CLEARVIEW EVENTS

User Guide

TABLE OF CONTENTS

CLEARVIEW EVENTS **3**

1. RULES **6**

1.1 Pre-Defined Rules 6

1.2 Update & Applying Changes 7

1.3 Edit Ruleset – Add or Modify 8

1.3.1 Add New Rule 8

1.3.2 Modify Rule 10

1.3.3 Delete Rule 10

1.4 Criteria to Trigger Rule 10

1.4.1 Edit Criteria 11

1.4.2 Delete Criteria 12

1.5 Rule Exclusions – Remove False Positives 13

1.5.1 Steps to Exclude 13

1.5.2 Exclude pattern words 14

1.6 Inclusions - Add Strings to Rule 14

2. RULE ACTIONS **16**

2.1 Default Actions 16

2.1.1 Blocked Message – Stop Processing 17

2.1.2 Block Messages – When to Use 17

2.2 Add, Modify or Delete an Action 17

2.2.1 Add New Action 18

2.2.2. Create a Custom Block Message Action 19

2.2.3 Modify Action 20

2.2.4 Delete Actions & Sub-Actions 20

3. QUERIES **21**

3.1 Default & Custom Queries 22

Default Rules for ClearView 22

3.1.1 Query Panels – Conditions, Graph & Results 23

Results Panel is your Report View 23

3.2 Modify Queries 23

3.2.1 Modify Condition Panel 24

Display more Results - Before and After Views 25

Modify or Add Conditions 27

3.2.2 Modify Graph Panel 29

3.2.3 Modify & Drill-down on Results Panel 29

Export Page 31

3.3 Saving Queries 31

3.3.1 Save 31

3.3.2 Save As 32

3.3.3 Unable to Save? 33
3.4 Create New Queries & Add Conditions 33
3.5 Deleting Queries & Conditions 34
3.5.1 Unable to Delete? 34
3.6 Exclusions in a Query 34
3.7 Conditions Definitions 36

4. REPORTING 38
4.1 Report Catalogue 38
4.1.1 Filter Reports 38
4.1.2 Create New Reports 39
Section Breaks 40
4.1.3 Edit, Duplicate & Delete Reports 40
Edit 40
Duplicate 41
Delete 41
4.1.4 Generate Reports 42
4.2 Schedule Reports 43
4.2.1 Add Schedule Report 44
4.2.2 Report Frequency 44
4.2.3 Modify Schedule Reports 45
4.2.4 Save Schedule Reports 45
4.2.5 Filter Schedule Reports 45
4.2.6 Delete or Disable Schedule Reports 46

5. GROUPS & PERMISSIONS 47
Add a Specific ClearView Access Group 47
5.1 Group Permissions 48
5.2 Data Source Permissions 50
5.2.1 Data Source Excluded Groups 50
5.3 User Groups - Interface Views 51

CLEARVIEW EVENTS

The ClearView platform acts as a catalyst to enable enhanced protection for students while at the same time reinforcing the training and policies set by the school around positive digital citizenship. As soon as the ClearView platform is implemented, it automatically identifies patterns of behaviour that indicate a risk or policy breach. It identifies evidence-based triggers that can support the circumstantial events and intuition of professionals within the school.

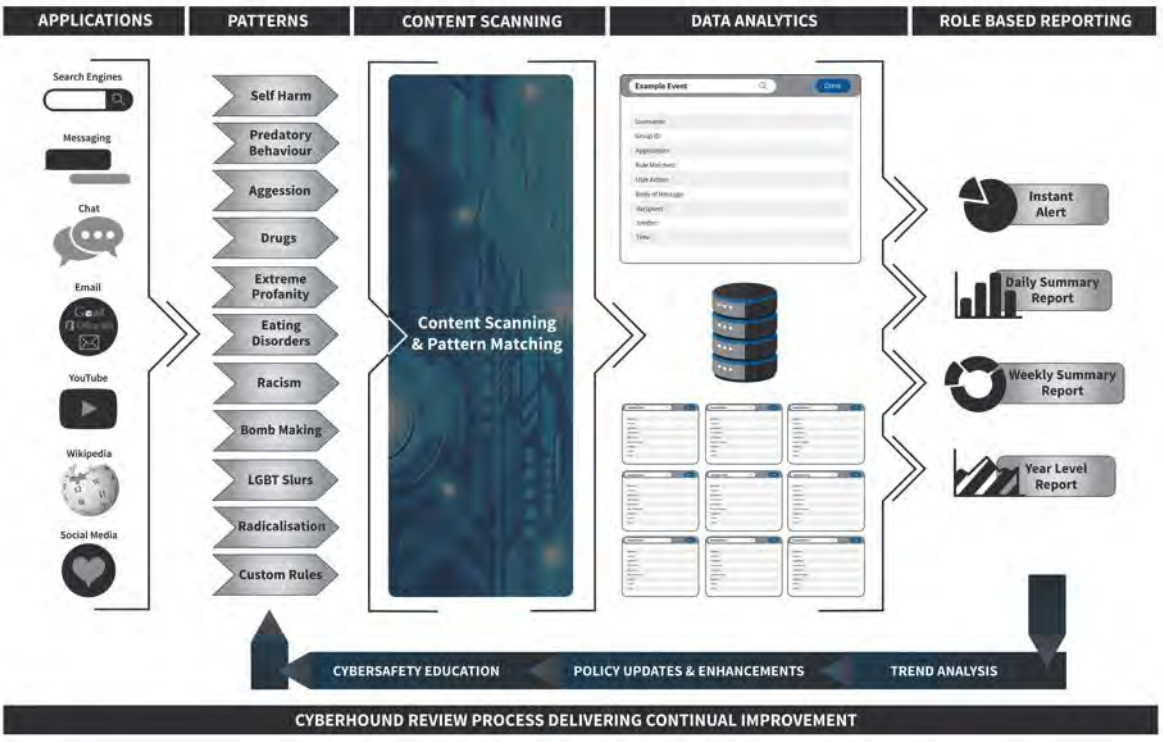
CyberHound ClearView scans all popular search engines, webmail and email (if configured), and social media traffic in real-time against predefined patterns. Creating Rules, Actions and Queries allows easy identification of patterns of behaviour requiring monitoring to help prevent and identify issues concerning student safety.

ClearView outcomes provide behavioural analysis for:

- Early intervention for at-risk students.
- Pro-active student protection or monitoring.
- Delivery of immediate feedback to promote responsible digital citizenship.
- Re-training and feedback to a student or cohort to align with school policies.
- Developing strategies to address new threats or to deal with the emergence of concerning patterns.

ClearView provides behavioural analysis via a process of:

- Scanning popular applications.
- Applying Rules and Actions that meet the school policies.
- Scanning content for pattern matching to words or phrases as set by the Rules.
- Collates data for detailed analysis to provide holistic view of the activity.
- Distributes reporting designed specifically for the user and delivered as required.

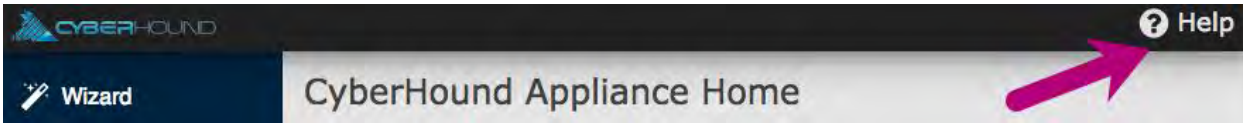


ClearView is constructed and viewed on the following areas:

1. RULES	Trigger the pre-defined patterns and populate the ClearView data source.
2. ACTIONS	Determine what needs to happen when the Rule is triggered. When all the Criteria for a Rule are met, then the Action is executed.
3. QUERIES	Are built with one or more conditions to refine the data triggered and provide the ability to filter and drill-down to reach detailed relevant information for reporting and analysis.
4. REPORTING	Manage and create custom reports for review and analysis of data and schedule for circulation to specific members of staff.
5. GROUPS & PERMISSIONS	Assign access permissions to the system relevant for user Groups for review and analysis of the data.

CyberHound provides predefined default Rules, Actions, Queries and Reports making use of ClearView easy for users. Understanding the construction and results of the pre-defined defaults, assists in considering any gaps that may require customisation or modification of existing parameters to meet the needs of the school. The following information will provide a 'how to' for each step and an understanding of why they are used or suggested.

PLEASE NOTE: Further technical information, for all areas of the CyberHound Appliance, is available in the **Help** content area within the Appliance. The following information only relates to ClearView to ensure all users are confident in obtaining relevant information.



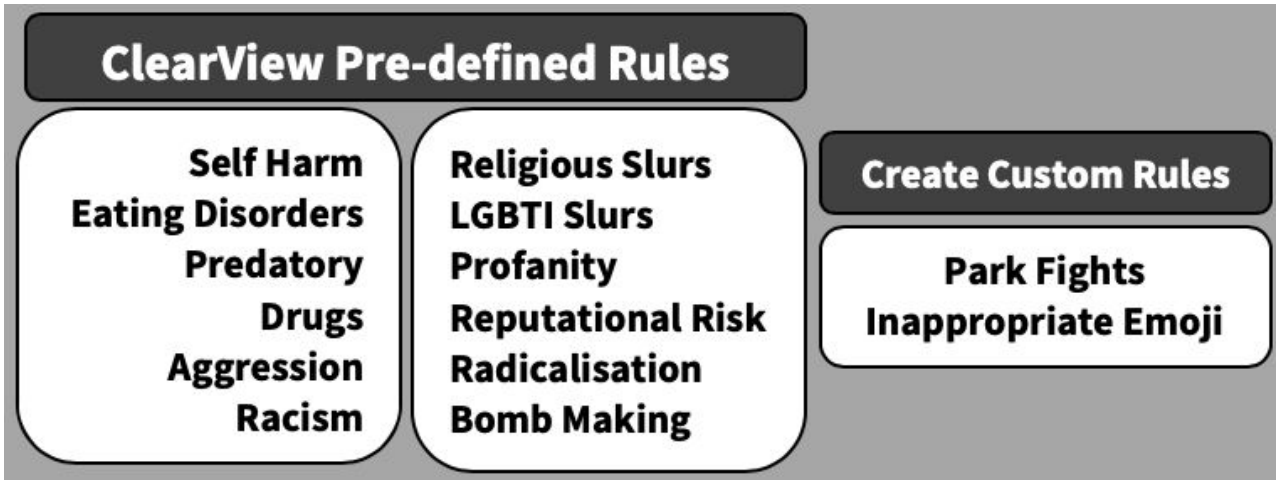
1. RULES

CyberHound ClearView has pre-defined Rules available offering a best practice implementation that can be used immediately to provide benefits. ClearView if fully customisable to create new Rules to capture specific needs of the school. When considering additional Rules, ensure descriptive names for easy identification when Queries and/or reporting are designed.

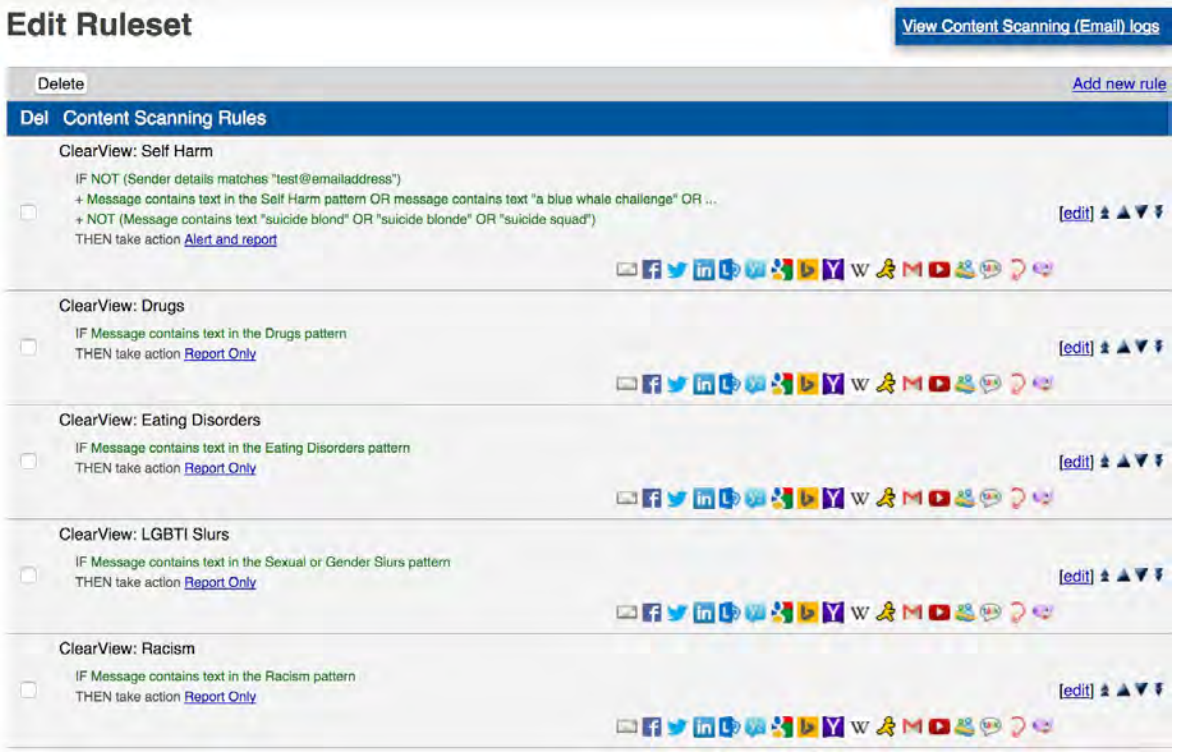
NOTE: The permissions to access and manage the Rules and Actions, are predominantly only assigned to IT System Administrators. Refer Groups & Permissions section for details.

1.1 Pre-Defined Rules

The following lists the default Rules available in ClearView. These Rules have been built on the most popular pattern matching requirements.



Access via: *Content Scanning > Rules*

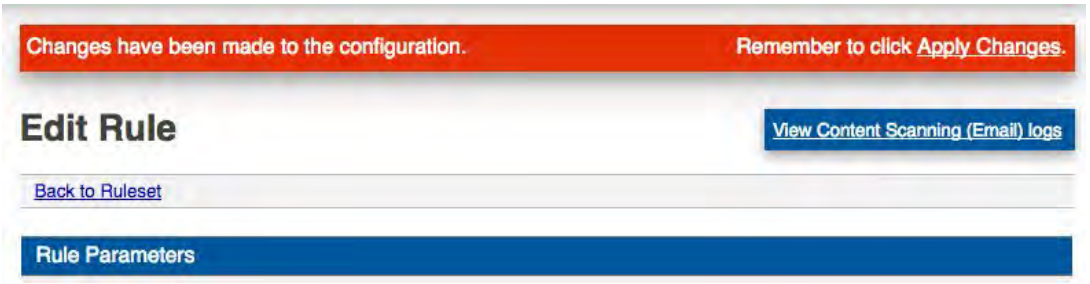


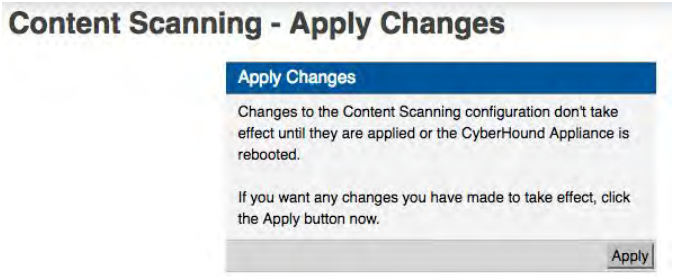
NOTE: Many requests for specific ClearView information is easily obtained by utilising existing Rules and creating a Query to achieve the desired results. Having a well-defined core group of Rules ensures easy maintenance for updates and changes.

1.2 Update & Applying Changes

When changes are made, click on *'Update'* for Rules or Actions, to apply the changes.

A prompt for any changes to the configuration will display and once *'Apply Changes'* is selected, a pop-up window notice will display. After confirming *'Apply'*, a second pop-up window to confirm the configuration is being applied will display.

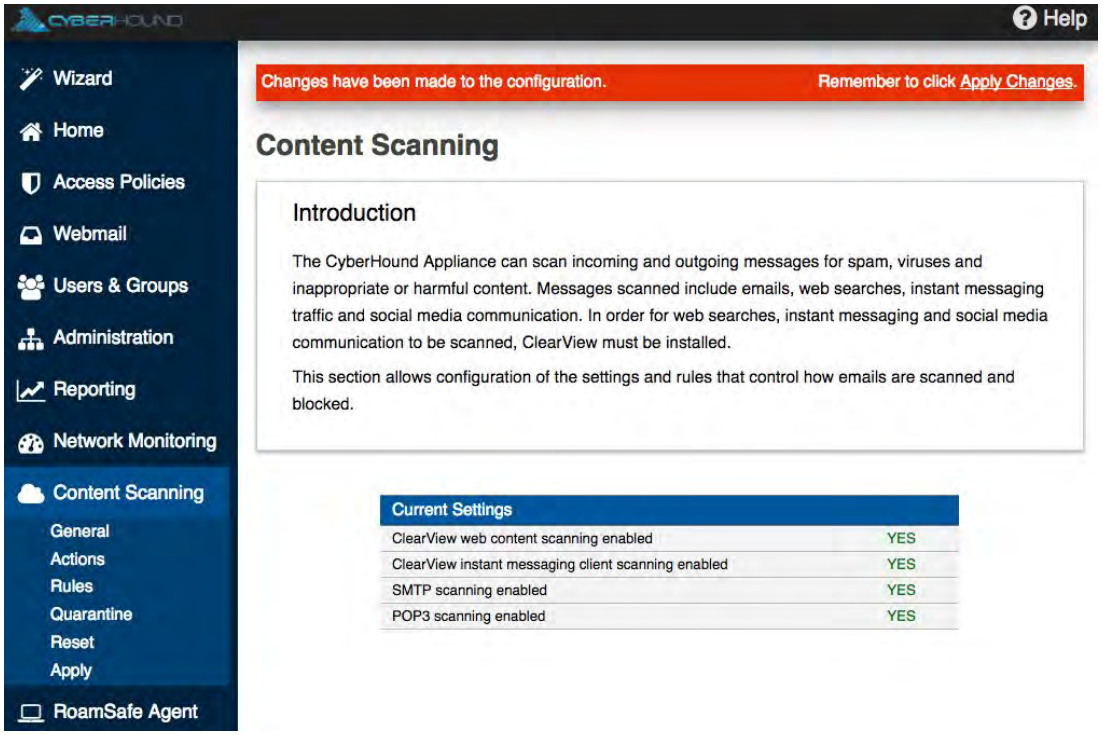




NOTE: If you make changes to an existing rule and DO NOT apply the changes, the changes remain visible but are not activated until *'Apply Changes'* is completed. The rule will perform as per the original settings, before the changes, however the original settings will not be visible.

When the changes have NOT been applied, the prompt to *'Apply Changes'* will be visible each time users log back into the system. The message will display on all pages within Content Scanning until being applied.

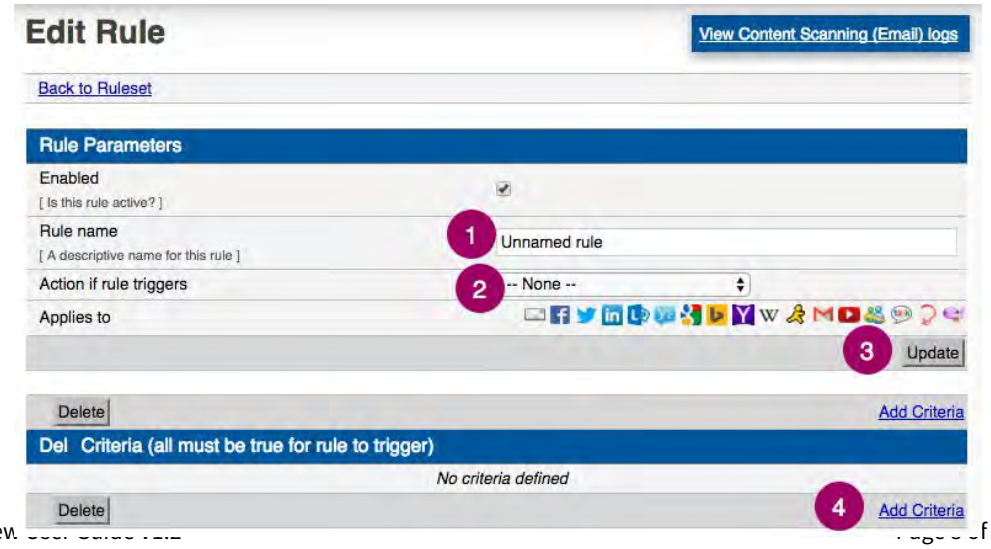
The message does NOT indicate which Rules or Actions have been modified and are waiting to be applied and could apply to several changes if multiple users have modified the system without applying the changes.



1.3 Edit Ruleset – Add or Modify

When there is a need to create a new rule, click on *'Add new rule'* from the Edit Ruleset page (top right) or click on *'[edit]'* for the Rule that requires changes.

1.3.1 Add New Rule

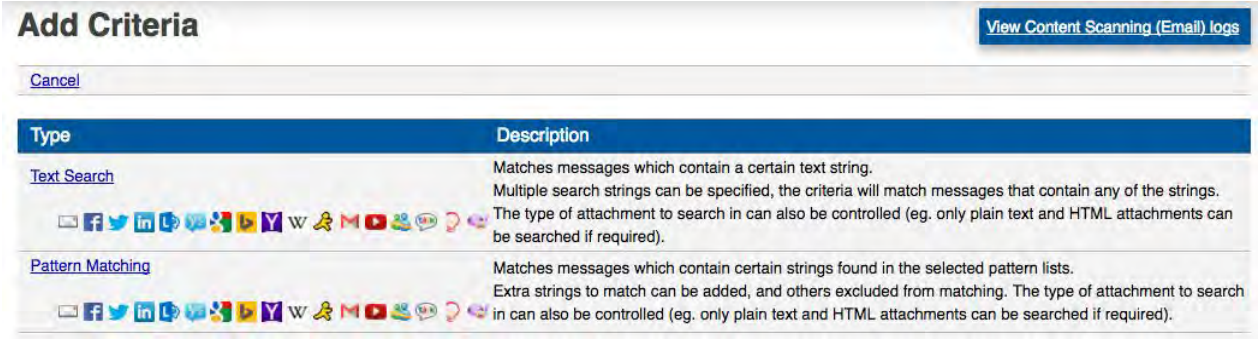


1. **RULE NAME & ENABLE** – Enter a descriptive name in the textbox or modify as required. If creating a new Rule, select the checkbox provided at the top of the page to enable the Rule, once you require it to become active.

2. **ACTION** – select from the drop-down, the action required if the Rule triggers. (Refer Action section for more details)

3. **UPDATE** – Click *'Update'* to create and save a new Rule or modification. **TIP:** If you don't click '*Update*', and choose *'OK'* to the prompt, and proceed, it will NOT save any changes made.

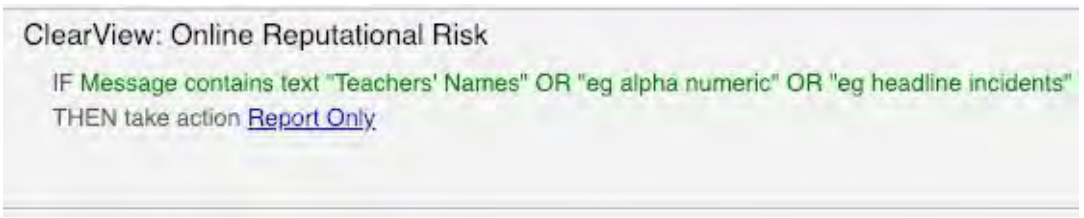
4. **ADD CRITERIA** – Click to open up the list of options for the Rule and select the type that is required. The Rule will be triggered when all of the listed Criteria are matched. If no Criteria are specified then this Rule will never be triggered. (Refer Criteria & Rule Exclusions sections for more detailed information on Criteria)



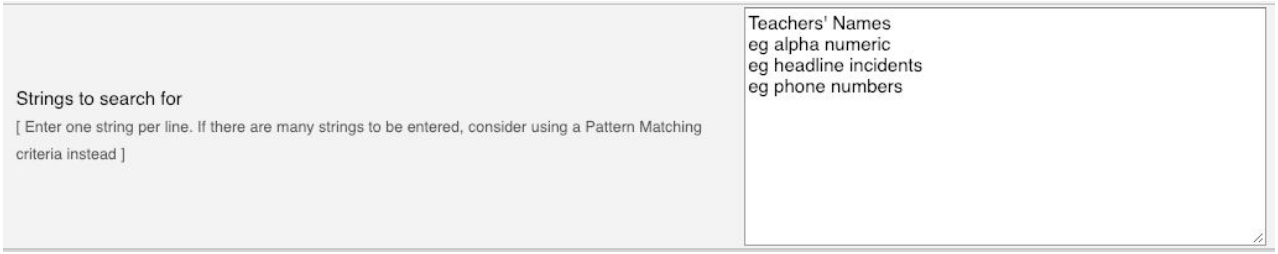
Along with the Rule parameters, the Edit Rule page shows which services and applications apply to the current Rule. This is displayed as a set of icons. Hovering over an icon will show the name of the service or application represented by that icon. The services, which a Rule applies to, are determined based on which Criteria are used in the Rule.

NOTE: There may be need a need to replicate a Rule due to the need for a unique alert Action when the rule is triggered. e.g. A Self Harm Rule could require an alert to go to different people depending on the users that triggered the rule. If the Action requires different alert instructions, then a separate Action is required for each and will need to be applied to separate Rules. e.g. Self Harm – Middle School.

Another Rule that is available is Online Reputational Risk. This provides the opportunity to monitor activity on specific teachers' names, if student have issues with or the school name or a headline grabbing incident, details can be added to monitor.



Each activity needs to be added to a Text Search Criteria *'Strings to search for'* field on a separate line. This Rule could be used and modified to suit situations that may arise and require monitoring at different times. As the text search needs to match exactly, it may require adding a nickname or abbreviated name that may be used.



1.3.2 Modify Rule

You can modify a Rule to add more words or phrases or remove words or phrases that you do not wish to capture. Refer section 1.5 and 1.6 for more details on exclusions and inclusions.

1.3.3 Delete Rule

You can use the *'Delete'* option provided on the *'Edit Ruleset'* page to remove an unwanted Rule.

1. Tick the Rule that is to be deleted.
2. Click the '*Delete*' button.

1.4 Criteria to Trigger Rule

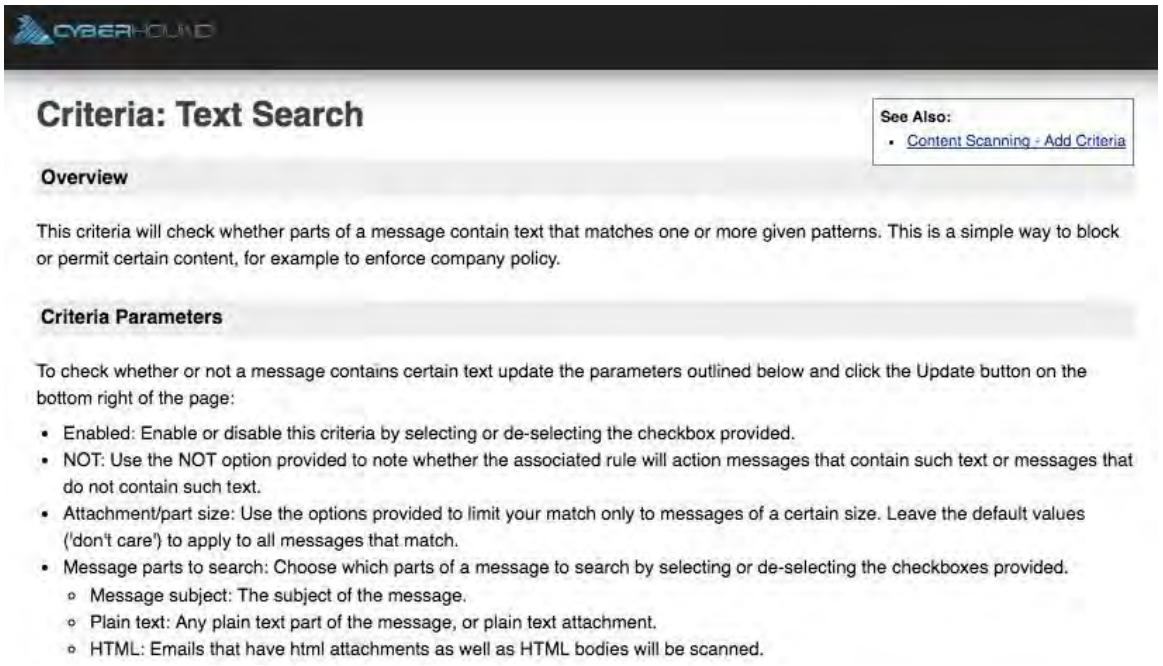
The lower half of the Edit Rule page allows viewing of the Criteria that are currently part of this Rule (if any), with options to add, modify, and delete Criteria. All of the listed Criteria must be met in order for the Rule to be triggered.

Many different types of Criteria exist and different types of Criteria may be used in the one Rule. This allows for complex match conditions to be configured. The list of Criteria available is displayed with a description for each and the applications which apply.

The following image provides details and description, on some of the Criteria commonly used for ClearView.

Text Search	Matches messages which contain a certain text string. Multiple search strings can be specified, the criteria will match messages that contain any of the strings. The type of attachment to search in can also be controlled (eg. only plain text and HTML attachments can be searched if required).
Pattern Matching	Matches messages which contain certain strings found in the selected pattern lists. Extra strings to match can be added, and others excluded from matching. The type of attachment to search in can also be controlled (eg. only plain text and HTML attachments can be searched if required).
Time of Day	Matches messages only during a particular time of day and/or on particular days of the week. This applies to the user's local time, not the time the message was sent or received. This is useful for restricting access to particular services to only during a particular time of day (eg. only accessing social media during lunchtimes and weekends). Only relevant to ClearView, does not apply to emails via SMTP or POP3
Group Match	Matches messages against the user's group. Only relevant to ClearView, does not apply to emails via SMTP or POP3.
Match All	Matches all messages (always true). Redundant if used with other criteria in the same rule.
Service Type	Match a specific service such as "Instant Messaging" or "Webmail". Only relevant to ClearView, does not apply to emails via SMTP or POP3.
Application Type	Match an internet application by name, such as 'Facebook' or 'Gmail', useful for applying a rule only to a specific service understood by ClearView.
Action Type	Match a particular action performed on a ClearView scanned service, such as 'Sending a status update'.

NEED MORE HELP? The CyberHound Appliance **Help**, located top right, can provide detailed technical assistance and examples for each of the Criteria and the parameters. The brief example provided below is for Text Search refer to **Help** for the full details. It is important to note that the parameters for each of Criteria are different.



Criteria: Text Search

See Also:
- Content Scanning - Add Criteria

Overview

This criteria will check whether parts of a message contain text that matches one or more given patterns. This is a simple way to block or permit certain content, for example to enforce company policy.

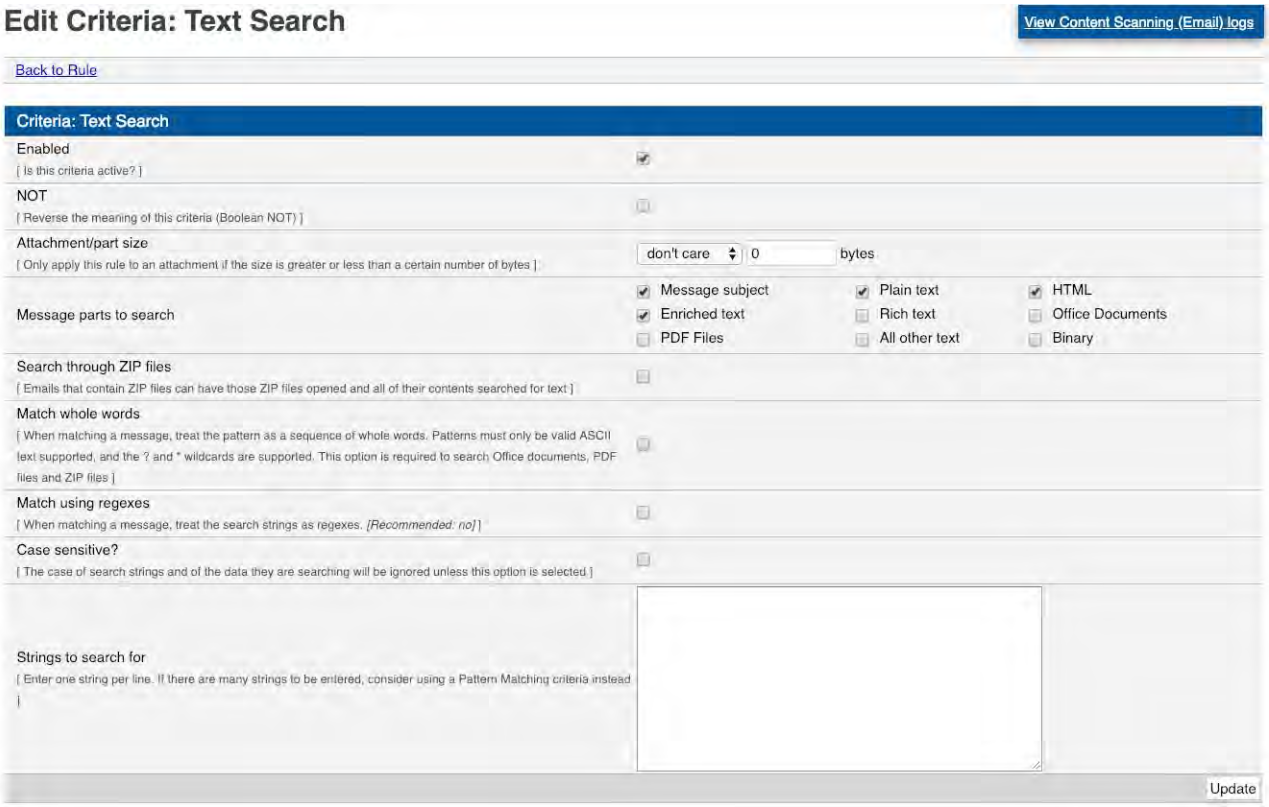
Criteria Parameters

To check whether or not a message contains certain text update the parameters outlined below and click the Update button on the bottom right of the page:

- Enabled: Enable or disable this criteria by selecting or de-selecting the checkbox provided.
- NOT: Use the NOT option provided to note whether the associated rule will action messages that contain such text or messages that do not contain such text.
- Attachment/part size: Use the options provided to limit your match only to messages of a certain size. Leave the default values ('don't care') to apply to all messages that match.
- Message parts to search: Choose which parts of a message to search by selecting or de-selecting the checkboxes provided.
  - Message subject: The subject of the message.
  - Plain text: Any plain text part of the message, or plain text attachment.
  - HTML: Emails that have html attachments as well as HTML bodies will be scanned.

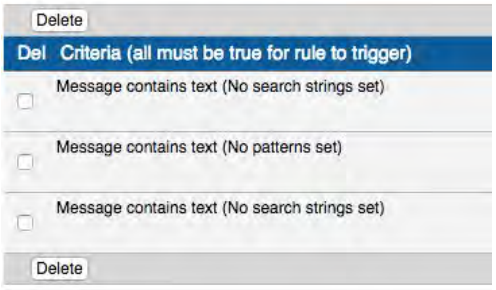
1.4.1 Edit Criteria

When you add or edit a Criteria, the *'Edit Criteria'* page will open to complete the parameters that apply for the Criteria. Parameters will be different for each Criteria except for the first two rows being Enabled (ticked is default) and NOT which is used for exclusions. (Refer to Rules Exclusions section)



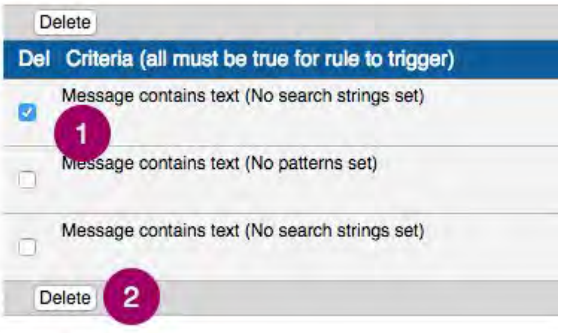
If you click on any Criteria and open the *'Edit Criteria:'* page, then the Criteria will be added to the current Rule even if you do not click the *'Update'* button. It will display, on both the Edit Rule and Ruleset pages, as part of the Rule and state in brackets that it not being used e.g. *'(No search strings set)'* as demonstrated in the images below.

Click on *'Back to Rule'* top left to return to the Edit Rule page.



1.4.2 Delete Criteria

You can use the *'Delete'* option to remove unwanted Criteria within the *'Edit Rule'* page.



1. Tick the Criteria that needs to be deleted.
2. Click the *'Delete'* button. It will remove the selected Criteria without the need to select *'Update'*. Simply click *'Back to Ruleset'* to return.

1.5 Rule Exclusions – Remove False Positives

It is worth reviewing the reports to check for any potential false positives that are being captured. By doing this regularly, and adding exclusions to the pattern matching (see below), it ensures the ongoing reporting accuracy and value. It is extremely simple to exclude words or phrases by adding an exclusion to remove any potential false positive results, logic that **will not** trigger the Rule. For example a student searching for the movie 'Suicide Squad' would trigger the Self-Harm Rule if an exclusion was not in place.

It is necessary to consider what popular expressions, language or trends may affect results and should be excluded in the Rules. As trends change, more words can be added to the existing exclusion.

As most users will not have access to the Rules to add exclusions to remove false positives, users could add exclusions to their Queries for refining the data results for an immediate solution. (Refer to Queries Exclusions) As there can be multiple Queries for different groups and users, it is best practice to apply exclusions to a Rule so irrelevant data is not captured and is not presented in any Query or report.

Users should advise the IT System Administrators that exclusions need to be applied to a Rule when they discover trends that are unnecessary in the results and will affect all users.

1.5.1 Steps to Exclude

Access the relevant Rule. In this example, to exclude 'Suicide Squad', it will be the Self Harm Rule.

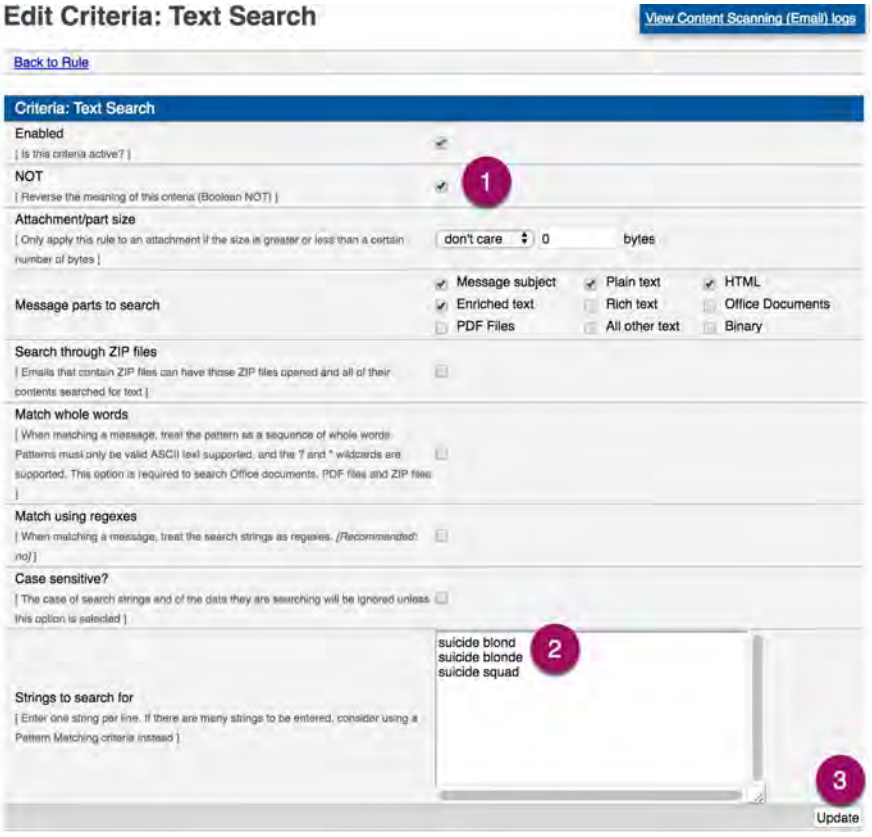
Click *'Add Criteria'* and choose the *'Text Search Criteria'* option.

1. Tick *'NOT'* to search for the string.

2. Type *'suicide squad'* in *'Strings to search for'* text field. More strings can be added to the text search Criteria as needed.

TIP: add all variations that could be used. e.g. two words or one word or blond with and without 'e' as shown.

3. Click *'Update'* and apply the changes. Click on '*Back to Rule*' to return to the Rules set and remember to *'Apply Changes'* to implement the changes.

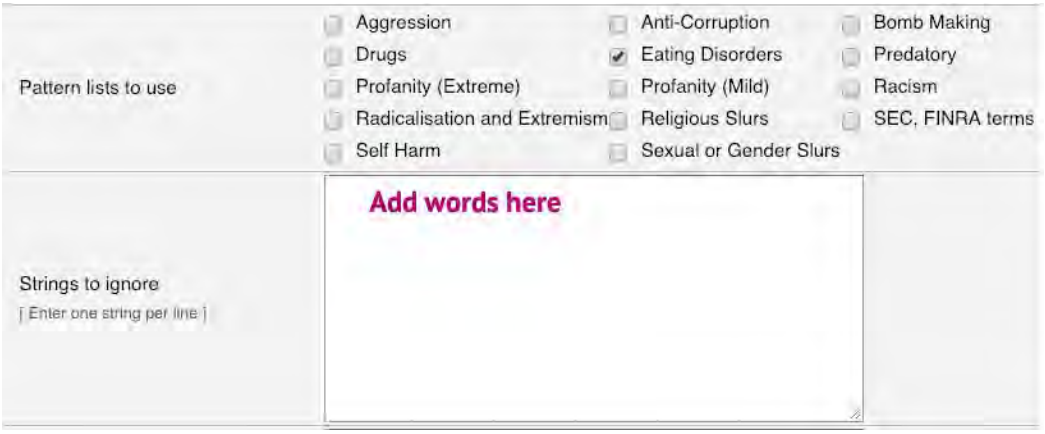


The Ruleset list will now show the new configuration.

NOTE: Changes to a rule only apply from the date the change is implemented. Any data captured preceding the change, would still report 'suicide squad' in Queries or reports on timeframes prior to the change date.

1.5.2 Exclude pattern words

On rare occasions, there may be a need to exclude a word that is in the predefined pattern list. Edit the pattern list and add the word or words you do not want to capture. This field only ignores words that are in the 'Pattern lists to use' as selected in the field above.



1.6 Inclusions - Add Strings to Rule

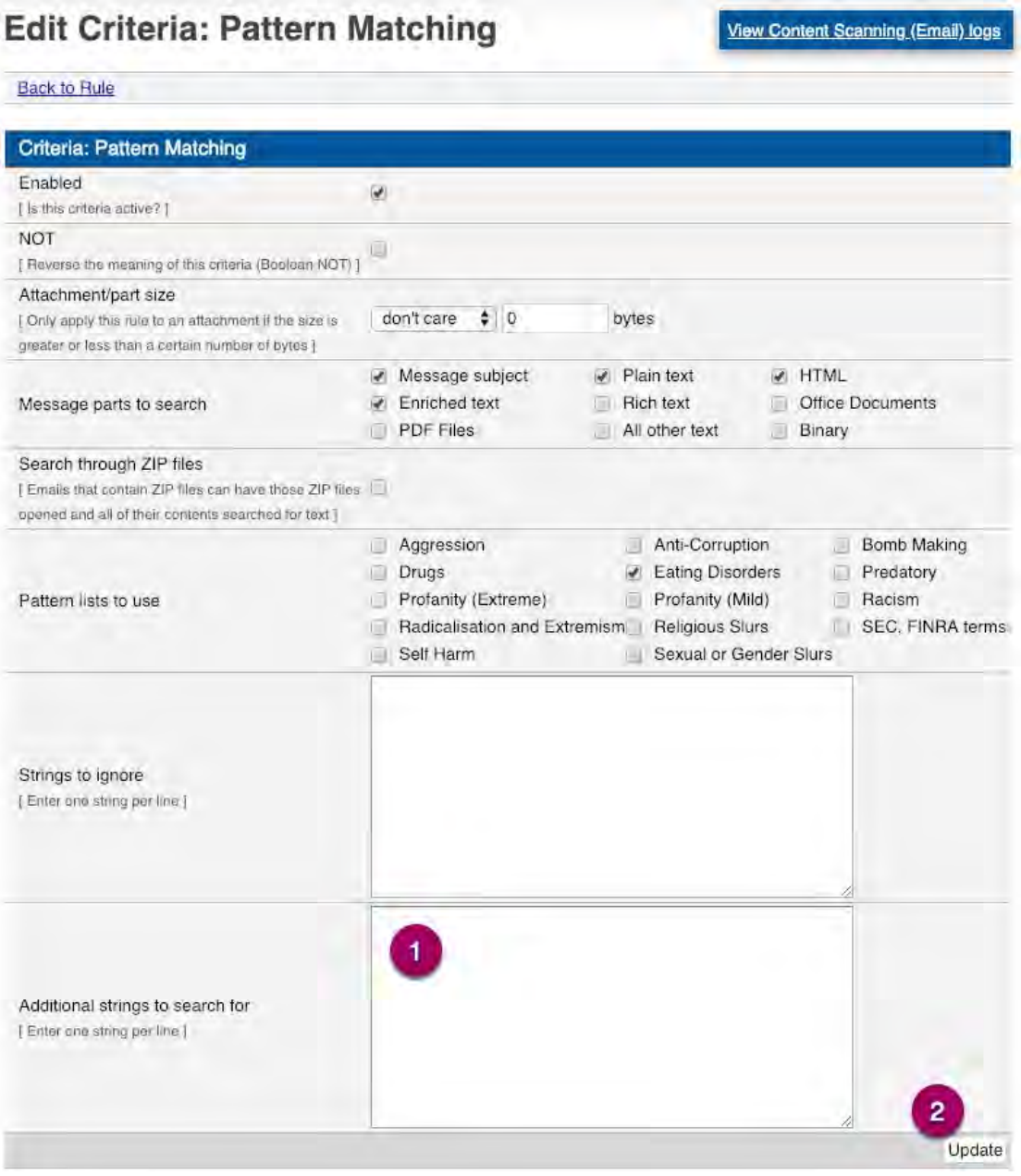
While it is important to remove unwanted results, there may also be a need to capture new popular expressions or words, or words that cause concern, which do require monitoring. Adding specific words or strings to the Pattern Matching Criteria for the relevant Rule or Rules, will ensure that important trends or concerns can be captured for reporting.

Some examples that provide welfare and support staff with evidence-based triggers are:

Fights - organised in a nearby park can be monitored easily by adding the name of the park to the Aggression Rule.
Drugs – new slang or street names can be added to the Drugs or Self Harm Rules.
Reputational Risk – school, teachers' names or nicknames can be added to an 'Online Reputational Risk' Rule to capture inappropriate comments.

Select the relevant Rule and click *'[edit]'*. Select the pattern Criteria for the Rule and click *'[edit]'*.

1. Type in the word or phrases in the *'Additional strings to search for'* field. Enter one word or phrases per line.
2. Click *'Update'* to add the string. Click on '*Back to Rule*' to return to the Ruleset and remember to *'Apply Changes'* to implement the changes.

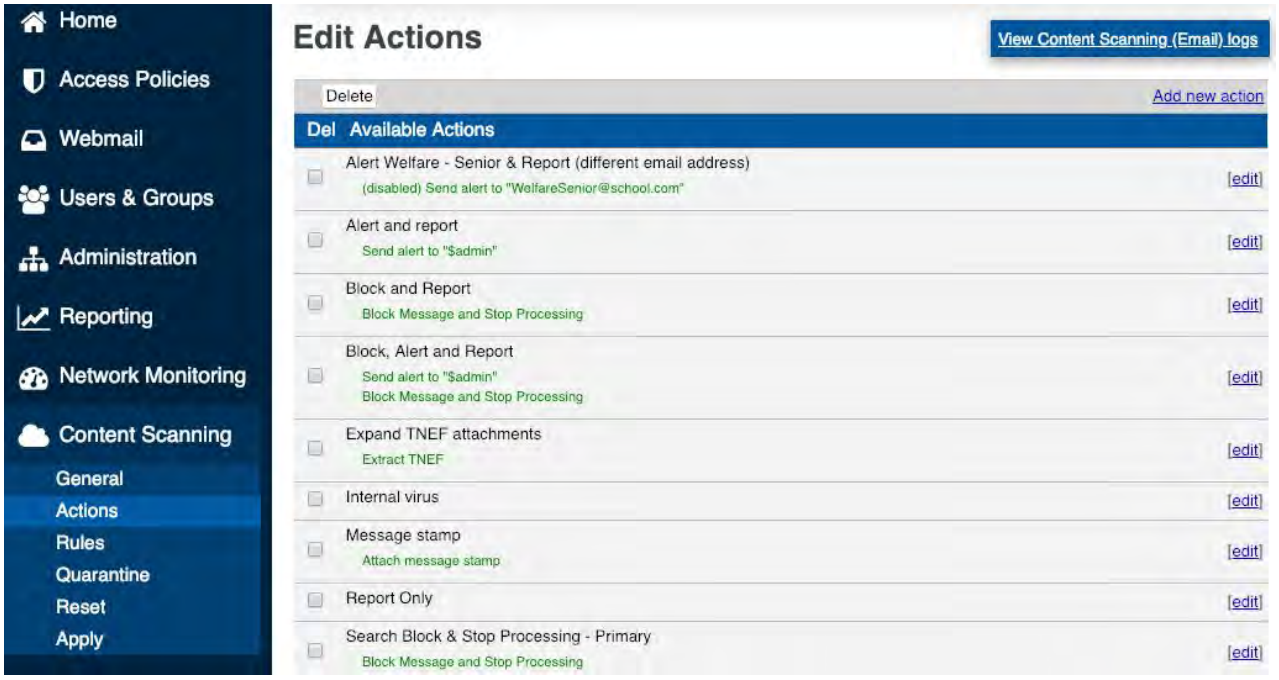


NOTE: Query searches for additional words or strings cannot be achieved as the results have not been captured in the data source until a Rule recognises the pattern matched.

2. RULE ACTIONS

Actions determine what needs to happen when the Rule is triggered. There can be more than one action executed when the Rule is triggered. When an action is invoked, the Sub-Actions are applied in order from top to bottom.

Access via: *Content Scanning > Actions*



2.1 Default Actions

The following are named Actions that typically apply to ClearView Events and are available.

- **Alert and report** – Online activity is **NOT** interrupted and triggers an immediate email to the nominated person/s.
    - Suggested Use: when you need to have instant visibility to any activity to assist with solutions and actions e.g. A custom rule for fights in the park as the activity maybe later today and you need to know as soon as possible.

- **Report Only** - Online activity is **NOT** interrupted and details are captured in ClearView data source.
    - Most commonly used Action as the data captured is provided in scheduled reports for review at convenient times.

- **Block and report** - Online activity **IS** interrupted and details are captured in ClearView data source.
    - Suggested Use: when the search is deemed inappropriate and individuals' online conduct should be halted immediately e.g. Extreme Profanity could be a Rule, which may warrant a block.

- **Block and alert** - Online activity **IS** interrupted and triggers immediate email to nominated person/s.
    - Not commonly used unless it is deemed imperative that inappropriate online activity requires immediate attention. Could be used short term for addressing new threats or emergence of concerning patterns requiring immediate attention.

2.1.1 Blocked Message – Stop Processing

Blocked content and/or messages are not delivered to the intended recipient(s) with advice that access has been blocked.

CyberHound provides the option to add a custom pop-up message to some Block Actions, promoting digital citizenship awareness and education. When the user is blocked by their online activity, a custom message can be created providing a reason why the block has occurred. Custom block messages can be created for each specific online activity.

2.1.2 Block Messages – When to Use

There is flexibility to apply blocking of online activity to specific groups. Access for the early years may be blocked and not blocked for mature students providing opportunities for educational growth and development of students' online responsibilities.

Using block messages does indicate to network users that the school has policies in place to stop particular online activity. Individuals may then seek other avenues in the future, resulting in no visibility of inappropriate online activity. Consequences of blocking online activity may be loss of early intervention, protection capabilities and missed opportunities for education on responsible online behaviours.

Separate Rules could be created and Block access could be applied accordingly for each cohort e.g. for Junior, Middle and Senior.

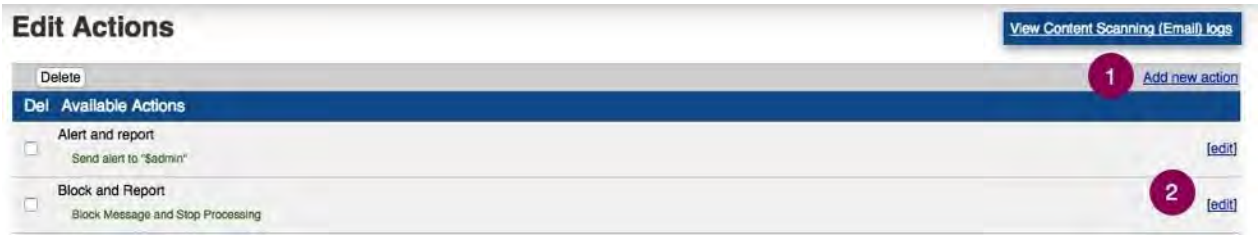
2.2 Add, Modify or Delete an Action

New Actions and modifications to existing Actions can be completed via *'Edit Actions'* page.

A new Action may be created with a combination of the default Sub-Actions e.g. Block and Alert. If a default Action is not suitable to apply to a Rule, then an Action may be created to allow customisation to address specific responses appropriate for the Rule. An example could be:

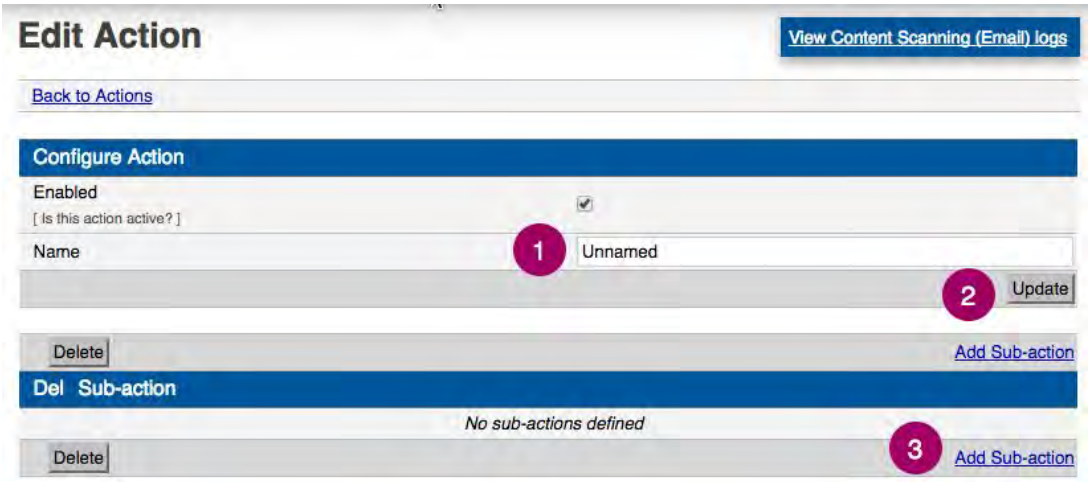
- **Alert and Report - Middle School:** Alert email to the person responsible for the students in this cohort. If the alert needs to go to different people, then a separate Action is required to add each different email and be applied to separate Rules.

TIP: When creating a new Action, name the Action and any Sub-Actions, to make it easy to identify when adding to a specific Rule. Reporting may include the Action taken when the Rule is triggered and it assists report recipients to easily understand what that Action was when it has a descriptive name.



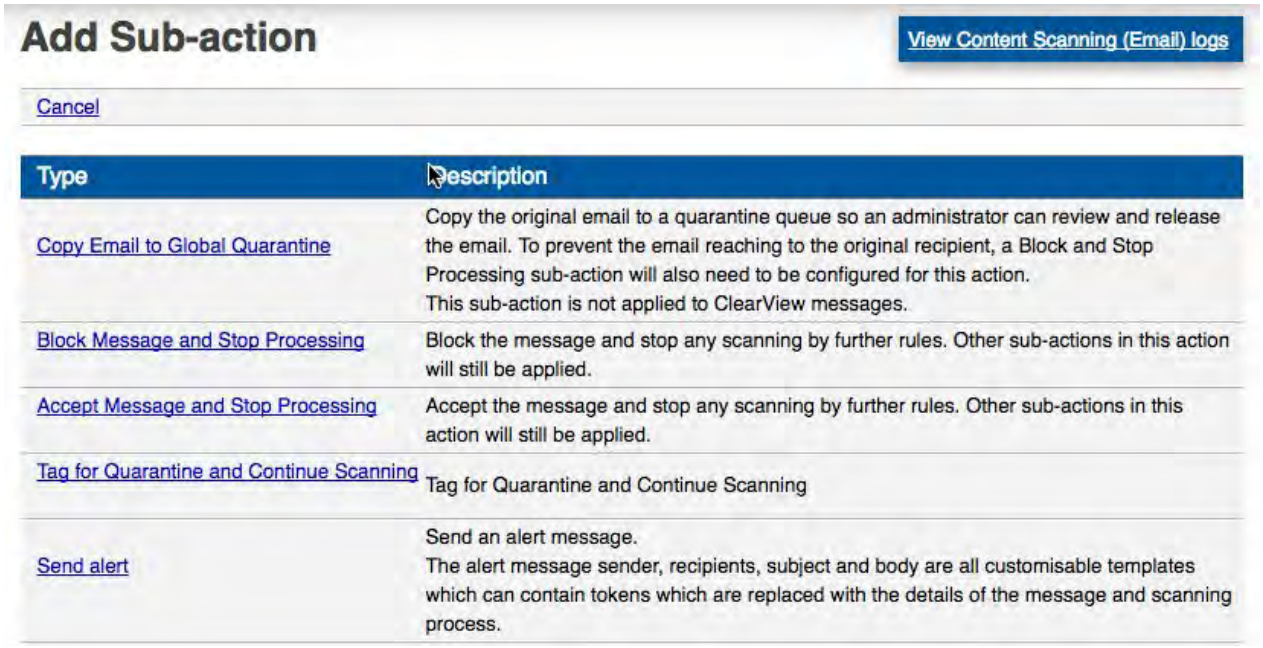
1. To add a new Action to the options available select *'Add new Action'*.
2. To modify an existing Action, select *'[edit]'*.

2.2.1 Add New Action



1. Name the Action with a description to identify the purpose of the Action.
2. Select *'Update'* to save the new Action.
3. Select '*Add Sub-Action'*

The system has built-in Sub-Actions to select from and you can add as many Sub-Actions to achieve the desired outcome when the Rule is triggered.



Depending on the Sub-Action selected, there may be other fields to complete.
For further details on the Sub-Actions, overview and customising, refer to the **Help** within the CyberHound Appliance. The following is a brief example from **Help** of the details for *'Sub-Action: Send Alert'* text fields.

When all the fields have been completed, select *'Update'* and *'Apply Changes'*.

Sub-action: Send Alert

See Also:
- Content Scanning - Add Sub-action

Overview

This sub-action causes an customised alert email to be sent to one or more addresses. A number of substitution tokens exist which may be used in the alert message's body and From, To, and Subject fields. These values used for these tokens when an alert message is sent depend on the message and the rule that was triggered. See below for more information on these tokens.

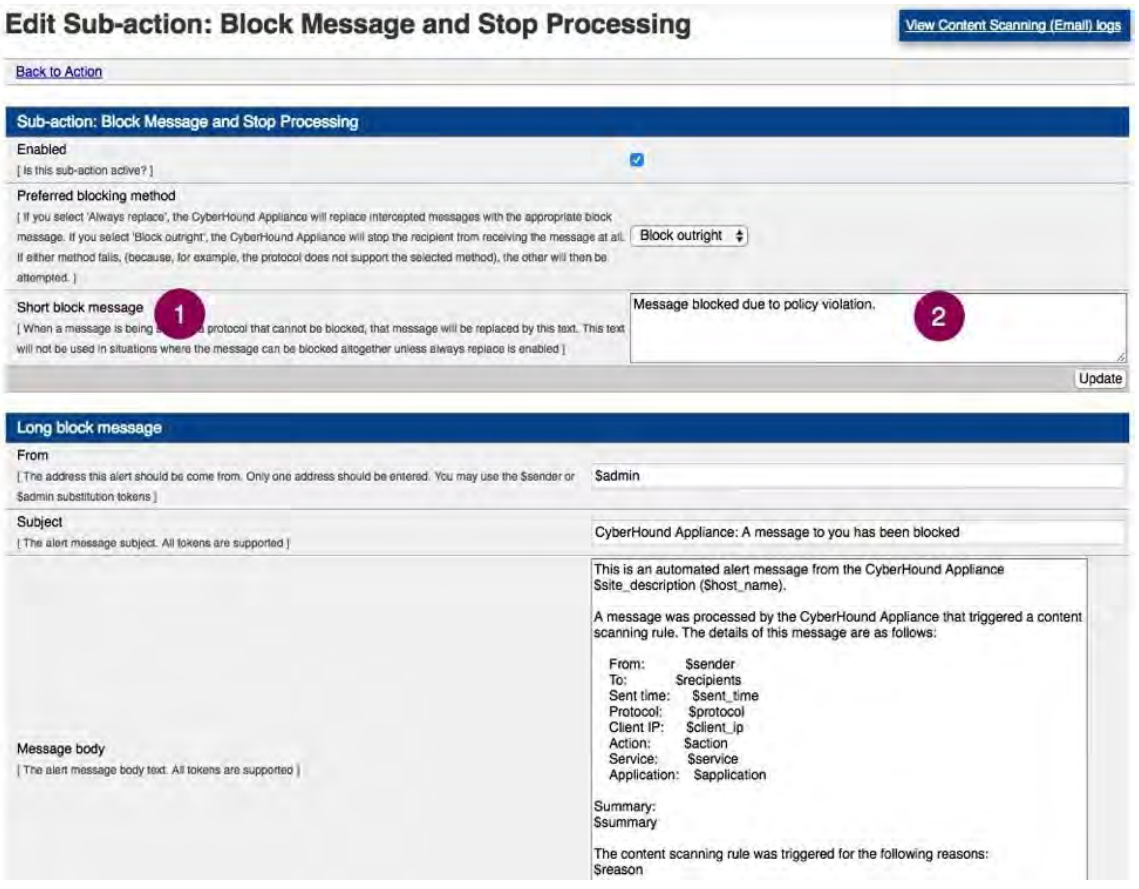
Customising the Alert

The following fields can be used to customise the alert message.

Field	Description
	If this setting is disabled, the alert will not be sent if the triggering email was received via the transparent POP3 proxy.
Send if protocol is POP3?	**Note:** This setting is useful for alerts that are intended for the original recipient of the triggering email. When a message that was received via the transparent POP3 proxy is blocked, the primary POP3 alert is always sent to the recipient (see *Content Scanning > POP3 Alert* in the web interface). In this case it is undesirable for a second alert to be sent to the recipient via SMTP. This setting can be used to prevent a second alert from being sent.
From	The address that the alert message will be addressed from. You can enter a fixed address directly or use the $sender or $admin tokens. Only one address may be entered.
To	The addresses that the alert message will be sent to. You can enter addresses directly and/or use the $recipients, $sender and $admin tokens. You can also use an address such as $username@example.com, which will send the alert to the authenticated user. Multiple addresses can be separated by a space or comma.
Subject	The subject that the alert message should have. You may use any of the available substitution tokens. Be aware that some tokens (such as $reason) may generate a multi-line output which might not look correct when the subject line is displayed in some email software.

2.2.2. Create a Custom Block Message Action

Sub-Actions can be used for multiple Rules and the default block message will apply to all Rules using this Action. When creating a new Action for a Custom Block message, choose the *'Block Message and Stop Processing'* Sub-Action from the list available.

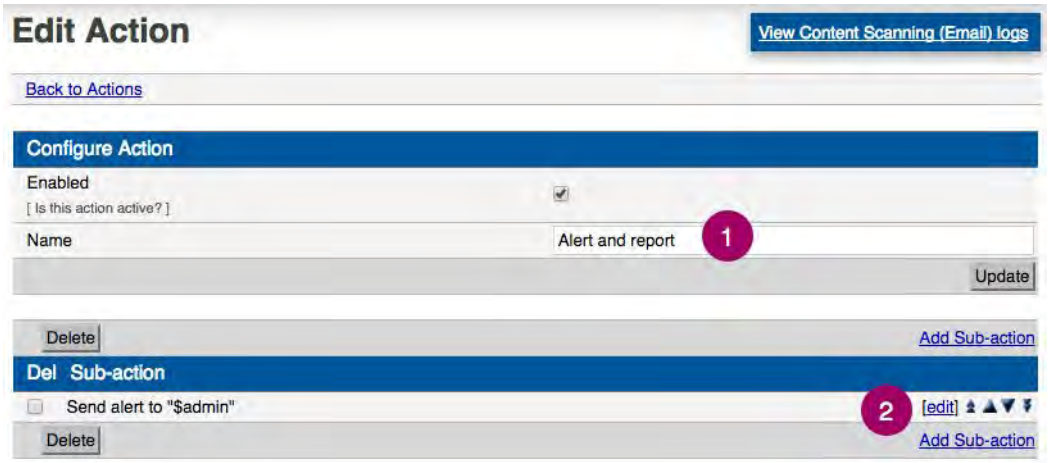


1. The *'Short block message'* allows customisation of the block message.
2. Add the message required for the custom message.

NOTE: Long block message is only applicable for email scanning. Messages blocked by ClearView will always use the *'Short block message'* field to replace blocked content or display a block message to the user.

2.2.3 Modify Action

After selecting *'[edit]'* for the Action requiring changes, the *'Edit Action'* page will display.



1. **Change name** – you can modify the description for the Action. Any Rule that has this Action applied will also be updated to reflect the new name.
2. **Edit Sub-Action** – option to change the parameters of the Sub-Action by clicking on *'[edit]'* or move the order of the Sub-Action up or down by using the arrows.

2.2.4 Delete Actions & Sub-Actions

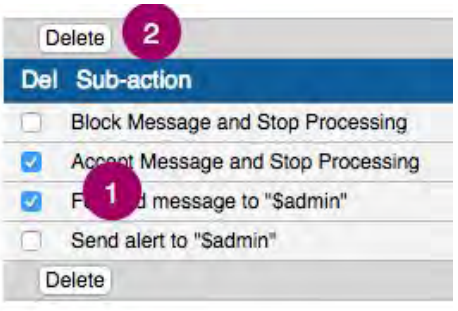
If an Action is no longer relevant, it can be deleted altogether or individual Sub-Actions within the Action can be removed.

To delete an Action:

1. Tick the box beside the relevant Action.
2. Click on *'Delete'*.

To delete a Sub-Action, edit the relevant Action:

1. Tick the box beside the relevant Sub-Action.
2. Click on *'Delete'*.



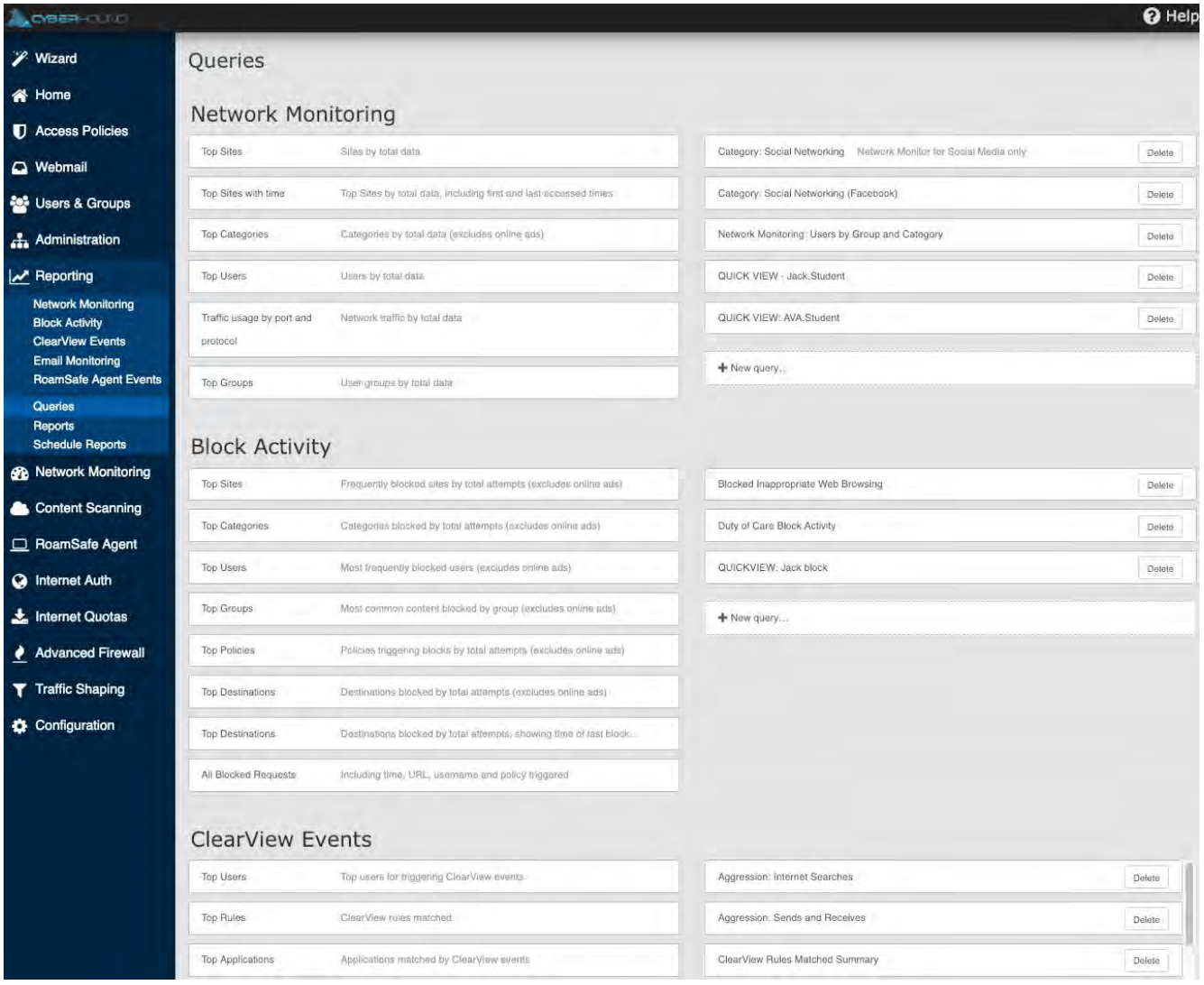
3. QUERIES

Queries allow refinement of the data to produce specific and relevant information. Queries can be used in real-time, for any time period, for specific details that need to be addressed or investigated e.g. an individual's behaviour or concerning patterns that have just occurred. Commonly used Queries can be saved to view again and saved Queries are used for building reports. Most organisations rely on reviewing data via scheduled reports at pre-arranged times.

Accessed via: *Reporting > Queries.*

Selecting Queries on the navigation side bar opens the full list of data source Queries. Simply scroll down to view the ClearView defaults and custom Query options if your permissions have provided more data sources.

NOTE: Depending on your access permissions, you may only see ClearView Events. The following example is a full access view for a System Administrator.

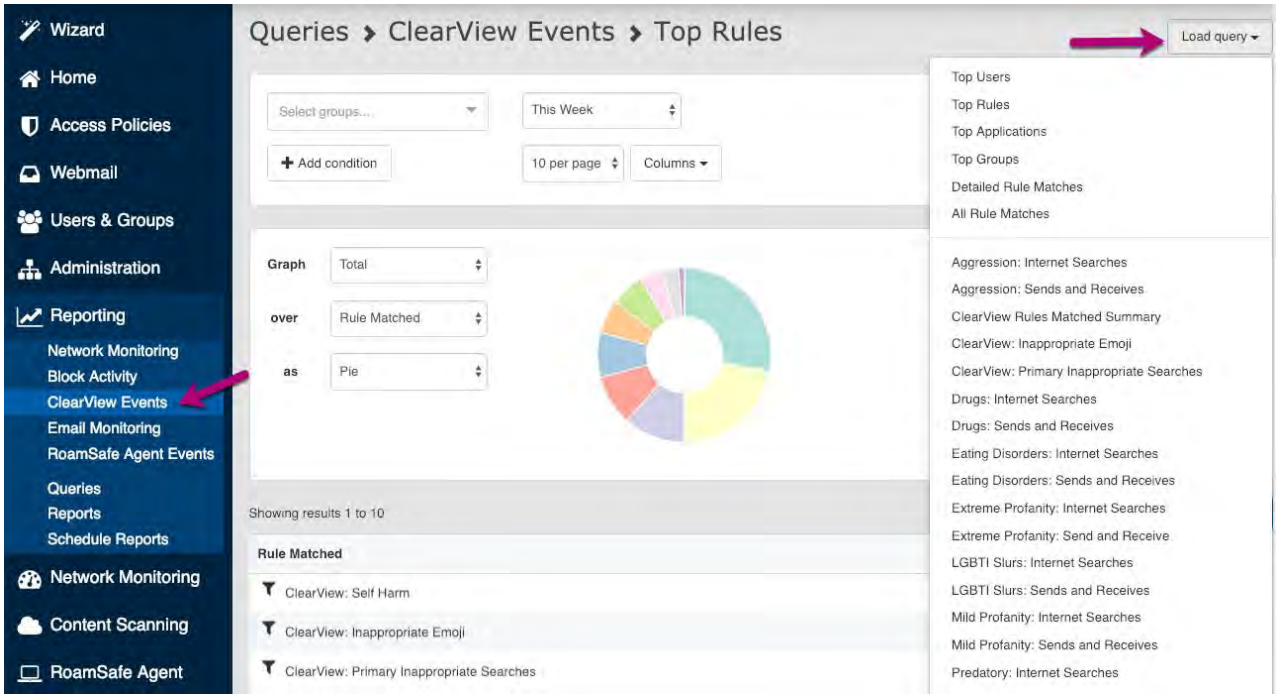


3.1 Default & Custom Queries

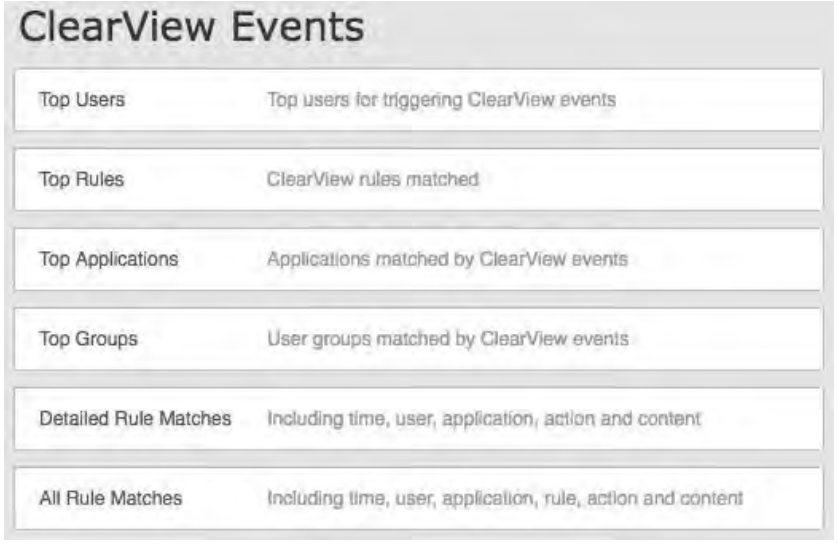
CyberHound provides default Queries for review of the most commonly scrutinized patterns. Results are displayed on screen in graphical and textual formats depending on the selections. It's easy to use an existing Query and modify the parameters to suit new user enquiries and save as a new custom Query for next time. The option is also available to build a Query from scratch.

Default Queries cannot be deleted, however they can be modified and saved as a custom Query if required.

Selecting *'ClearView Events'* from the navigation sidebar will load a default Query with the option to select and view other Queries from the *'Load Query'* drop-down list available on the top right of page. The drop-down list will display the other default Queries available and custom Queries (if any) will be displayed below the line in the list. Navigating to other Queries is quick and easy from within the one page.



Default Rules for ClearView



3.1.1 Query Panels – Conditions, Graph & Results

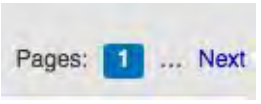
The Query page is broken up into three panels.

Query condition panel - The top panel of the view contains controls that allow modification of the Query itself.

Graph panel - Most Queries are configured to display their results in a graph. The exceptions are Queries that produce lists of individual events that do not make sense to show in a graph.
If a Query has at least one column that is meaningful to display in a graph, the middle panel of the Query view will display a graph with associated controls to select the:

- Column(s) to be graphed (y-axis)
- Column to graph over (x-axis)
- Graph type (Pie, Bar or Time Graph)

Results table panel - The bottom panel is a table with the Query results. When there are more results than can be displayed on one page, a pagination control is active on the right hand side. Clicking on '*Next*' will get the next set of results from the data source.



Results Panel is your Report View

The Query results panel is reflected in the reports that are distributed daily, weekly etc. The more 'conditions' that are added and saved, makes the report more meaningful and provides the opportunity to determine actions required. A more informative report saves time by not needing to log into the CyberHound Appliance to access the query to modify and gain context of the event activity. Defining what conditions need to be displayed in the Query that flow into reports, makes analysis much easier. IT System Administrators can save Queries that meets the needs of a report recipient and update the reports.

Example of Query results displaying only 2 conditions. This view of the results panel does not provide context to understand the users activity, it would be necessary to modify and add conditions to view more details.

Showing results 1 to 5

Username	Total
ava.student	10
jack.student	9
lucas.student	6
sophia.student	1
jessica.teacher	1

Example of the same Query with more conditions added. If results with additional conditions were displayed in a report, decisions on actions that may be required are more obvious. e.g. Ava was searching on the movie Suicide Squad whereas the results displaying for Jack could raise concern and warrant further investigation.

Showing results 1 to 5 Pages: 1 ... Next

Username	Full Name	Application	User Action	Body	Total
ava.student	Ava.student	Google	Search	[more] suicide squad cha...	1
jack.student	Jack.student	Google	Search	[more] pills you can ove...	1
jack.student	Jack.student	Google	Search	[more] pills you can ove...	1
ava.student	Ava.student	Google	Search	[more] suicide squad	1
ava.student	Ava.student	Google	Search	[more] suicide squad	1

3.2

Each panel of the Query can be easily modified to view the data results in different configurations by adding or removing data for finer analysis.

3.2.1 Modify Condition Panel

1. SELECT GROUPS - with the option to add more than one from the groups available in the drop-down. If no selection is made, then results will return all user groups' activity. Selecting a group provides focused results relevant for the user. Groups are defined in the CyberHound Appliance as part of the initial set up and are maintained by an IT System Administrator.

2. CHANGING THE TIME FRAME – options to refine data to specific periods. Options available from Last hour, today, last 24 hours yesterday, this week, last week, last 7 days, this month, last 30 days, last month, this quarter, last quarter and all of time. There is also an *'Other'* option where specific details can be entered e.g. need data on what a user actions for a specific period.

3. MODIFY OR ADD CONDITIONS - Click *'+Add condition'* to add data or modify the existing condition to meet requirements. You can add as many conditions as you need to tailor your results to capture specific and relevant details. (See below for further details on each parameter for Condition options).

4. RESULTS PER PAGE - Add more results to the page by selecting the options from the drop-down menu. Options from 5 to 500 per page are available.

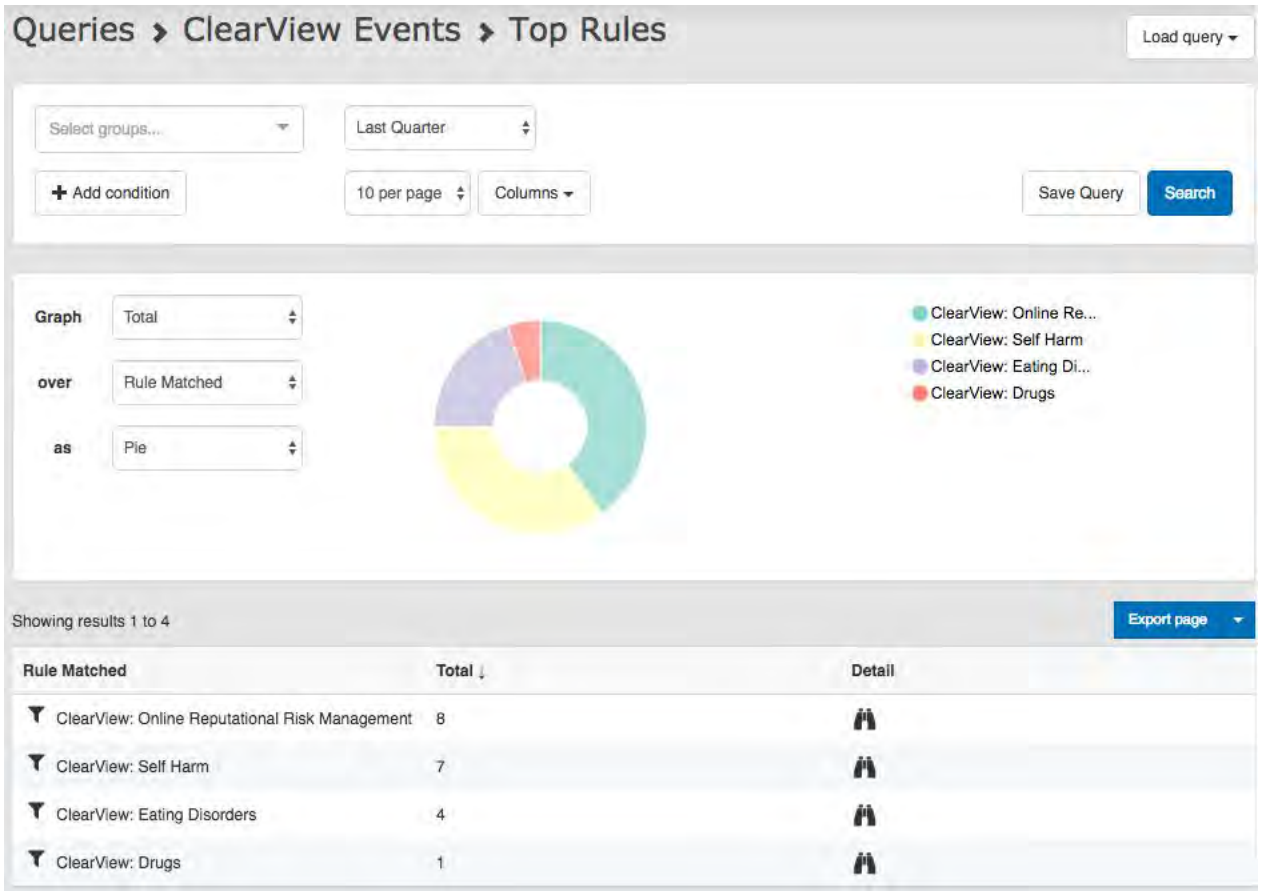
5. COLUMN DATA - Tick or untick the options to modify the data results and the results displayed. This is the easiest way to add more data to the results panel.

6. SEARCH & SAVE - When the selections have been made to the parameters, click *'Search'* and the graph and results will be updated to reflect the new selections. If required, *'Save Query'* or *'Save As' the* Query for future use or to add to a report. Access Permissions control the ability to save Queries. (Refer Saving Queries section for more detail).

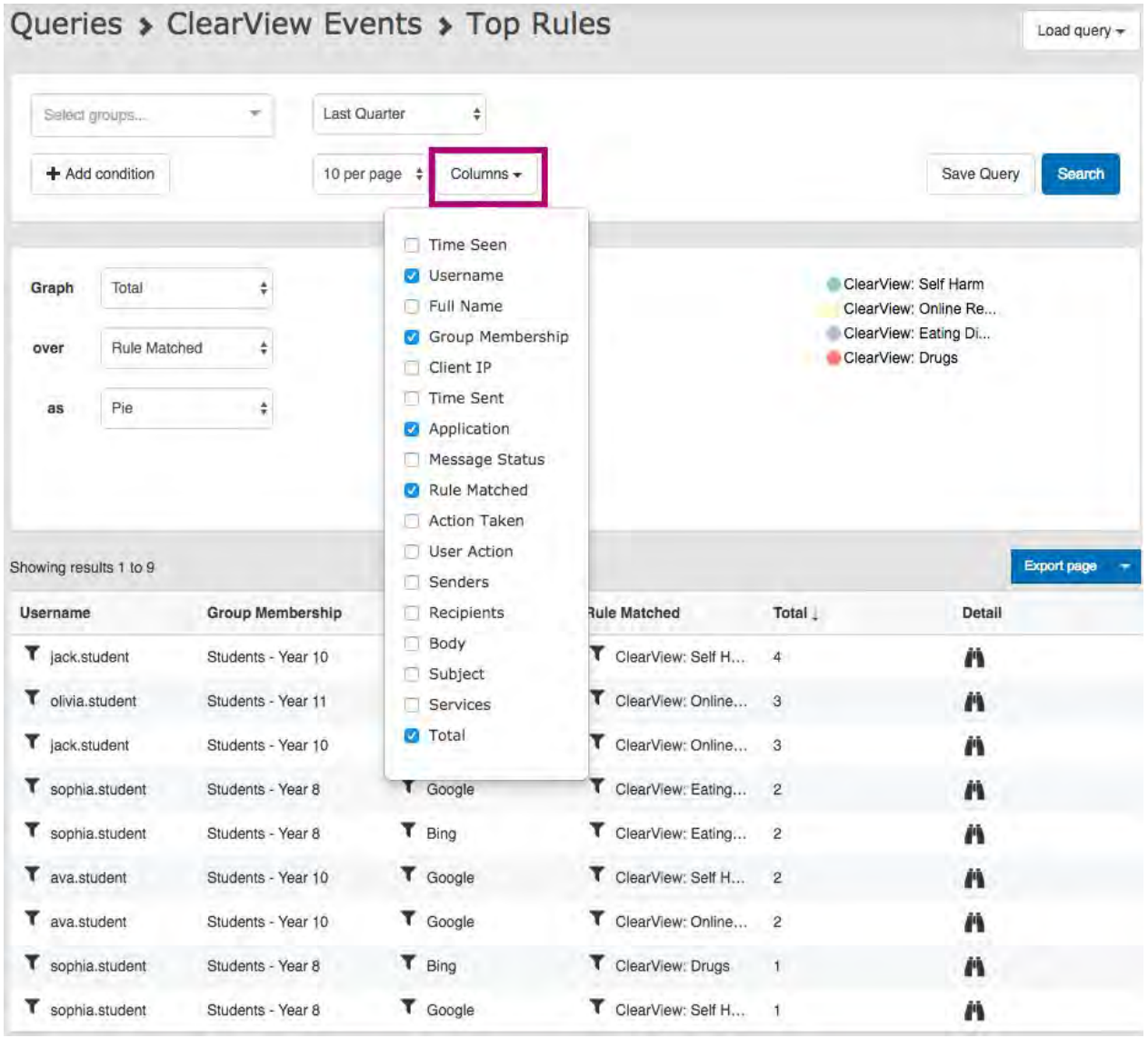
TIP: Clicking *'Search'* as you add each condition may help determine the need for more or less refinement of the Query.

Display more Results - Before and After Views

BEFORE - The following image demonstrates the Top Rules default Query before changing any conditions. The default displays the Rules that have been triggered by the Rule name and a total.



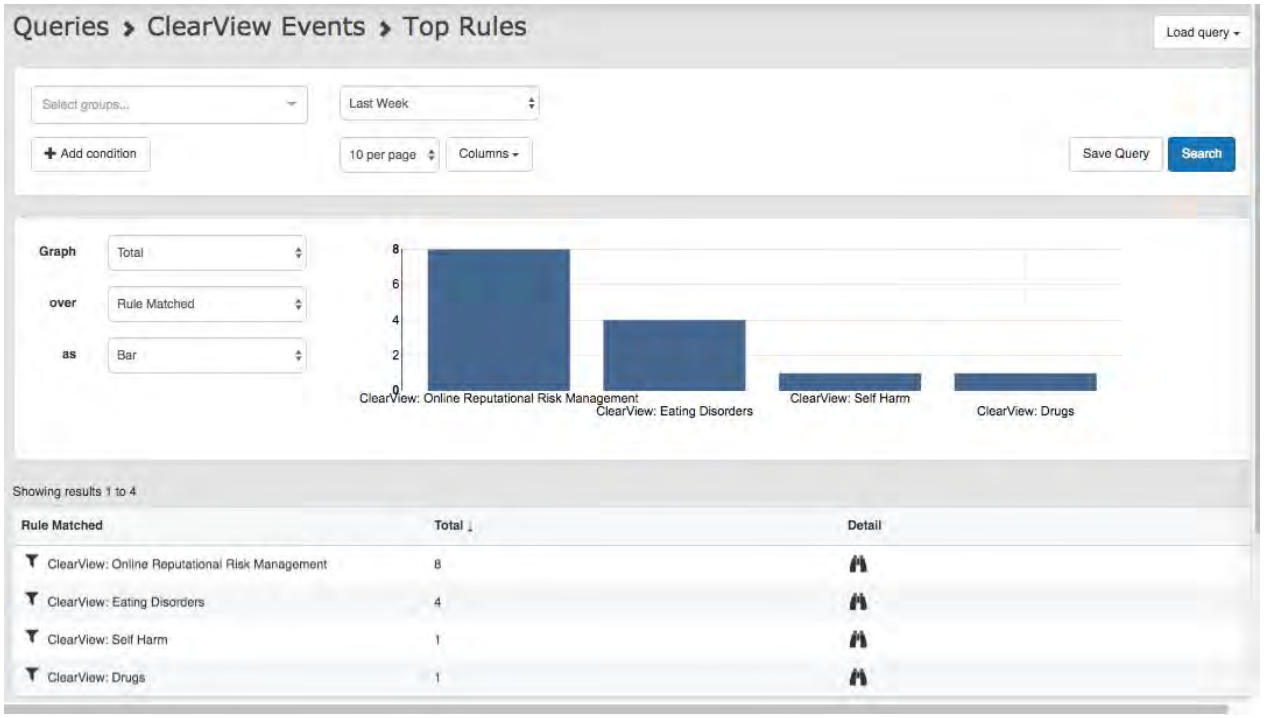
AFTER - Using the same time period, simply tick additional conditions in the column drop-down list, then click '*Search*'. Results panel now displays more information.



Modify or Add Conditions

The *'Conditions'* row is in three parts with the first selection determining the second and third options of drop-down or pre-defined fields. The third selection may also have a free text field option, again dependant on the first selection field.

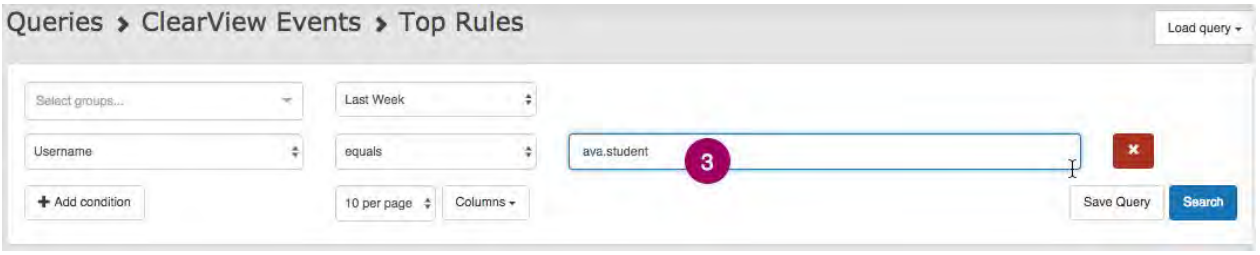
The following image displays the results of the default Query *'Top Rules'*, for last week before adding a Condition.



1. **1st SELECTION –** Drop-down list of choices to build your report or modify existing to refine details. (Refer section Condition Definitions for explanation of each option)

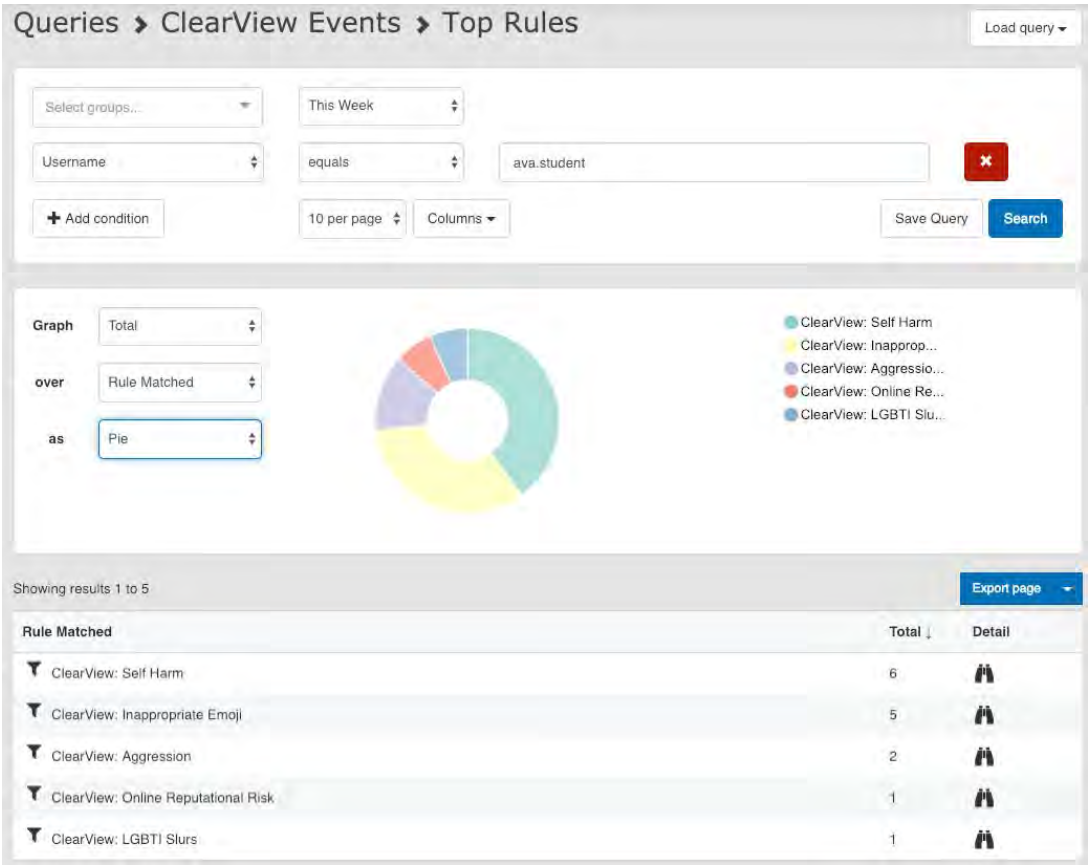
2. **2nd SELECTION** – Drop-down list of choices to refine the Query. Drop-down options will change depending on the 1st Selection.

(**NOTE:** The Doesn't option can be used for Exclusions – Refer to Query Exclusions section.)



3. **3rd SELECTION** – enter the details that refine the first two selections e.g. As the example above demonstrates the 1st selection was *'Username'*, the 2nd selection was *'equals'* and the 3rd selection is a free text field. When the 3rd field is a free text field, and the 2nd selection is '*equals*' for the result to be recognised, the text must match exactly the naming convention as defined in the system. If the 2nd selection was *'begins with'* or *'ends with'* then a partial name could be entered and would return more results.

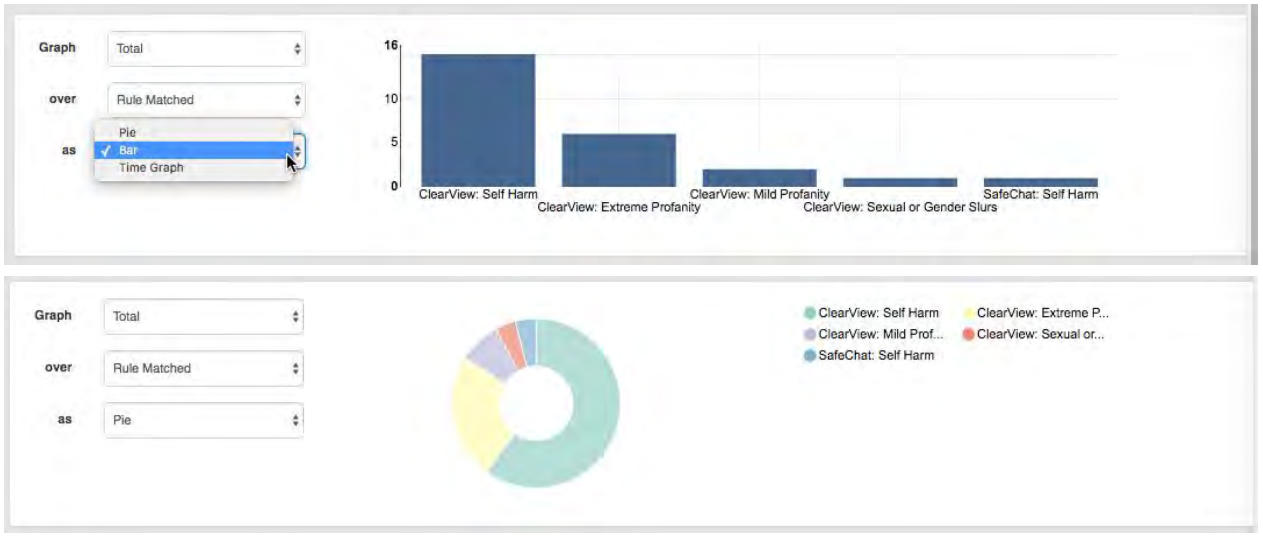
This image demonstrates the changes to the Top Rules Default, when adding a Condition of *'Username'*, *'Equals'* and the user *'Ava student'*.



TIP: Clicking *'Search'* and then using the Columns drop-down tick selection to check the results and naming convention, ensures the correct name to copy and paste to reduce the results to the specific requirements.

3.2.2 Modify Graph Panel

The option is available to change the graphical display by choosing from the drop-down options for all three of the options (if available). The choice of display for this data will be reflected in any report that utilises this Query. Changes made to the graph panel are applied instantly.

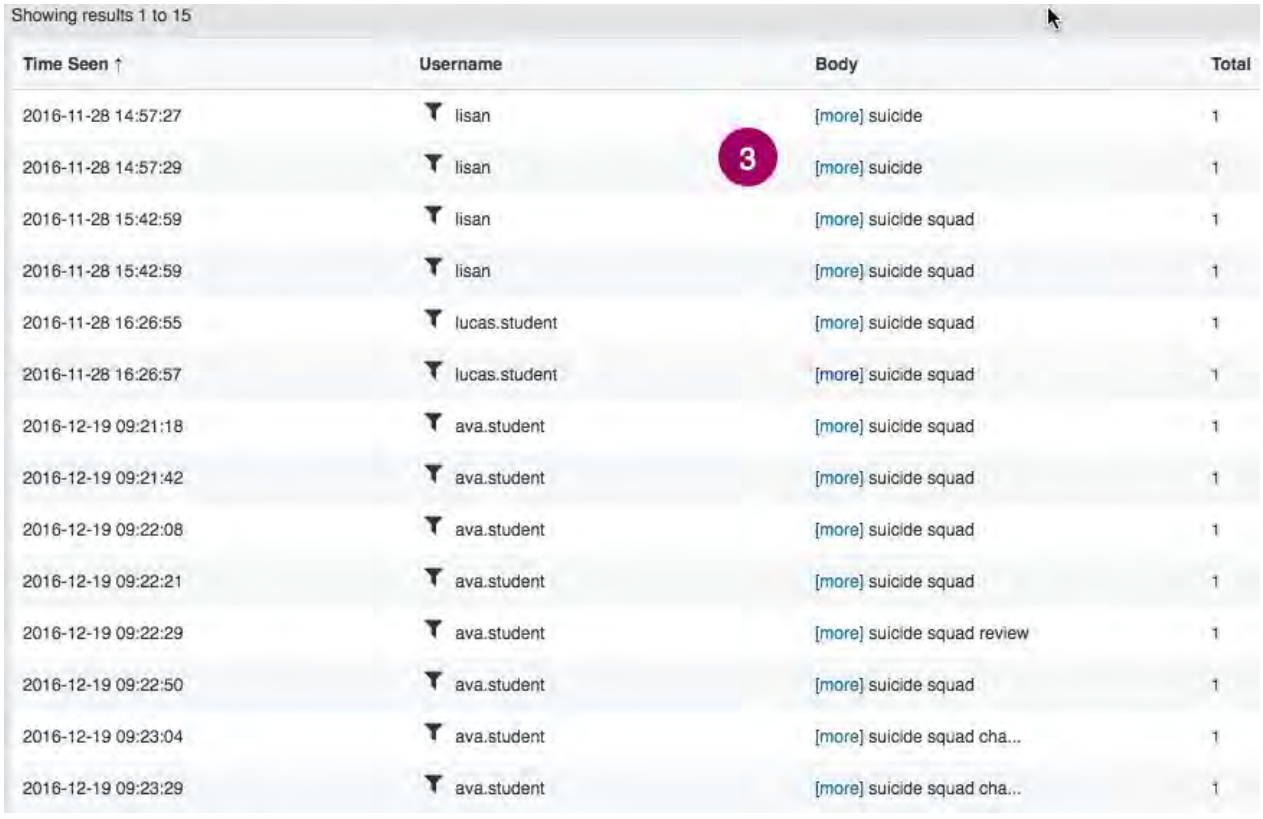


3.2.3 Modify & Drill-down on Results Panel

The results panel of the Query will display as a list with different options available and drill-down capabilities.

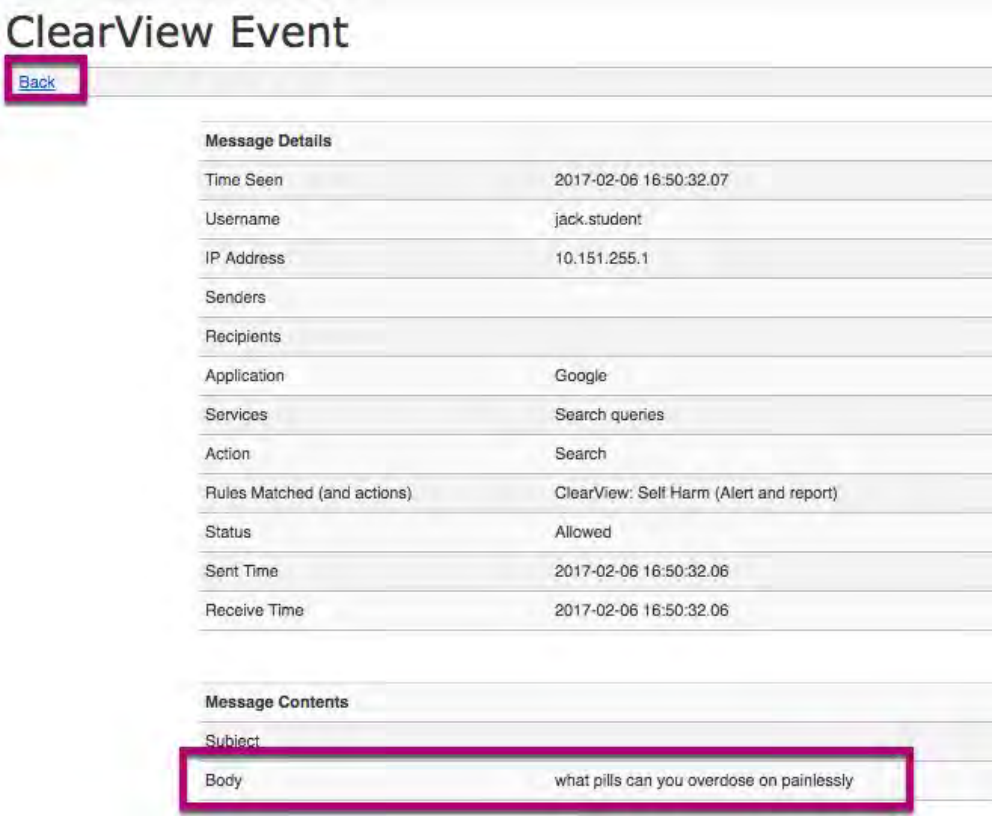
1. Depending on the selection in the conditions panel, *'results per page'*, there may be more than one page of results to display. Simply click *'Next'* to move to the next page of results. The graph panel will only display the current results list, and changes as you move to the next page.

2. The ability to drill-down for granularity on the results is achieved simply by clicking on the binocular symbol in the detail column (if available).



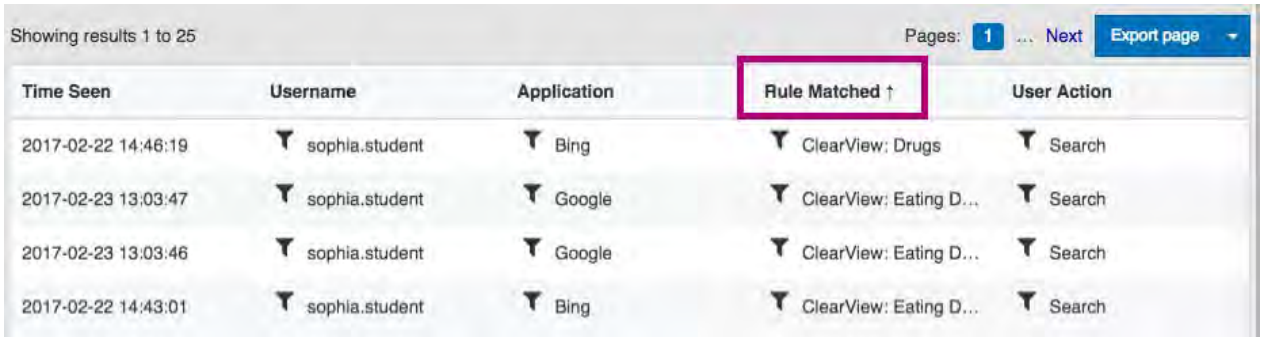
3. After selecting one of the results to drill-down on, the results for that Rule will display. Further drill-down is possible on the column *'Body'* by clicking *[more]* to view the details.

The column named '*Body'*, displays the specific details of the message content. Simply click '*Back*' to return to the list of results.



Sort - There is flexibility to sort the results by clicking on the column name to change the order. An arrow will display to show the order direction.

Remove Results - By clicking on the funnel symbol beside a column result, will remove the results from the Query results panel and add it back into the condition panel. (Refer section Deleting Queries and Conditions for further details).



Export Page

The '*Export Page'* button will download the results of the current page in a CSV file format which can be imported to other spreadsheet programs. If the results of all pages are needed, the '*Export All Pages'* button is available when clicking on the arrow beside *'Export Page'*. Please note that this could take some time for certain data sources and will time out if the Query takes more than a minute.

Exporting the data can be used to transfer the results on specific incidents for future reference or may be used to add to an executive report to a Board, etc.

3.3 Saving Queries

Queries are saved to re-use at a later date for quick reference or to be added to reports that can be scheduled and distributed. There are two options, *'Save Query'* to update any modifications to an existing Query or *'Save As'* to change the name thus creating an additional Query in the custom list.

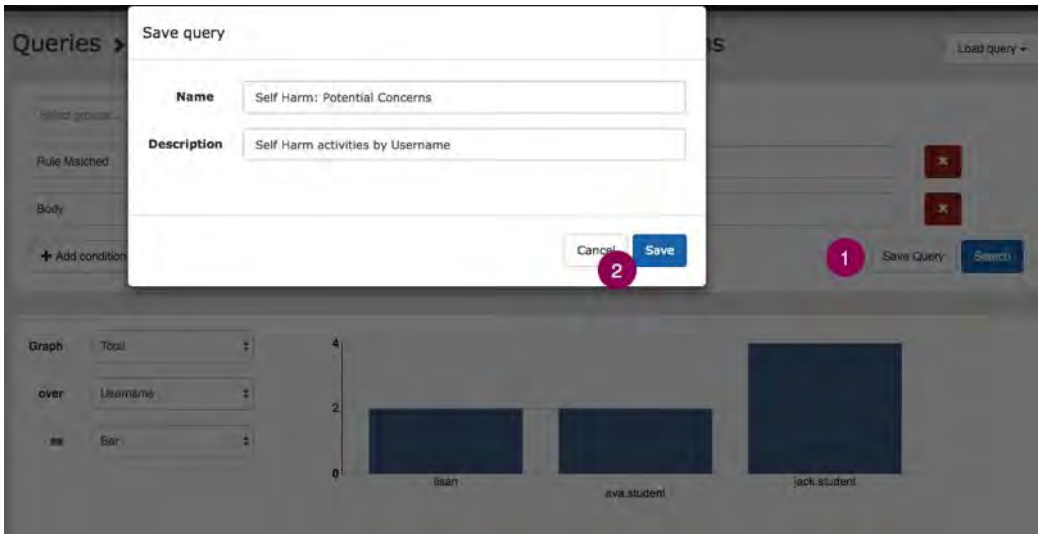
NOTE: Default Queries cannot be *'Saved'*. They can be modified and *'Saved As'* a new named Query and added to the Custom Queries list.

3.3.1 Save

'Save Query' will update and save any modifications made to the Query.

IMPORTANT: Modifying and then saving an existing custom Query will also change any report that is using the Query. As there may be several users who have access to Queries, it is important to understand that this may impact the content of reports for other users.

1. A pop up box will display when *'Save Query'* is selected.
2. Simply click *'Save'* to update the Query or *'Cancel'* to return to the Query.

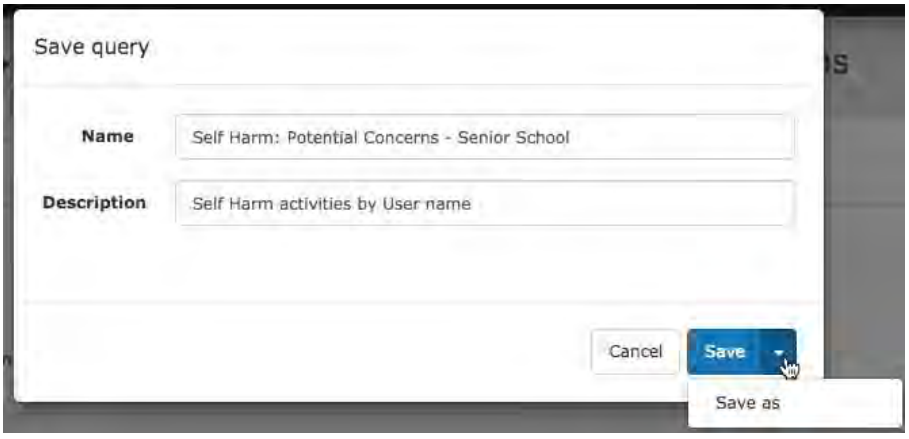


Saved Queries will be available in the custom list for all users to view, however the data displayed will be defined by the user's permissions. e.g. If a user is excluded from viewing another Group's data, the data will NOT be available to view for the excluded Group.

3.3.2 Save As

'Save As' allows a modified Query to be saved as a new named Query. The option to choose *'Save As'* will be available when any change to the *'Name'* field is made. A default Query that is being modified will only offer a pop up window to add a name and description, as defaults cannot be amended. *'Save As'* will add the modified Query to the custom list and can be used in new reports if required.

By changing the name of the Query to include 'Senior School', the option to select *'Save as'* is now available on the Save button.

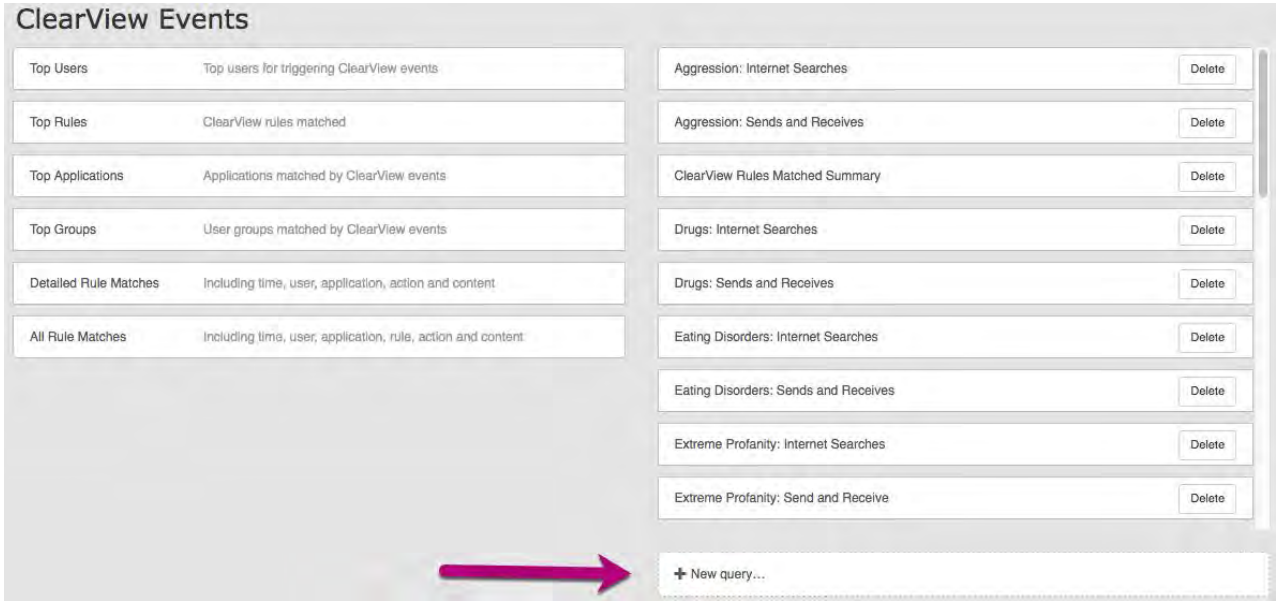


3.3.3 Unable to Save?

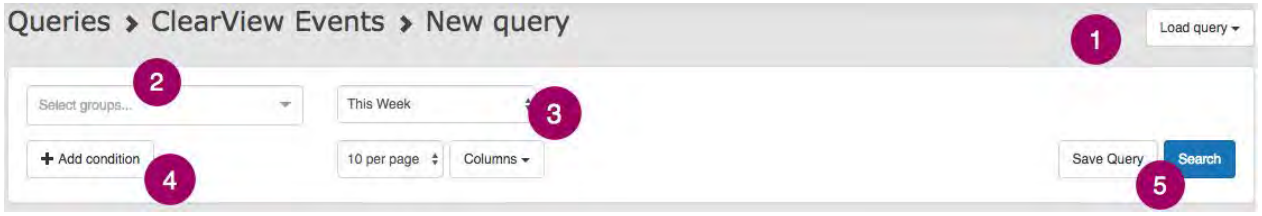
Saving Queries is available to users based on their Group permissions. A user may not be able to save the Query for future use. However access to the other functions are still available to add conditions, to change the graph or details list and drill-down results to view the information they require at that particular point in time. The IT System Administrator manages Group permissions or can save the Query for future use if required. (Refer to Groups and Permissions section for more detail).

3.4 Create New Queries & Add Conditions

Queries can be built on one or a collection of conditions to obtain the desired results. There are two options to create a new Query. Access from the Queries menu on the navigation side bar and choose *'+New Query'*, located under the list of custom Queries, to build from scratch, or open an existing Query and modify as required.



Selecting *'+New Query'* will open a *'New Query'* page.



1. **LOAD QUERY** – (Optional) Default list and previously saved custom Queries are available to use as a starting point. If using a pre-existing Query, Steps 2 to 4 have already been completed, however, these can be modified to change or refine results.

2. **SELECT GROUPS** – Select group from the list available in the drop-down or leave blank to capture all users.

3. **TIME PERIOD** – allows a selection of timeframes from last hour to all time.

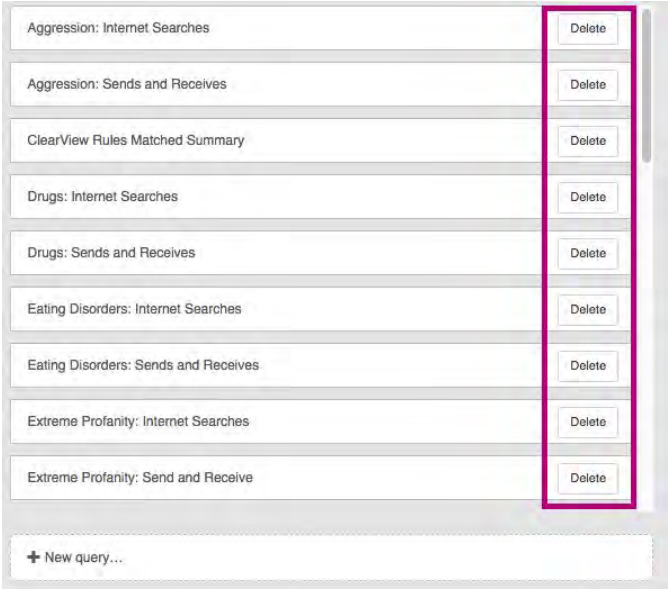
4. **ADD OR MODIFY CONDITION** - Click to add the required parameters. (Refer Modify Conditions Panel for detailed steps).

5. **SEARCH & SAVE** - *'Search'* to display results or *'Save Query'* if need to use again.

3.5 Deleting Queries & Conditions

Simply click the **X** checkmark for any selections not required, either the whole row or elements within the selection field.

To delete a Query no longer required, simply select *'Delete'* from the custom list. Default Queries cannot be deleted.



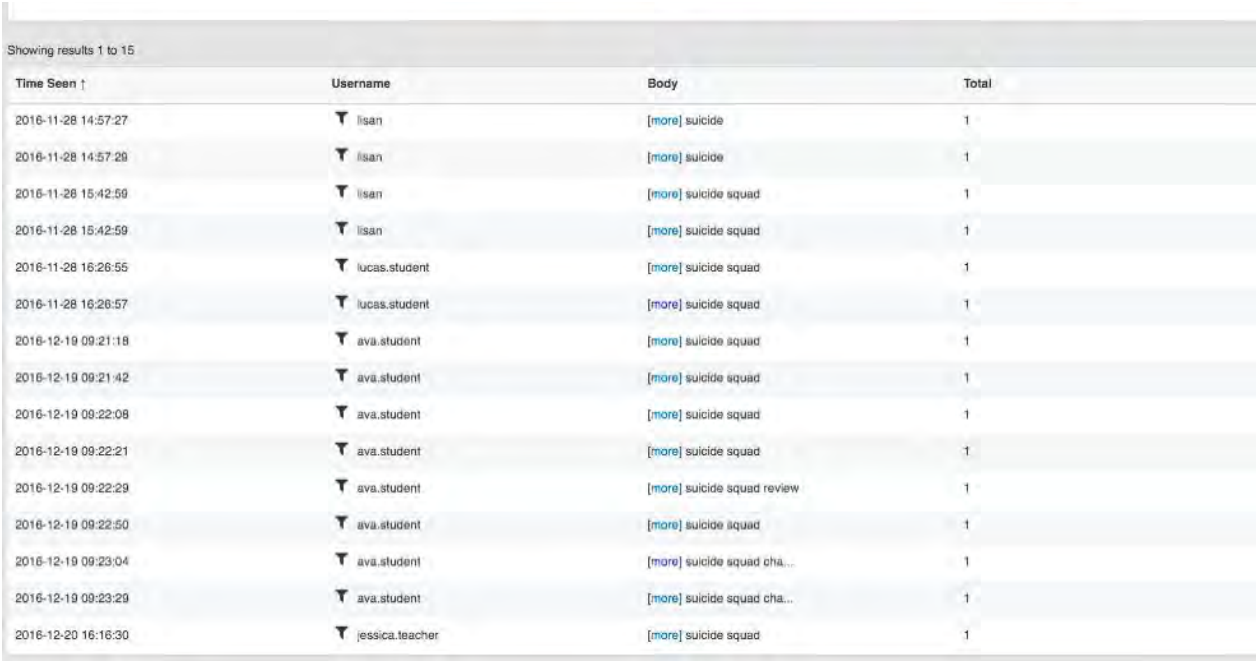
3.5.1 Unable to Delete?

Deleting Queries is available for System Administration only. Queries are used to build reports and accidental deletion could result in breaking reports for other users.

3.6 Exclusions in a Query

Data captured can produce false positives, generating irrelevant information populating the Query results. e.g. A search for the movie 'Suicide Squad' would trigger the Self-Harm Rule. Creating a *'Condition'* to exclude specific text provides more relevant results.

In the example below, only two results in the report would require analysis. Applying an exclusion condition would greatly reduce the number of results to review.



Showing results 1 to 15

Time Seen ↑	Username	Body	Total
2016-11-28 14:57:27	lisan	[more] suicide	1
2016-11-28 14:57:29	lisan	[more] suicide	1
2016-11-28 15:42:59	lisan	[more] suicide squad	1
2016-11-28 15:42:59	lisan	[more] suicide squad	1
2016-11-28 16:26:55	lucas.student	[more] suicide squad	1
2016-11-28 16:26:57	lucas.student	[more] suicide squad	1
2016-12-19 09:21:18	ava.student	[more] suicide squad	1
2016-12-19 09:21:42	ava.student	[more] suicide squad	1
2016-12-19 09:22:08	ava.student	[more] suicide squad	1
2016-12-19 09:22:21	ava.student	[more] suicide squad	1
2016-12-19 09:22:29	ava.student	[more] suicide squad review	1
2016-12-19 09:22:50	ava.student	[more] suicide squad	1
2016-12-19 09:23:04	ava.student	[more] suicide squad cha...	1
2016-12-19 09:23:29	ava.student	[more] suicide squad cha...	1
2016-12-20 16:16:30	jessica.teacher	[more] suicide squad	1

When determining what's needed to be monitored, it is necessary to consider what popular expressions, language or trends may affect results and should be excluded as part of the Query.
As new trends come into play, simply *'+add Condition'* to filter out unwanted results.

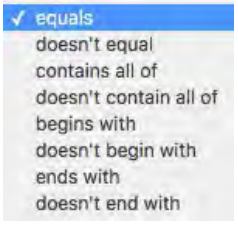
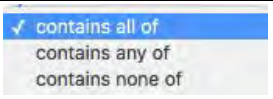
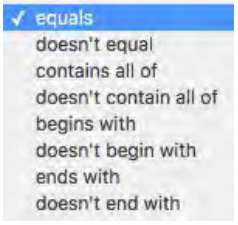
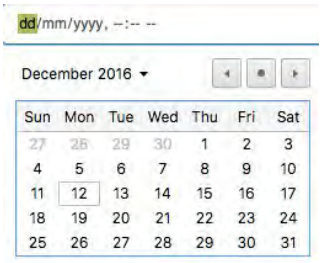
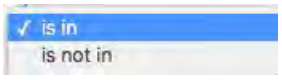
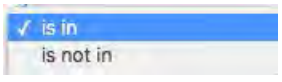
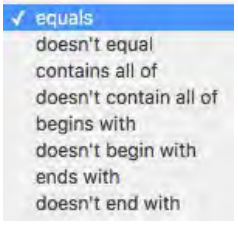
By adding conditions *'Body'* or *'Subject' with 'doesn't begin with'* and 'suicide squad', the results are reduced to reflect activity that would need to be actioned or reviewed.

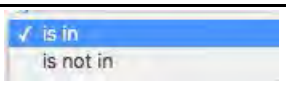
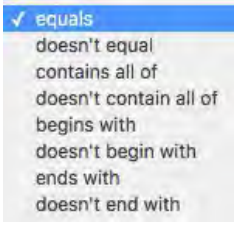
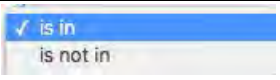
RECOMMENDATION: The best option to ensure that exclusions are not tainting results is to have the IT System Administrator make exclusions in the Rule (refer Rules Exclusion section for steps). Updating the Rule will stop all data collection therefore minimising maintenance on Queries affected by a false positive.

NOTE: Changes to a saved Query only apply from the date of the saved change. Any data captured preceding the change date, would still report 'suicide squad' in Queries or reports on any timeframe prior to the change date. Query exclusions only reduce the results displayed, the data is still captured until a Rule exclusion is applied.

3.7 Conditions Definitions

The following table provides the options available when choosing to *'+Add condition'* to a Query to refine the results.

1ST SELECTION	2ND SELECTION	3RD SELECTION
USERNAME		**Free text field:** System username as configured in Appliance User Management and generally aligns with the Active Directory username.
GROUP MEMBERSHIP		**Drop-down available:** User groups assigned as configured in Appliance User and Group Management module. e.g. Junior, Middle, Staff, Welfare.
CLIENT IP		**Free text field:** Matches the IP address or network a message is sent from or received on.
TIME SENT		**Drop-down available:** not commonly used. Allows to search on a specific day or time. 
APPLICATION		**Drop-down available:** Match an internet application by name, such as 'Facebook' or 'Gmail'.
MESSAGE STATUS		**Drop-down available:** Shows if the original message or search was allowed or blocked.
RULE MATCHED		**Free text field:** requires to be typed as named in the list of Rules e.g. ClearView: Eating Disorders **Note:** While it is not case sensitive, it does require the punctuation e.g. the colon :
ACTION TAKEN	As above	**Free text field:** the Action that relates to a Rule. e.g. Alert or report only. To return results, text needs to match exactly the types of Actions that are defined for Rules.

USER ACTION		**Drop-down available:** Match a particular action performed on a ClearView scanned service, such as 'Sending a status update'. Examples include: Read, Receive, Search, Send.
SENDERS		**Free text field:** Matches messages where the sender has specific details. Wildcard patterns such as "*@mydomain.com" can be used.
RECIPIENTS	As above	**Free text field:** Matches messages where the recipient has specific details. Wildcard patterns such as "*@mydomain.com" can be used.
BODY	As above	**Free text field:** If the message contains text in the body of the communication that matches a pattern triggered by the Rule.
SUBJECT	As above	**Free text field:** If the message subject contains text that matches a pattern triggered by the Rule.
SERVICES		Match a specific service such as "Instant Messaging" or "Webmail". Does not apply to emails via SMTP or POP3.

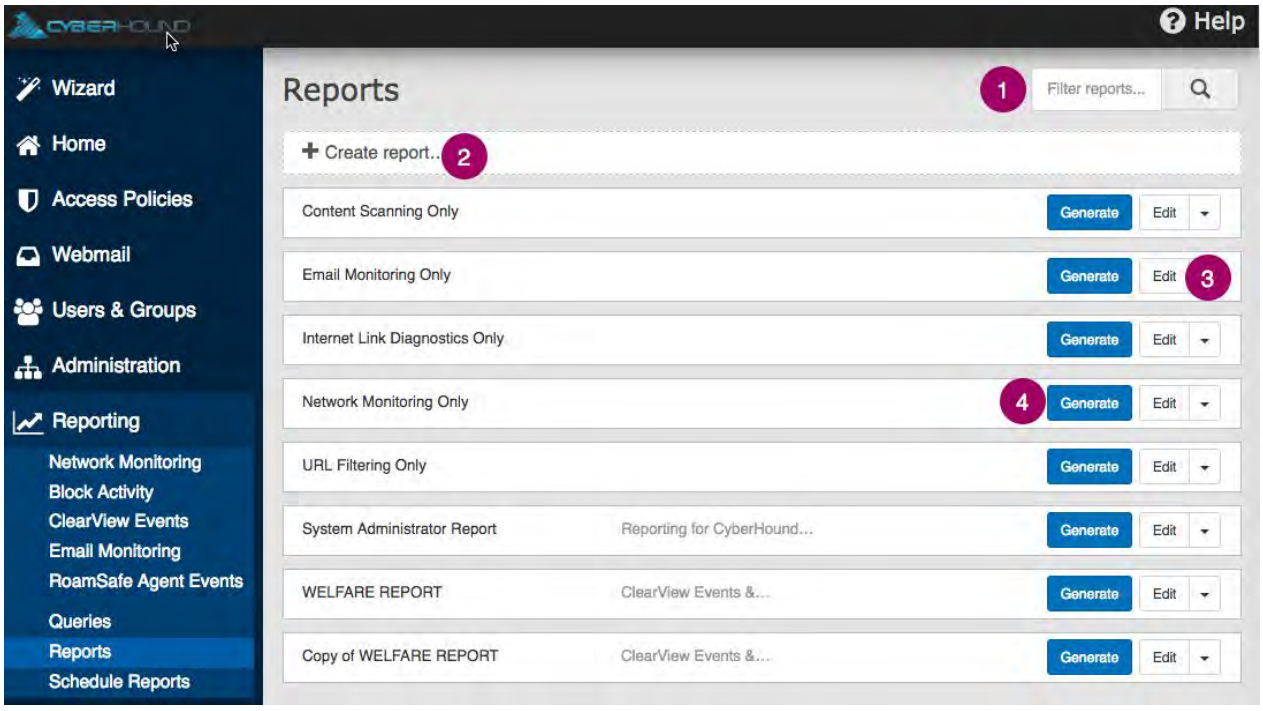
4. REPORTING

The CyberHound Appliance reporting module provides the facility to configure, view and schedule reports. Report data is shown in textual and graphical formats. A default ClearView report named *'ClearView Welfare Report'* is provided for ClearView Events.

4.1 Report Catalogue

The Reports selection allows viewing of the reports that are currently on the CyberHound Appliance and the ability to create and manage the list of reports.

Accessed via: *Reporting > Reports.*

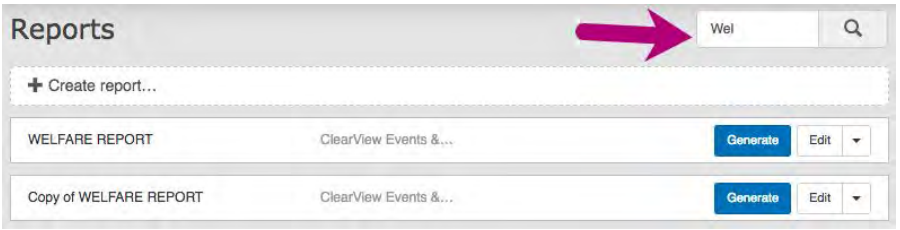


1. Filter Reports
2. Create Reports
3. Edit, Delete or Duplicate
4. Generate a preview of the report

4.1.1 Filter Reports

The *'Filter Reports'* function, searches on a report name or description and reduces the list to display those reports matching the search parameters. Typically used to search for a report that may need amendments or to locate a report to duplicate and re-work for another user. Ensuring a naming convention guideline is consistent and descriptions define the purpose of the report, makes this filter function more effective.

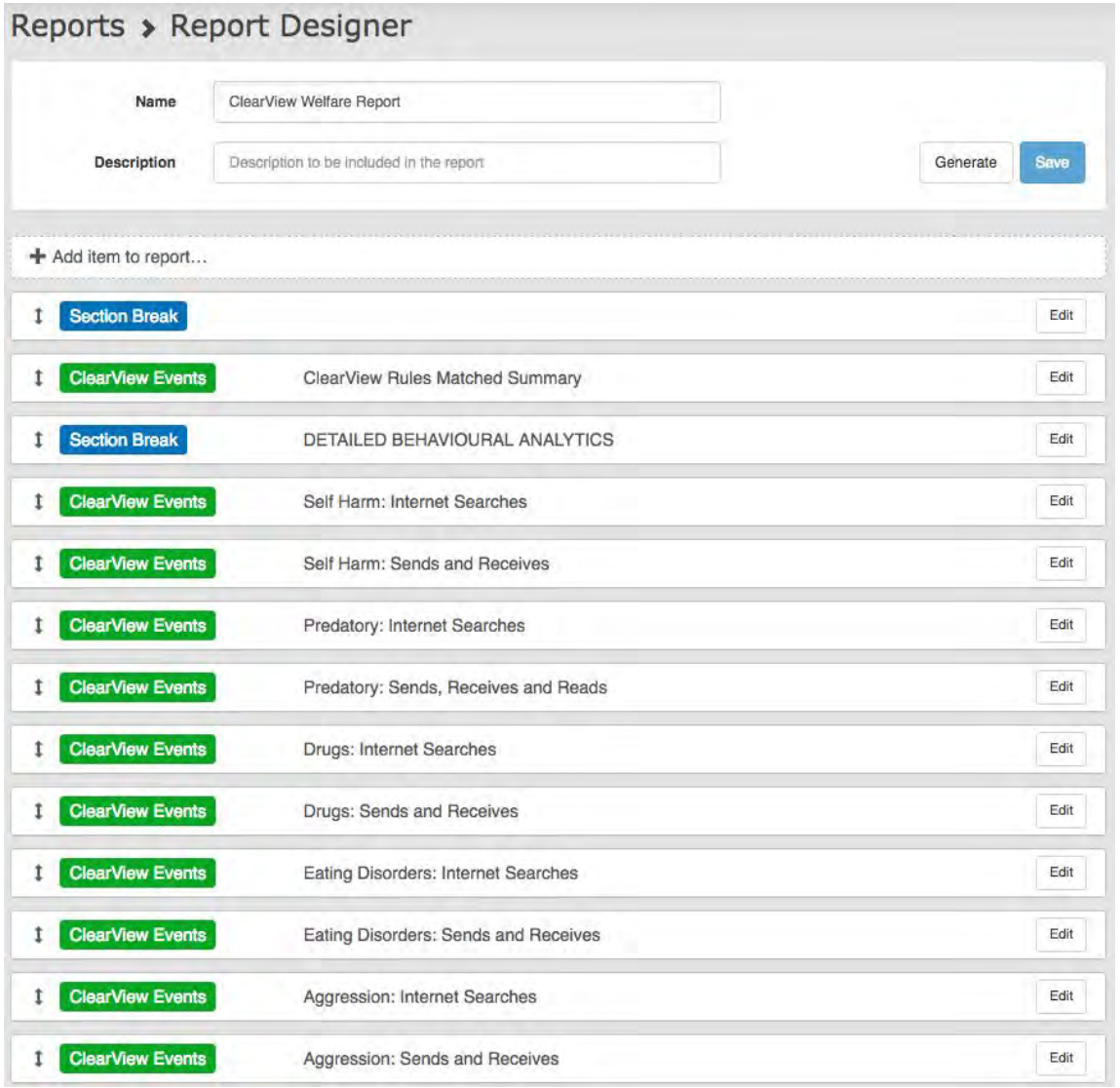
Start typing '*Wel*' into the filter search to reduce the list to display the reports that contain the search requirements for 'Welfare'.



4.1.2 Create New Reports

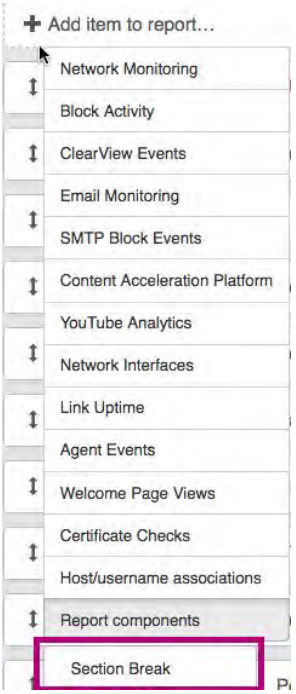
The simplest way to create a new report is to utilise existing reports, edit or duplicate, and make the necessary changes to achieve report requirements. Building a new report in *'Report Designer'* is available. Simply complete the name, description and *'+Add item to report'* with the necessary Queries or section breaks to build the report required.

Example of report complete with multiple Queries and section breaks.



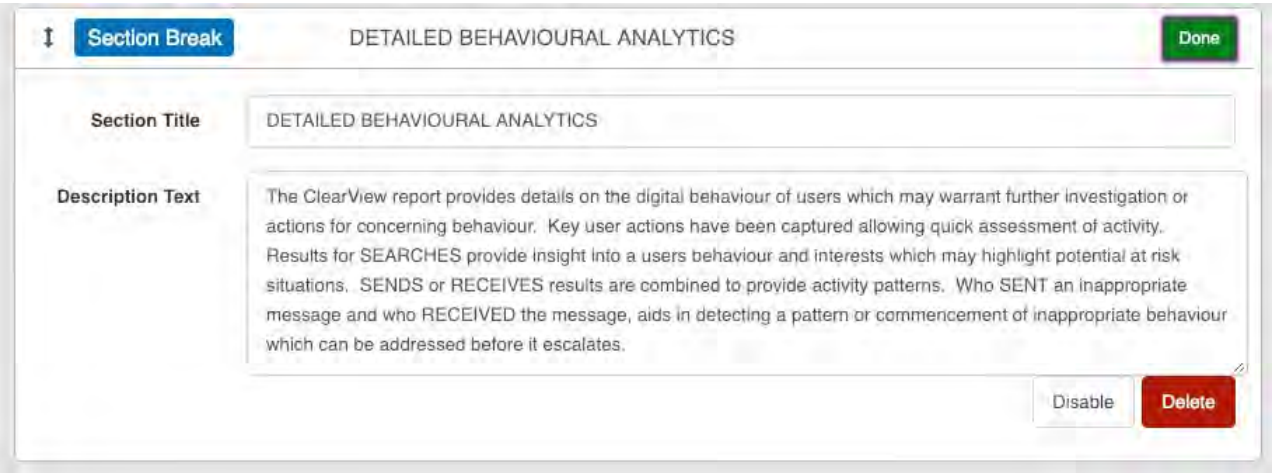
Section Breaks

Section breaks and descriptions are inserted to separate the data results and state the purpose of the section when the report is viewed.
The order can be rearranged, simply click and drag the row, up or down the list, to the desired location.



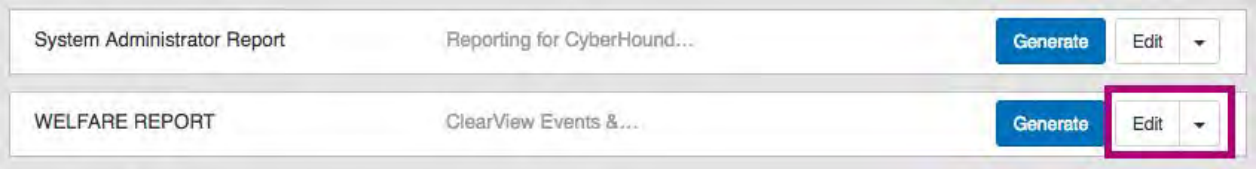
Create a section break to add to the report by selecting:
+Add item to report > report components > section break

Once created, select *'Edit'* to complete the details for the section break.
Add an appropriate title and description to provide details. Section breaks can be disabled from appearing in the report or deleted permanently when in edit mode.



4.1.3 Edit, Duplicate & Delete Reports

Edit



Selecting *'Edit'* on the relevant existing report will open the *'Report Designer'* page and allow modifications of the report. Options are available to add more Queries, modify the existing Query parameters or change the name and description of the report.

NOTE: Changes made to an existing Query is the same as if the Query had been edited through the Queries screen, and any changes are propagated to all reports using that Query.

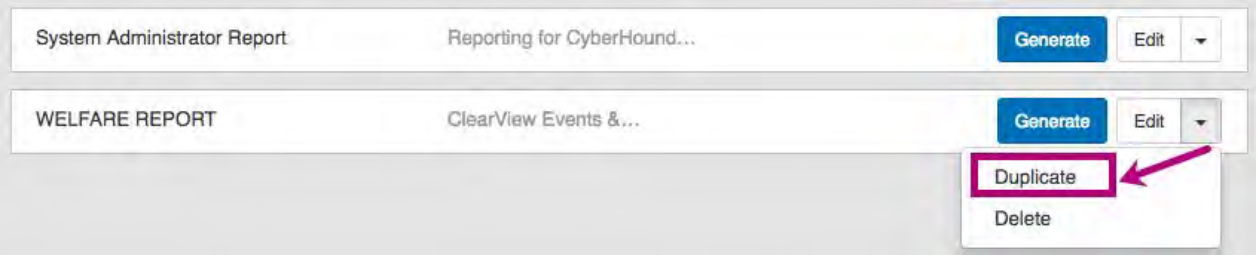
Once changes are made, select *'Save'* to retain modifications or rename to create a new custom report.

Duplicate

Select *'Duplicate'* from the drop-down beside the *'Edit'* button to duplicate a selected report. Often the same report, with minor modifications, is useful for multiple users and the duplicate option provides a quick solution to create the same report for each of these users and then refine the data to meet their specific needs.

Duplicating a report and modifying to refine the data slightly, provides consistency with comprehension and interpretation of the results across all users allowing comparisons to address related concerns and consistency of actions. Familiarity with the purpose and interpretation of a report offers seamless transfer of responsibility when required e.g. someone is on extended leave or secondment to another area of responsibility.

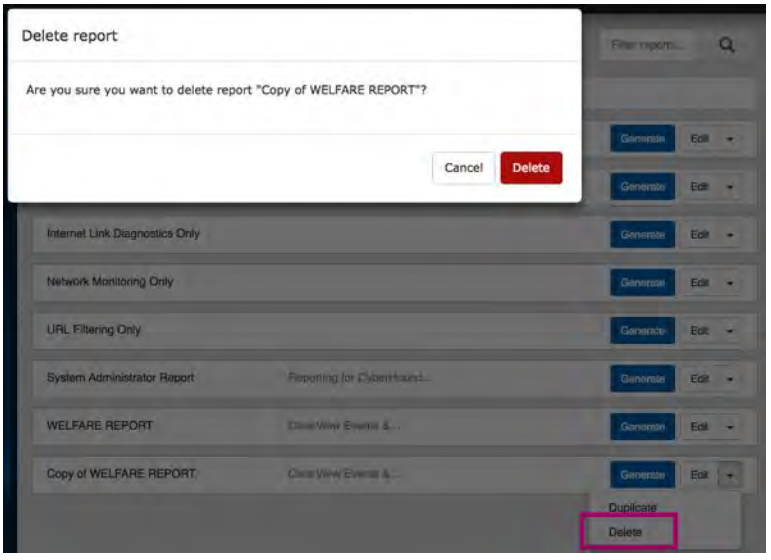
NOTE: There is NO need to duplicate a report to modify only on Groups. When scheduling the report, the same report could be used multiple times and *'Filter Report by Group'* to different Groups and add emails for the relevant recipients.



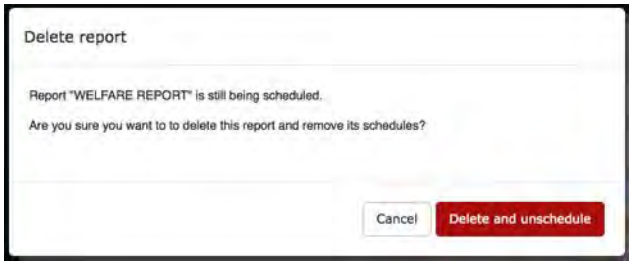
A copy of the report will be added to the bottom of the list of reports. The copy of the report can then be edited, modified and saved as a new report to reflect the requirements for another user.

Delete

When a report is no longer required, simply select *'Delete'* from the drop-down option beside the *'Edit'* button to remove the report from the list. A confirmation to delete will display, select *'Delete'* to remove or *'Cancel'* to return to the report lists.

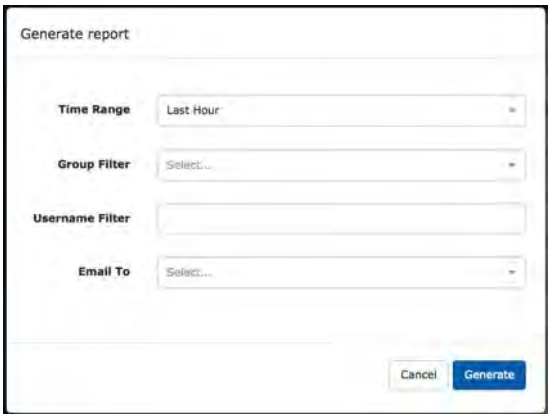


IMPORTANT: If the report to be deleted has been scheduled, the prompt will indicate it is a scheduled report.



4.1.4 Generate Reports

This provides the opportunity to view a preview of the report in a new tab on the browser. Selecting the *'Generate'* button displays a pop up window to refine the report for preview purposes.



Time Range – select from the drop-down the timeframe that is appropriate. The default is Last Hour.
Group Filter – option to select from the drop-down list of Groups that are defined in the system.
Username Filter – is a free text field that allows input of a username as defined in the system.
Email To – option to enter an email address and send real-time data results when requested.

WELFARE REPORT

Period: Sun 1 Jan 2017 - Fri 31 Mar 2017

Site key: lisanicholls

ClearView Events & Inappropriate Browsing

SUMMARY

This report is designed to give the senior staff in a school a summary of potentially inappropriate online behaviour or activity that may indicate a student requires welfare support. Further information can easily be sourced through the IT department or by simply clicking through the detail that is presented.

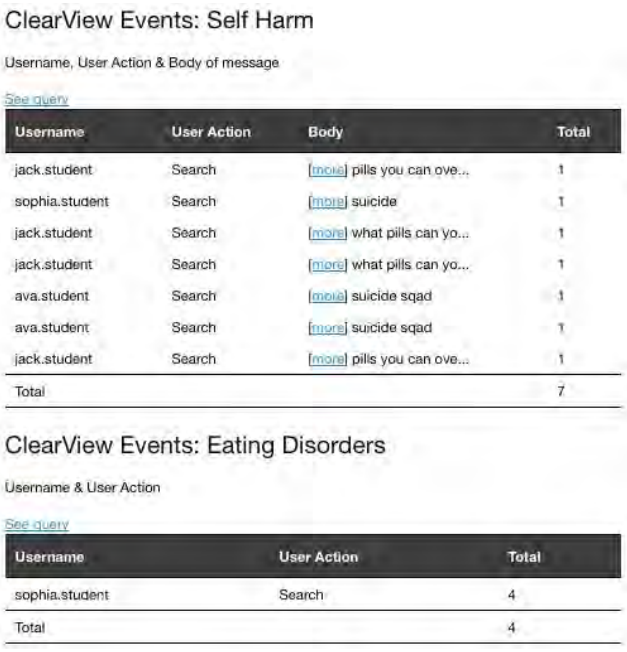
ClearView Events: Summary ClearView Events

See query

Rule Matched	Action Taken	Total
ClearView: Self Harm	Alert and report	7
ClearView: Online Reputational Risk Management	Report Only	8
ClearView: Eating Disorders	Block with Support and Report	4
ClearView: Drugs	Report Only	1
Total		20

Click *'Generate'* button to create the preview report. Once the report is displayed, there is the opportunity to drill-down into the results by clicking on the *'See Query'* or *'[more]'* link beside each of the data graphs or result lists.

NOTE: Accessing Query from report will open the default Query. The report recipient will need to enter the report period to view the same details as displayed in the report.



ClearView Events: Self Harm

Username, User Action & Body of message

See query

Username	User Action	Body	Total
jack.student	Search	[more] pills you can ove...	1
sophia.student	Search	[more] suicide	1
jack.student	Search	[more] what pills can yo...	1
jack.student	Search	[more] what pills can yo...	1
ava.student	Search	[more] suicide squad	1
ava.student	Search	[more] suicide squad	1
jack.student	Search	[more] pills you can ove...	1
Total			7

ClearView Events: Eating Disorders

Username & User Action

See query

Username	User Action	Total
sophia.student	Search	4
Total		4

4.2 Schedule Reports

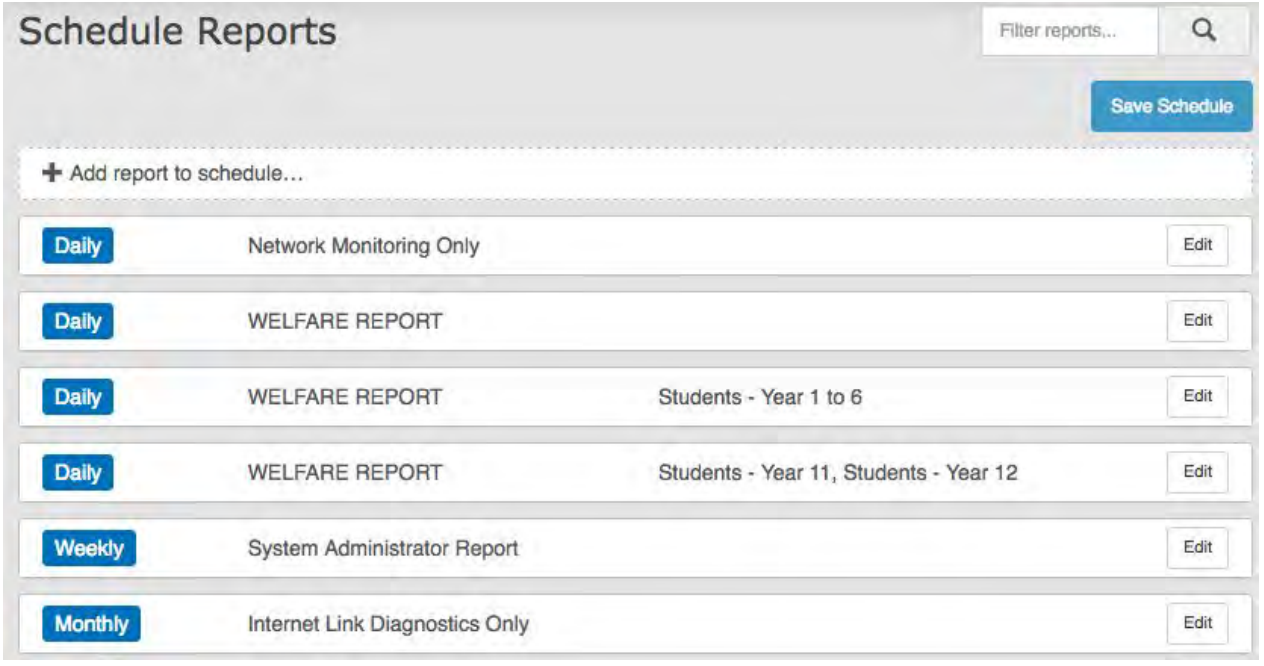
Schedule Reports allows for administration of previously specified reports to be periodically sent to nominated email addresses.

Scheduled reports can be easily modified to:

- **Enact contingencies as needed** e.g. to add or change email address when someone is on leave.
- **React to special circumstances** e.g. need to change a fortnightly report to daily for a short period of time to monitor activities more closely.

Schedule Reports also provides the flexibility of adding the same report and to schedule each one differently. An example could be a Welfare Report is added multiple times to the Schedule Reports list and each scheduled report could have different scheduled parameters of frequency, email addresses and filtered to different User Groups. The benefit is ensuring the report data is the same for everyone to interpret. The executive team may require reports on all student groups on a quarterly basis whereas welfare staff members responsible for different student cohorts, may need their reports daily and their manager may need to review all students on a weekly or monthly basis.

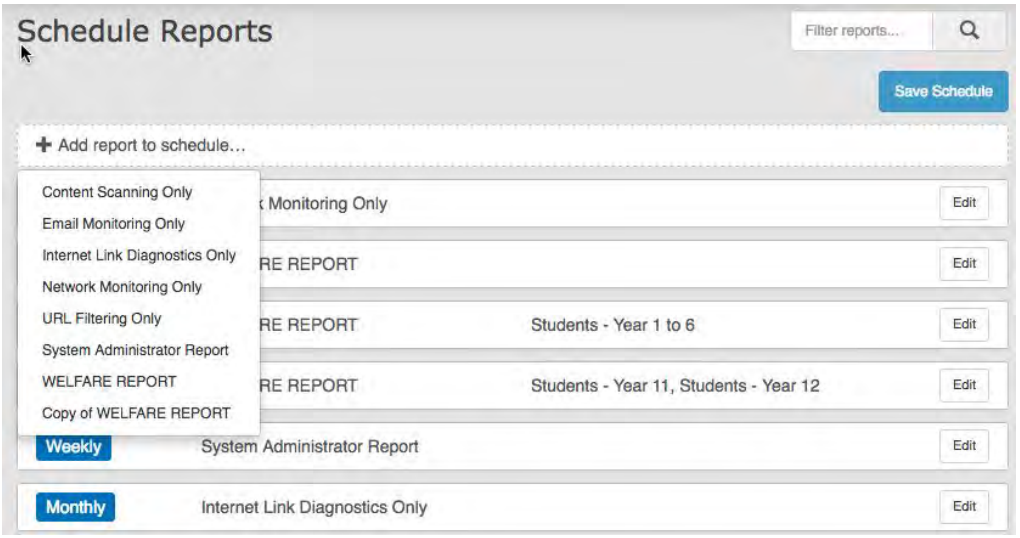
It's important to note that the name of the report cannot be changed in Schedule Report, however the Groups selected for the schedule report will display making it easier to identify. Reports are displayed in order of frequency selected for the report.



NOTE: It is the report administrator's responsibility to apply the appropriate group filters for the report to ensure that the data contained in the reports is appropriate for the intended recipient(s), i.e. the data source permission and group exclusions of individual recipients is not taken into account when generating the report. As the system does not recognise email addresses only usernames, any email address could be added to a scheduled report and may inadvertently be distributed to a recipient not intended to view the data.

4.2.1 Add Schedule Report

Selecting *'+Add report to schedule'* provides a drop-down list of reports that have been saved under the Reports section. Simply choose the report required to be scheduled and emailed to specific recipient/s.



Enter the schedule details required for the report.

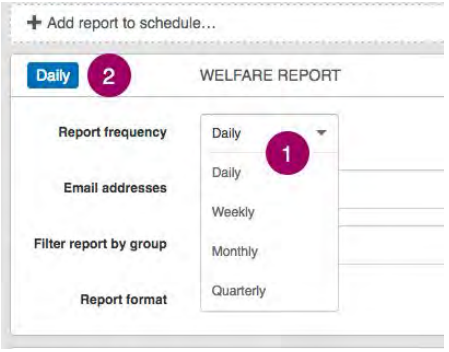
1. **Report Frequency** – choose options from Daily, Weekly, Monthly or Quarterly.
2. **Email Addresses** – enter as many email addresses as needed. If no email address is added, a message to indicate one is required will display in red.
3. **Filter report by Group** - Report can provide results for specific groups.
4. **Done** – expands and collapses the report view.

IMPORTANT: If no Group is selected, then the results of the report will display all users activity.

4.2.2 Report Frequency

All reports are generated and emailed just after midnight, as below:

- Daily - At the end of every day.
- Weekly - On Sunday night.
- Fortnightly - On Sunday night at the end of each fortnight.
- Monthly - At the end of the last day of the calendar month.

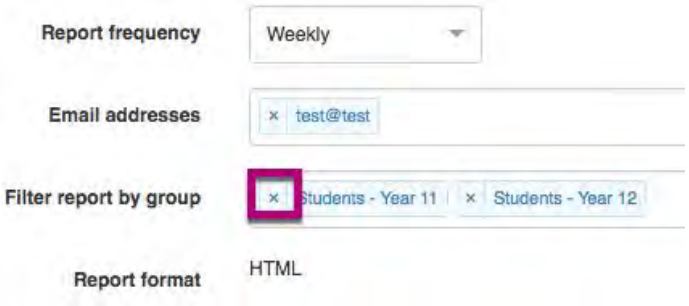


1. Select from the drop-down list the frequency required for the report.
2. The chosen option will display on the report header line.

4.2.3 Modify Schedule Reports

When changes are required to the scheduled report, you can simply:

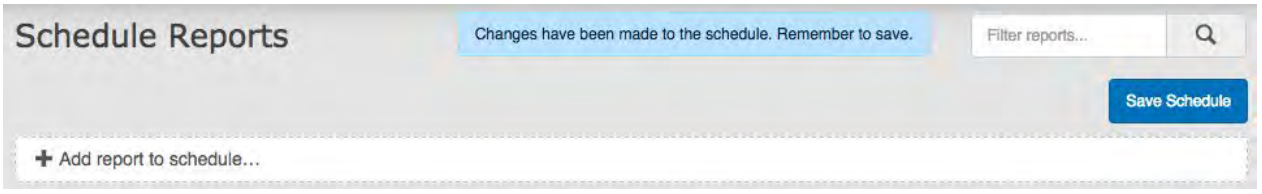
- Change the frequency of report by selecting from the drop-down.
- Add or delete email addresses.
- Add or delete Groups.



Simply click the **X** checkmark for any selections not required to delete and save schedule when completed.

4.2.4 Save Schedule Reports

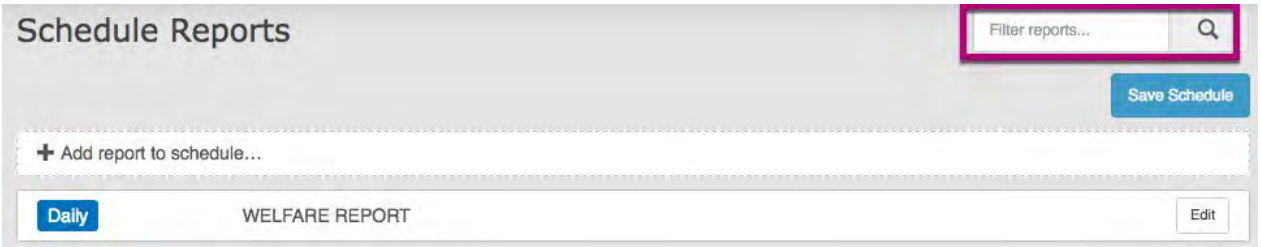
When reports are added to the schedule, before exiting the page you need to *'Save Schedule'* to retain the additions or deletion of reports. A prompt at the top will display when any additions or changes are made, as a reminder to save the changes.



If you forget to add an email address and click on *'Save Schedule'* the report with missing data will open for the data to be completed before '*Save Schedule'* function is actioned.

4.2.5 Filter Schedule Reports

The *'Filter Reports'* function, searches on a report name, email address or group and reduces the list to display those reports matching the search parameters. Typically used to search for a report that may need amendments e.g. Replacement of an email address or Group.

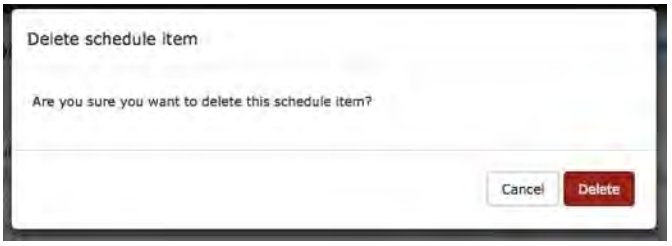


4.2.6 Delete or Disable Schedule Reports

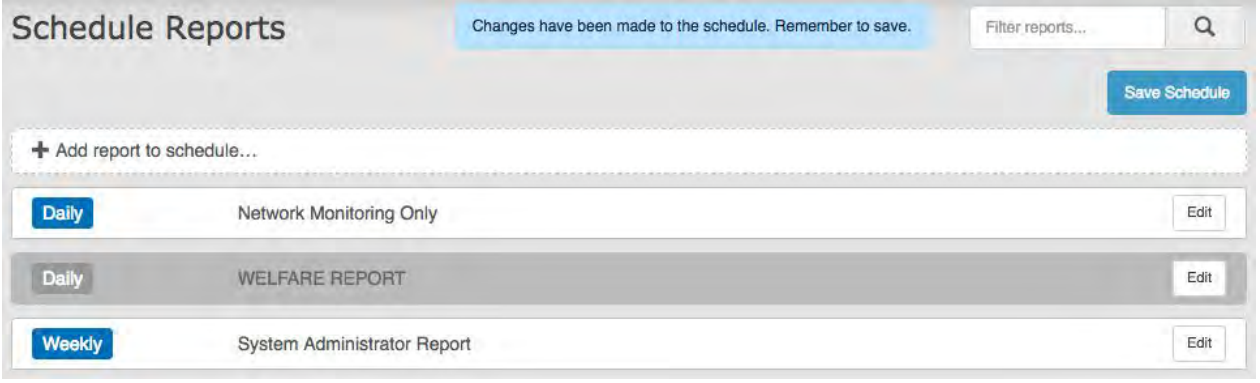
Obsolete reports or reports that may not be required for a period of time, are easily managed. Simply open the relevant report and select either option.

- *'Disable'* to place distribution of the report on hold until required again.
- *'Delete'* to remove the report from the schedule altogether.

A prompt will display to confirm *'Delete'*.



DISABLE & ENABLE – simply toggle between disable and enable to use this feature. The header of the report will be greyed out when disable is on. In the report list it is easy to identify which reports are disabled. Simply click *'Enable'* to reactivate the report.

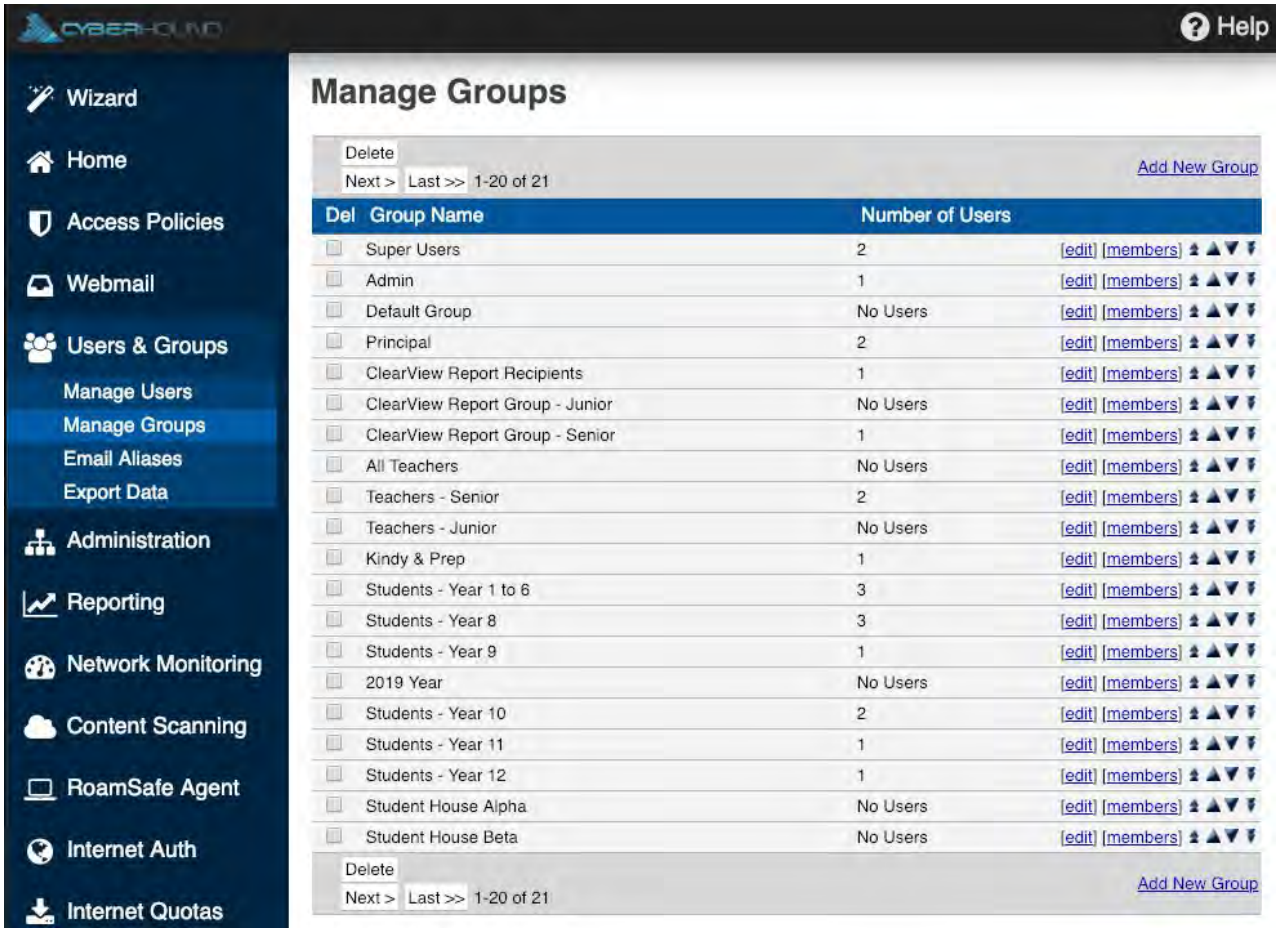


5. GROUPS & PERMISSIONS

The Groups assigned determine all CyberHound Appliance user permissions. Groups should align with Active Directory and whilst a user can belong to multiple groups, their permissions to access CyberHound data source queries, etc., are pulled from their primary group. The primary group is the highest group in the group list that they are a member of.

Changes to the permissions are updated every 30 minutes (or the time defined by the *LDAP Lookup Caching* option under *Configuration > Advanced*, or can be pushed through by Flush Authentication Cache. Assigning and managing the permissions for *'Users & Groups'* is predominantly the responsibility of an IT System Administrator.

Access via: *Users & Groups > Manage Groups*



Add a Specific ClearView Access Group

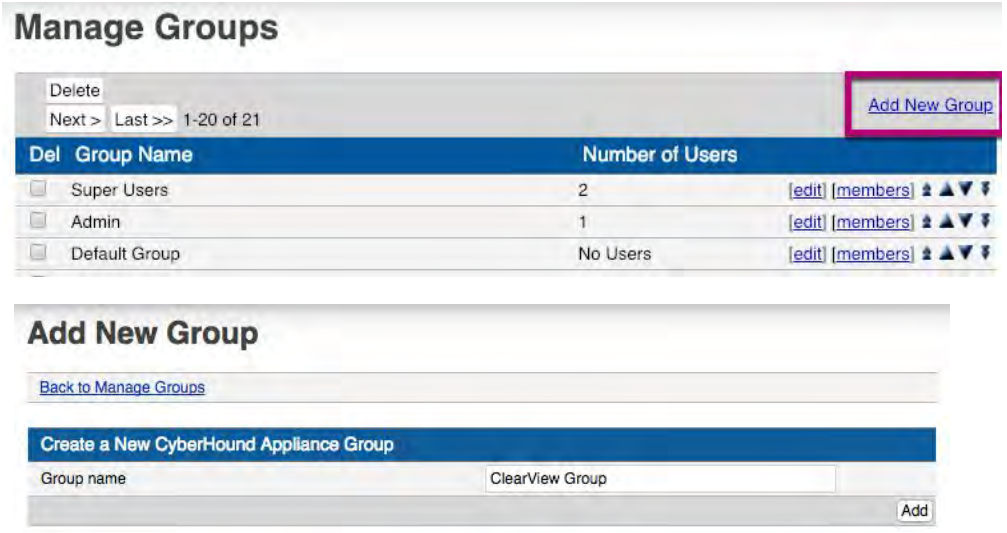
Active Directory may be configured with only one or two staff groups. Generally only a limited number of staff will have the responsibility to access and review ClearView Events. As an example, there maybe 100 users in one Staff Group and only 6 of those staff will require access to investigate concerning patterns. To isolate these 6 staff members to provide access, creating another AD group named ClearView Group or Welfare Group may be necessary.

IMPORTANT: CyberHound Appliance will not recognise a nested group from AD.

Once you have created your new AD Group and included the users, the Group will need to be added to the CyberHound Appliance.

Select *'Add New Group'* and enter the name of the new Group (Tip: copy and paste from AD so it matches exactly to allow sync.). Click *'Add'* and set the relevant permissions and *'Update'* to save changes. (Refer to next section for permission settings).

The newly created group will be added to the end of the list of Groups. Each group has a priority, which is used when authenticating. The highest priority group is at the top of the page and priority can be adjusted using the arrows at the right of each row. The new 'ClearView Group' would need to be positioned above all other groups that the user is also a member of.



5.1 Group Permissions

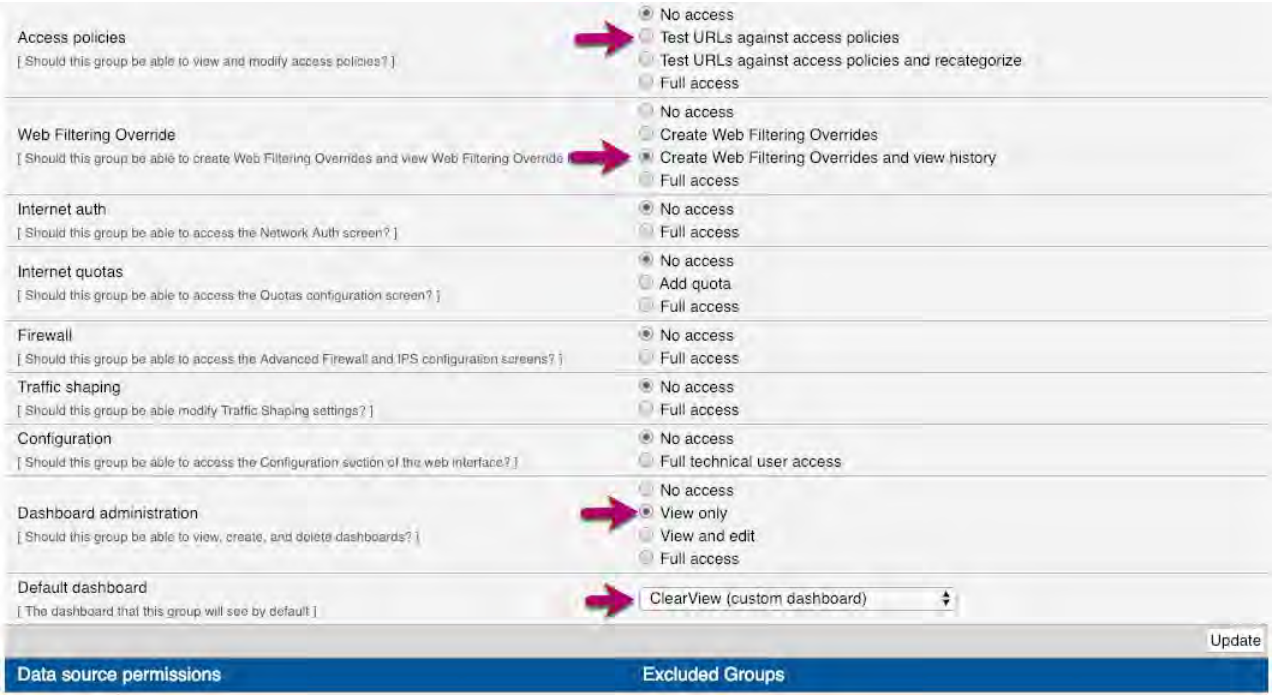
Access via: *Users & Groups > Manage Groups [select group]*

When *'[edit]'* is selected for the relevant Group, the top half of the page is for *'Group Permission'* settings. ClearView Event permissions are granted in *'Data Source Permissions'*. If a user does require permission to access reporting or modifying of Rules and Actions, then Reporting and Content Scanning permissions would need to be granted.

IMPORTANT: If Reporting Administration or Content Scanning *'Full Access'* is granted, the User Group will have access to all the reporting functions (create/modify and schedule reports functions) and all the other data sources including the Dashboard on the Home page and access to modify and change the Rulesets and actions in Content Scanning. To restrict visibility to users results you could apply data source permissions exclusions (see below) to every data source, however with access to reporting, visibility to every user on the network is possible via generate report or schedule to deliver with their email address.

The following is an example of the permissions that are generally considered for a group who needs access to the ClearView data source.

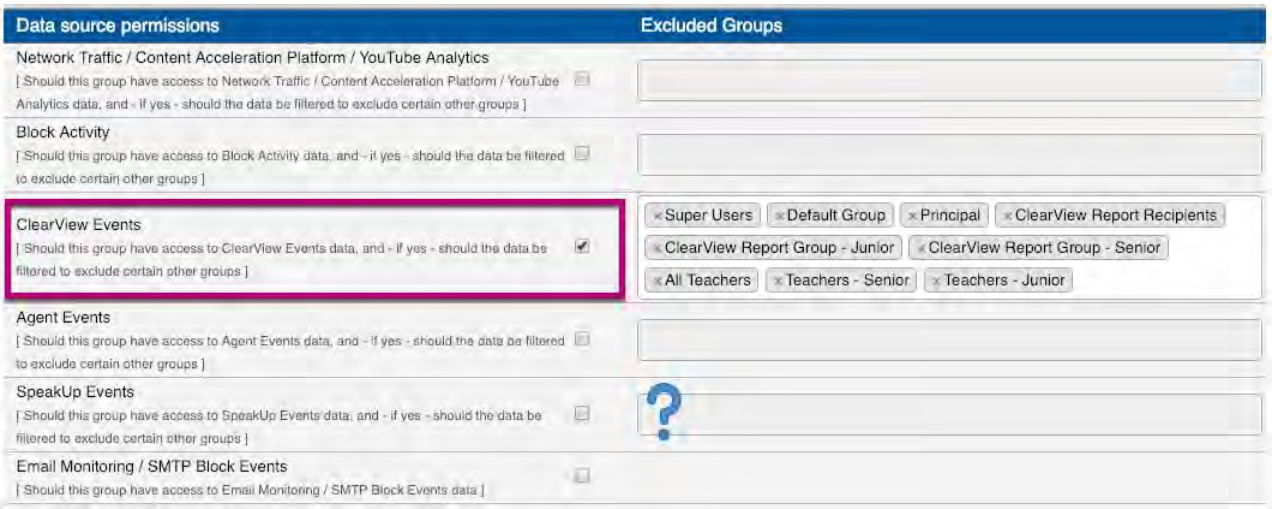
- **Access Polices** – test URL's for Classroom Control.
- **Web Filtering Override** – access to create Classroom Control lessons.
- **Dashboard** – on the Home page a view of perhaps a custom dashboard with ClearView events.



5.2 Data Source Permissions

Access to ClearView Events is granted via the *'Data Source Permissions'*.
Step one is to tick '*ClearView Events'* to provide the access permissions for the Group.

NOTE: ? Consider if this group is also going to have access to SpeakUp events.

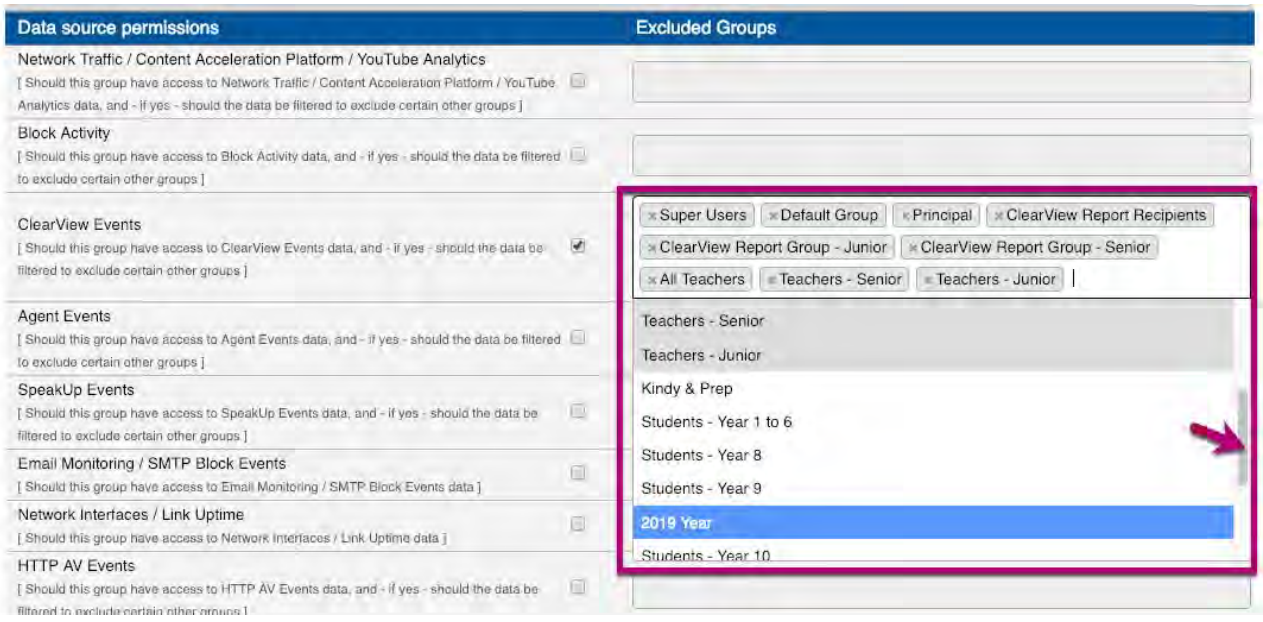


5.2.1 Data Source Excluded Groups

Step two is to consider exclusions to restrict access to other Groups making the results more refined for the users. The exclusions selected will apply to all the users in the Group and provides the ability to:

- Match student cohorts to relevant welfare's person area of responsibility.
- Restrict access of staff to view other staff activity.

To add excluded groups, simply click into the field and select from the drop-down list available and add as many other groups as is relevant for this user group by scrolling through the list.

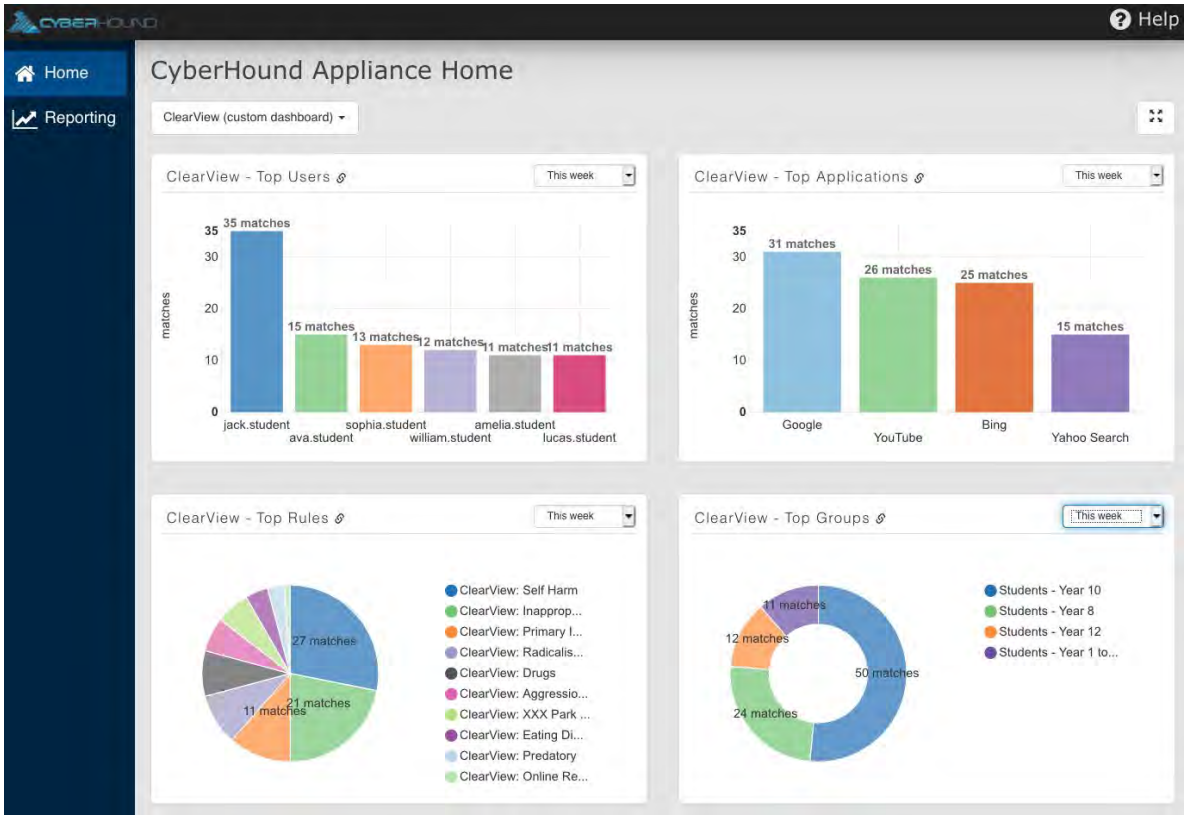


NOTE: If this group is going to have access to other data sources e.g. SpeakUp or Network Monitoring, simply tick the relevant data source and add the exclusions required.

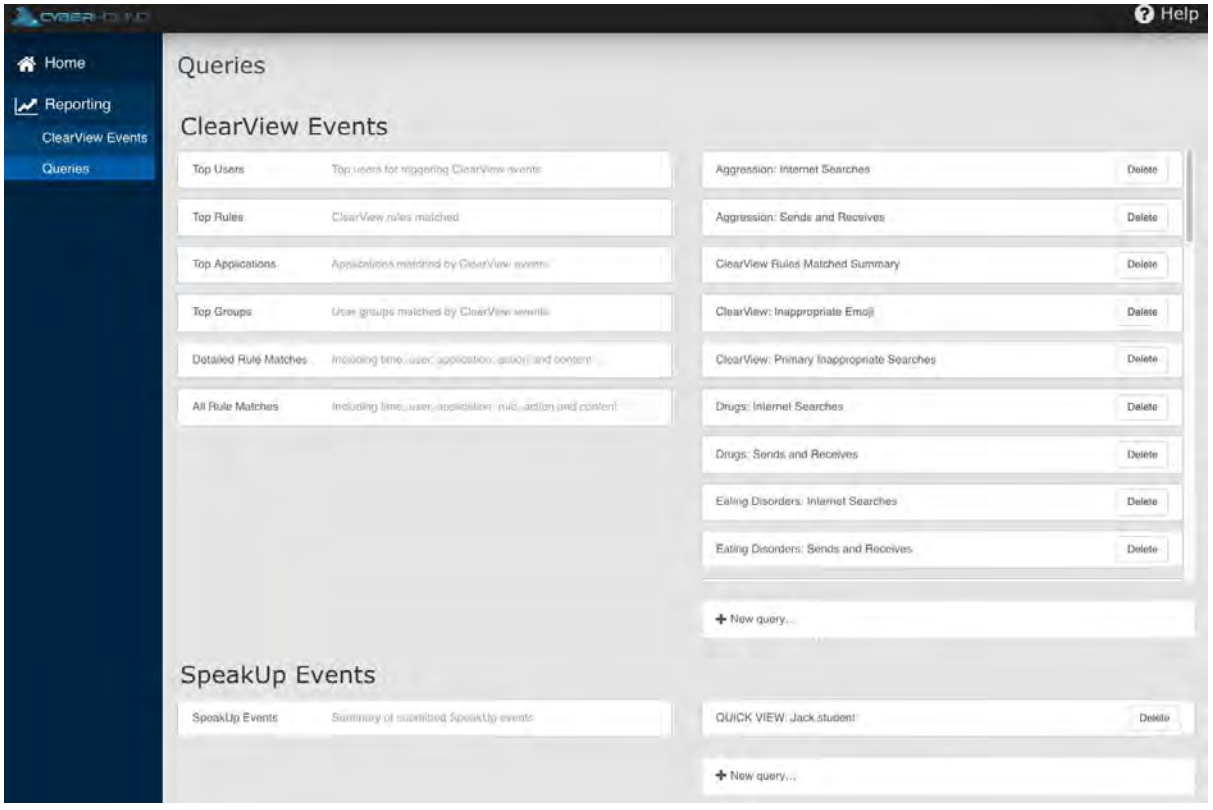
5.3 User Groups - Interface Views

The following are examples of a user interface view when data source permission is granted.

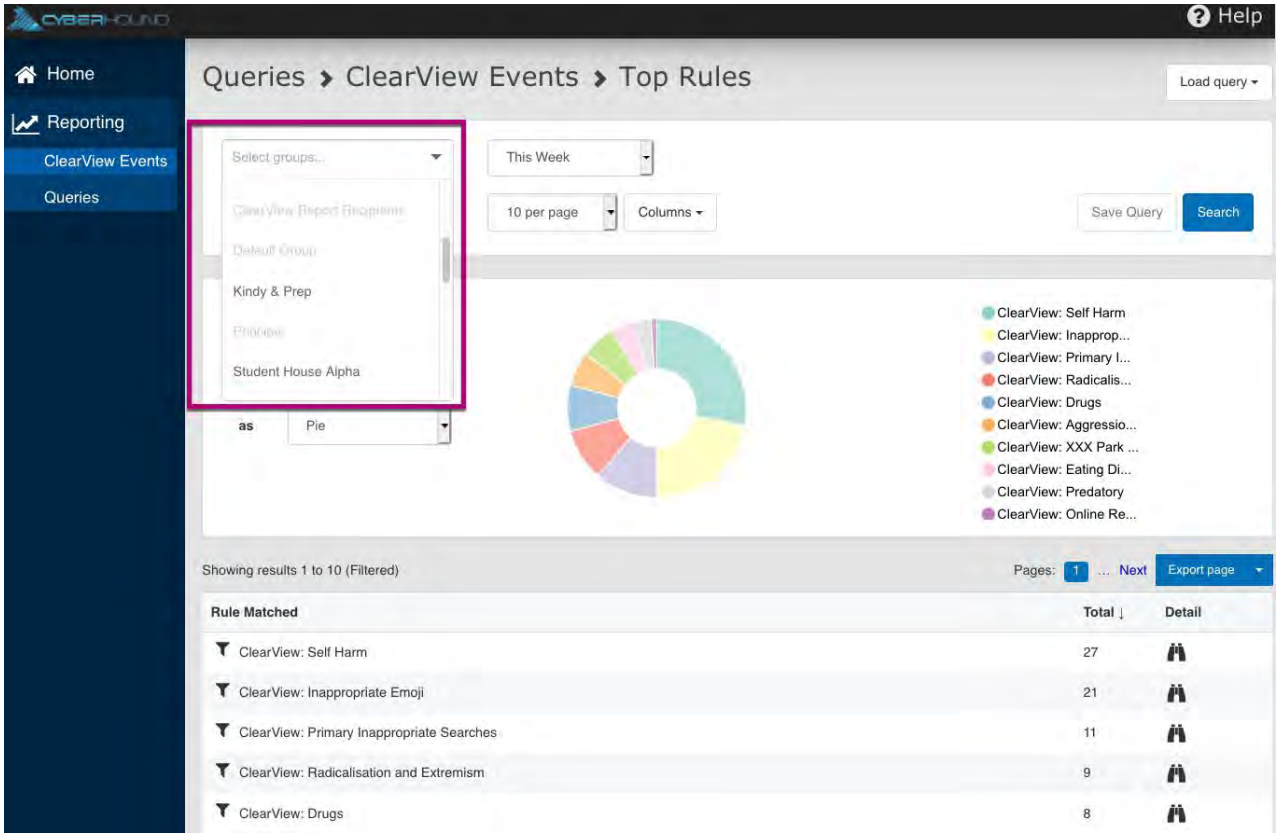
Dashboard group permission and applied view only to custom ClearView results.



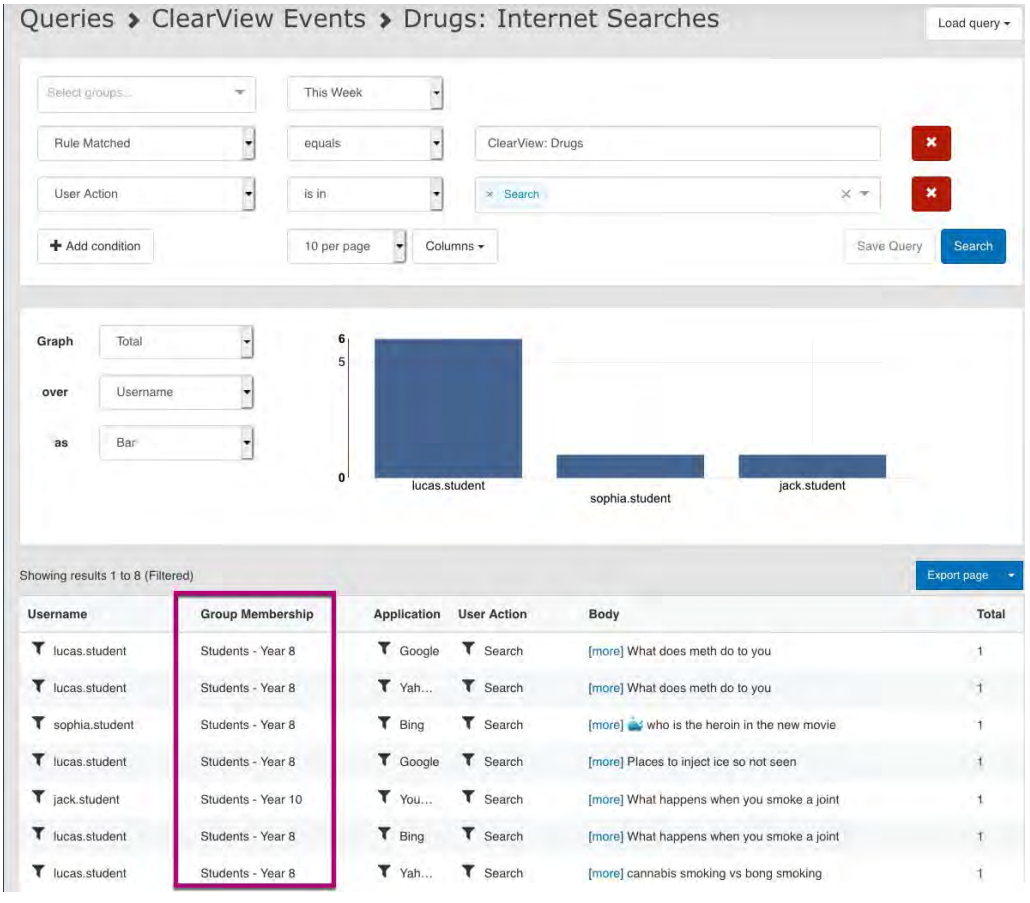
Data source permission for ClearView Events and SpeakUp only data sources.



Data source permission for ClearView Events. Note that the Groups that are excluded are greyed out and NOT able to be selected.



Only the Groups that are allowed will be visible in the results.



superloop

CYBERHOUND

CyberHound provides schools and universities with the ability to optimise, secure and manage their internet services. We help students engage in new forms of learning and help staff confidently use digital content and resources without the worry of access, internet speed or reliability. For over 18 years CyberHound has developed the most comprehensive behavioural analytics and cybersafety solutions and is now the benchmark for the education sector internationally. CyberHound is part of the Superloop Group, a leading independent provider of digital services across the Asia Pacific region (ASX: SLC).