HICS - How to view RM SafetyNet logs when a Prevent/IWF alarm is triggered

Updated January 2019

Summary

All HICS schools by default have Internet Watch Foundation and Prevent alerts deployed. If an alarm gets generated, RM (the HICS broadband provider) will contact Herts for Learning (HfL), who in turn will contact the relevant school. This document is a guide for schools to help them carry out steps in what to do when an alert is triggered.

It is important to note that it is very likely the alert triggered is a 'false positive'. However, schools will naturally wish to carry out additional investigation work.

Potential challenges

The list of websites and searches that generate an IWF alert are a closely guarded secret, as per instruction from the Police. HfL are not aware of what triggers an IWF alert. Even when an IWF alert occurs, HfL nor the school can be notified as to what specifically caused this to happen. Prevent alerts do however provide the URL/keyword search that triggered the alarm.

Another challenge will be that unless the school have User Based Filtering (UBF) deployed, schools/HfL will only see which IP addresses have accessed the content, instead of network usernames. IP addresses are often dynamically assigned and change frequently. With this in mind, identifying the person who triggered the alert will require immediate action, and even then this may not be possible. Schools are advised to speak to their local IT Support staff to assist with marrying up IP addresses to network usernames to see if the relevant people can be identified.

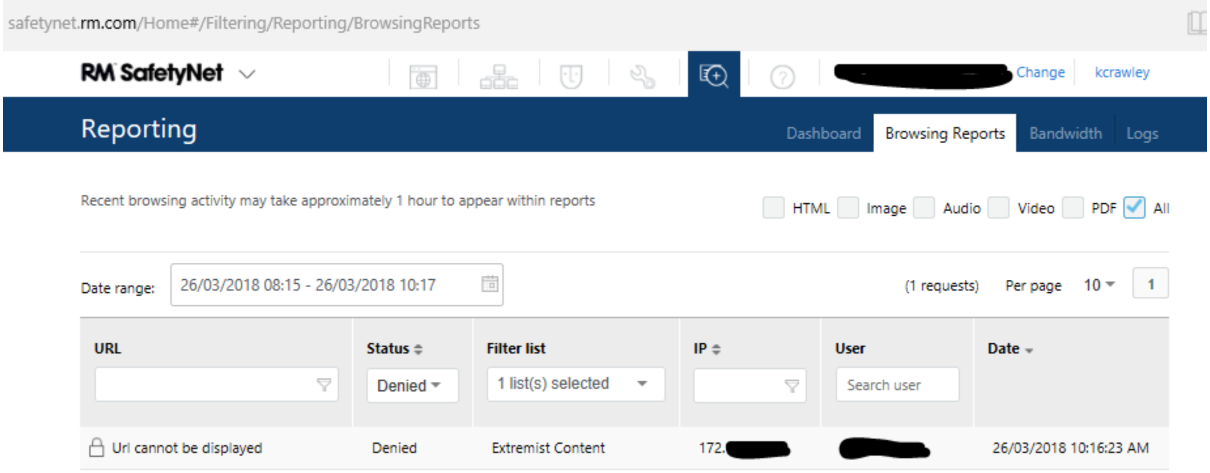
Alerts can also be triggered on the school's transparent proxy network, which is often used for bring your own device (BYOD) users. As the transparent proxy is segregated from the school's network, user identification will also be a problematic.

Steps for schools to carry out

Once notified by HfL, schools will need to log into the HICS filtering platform, RM SafetyNet to interrogate the proxy logs. To access RM SafetyNet, schools will need to browse to https://safetynet.rm.com and enter the required credentials. If the school does not have their credentials, then they will need to contact the HICS Service Desk either by phone: 01438 844777 (option 1 followed by option 2), or by email: help@sd.hertsforlearning.co.uk.

Along with this guide, in the body of the email, HfL will have also provided you the following:
1) The time and date that the activity was carried out
2) The internal IP address and/or Network user ID

Using this information, School/IT Support staff can log into RM SafetyNet to extract the relevant data. The steps to follow for investigating the report are for you to go to the 'Browsing Reports' tab, select the day/time window in question and select the ‘Extremist Content’ filter list. This will then bring back all of the details including IP, username for UBF etc – as shown below:



Recent browsing activity may take approximately 1 hour to appear within reports

□ HTML □ Image □ Audio □ Video □ PDF ☑ All

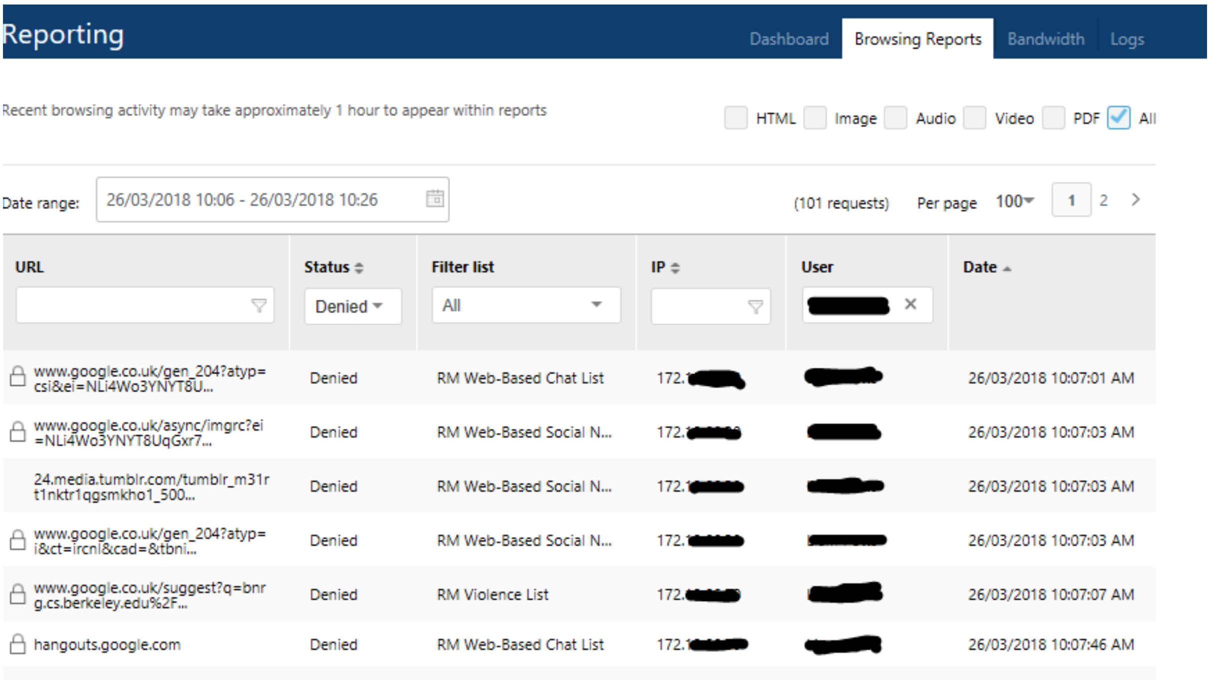
Date range: 26/03/2018 08:15 - 26/03/2018 10:17

(1 requests) Per page 10 1

URL	Status	Filter list	IP	User	Date
	Denied	1 list(s) selected		Search user	
Url cannot be displayed	Denied	Extremist Content	172.[redacted]	[redacted]	26/03/2018 10:16:23 AM

As mentioned above, if you have received an IWF alert, the report will not inform you on the content the IP address/user accessed that triggered the alert. You will then need to use the same reporting tool in RM Safetynet to check the activity of the IP address/user immediately before/after the alert was triggered. This should help put together a clearer picture as to what was being viewed before/after the time in question. For Prevent alerts the URL/keyword search will be visible.

Please note that when using the browsing reports tool in RM Safetynet, lots of activity is recorded. With this in mind, the more specific you can be in the search fields, the more the returned data will be relevant. When viewing the report you can hover over the URL result, copy it and then paste it into the address bar.



Recent browsing activity may take approximately 1 hour to appear within reports

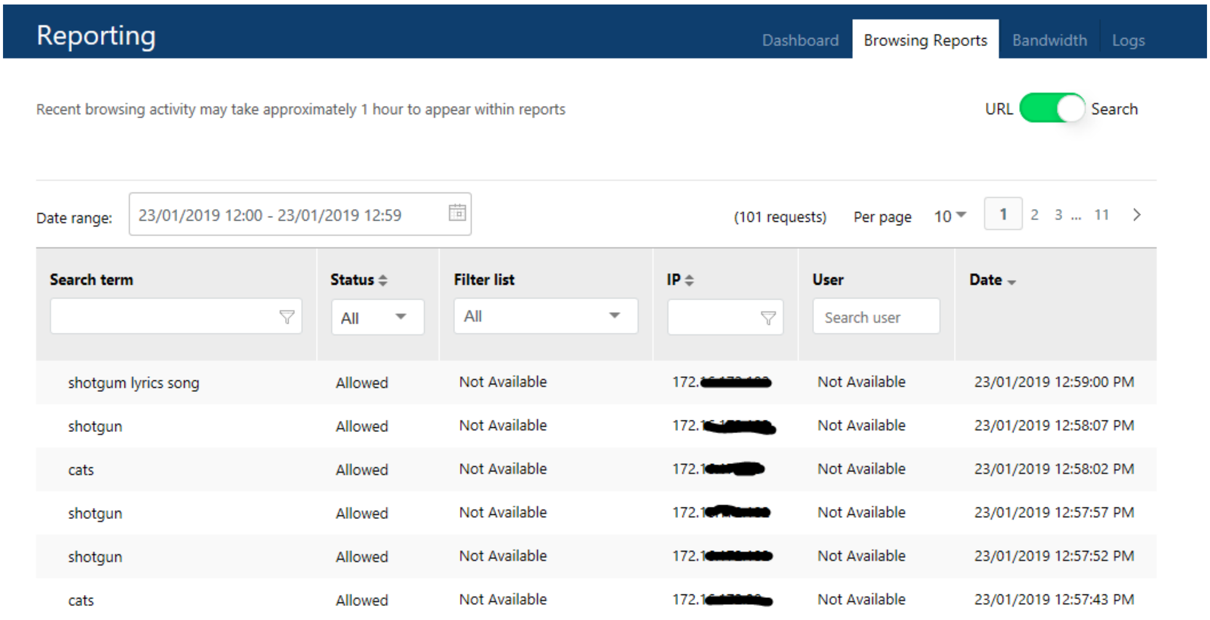
□ HTML □ Image □ Audio □ Video □ PDF ☑ All

Date range: 26/03/2018 10:06 - 26/03/2018 10:26

(101 requests) Per page 100 1 2 >

URL	Status	Filter list	IP	User	Date
	Denied	All		[redacted] ×	
www.google.co.uk/gen_204?atyp=csi&ei=NLi4Wo3YNYT8U...	Denied	RM Web-Based Chat List	172.[redacted]	[redacted]	26/03/2018 10:07:01 AM
www.google.co.uk/async/imgrc?ei=NLi4Wo3YNYT8UqGxr7...	Denied	RM Web-Based Social N...	172.[redacted]	[redacted]	26/03/2018 10:07:03 AM
24.media.tumblr.com/tumblr_m31rt1nktr1qgsmkho1_500...	Denied	RM Web-Based Social N...	172.[redacted]	[redacted]	26/03/2018 10:07:03 AM
www.google.co.uk/gen_204?atyp=i&ct=ircnl&cad=&tbni...	Denied	RM Web-Based Social N...	172.[redacted]	[redacted]	26/03/2018 10:07:03 AM
www.google.co.uk/suggest?q=bnrg.cs.berkeley.edu%2F...	Denied	RM Violence List	172.[redacted]	[redacted]	26/03/2018 10:07:07 AM
hangouts.google.com	Denied	RM Web-Based Chat List	172.[redacted]	[redacted]	26/03/2018 10:07:46 AM

At the top right-hand corner you can now, move the slider across from ‘URL’ to ‘Search’. The report will then provide details of searches the user/IP address has looked up, rather than listing all the URLs accessed. This can often be insightful:



Recent browsing activity may take approximately 1 hour to appear within reports

URL Search

Date range: 23/01/2019 12:00 - 23/01/2019 12:59

(101 requests) Per page 10 1 2 3 ... 11

Search term	Status	Filter list	IP	User	Date
	All	All		Search user	
shotgum lyrics song	Allowed	Not Available	172.[redacted]	Not Available	23/01/2019 12:59:00 PM
shotgun	Allowed	Not Available	172.[redacted]	Not Available	23/01/2019 12:58:07 PM
cats	Allowed	Not Available	172.1[redacted]	Not Available	23/01/2019 12:58:02 PM
shotgun	Allowed	Not Available	172.1[redacted]	Not Available	23/01/2019 12:57:57 PM
shotgun	Allowed	Not Available	172.1[redacted]	Not Available	23/01/2019 12:57:52 PM
cats	Allowed	Not Available	172.1[redacted]	Not Available	23/01/2019 12:57:43 PM

Advice

Should you have any further queries, please contact the HICS Service Desk either by phone: 01438 844777 (option 1 followed by option 2), or by email: help@sd.hertsforlearning.co.uk.

Additional reading from the HICS website

Setting up UBF - http://hics.hertsforlearning.co.uk/filtering/user-based-filtering/

Alerts - http://hics.hertsforlearning.co.uk/filtering/monitoring-alerts/

RM SafetyNet - http://hics.hertsforlearning.co.uk/filtering/rm-safetynet/