SurfProtect®

Analytics Guide

Issue 6.0
Oct.2022

Understanding Analytics

With monitoring now forming a key part of a school's online safety requirements, we have worked tirelessly to introduce these features to our SurfProtect content filtering service. If you have previously purchased a Stormshield device, you'll be aware that you have always had access to a degree of reporting and visibility, however our SurfProtect Quantum service brings this capability to every user - and also introduces additional, brand new, features. In this guide, we will take a look at exactly what you can see in the SurfProtect Quantum reporting panel.

How Does It Work?

Located entirely in the cloud, SurfProtect Quantum does not require an on-site device to be configured and installed - you are even able to receive AD integration by simply installing an AD proxy. In doing this, your AD server is able to communicate with SurfProtect; as a result, every time a user visits a website, attempts to access a banned site, searches for blocked material, or simply enters an allowed search term, we are able to record this activity - ensuring that you have complete visibility over the online activity of each and every user within the school.

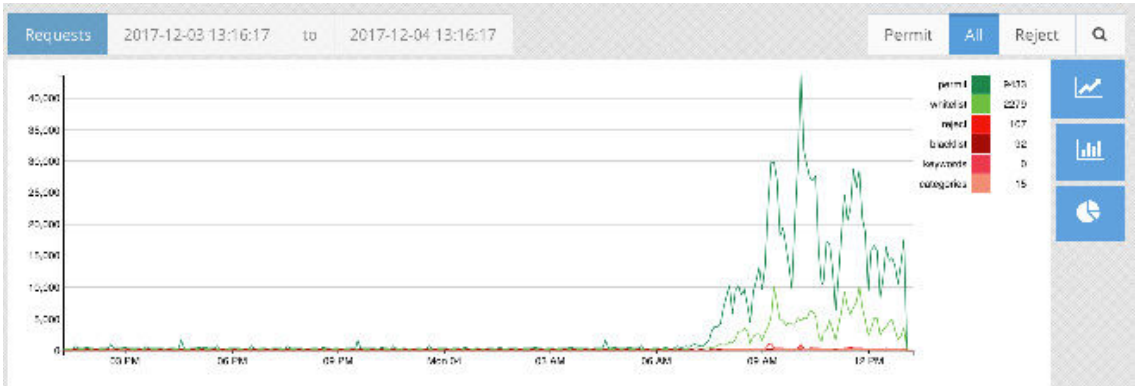
Our SurfProtect Fusion service utilises a Stormshield UTM device to provide AD integration, so this level of user reporting is also available to these schools.

If you do not wish to employ the AD integration aspect of SurfProtect Quantum you will still receive online analytics but will be unable to identify the individual user of any activity, and will instead only see the external IP an event is associated with.

So, what can you see?

The Big Picture

Upon logging into your SurfProtect Quantum panel, you will see a tab on the left hand side titled 'Website Analytics' - click on this, and you will be provided with a graphical overview of all activity performed on your school's internet connection in the previous twenty four hour period. This can then be selected to view filtered views of blocked, allowed, and complete traffic.



Key

- **Permit:** Websites and search terms which were allowed as they did not contain any restricted material or keywords
- **Whitelist:** Websites which have been explicitly allowed by the school
- **Reject:** The total number of all blocked requests
- **Blacklist:** Websites that the school has explicitly restricted access to
- **Keywords:** Search terms which contained words blocked by the school's 'Keyword' filtering
- **Categories:** Websites which were blocked as they belonged to a banned category

A Finer View

Beneath the graph, you will see a bar which provides a numerical representation of all activity performed over the last twenty four hours.

This is divided into four categories:

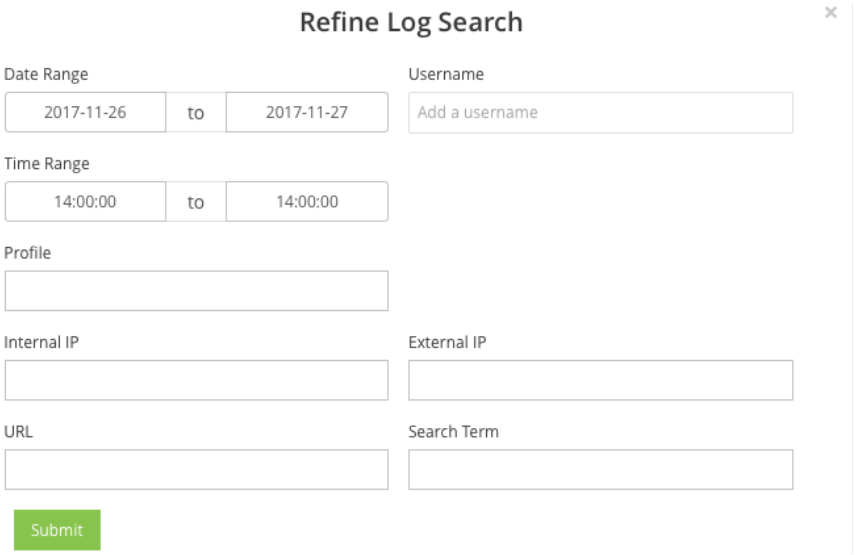
- **Activities:** This is where you will see every activity that has occurred; including every website requested, every download made, and every image viewed.
- **Unique Activities:** If a website or activity has occurred multiple times it will be listed here just once, providing you with a more concise view.
- **Searches:** Search terms entered into Google, or alternative search engines, will be visible here
- **Unique Searches:** If a search term has been entered multiple times, it will again be displayed here just once

Clicking on the relevant button will then provide a list of the individual actions within the category, and can again be filtered to display blocked, allowed, and complete traffic. For example, clicking on the 'Searches' tab and selecting 'Reject' as the filter will bring up a list like the one shown below:

Time	Username	Status	Host	Query	Profile		Decision Item
27-11-17 07:3...	emp	reject	www.google.c...	porn	students - Ext...	search terms	Keyword: porn
27-11-17 07:4...	cdh	reject	www.google.c...	aq	students - Ext...	search terms	Keyword: porn

As you can see, we are able to identify the time the incident took place, the term that was entered, the Keyword which caused it to be rejected and, if AD integration has been enacted, the user that performed the search and the AD profile they are associated with.

When viewing this list with AD integration, you may notice that an individual has performed a search which raises concern. If this should happen, you are able to filter the data records to only display their web activity over a specified period of time. This is done using the 'Refine Log Search' feature shown below.



You are also able to perform this search for multiple users or, alternatively, see all the activity performed under an AD profile - such as Students, or even find out who has been searching for a specific term or attempting to visit a banned site.

SurfProtect.co.uk | exa.net.uk | 0345 145 1234