precisely

Spectrum Screener

User Guide

Version 2020.1.0

Table of Contents

1 - Getting Started

In this section

A First Look at Screener

Screener is a comprehensive screening solution to help banks and financial institutions to step up to a cost-effective compliance. It helps in:

- Reducing false positives
- Improving compliance
- Managing sanction lists
- Boosting productivity of the entire team

Watchlists are the key to prevent financial crimes. However, when it comes to screening, bad data and bad matches result in a stream of false positives leading to costly and wasteful investigations.

Screener comes in handy here. Behind the user-friendly interface of the application are robust features working in absolute tandem to add data quality, list management, and much needed transparency to avoid false negatives, reduce false positives, and resolve alerts faster. Screener also integrates seamlessly with your case management system. It manages internal and external lists along with the entries in those lists. It also version the lists and the entries. Screener can either screen parties (customers/prospects) against those lists, or can disseminate the lists (Precisely Services) to a screening system.

Some of the features that makes Screener stand out are:

Entity Resolution

Screener reconciles customer data across different systems and formats to overcome variance and create an accurate view.

- It normalizes and standardizes names and addresses.
- Accounts for name variants, gender and cultural differences.
- Enriches missing, misfielded or incorrect country codes.
- Enriches customer profiles. Produce a streamlined view for screening.

List Management

Screener consolidates and reconciles lists and watchlists. It aggregates list entries from multiple data vendors, reduces duplication and increases list quality. The list management feature helps you:

- Automate list importing and archiving processes.
- Aggregate list entries from multiple data vendors.
- Enable global or, local, centralized and distributed administration.
- Apply robust entity resolution across internal and external lists.
- Automatically assign globally unique identifiers (GUIDs) for efficient identification and matching.

- Produce a fully auditable, streamlined list for screening.

Screening

Screener has a fully integrated matching engine that identifies which cases need to be reviewed. It provides a transparent view of the data lineage and audit trail.

- Matches parties (customers, counterparties, employees, vendors, and more) with list members and negative media candidates.
- Generates clear, easily accessible data lineage and audit trail.
- Transparently provides alert context to investigators.

Generating alerts

Screener consolidates and prioritizes every event, automatically closing those that don't require any action.

- Introduces new efficiencies prior to case management.
- Automates closure and audit history of common alerts according to your rules.

Secured Entities

Secured entities are:

- Lists – Metadata about a list and the set of entries within a list
- List Entries – Individual records containing information about a person or organization.
- Screener Groups – A group of lists to screen parties against.
- User Defined Attributes (UDAs) – Extra information that an organization wants to add to any of the above secured entities.

> **Note:** Parties (the banks customers and prospective customer that need to be 'sanctions screened') are not Secured Entities in Screener.

Permissions and Access Control

You can manage the permissions and controls for accessing the Screener features through the **System** menu option of **Management Console**. You can grant accesses at a granular level as well, such as specific lists.

Installing Screener

Your installation will fall in one of these scenarios.

1. This is the first time you are installing the Spectrum Technology Platform and configuring Screener. See section **Installing Screener for the first time** on page 6.
2. You need to upgrade to the latest version of Screener without losing any of your previous data. See the section **Upgrading Screener** on page 9.

Installing Screener for the first time

This section guides you through the steps for installing the Spectrum Technology Platform and running the script to set up **Screener** for the first time.

1. Install the Spectrum Technology Platform. For steps on installing the server, see **Installing a New Server** section of the **Installation Guide**.

   Note: When prompted to choose the modules, ensure that you select all these:

   - Data Stewardship
   - Data Integration
   - Context Graph
   - Screener
   - Universal Addressing
   - Universal Name, Data Normalization, and Advanced Matching

2. Stop the Spectrum server and run the **Data Normalization** database utility. Select **Advanced Transformer** and enter this path for the source folder: `<SpectrumLocation>/server/modules/fcc/FCC_Repo/setup/baseTables`. Repeat this step by selecting **Open Parser** and **Table Lookup**.

   Note: For information about database utility, see *Installing Advanced Matching Database* section of the *Installation Guide*.

   Note: For Linux, you must stop the server prior to importing base tables. For more information, see *Installing Data Normalization databases* section of the *Linux Install Guide*.

3. Configure these properties in the `fcc.properties` file here: `<SpectrumLocation>\server\modules\fcc\fcc.properties`

   a. The base path where the List Import/Export files are created: `fcc.spectrum.list.job.base.path`

b. FCC Repo base path: `fcc.spectrum.base.path`
c. The polling directory for list ingestion: `fcc.spectrum.list.job.poll.dir`
d. Upload path for Attachments: `fcc.spectrum.attachments.upload.path`

4. Start the Spectrum server and import the Spectrum Technology Platform license key. For more information, see **Installing a License Key** in the Installation Guide.
5. Deploy the SPD files for Spectrum data sets (UAM-US, UAM-CAN, Loqate) to the server here : `<SpectrumLocation>\server\import`.

   Note: If you do not deploy the SPDs to import directory, that is, if you do not have SPD files, you will be prompted to provide the base paths for respective data bases while running the setup script. See step 8 below.

6. Ensure these pre-requisites are met before you run the set-up script.

   - JDK 8+ is installed and JAVA_HOME environment variable is set accordingly.
   - *jar* command is running fine from command line.

     Note: To verify, open the **Command Prompt** and enter *jar*. If you see *Command not recognized* message, add the JDK/bin path to *Path* environment variable. Verify the jar command again in a new Command Prompt.

   - For Windows system, powershell and other commands, such as xcopy and findstr, which are contained in C:/Windows/System32, are working fine.

     Note: Type these commands in the Windows command prompt, and in case you get the error: *Not recognized as an internal or external command*, append the paths for powershell (`C:\Windows\System32\WindowsPowerShell\<versionNo>`) and System32 (`C:\Windows\System32`) to the Path environment variable.

7. Set up these configurable properties in the `screener_setup_win.txt` file for Windows and `screener_setup.txt` file for Unix systems at: `<SpectrumLocation>/server/modules/fcc/FCC_Repo/setup/cli`.

   a. **host:** Machine where the Spectrum Technology Platform Server needs to be setup is running.
   b. **port:** Port on which Spectrum Technology Platform is running
   c. **user:** Spectrum Technology Platform User, should be an *administrative* user
   d. **password:** Spectrum Technology Platform Password

8. Run the set-up script (*ScreenerSetup.bat* for Windows systems and *ScreenerSetup.sh* for Unix systems.

   Note: For Solaris and AIX platforms, automated scripts are not supported. In these cases, you can only manually install the Screener setup.

   - For Windows systems:

     a. Run Command Prompt as Administrator

b. Change directory to location of the script (`<SpectrumLocation>\server\modules\fcc`)
c. Run the script

- For Unix systems:

a. Go to the folder where the script is placed:
`<SpectrumLocation>\server\modules\fcc`
b. Run the script.

The script performs these tasks:

a. Installs your custom tables and open parser domains
b. Imports match rules and flows
c. Creates database resources
d. Creates graph metadata model
e. Creates list and party search indexes
f. Runs the flow to load graph **FCC_METADATA** model with basic data which is required to run **Screener**

Note: To run the Unix script, you need to have appropriate permissions.

9. If you have not already deployed the Spectrum dataset SPDs, the script prompts you for the same. In case you do not have SPDs enter the base DB path instead. For example,

```
"LOQATE folder not found."
No Vintage found for LOQATE.
Enter base DB path for LOQATE or deploy the SPD and copy the exact
vintage name here:
```

10. If multiple vintages are installed for any of the dataset types, the script lists the vintage names with count, and prompts you to provide the exact vintage to be used.

```
"C:\Program
Files\Precisely\Spectrum\Server\ref-data\Universal_Addressing_Module
\c1p\UAM-US_JAN2019\UAM-US\metadata.json"
"VINTAGE NAMES" - JAN2019 JUN2018
VINTAGE COUNT 2
2 VINTAGE for UAM US - JAN2019 JUN2018
```

11. **Invoke the Screener Secured Entity Manager and List Ingestion Utility Manager:**

a. To synchronize secured entities such as **ListType**, **List**, and **Party Group**, invoke the **Screener Secured Entity Manager** through **JMX Console** using these steps:

1. Go to `http://`*`server`*`:`*`port`*`/jmx-console`

Where *server* is the server name or IP address of your Spectrum Technology Platform server and *port* is the HTTP port. By default, the HTTP port is 8080.

2. Log in using your credentials.
3. Search for **Screener Secured Entity Manager**, and click the ScreenerSecuredEntityManager link. The **Screener Secured Entity Manager** page is displayed.
4. Of all the operations displayed, invoke **refreshSecuredEntities** operation.
5. Close the page when you receive the **Invocation successful** message.

b. Invoke the **List Injestion Utility Manager** through **JMX Console** using these steps:

1. Go back to All MBeans (upper right hand corner). Search for **List Injestion Utility Manager**, and click the ListInjestionUtilityManager link. The List Injestion Utility Manager page is displayed.
2. Of all the operations displayed, invoke `autoRestartPoller` operation.

12. Configuring a Mail Server using the **Management Console**: This is mandatory for enabling **Screener** to send out mail alerts to you. For steps on configuring, see *Configuring a Mail Server* section in the **Administration Guide**.

> **Note:** To map users who will be notified of list ingestion through file, go to the `fcc.properties file` at this path: `<Spectrum_Installation_Location>\server\modules\fcc`, and map the users in the `fcc.spectrum.list.ingestion.email.roles.configurable` property.

Upgrading Screener

This section guides you through the process of upgrading **Screener** from version *18.2* (patch *2018.2 O08* installed) to version *19.1*.

> **Note:** It assumes you have the Spectrum Technology Platform installed and these modules selected while installing. For steps on installation see **Installing a New Server** section of the **Installation Guide**.
>
> - Data Stewardship
> - Data Integration
> - Context Graph
> - Screener
> - Universal Addressing
> - Universal Name, Data Normalization, and Advanced Matching

Steps for Upgrade

1. Stop the Spectrum Technology Platform server.

a. For Windows system: Right-click the Spectrum Technology Platform icon in the Windows system tray and select Stop Spectrum. Alternatively, you can use the Windows Services Control Panel and stop the Precisely Spectrum Technology Platform service.
b. For Unix systems: Run the `<SpectrumLocation>/server/bin/server.stop` script.

2. Back up this folder to a different location: `<SpectrumDirectory>\server\modules\hub\db\model.FCC_METADATA`.
3. Run the current version of the installer.
4. Configure these properties in the `fcc.properties` file here: `<SpectrumLocation>\server\modules\fcc\fcc.properties`

   a. The base path where the List Import/Export files are created: `fcc.spectrum.list.job.base.path`
   b. FCC Repo base path: `fcc.spectrum.base.path`
   c. The polling directory for list ingestion: `fcc.spectrum.list.job.poll.dir`
   d. Upload path for Attachments: `fcc.spectrum.attachments.upload.path`

5. To import the model successfully, set `dbms.allow_upgrade=true` in the `neo4j.properties` file at this location: `<SpectrumLocation>\server\modules\hub\db`. Comment out this property after completing the import.
6. Set up these configurable properties in the `screener_setup_win.txt` file for Windows and `screener_setup.txt` file for Unix systems at: `<SpectrumLocation>/server/modules/fcc/FCC_Repo/setup/cli`.

   a. **host:** Machine where the Spectrum Technology Platform Server needs to be setup is running.
   b. **port:** Port on which Spectrum Technology Platform is running
   c. **user:** Spectrum Technology Platform User, should be an *administrative* user
   d. **password:** Spectrum Technology Platform Password

7. Run the upgrade script (*ScreenerSetupUpgarde.bat* for Windows systems and *ScreenerSetupUpgarde.sh* for Unix systems).

   - For Windows systems:

     a. Run Command Prompt as Administrator
     b. Change directory to location of the script (`<SpectrumLocation>\server\modules\fcc`)
     c. Run the script

   - For Unix systems:

     a. Go to the folder where the script is placed: `<SpectrumLocation>\server\modules\fcc`
     b. Run the script.

     Note: To run the Unix script, you need to have appropriate permissions.

8. Resolve errors, if any, till the upgrade is complete.

Accessing Screener Home Page

To access Spectrum Technology Platform **Screener**, perform these steps:

1. Open a web browser.
2. Go to: `http://Server:Port/fcc`.

   Where *server* is the server name or IP address of your Spectrum Technology Platform server and *port* is the HTTP port. By default, the HTTP port is 8080.
3. Enter your credentials, and Sign in

2 - Managing Configurations

In this section

Maintaining Approval Rules

The approval rules to be applied on the **UDAs**, **Lists**, **List Entries**, and **Screener Groups** are managed using the **Configuration** tab of Screener. These rules define the review process.

Note: Only admin users can maintain the approval rules.

You can:

- Add a new approval rule
- View an existing approval rule
- Update an existing approval rule
- Delete an approval rule
- Enable or disable a rule

Create an Approval Rule

1. On the **Screener** main menu, click **Configurations**.
   The **Configuration** page is displayed.
2. Click the **Approval Rules** tab.
3. Click the **Add approval rule** + icon.
   The **Add Approval Rule** page is displayed.
4. Enter the **Name** of the rule.
5. From the **Applies to drop-down** list, select if the rule applies to a `Lists`, `UDAs`, `List Entries`, `Screener Groups` or all of these.
6. Specify the **Number of levels** of approval for the rule.
   The selected number of levels are displayed below the field. For example, if you have selected three levels three rows are displayed for specifying the name of the level, if it is a reviewer or approver, and the role assigned to the approving level.
7. For each of review or approval level, specify these details:
   a. Level Name
   b. Select the approval status, this status is derived from the **Workflow Status** UDA. The predefined values are `Review` and `Approve`. However, you can modify the **Workflow Status** UDA to conform to your organization's requirements. For more information about maintaining UDAs, see **Maintaining User Defined Attributes** on page 14.
   c. The role of the approver or reviewer. The drop-down displays values based on the defined **List Management Roles**.

8. Click **Save**.
   The rule is saved and added to the list of rules.
9. To enable or disable a rule, toggle **Enable** in the list of rules.

   Note: If a rule attached to any entity is disabled, the entity will not undergo any approval stage and will get auto approved.

   Note: Only one rule can be applied to an entity.

Modify details of an Approval Rule

1. On the **Approval Rules** tab, select the check-box of the desired rule and click the **Edit approval rule** icon.
2. Make necessary modifications to this rule and click **Save**.

View an existing Approval Rule

You can view an existing approval rule.

1. On the Screener main menu, click **Configurations**.
   The **Configuration** page is displayed.
2. Click the **Approval Rules** tab.
3. Select the check-box of the approval rule you wish to view
4. Click the **view approval rule** icon.
   The **View Approval Rule** page is displayed.

Maintaining User Defined Attributes

The *user defined attributes* (UDA) which can be applied on the **Lists** and **List Entries**, and **Screener Group** are managed using the **Configuration** tab of Screener. You can perform these operations:

- Add a new user defined attribute
- View an existing user defined attribute
- Update an existing user defined attribute
- Delete an approved user defined attribute
- Enable or disable user defined attribute

Create a new User Defined Attribute

1. On the Screener main menu, click **Configurations**.
   The **Configuration** page is displayed.
2. Click the **User Defined Attributes** tab.
3. Click the **Add user defined attribute** + icon.
   The **Add user defined attribute** page is displayed.
4. Enter the name of the attribute in the **Name** field.
5. From the table displayed below the *UDA* name, select these check-boxes for **Lists**, **Screener Groups**, and **List Entries**:
   - **Applies To**: Select this check-box to make any *UDA* applicable for any list, Screener group, or list entry.
   - **Always Show**: On selecting this check-box, the UDA would be available while creating or editing list, Screener group, or list entry.
   - **Value Required**: If you select this check-box, you would be required to provide a UDA value while creating or modifying a list, list entry, and screener group.
6. Use the **Value options** field to add values for a *UDA* and click **Add**.
   The added valid value is displayed below the **Value options** field; the selected option will be considered as a default value. If no value is specified, you can enter any value during creation of list, list entry, and screener group.
7. Use the **Comments** text box to add relevant comments. These comments will be visible to all users who can view the UDA on the **Configuration** menu.
8. Click **Save** to save your *UDA* or click **Submit for Approval** to send it for approval.
   The *UDA* is saved and added to the list of user defined attributes showing the **Status** as **Unapproved**. If the reviewer takes an action and the review is in process, the **Action** changes to **Pending@level name for action**.
9. To deactivate a *UDA*, toggle **Enabled** in the list of user defined attributes.
   A **Deactivate User Defined Attribute** pop-up is displayed, you must provide a comment and click **OK** to deactivate any *UDA*. On clicking **OK**, it is sent for approval and the *UDA* gets deactivated only after the deactivation of the UDA is approved.

   Note: A deactivated UDA can't be added to any **List Entry**, **List**, or **Screener Group** and you can't delete or deactivate a UDA if it is mapped to any of the entities.

View an existing User Defined Attribute

You can view an existing user defined attribute if you have the necessary permissions. For details on access control, see **Controlling accesses at Secured Entities level** on page 64.

1. On the Screener main menu, click **Configurations**.
   The **Configuration** page is displayed.
2. Click the **User Defined Attributes** tab.
3. Select the check-box of the *UDA* you wish to view.
4. Click the **view user defined attribute** icon.
   The **View User Defined Attribute** page is displayed.

Modify details of an User Defined Attribute

1. On the **User Defined Attributes** tab, select the check-box of the desired *UDA* and click the **edit user defined attribute** icon.
2. Make necessary modifications to this attribute and click **Save** to save your *UDA* or click **Submit for Approval** to send it for approval.

Adding UDAs to an entity

You can add the configured UDAs to a **List Entry**, **List**, or **Screener Groups** in both Add (**Add List Entry** page, **Add List** page, and **Add Screener Groups** page) and Modify mode (**Edit List Entry** page, **Edit List** page, and **Edit Screener Groups** page).

1. On the required page (**Add List Entry**, **Edit List Entry Add List**, **Edit List**, **Add Screener Groups**, or **Edit Screener Groups**), click + icon.
2. On the page that is displayed, go to the **User Defined Attributes** section, and click the **Add** + icon.
3. Select the required UDA from the list of configured UDAs.
   The selected UDAs get added to the entity. It is displayed in a tabular form as **Field Name** and **Values**.

   Note: In case of long UDA values, click on the value to view it in a pop-up window.

4. Click **Save** or **Submit for Approval** as needed.

3 - Managing Lists

Screener consolidates and reconciles lists and watchlists. It aggregates list entries from multiple data vendors, reduces duplication and increases list quality. The list management feature helps you:

- Automate list importing and archiving processes.
- Aggregate list entries from multiple data vendors.
- Enable global or, local, centralized and distributed administration.
- Apply robust entity resolution across internal and external lists.
- Automatically assign globally unique identifiers (GUIDs) for efficient identification and matching.
- Produce a fully auditable, streamlined list for screening.

In this section

Creating Lists

In addition to the out-of-the-box list provided to you, Screener allows you to add and configure lists of your choice. To create a new list, perform these steps.

1. On the **Screener** home page, click **Lists**.
2. Click the **Add List** + icon.
   The **Add List** page is displayed.
3. Enter these details for the list you are creating:

Field	Description
List name	Specify a name for this list. **Note:** It is a mandatory field.
Source	Select if the list in **Internal** or **External**.
Location	Displays the location of the list.
Countries	Select the countries to which the list will apply. Your level of access to the Countries list is linked to the **FCC.ListCountry** access control.
Auto data sync	Select this checkbox to configure a URL as source of the list data.
Data URL	Enter the relevant URL, and click the **Test** button to ensure it is correct. **Note:** By default, updates to these lists run on a nightly basis. However, you can configure the schedule per your convenience by using **Flows** > **Schedule** in **Management Console**. **Note:** In consecutive runs, data is updated only when there is a change in it in the source URL.

Field	Description
User Defined Attributes	Select appropriate values for the user defined attributes (UDAs). **Note:** These UDAs are displayed here based on the definitions in the **Configuration** page. To add a new UDA or update an existing one, go to the **User Defined Attributes** tab on the **Configuration** page. • **List Type**: Select one of the defined list types. • **Vendor**: Select one of the defined vendors. **Note:** These are mandatory fields.
Comments	Enter your comment on this list. **Note:** It is a mandatory field.
Screener Groups	Displays the Screener group for this list.

4. Click **Save** to save the list.
5. Click **Submit for Approval**, to send the list for approval.
   The list will run through an approval cycle based on the defined rules.

   Note: If you haven't defined any approval rule, the list will get auto-approved and appear on the **Lists** page. You can add entries to this list.

The Lists page

The **Lists** page displays all the lists defined in the system. There are few lists that are shipped to you along with the product. These out-of-the-box lists are displayed automatically on the **Lists** page after you install and configure **Screener**. For details, see **Out-of-the-box lists** on page 21.

The **Lists** page allows you to perform these tasks:

1. View details of the lists, such as the name, type, and source of the list, action taken on the list, its status, countries applicable, and whether the list is enabled.
2. Upload files to the list by using the **Upload file** icon.
3. Export list by using the **Export** icon.
4. Perform advanced search on the lists.

View list details

To view details of a list, click the name of the list. The **View List** page is displayed. These details are displayed for the list.

- Version number
- Status
- Whether the list is active
- List name
- Source of the list
- Location where the list resides
- Applicable countries
- Auto data sync: If the check box is marked, the list gets updated automatically
- Data URL
- User defined attributes in the list
- The mapped Screener Groups
- Comments on the list

*Using **Advanced Search***

Use the **Advanced Search** to filter the lists on various criteria. For each of these criteria, you need to select the required option from the corresponding drop-down list, specify the criteria, and click the Filter icon. The lists matching the selected criteria are displayed on the right side of the filter panel. The criteria are:

- **Name** of the list
- **Country** for which the list has been defined
- **List type**
- **Source**: Internal or External list
- **Vendor** defined in the list
- **Status** of the list: Approved, Unapproved
- **User Defined Attributes** included in the list

> **Example:** To filter the all the lists of **Sanctions** list type, perform these steps:
>
> 1. In the **Advanced Search** panel, click the arrow next to **List type** criteria.
> 2. Click the drop-down and select Sanctions from all the defined list types.
> 3. Click the Filter icon. The selected lists are displayed to the right of the filter panel.

Out-of-the-box lists

The **Lists** dashboard displays all the lists defined in the system. There are few lists that are shipped to you along with the product. These out-of-the-box lists are displayed automatically on the **Lists** page after you install and configure **Screener**.

Out-of-the-box lists

These lists are shipped along with the product. These are automatically configured when you run the set-up script as detailed out in the **Installing Screener for the first time** on page 6 section. By default, updates to these lists run on a nightly basis. However, you can configure the schedule according to your convenience by using **Flows** > **Schedules** in **Management Console**.

Note: The lists are updated only when there is a change in the source data.

Name of the list	Type	Vendor
OFAC Sanctions (US)	Sanctions or SDN	US Department of Treasury
BIS Unverified List (US)	Sanctions or SDN	US Department of Commerce, Bureau of Industry and Security
Public Safety Canada Listed Terrorist Entities (CAN)	Listed Terrorist Entities	Public Safety Canada, National Security Counter-Terrorism
Financial Sanctions Targets (UK)	Sanctions or SDN	Office of Financial Sanctions Implementation, HM Treasury, GOV.UK
BIS Denied Persons List (US)	Sanctions or SDN	US Department of Commerce, Bureau of Industry and Security
DFAT Consolidated List (AUS)	Sanctions or SDN	Australia Government, Department of Foreign Affairs and Trade
Common and Foreign Security Policy (EU)	Sanctions	European Union External Relations

Viewing list details

To view details of a list, click the name of the list. The **View List** page is displayed. These details are displayed for the list.

- Version number
- Status
- Whether the list is active
- List name
- Source of the list
- Location where the list resides
- Applicable countries
- Auto data sync: If the check box is marked, the list gets updated automatically
- Data URL
- User defined attribtes in the list
- The mapped Screener Groups
- Comments on the list

*Using **Advanced Search***

Use the **Advanced Search** to filter the lists on these criteria. For each of these criteria, you need to select the required option from the corresponding drop-down list, and click the Filter icon. The lists matching the selected criteria are displayed on the right side of the filter panel.

- Name of the list
- Country for which the list has been defined
- List type
- Source: Internal or External list
- Vendor defined in the list
- Status of the list: Approved, Unapproved
- User Defined Attributes included in the list

> **Example:** To filter the all the lists of **Sanctions** list type, perform these steps:
>
> 1. In the **Advanced Search** panel, click the forward arrow next to **List type** criteria.
> 2. Click the drop-down and select Sanctions from all the defined list types.
> 3. Click the Filter icon. The selected lists are displayed to the right of the filter panel.

Viewing List Versions

Lists are of two types:

- Internal list: Internal entries get updated by batch loads or manual edits. Every edit needs to go through the defined approval cycle to become effective.

- External list: The versions of the external lists are auto incremented on each load. You cannot make manual edits in this case. You can not activate, deactivate, and delete any of the external list entries.

However, in both cases, the unique entry id must be persisted across all the records in each batch load.

Viewing Versions of Internal Lists

In **Screener**, every modification needs to be approved (per the defined approval rules), and after every approval, a new version is created. On the **Lists** page, you can view all the versions and also see the entries corresponding to each of these versions.

> **Note:** The list needs to be in the `Approved` stage for the versions to appear. When a version is pending approval, the current approved version is displayed. This holds true for the other entities as well (List entry, UDAs).

1. On the **Lists** page, click the name of the list.
   The **View list** page is displayed, showing the version number on the top left of the page.

   a. To navigate between the versions, click the < or > icon adjacent to the **Cancel** button.
   b. Click the **Field Deltas** link on the top right of the page. The **Updates - Previous and Present Values** pop-up is displayed. The pop-up shows the **Current Value** and **Previous Value** for each of the fields.

2. To view the various versions uploaded for the list:

   a. Click the forward arrow **>** corresponding to the list. All the versions are displayed sequentially, showing the **Version Number**, **Last Modified**, and **Record Count**.
   b. Click the **View** icon for the version, details of which you want to see. The **List Entries** page is displayed, showing the entries made in this version.

Editing Lists

To edit any of the defined lists, perform these steps:

1. On the **Lists** page, mark the check-box corresponding to the list you want to modify, and click the **Edit List** icon.
   The list displays in edit mode.
2. Make modifications, as needed.

3. Click **Save** to save the list.
4. Click **Submit for Approval**, to send the list for approval.
   The list will run through an approval cycle based on the defined rules.

   Note: If you haven't defined any approval rule, the list will get auto-approved and appear on the **Lists** page. You can add entries to this list.

Entries for Lists

You can perform create, read, update, and delete operations on the Internal Lists.

Note: You can not perform these functions on external list entries.

The Internal Lists defined in **Screener** are editable. You can perform these actions on any Internal List:

1. Add a list entry
2. Modify or update the entry
3. Deactivate or delete the entry

Note: All these tasks need to go through the defined approval cycle to take effect. If no rules are defined, the actions get automatically approved.

Manually adding an entry to an internal List

You can add entries to an Internal List using the **List entries <name of the list>** page.

1. On the **Screener** main menu, click **Lists**.
   All the lists defined in the system are displayed.
2. Click **View all entries** icon corresponding to the list to which you want to add the entry.
   The **List entries : <name of the list>** page is displayed, showing all the entries made so far to this list.
3. To add an entry to this list, click the **Add List Entry** icon .
   The **Add List Entry** page is displayed.
4. In the **Entry ID** field, enter an identification for this list entry.
5. To add multiple Entity Details for this entry, click the **Add** icon , and enter these details:
   - Name

- First Name
- Last Name
- Nationality
- Date of birth
- Place of birth

6. To add multiple aliases for this entry, click the **Alias** + icon, and add these details:

   - Title
   - Name
   - First Name
   - Last Name
   - Name ID
   - Title Honorific: Honorary title, if any.

7. Click **Duplicates** to check if any duplicate record exists for the entry you are making. Use the forward arrow > and expand various sections to view duplicates, if there are any, and determine if you want to save and submit the current list entry.

   Note: In case you have uploaded the entries through file, go to the **Duplicates** section in the **Edit List Entry** page to see if this list entry has any duplicates in any previously loaded list entries.

8. To add multiple addresses, click the **Addresses** + icon, and enter these details:

   - Address line 1
   - Address line 2
   - City
   - State/Province
   - Country
   - Postal code
   - Remarks

9. Under the **User Defined Attributes**, use the **Entity type** field to select the entities you want to add to the list entry. To add any new field to the list entry, click the **User Defined Attributes** + icon.
   The **User Defined Attributes** pop-up is displayed, which allows you to select the approved UDAs and add those to this entry.

   Note: You can add a new UDA or update the existing ones through the **User Defined Attributes** tab on the **Configuration** page. **Entity Type** is also a UDA and can be configured using the **Configuration** page.

10. To add identification Ids for this list entry, click the **Identities** + icon, and enter these details:

    - Identifier Id

- Identity Number
- Identify Type
- **Notes** for this identity.

11. To add an attachment to the list entry, click **Attachments** followed by the **Add attachment** button. In the browser window, select the required files and click the **Open** button.
The selected file(s) are displayed below the **Add attachment** button, showing these details:

    Note: The attachments get added to the list entry only when you save the list entry. To download the attachment before that, click the document name hyperlink.

    - **Name** of the file
    - **Date** and time of upload
    - **Uploaded by**: The user who uploaded it
    - **Action**: Delete icon to delete the file.

    Note: You can not delete an attachment after the list entry is approved. Although, the files attached to the unapproved version of an entry can be deleted.

12. Add your **Comments**.

    Note: This is a mandatory field.

13. Click **Save** on the top of the page, to save the entry.

    Note: To download a list entry click the **Download** button. If you download multiple files together, those are downloaded as a zip file. To download a single attachment, you can also use the document name link.

14. Click **Submit for Approval**, to send the list entry for approval.
The list entry will run through an approval cycle based on the defined rules.

    Note: If you haven't defined any approval rule, the list entry will get auto-approved.

Uploading the list entries

You can upload the list entries file to the Screener using the **Upload File** icon on the **Lists** page. Upload of *Excel* files are also supported.

Prerequisite

The list you are uploading must be in the canonical format, as described in **The canonical schema for List data** on page 27 section below.

If your list is not in the specified canonical format, you need to configure a pre-process flow using the **Enterprise Designer** to convert the format. In case of an Excel file, you need to configure a pre-process flow with **Read from Excel** and **Write to File** stages in the **Enterprise Designer** to convert the format before ingesting the file, irrespective whether the file adheres to the canonical format.

> **Note:** For more information about designing this flow, see the **List Import utility – Upload and Polling** on page 29 section.

1. On the **Screener** main menu, click **Lists**.
   The **Lists** page is displayed showing all the lists.
2. Click the **Upload File** icon corresponding to the list to which you want to upload your file.
3. Go to the location where the file is saved, select it, and click the **Open** button.
   The list upload begins and you can see the status by hovering your curser on the **Import** field of the list on the **Lists** page. While the update is in progress, the field shows **Running** as the status, which changes to a tick mark when it is completed. It also shows the number of records uploaded.

   > **Note:** If any record throws an error, the entire file is rejected.

4. To view the uploaded list entries, click the **View all entries** icon.

The canonical schema for List data

The files you are uploading to the **Screener** need to adhere to this canonical schema. The file must contain all of these field names in this order, whether data exists in each field or not. The field length also does not matter.

```
ActiveFlag|AddressKey|AddressLine1|AddressLine2|AddressType|Alias_CompanyName|
Alias_FirstName|Alias_FourthName|Alias_LastName|Alias_MaturitySuffix|Alias_Name|
Alias_SecondName|Alias_ThirdName|AliasID|AliasQuality|AltCitizenship|AlternateSpelling|
ApartmentNumber|Category|Citizenship|City|Country|Deceased|Designation|Details|DOB|
EmailAddress|FirstName|FourthName|Gender|HouseNumber|IdentifierCountry|IdentifierID|
Identity_CityOfIssue|Identity_DateOfExpiration|Identity_DateOfIssue|IdentityNumber|
IdentityType|LastName|LastUpdateDate|LeadingDirectional|List_UDAID|ListSourceType|
MaturitySuffix|Name|NationalID|Nationality|Organization|PlaceOfBirth|PostalCode|
RecordCreationDate|RecordEndDate|RecordLastUpdateDate|ReferenceNumber|SecondName|
StateProvince|StreetName|StreetSuffix|SubCategory|ThirdName|TrailingDirectional|
UDA_EffectiveEndDate|UDA_EffectiveStartDate|UDA_Name|UDA_Type|UDA_Value|UID|EntityType|
ActiveStatus|TitleHonorific|ScriptLanguage|NameType|AddressRemarks|IdentityNotes|NameId|
ReferenceGroup|ActiveDate|AliasTitle|AliasTitleHonorific|AliasScriptLanguage|Title|AliasNameType|
AliasRemarks|Remarks
```

Versions of list entries

A new version of a list entry is created when you edit any approved version of the entry. When you edit an unapproved version, the previous data gets overwritten and no new version of the list entry

is created. You can perform Create, Edit, Update, Delete, and Deactivate operation only on the current version any list entry. All the previous versions are in the read-only mode.

You can view the versions and the modifications done in each version by using the **View List Entry** page.

1. On the **Lists** page, click the **View all entries** icon corresponding to the list for which you want to view the entry versions.
   The **List entries : <name of the list>** page is displayed listing all the entries.
2. Click the **Entry ID**, version of which, you want to view.
   The **View List Entry** page is displayed, which shows these details of this list entry:
   - **Version Number**
   - **Status** of the entry
   - **Is Active Version**: Indicates if this is the active version of the list entry
   - **Entry ID**
   - **Entity type**
   - **List version**
3. Use the forward > and back < arrows at the top of the page move through the various versions of the entries.
4. Each section of the page, such as **Primary Details**, **Comments**, **Aliases**, **Addresses**, **User Defined Attributes**, and **Identities** shows information in different versions in different rows.

List entry ingestion scenarios

This section describes the guidelines governing duplicate data and versions in list entry ingestion.

1. A list entry is considered duplicate if the data in all the fields of the incoming list entry is same as that of the existing list entry, with same Entry ID (UID).
2. The system matches only raw uncleansed data for identifying a duplicate entry during list ingestion.
3. The state of an approved list entry version never changes.
4. An incoming list entry is always discarded if it is a duplicate of a currently approved version in the system (Case #1 and #2 in the table below).
5. An incoming list entry overwrites the unapproved version if it is different from the approved version (Case #3 in the table below).
6. In case the current version is approved, an incoming list entry, which is different from the approved version will create an unapproved version (Case #4 in the table below).

   Note: The fields to which this applies includes a combination of data in any of these sections in the **List Entry** page: Entity Details (such as names), Aliases, Addresses, User Defined Attributes, and Identities.

Case #	Approved version Ist Ingestion	Current revision 2nd Ingestion	State of current version	Newly ingested entry 3rd Ingestion	Result
1	Robert Smith	Michael Smith	**Unapproved**	Robert Smith (The same list entry is ingested, a duplicate of the approved version)	Robert Smith does not overwrite Michael Smith. Michael Smith remains as the entry contents and entry remains in unapproved state.
2	Robert Smith	Michael Smith	**Unapproved**	Stephan Williams (The list entry has a different data from the approved and current versions)	Stephan Williams overwrites Michael Smith. The list entry does not match the current or approved version. The unapproved version is replaced by the new entry.
3	Robert Smith	Michael Smith	**Pending Approval**	Stephan Williams (The list entry has a different data from the approved and current versions)	Stephan Williams becomes the unapproved version. Michael Smith becomes obsolete (it cannot be modified or updated).

List entry ingestion in cluster

In a cluster set-up, you need to take care of these aspects for successful ingestion of list entries.

- If multiple files are dropped in one import folder, no processing is done unless a pre-flow configuration with same number of input files is present.
- If a processing node gets down while ingesting a file, re-import the file through another node or when the same node it up.
- All nodes in the cluster must be available to open or create a model.
- The list ingestion path should not be a shared or mapped drive path.

List Import utility – Upload and Polling

To import any List files from the Screener or to directly upload these to the polling or base directory the `<Path of List Polling Directory>` must match the

`fcc.spectrum.list.job.poll.dir`property file placed at `modules/fcc/fcc.properties`. This path should also exist on the server.

> **Note:** Restart the poller if list ingestion does not start when a file is dropped in the import folder. In case of load balancer, restart the poller from jmx-console of a particular node and not via the load balancer URL as that may restart an incorrect poller.

Configuring a Pre-process Flow

For ingesting a list to Screener, it should be in a standard canonical format. A sample of the same resides at `<SpectrumLocation>\server\modules\fcc\FCC_Repo\CreateListIndex\Input\List_in.csv`.

If the list is not in the canonical format, perform these two tasks:

1. Convert the list to the canonical format by creating a pre-flow for every unique combination of List Type and Vendor.
2. Register this pre-flow by executing `'setflowconfig.df'` from **Enterprise Designer**.

> **Note:** It is shipped to you with the product.

In the Enterprise Designer, all the fields, such as **ListType**, **Vendor**, **Mappings**, and **FlowName** of the **Inspection Input** tab are mandatory. The **Mappings** section displays a list of files and their Mode, Info and Stage. The **Label** field gets generated in the flow.

- The Mapping Mode can be **IN** or **OUT**. Specify **IN** if you want to want to **Read from File** and **OUT** to **Write to File**.
- The **Info** field specifies the information about the file such as address, email, and name. This is helpful during uploading a file.

The output of this flow is a file in canonical format.

Managing List Ingestion Utility through JMX Console

This table describes the operations you can manage through the JMX Console. To access this table, perform these steps:

1. Open a web browser and go to `http://`*`server`*`:`*`port`*`/jmx-console`

   Where:

   - *server* is the IP address or host name of your Spectrum Technology Platform server.
   - *port* is the HTTP port used by Spectrum Technology Platform. The default is 8080.

2. Log in using the admin account.
3. Click the **ListInjestionUtilityManager** link, and use these operations, as required.

Operations	Description
autoRestartPoller	Auto restart list ingestion poller
refreshFileEventGenerator	Force poll idle files
shutDownAutoRestartPoller	Shut down auto restart list ingestion poller
failRunningJobs	Fail running jobs
shutDownPoller	Shut down list ingestion poller
restartPoller	Restart list ingestion poller

Updating an internal list entry

You can view the different entries made for an Internal List using the **List entries : <name of the list>** page. To modify or update any of the list entries, perform these steps:

1. Select the entry from the list, and click the **Edit List Entry** icon at the top left of the page. The **Edit List Entry** page is displayed allowing you to make the required updates.
2. Make necessary modifications to the entry and click **Save** or **Submit for Approval**, as needed. A new version of the list entry is created. These fields display the update you made:
   a. **Action**: Shows the most recent action you took on the list entry. For example, it displays **Updated** if you made change to any value in the list entry and **Enabled** or **Disabled** if you did that with the list entry.
   b. **List Version Number**: Shows the updated version of the list entry in blue colour.

      Note: The list entries not updated are in grey colour with **(Unchanged)** appended to the version number.

   If you clicked **Save**, the new version shows **Unapproved** state. If you clicked **Submit for Approval**, the new version shows **Pending for review** stage.

      Note: You can not delete any attachment from a list entry once the entry is approved. However, you can delete attachments from an unapproved version of list entry.

Exporting the List Entries

You can export the list entries using the **Export File** icon on the **Lists** page. The exported files give you a consolidated view of all the list entries of a particular version. The set of exported files include:

- *Address.csv*
- *Alias.csv*
- *Comments.csv*
- *Identity.csv*
- *ListEntries_Flat_File.csv*
- *ListEntry.csv*
- *ListEntryData.csv*
- *UDA.csv*

All these files correspond to the information sections in the **List Entry** page. For example, *Address.csv* file has information in the **Addresses** section of all the list entries, *ListEntryData.csv* file contains data in the canonical schema in pipe delimited format, and *ListEntry.csv* file lists data across all the sections in the **List Entry** page.

To export the list entries, perform these steps:

1. On the **Screener** main menu, click **Lists**.
   The **Lists** page is displayed showing all the lists.
2. Click the **Export Entries** icon corresponding to the list, entries of which you want to export. The request is **Submitted** and when the entries are ready to be downloaded, the **Export Entries** icon changes to **Download**.
3. Click the **Download** icon to download the zipped set of `csv` files in the Downloads folder. Each section of the list entry, such as UDA, Addresses, Alias, and Identity is converted to one `csv` file.

   Note: In case there is update to the list after you exported, use the **Re-export** icon to download it. The list is replaced with the updated one.

   Note: The base path where the List Import and Export files are created is maintained in the `fcc.spectrum.list.job.base.path` properties of the `fcc.properties` file here: `<SpectrumLocation>\server\modules\fcc`.

4. To export a specific version of the list, click the forward arrow corresponding to the list, and click **Export Entries** icon for the required version.

   Note: Consider this scenario: You have downloaded the consolidated list view and uploaded few more entries. Now, when you again download, the new entries are not downloaded. In such a case, you need to press **Re-Export** before downloading.

Making a list entry inaccessible

You cannot delete a list entry permanently from the system. You can hide it (make it inaccessible) using the **List entries : <name of the list>** page. To hide a list entry, it needs to go through at least one round of the approval process.

1. On the **List entries : <name of the list>** page, select the entry that you want to hide, and click the **Delete List Entry** icon. To hide multiple entries, select all of those.
2. Enter the reason of deletion in the **Comments** text box of the **Delete List Entry pop-up**.
   The list entry is no more visible and accessible.

Deactivating a list entry

You can deactivate the list entries that should no longer be used. However, the process of deactivating a list entry and activating if has to go through the approval process to take effect.

> **Note:** For a list entry to be deleted or deactivated, it needs to go through at least one round of the approval process.

To deactivate a list entry, perform these steps:

1. On the **List entries : <name of the list>** page, set the **Enabled** toggle button to `No`.
2. In the **Comments** text box of the **Deactivate List Entry** pop-up, enter the reasons of deactivation.

Viewing cleansed data in entries

Whenever a list entry is added, either through a file or manual addition, it gets cleansed by Screener and is stored. You can view the cleansed version using the Cleansed button on the **View List Entry** page. This version shows parsed, normalized, and validated data.

To view the cleansed data for a list entry,

1. On the corresponding **View List Entry** page, click the **Cleansed** button.
   The cleansed, parsed, and normalized data is displayed in each of the fields of the page.

   > **Note:** A blue colour of the button indicates it has been clicked.

2. To go back to the uncleansed view, click the **Uncleansed** button.

   > **Note:** You can update the entry only in the uncleansed version. The cleansed version is for viewing purposes only.

Viewing duplicate entries

If the file you have uploaded has duplicate entries in forms such as first name, last name, alias, or organization name, you can view those in the **Duplicates** section of the **Edit List Entry**, **Add List Entry** page, and **View List Entry** page. For more information, see the Duplicates section in **Manually adding an entry to an internal List** on page 24.

Sending list entries for approval

You can initiate the approval process from **Edit List Entry** page as well as the **List Entries: <name of the list>** page.

1. On the **Screener** Home page, click **Lists**.
2. Click the **View all entries** icon corresponding to the list to which the entries belong. The **List Entries: <name of the list>** page is displayed.
3. Use one of these methods to send the list entries for approval.

   a. Select the list entries that you want to send for the approval, click the **Submit List Entry** icon from the list of icons on the top left side of the page, and enter your comment. This comment will be applied to all the selected list entries.

   b. Select the list entry and click the **Edit List Entry** icon. On the **Edit List Entry** page, enter your comments, and click **Submit for Approval** button.

   The list entry or all the selected entries are get approved and the status changes to `Approved`.

4 - Reviewing Entities

In this section

Reviewing Entities

Every new entity, such as a **List**, **List Entry**, **User Defined Attribute**, and **Screener Group** needs to be reviewed and approved to become effective in the system.

Once approved, the entity is versioned. If you make an edit to an approved entity, it again needs to undergo the approval cycle to be effective and when done, the version gets updated.

To review a **List**, **List Entry**, **User Defined Attribute**, or a **Screener Group**, you need to go to the **Review** tab on the Screener main menu.

Review lists

1. On the **Screener** main menu, click **Review** > **Lists**.
   The **Lists** in review queue are displayed.
2. Click any **List**.
   These details are displayed.

Field name	Description
Action	The action which was last performed on this list.
Comment	Displays the number of comments in this list.
Name	Name of the list.
Status	The current status of the list
List Type	The list type of the current list.
Vendor	The list vendor.
Country	Countries covered by the list
Screener Groups	Displays the screener groups associated with this list. **Note:** You need to remove the list from all the associated screener groups before you delete it.

3. To review and `Approve` or `Reject` a list , select the check-box of the list to be reviewed and click the **Review/Approve** icon.
   Review List page is displayed.
4. Review the list and enter a comment in the **Comments** text box by clicking the **Add** button.
   Your comment is added and displayed.
5. `Approve` or `Reject` the list by using the respective buttons.
   The list is approved or rejected.

You can compare the current version of any approved list with its previous version using the **Field Deltas** link on the **View list** page. When you click the link, Updates - Previous and Present Values pop-up is displayed.

The pop-up shows the **Current Value** and **Previous Value** for each of the fields.

> **Note:** Click the < or > icon to view the previous and next version of any **List** while *creating*, *viewing*, or *reviewing*.

Reviewing List Entries

1. On the **Screener** main menu, click **Review** > **List Entries**.
   All the list entries queued for review are displayed.
2. Select the check-box corresponding to the list entry you want to approve, and click the **Review List Entries** icon on the top left of the list.
   The **Review List Entries** page is displayed.
3. Review the details, enter your comment for approval or rejection in the **Comments** text box, and click the adjacent **Add** button.
   Your comment is added and displayed.
4. Click **Duplicates** to check if any duplicate record exists for this entry. Use the forward arrow > and expand various sections to view duplicates, if there are any, and determine if you want to approve the current list entry.

   > **Note:** The number of duplicates for a list entry is restricted to 2000. Screener uses algorithms based on industry best practices to find the duplicates. It searches for duplicates entries within and among the list (both internal and external) on these fields:
   >
   > a. **Personal name:** First name, Second name, Last name, and Title
   > b. **Organization**, in cases where the entity is a business name or organization
   > c. **Alias name:** Alias First name, Alias Second Name, Alias Last name, Alias Title
   > d. **Full name**
   > e. **Full Alias name**
   >
   > For more information about matching process, see **Interflow Match**.

5. Use appropriate button on the top right of the page to **Approve** or **Reject** the list entry.

Go back to the **List Entries** page and to see the list entry appear as `Approved`.

Reviewing Screener Groups

1. On the **Screener** main menu, click **Review** > **Screener Groups**.
   All the screener groups queued for review are displayed.
2. Select the checkbox corresponding to the screener group you want to approve, and click the **Review Screener Group** icon on the top left of the list.
   The **Review Screener Group** page is displayed.
3. Review the details, enter your comment for approval or rejection in the **Comments** text box, and click the adjacent **Add** button.
   Your comment is added and displayed.
4. Use appropriate button on the top right of the page to **Approve** or **Reject** the screener group.

Go back to the **Screener Groups** page and to see the screener group appear as `Approved`.

Review User Defined Attributes

1. On the **Screener** main menu, click **Review**.
   The **User Defined Attributes** in review queue are displayed. These are the details displayed for each of the entries.

Field name	Description
Action	The last action performed on this UDA.
Comment	Displays the number comments on this UDA.
Name	Name of the UDA.
Status	Current status of the UDA.
Applicable To	The entities on which the UDA is applicable.
Valid Values	Valid values attached to the UDA

2. To review and `Approve` or `Reject` a UDA, select the check-box of the UDA to be reviewed and click the  icon.
   The **Review User Defined Attribute** page is displayed.
3. Review the UDA and enter a comment in the **Comments** text box by clicking the **Add** button. Your comment is added and displayed.
4. `Approve` or `Reject` the list by using the respective buttons.

You can compare the current version of any approved list with its previous version using the **Field Deltas** link on the **View list** page. When you click the link, Updates - Previous and Present Values pop-up is displayed.

The pop-up shows the **Current Value** and **Previous Value** for each of the fields.

> **Note:** Click the  or  icon to view the previous and next version of any **List** while *creating*, *viewing*, or *reviewing*.

5 - Managing Screener Groups

In this section

Managing Screener Groups

Screener Groups define a set of Lists to screen parties against. The screening can be done with Screener, or Screener Groups can be used to define the mappings of lists to third party screening systems. However, our Services are needed to disseminate the lists to the third party screening systems following the business rules of the organisation.

You can add Screener Groups and perform these actions on the Groups:

- View an existing Screener Group
- Modify or update a Screener Group
- Approve a Screener Group
- Delete a Screener Group

> **Note:** All these tasks need to go through the defined approval cycle to take effect. If no rules are defined, the actions get automatically approved.

Adding Screener Groups

To add Screener Groups, perform these steps.

1. On the **Screener** main menu, click **Screener Groups**.
   The **Screener Groups** page is displayed.
2. Click the **Add Screener Group** icon ➕.
   The **Add Screener Group** page is displayed.
3. In the **Screener group name** field, enter a name for this Screener Group.
4. Enter your **Comments** for this Screener Group, and click the **Add** button.

   > **Note:** This is a mandatory field.

5. To add any new field to the Screener Group, click the **User Defined Attributes** ➕ icon.
   The **User Defined Attributes** pop-up is displayed, which allows you to select the approved UDAs and add those to this entry.

   > **Note:** You can add a new UDA through the **User Defined Attributes** tab on the **Configuration** page.

6. From the **Lists** section, select the lists that you want to add this Screener Group.

Note: All the lists that are neither deleted nor disabled, are available here for mapping.

a. To select all the lists, click the check-box in the header on the right pane. Use the type-ahead filter at the top of the table to filter the lists on the basis of their names and types.
b. For a more specific search, use the **Advanced Search** in the right pane. You can filter on the basis of **Name**, **Country**, **List type**, **Source**, **Vendor**, **Effective status**, and **User Defined Attributes**. Click the relevant criteria, write the search string in the text box, and click the Filter icon.

The searched Lists are displayed in the right pane.

7. Click the **Save** button on the top of the page to save the Screener Group.
8. To save and submit the Screener Group for approval, click **Submit for Approval**.

Note: Any list mapped to an approved screener group can not be disabled or deleted.

Screener Groups Page

The Screener Groups page displays these details for all the groups defined in the system.

- **Name** of the screener group
- The last **Action** performed on the group, such as **Created** or **Updated**
- **Status** of the group
- Last **Modified By**
- **Last Modified** date and time
- Whether the group is **Enabled**

The page allows you to perform these actions:

- **Add** + a new Screener Group
- **View** Screener Group
- **Edit** Screener Group
- **Delete** Screener Group
- **Refresh** Screener Group

Viewing details of Screener Groups

To view details on the existing Screener Groups, perform these steps:

1. On the **Screener Groups** page, click the check-box corresponding to the Screener Group you want to view.

The **View Screener Group** icon is enabled in the icon bar.

2. Click the **View Screener Group** icon.
   The selected Screener Group is displayed in the view mode, with all the fields disabled.

Updating a Screener Group

To modify or update any of the list entries, perform these steps:

1. On the **Screener Groups** page, click the check-box corresponding to the Screener Group you want to update.
   The **Edit Screener Group** icon is enabled in the icon bar.
2. Click the **Edit Screener Group** icon.
   The selected Screener Group is displayed in the edit mode, with **Version Number**, **Status**, **Is Active Version**, and **Screener Group Name**, fields disabled.
3. Make modifications, as needed.
4. Click the **Save** button to save the Screener Group.
5. To save and submit the Screener Group for approval, click **Submit for Approval**.

Deleting a Screener Group

To delete a Screener Group, perform these steps:

1. On the **Screener Groups** page, click the check-box corresponding to the Screener Group you want to delete.
   The **Delete Screener Group** icon is enabled in the icon bar.
2. Click the **Delete Screener Group** icon.
   The **Delete Screener Group** pop-up is displayed.
3. Enter your Comments for this delete operation and click the **OK** button.
   The selected Screener Group is deleted. However, this operation needs to be approved, per the defined approval rules for it to become effective.

Managing accesses to the Screener Groups

Your permission levels to the screener groups are governed by the accesses to the role you have been assigned. To add, modify, or remove the accesses corresponding to your role, the administrative users use the **Security** page of **Management Console**.

1. On the **Management Console** main menu, click **System** > **Security** > **Roles**.
2. Do one of these, depending on whether you want to create a new role and assign the permission or modify permissions to an existing role:

   a. Click the **Add role** + icon to create a new role and assign accesses to it.
   b. From the displayed list of roles, select the one to which you want to give accesses to the screener groups, and click the **Edit role** icon above the list.

3. On the page that is displayed, scroll down the list till you see **FCC**, and click it.
   A list of entities and permissions is displayed.
4. Scroll down to **ScreenerGroup**, and assign the required **Create**, **View**, **Modify**, **Delete**, and **Execute** accesses to this role.

Table 1: The access matrix for Screener Groups

Accesses	Actions that can be performed
Create	Create a Screener Group
View	Only view the Screener Group
Modify	Edit a Screener Group, activate and deactivate a Screener Group, disable or enable a Screener Group, and send it for review and approval.
Delete	Delete a Screener Group
Execute	Review, approve, or reject a Screener Group

6 - Screening

In this section

Introduction to Screening

Screening is a process of matching parties to your lists such as, internal or sanctions list or any individual. Their suitability is checked for current and further transactions.

The Screen Page

The **Screen** page consists of two tabs:

- **Batch** - Use this tab to interactively process batches of records.

  Note: You have the flexibility of performing batch screening through the *User Interface* or through an *API*. For information about batch screening through *User Interface*, see **Interactive Batch Screening** on page 46 and to perform through *API*, see **Scheduled Batch Screening** on page 48.

- **Manual**- Use this tab to interactively process single records. For more information, see **Manual Screening** on page 51.

Interactive Batch Screening

Adding a new job for interactive batch screening

Follow these steps to add a new job:

1. Log in to **Screener** and click **Screen** from the top menu options.
2. Click the **Batch** tab. This tab displays a list of batch jobs added by you along with the *latest run* of a job such as **Job Name**, **Description**, **Job Status**, **Duration**, **Records**, **Matched** records, **Non-Matched** records, and **% Matched**.

   This list is pre-sorted on the basis of *latest job creation* or *edit date*.

   You also have the capability of *adding*, *editing*, *deleting*, *running*, and *re-run* any job with the help of respective icons.

   Note: This list will be blank if you are creating a job for the first time.

3. Click the  icon to add a new job. The **New Job** page opens up.

4. Enter your unique job name in the **Job Name** field.
5. If required, enter a description for your job in the **Description** field.
6. Click the **Browse** button, go to your **Party data file** and click **OK**.

   Note: The party data schema should be in this format: the *in_PartyID* field must be *unique* and *not blank*.

   Party Data Schema

   in_PartyID|in_Portfolio|in_SourceSystem|in_PartyName|in_PartyFirmName|
   in_PartyFirstName|in_PartyMiddleName|in_PartyLastName|in_PartyMaturitySuffix|
   in_PartyGender|in_PartyIdentifier|in_PartyIdentifierCountry|in_PartyIdentifierFormat|
   in_PartyBirthDate|in_PartyBirthCountry|in_PartyPrimaryCitizenshipCountry|in_PartyResidenceCountry|
   in_PartyPhoneNumber|in_PartyPhoneNumberCountryCode|in_PartyPhoneNumberExtension|
   in_PartyPhoneUsageType|in_PartyType|in_PartyEmailID|in_PartyAddressLine1|in_PartyAddressLine2|
   in_PartyAddressLine3|in_PartyAddressLine4|in_PartyAddressUsageType|in_PartyCity|
   in_PartyPostalCode|in_PartyRegion|in_PartyState|in_PartyCountry|in_PartyGUID

7. Select the **Party Group** to define lists against which you want to screen from the list available in the drop-down.
8. Select the **Match Rule** for cleansed and uncleansed list from the drop-down.
9. Set the **Match Threshold**.
10. Select the **Match Key** from the list displayed. The available options are **Soundex**, **Metaphone**, **Phonix**, or **no match key**.

    Select the check-box if you wish to **Use substring as match key for company**; this check-box is disabled for **no match key**. If you select **Soundex**, **Metaphone**, or **Phonix**, the value of **Candidate Count** will be set to `300` by default; and if you select **No Match Key**, by default it will be set to `1000`. You have the flexibility of overriding these values.

    Note: **No Match Key** option should not be used for a large party data.

11. Click the Save button to save your new job or the Save & Run button to run the newly created job.

Viewing Details of Batch Screen Jobs

Job details and run history of previously run batch jobs can be viewed through the **Batch Screen** homepage. Click the desired job name from the list of batch jobs, the **Job Details** page is displayed.

Viewing Job Details

This page displays various details such as the **Job Name**, **Description**, **Last Run Status**, and the **Job Run History**.

The last run status and job run history specifies details such as **Match Rule Name**, **Match Threshold**, **Match Keys**, **Start Time**, **Job Status**, total number of **Records**, **Matched** records, **Non-Matched** records, and **% Matched**.

> **Note:** You can re-run any job with the same configuration and party data by clicking the button. You must not try to multiple job re-runs when it is already in a running state.

Editing and Running

If you wish to run the same job with a different configuration or party data, click Edit & Run placed on the top-right of the screen.

A **New Run** pop-up is displayed showing configurations of the selected job.

You can choose to replace the **Party data file** by clicking on Change and go to the path where your new party data file resides. **Party Group** and **Match Rule for cleansed and uncleansed list** can be modified using the respective drop-downs. You also have the flexibility of modifying the **Match Threshold** and **Match Keys**.

After specifying the new configurations, click Save & Run to re-run the job.

> **Note:** Job configurations once edited by any user gets locked for all other users. This ensures that only one job can be edited at a time by a user.

Scheduled Batch Screening

Use this API to run or schedule batch screening from outside of **Screener**. This call requires a valid Spectrum token to be passed for authentication. For details on obtaining web service authentication tokens, see **Web Service Authentication** in the Administration Guide and **Getting a Token**, and **Using a Token** in the API Guide .

HTTP Method

POST

URL

```
http://<spectrum-server>:<port>/managers/fccRuntime/job/execute
```

Where *spectrum-server* is the server name or IP address of your Spectrum Technology Platform server and *port* is the HTTP port. By default, the HTTP port is 8080.

Input Parameters

Parameter	Description
jobName	It should be an already existing job created from the **Screener** user interface. Else, you receive error code *400* with appropriate message.
filePath	Path where the party data file is placed. It should be a valid and accessible path on the Spectrum server. Else, you receive error code *400*.

Result

When you successfully submit the request, a new version is created for the given screening job, with all configurations copied from the current version, the only difference being a new party data file (the path of which you passed as input). A new screening job is triggered for this new job definition version. You can verify it with the Screener user interface.

Viewing Batch Screening Results

You can view matched and non-matched data records detected in a batch job. Click on the *number* displayed under the **Matched** or **Non matched** column to view details.

Viewing Matched Data

This page displays matched party details such as **Party ID**, **First name**, **Last name**, **Name**, **City**, **State/Province**, **Country**, and **Match score**.

> **Note:** You can set the **Matching Threshold** through the sliding bar. The *configure threshold window* is also displayed here. For more information about how to set the configure threshold window, see **Configuration**.
>
> By setting this threshold, you can choose to analyze non-matched records which fall outside the matching threshold. For example,**Matching Threshold** is set as `60`, and the configure threshold window is set to `10%`. Then, the non-matched records having match score less than `60` but more than `54` will also be displayed for analysis. The value of **configure threshold window** can vary between `0` and `20`.

You have the flexibility of filtering data on the basis of **Match Score**.

To view a detailed analysis of the matched party, click the **Party ID**, the **Alert** page displaying a detailed analysis of that party opens up. These details are displayed here:

- **Name** of the party along with the **Party ID**
- **Maximum list match score**- The cleansing match score is represented in percentage form.
- **Negative media match score**- The negative media match score is represented in percentage form. A score closer to *zero* is desirable and can be considered for *adding to whitelist* or giving a **Discount**.
- **Alert Status** and **Alert Status Reason**.
- **List Matches**- This section lists the number of matches for the party and displays these details:
  - **List name**
  - **Party name**
  - **Street**
  - **City**
  - **State/Province**
  - **Country**
  - **Match Score**: The matching score of the party with the list in percentage.

  Each list is further divided into *Cleansed* and *Uncleansed*. Click the › icon to view a detailed analysis of cleansed and uncleansed matches. These details are displayed here:

  - **Attributes**- Components used for matching party and lists.
  - **List**
  - **Party**
  - **Match Score**

    Note: Click the **Match Rule** hyperlink to view the match rule and corresponding match scores.

- **Document Links**- This section lists all the articles in which a person's name is featured. You can also add an article to support a case for better analysis of the person or party using the *Add Document* icon.

To send a party for discount consideration, click Discount or to add a party to whitelist, click Add to whitelist. You can also send a party to case management for further review by clicking Send to case management.

Viewing Non Matched Data

This page displays non matched party details such as **Party ID**, **First name**, **Last name**, **Name**, **City**, **State/Province**, and **Country**.

Note: The records lying below the *match threshold* but greater than the set *configure threshold window* are also displayed here.

Manual Screening

Manual screening is a process in which you can interactively process single records and match them against multiple watchlists.

Follow these steps to perform manual screening:

1. On the home page, click **Screen** from the top menu options.
2. Click the **Manual** tab.
3. Select the party group name from the **Use lists from party group** drop-down.
4. Select the **cleansed and uncleansed match rule**, **match key**, and set the **Match threshold**.

You can perform manual screening by using:

- **Party details** - To perform screening through **Party details**, enter the required details and click **Screen**.
- **Pre-existing Party IDs**- To perform screening through **Party IDs**, enter the **Party ID** and **Reference Number**. Click **Screen** to begin screening.

  You will be redirected to the **Alerts** page displaying the manual screening results. For more information, see **Viewing Manual Screening Results** on page 51.

Viewing Manual Screening Results

The **Alerts** page displays the manual screening results. A detailed analysis of the screening results are shown here with these components:

- **Maximum list match score**- The cleansing match score is represented in percentage form.
- **Negative media match score**- The negative media match score is represented in percentage form. A score closer to *zero* is desirable and can be considered for *adding to whitelist* or giving a **Discount**.
- **Alert Status** and **Alert Status Reason**.
- **List Matches**- This section lists the number of matches for the party and displays these details:
  - **List name**
  - **Party name**
  - **Street**

- **City**
- **State/Province**
- **Country**
- **Match Score**: The matching score of the party with the list in percentage.

Each list is further divided into *Cleansed* and *Uncleansed*. Click the  icon to view a detailed analysis of cleansed and uncleansed matches. These details are displayed here:

- **Attributes**- Components used for matching party and lists.
- **List**
- **Party**
- **Match Score**

> **Note:** Click the **Match Rule** hyperlink to view the match rule and corresponding match scores.

- **Negative Media Matches**- This section lists the negative media matches detected during screening. These details are displayed here:
  - **Domain**
  - **URL**
  - **Abstract**
  - **Word Density**
- **Document Links**- This section lists all the articles in which a person's name is featured. You can also add an article to support a case for better analysis of the person or party using the *Add Document* icon.

To send a party for discount consideration, click 

or to add a party to whitelist, click 

. You can also send a party to case management for further review by clicking 

.

Flow Details

This section describes the flows you need to run while performing scheduled batch screening.

Placement of Data Files

Copy your **FCC_Repo** to the **C:** drive. If you are not using the **C:** drive, change the paths of input and output files for the flows mentioned in the **Screening Data/Process flow** table. For more information, see **Screening Data/Process Flows**.

Process Flows

Data flow process data from one stage to the other. Output of one flow becomes the input of the next, this is not true always. There are process flows which use main flows for processing.

- **FCC-Integrated-Flow:** An end-to-end integrated flow. It cleanses, screens and creates an alert for the data if any hit is found. This flow contains *ProcFlow_PartyER_N_Screening*

Process flows and their main data flows of various modules are summarized in these sections:

- **Party Management Data/Process:** Run the **FCC_ER_Party_PostProc1_CreatePartySearchIndex_v1** job before running any other flow. The input file for this job is *DummyPartySearchIndex.txt* and the outputs generated are:
  - *To Index: ER_Party_SearchIndex*
  - *To File: SI_Update_All_Test.csv*

Party Management flows:

Process Flow	Main Flow	Input	Output
FCC_ER_Full LoadInitial_ProcessFlow_V1: This flow takes party data as input and performs cleansing, normalization, and intraflow matching before producing the output.	**FCC_ER_Party_ MainFlow1_Normalization _v1.df**: For normalization of data.	Takes a file with party data. Fields include: • inParty • inPartyAddress • inPartyPhone • inPartyEmail • inAccount • inPartyAccount	It produces: *Party_MainFlow2_1_input.txt*
	FCC_ER_Party_ MainFlow2_1_ IntraflowMatch_v1.df: Finds matches between similar data records.	*Party_MainFlow2_1_input.txt'* which is the output of *FCC_ER_Party_ MainFlow1_ Normalization_v1.df*	It produces: *Party_MainFlow2_2_input.txt*
	FCC_ER_Party_ MainFlow2_2_ TransactionalMatch AndSurvivorship_v1.df: Finds interflow matches.	*Party_MainFlow2_2_input.txt* which is the output of *FCC_ER_Party_ MainFlow2_1_ IntraflowMatch_v1.df*	It produces: *Party_MainFlow3_input.txt*
	FCC_ER_Party _PostProc1_Update PartySearchIndex_v1: Updates a party search index based on Party ID.	*Party_MainFlow3_input.txt* which is output of *FCC_ER_Party_ MainFlow2_2_Transactional MatchAndSurvivorship_v1.df*	It produces: To Index: *ER_Party_SearchIndex*

Screening Data/Process Flows: This table summarizes the screening flows:

Process Flow	Flow	Input	Output
Screening_Process: Performs screening and loads data into the graph database.	**Party_Screening:** It performs party screening and stores results in a file. This will screen the parties against both cleansed and uncleansed List data.	Party_MainFlow3_input.txt This is the output of: *FCC_ER_Party _MainFlow2_2_ TransactionalMatchAnd Survivorship_v1.df*	It produces these: • To File: *Party_Cleansed _Hits.csv* • To Uncleansed List: *Party_ UnCleansed _Hits.csv*
	Screening_Output: Combines the results of cleansed and uncleansed matches and performs consolidation. This essentially means creating an alert in the Context Graph model and consolidating all the matches in a single alert.	It takes cleansed data file *Party_Cleansed_Hits.csv* and uncleansed data file *Party_UnCleansed_Hits.csv*. These are output of: *Party_Screneing.df*	Loads the data into graph database.

7 - Alert Management

In this section

Introduction to Alert Management

An alert is way to update the parties and bank about a sudden change in the financial status of a party or individual. When the financial changes happen or any negative news is flashed for any party, the bank gets a notification flag which helps them review the current and future financial liabilities associated with the affected party. Alert Management includes consolidation of alerts into cases and enabling prioritization of those cases.

Viewing Alerts

An alert appears only when system configuration is complete. **Alert** signifies that the screening stage is complete for the party.

The **View Alert** page displays consolidated alerts for parties and individuals.

Viewing Alerts

To view alerts, perform these steps:

1. Login to **Screener**.
2. Click **Alerts**. The **View Alert Page** is displayed.

   View Alert page displays this information:

Control	Description
Title	The title header displays identification of the list, name, and its current version number.
Advanced Search	Filter the search using advanced options, such as party id, alert status, alert status reason and generated by.
Filter	Select a parameter to filter the results in the list.

Control	Description
List Components	This part of the page displays the list and its content in tabular format. Each of the rows can be selected for different operations and some columns also allow sorting. Components of the list table are: 1. **Select All:** You can select all the records of the list on the page. 2. **Relevance Alert ID:** A unique ID assigned to the alert prior to consolidation. Click an ID to open a **detailed alert page** where the alert is described in detail. 3. **Date:** The date on which the alert was created. 4. **Party name:** The title of the party. It can be an individual or a party group name. 5. **Maximum list match score:** The cleansing match score is represented in percentage. A score closer to 100 is positive one. 6. **Negative media match score:** The negative media match score is represented in percentage. A score close to zero is good for alert to move into whitelist or get a discount. 7. **List:** Name of the list the alert belongs to. 8. **List type:** The type of the list. It can be PEP, SDN, or other. 9. **Alert status:** The status of the alert at present. It can be: a. Created b. Discounted c. Send To Case Management
Showing n of n records	This label signifies the number of records being displayed against the total number of records matching the present match criteria.
Rows per page	This drop down allows you to select the number of records you want to list on a single page. Possible values are: • 5 • 10 • 15 • 20 • 25

Business Rules for Alerts

The **Screening Solution** checks all the alerts generated since the last run.

Alert Consolidation and Auto Discount: If the party meets the criteria for discount, the discount is processed according to these rules:

1. **Discount Duplicacy:** There can be two cases:
   a. If the alert already exists with the same **List** and **Party details**, all the alerts will be combined into one.
   b. Its alert status is other than created, it is changed to **Discounted** and the Alert status reason will be set to **Duplicate Alert**.

Note: This rule is applicable only if the Alert Status is **Created**.

2. **Discount Whitelist:** There can be two cases:
   a. If the Party/List information for the Alert matches with that of Whitelist, the alert status is changed to **Discounted** and Alert Status Reason is changed to **Whitelist**. In this case, the alert is assigned to the Whitelist Queue if specified in the system configuration.
   b. If the Party exists in multiple lists and not all lists are Whitelisted, then the Alert remains unchanged.

      Note: This rule is applicable only if the Alert Status is **Created**.

3. **Alert Discount – Repeated Occurrences or Feedback Loop from Case Management:** If the Party has previous alerts with the same matching characteristics with an Alert Status of **Discounted** then:
   a. If the Alert Status Reason is **Feedback from Case Management**, then the Alert status will be set to **Discounted** and Alert Status Reason to **Feedback from Case Management**. The system will also capture the previous alert id.
   b. If the Alert Status Reason is not **Feedback from Case Management** and the count of alerts is greater than Number of occurrences for Auto Discount in Configuration then the alert status is set to **Awaiting Approval** and it is sent to Data Stewardship for approval. If the Steward approves it, the party list is added to the Whilelist and Alert status is changed to Discounted while the reason gets changed to Whitelist. However, if the Steward does not approve the request, the alert status is changed to **Processed**.

      Note: This rule is applicable only if the Alert Status is **Created**.

4. **Alert Discount – Confidence Threshold:** If the Alert Confidence Score is less than threshold specified in the Configuration for Auto Discount, then the Alert Status is updated to **Discounted** and Alert Reason is changed to **Below Configuration Threshold**.

   Note: This rule is applicable only if the Alert Status is **Created**.

Viewing Detailed Alert

This page displays details about the selected alerts. When you visit the **View Alert** page and select a particular party to view the alert details, this page is displayed.

The page is divided into sections elaborating details about the selected alert. It includes a graphical representation of **Maximum Cleansed List Match Score** and **Maximum Uncleansed List Match Score**. You can review the alert to take decision to allow a discount, move it to whitelist, or raise a case for further review.

For more information, see **Viewing Batch Screening Results** on page 49.

Extracting Alert Data

To extract your alert data to files of *.txt* format using filters such as **AlertStatus** and **AlertStatusReason**, follow this procedure:

Log in to the **Enterprise Designer** using your credentials and open the *Alerts_Interface_V1* job. Set the dataflow options and run the dataflow. For information on setting the dataflow options, see the **Adding Dataflow Runtime Options** section of the Dataflow Designer's Guide.

Output files *Hit.txt*, *Hit_Match.txt*, *Match.txt*, *MatchScore.txt*, *Alert.txt*, and *Alert_Hit.txt* are generated at the paths specified in the corresponding **File name** field of the **Write to File Options** window.

8 - Permissions and Access Controls

The permissions and access controls required for accessing **Screener** features are managed through the **System** menu option of **Management Console**. You can *view* or *modify* the approval rules, UDAs, and list metadata according to the settings specified here.

In this section

Granting access of Secured Entity Types

The secured entity types, such as UDA, ListEntry, Approval Rule, and ScreenerGroup are a category of items to which you want to grant or deny accesses. You can do this using the **Add Role** page in **Management Console**.

Note: All the Screener users need to be assigned the **BaseRole** in the FCC securities.

1. On the **Management Console** main menu, click **System** > **Security**.
   The **Roles** tab is displayed in the **Security** page.
2. Click the **Add Role** + icon.
   The **Add Role** page is displayed listing down the various modules.
3. Click the forward arrow > corresponding to FCC.
   A list of Screener-specific secured entity types is displayed.
4. Use the **Create**, **View**, **Modify**, **Delete**, and **Execute** check-boxes to grant the required accesses. This table describes the various accesses and the activities these enable.

   Note: To perform any action, the user first needs to have **view** permission to view the *UDA/list/rule*.

Secured entities	Access types
UDA	These permissions are required to perform specific operations on UDAs. • **Create**: To create a UDA and submit it for approval • **View**: To view a UDA • **Modify**: To edit a UDA and submit again for approval. To activate or deactivate a UDA • **Delete**: To delete a UDA • **Execute**: To approve or reject a UDA. This is needed only for the approvers.
UDA name	These permissions are required to perform specific operations on lists where UDA names are applied. • If you do not have access to a **UDA name**, you will not see it while creating a list • If another user has already created a list with the **UDA name** for which you do not have access, you will not see that list. • You can override permissions to specific UDA values (secured entities) through the **Access Control** page. For more information, see **Controlling accesses at Secured Entities level** on page 64.

Secured entities	Access types
List Country	The permissions are required to view and add countries during list creation. • If you do not have access to a **Country**, you will not see it while creating a list. • If another user has already created a list with the **Country** for which you do not have access, you will not see that list.
ListEntry	• View: View or export the list entries • Modify: Create a list entry, edit a list entry, activate and deactivate a list entry, disable or enable a list entry, import it, and send it for review and approval • Delete: Delete a list entry • Execute: Review, approve, or reject a list entry **Note:** You can control accesses to the list entry of different lists by using the **Access Control** page.
Approval Rule	The permissions are required to perform specific operations in the **Approval Rule** tab. • **Create**: To create a rule and submit for approval. • **View**: To view an approval rule • **Modify**: To edit a rule and submit again for approval. To activate or deactivate a rule. • **Delete**: To delete a rule

Permissions on Predefined UDAs:

- *UDA.WorkflowStatus*: Permissions do not have any impact on this UDA name, it is used to define the status displayed for each level.
- *UDA.Vendor*: These are available in **Roles** tab of the **Management Console**, you can add, delete, or modify the list of vendors.
- *UDA.ListType.PEP*, *UDA.ListType.SANCTIONS*, *UDA.ListType.SDN*: Permissions for this UDA are granted in the **Roles** tab of the **Management Console**. You can add new list types using the Add User Defined Attribute page. Any new *ListType* you add becomes available under the **FCC** secured entity type in the **Edit Roles** page, on which permissions can be granted. These are the permissions you can grant on ListTypes.
  - **Create**: To create a list and submit it for approval.

    Note: If you do not have access to **UDA**, you will not see it while creating a list. If another user has already created a list with the **UDA** for which you do not have access, you will not see that list.

  - **View**: To view a list
  - **Modify**: To edit a list and submit again for approval. To activate or deactivate a list
  - **Delete**: To delete a list

- **Execute**: To approve or reject a list. This is needed only for the approvers.

  Note: You can restrict accesses to specific secured entities in the ListType secured entity type by using the **Access Control** page. For more information, see **Controlling accesses at Secured Entities level** on page 64.

Controlling accesses at Secured Entities level

1. In the **Management Console** main menu, click **System** > **Security**.
   The **Security** page is displayed.
2. Click the **Access Control** tab.
3. Click the **Add access control** + icon.
   The **Add Access Control** page is displayed.
4. You can toggle between **Role** and **User**.
5. Select the *user* or *role* name from the drop-down list.
6. Click the **Add entity override** + icon.
   Add Entity pop-up is displayed.
7. Select the desired **FCC** secured entity types from the drop-down list. Some examples are: *FCC.ListEntry*, *FCC.UDA.ListType.Sanctions*, and *FCC.UDA.UDAName*.
   A list of the secured entities in the selected secured entity type is displayed.
8. Select the desired secured entities and click  .
   The chosen entities are displayed under the **Selected Entities** table.
9. Click **Add**.
   The selected entities are integrated with the selected role and displayed in the form of a list on the **Add Access Control** page.
10. To override permissions for the selected *user* or *role*, deselect or select the check-boxes corresponding to the desired attributes.

    Note: If permissions are not assigned to the parent entity type, you can assign the permissions here.

11. Click **Save**.
    The selected *user* or *role* would not be able to access the revoked attributes.

Providing differential access for List Entries

You can have different set of accesses for list entries of different lists. Use the **Access Control** tab on the **Security** page to grant this level of access. The accesses are:

- *Modify* access for uploading *ListEntry*
- *View* access for exporting *ListEntry*
- *Modify* access on a particular *ListType*, such as *UDA.ListType.Sanctions* to *Disable/Enable* List Metadata
- *Modify* access of *ListEntry* to *Disable/Enable ListEntry*

1. On the **Management Console** main menu, click **System** > **Security**.
   The **Security** page is displayed.
2. Click the **Access Control** tab.
3. Click the **Add Access Control** + icon.
   The **Add Access Control** page is displayed.
4. From the drop-down menu, select the Role to which you want to grant this granular access.
5. Click the Add entity override + icon.
   The **Add Entity** pop-up is displayed.
6. From the drop-down, select **FCC.ListEntry** secured entity.
7. In the left list box, select the list entries for which you want granular access and use the arrow to move those to the **Selected Entities** box.
8. Click the **Add** button.
   The selected list entries are displayed on the **Add Access Control** page under the *FCC.ListEntry* secured entity.
9. Assign the required **Create**, **View**, **Modify**, **Delete**, and **Execute** accesses to this role for the list entries.
   The users mapped to this role for the selected list entries will be able to perform differential tasks based on the accesses you just assigned. See the example below.

Example: In this scenario, no access has been granted to the secured entity type *FCC.UDA.ListType.SANCTIONS* in the *Role* page. In the **Access Control** page, you selected List1 and List2 secured entities in the *FCC.UDA.ListType.SANCTIONS* parent secured entity type. You assigned these accesses to *Role 1* and *Role 2*. (User 1 is mapped to Role1 and User 2 is mapped to Role 2).

Table 2: Role 1

	Create	View	Modify	Delete	Execute
List1		Yes			
List2			Yes		

Table 3: Role 2

	Create	View	Modify	Delete	Execute
List1			Yes		
List2		Yes			

These are the user actions and system responses based on the provided accesses for the list entries:

Action: User 1 tries to modify List1; **System Response**: Failure

Action: User 1 tries to view List1; **System Response**: Success

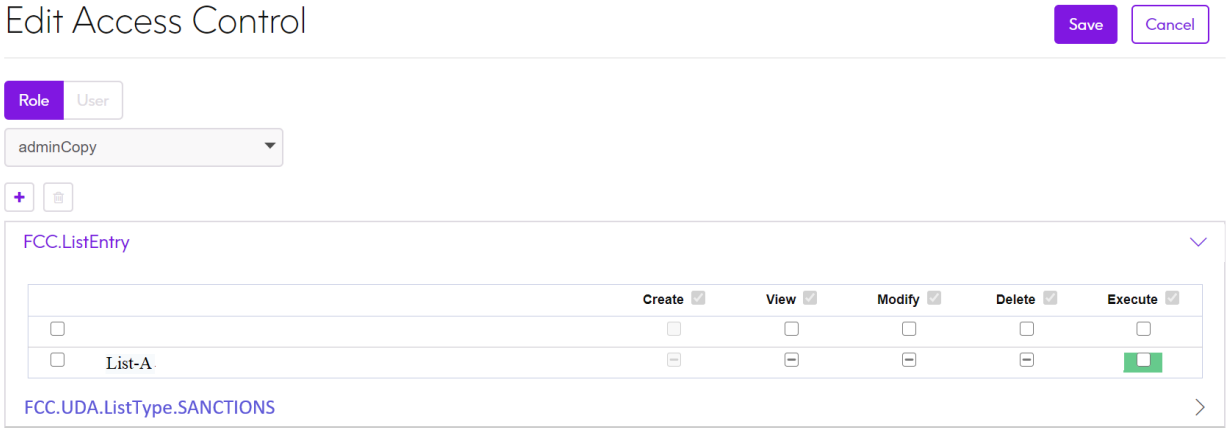
Action: User 1 tries to Modify List2; **System Response**: Success

Action: User 2 tries to modify List1; **System Response**: Success

Screener Access Control FAQs

1. What permissions do I assign to a user so he can only *Review/Approve* entries of a *List-A*, while for all other lists he can *View/Edit/Delete* but not *Approve/Reject*?

Remove the *Execute* permission on the parent entity type *ListEntry*. Go to **Access Control** and under *FCC.ListEntry* select *List-A* and override the *Execute* permission, as shown below.

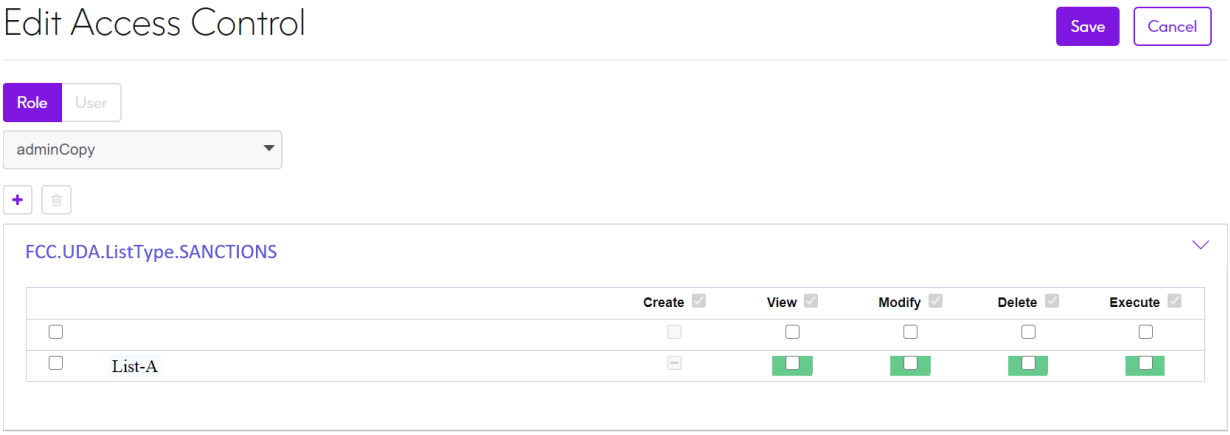


2. I want the user to *Create/View/Modify/Delete* only *Sanctions* type of list and not any other type of lists. What do I do?

   Only assign permissions to the entity type *UDA.ListType.Sanctions* and remove from other *ListTypes*.

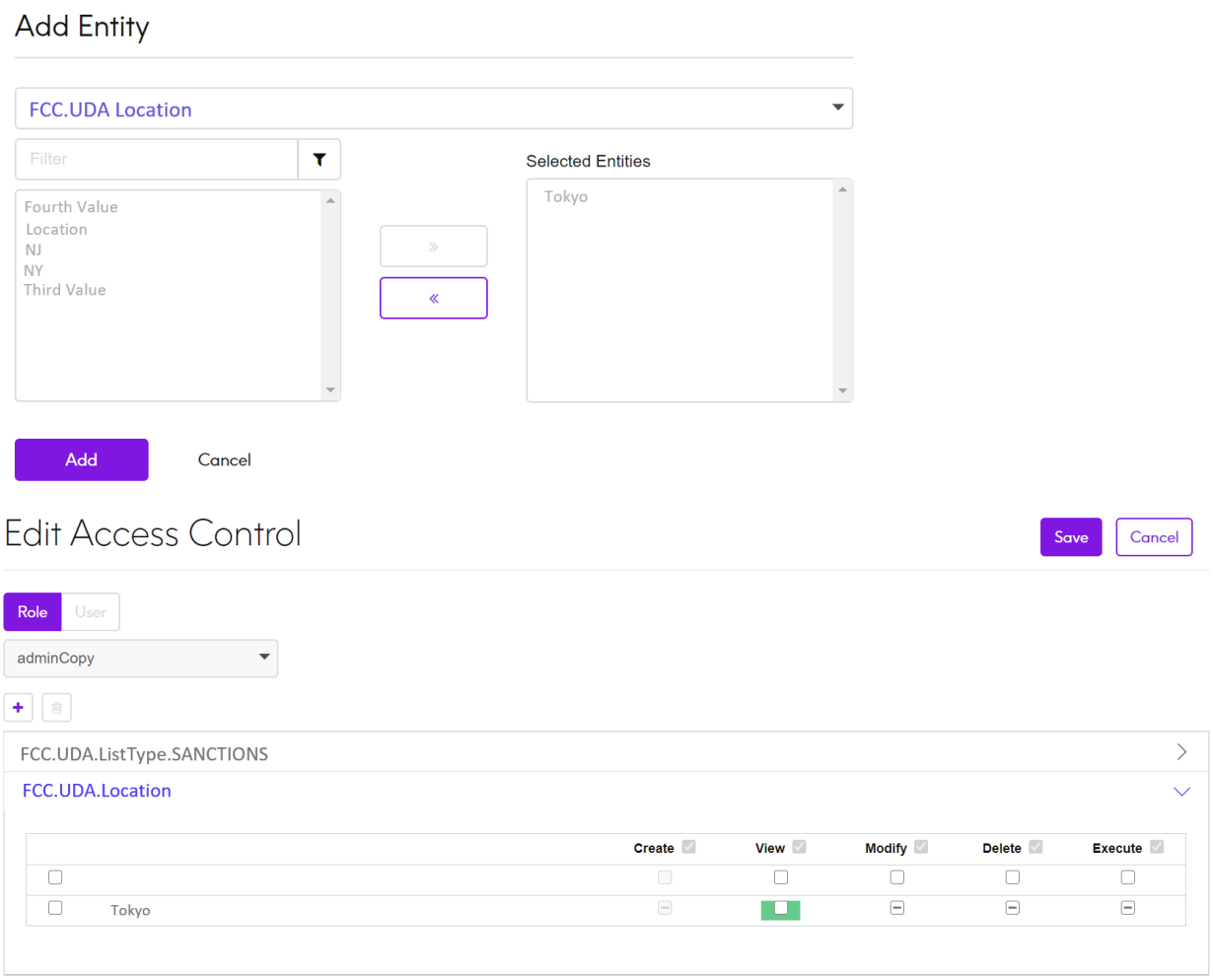
3. I want the user to *Create/view/Modify/Delete* only *Sanctions* type of list and not any other type of list. Also, the user should not be able to see a specific *List-A* which is of type *Sanctions*.

   Assign permissions as mentioned in question 2 above. After that, go to **Access control** and override the permission for *List-A*.



4. I have a list where I have a UDA named *Location* with values *Tokyo* and *NY*. How can I restrict the list view, so that a user can only view *NY* lists?

You will find an entity type *UDA.Location*. Assign view permission on the entity type *Location* and in the **Access control**, under *FCC.UDA.Location* select *Tokyo* and remove *View* permission for the *Role* or the *User*.



5. I am not able to create a list and the error says that mandatory field *Vendor* cannot be blank, but my form does not even display that field. What is the issue?

   You do not have permission on *UDA.Vendor*.

6. On the Add List page, the *Country* combo does not display any country name and the system does not allow me to save the list without country. What is going on?

   You do not have permission on *ListCountry*.

7. I have the appropriate permissions (*Execute*) to *Review/Approve* a list entry but I cannot see the entry in the **Review** tab. What could be the issue?

   This could be a case where the same user has submitted that list entry or the same user has approved it at previous level.

8. I have *Modify* permission on List but the **Edit** button is still disabled. What is the issue?

   Either the List is *Pending for Review* or is *Disabled*.

9 - Managing Reports

Screener helps you to view reports of the secured entities - **Lists**, **Screener Groups**, and **List Entries**, in a graphical form that conveys the relational information quickly and effortlessly. The reports improve decision-making, helping you identify potential deviations right on time for corrective actions.

In this section

Understanding Your Reports Dashboard

The **Reports** dashboard graphically shows the current status of the secured entities - **Lists**, **Screener Groups**, and **List Entries**, through bar charts showing the state of the **Actions** and the **Count** of the secured entity. For more information about secured entities, see **Secured Entities** on page 5.

The dashboard allows you to perform these tasks:

- Refresh reports: Click the **Refresh Report** icon to refresh the reports.
- Filter reports: Click **Create Custom Report** at the top-right corner of the dashboard to filter the reports. For more information, see **Creating Custom Reports** on page 71.
- Download reports: Click the **Menu** icon at the right corner of the secured entity to download the report in three formats as listed below:
  - SVG
  - PNG
  - CSV
- View **List Entries** status: Select a **List** from the drop-down menu of the **List Entries** to view the status of the **List Entries** that belongs to a particular **List**.

Viewing status of secured entities

The dashboard is divided into three sections, one each for **Lists**, **Screener Groups**, and **List Entries**.

For **Lists** and **Screener Groups**, the information block on the left side displays these details:

- **Total**: The total number of **Lists** or **Screener Groups** defined in the system.
- **Inactive**: The number of inactive **Lists** or **Screener Groups** in the system.
- **Active**: The number of active **Lists** or **Screener Groups** in the system.

The bar chart adjacent to the information blocks displays the number of **Lists** or **Screener Groups** in various stages of action, such as:

- **Create**
- **Modify**: The colour coding further segregates the entities based on whether the modification is approved or is pending approval.
- **Enable**
- **Disable**: You can see how many disabled entities have been approved, how many are still pending approval, and the number of rejected disablement of entities.
- **Delete**: Shows the number of approved deletions and rejected deletion.

In case of **List Entries**, use the **List** drop-down menu to select the entry for which you want to see the details. All the information described above for **Lists** and **Screener Groups** are displayed for the selected list entry.

Creating Custom Reports

You can filter the entities based on your requirement of a customized report. For example, you want to view all the **Screener Groups** in an active state by a specified date, or you want to view all the **Screener Groups** approved by a specified user. You can do this, using the **Create Custom Report** button on the dashboard. The custom report also allows you to view the history of the secured entities by selecting the past dates.

Note: The custom report is useful for audit purposes.

To create a custom report, perform these steps:

1. On the **Reports** dashboard, click **Create Custom Report**.
   The **Custom Report** page is displayed.
2. In the **Date** field, use the icon to select a date and time.
3. In the **Entity Type** field, select the type of entity, for example, **Screener Group** or **List**.
4. In the **Activation Status** field, select the report status, for example, **Active** or **InActive**.
5. In the **Approval Status** field, select the status for which you want to view entity reports. For example, if you select **Pending**, the report will be for all the entities that are in pending state of various activities. The options are:
   - **Pending**
   - **Approved**
   - **Rejected**
   - **Deleted**
   - **Disabled**
   - **Not Submitted**
6. In the **Approval By** field, select the approver for the entities that you want in your report.
7. In the **Submitted By** field, select the submitter for the entities that you want in your report.
8. Click the **Filter** icon.
   These details are displayed based on your filter criteria:
   - **Name** of the entities
   - **Source** of the entities
   - **State** of the entities, such as **Update-Approved** or **Create-Approved**
   - If the entity is **Active**

9. To view the metadata events related to any of the filtered secured entity, click its name in the list.
   The **History : List** page is displayed showing these details:
   - A graphical timeline of metadata events related to the selected entity.
   - A list of metadata events below the bar chart.

   a. Use the **Start Date** and **End Date**  icons on the top of the page to select the date range for which you want to view the metadata event.
   b. Use the drop down list on the top-right corner of the page to select if you want to view the metadata events for every **Minute**, **Hour**, **Day** or **Month**.
   c. Click the **Filter**  icon to view the results for the selected parameters.
   d. Use the forward  and the backward  arrows on the sides of the drop-down to move through the events.
   e. Use the **Menu**  icon to download the metadata event history as PNG or SVG.

10 - Audit Logs

In this section

Audit Logs

The audit log records all the activities you perform using the Screener. It records events that occur when you create and modify objects on your system, as well as events that occur when you run jobs.

Some examples of events recorded in the audit log include creating, viewing, approving, disabling, or deleting a list, list entries, or a screener group. It also records activities peformed on UDAs.

To access the audit log, perform these steps:

1. Open **Management Console**.
2. Go to **System** > **Logs**.
3. Click **Audit Log**.
4. In the left panel, select `FCC Screening` as **Source**.
   It lists a log of all the activities (Events) performed by different users on Screener . The details displayed are:
   - **Severity**: Indicates if the event is an error, warning, or an information.
   - **Date/Time**: The date and time of the event.
   - **User**: The user account that performed the action.
   - **Source**: The software component that generated the event. **FCC Screening** in this case.
   - **Event**: The action that occurred. For example, `Read`, `Update-Approve`, `Uploaded`, `Create`, `List Ingestion`, and `Create-Approve`.
   - **Type**: The part of the system that was modified by the event. For example, `List Entry`, `List`, `UDA`, and `Screener Group`.
   - **Object Name**: The name of the item that generated the log entry.
5. To view additional details about any of the log entry, click the arrow next to the **Severity** field.
   A sample additional data is given below:

   Details: List Entry : Update-Approve

   Server: 172.31.6.103

   Additional Data:

   Update-Approve List Entry: {"CurrentStatus":"Updated","mailToUser":"admin",

   "entityName":"U03","active":true,"id":"1558938262735_U03_UnCleansed"}

11 - Mail Notifications

In this section

Mail Notifications

In Screener, you receive a mail notification for every approval or rejection you perform for the entities (List, List Entries, UDAs, and Screener Groups). You receive notification for every list ingestion too.

> **Note:** You need to set up a mail server in Management Console in order to receive the email alerts. For more information, see **Configuring a Mail Server** in the Administration Guide.

Notifications are based on the Approval Rule applied to the entities. Let us take example of an approval rule "*Rule1*" that applies to lists, where,

- Two levels of approval are required
- Level 1 approval is assigned to the *Role 1*
- Level 2 approval is assigned to *Role 2*
- Role 1 is mapped to user *U1*, *U3*, and *U5*
- Role 2 is mapped to users *U2*, *U4*, and *U6*

Now, if a user, *U7* creates a list and sends it out for review, it will go for Level 1 approval and notification will be sent to:

- *U7* (submitter of review)
- *U1*, *U3*, and *U5* (mapped to Role 1)

For list ingestion through file, all the users mapped to roles defined in this property of the `fcc.properties` file will be notified:
`fcc.spectrum.list.ingestion.email.roles.configurable`

Table 4: This table describes the scenarios in which notifications are sent to users

Entities	Actions that trigger notifications	Approval rule applied?	Notification sent to
List, ListEntry, UDA, and ScreenerGroup	Submit for approval, Enable, Disable, Delete	No	Creator
		Yes	Notification sent to approver for action and to creator at each stage

For list ingestion, all users mapped to the role <*ListIngestionNotifiers*> get notifications for ingestion and any errors encountered in the process.

A sample mail notification:

Some items have been Submitted for Approval. Refer below details for individual statuses.

Item Type: *Portfolio*, Item id: *6af6b82f-3548-445a-8e49-5ce6de51065e*, Item Name: *SG8*, Status: *Submitted for Approval*.

Thanks,

Screener Team

> **Note:** The templates of notification mails are at this location: `<folder where you installed Spectrum>\server\modules\fcc\Email`

precisely

2 Blue Hill Plaza, #1563
Pearl River, NY 10965
USA

www.precisely.com