
Aggie Documentation

Release 2.0

Tom Smyth and many others

Mar 03, 2022

Contents

1	Introduction	1
1.1	Achitectural Design	1
1.2	Acknowledgements	2
2	Installation	3
3	Settings	5
3.1	Fetching	5
3.2	Social Media Feed Authentication	6
3.3	Generating Source Tokens	8
3.4	Email Settings	12
3.5	Widgets	16
4	Establishing the SMTC	19
4.1	What is the SMTC?	19
4.2	Key Term Definitions	20
4.3	Public Event Monitoring Checklist	20
5	Using Aggie	21
5.1	Sources	21
5.2	Reports Page Activities	22
5.3	Batch Mode	31
5.4	Tags	33
5.5	Groups Page Activities	41
6	User Management	47
6.1	User privileges	47
6.2	Creating a New User	47
7	Indices and Tables	49

CHAPTER 1

Introduction

Aggie is a real-time, user-generated content aggregation and analysis platform premised on the core principles of:

Technological neutrality: Support content from popular social media platforms along with media originating from purpose-built systems (namely those specific to election monitoring, crises, or conflict response).

Computer enabled expert analysis: Automated computer analysis augments and enhances expert human real-time reasoning and decision making.

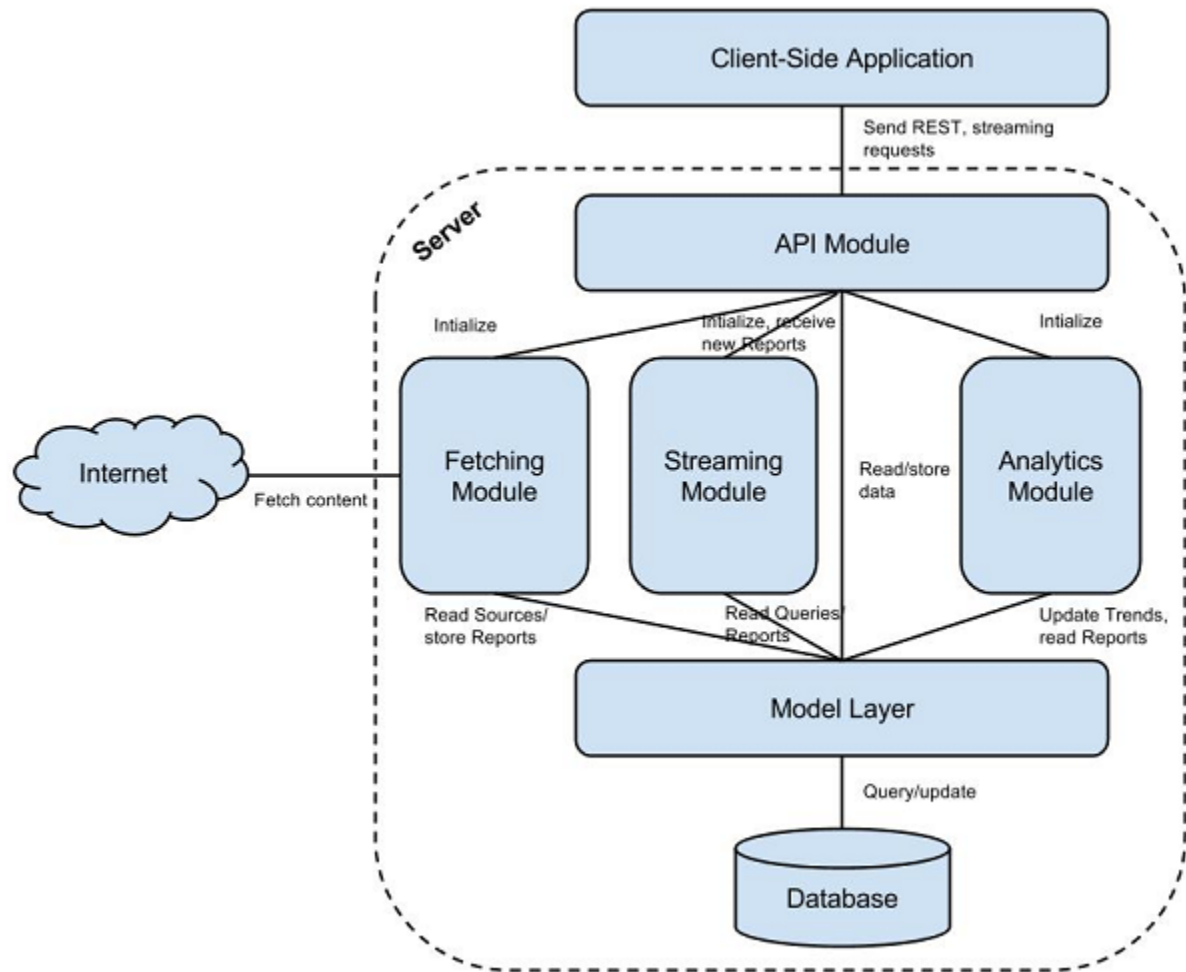
Real-time response: Moving from online report aggregation to analysis, escalation and response within one hour.

Big data: Supporting up to 1,000 incoming reports per second.

Open source principles: Aggie is fully open source and welcomes contributions.

1.1 Architectural Design

Architecturally, Aggie has two modules; the backend server that crawls the internet to aggregate user generated content, and a front end client API that runs on a browser.



Architectural

Design

1.2 Acknowledgements

Aggie has reached thus far from the generous contributions of many developers and collaborators. To date, sixteen developers have contributed code to Aggie’s Project ([list here](#)). We thank everyone involved in the open source community of Aggie.

CHAPTER 2

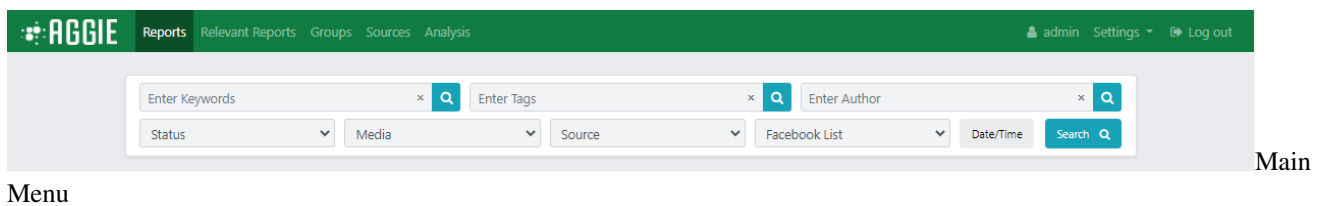
Installation

Aggie can be installed by following the instructions in the [GitHub repository](#).

CHAPTER 3

Settings

After a successful login, you will see Aggie's front end interface as below.



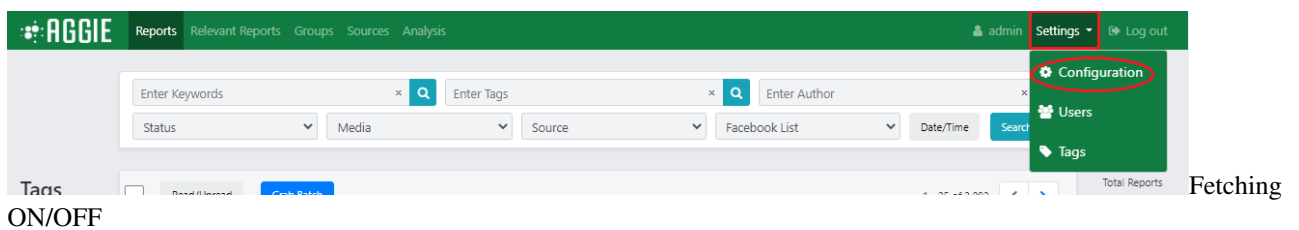
3.1 Fetching

Fetching allows Aggie to receive feeds from all sources at a global level.

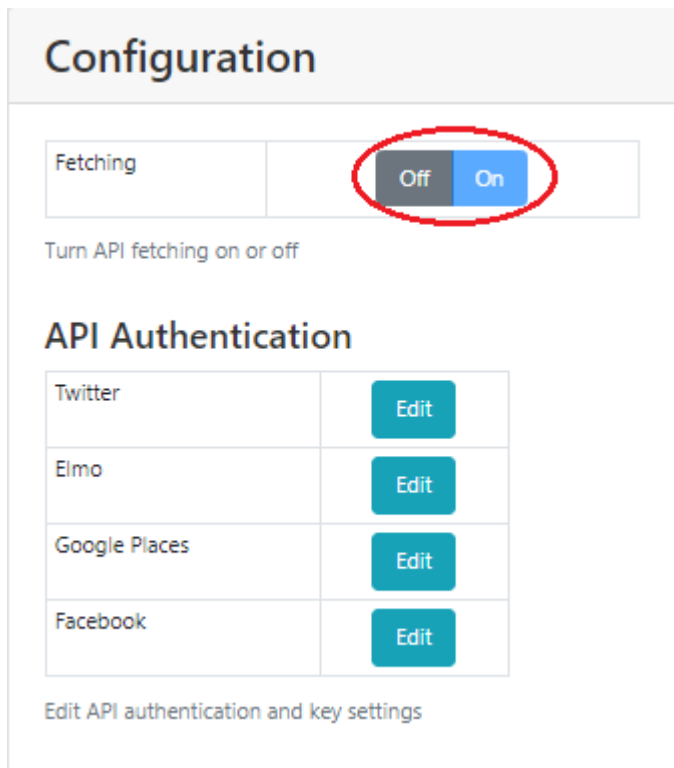
3.1.1 Toggling ON/OFF Fetching

Fetching can be enabled or disabled by toggling ON/OFF the fetching toggle. To toggle ON/OFF fetching, please follow the steps below.

1. From the menu bar, click **Settings** and select **Configuration**.



2. Click **ON/OFF** on the fetching toggle to switch fetching ON/OFF.

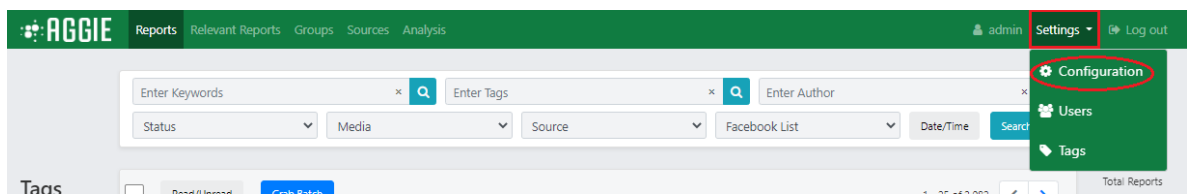


Fetching ON/OFF

3.2 Social Media Feed Authentication

3.2.1 Adding Media Feeds to Aggie

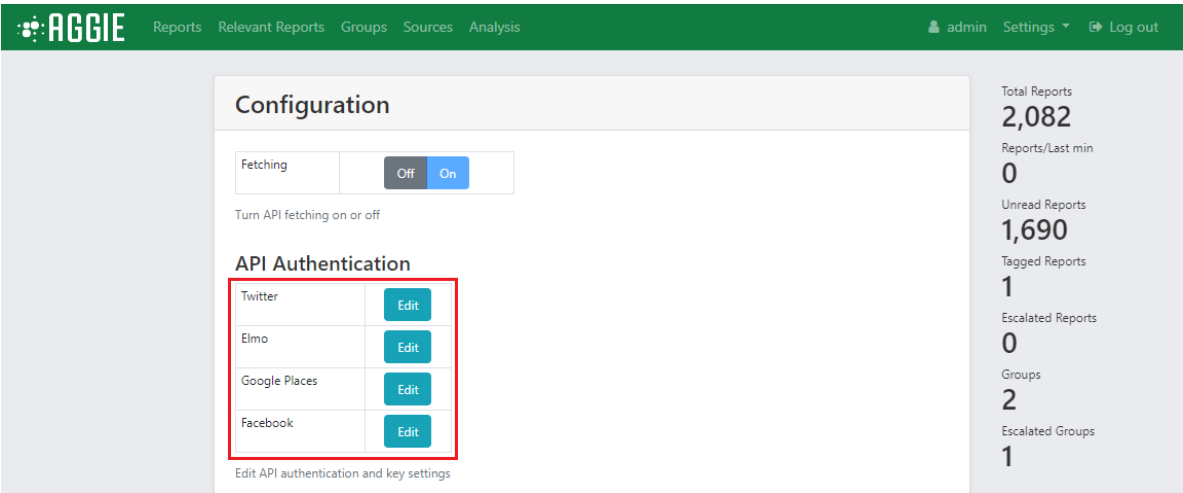
1. From the header menu, click on **Settings**.



Menu

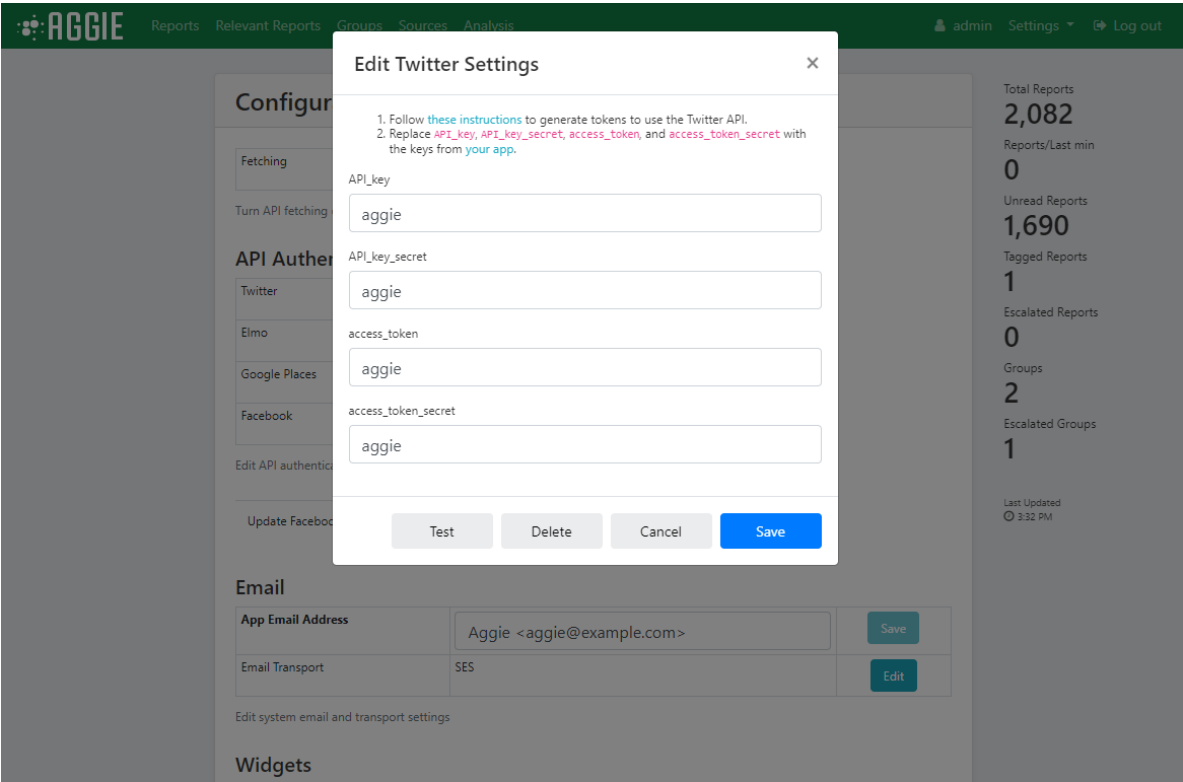
Settings

2. From the dropdown list, click on **Configuration**.



Authentication

3. Click on **Edit** to authenticate the Twitter, Facebook, or Elmo feed settings.



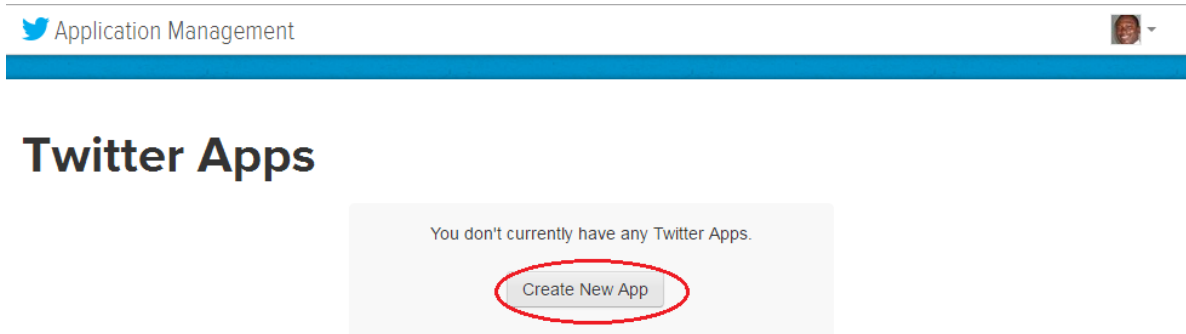
Authentication

Note: Now we need to generate the access tokens for all social media sources. After that, we would copy and paste respective authentication tokens generated for each of the social media feeds, save the settings and toggle the Fetching switch ON.

3.3 Generating Source Tokens

3.3.1 Twitter API Access Token

1. Visit [Twitter's Apps Page](#) and login with your Twitter Credentials.
2. Click on the **Create New App** Tab.



Twitter

Apps

3. Fill in the *Application Details* and agree to the developer agreement at the bottom to create the app.


The screenshot shows the 'Create an application' form on the Twitter 'Application Management' page. The form is titled 'Application Details' and contains four main sections, each with a text input field and a descriptive note:


- Name ***: A text input field. Below it, a note says: 'Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.'
- Description ***: A text input field. Below it, a note says: 'Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.'
- Website ***: A text input field. Below it, a note says: 'Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens. (If you don't have a URL yet, just put a placeholder here but remember to change it later.)'
- Callback URL**: A text input field. Below it, a note says: 'Where should we return after successfully authenticating? OAuth 1.0a applications should explicitly specify their oauth_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.'

Twitter

Apps

- This will create access tokens as indicated below.

 Application Management



Aggie Test

[Details](#)
[Settings](#)
[Keys and Access Tokens](#)
[Permissions](#)

Test OAuth

Application Settings

Keep the "Consumer Secret" a secret. This key should never be human-readable in your application.

Consumer Key (API Key)	1KnQdVO3loP2cUzOg4d5T8TY3
Consumer Secret (API Secret)	Mw1moGZ28adOgGBAz95FZB6CGxeHbTM03ND5OEWt9K0xgUAKcH
Access Level	Read and write (modify app permissions)
Owner	bayor83
Owner ID	148665540

Application Actions

Regenerate Consumer Key and Secret
Change App Permissions

Your Access Token

You haven't authorized this application for your own account yet.

By creating your access token here, you will have everything you need to make API calls right away. The access token generated will be assigned your application's current permission level.

Token Actions

Create my access token

Twitter

Apps

- Click on **Create My Access Token** to create *Access Token* and *Access Token Secret*.

Your Access Token

This access token can be used to make API requests on your own account's behalf. Do not share your access token secret with anyone.

Access Token	148665540-XbYu1STZA7PevfCQrdAh53ZSbvZ6iUBw888YGPxt
Access Token Secret	GI1PzdiZ7IsNPOHpG8Ej2MqT9n6B6DCD1Ch06HLHIsL70
Access Level	Read and write
Owner	bayor83
Owner ID	148665540

Token Actions

Regenerate My Access Token and Token Secret Revoke Token Access

Twitter


Apps

- With these access tokens, follow the instructions from [Adding Media Feeds to Aggie](#) section and edit the Twitter settings in Aggie.

3.3.2 WhatsApp messages


The WhatsApp feature is documented in a [conference paper](#). As WhatsApp does not currently offer an API, a Firefox extension in Linux is used to redirect notifications from [web.whatsapp.com](#) to Aggie server. Thus, you need a Linux computer accessing WhatsApp through Firefox for this to work. Follow these steps to have it working.

- Install Firefox in Linux using your distribution preferred method.
- Install [GNNotifier](#) add-on in Firefox.
- Configure the add-on [about:addons](#):
 - Set Notification Engine to Custom command
 - Set the custom command to `curl --data-urlencode "keyword=<your own keyword>" --data-urlencode "from=%title" --data-urlencode "text=%text" http://<IP address|domain name>:2222/whatsapp`
 - We suggest setting your keyword to a unique string of text with out spaces or symbols, e.g., the phone number of the WhatsApp account used for Aggie. *This keyword must be the same one as the one specified in the Aggie application, when creating the WhatsApp Aggie source.*
 - Replace `IP address|domain` with the address or domain where Aggie is installed (e.g., `localhost` for testing).



GNotifier 1.11.0

By **mkio**



Replaces built-in notifications with the OS native notifications. It works on Linux and Windows 10.

This add-on makes notifications nicely fitted in to style of Linux desktop or Windows 8.1/10. It replaces all standard notifications from web-pages or other add-ons with native OS notifications. Additionally to above, GNotifier provides own implementation of two new types of alerts: "Downloads Complete" and "New E-mail".

In Linux environment, GNotifier entirely relies on libnotify library, so if libnotify is not present in your system, it will not work.

Automatic Updates	<input checked="" type="radio"/> Default <input type="radio"/> On <input type="radio"/> Off
Last Updated	October 18, 2017
Homepage	https://github.com/mkiol/GNotifier
Rating	★★★★★ 39 reviews
Notification engine	Custom command
Custom command	<code>curl -data-urlencode "keyword=<your own keyword>" -data-</code>

Add-on for Firefox

4. Visit web.whatsapp.com, follow instructions, and *enable browser notifications*
5. Notifications will not be sent to Aggie when browser focus is on the WhatsApp tab, so move away from that tab if not replying to anyone.

3.3.3 Google Places API

Aggie uses Google Places API to add location to the groups, letting users to search for groups by location. It also powers the maps generated by Aggie. Google accounts with a credit card get a higher free quota of API calls than those accounts without credit card.

1. Get your key for [Google Places API](#) from your Google account and copy it here. Remember to limit the domain to where Aggie is hosted (e.g., aggie.africanelections.org) when creating you new key.

3.3.4 ELMO

1. Log into your *ELMO* instance with an account having *coordinator* or higher privileges on the mission you want to track.
2. In your ELMO instance, mark one or more forms as *public* (via the Edit Form page). *Note the Form ID in the URL bar (e.g. if URL ends in /m/mymission/forms/123, the ID is 123).*
3. Visit your profile page (click the **icon bearing your username** in the top-right corner) and copy your *API key* (click **'Regenerate'** if necessary).
4. From Aggie, click **Settings > Configuration** and edit the ELMO settings. Remember to toggle the switch on, once you have saved the settings

3.4 Email Settings

This must be set up to allow newly created users to receive emails from Aggie with their login credentials. Three transport options have been implemented using nodemailer.js:

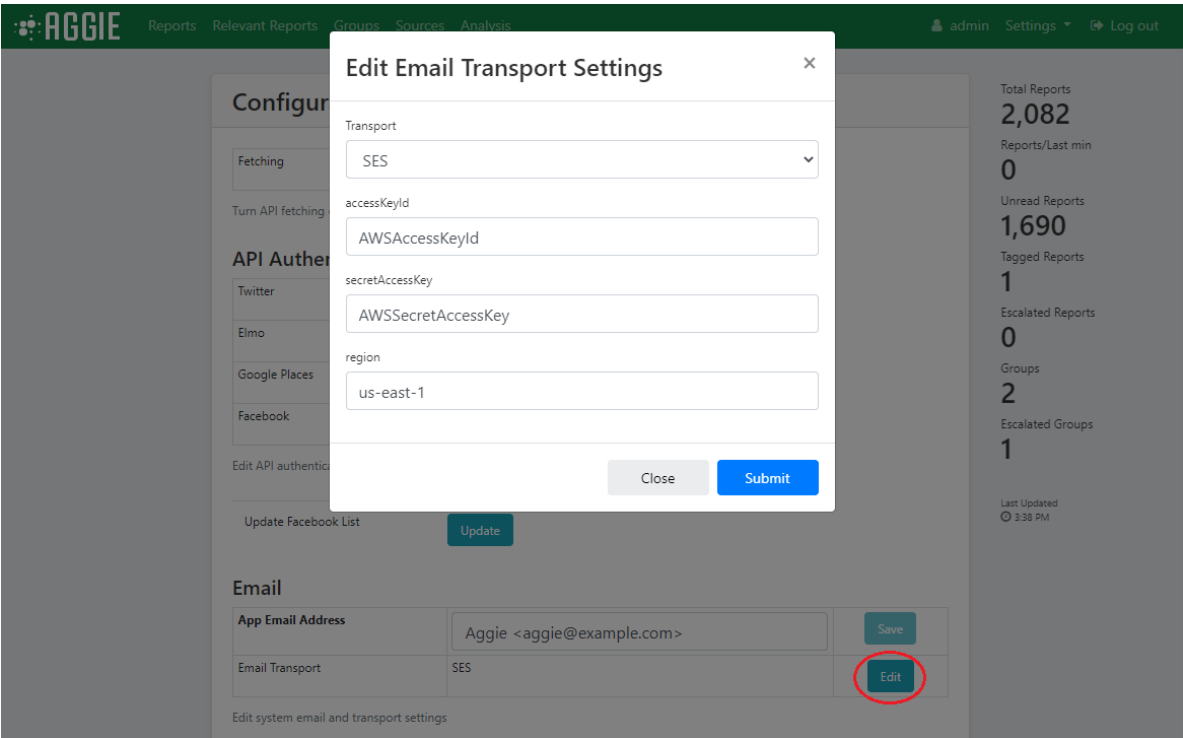
1. SMTP, which requires having access to a working SMTP server.
2. Amazon Simple Email Service (SES).
3. Sendgrid, an online mail service accessible through a simple API.

In this example we are going to set up the email with Sendgrid's service.

1. Click the **Settings** tab and select the **Configuration** option in the dropdown list.

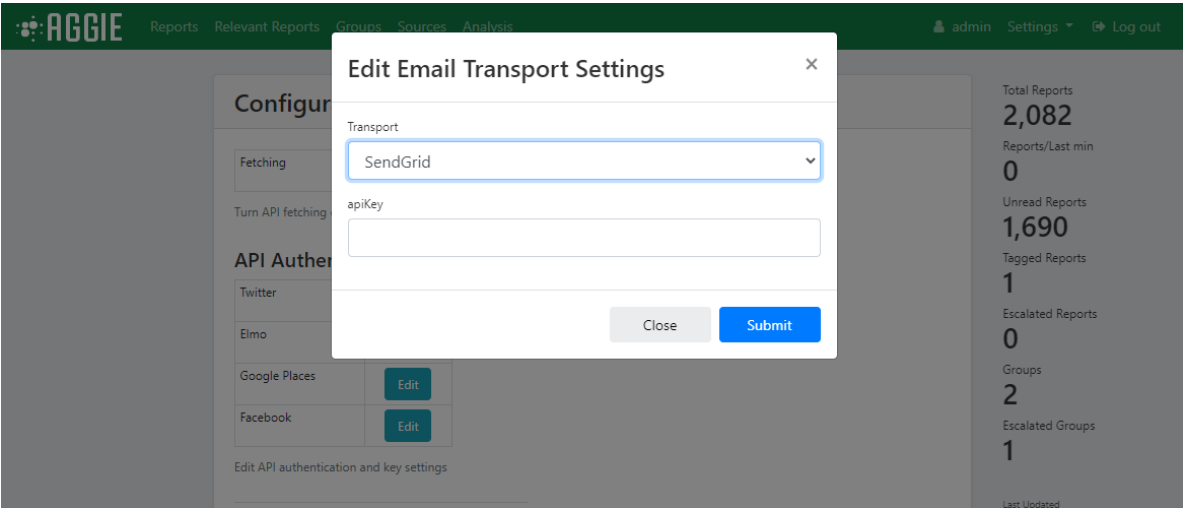
The screenshot shows the Aggie web interface. The top navigation bar has a green header with the Aggie logo and links for Reports, Relevant Reports, Groups, Sources, and Analysis. The user is logged in as 'admin' and the 'Settings' tab is selected. The main content area is titled 'Configuration'. It includes a 'Fetching' toggle set to 'On', a section for 'API Authentication' with 'Edit' buttons for Twitter, Elmo, Google Places, and Facebook, and an 'Email' section. The 'Email' section is highlighted with a red box and contains 'App Email Address' (Aggie <aggie@example.com>) and 'Email Transport' (SES). The 'Edit' button for the Email Transport is circled in red. A sidebar on the right displays various statistics. The bottom right of the page is labeled 'Email'.

2. Click **Edit** on the Email transport row of the email section (the last Edit).



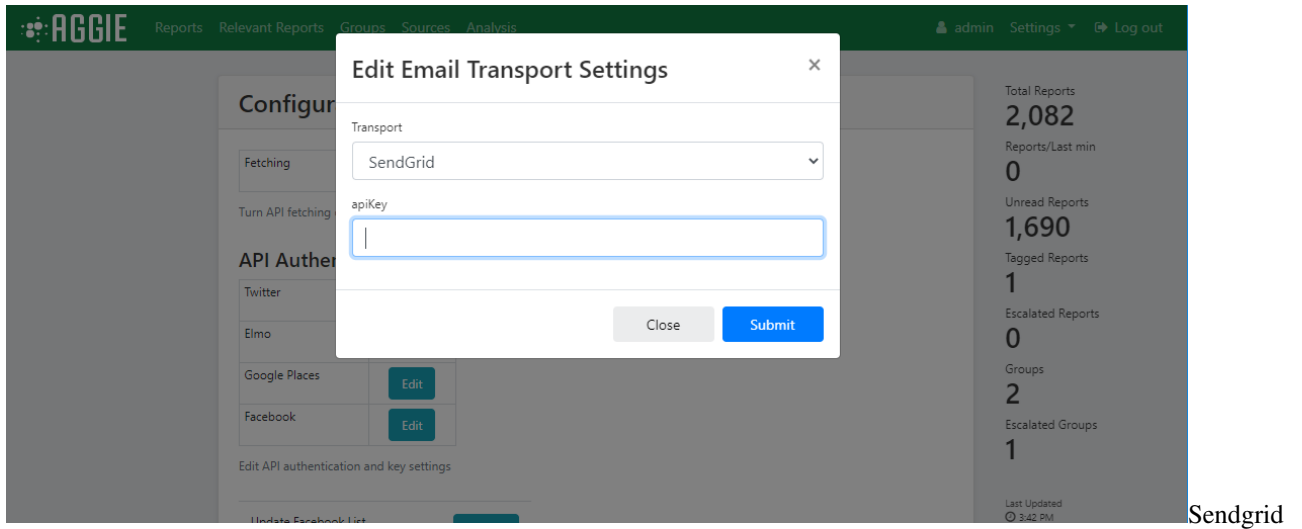
Sendgrid

3. Choose the *Transport method* as *SendGrid*.



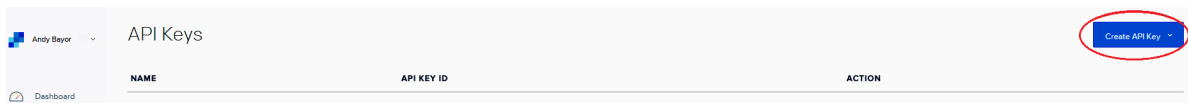
Sendgrid

4. Aggie then requests an *API key* for use with SendGrid as in the screenshot below.



3.4.1 Generating SendGrid API Key

1. Visit [SendGrid's Page](#) and set up an account. Sendgrid will take one or two days to verify your account before activating it.
2. From your account click the **Settings Menu** and select *API keys*
3. Click the blue **Create API Key** on the top right.



4. Select *General API key*.



5. Type a name for the API e.g. *Aggie API key* and set the appropriate *permissions*. The only permission needed for this key is the '*Mail Send*' one.

Add New General API Key

Cancel

Save

API keys are a great way for you to manage your permissions around how your account uses our API. Greater security and flexibility can be leveraged through the use of our API keys.

NAME OF THIS KEY*

Aggie API key

	NO ACCESS	READ ACCESS	FULL ACCESS
Mail Send	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mail Send	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

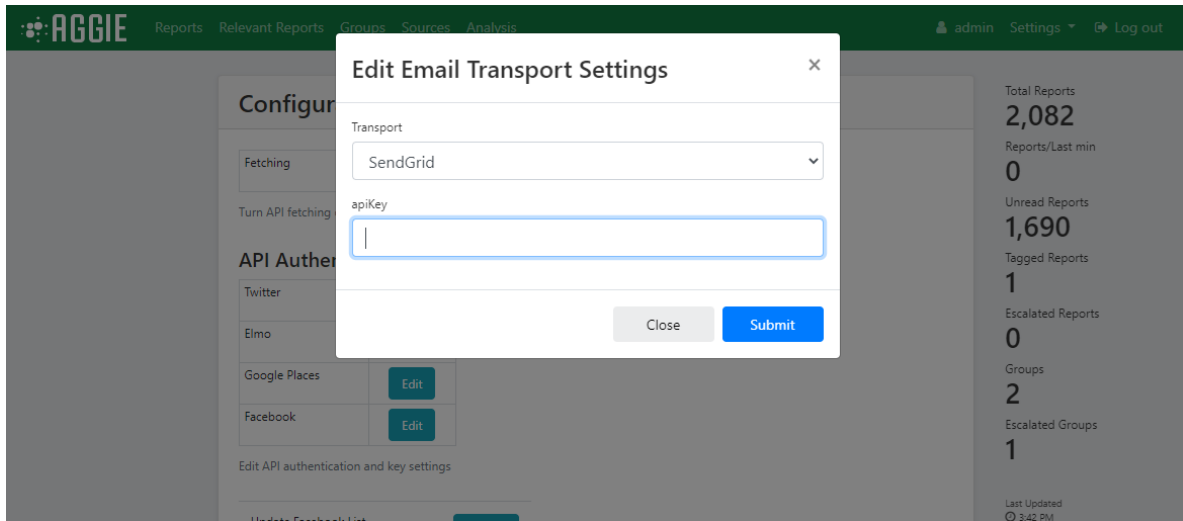
	NO ACCESS	READ ACCESS	FULL ACCESS
Alerts	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Alerts	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

	NO ACCESS	READ ACCESS	FULL ACCESS
Email Activity	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email Activity	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Feedback

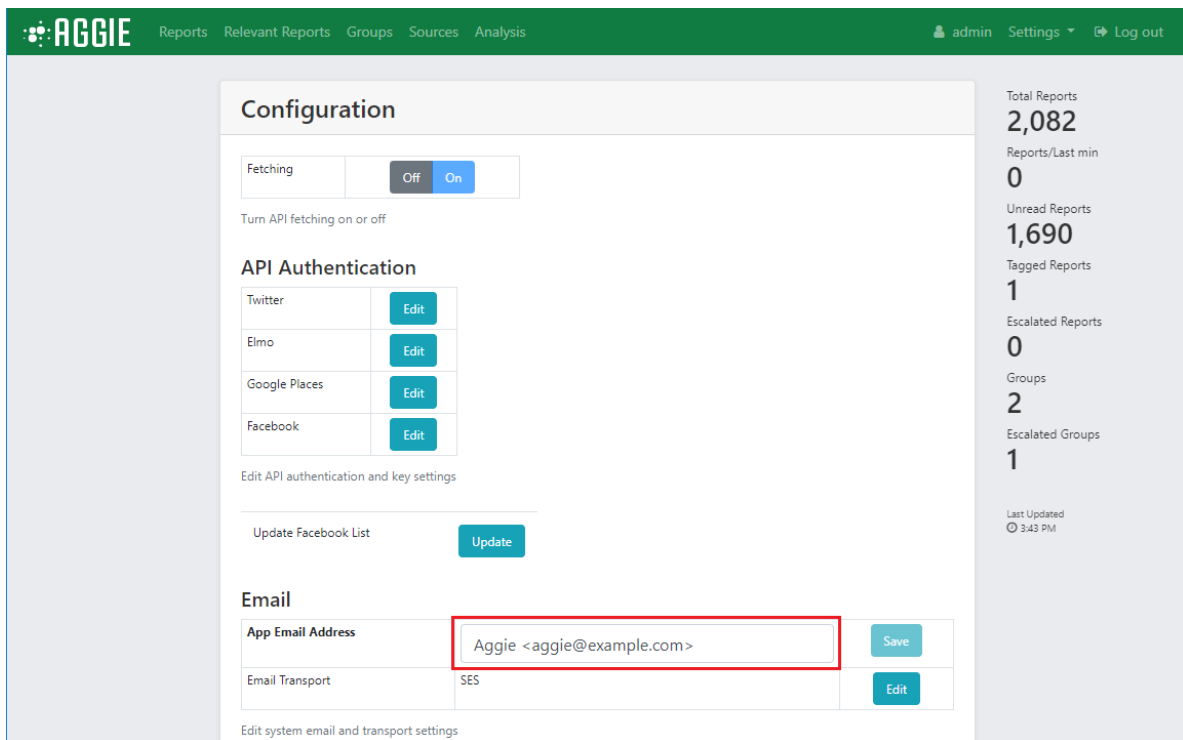
Sendgrid

- 6. Click **Save** to generate an API key for use with Aggie.
- 7. Copy the API key and paste it into the *api_key* field referred to in *Transport Email* section and click on Submit.



Sendgrid

8. Set the *App Email Address* as the email address you used for your SendGrid application.



Sendgrid

3.5 Widgets

Widgets are web components that can be added to webpages. In Aggie, widgets are used to display information for public consumption outside of the [SMTC](#). As usual, there is need to be careful with what information is made public, so use widgets with care so not to link individuals with information that may compromise them. At the moment there is only one widget available, the Public Group Map.

3.5.1 Public Group Map

The Public Group Map displays those *groups* that have been marked *public* by the escalation team. It uses the Google Places API, and thus, should be *set* before using the map.

1. *Center* and *zoom* define the main variables for the map. It will be centered in the country, city or other location you choose. The *zoom* variable specifies how large area will be displayed in the map.
2. You can see the result at https://widget/public_incident_map.html
3. You can add the map to any webpage with the following code:

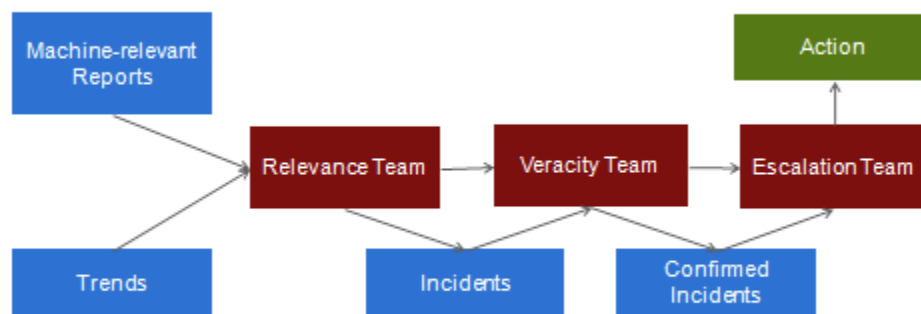
```
<iframe src="https://<your-domain>/widget/public_incident_map.html" width="xxx"
↪height="yyy"></iframe>
```

1. Markers in the map have different meanings according to the their color, as shown in the table below. You can copy this table for your site if needed.

Establishing the SMTC

4.1 What is the SMTC?

The **Social Media Tracking Centre** (SMTC) serves as a physical space in which volunteers gather and work around the clock to monitor social media traffic via Aggie. SMTC members monitor and respond in real-time to reports from digital platforms such as Twitter, Facebook, ELMO, Ushahidi, and RSS feeds from blogs or traditional media sites. Key teams of the SMTC include the *tracking team*, the *veracity team*, the *escalation team*, the *leadership team* and the *embedded stakeholder team*. Team members need training on Aggie prior to the event being monitored. The SMTC Leadership Team is essential for coordinating activities in the centre. The diagram below indicates the operational flow of the various teams in the SMTC.



Work Flow

SMTC

4.2 Key Term Definitions

4.2.1 Tracking Team

The *tracking team* is responsible for reading through the real-time streams of social media reports aggregated by Aggie either in batches or by navigating through pages. Their workflow involves going through each report and creating an incident from actionable reports.

4.2.2 Veracity Team

After the tracking team creates an incident, the *veracity team* takes over to investigate and verify the truthfulness of the incident created by trackers using some of the below strategies:

1. Using social media platforms to communicate with the author of the report (i.e. Tweeting at the author).
2. Using triangulation to build evidence from other reports and sources.
3. Contacting formal monitors in the field.
4. Contacting embedded SMTC representatives who can ask relevant stakeholders to confirm or deny veracity.

4.2.3 Escalation Team

Once the veracity team has confidently verified an incident to be true, the *escalation team* reports the incident to the SMTC embed assigned to relevant stakeholders, providing all relevant information gathered. The escalation team will move swiftly to communicate verified incidents so that relevant stakeholders may respond in real-time.

4.2.4 Stakeholder/Embedded Team

Embeds are key persons placed in civil organizations or government institutions invested in the coordination and supervision of the event being monitored. Embeds communicate verified incidents to these organizations, called stakeholders, which get more details about and respond to these incidents. Ideally, embeds are known and trusted by stakeholders to ensure information reported from the SMTC is valued.

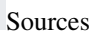
4.3 Public Event Monitoring Checklist

To be set for a monitoring event, cross check the status of the items and activities in the table below a day to deployment of the monitoring.

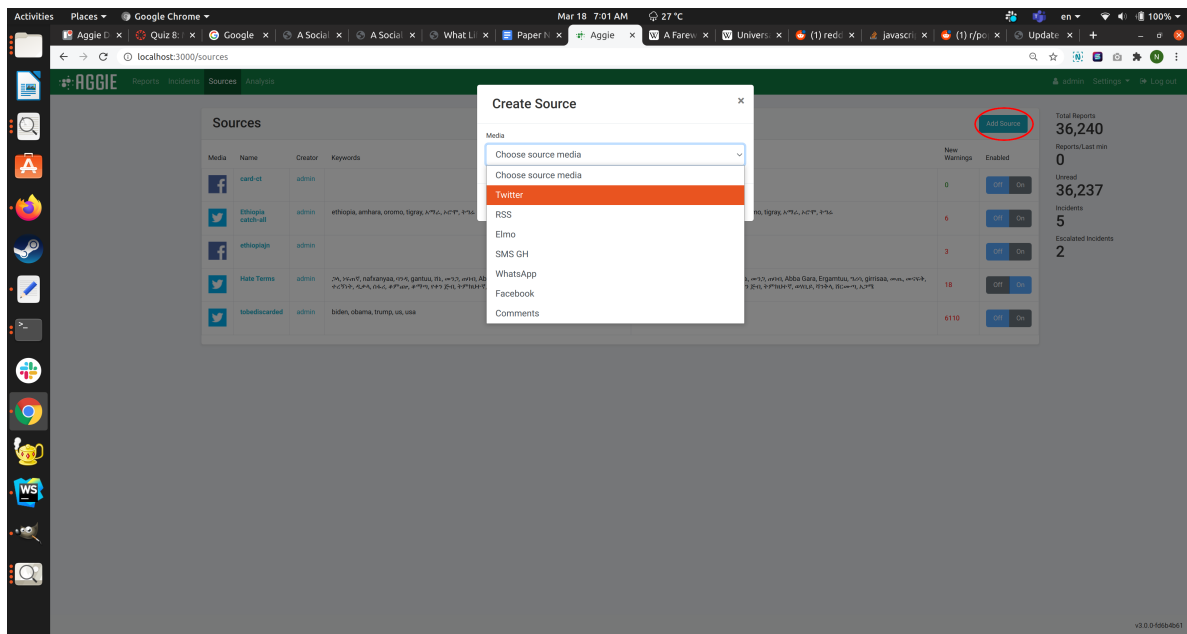
5.1.1 What is a Source?

Sources can also be services that send reports directly to Aggie. Currently, we have implemented support for WhatsApp and [SMSGH](#), a service that forwards SMS text messages sent to [short codes](#).

1. Click on **Sources** on the Header Menu of Aggie's main page.

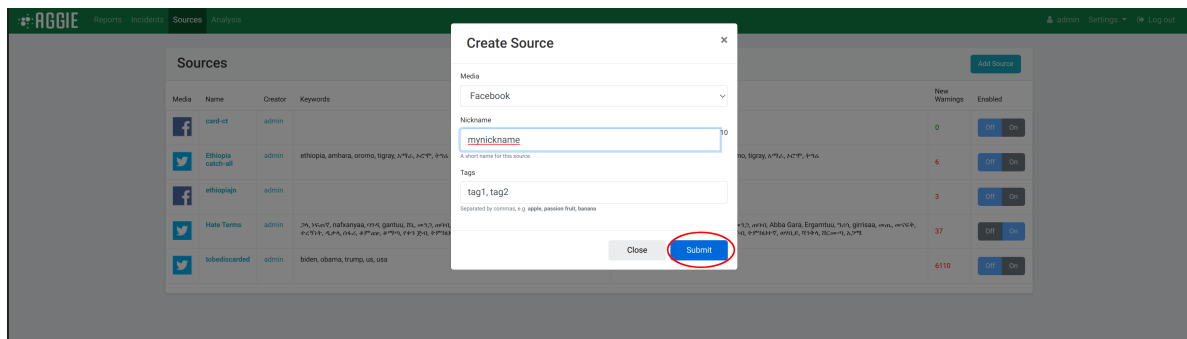


2. Click on the blue **Create Source** button on the left.
3. Choose the *Source Media*.



Sources

4. Enter a *Name* for the source.
5. Copy and Paste the *URL* of the source page and click **Submit**.



Sources

5.1.3 Warnings

As the application pulls in data, the app may encounter warnings. These warnings help determine whether or not a feed is pulling in data correctly.

1. Go to Sources.
2. In the Name column, click the appropriate source.
3. Under Recent Events, you can see recent warnings for the source.

5.2 Reports Page Activities

5.2.1 What is a Report?

A report is any post collected from a *source*. Examples include *tweets*, *Facebook posts* and *blog posts*.

5.2.2 The Reports Page

From your Aggie header bar, click the **Reports** Tab. This will show you the reports page as indicated below.

5.2.3 Actions on the Reports Page

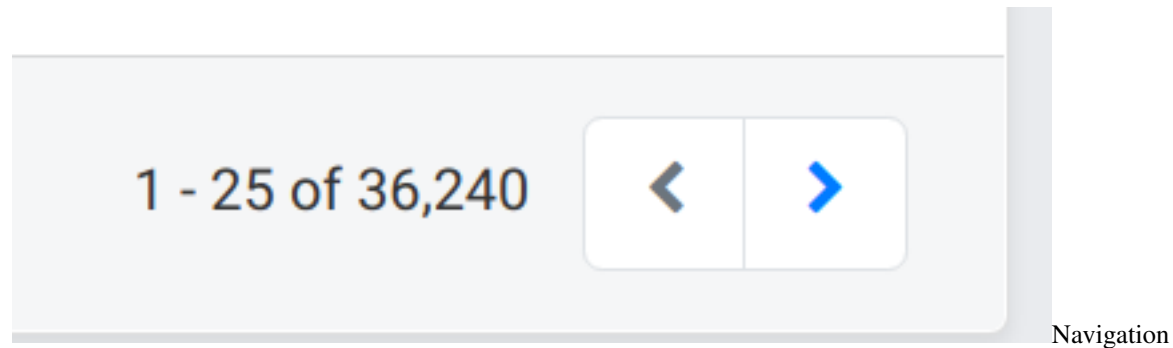
There are several actions you can take on the reports page of Aggie. You can *Read reports*, *Create Groups*, *Filter reports* or add a report to an *Group*. Besides the *filter bar* and the *action* and *navigation buttons*, there are eight columns on the Reports Page of Aggie.

5.2.4 Sections of the Reports Page

- **The Checkbox column:** This is used to select one or more reports that some actions can be applied to.
- **The Time column:** This indicates the time the report was published on the source feed that Aggie collected the report from.
- **The Media column:** This indicates the platform where the report was published.
- **The Source column:** This column indicates the name of the source, as set in the Sources tab. In the case of Twitter, they all originate from Twitter search but, for example, each Facebook group or page is a separate source. Advisably, the source name should be set the same name as the social media account name.
- **The Author column:** This indicates the social media account of the person who authored the report.
- **The Content column:** This column shows the exact content of the report published by the author.
- **The Group column:** This column is used to add a report to an existing group or create a new group.

5.2.5 Navigating within the Reports page.

In order to navigate to and from pages, the blue navigation arrows below the filter bar are used.



5.2.6 Reading Reports

There are two ways to read reports in Aggie. One way is to grab a batch using the “*Grab Batch*” button. The other is to go through reports on the reports page, navigating from one page to another using the *navigation buttons* on the reports page. Grabbing a batch is a faster and a more efficient way of reading reports in Aggie.

Reading using the “Grab Batch” button

The “*Grab Batch*” automatically pulls a set of ten unread reports that are displayed in batch mode. The batch mode is noted by the indication of a *blue bar* on the reports page. Users can take certain actions on these ten reports – like “*adding reports to groups*”. Upon completely taking desired action on the collected reports, trackers can grab another batch by clicking the “**Mark All Read & Grab Another**” button.

Batch Mode

The reports below have been assigned to you for review. When you are finished, click one of the buttons to the right.

Below are unread reports matching your filter.

☐ Read/Unread ☐ Add to Incident

Source Info	Thumbnail	Content	Tags	Incident
13 min ago TegadeTea Hate Terms Link ↗		ግድር የነበረ ሕይወት በጥቅም አልተጠየቀምም	ታላ ዓመት, nakanyaa, ጥፋ, gantuu, ሽኔ, ሙንጊ, ጣሳ, Abba Gara, Ergamtuu, ኃላ, ghirisaa, ሙጝ, ማቆራ, ተናገሩ, ፊዳላ, ቡሩ, ጸያሎ, ፉማሲ, የቀን ድብ, ሶጥነአቱት, ማህሊይ, ስንቅላ, ዘርውጣ, ኢሞ, NO_RT, Edit Tags	Add
15 min ago girma1234 Hate Terms Link ↗		@RasBittedweYY NGO በጥንቁቅ የቀደምት ስልጣን ስለሚሰጥ ለሕዝብ እንዲሰጥ ይጠይቃል	ታላ ዓመት, nakanyaa, ጥፋ, gantuu, ሽኔ, ሙንጊ, ጣሳ, Abba Gara, Ergamtuu, ኃላ, ghirisaa, ሙጝ, ማቆራ, ተናገሩ, ፊዳላ, ቡሩ, ጸያሎ, ፉማሲ, የቀን ድብ, ሶጥነአቱት, ማህሊይ, ስንቅላ, ዘርውጣ, ኢሞ, NO_RT, Edit Tags	Add
15 min ago IskinderBerhane Hate Terms Link ↗		RT @ErytheanSea: @ervstours at TeferiM08186473 @NeaminZekele @Martha_Eyob @GTWTW_Now @Abe_tokichaw @Lion_King_ET @AsqalTT @LeinadTarsa @mam...	ታላ ዓመት, nakanyaa, ጥፋ, gantuu, ሽኔ, ሙንጊ, ጣሳ, Abba Gara, Ergamtuu, ኃላ, ghirisaa, ሙጝ, ማቆራ, ተናገሩ, ፊዳላ, ቡሩ, ጸያሎ, ፉማሲ, የቀን ድብ, ሶጥነአቱት, ማህሊይ, ስንቅላ, ዘርውጣ, ኢሞ, RT, Edit Tags	Add
15 min ago Bthegemini2 Hate Terms Link ↗		RT @Fao75198199: 80% ኢሮፊል ሕዝቦች በክፍለ-ገጥሞች ለሰላም ስለተጓዙ ለሰላም ስለተጓዙ ለሰላም ስለተጓዙ... ለሰላም ስለተጓዙ ለሰላም ስለተጓዙ...	ታላ ዓመት, nakanyaa, ጥፋ, gantuu, ሽኔ, ሙንጊ, ጣሳ, Abba Gara, Ergamtuu, ኃላ, ghirisaa, ሙጝ, ማቆራ, ተናገሩ, ፊዳላ, ቡሩ, ጸያሎ, ፉማሲ, የቀን ድብ, ሶጥነአቱት, ማህሊይ, ስንቅላ, ዘርውጣ, ኢሞ, RT, Edit Tags	Add
15 min ago EthiopianFair Hate Terms Link ↗		RT @teider_ba: #AbiyisResponsiblefor the genocide Amharas are facing in Fwellega #metekel and #MaKadra. Now is the time to break our sil...	ታላ ዓመት, nakanyaa, ጥፋ, gantuu, ሽኔ, ሙንጊ, ጣሳ, Abba Gara, Ergamtuu, ኃላ, ghirisaa, ሙጝ, ማቆራ, ተናገሩ, ፊዳላ, ቡሩ, ጸያሎ, ፉማሲ, የቀን ድብ, ሶጥነአቱት, ማህሊይ, ስንቅላ, ዘርውጣ, ኢሞ, RT, Edit Tags	Add
15 min ago EthiopianFair Hate Terms Link ↗		RT @Amhara_Nation: #AmharaGenocide #StopAmharaGenocide #AmharaMassacre #WollegaMassacre #MetekelMassacre #Oromoterrorism #OromoExtremists	ታላ ዓመት, nakanyaa, ጥፋ, gantuu, ሽኔ, ሙንጊ, ጣሳ, Abba Gara, Ergamtuu, ኃላ, ghirisaa, ሙጝ, ማቆራ, ተናገሩ, ፊዳላ, ቡሩ, ጸያሎ, ፉማሲ, የቀን ድብ, ሶጥነአቱት, ማህሊይ, ስንቅላ, ዘርውጣ, ኢሞ, RT, Edit Tags	Add

Mark All Read & Grab Another
Mark All Read & Done
Cancel

Total Reports

36,232

Reports/Last min

0

Unread

36,229

Incidents

2

Escalated Incidents

1

Batch

Marking Reports as Read

A report can be manually marked as read. More than one reports can be marked as read by checking their respective checkboxes or with the “*Mark all Read*” button. When a tracker grabs a new batch, it is recommended that the tracker

selects either “*Mark All Read & Grab Another*” or “*Mark All Read & Done*”. If the batch was accidentally grabbed, the tracker should click the “*Cancel*” button.

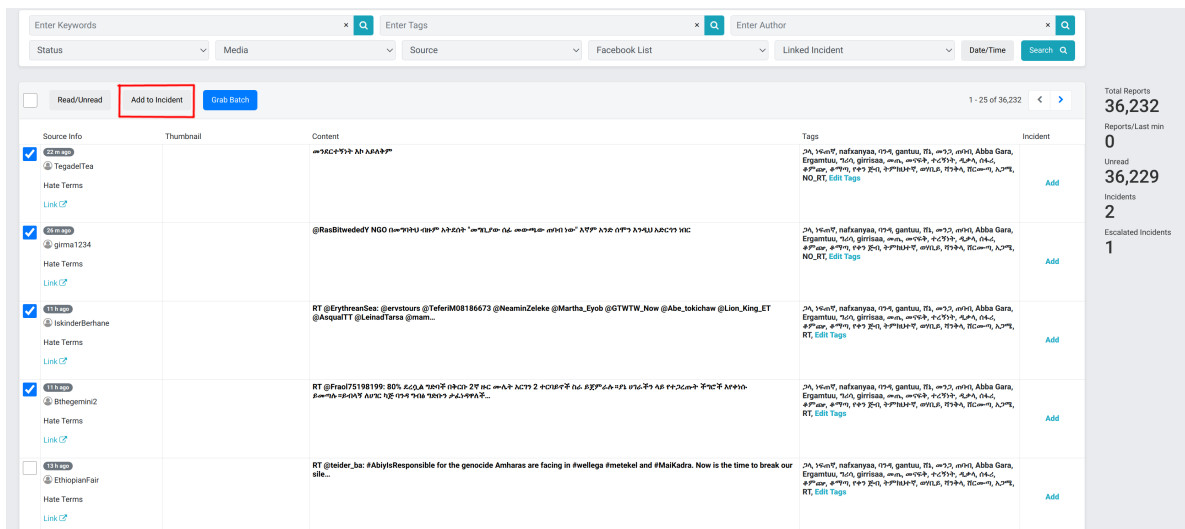
5.2.7 Creating Groups

Adding a report to an existing Group

When trackers come across reports that, if verified, require action, they create a group from that report. Or, if the report is associated with an already existing group, the tracker may add the report to the existing group.

Creating a New Group

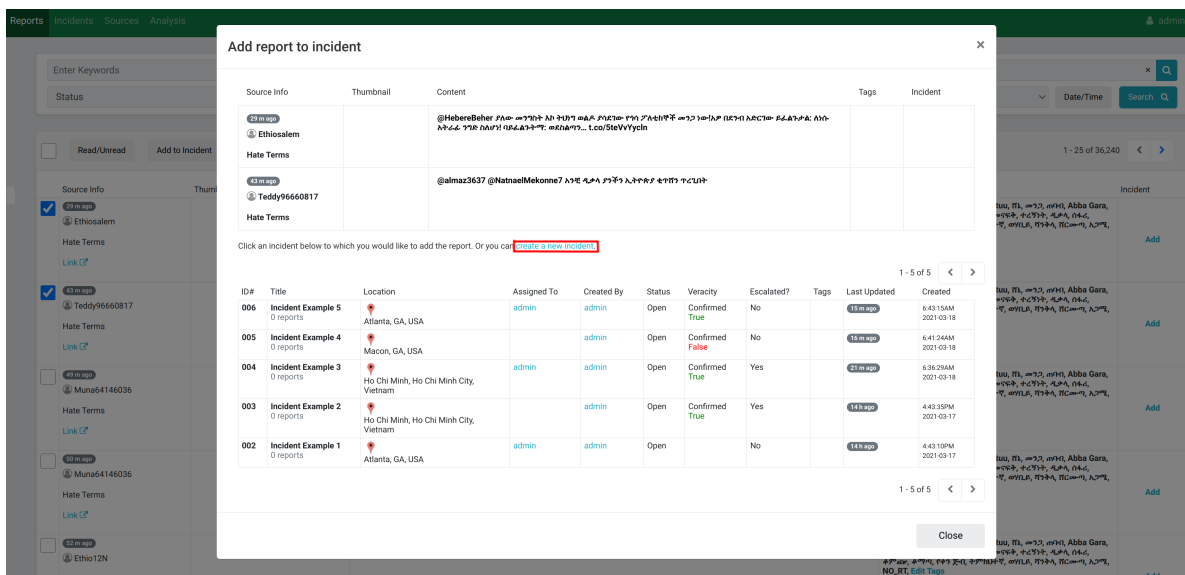
1. Select the report(s) you are creating the *Group* for by checking its/their *checkbox(es)* on the first column to the left of the reports page.



The screenshot shows the 'Reports' page in the Aggie interface. At the top, there are search bars for 'Enter Keywords', 'Enter Tags', and 'Enter Author'. Below these are filters for 'Status', 'Media', 'Source', 'Facebook List', 'Linked Incident', and 'Date/Time'. A table of reports is displayed with columns for 'Source Info', 'Thumbnail', 'Content', 'Tags', and 'Incident'. The first column has checkboxes for selecting reports. The 'Add to Incident' button is highlighted in red. On the right side, there is a summary of reports: Total Reports: 36,232, Reports/Last min: 0, Unread: 36,229, Incidents: 2, and Escalated Incidents: 1.

Groups

2. Click the **Add to Group** button beneath the filter bar.



The screenshot shows the 'Reports' page with the 'Add report to incident' dialog box open. The dialog box has a title bar 'Add report to incident' and a close button. It contains a table with columns for 'Source Info', 'Thumbnail', 'Content', 'Tags', and 'Incident'. The 'Add to Group' button is highlighted in red. Below the table, there is a section for 'Click an incident below to which you would like to add the report. Or you can create a new incident'. This section contains a table with columns for 'ID#', 'Title', 'Location', 'Assigned To', 'Created By', 'Status', 'Veracity', 'Escalated?', 'Tags', 'Last Updated', and 'Created'. The table lists several incidents, including 'Incident Example 5', 'Incident Example 4', 'Incident Example 3', 'Incident Example 2', and 'Incident Example 1'.

Groups

3. Select the related category of an *existing group* to add the report to that group or... **If it's a new Group;**
4. Click on the *blue* **Create a new Group** link to create the new group.

Create Incident

Title*

Veracity

Unconfirmed

Status

Open

Escalated

Location

Enter a location

Tags

[Edit coordinates...](#)

Assign To

Select User

Notes

Public

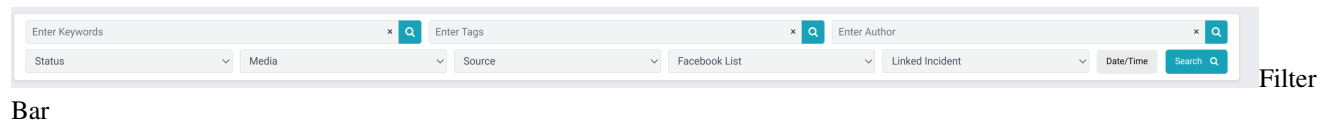
Group

5. Type in the *Title* of the group (e.g. *Polling station not open, Voter intimidation etc*), the *Location* of the group and a brief *note* describing the group. Leave out the *veracity* and *assignment* fields for the veracity team and click **submit** to create a new group. The verification and escalation team will be using the *note* field to keep track of the verification and escalation steps taken.
6. The *Public* and *Public Description* fields are used by the escalation team to add the group to the list of public groups. The *Public Description* will appear attached to the group, for example, in the *Public Group Map*.

5.2.8 Filtering Reports

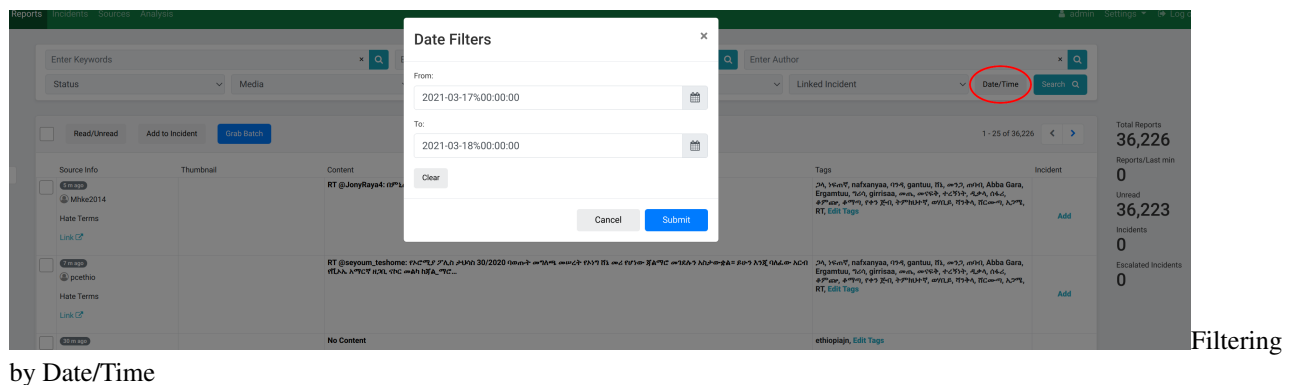
The Filter Bar

With the *filter bar*, trackers can narrow down their search for specific types of reports. The screenshot below shows the filter bar and a number of filters that can be used.



Filtering by Date/Time

1. Click on **Date/Time** button on the right end of the filter bar.
2. Select a Date/Time range by specifying the *From* and *To* fields.
3. Click **Submit** to filter and display reports aggregated within that date and time range.



Filtering by Group

1. Click on the **Linked Group** tab and select a group to view all related reports tagged to that group.
2. In this example, selecting the group *Hate Speech* shows the three reports which have been linked to that group.



Filtering by Source

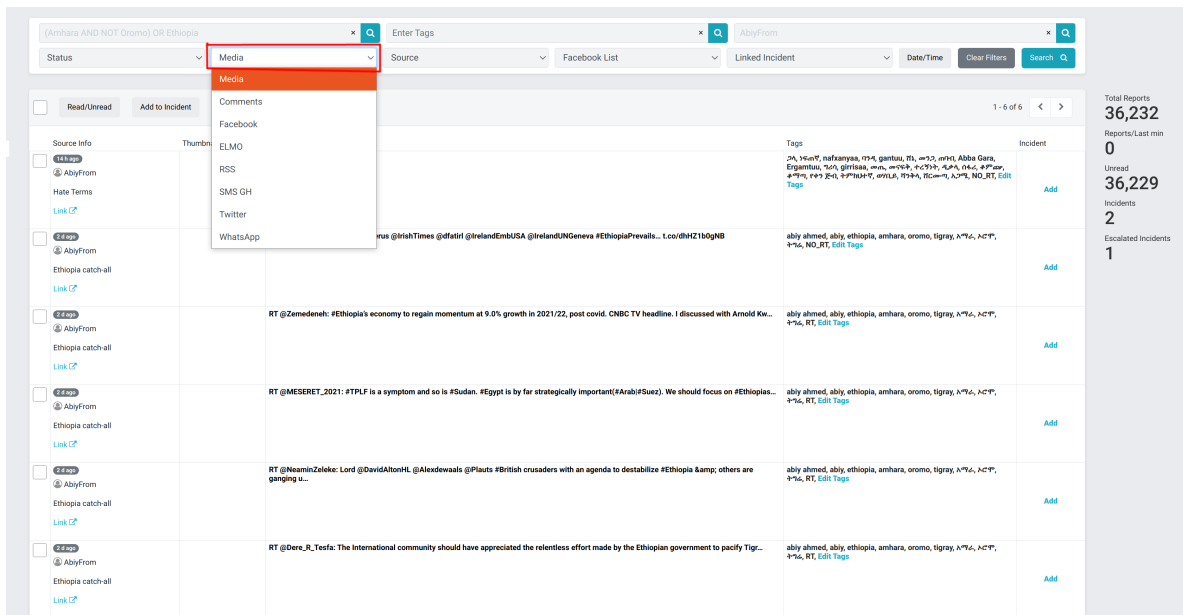
1. Click the **Source** menu from the header bar.
2. Select the *Source type* (e.g. *Twitter Search*) to filter and display only reports from that source.



Filtering by Source

Filtering by Media Type

1. From the header bar, click the **Media** menu.
2. Select the *Media type* (e.g. *Twitter*, *RSS*) to filter and display reports from sources of that media type.



Filtering

by Media

Filtering by Status

1. From the Header Bar, click the **Status** menu.
2. Select the report *Status* (e.g. *Unread*, *Read*) to display the reports of that status.

Filtering

by Status

Filtering by Author

1. Type in all or part of the name of an *Author*, e.g. *the user name of a Facebook account or a Twitter handle*, in the **Enter author** space on the filter bar.
2. Click **Go** to show only reports by authors with matching names. For example, entering the author *JoyNews*, and clicking **Go** displays all the reports published by JoyNews.

Filtering

by Author

Filtering by Keywords

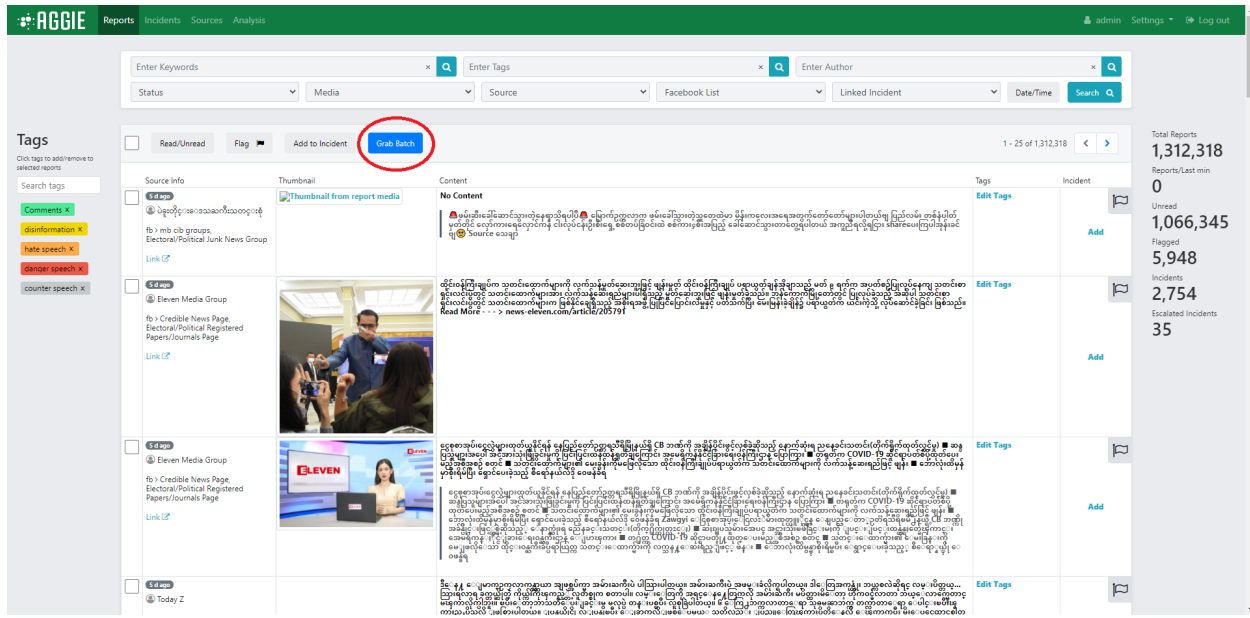
1. Type in a *query keyword*, term or set of terms separated by commas, quotations or operators in the **Enter keywords** space on the Filter bar.
2. Click **Go** or the return key to display all reports that include the keyword or set of terms. For example, by searching the keywords, *Ghana*, *ECG* and *Free n Fair Election*, there is a display of all reports containing one or more of the keywords.

Filtering

5.3.1 What does Batch Mode do?

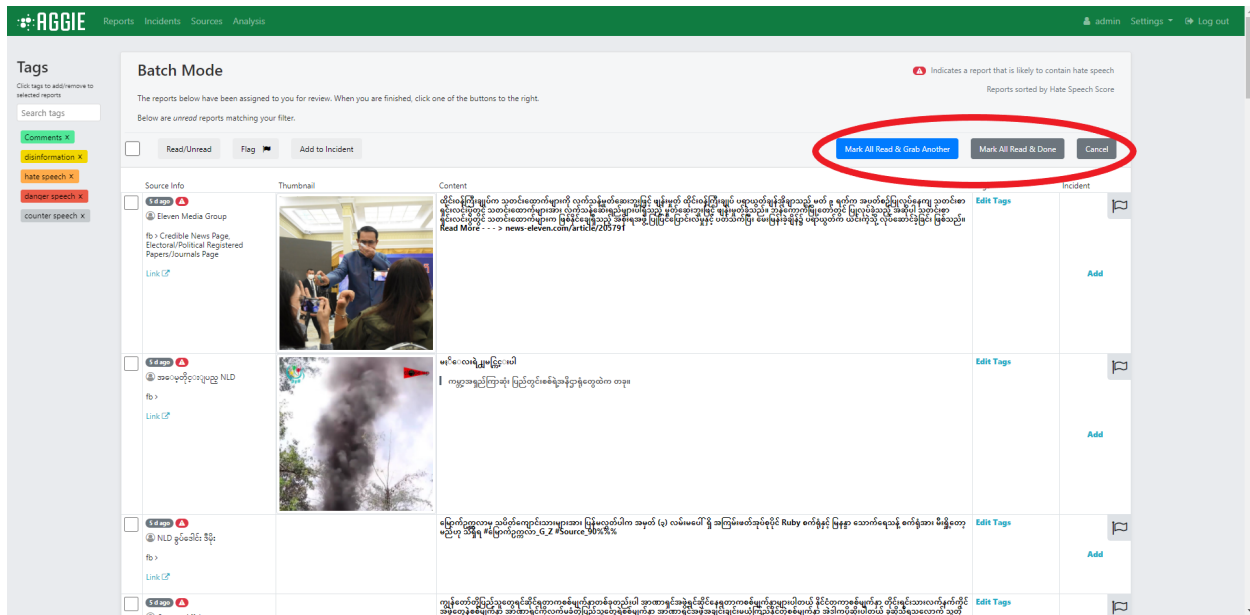
This marks those reports as that user's and prevents any other user from seeing those reports on their respective batch modes. This means that a report in one user's batch mode cannot show up in another user's batch mode. In addition, Batch Mode has NLP functionality and displays reports that are highly scored near the top of the screen and adds a warning icon to reports that meet a certain threshold.

On the Reports screen, click the Grab Batch button. This button is in blue.



Page

From the Batch Page, go through reports and triage those that are relevant.



Batch

Page Once you are completed with a batch of reports, click either “Mark All Read & Grab Another” to mark all the reports in that batch read and grab another batch, or “Mark All Read & Done” which marks all the reports in the batch read then returns to the report screen. “Cancel” will simply return to the reports screen.

NLP Indication and Ordering

According to the NLP classifier linked with Aggie, Batch mode will order reports based on the likelihood a report is hate speech. This will appear in two ways: the higher scoring (more likely hate speech) reports will appear on the top of the page and reports that meet a threshold will show a warning indication in the Source Info column of the report. You can see the icon attached to several reports below. These orderings and icons will not appear in the reports page, only the batch mode.

Batch Mode

Indicates a report that is likely to contain hate speech

Reports sorted by Hate Speech Score

The reports below have been assigned to you for review. When you are finished, click one of the buttons to the right.

Below are unread reports matching your filter.

Read/Unread

Flag

Add to Incident

Mark All Read & Grab Another

Mark All Read & Done

Cancel

Source Info	Thumbnail	Content	Tags	Incident
<div><div><div>5 d ago</div><div>Eleven Media Group</div><div>fb > Credible News Page, Electoral/Political Registered Papers/Journals Page</div><div>Link</div></div></div>		<div><div>တိုင်းရင်းသားများကို လက်သံနှိုးဆော်ခြင်း ဖြစ်ပွားခဲ့ပြီး ပစ္စည်းများကို ဖျက်ဆီးခဲ့သည်။ မတ် ၉ ရက်က အပတ်စဉ်ပြုလုပ်သော သတင်းစာ ရုပ်ရှင်တွင် သတင်းစာများအား လက်သံနှိုးဆော်ခြင်း ဖြစ်ပွားခဲ့သည်။ မတ် ၉ ရက်က အပတ်စဉ်ပြုလုပ်သော သတင်းစာ ရုပ်ရှင်တွင် သတင်းစာများအား လက်သံနှိုးဆော်ခြင်း ဖြစ်ပွားခဲ့သည်။ မတ် ၉ ရက်က အပတ်စဉ်ပြုလုပ်သော သတင်းစာ ရုပ်ရှင်တွင် သတင်းစာများအား လက်သံနှိုးဆော်ခြင်း ဖြစ်ပွားခဲ့သည်။</div><div>Read More - - - > news-eleven.com/article/205791</div></div>	<div><div>Edit Tags</div></div>	<div><div>Add</div></div>
<div><div><div>5 d ago</div><div>NLD</div><div>သတင်းစာများ</div><div>Link</div></div></div>		<div><div>မင်းလေးရဲ့အမည်</div><div>ကမ္ဘာ့အရှင်ကြီး၏ ပြည်တွင်းစစ်ချီနာနဲ့တွေ့မိက တခု။</div></div>	<div><div>Edit Tags</div></div>	<div><div>Add</div></div>
<div><div><div>5 d ago</div><div>NLD</div><div>သတင်းစာများ</div><div>Link</div></div></div>		<div><div>ပြောကြားလာမယ့် သတင်းစာများအား ပြန်လည်ပါက အမှတ် (၃) လမ်းမပေါ်၌ အကြမ်းမတ်အုပ်စုနှင့် Ruby ဇော်နှင့် ပြန်ဆွဲ ဆောင်းရသည့် ဇော်နဲ့အား စီမံခန့်ခွဲမှု မဟုတ် သိရှိရ #ပြောကြားသူ G_Z #Source 90%။</div></div>	<div><div>Edit Tags</div></div>	<div><div>Add</div></div>

Batch

Page Hate Speech Indication

5.4 Tags

A tag is a method of categorizing reports at an individual level. Whereas groups allow for clusters of reports based whether reports require action, tags allow for categorization of reports based on a report’s qualities. In order to create a tag, you must have permission to do so.

5.4.1 Creating Tags

- 1. Navigate to the Tags page of the Aggie platform in order to create/edit/delete tags.

AGGIE

Reports Incidents Sources Analysis

Settings

Log out

Tags

Create Tag

Tag Name	Color	Created By	Description	Edit or Delete
Hate Speech		Incubator	Hate speech of any kind.	<div><div></div><div></div></div>
Shopping		Incubator	Any spam posts about shopping.	<div><div></div><div></div></div>
Politician		Incubator	Politician is responsible for post.	<div><div></div><div></div></div>
Activist Group		Incubator	Posted by an activist group.	<div><div></div><div></div></div>
Pro-Buddhist		Incubator	Post is pro-buddhist.	<div><div></div><div></div></div>
Pro-Muslim		Incubator	Any pro-muslim report.	<div><div></div><div></div></div>

Total Reports: 2,285

Unread: 0

Flagged: 13

Incidents: 1

Escalated Incidents: 1

Configuration

Users

Tags

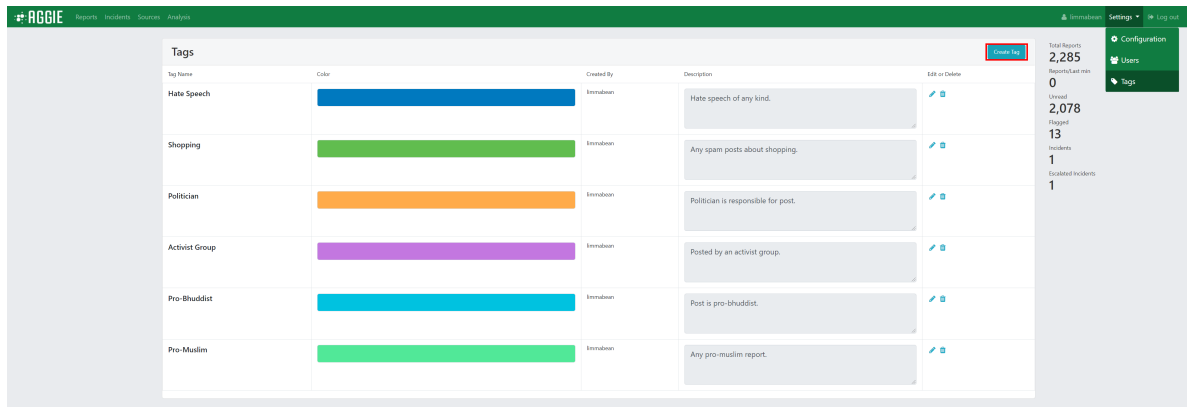
Page

Tags

- 2. Click the **Create Tag** button in the heard of the Tags card.

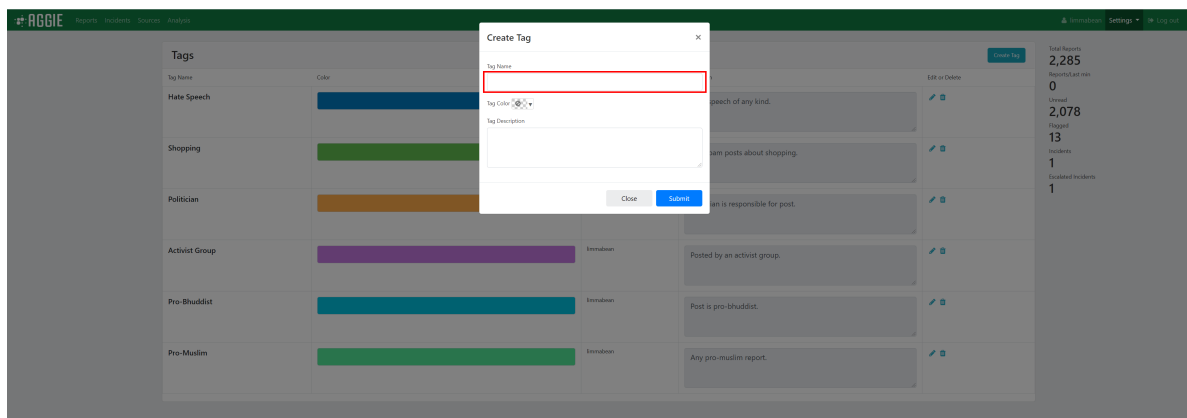
5.4. Tags

33



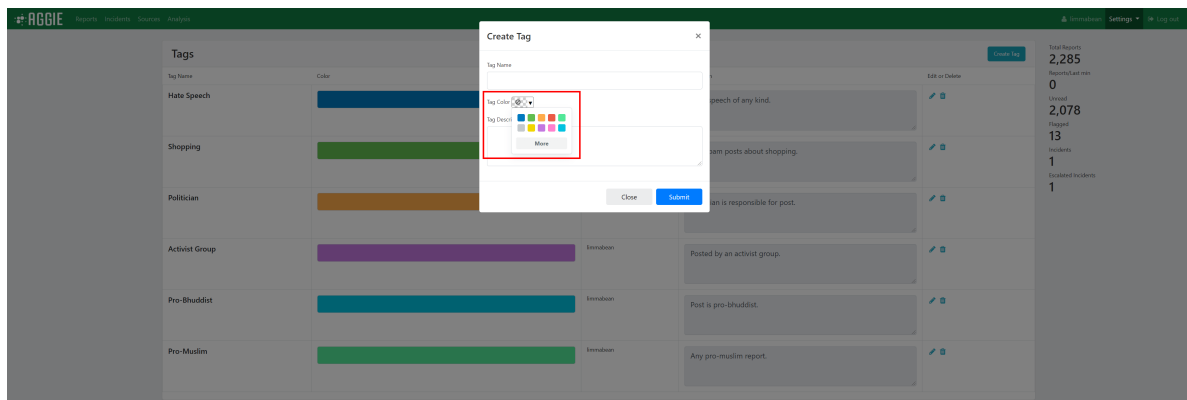
Tags_Create_Butt

3. Fill out tag name (this is what is shown as the tag). Tag names can be edited after creation and will be updated on any reports it was applied to. Tags can only be 15 characters long.



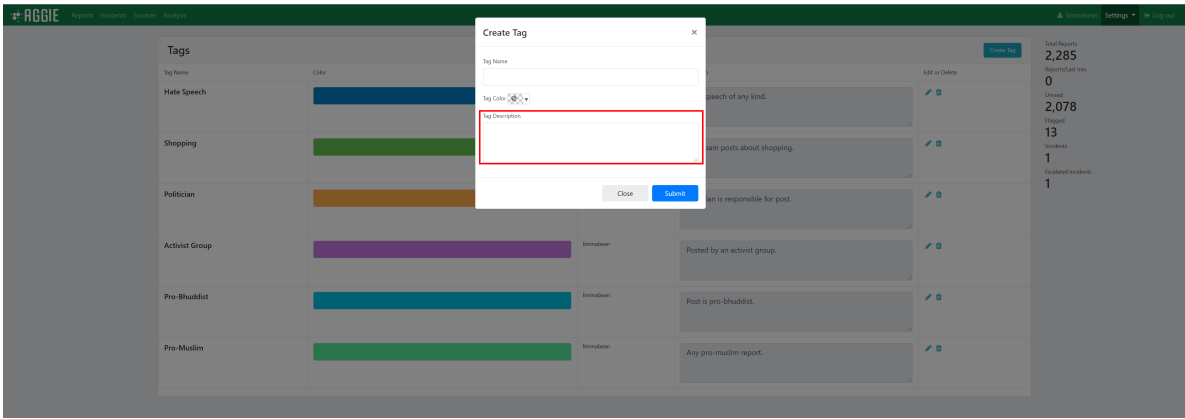
Tags_Form_Name

4. Fill out tag color (this is what is shown as the tag's background color). Tag colors can be picked using the present color values or custom hex values. Tag color can be edited after creation and will be updated on any reports it was applied to.



Tags_Form_Color

5. Fill out optional tag description (this is not shown but helps trackers understand what a tag is used for). Tag description can also be edited after creation.



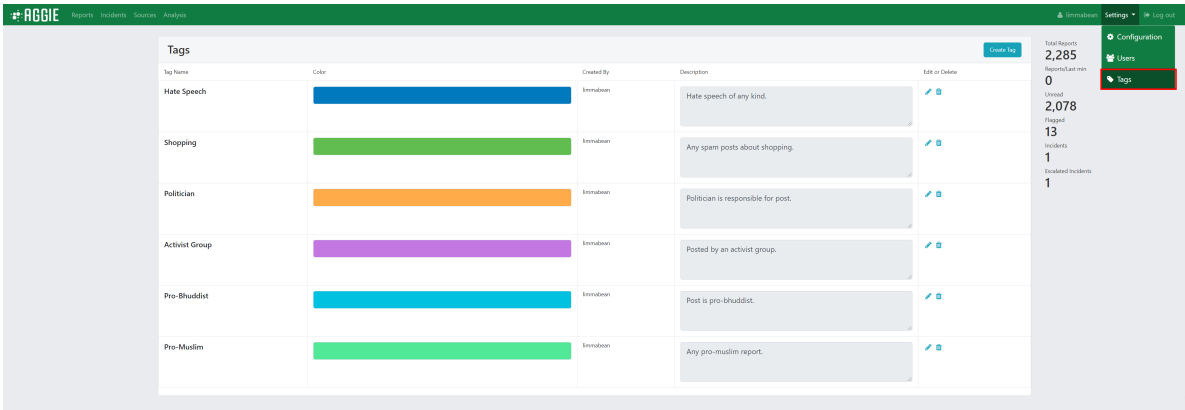
Tags_Form_Descr

6. Click the **Submit** to finish creating your tag.

5.4.2 Deleting Tags

Removing tags will cause them to be removed from the reports they are added to. *Do not remove tags that are still in use.* If a tag change must be made, edit the tag.

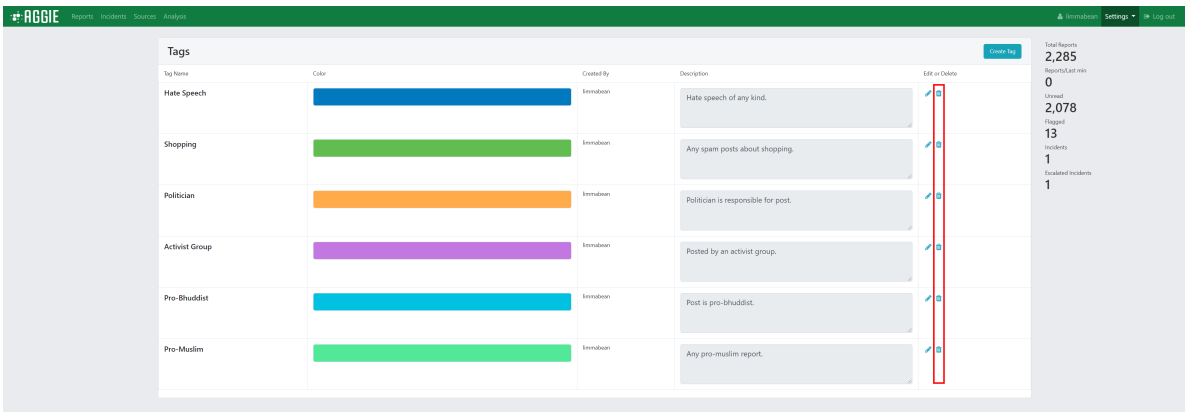
1. Navigate to the Tags page of the Aggie platform in order to delete tags.



Tags

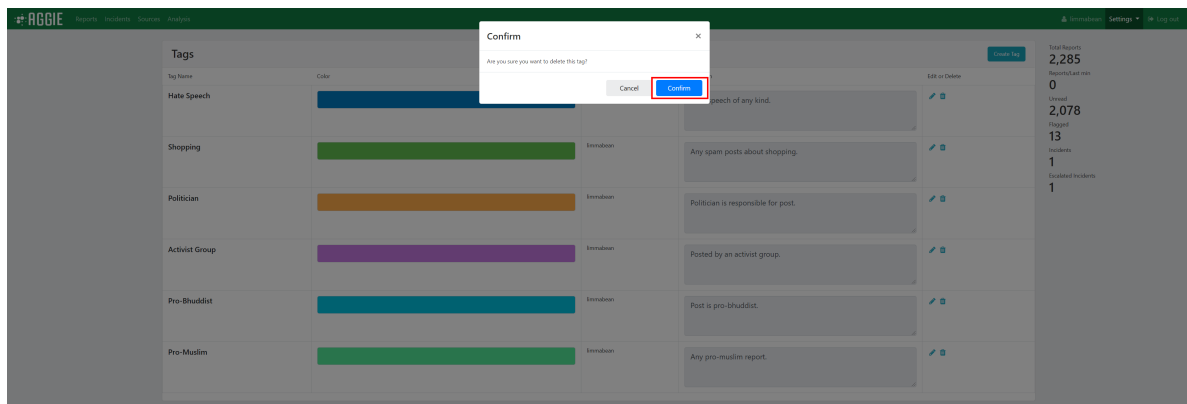
Page

2. Click the **Trash Icon** located within the same row of the tag you would like to delete.



Tags_Delete_Butt

3. You will receive a confirmation modal after you click the **Trash Icon**. Press the **Confirm** button to continue with deletion.

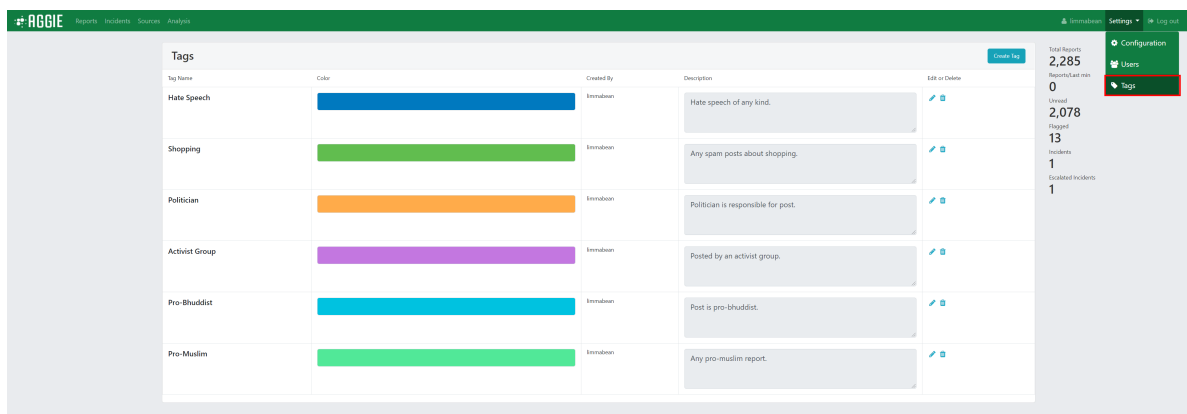


Tags_Delete_Con

5.4.3 Editing Tags

Editing tags will cause an existing tag and all the Reports that contain that tag to update said existing tag. *This does not remove the tag from any reports.*

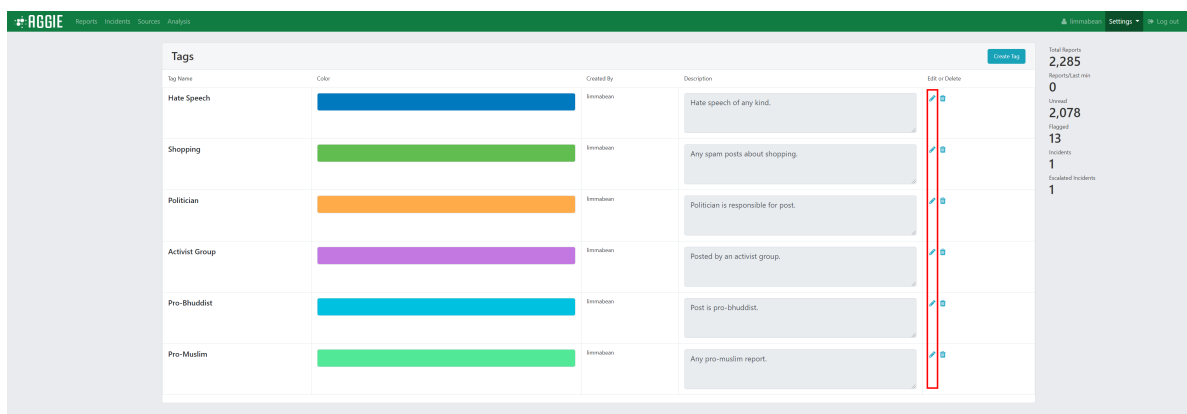
1. Navigate to the Tags page of the Aggie platform in order to edit tags.



Tags

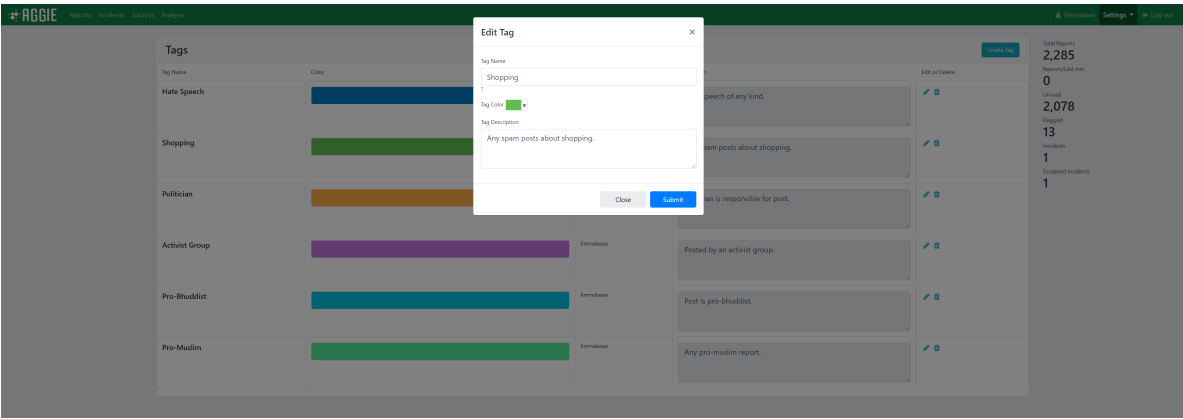
Page

2. Click the **Pencil Icon** located within the same row of the tag you would like to edit.



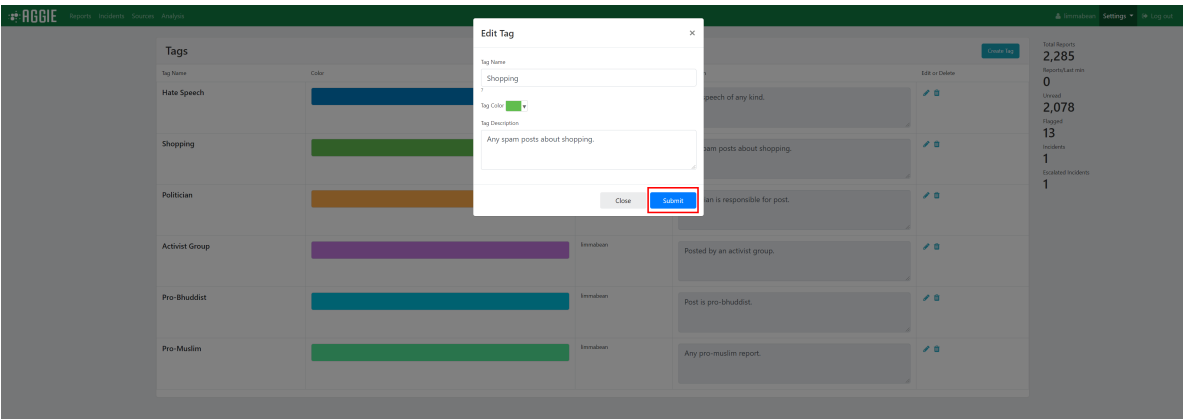
Tags_Edit_Button

3. The form that appears upon clicking should be populated with the tag's previous information.



Tags_Edit_Form

4. Fill the form with updated name/color/description. Then click submit to update the tag's properties.



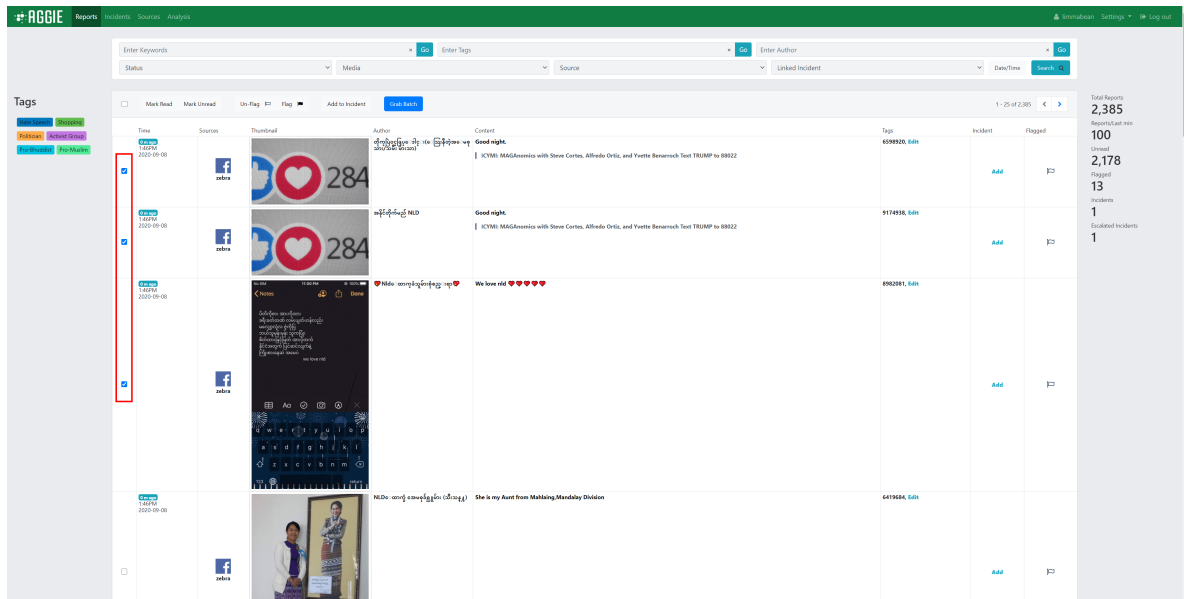
Tags_Edit_Submit

5.4.4 Adding/Removing Tags to Reports

There are two methods of adding/removing tags to reports. Tags may be added to every report selected. The second method is adding tags to individual reports.

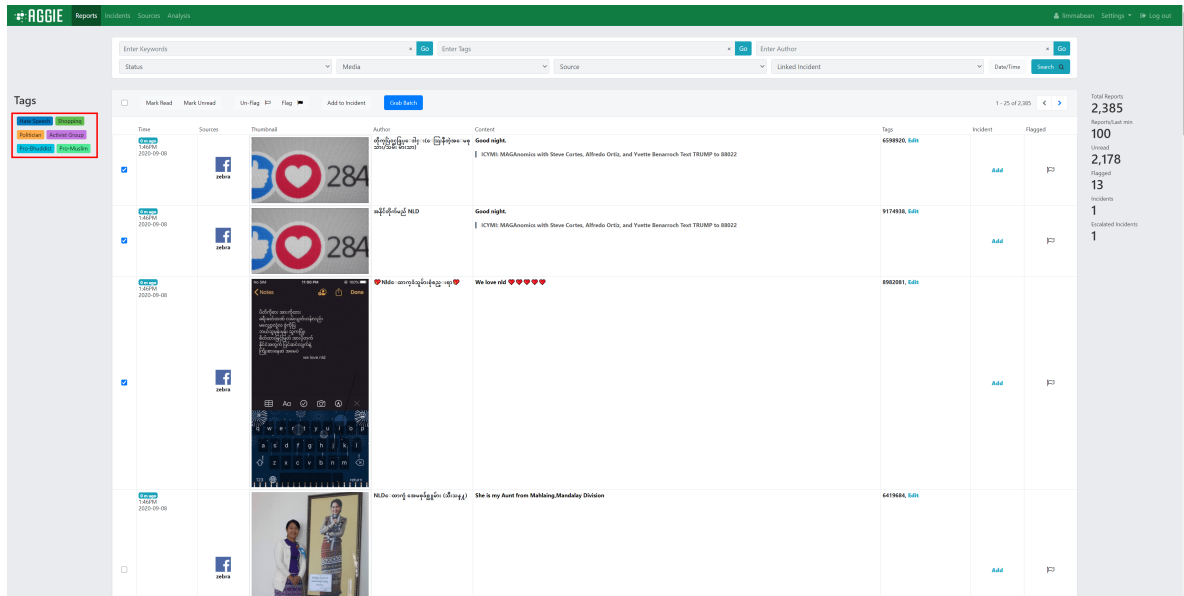
Method 1: Adding/Removing Tags to Many Reports

1. On the reports page (or the batch page), select the reports you would to add a tag to.



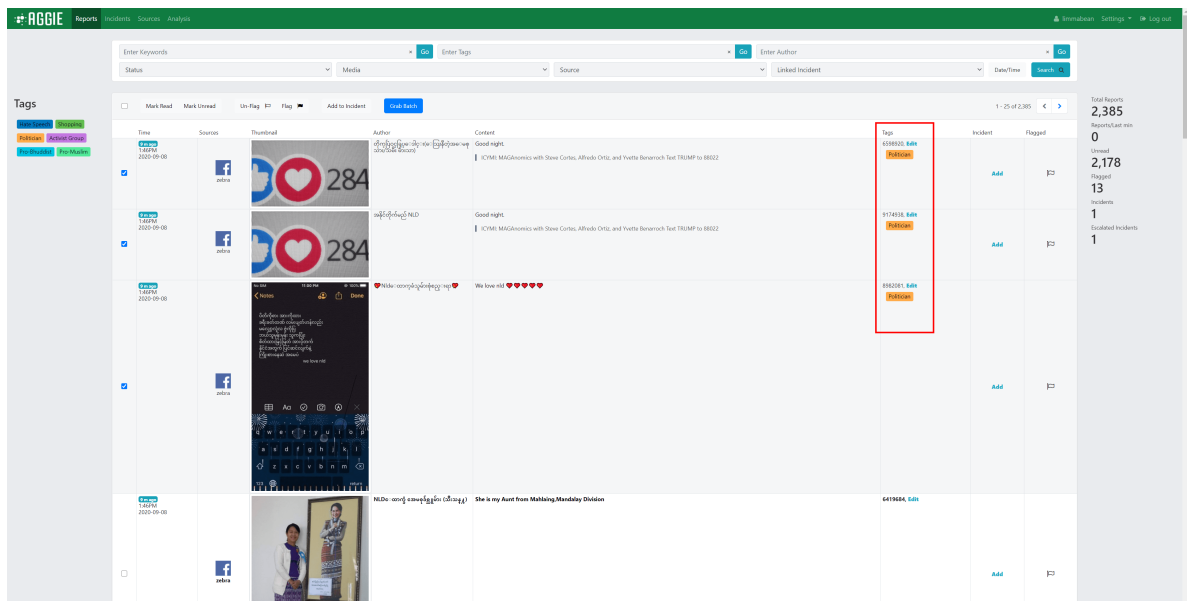
Tags_Report_Select

2. Then click the tag button on the left sidebar of the tag that you would like to add to each report. These tags operate as toggles. If all selected reports have that tag, it will remove that tag from each report selected. If none or only some of the reports have that tag, it will add that tag to each report selected.



Tags_Report_Toggle

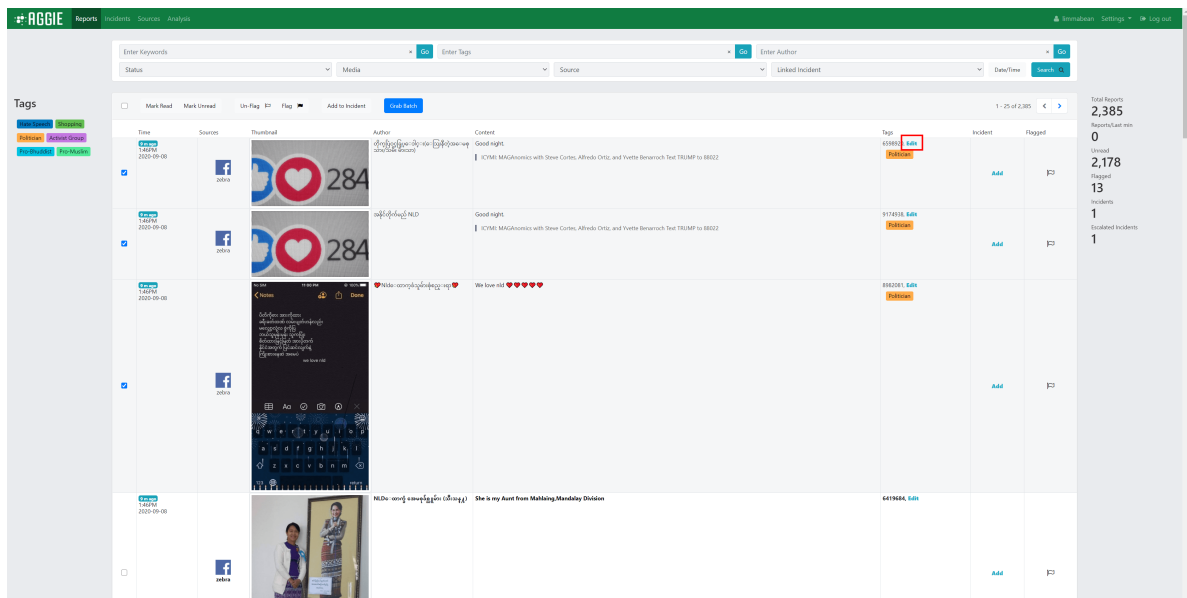
3. This should add the tag to each Report that was selected. Clicking that tag button again will remove the tag from the selected reports.



Tags_Reports_Res

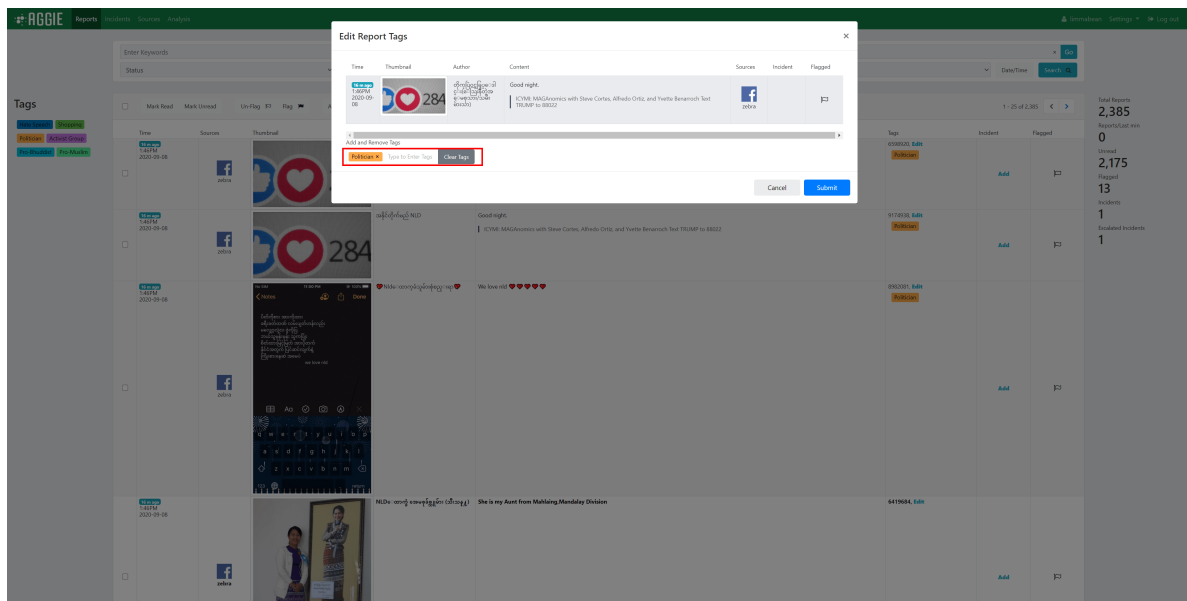
Method 2: Adding/Removing Tags to a Single Report

1. On the reports page (or the batch page), click the **Edit** text of the report row and tags column of the report you would like to edit. This functionality can also be accessed through the report details page.



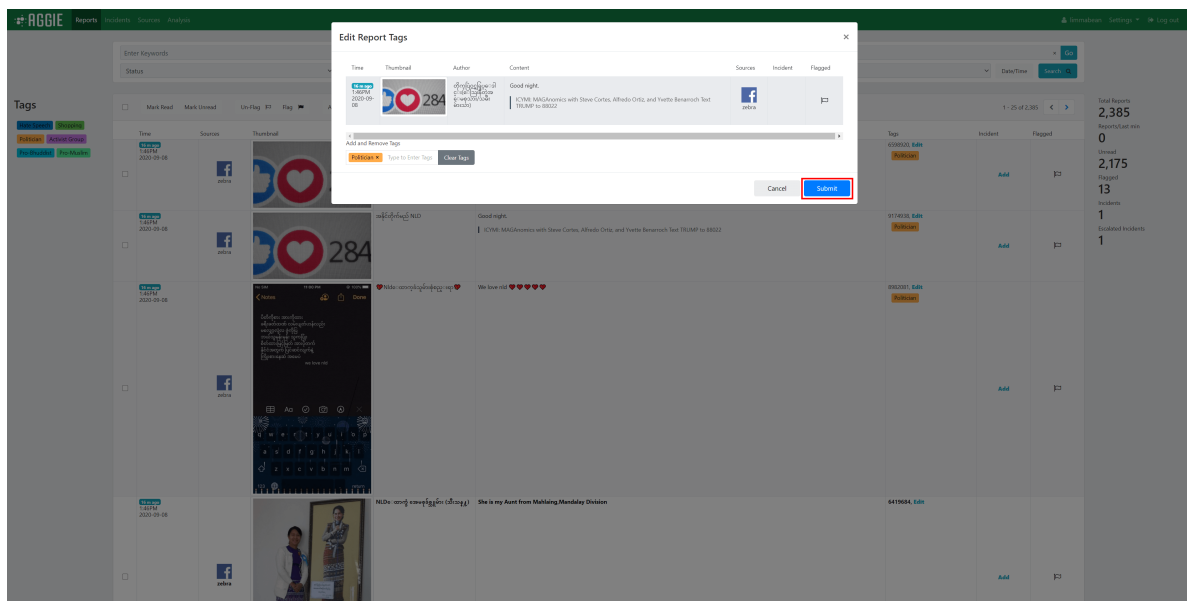
Tags_Report_Edit

2. The form that appears should have the selected report's information, and an input box to add and remove tags. Tags can be added by typing the full tag then pressing the **Enter** key, using autocomplete functionality, clicking tag dropdown options. Tags can be removed using the backspace key, clicking the **x** on each tag, or clearing all tags. None of these changes will take place until the **Submit** button has been pressed.



Tags_Report_Edit

3. Click the **Submit** Button to finalize changes to the report's tags.

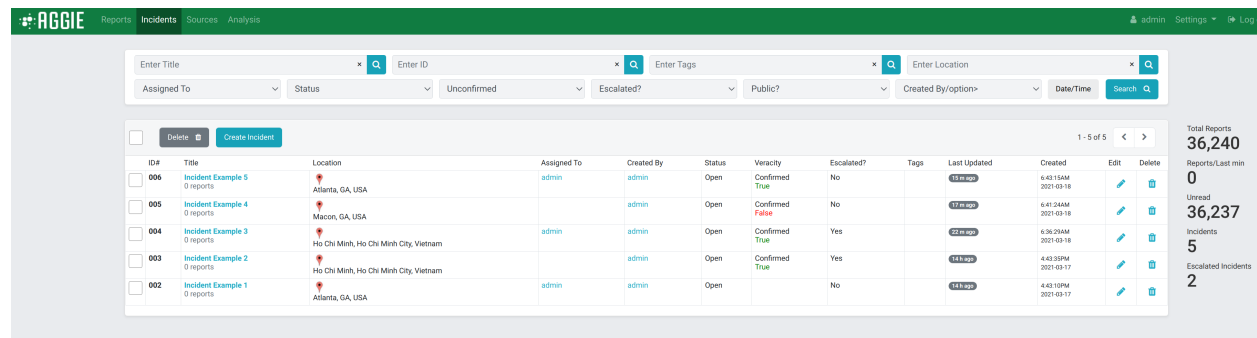


Tags_Report_Edit

5.4.5 Quick Removal of Tags on Single Report

1. On the reports page (or the batch page), click a tag on a report row to remove the tag from that report.

Tags_Report_QuickTags_Quick_Rem



ID#	Title	Location	Assigned To	Created By	Status	Veracity	Escalated?	Tags	Last Updated	Created	Edit	Delete
006	Incident Example 5 0 reports	Atlanta, GA, USA	admin	admin	Open	Confirmed True	No		15 min ago	6:43:15AM 2021-03-18		
005	Incident Example 4 0 reports	Macon, GA, USA		admin	Open	Confirmed False	No		17 min ago	6:41:24AM 2021-03-18		
004	Incident Example 3 0 reports	Ho Chi Minh, Ho Chi Minh City, Vietnam	admin	admin	Open	Confirmed True	Yes		22 min ago	6:36:29AM 2021-03-18		
003	Incident Example 2 0 reports	Ho Chi Minh, Ho Chi Minh City, Vietnam		admin	Open	Confirmed True	Yes		18 min ago	4:43:39PM 2021-03-17		
002	Incident Example 1 0 reports	Atlanta, GA, USA	admin	admin	Open		No		18 min ago	4:43:10PM 2021-03-17		

Total Reports
36,240

Reports/Last min
0

Unread
36,237

Incidents
5

Escalated Incidents
2

Groups

Main Page

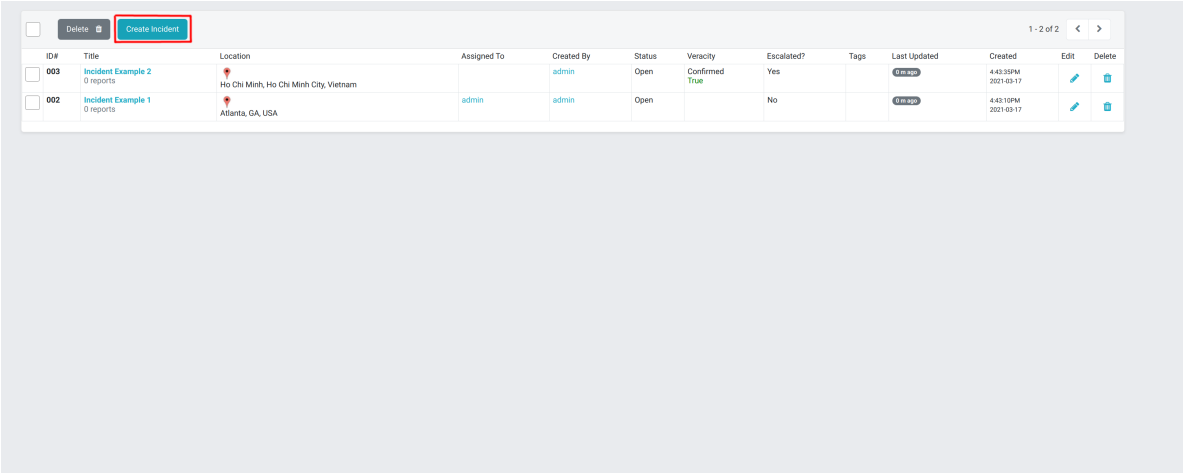
5.5.3 Sections of the Groups Page

- **The Checkbox column:** This is used to select one or more groups that some actions can be applied to.
- **The ID# column:** This column indicates the unique identification number generated for each group created. This example starts with 003 because group 001 and 002 have been deleted.
- **The Title column:** This column shows the name given to the group and the number of reports associated with the particular group.
- **The Location column:** This column shows the place where the group occurred.
- **The Assigned to column:** This column indicates the veracity team member who has been assigned to verify the group for confirmation (and then escalation) or closure.
- **The Status column:** This column shows whether the group has been escalated or confirmed false, and closed, or is still open and thus needs to be verified or escalated.
- **The Veracity column:** This shows the verification status of the group. Whether the investigations confirmed the group to be true or false.
- **The Escalated column:** This column show whether a confirmed group been reported to stakeholders and embeds for management and resolution.
- **The Last Updated column:** This column tracks and indicates the time of the last activity such as editing or updating on the group.
- **The Edit/Delete Column:** This column contains two tools for editing or deleting an group; to edit the group, click the blue **Pencil Icon** or to **delete** the group click the blue **small bin**.

5.5.4 Creating a Group

Normally, *groups* are created by Trackers. However, should the need arise, verifiers can create *groups* from the groups page. To do this, refer to [Creating a New Group](#) section.

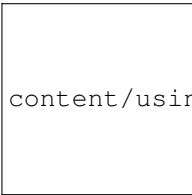
1. Click the **Groups** tab from the header bar.



Creating

Groups

- From the groups page, click the blue colored **Create Group** tab.



content/usingaggie/incident_creation.png

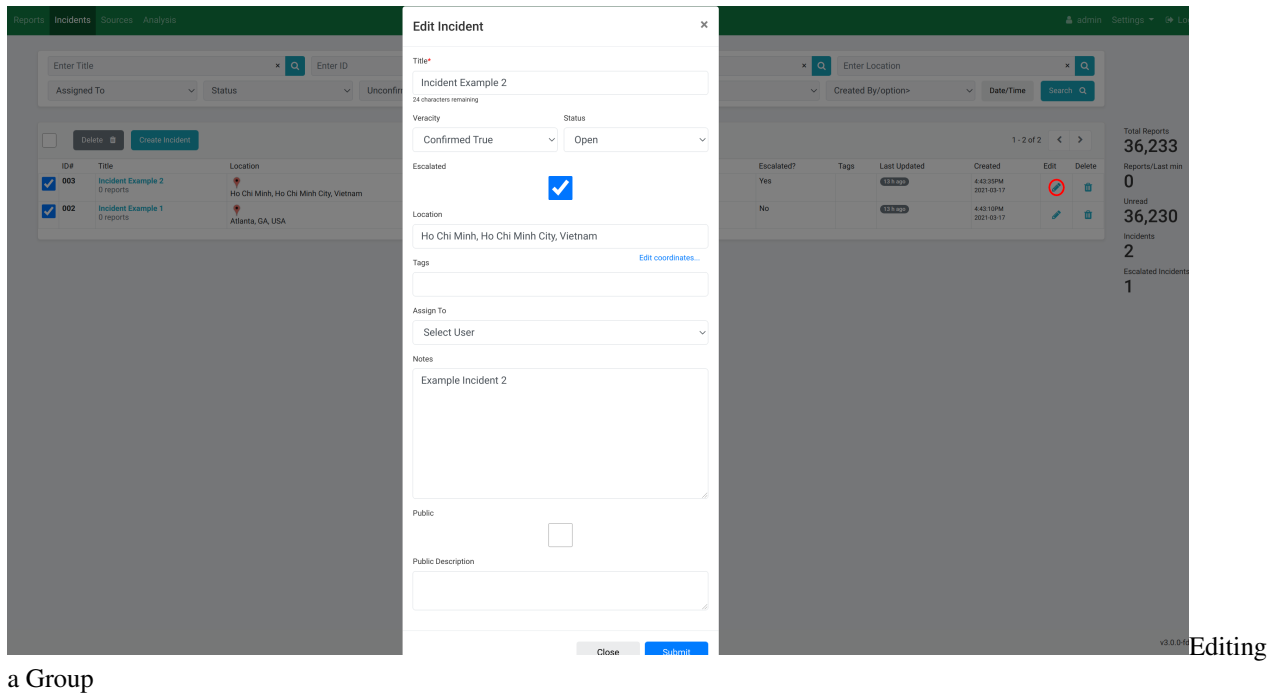
Creating a Group

- Type in the *Title* of the group (e.g. *Polling Station not open, Voter Intimidation etc*), the *Location* of the Group and a brief note describing the group. Set the veracity and status fields as applicable.

5.5.5 Editing a Group

Verifiers can always update the status of groups by editing them. It is recommended that you keep a log of the actions taken while confirming or denying veracity in the notes section of a Group. To do this:

- From the groups page, click the **blue edit pencil** at the end of the group row (last column).



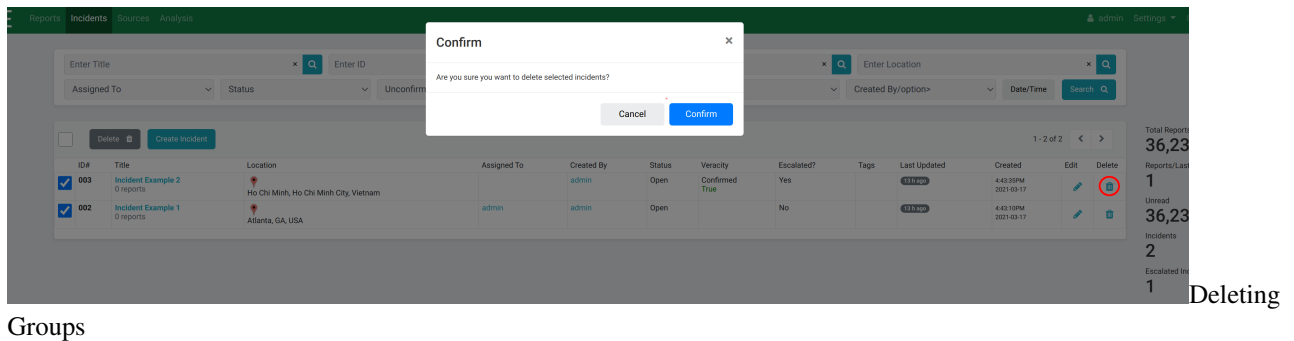
a Group

2. Update the group by editing appropriate sections. For example, you can edit the *veracity* and *status* of the group, add any helpful *notes* or *escalate* the group.

5.5.6 Deleting an Group

If a veracity team member notices a redundancy in groups, they may *delete* an group from the Groups page. To do this:

1. Select the *group(s)* you wish to delete by checking its/their respective *checkbox(es)*.
2. Click the **Delete** button below the filter bar to the left.



Groups

3. Click **Confirm** to delete the selected group(s).

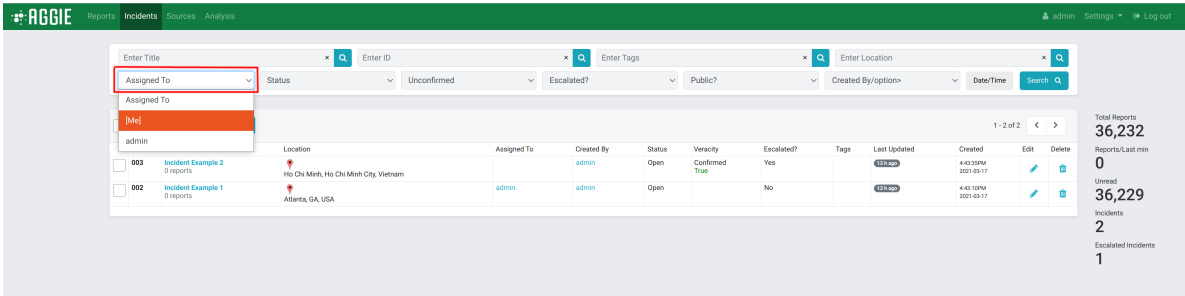
Alternatively, you can delete an group by clicking the little bin on the last column of the group row.

5.5.7 The Group Filter Bar

With *filters*, verifiers can narrow down their search. In some cases, there might arise the need to search for specific types of groups. Filters are the best way to achieve this. Below are a number of filters that can be used.

Filtering by Assigned User

- 1. From the groups page, click the **Assigned To** menu on the filter bar.
- 2. Select an *assignee (username)* to display only the groups assigned to that verifier.

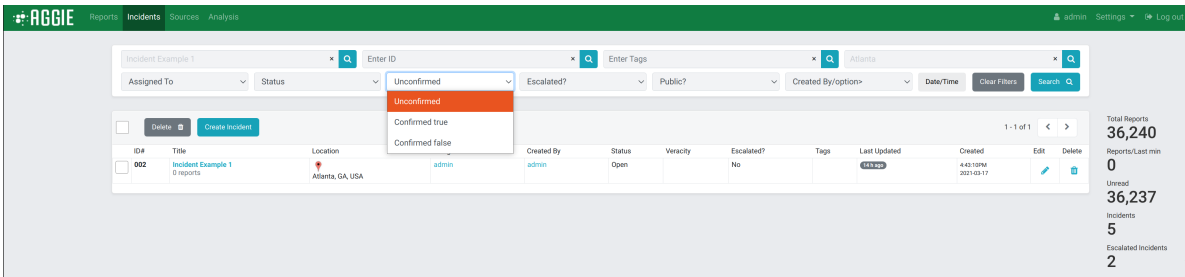


Filtering

by Assigned User

Filtering by Status

- 1. Click the **Status** menu on the filter bar.
- 2. Select *Open* or *Closed* to view groups in these categories.

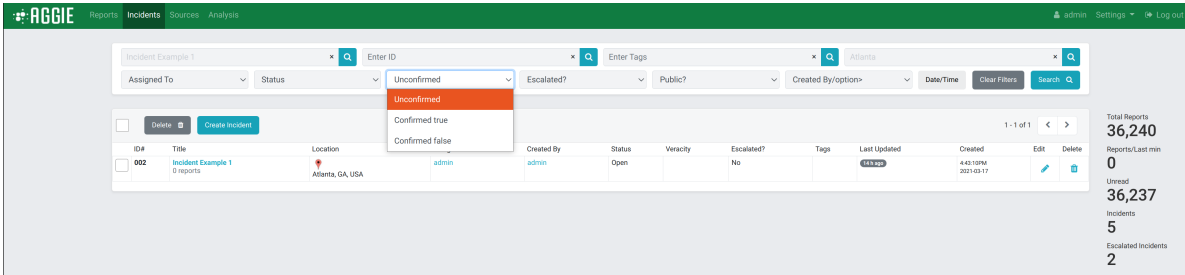


Filtering

by Status

Filtering by Veracity

- 1. Click the **Veracity** menu on the filter bar.
- 2. Select the veracity status (*unconfirmed, confirmed, confirmed true* etc.) to display all groups associated with that veracity status.



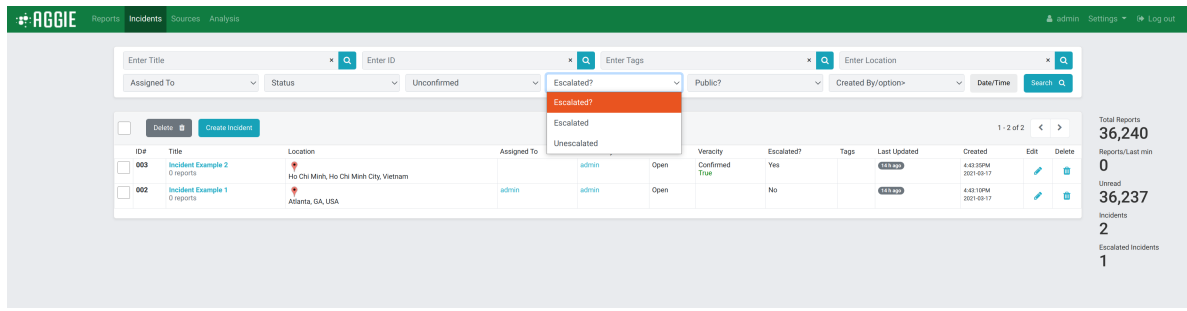
filtering

by Veracity

Filtering by Escalation

- 1. Click the **Escalated?** menu on the filter bar

2. Select the *escalation status (Escalated or Unescalated)* to display groups accordingly.

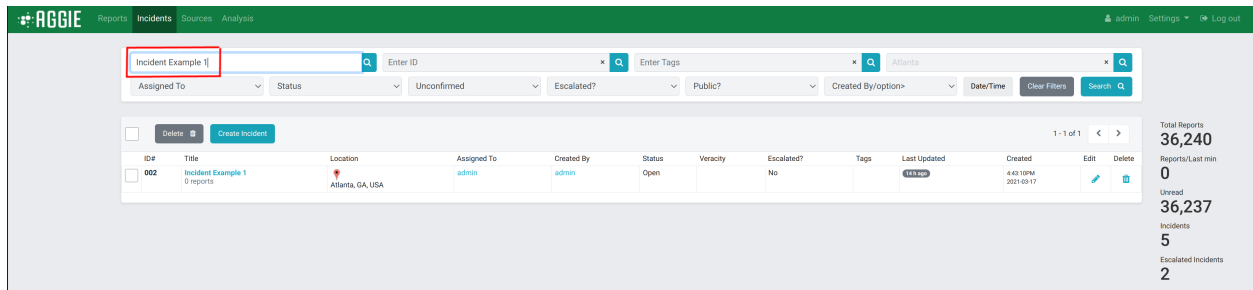


by Escalation

Filtering

Filtering by Title Search

1. Type in a *group title* in the **Enter title** space on the filter bar.
2. Click **Go** or hit the return key to *filter and display only groups* that include the entered title. For example by searching the group title “attacks”, there is a display of all groups containing this keyword.

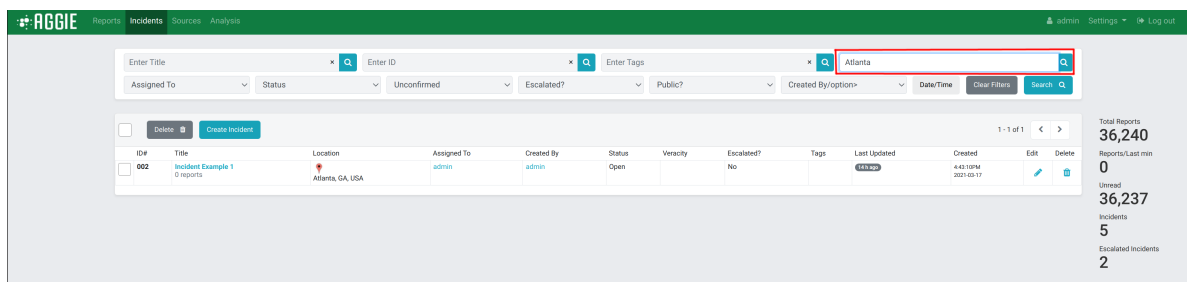


by Title Search

Filtering

Filtering by Location Search

1. Type in the name of a *location (town, polling station etc.)* in the **Enter Location** text box on the filter bar.
2. Click **Go** to display all groups associated with that location. For example, typing in *Ghana* in the *Location Text box*, display all groups whose location was entered as “Ghana”.



by Location Search

Filtering

CHAPTER 6

User Management

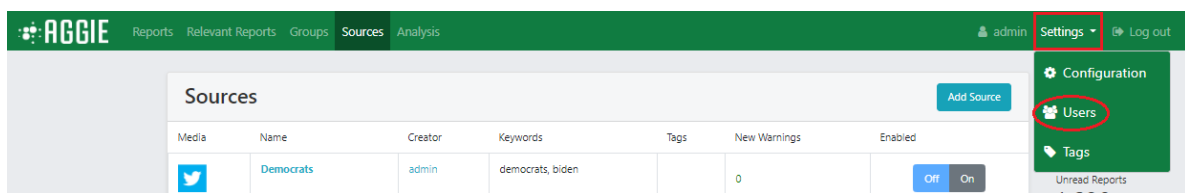
There are three main user categories in Aggie with varying Privileges: *Viewer*, *Monitor* and *Admin*. The table below indicates the privileges associated with each user category.

6.1 User privileges

6.2 Creating a New User

Only an *Admin* user can create a *new user*. To create a *new user*, follow the steps below.

1. Click the **Settings** tab.

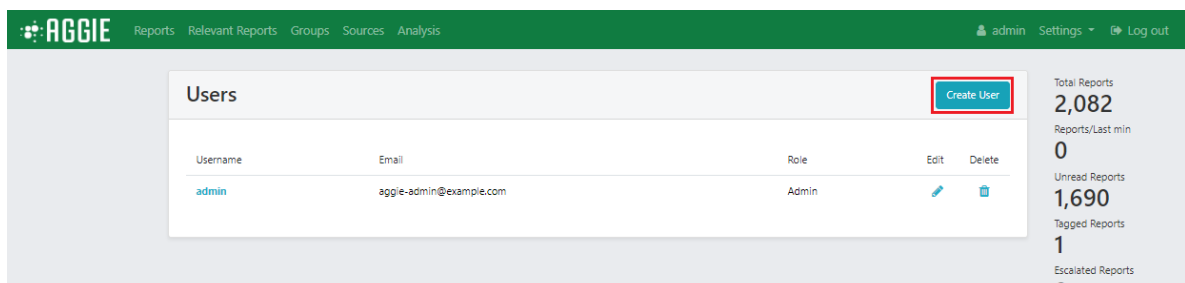


The screenshot shows the Aggie interface with the 'Sources' tab selected. The 'Settings' dropdown menu is open, and the 'Users' option is highlighted with a red circle. The 'Sources' table is visible below the header.

Media	Name	Creator	Keywords	Tags	New Warnings	Enabled
	Democrats	admin	democrats, biden		0	<input type="checkbox"/> Off <input type="checkbox"/> On

Creating a New User

2. From the drop down list click **Users**.



The screenshot shows the Aggie interface with the 'Users' tab selected. The 'Create User' button is highlighted with a red box. The 'Users' table is visible below the header.

Username	Email	Role	Edit	Delete
admin	aggie-admin@example.com	Admin		

Creating a new User

3. Click on blue **Create User** button on the left of the page.

Create User ×

Username

Email

Role
 ▼

Close Submit

Creating a new User

4. Type in the *Username* and the *user's email* address in the first two fields.
5. Select a *Role* (*Viewer*, *Monitor* or *Admin*) for the user. A user's role determines which actions they have permission to access, as per the table in the [User Privileges](#) section.
6. Click **Submit** to create a *new user*. The user will receive an email with a link to Aggie and the user can change their password after logging in.

CHAPTER 7

Indices and Tables

- `genindex`
- `search`