Aggie Documentation

Release 2.0

Tom Smyth and many others

Jul 22, 2020

Contents

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 Achitectural Design

Achitecturally, 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.
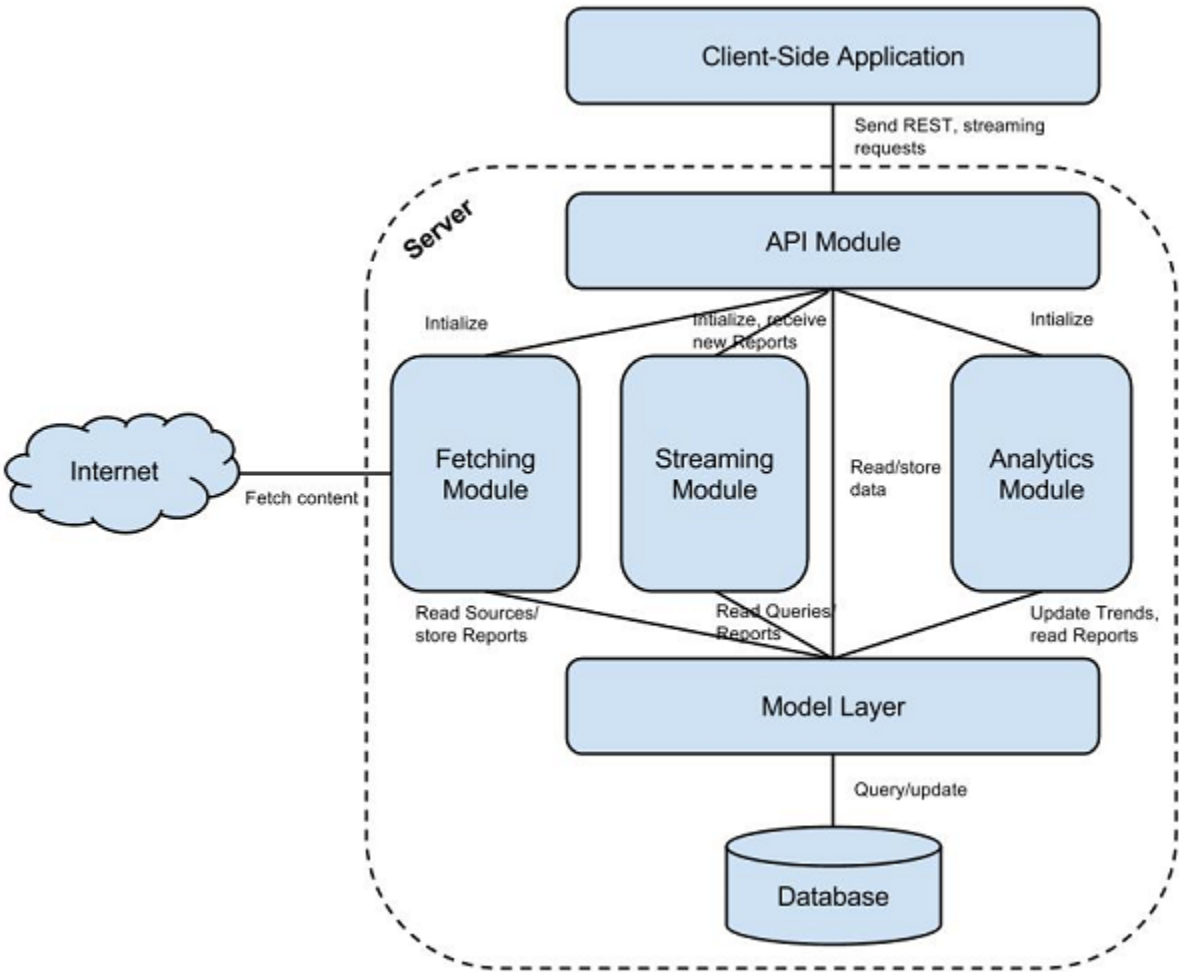
Achitectural Design

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 using docker by following the installation instructions on the GitHub repository.

For production and development, Aggie can also be installed from source after installing the right version of its dependencies, Node.js and MongoDB. See more details on the GitHub repository.

For production we PM2 process manager, and nginx as a web-server. You can get an example of our config file here, which enables https, cache, compression and http2.

Settings

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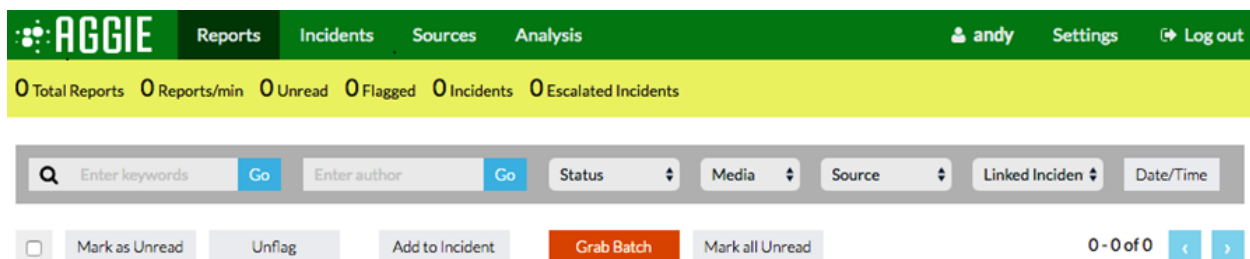
Main Menu

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 **Settings**.
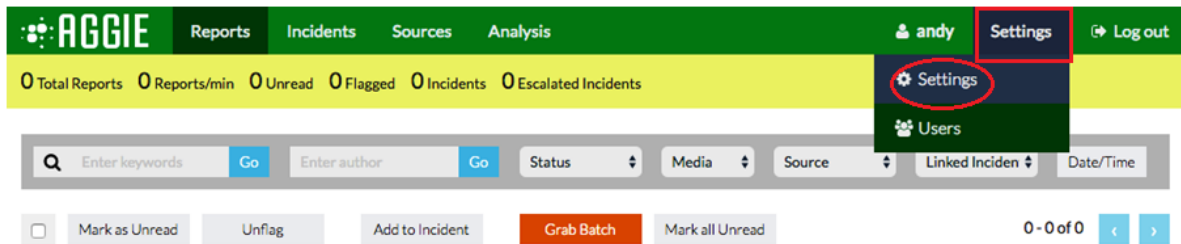
Fetching ON/OFF

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**.
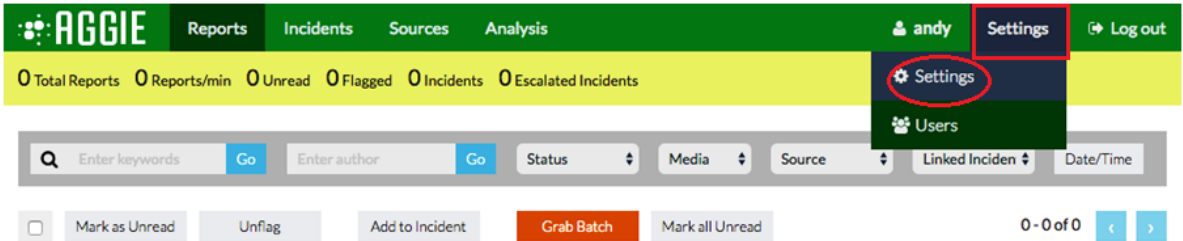
Settings
Menu

2. From the dropdown list, click on **Settings**.
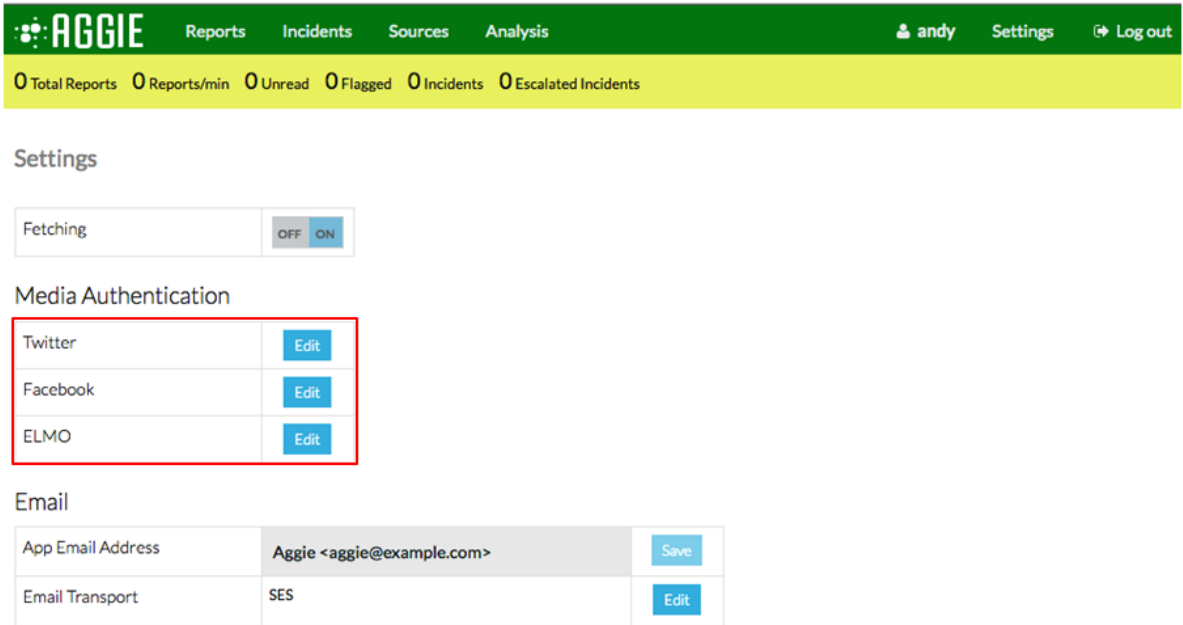
Media
Authentication

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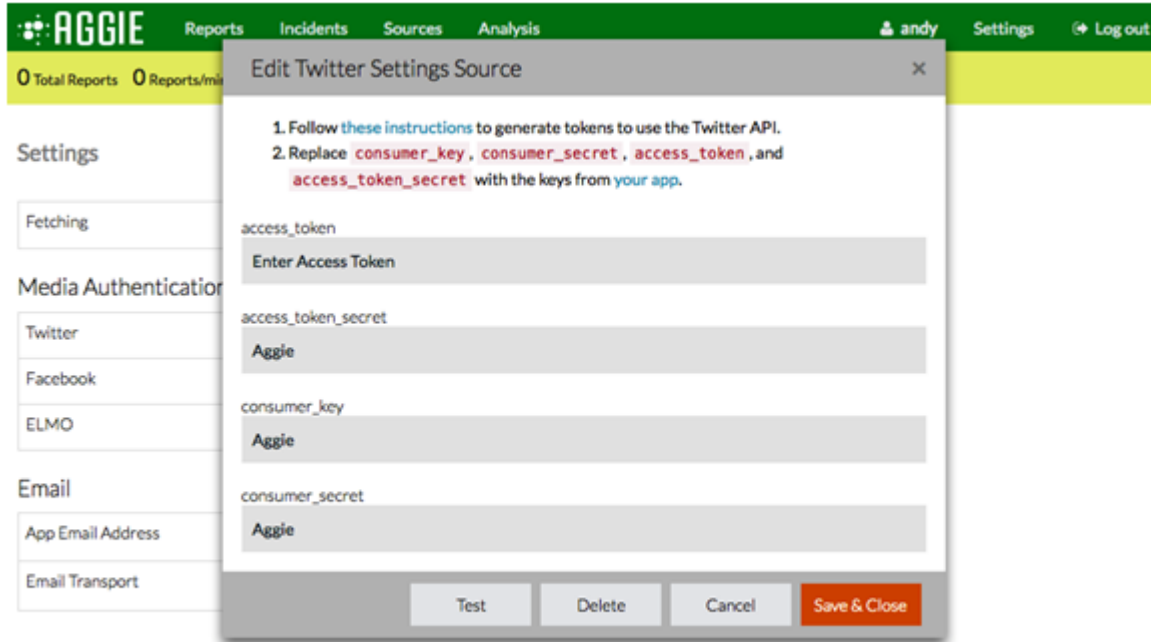
Media
Authentication

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.
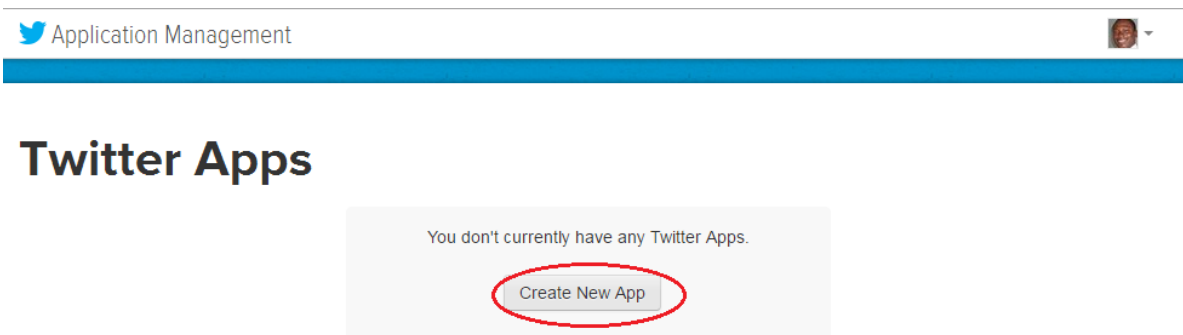
Twitter
Apps

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

Twitter Apps

4. This will create access tokens as indicated below.

Twitter Apps

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

Twitter
Apps

6. With these access tokens, fellow the instructions from *Adding Media Feeds to Aggie* section and edit the Twitter settings in Aggie.
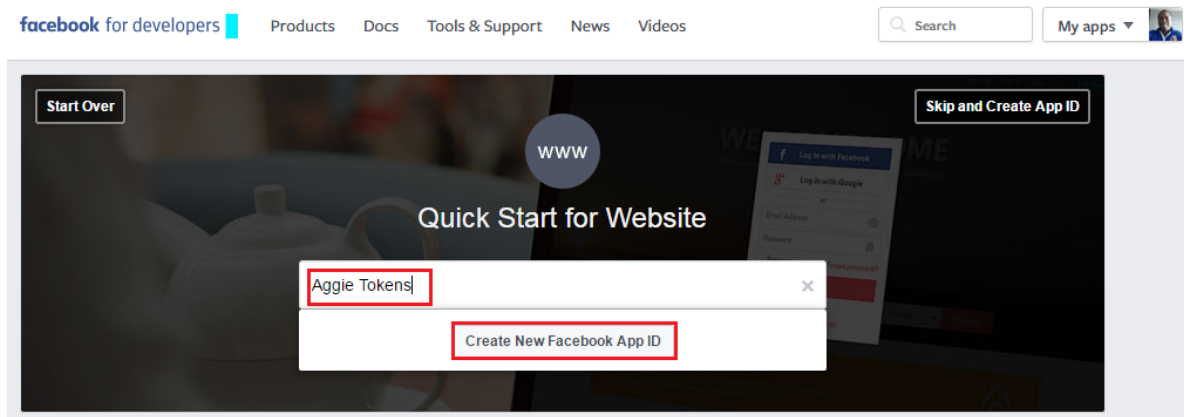
3.3.2 Facebook API Access Tokens

1. Visit Facebook's Apps page and login with your credentials.

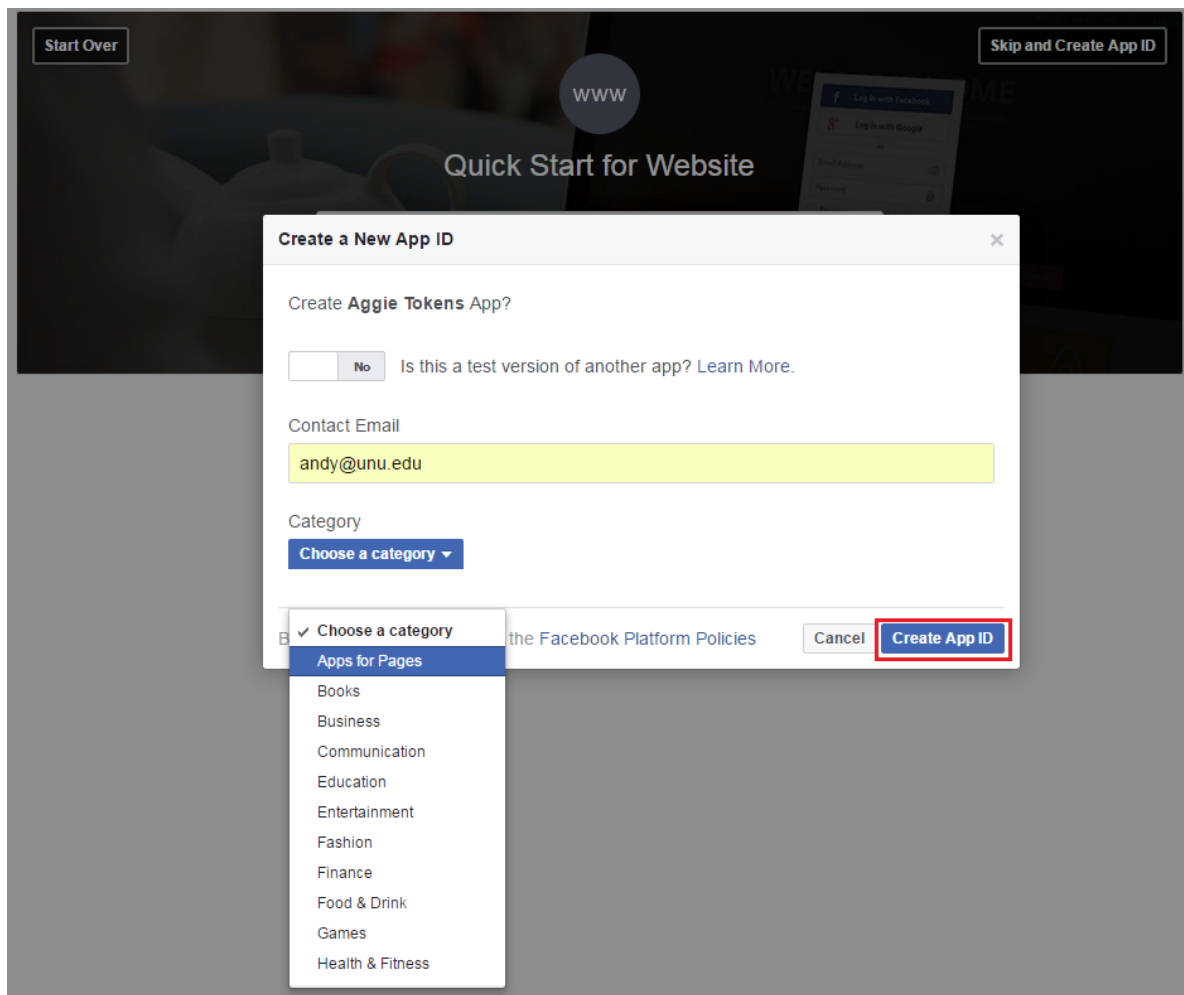2. Click on **Create a new app** at the top right corner.
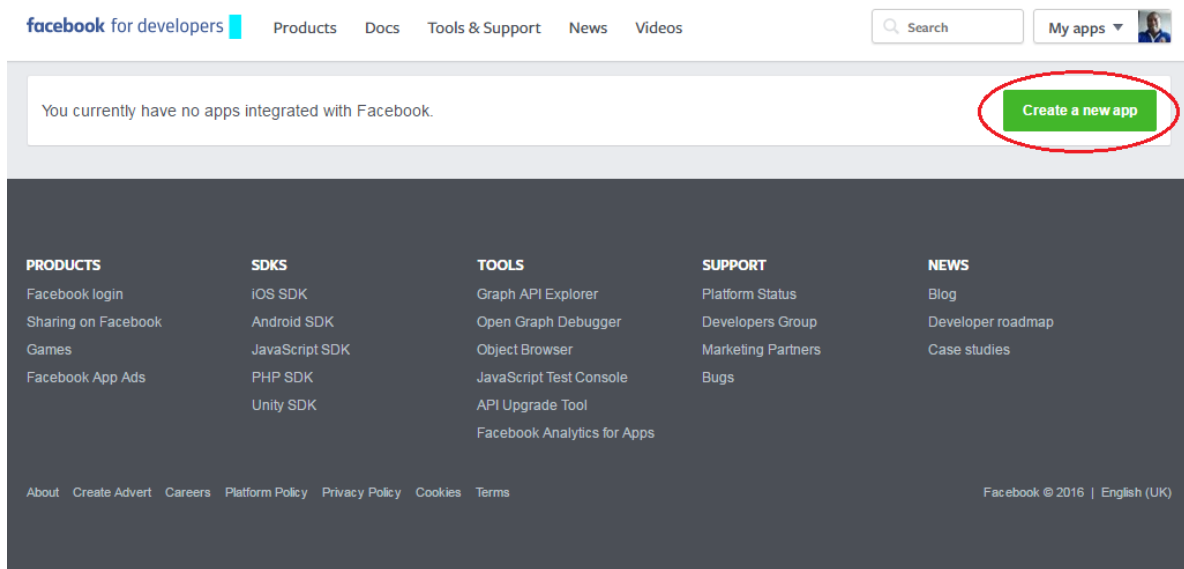
Facebook
Apps

3. Type in the *name* of your app and click on **Create New Facebook App ID**.

Facebook
Apps

4. Type in your *email address* and choose the *app category*, eg. *Apps for Pages* and click on **Create App ID**.
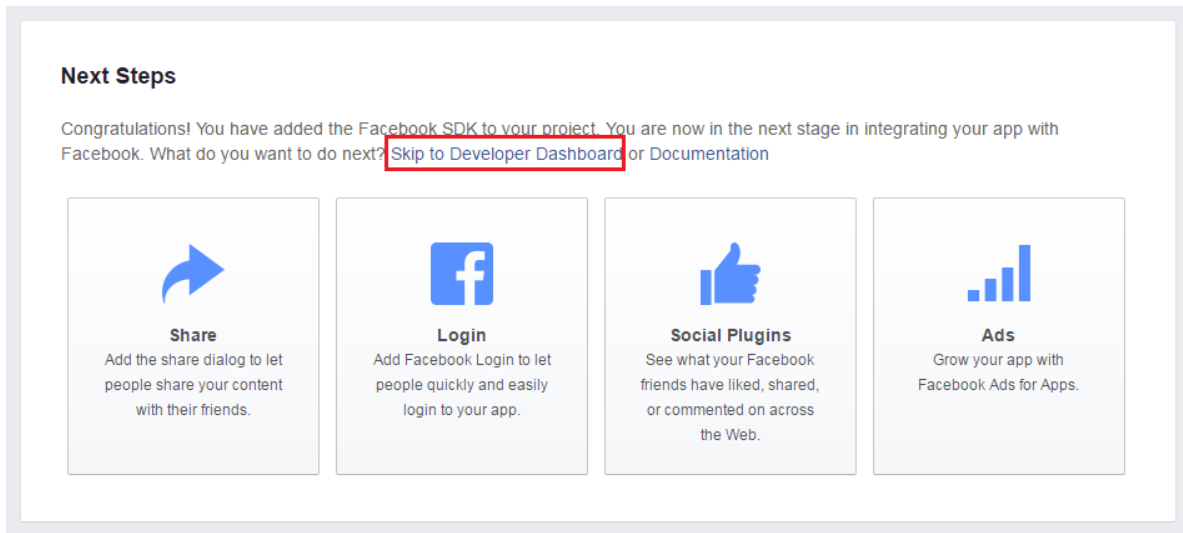

Facebook
Apps

5. Select the pictures that apply and click **Submit**.

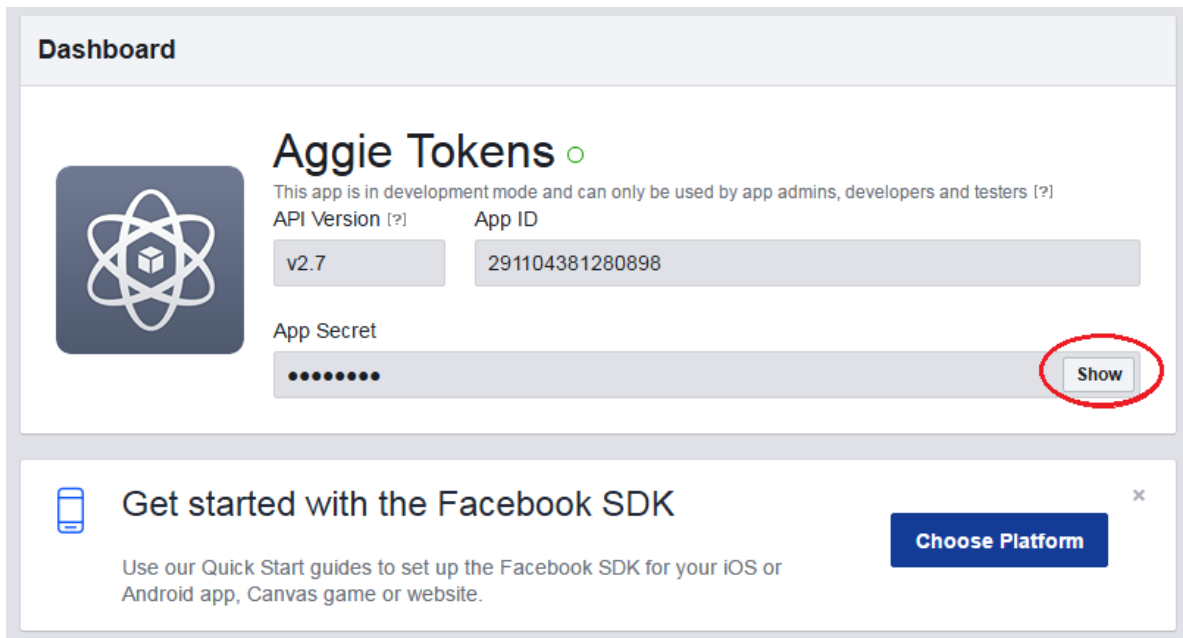6. Enter a *site URL* and click on **next**.

7. Click **Skip to Developer Dashboard** to retrieve your *App ID* and *App Secret*.

Facebook
Apps

8. Click on the **Show button** and enter your password to show your *App Secret*.

Facebook
App

9. Now with your Facebook *App ID* and *App Secret*, copy **https://graph.facebook.com/oauth/access_token?client_secret=xxx&cli** into your web browser, replacing the (**xxx**) in **secret = xxx** and **id=xxx** with your *App Secret* and *App ID* respectively.

10. Hit the return key to show your access token.

11. With this access token,fellow the instructions from *Adding Media Feeds to Aggie* section and edit the Facebook settings on Aggie.

3.3.3 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.

1. Install Firefox in Linux using your distribution preferred method.

2. Install GNotifier add-on in Firefox.

3. 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 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.

3.3.4 Google Places API

Aggie uses Google Places API to add location to the incidents, letting users to search for incidents 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.

3.3.5 ELMO Tokens

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 -> Settings** 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 **Settings** option in the dropdown list.

Email

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

Sendgrid

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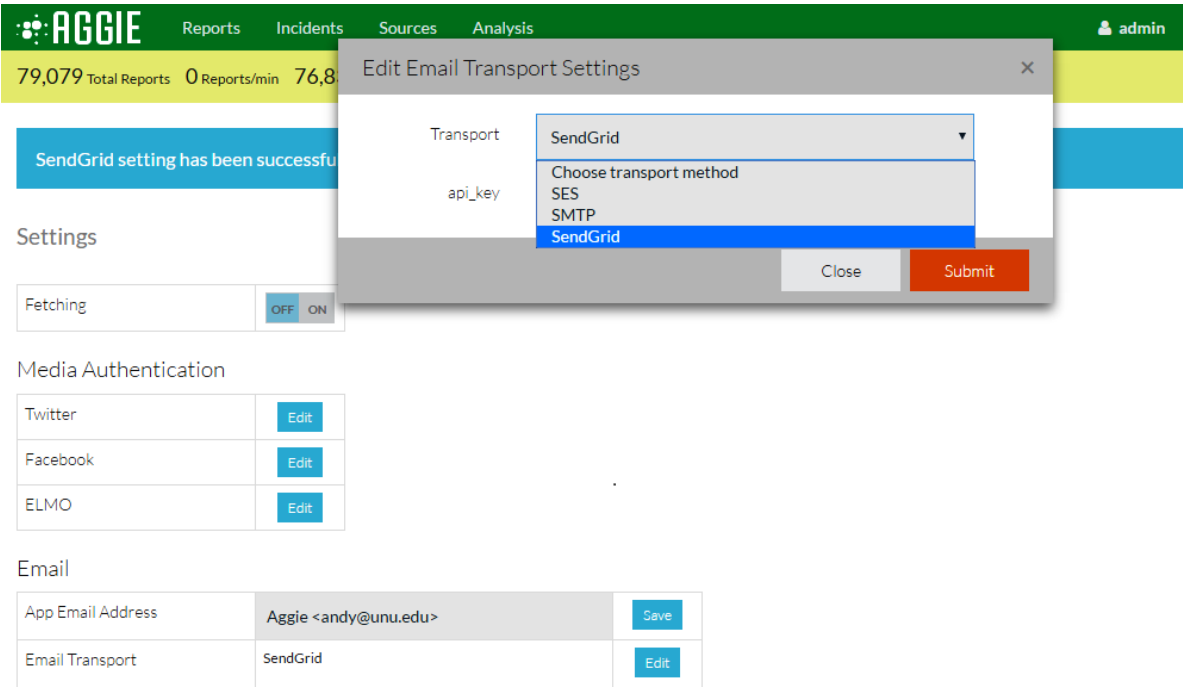
Sendgrid

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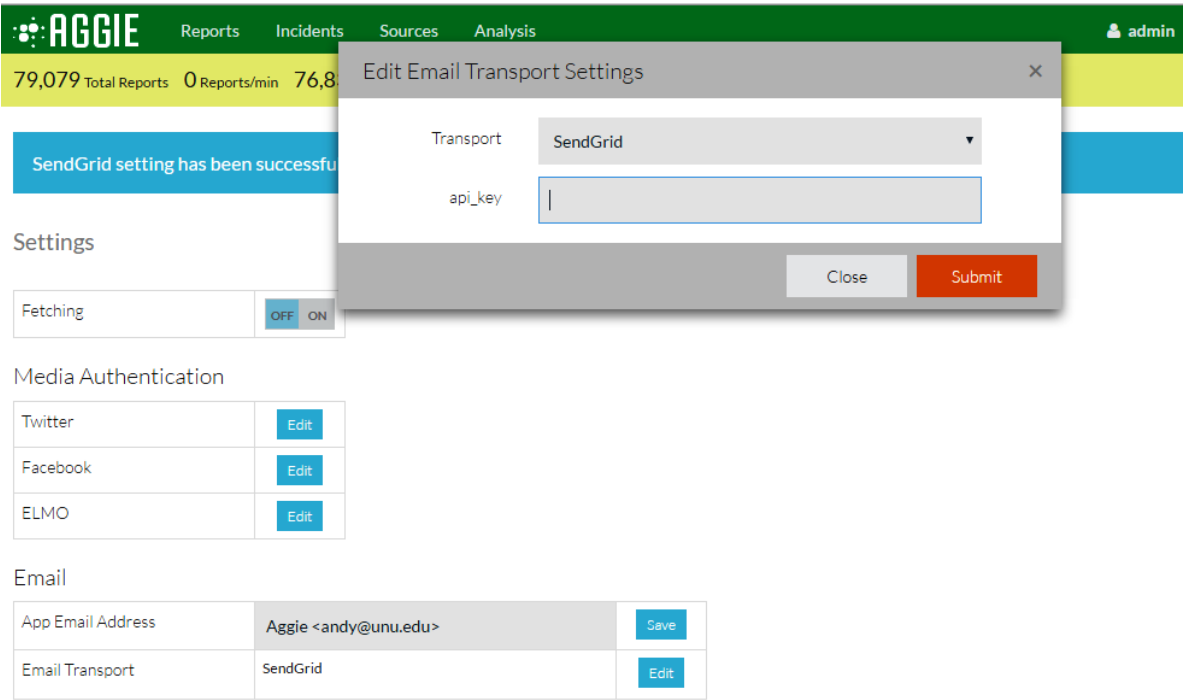
Sendgrid

3.4.1 Generating SendGrid API Key

1. Visit SentGrid'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.
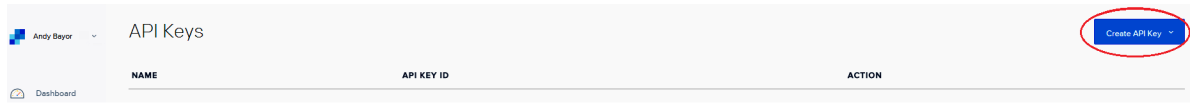
Sendgrid

4. Select *General API key*.

Sendgrid

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.

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 Incident Map.

3.5.1 Public Incident Map

The Public Incident Map displays those *incidents* 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.
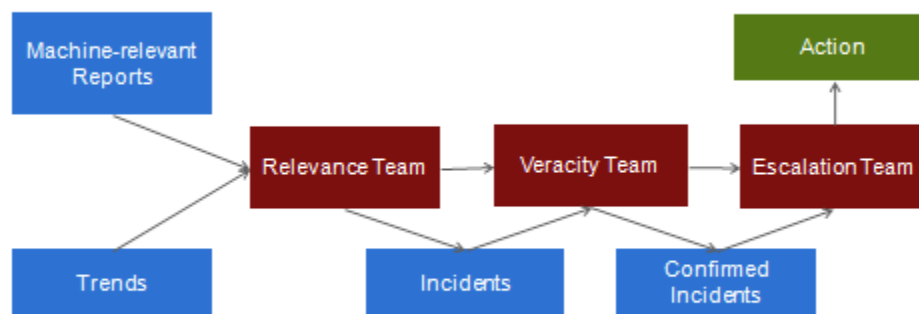
SMTC
Work Flow

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.

Using Aggie

5.1 Sources

5.1.1 What is a Source?

Sources are the social media platforms such as *Twitter, Facebook, Ushahidi, and RSS feeds* that Aggie crawls through to aggregate reports relevant to the event being monitored.

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.

5.1.2 Adding Sources to Aggie

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

Sources

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

5.2 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.

Sources

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*, *Flag reports*, *Create Incidents*,*Filter reports* or add a report to an *Incident*. 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 Incident column**: This column is used to add a report to an existing incident or create a new incident.
- **The Flagged column**: This column is used to note/identify reports for reference.

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.

Navigation

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 – such as *"flagging"* or *"adding reports to incidents"*. Upon completely taking desired action on the collected reports, trackers can grab another batch by clicking the "**Mark All Read & Grab Another**" button.

Grab

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 Flagging Reports

A *flag* is a way of marking a report for future reference. Trackers might come across certain reports they wish to revisit and easily find. In situations like that, trackers can flag the report and then *filter* it latter by using *flagged reports* filter.

To Flag a Report

1. Select the report(s) to be flagged using the *checkboxes* on each report row.

2. Click the **Flag** tab beneath the filter bar if multiple reports are selected.

3. You can flag a single message by clicking the **little flag** in the last column of the report's row.

For example to flag the sixth report, you click on the *flag* in the last column of the first row. You notice that a report is flagged by the *light pink highlight* and the *black flag* on the report as indicated below.

Flagged

5.2.8 Creating Incidents

Adding a report to an existing Incident

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

Creating a New Incident

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

Incidents

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

Incidents

3. Select the related category of an *existing incident* to add the report to that incident or. . . **If it's a new Incident**;

4. Click on the *blue* **Create a new Incident** link to create the new incident.
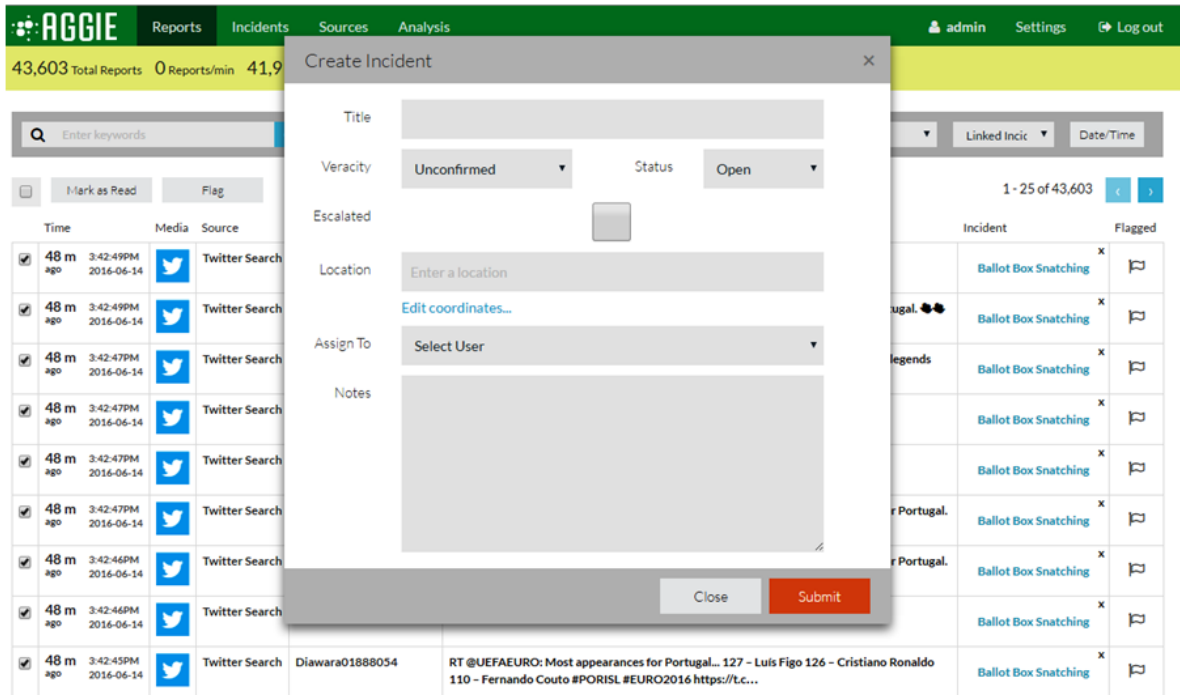
Adding Incident

5. Type in the *Title* of the incident (*e.g. Polling station not open, Voter intimidation etc*), the *Location* of the incident and a brief *note* describing the incident. Leave out the *veracity* and *assignment* fields for the veracity team and click **submit** to create a new incident. 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 incident to the list of public incidents. The *Public Description* will appear attached to the incident, for example, in the *Public Incident Map*.

5.2.9 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.

```
![Filter Bar](filter_bar.png)
```

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 Date/Time

Filtering by Incident

1. Click on the **Linked Incident** tab and select an incident to view all related reports tagged to that incident.

2. In this example, selecting the incident *Hate Speech* shows the three reports which have been linked to that incident.

Filtering by Incidence

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 Incidence

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. Flagged, 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 by Keywords

5.3 Incidents Page Activities

5.3.1 What is an Incident?

Incidents are groups of one or more *reports* that, once verified, require an action. As Aggie aggregates reports from different sources, tracking team members in the SMTC collect reports into incidents.

5.3.2 The Incidents Page

From your Aggie header page, click the **Incidents** Tab. This will show you the incidents page as indicated below.

Incidents Main Page

5.3.3 Sections of the Incidents Page

- **The Checkbox column:** This is used to select one or more incidents that some actions can be applied to.

- **The ID# column:** This column indicates the unique identification number generated for each incident created. This example starts with 003 because incident 001 and 002 have been deleted.

- **The Title column:** This column shows the name given to the incident and the number of reports associated with the particular incident.

- **The Location column:** This column shows the place where the incident occurred.

- **The Assigned to column:** This column indicates the veracity team member who has been assigned to verify the incident for confirmation (and then escalation) or closure.

- **The Status column:** This column shows whether the incident 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 incident. Whether the investigations confirmed the incident to be true or false.

- **The Escalated column:** This column show whether a confirmed incident 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 incident.

- **The Edit/Delete Column:** This column contains two tools for editing or deleting an incident; to edit the incident, click the blue **Pencil Icon** or to **delete** the incident click the blue **small bin**.

5.3.4 Creating an Incident

Normally, *incidents* are created by Trackers. However, should the need arise, verifiers can create *incidents* from the incidents page. To do this, refer to *Creating a New Incident* section.

---

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

Creating Incidents

2. From the incidents page, click the blue colored **Create Incident** tab.

Creating an Incident

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

5.3.5 Editing an Incident

Verifiers can always update the status of incidents 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 an Incident. To do this:

1. From the incidents page, click the **blue edit pencil** at the end of the incident row (last column).
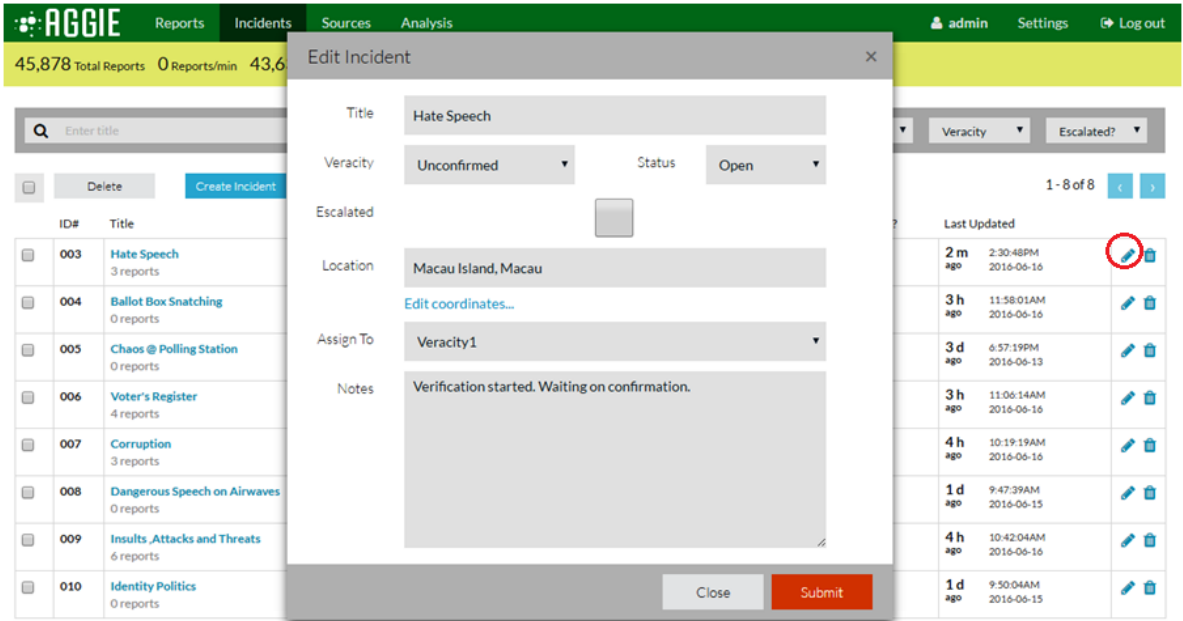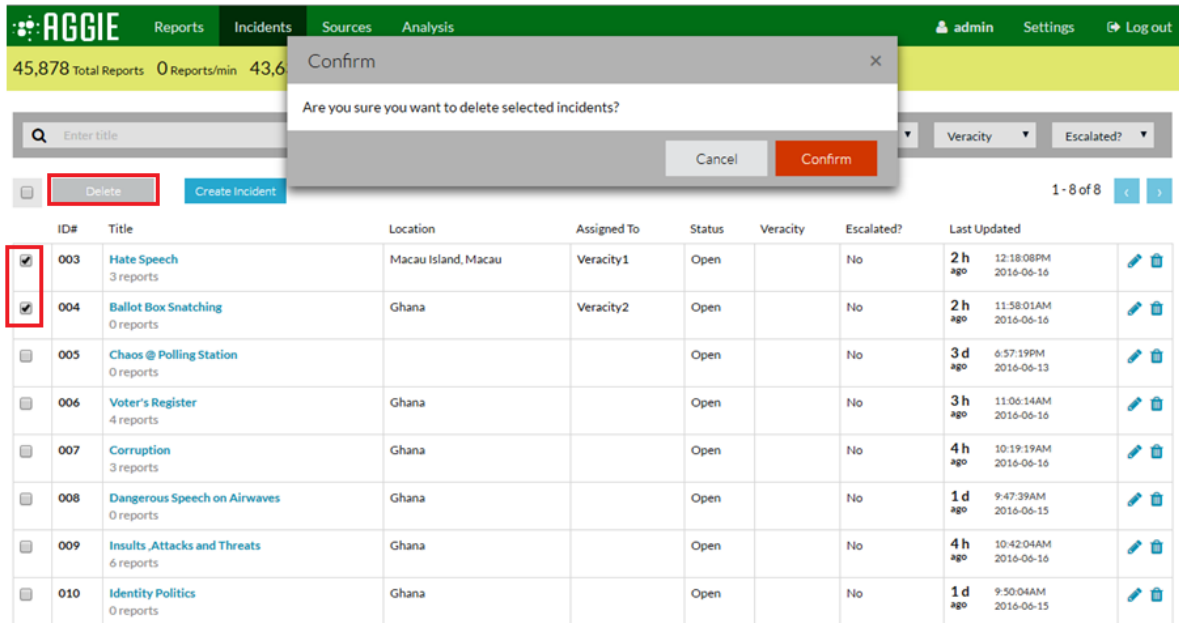
Editing an Incident

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

5.3.6 Deleting an Incident

If a veracity team member notices a redundancy in incidents, they may *delete* an incident from the Incidents page. To do this:

1. Select the *incident(s)* you wish to delete by checking its/their respective *checkbox(es)*.

2. Click the **Delete** button below the filter bar to the left.

Deleting Incidents

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

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

5.3.7 The Incident Filter Bar

With *filters*, verifiers can narrow down their search. In some cases, there might arise the need to search for specific types of incidents. 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 incidents page, click the **Assigned To** menu on the filter bar.

2. Select an *assignee (username)* to display only the incidents assigned to that verifier.

Filtering by Assigned User

Filtering by Status

1. Click the **Status** menu on the filter bar.

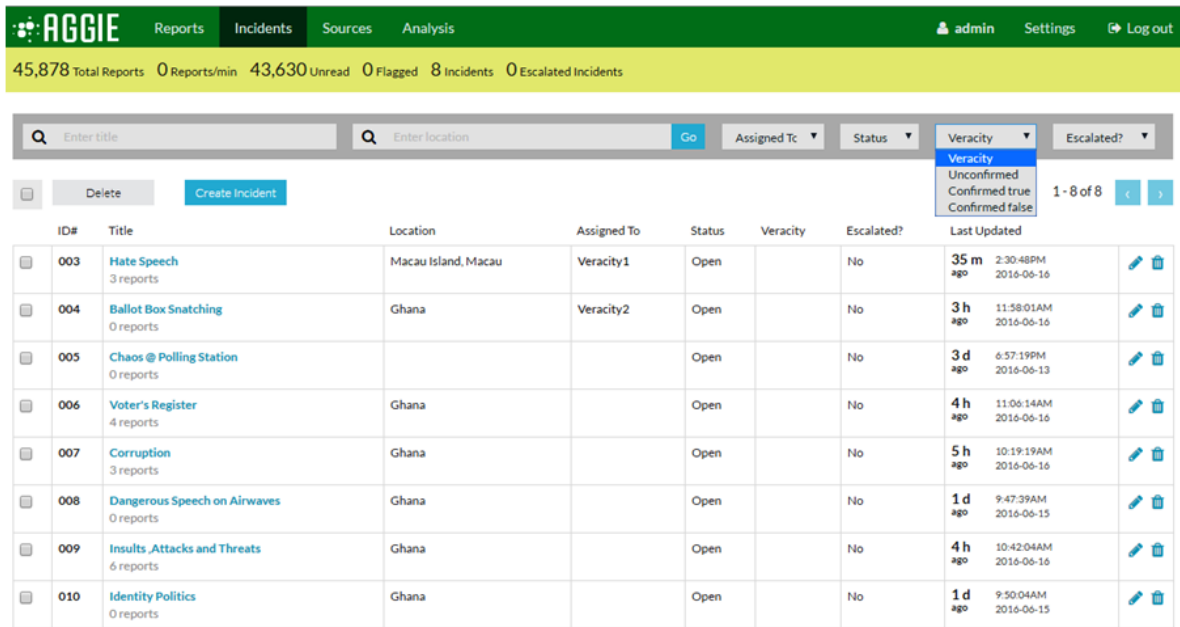2. Select *Open* or *Closed* to view incidents in these categories.

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 incidents associated with that veracity status.
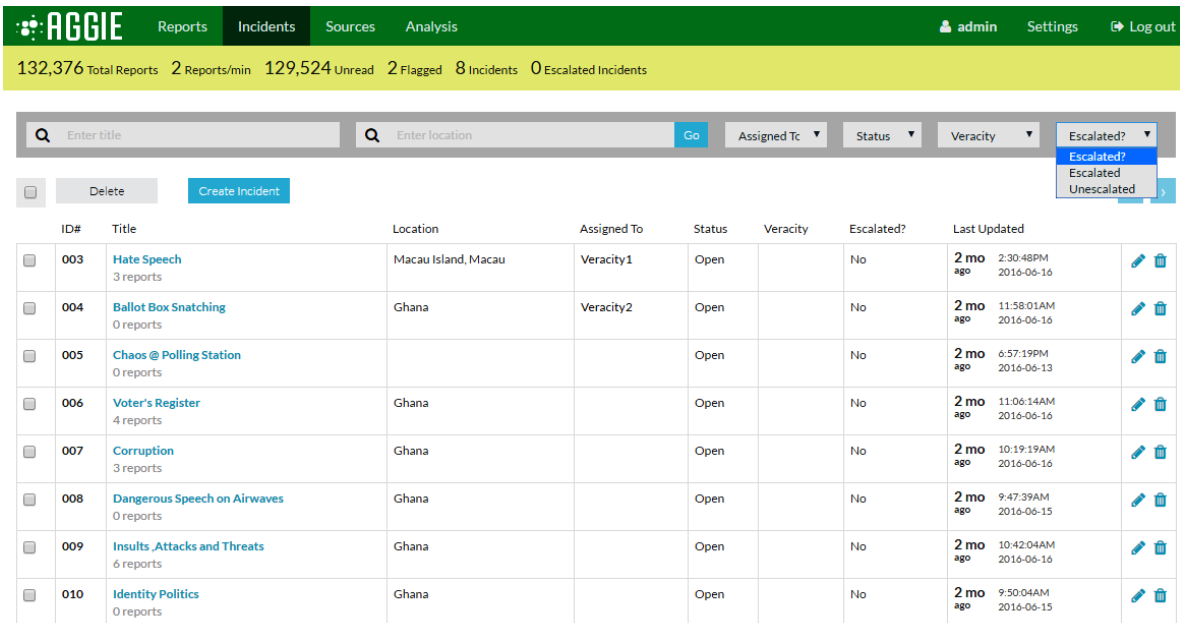

filtering by Veracity

Filtering by Escalation

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

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

Filtering by Escalation

Filtering by Title Search

1. Type in an *incident title* in the **Enter title** space on the filter bar.

2. Click **Go** or hit the return key to *filter and display only incidents* that include the entered title.For example by searching the incident title *"attacks",* there is a display of all incidents containing this keyword.

Filtering by Tittle Search

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 incidents associated with that location. For example, typing in *Ghana* in the *Location Text box*, display all incidents whose location was entered as *"Ghana"*.

Filtering by Location Search

5.4 Trend Analysis

Trend analysis give snappy and easy graphical visualizations of the occurrences of incidents using keywords, social media type, the Twitter handles, or Facebook groups/pages to build trends.
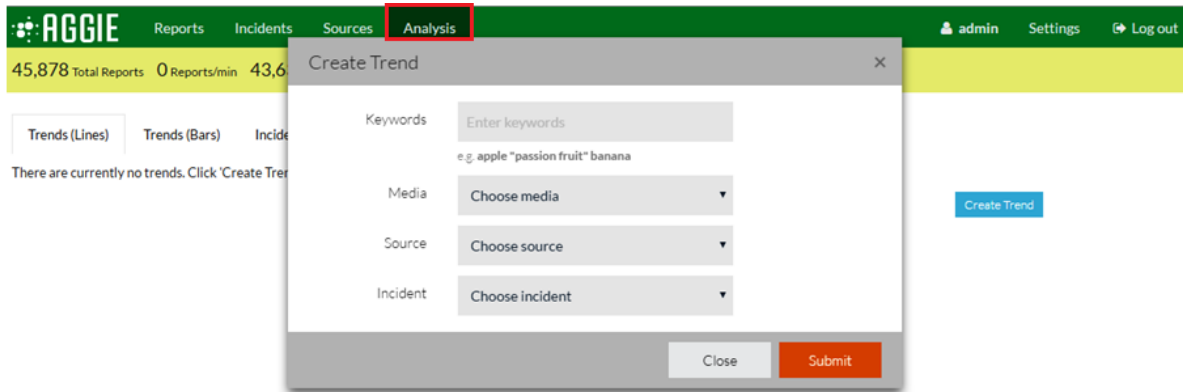
5.4.1 What is an Analytic Trend?

An analytic trend is a graphical visualizations of incidents as bar charts or stacked lines.

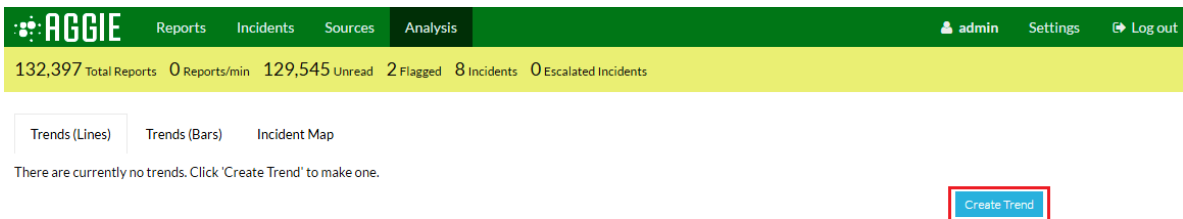## 5.4.2 Creating a Trend

To create a trend visualization:

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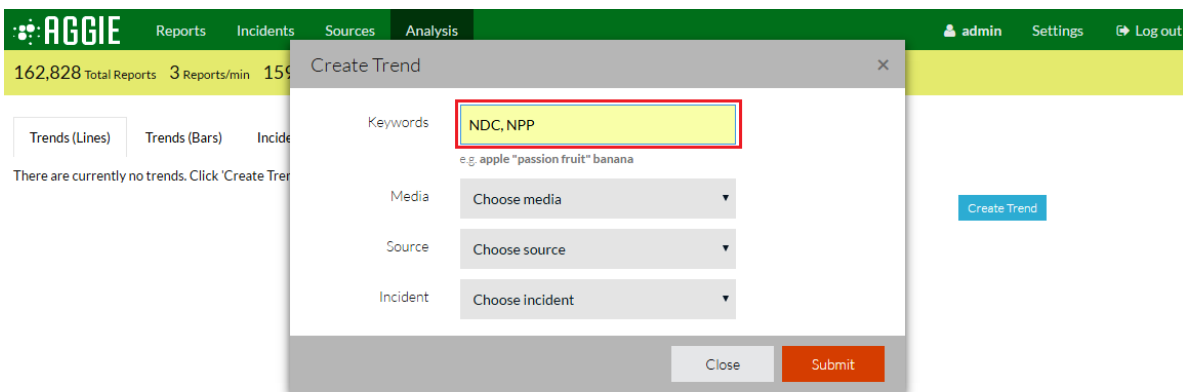

Trends
Main Page

2. Click the blue **Create Trend** button.
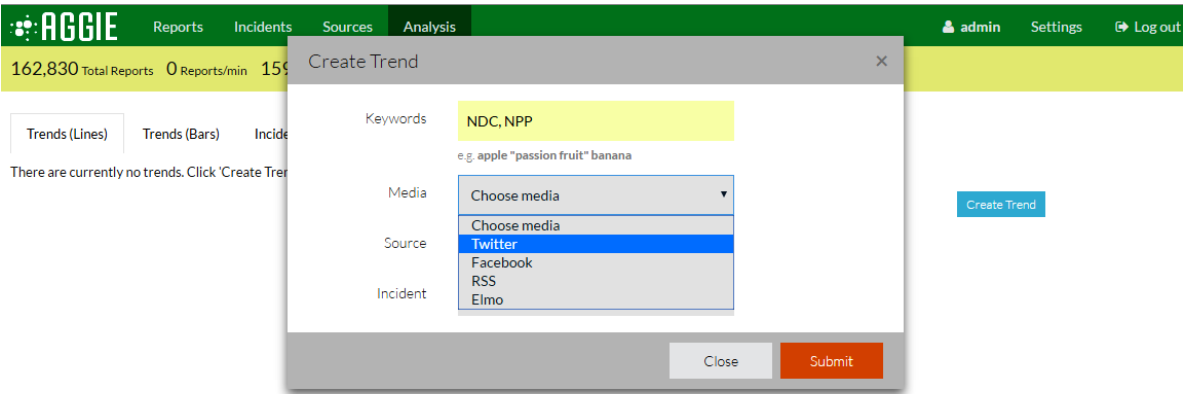

Creating
a Trend

3. Enter the *keyword(s)* you want to create the trend for. For example *NDC, NPP*.
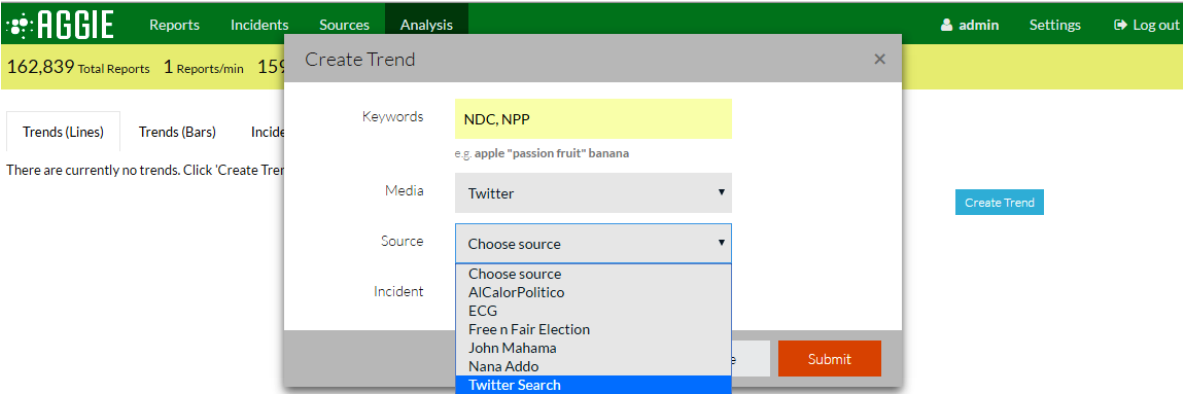

Trend
Keywords

4. Choose a *Social Media Source* for the trend e.g. Twitter, RSS or Facebook.
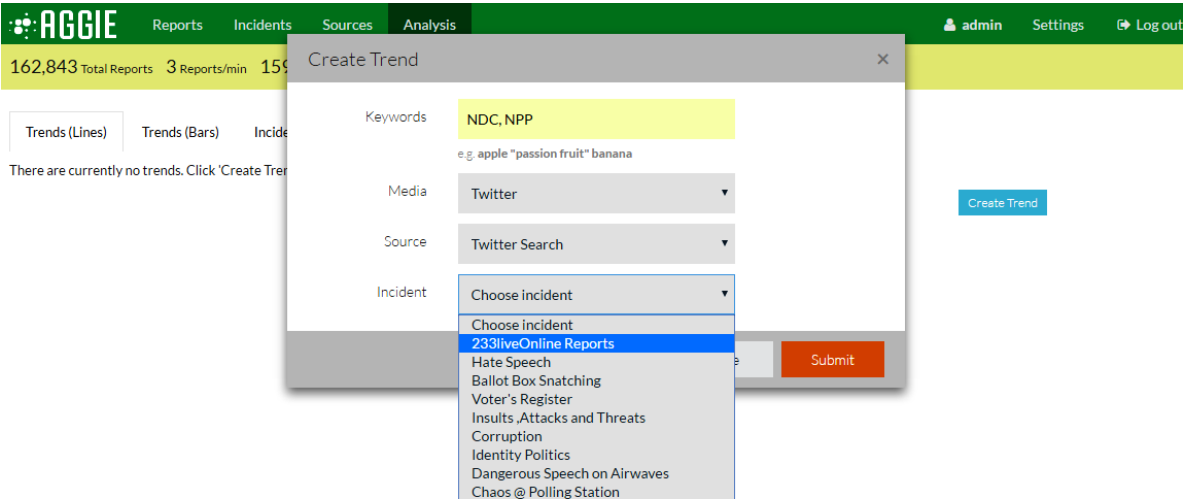
Trend Media Type

5. Choose the *Source* of the trend i.e. the *social media account* been followed.
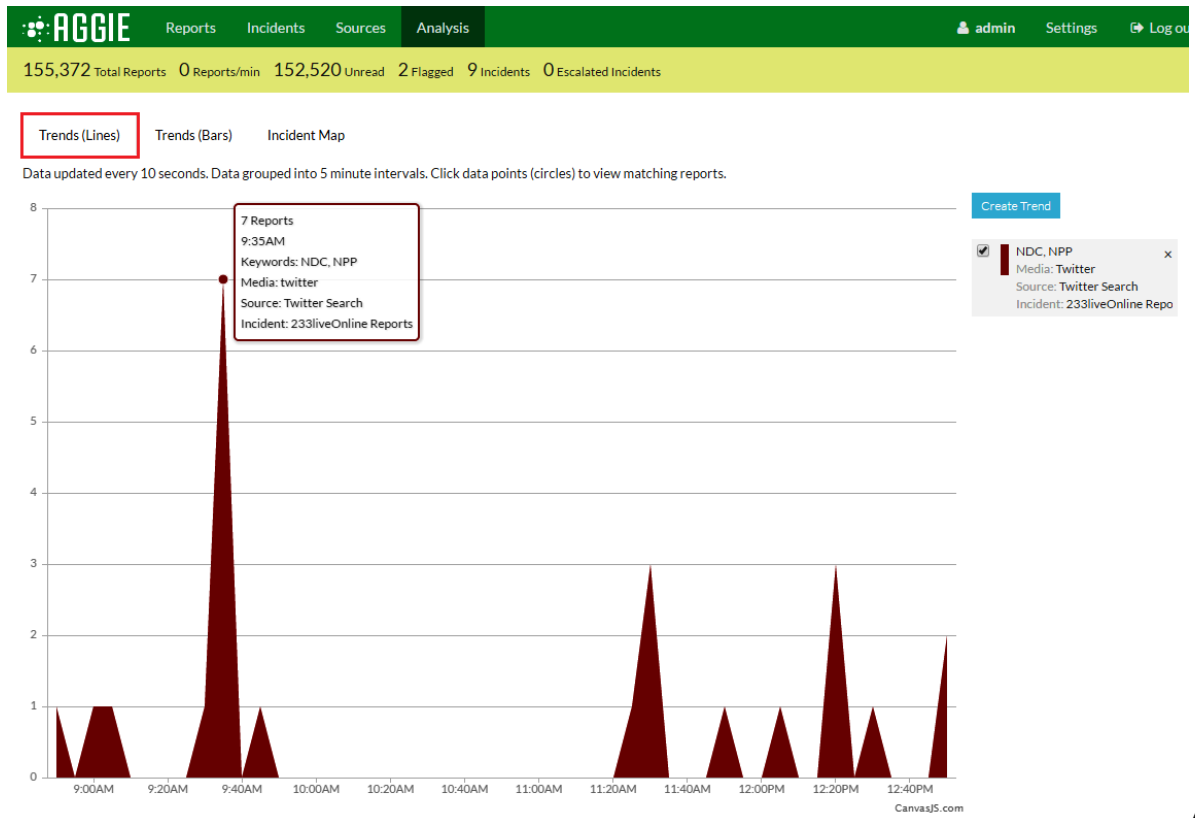

Trend Source

6. Choose the *Incident* for the trend e.g. *233liveOnline Reports*

Trend Incidents

7. Submit and view the analytics by *Trend (Lines or Bars)* and *Incident Maps*.

Analysis

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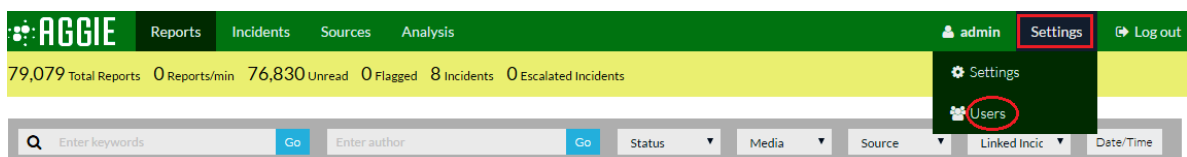
There are three main user categories in Aggie with varying Privileges: *Viewer, Monitor* and *Admin*. The table below indicates the privileges associated with each user category.

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.
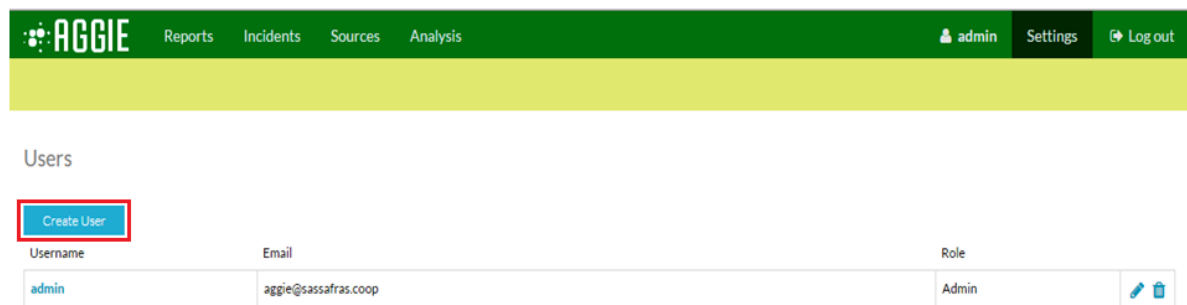
1. Click the **Settings** tab.

Creating a New User

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

Creating

a new User

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

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.

Indices and Tables

- genindex
- search