Change	BofE	Full	Sanctions Only	20140822114306
09/29/2014 10:24:17	Customer Data Change	AU	Full	Sanctions Only	20140627151602
09/29/2014 10:24:16	Customer Data Change	Accuity's OFAC List	Full	Sanctions Only	20140902191038

Show Full Audit Trail

Cancel   Next

21.6. Previous Case Search

Start by clicking Previous Case Search under the Case Search tab in Automated Screening Manager. This will allow you to quickly access all of your previous Case Searches. This search has all of same functions as the Case Search screen.
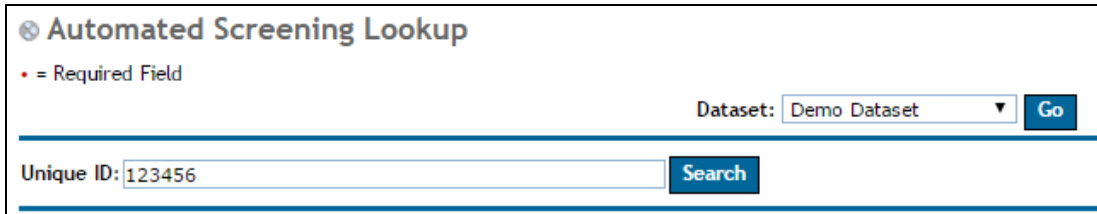

22. AUTOMATED SCREENING LOOKUP

The Automated Screening Lookup allows for users to search for existing data within a dataset, as well as, import/edit and screen new, or existing, input records manually through the interface. Access to the Automated Screening Lookup screen is determined by the feature set, Automated Screening Lookup, and the User Groups assigned to the dataset from the Manage Datasets screen.

Search for Existing Records

1. Click on Automated Screening Lookup from the sidebar
2. Select the dataset from the Dataset dropdown. If you have access to one dataset, no dropdown will appear.
3. Enter the Input Record's Unique ID in the top section of the screen
4. Click on **Search**

5. If the Input Record exists in the dataset, the fields will be populated with the existing record, if not, an error message
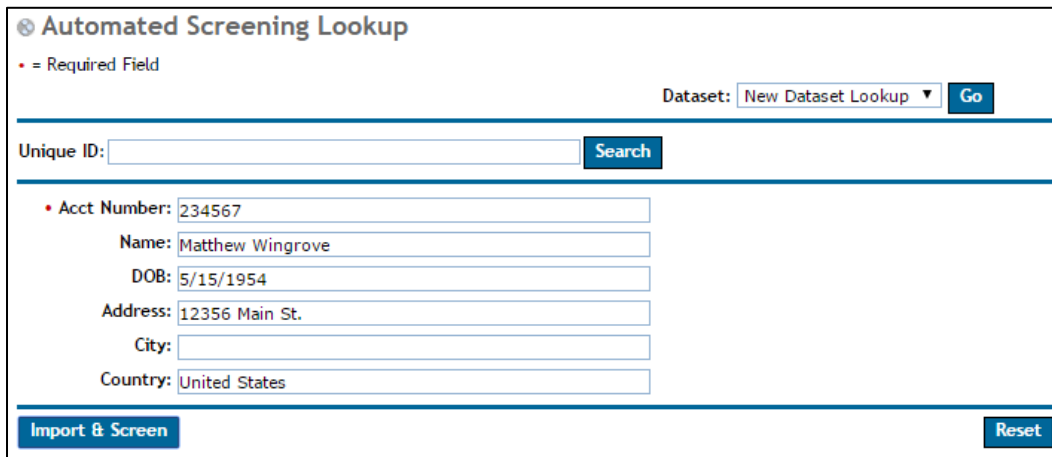

Import and Screen Data

1. Click on Automated Screening Lookup from the sidebar
2. Select the dataset from the Dataset dropdown. If you have access to one dataset, no dropdown will appear.
3. Enter the information in the available fields
4. Click on **Import & Screen**

ACCUITY

Reviewing Cases

All cases created through the Automated Screening Lookup screen will go through the same workflow for file import and automated screening records. Depending on the Case Assignment, the lookup user may, or may not, be able to access the case. If they have access, a hyperlink that will take them to the Case Review screen will appear in the Response section.

⊗ **Automated Screening Lookup**

• = Required Field

Dataset: [New Dataset Lookup ▼] [Go]

Unique ID: [ ] [Search]

• Acct Number:	234567
Name:	Matthew Wingrove
DOB:	5/15/1954
Address:	12356 Main St.
City:	
Country:	United States

[Import & Screen]   [Reset]

⊗ **Response**

Case ID: 155184   Unique ID: 234567   Dataset Name: New Dataset Lookup   Assigned User: N/A - Unassigned   Case Status: - No Matches

User Name	User Group	Screened Date	Screening List(s)
Demo Admin	Test	08/19/2015 12:15:52	US PEP List powered by WorldCompliance PEP List powered by WorldCompliance 314a PLM Test List

23.   ERRORS

All errors will be displayed at the top of the current screen and surrounded by a red box. One example below: