



SurfProtect®

Panel Guide

The SurfProtect Panel Guide

Welcome to the all-new SurfProtect - even if you are a veteran SurfProtect user, you will still benefit from familiarising yourself with the interface with the help of this guide.

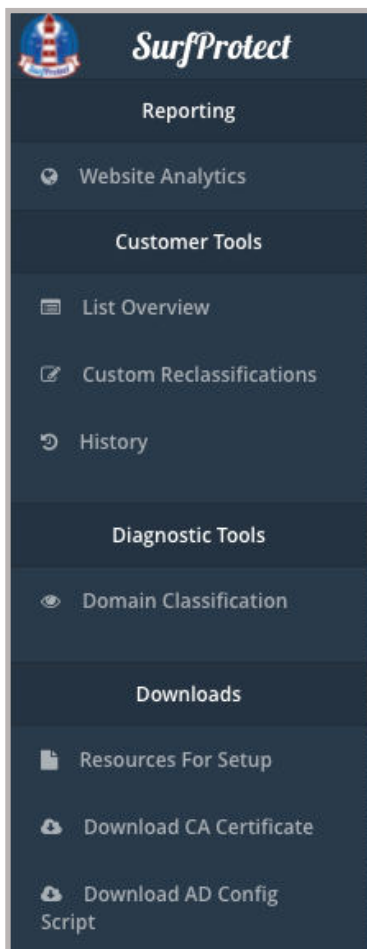
As always, if you require help with any aspect of your content filtering solution, please do not hesitate to get in touch.

Contents	Page
Login	3
Locations & Connections within a Location	4
Default Policies	4
Categories	6
Restricted Search Terms	7
Umbrella Behaviours	8
Search Engine Settings	8
Allowed / Blocked URLs	9
Video Site Settings	9
Content Types	10
Filtering Profiles	11
Using Lists across multiple Profiles	13
Profile Overview	14
List Overview	15
Custom Reclassifications	15
Diagnostic Tools - Domain Classification	16
Domain Doctor	16
List Subscriptions	17
Analytics	18

Log in!

Navigate to the SurfProtect administration panel by visiting panel.surfprotect.co.uk, or by visiting surfprotectpanel.exa.co.uk.

Once logged in you'll be presented with the landing page for most users; the filtering-locations overview.



General Navigation

Before explaining the content of your home page, let's take a moment to explain the navigation options which will be available as you move around your SurfProtect service.

The left side navigation is split into four sections:

- **Reporting**

This section will contain the available analytic tools for your SurfProtect service.

These tools are location agnostic, meaning you can view them whether you are in a location or not and that the content applies to all locations.

You can find more information about the reporting tools later in this guide. [Click here to jump to Reporting Tools.](#)

- **Customer Tools**

The section contains a number of quick navigation links, and filtering settings which apply to all locations such as customer reclassifications.

These tools are covered in more detail later in this guide. [Click here to jump to Customer Tools.](#)

- **Diagnostic Tools**

These tools allow you to find out why something was filtered a certain way. These tools generally require for you to have navigated into a Location or Profile within a Location for them to be available.

These tools are covered in more detail later in this guide. [Click here to jump to Diagnostic Tools.](#)

- **Downloads**

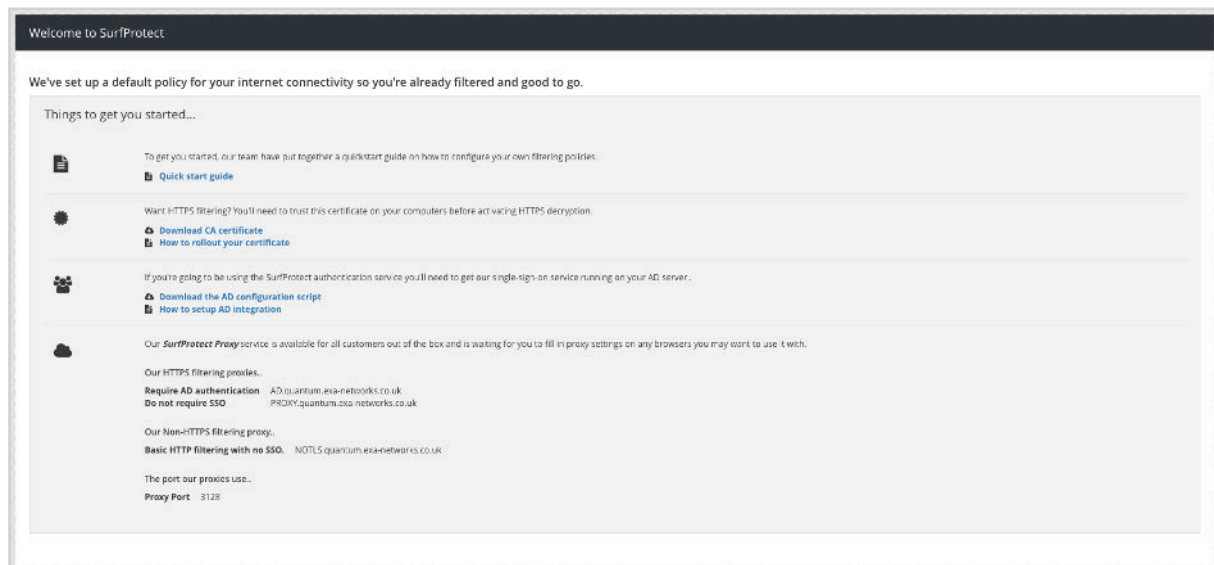
These are quick navigation links to the various resources for setting up and configuring your SurfProtect service. .

Locations Overview

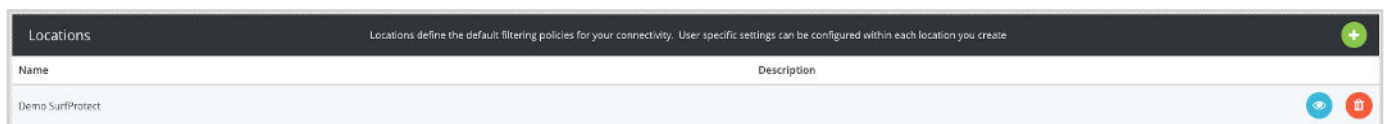
The locations overview is split into two separate sections:

The first portion of the page is dedicated to documentation and resources you will / might need to get your filtering up and running.

This includes proxy configuration settings, the SurfProtect certificate and resources to optionally set up Active-Directory filtering.



The second portion of the page is a list of the currently configured filtering locations:



A location is defined as a physical site. For the majority of customers there will just be one location which is the school. However, some schools may wish to define a separate location for other sites such as remote campuses or boarding dormitories. To add more locations, click the plus icon in the Locations header and follow the creation wizard which pops up.

Filtering policies are defined per location, however filtering lists are shared across all locations.


Viewing and managing a specific Location

Selecting to view a specific location from the location overview will take you to the overview for that specific location. This page is broken down into a number of sections:

- **Location & Profile specific tools**
When managing a location, and the profiles within it, there are a number of tools and features which become available:
 - Application Controls
 - Profile Comparison
 - Single Sign On data management

- **Services filtered by this location**

This section lists all connectivity services which are being filtered in this location.

Services filtered in this location		
Product type	Identifier	
DSL	EXA0002	

For many of our customers this will be just the one connection, however, if you have more than one connection (e.g. a back-up or an additional connection) they can be added easily by clicking the plus icon (so long as the connection is not already assigned to a location).

Add services to this location: Demo SurfProtect

Service Type	Service Identifier	
DSL	EXA0002	<input type="checkbox"/>

Add









- **Filtering Profiles**

Filtering profiles are split into two types, Overriding profiles and the Default profile.

The Default profile defines the default filtering policy for a location.

Default Filtering Profile	
Default filtering rules when no other profile is matched.	
Default Profile	

Overriding profiles define exceptions to the Default profile. For example you may want Teachers and Students to have different filtering policies applied to them.

Filtering profiles			
Tailored filtering for matched users and machines. Ordered in matching priority from top to bottom.			
Name	Description	Profile Type	Internal
Users profile	Matches specific users	User Name	 
Groups profile	Matches specific groups	Group Name	 
Internal IP profile	Matches specific internal IPs	Internal IP	 
External IP profile	Matches specific external IPs	External IP	 
Staff	The staff filtering profile	Group Name	 

Profiles, how they work and how to configure them are covered in more detail [here](#).

Configuring a Filtering Profile

When configuring a profile, either the default profile for a location or the overriding profiles, you will be presented with a number of distinct sections which define a profile.

Matching Rules

When configuring a profile, either the default profile for a location or the overriding profiles, you will be presented with a number of distinct sections which define a profile.

Matching rules		
Type	External Ip	
External IP	82.219.221.222	

When viewing a location's default profile these matching rules are replaced by a note that you are viewing the default filtering profile for the current SurfProtect location.

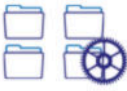
Note: Matching against Internal IPs, SSO usernames and SSO group names does require using certain SurfProtect setups which give SurfProtect access to that data. See the [section on SSO integrations](#) for more information on these solutions.

Policy Settings


These settings make up the core of a filtering profile, and are broken up into a number of manageable sections.

Policy for profile: Demo profile

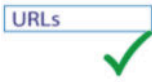
Control profile filtering rules.




Categories
Demo profile.




Umbrella Behaviours




Allowed URLs
Demo profile.




Blocked URLs
Demo profile.




Restricted Search Terms
Demo profile.




Search Engine Settings



Video site settings



Content Types



HTTPS Bypasses
No Filtering.

Categories

SurfProtect treats websites differently depending on how we have classified them. When a site is classified it will fall into a category such as Sports or Arts etc. A policy defining which categories are permitted or blocked on your connection is called a List.

Underneath the icon you will see which category List is currently assigned. By hovering over the icon you can then choose an alternative list to apply, remove all category filtering, or, edit the current list. Let's look at editing a list; hover over the icon and choose 'Edit'.

The first thing you will see is a list of categories that are blocked by your Umbrella Behaviour settings, the middle column displays the Umbrella Behaviour that the category falls under. For your protection these cannot be unblocked here and must be done on the Umbrella Behaviour page. Click on the Behaviour to jump straight to that page.

Lower down the page shows the Active Categories and their current status. You can change the status between Block and Allow by simply clicking the status indicator. You can also add in any categories from the Inactive Categories list on the right hand side by just dragging them over.

One of the biggest changes for our new SurfProtect product is the ability to order the list, this is made possible by an all-new classification system which allows for a website to have multiple classifications and this is where the ordering comes into play:

Let's take the ESPN website as an example. This website is classified as both Sports and News. It might be that you would like News sites to be accessible on your connection, but not general Sports sites. In this scenario you would place the category News above Sports and set the status to Allow for News and Block for Sports (see below). Now, SurfProtect will allow the page to be loaded as the first classification it matches in the list is News, which is permitted. However a site which is classified as Sports, such as nba.com will continue to be blocked as Sports is the first category in the list which nba.com matches.

Behaviourally Blocked			Review your behaviour policies to change these settings
Name	Behaviour	Status	
Illegal Drugs	Drugs	BLOCK	
Intolerance & Hate	Prevent	BLOCK	
Proxies / Translators	Privacy Filtering	BLOCK	

Active Categories		Prioritise categories to allow or restrict access to content
Name	Status	
Adult / Sexually Explicit	BLOCK	
Advertisements or Pop Ups	BLOCK	
Alcohol & Tobacco	BLOCK	
Criminal Activity	BLOCK	
Gambling	BLOCK	
Games	BLOCK	
Hacking	BLOCK	
Illegal Filesharing	BLOCK	
Intimate Apparel / Swimwear	BLOCK	
News	ALLOW	
Peer to Peer	BLOCK	
Personals & Dating	BLOCK	
Phishing / Online Fraud	BLOCK	
Ringtones / Mobile Downloads	BLOCK	
Social Networking	BLOCK	
Spam URLs	BLOCK	

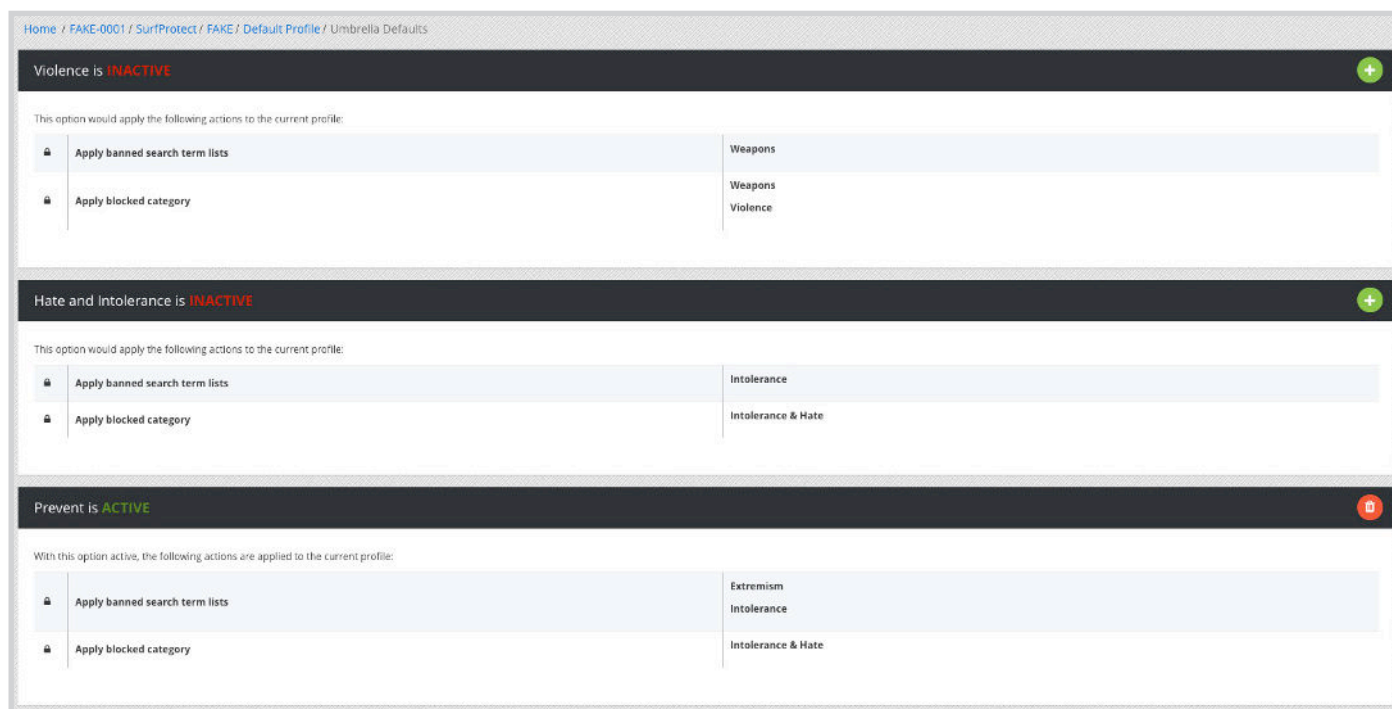
Inactive Categories		Drag to Active Categories to restrict access
Name		
Arts		
Business		
Chat		
Computing / Internet		
Downloads		
Education		
Entertainment		
Fashion & Beauty		
Finance & Investments		
Food & Dining		
Forums or Blogs		
Government		
Health & Medicine		
Hobbies / Recreation		
Hosting Sites		
ISP/Network Infrastructure		

Umbrella Behaviours


A new feature of SurfProtect is the ability to apply a group of settings in one click. For example, you can apply all relevant settings for 'The Prevent Duty' by simply clicking the 'Prevent' Umbrella Behaviour.

Click the icon to select the Umbrella Behaviours that apply to your policy.



The Umbrella page shows the available behaviours and their current status. It also shows you the search term categories and website categories that are applied by each Behaviour. You can easily toggle whether a Behaviour is Active or Inactive by clicking  or .




Home / FAKE-0001 / SurfProtect / FAKE / Default Profile / Umbrella Defaults



Violence is **INACTIVE** 


This option would apply the following actions to the current profile:

 Apply banned search term lists	Weapons
 Apply blocked category	Weapons Violence



Hate and Intolerance is **INACTIVE** 

This option would apply the following actions to the current profile:

 Apply banned search term lists	Intolerance
 Apply blocked category	Intolerance & Hate

Prevent is **ACTIVE** 

With this option active, the following actions are applied to the current profile:

 Apply banned search term lists	Extremism Intolerance
 Apply blocked category	Intolerance & Hate

Allowed URLs

There may be a time where websites that would normally be blocked by your filtering policies are legitimately required. Here you can override your other filtering policies and explicitly permit access to a web page or domain.

Underneath the icon you will see which Allowed List is currently assigned. Hovering over the icon lets you choose an alternative list, remove filtering, or, edit the current list. Let's look at editing a list; hover over the icon and choose 'Edit'.

Hit the  icon to add a URL to your allowed list.

Either add the site by typing (for example) `bbc.co.uk` or permit the entire domain by adding a '.' before - e.g. `.bbc.co.uk`

The search bar allows you to easily search through your allowed URL list, the search bar works in real-time and will search for strings of text as well as full words / sites.

Home / FAKE-0001 / SurfProtect / FAKE / Default Profile / FAKE

Subscriptions

Allowed URLs: FAKE URLs or hostnames listed here are explicitly accessible within the current profile, overriding any other content filtering policies.

URL		
.3dwarehouse.sketchup.com	List: Current list	
.afcmfo.co.uk	List: Current list	
.amplience.net	List: Current list	
.arts.ac.uk	List: Current list	
.asos.com	List: Current list	
.berkeley.edu	List: Current list	
.clickprotects.com	List: Current list	
.castletwater.co.uk	List: Current list	
.channel4.com	List: Current list	
.edu.sketchup.com	List: Current list	
.fermrs.net	List: Current list	
.ggpht.com	List: Current list	
.googletagmanager.com	List: Current list	
.googlevideo.com	List: Current list	

Blocked URLs

Blocked URLs work in much the same way as Allowed URLs above - you may become aware of a website that you do not want to be accessed on your connection - regardless of any filtering policies in place.

SurfProtect allows for inherited Blocked lists which are displayed at the top of this page. The shows you the sites belonging to the inherited list and the allows you to opt out. Note, the List remains there for you to opt back in at any time.

Hit the icon on to add a URL to your blocked list.

Either add the site by typing (for example) `bbc.co.uk` or to block the entire domain add a `'.'` before - e.g. `.bbc.co.uk`


The search bar allows you to easily search through your allowed URL list, the search bar works in real-time and will search for strings of text as well as full words / sites.



Restricted Search Terms

Further than the ability to block websites, SurfProtect can also affect particular parts of a site. Search Terms are indicative of this ability. Where Search Engine sites can be allowed, yet the input of inappropriate words can be blocked.

Underneath the icon you will see which Search Term List is currently assigned. By hovering over the icon you can then choose an alternative list to apply, remove all Search Term filtering, or edit the current list. Let's look at editing a list; hover over the icon and choose 'Edit'.

On the resulting screen you are shown the pre-populated groups of keywords at the top of the page, by default these are all active. To view the keywords that are restricted by each group you can click , to opt out of that category simply click . Groups that are inherited by Umbrella Presets cannot be opted out of and will display .

Below the groups are all the resulting restricted search terms, to add your own search terms simply click . You can add a single, or multiple terms by just hitting enter after each keyword. Any user added Search Term automatically gets grouped for your convenience under a 'User Added' group.

Manually added terms can be deleted from your list, however, terms that are inherited from the categories cannot be deleted but can be opted out of by clicking  and will show an 'opted out' status letting you opt back in at any time. Terms belonging to Umbrella Presets will show a  and cannot be opted out of.

Home / FAKE-0001 / SurfProtect / FAKE / Default Profile / FAKE

Weapons	Sex	Swearing	Extremism <small>Locked by: Prevent</small>
Intolerance <small>Locked by: Prevent</small>	Games	Drugs <small>Locked by: Drugs</small>	Inappropriate
Customer defined list			

Restricted Search Terms: FAKE

Search queries containing restricted keywords will be blocked

Item	Origin	Status
	List: Inappropriate	
	List: Inappropriate	
	List: Inappropriate	
	List: Inappropriate	
	List: Inappropriate	
	List: Inappropriate	
	List: Drugs	
	List: Drugs	
	List: Drugs	
	List: Drugs	
	List: Drugs	

Search Engine Settings

Here you can not only select your preferred Search Engine for your connection, but also decide whether to force your preferred search engine's Safe Search feature.

Hover over the icon to access the search engine menu.

Home / FAKE-0001 / SurfProtect / FAKE / Default Profile / searchsettings

Search Engine Controls		Restrict access to inappropriate content in web searches.
Preferred search engine	Disabled	
Search engine safe search	Active	

Search Engine Settings

Hover over the icon to access the menu, from here you can add your YouTube ID and force Safe Search to work seamlessly with YouTube videos.

Home / FAKE-0001 / SurfProtect / FAKE / Default Profile / video settings

Video settings		Add YouTube ID and safe search for video sites.
YouTube ID	Disabled	
Safe Search	Active	

Content Types

Another new feature of SurfProtect allows you to now control elements of content from being downloaded from the Internet. Whilst this is now a possibility, we believe that the default settings are ideal for most users.

The top section refers to External Resource Compatibility and you are given the option to Always Allow:

- **Style content types (css, icon and font files)**
These are the building blocks of websites, the default status is Inactive which means that the content will load if your other content-filtering settings permit that site from being displayed.
- **JavaScript files**
JavaScript is a commonly used Internet language, however can be used for malicious ends. Again, the default status is set to Inactive.

Note: By changing the status of either of these you are bypassing your current content-filtering policy and explicitly allowing this type of content to be downloaded regardless of their origin.

The lower section looks after the Security Safeguarding and allows you to Always Block the following, regardless of their origin:

- Flash files
- Macro Enabled Documents - including Macro enabled Word and Excel files
- Mobile Application Package Files - Android, Apple and Blackberry applications
- Archive Files - such as Zip, RAR and Tar files
- Executable Files - .exe and shell scripts

This can be particularly helpful to defend against harmful files that are disguised as legitimate programs and files.

Home / FAKE-0001 / SurfProtect / FAKE / Default Profile / Permitted Content		
External Resource Compatibility		
Always permit access to safe resources that affect the behaviour or appearance of websites.		
Action	Description	Status
Allow JavaScript files	Allow js files	Always Allow
Allow Style content types	Allow css files, icon files and font files	Inactive
Security Safeguarding		
Restrict access to content types that may be considered harmful to your computer.		
Action	Description	Status
Block archive files	Block ZIP, RAR and Tar files	Always Block
Block Executable Files	Block exe and shell scripts	Always Block
Block Flash Files		Inactive
Block Macro Enabled Documents		Inactive
Block Mobile Application Package Files	Block Android, Apple and Blackberry application package files	Inactive

HTTPS Bypasses

Further than the ability to allow websites, SurfProtect can also avoid decrypting traffic from HTTPS sites. HTTPS bypasses is a list of websites that will not be decrypted when using HTTPS, which is used to allow trusted sites to be accessed.

Note: Not decrypting requests from these URLs will result in certain features being disabled. Specifically, the query string will not be available if the request is bypassed.

Underneath the icon you will see which HTTPS Bypasses List is currently assigned. By hovering over the icon you can then choose an alternative list to apply, remove all Search Term filtering, or edit the current list. Let's look at editing a list; hover over the icon and choose 'Edit'.

On this screen you will be shown a table of bypassed sites. To add a new site to this list, press the {plus} and enter the site you would like to bypass. This works similarly to the allowed and blocked URL lists, where you can add the site by typing (for example) `bbc.co.uk` or permit the entire domain by adding a `.` before - e.g. `.bbc.co.uk`.

[illegible]

Advanced Policy Settings

The advanced policy settings contain the more powerful, behaviour changing tools.

Advanced Policy Settings

Decrypt HTTPS

Enabled

Decrypt HTTPS




This option allows you to toggle if HTTPS decryption happens when using this profile.

When this option is enabled then HTTPS requests are decrypted, allowing SurfProtect access to the entire URL, along with the data for the request itself.

When this option is disabled then HTTPS requests are not decrypted. This limits SurfProtect to only being able to see the hostname for a URL and removes the ability to read the data for the request itself. For search engines, this disables the ability to filter keywords.

Creating and working with Overriding profiles

As previously mentioned, an Overriding Profile is an exception to the filtering in the Default profile.

Filtering profiles			
Tailored filtering for matched users and machines. Ordered in matching priority from top to bottom.			
Name	Description	Profile Type	Internal
Users profile	Matches specific users	User Name	 
Groups profile	Matches specific groups	Group Name	 
Internal IP profile	Matches specific internal IPs	Internal IP	 
External IP profile	Matches specific external IPs	External IP	 

These profiles allow you to set up policies tailored more towards specific groups or scenarios, leaving the default profile as a catch all for anything that doesn't match the rules of an overriding profile.

When a location is initially created the section for overriding profiles will be empty. You can create an overriding profile by clicking the green plus icon, which will launch the profile setup wizard to guide you through the process.

Note: The ability to match Internal IP addresses, SSO usernames or SSO user groups requires certain SurfProtect setups to allow SurfProtect access to that data. See the [section on SSO integrations](#) for different solutions and what data each gives access to.

Profile Creation

1.

Create new Profile

Info Matching Policy Umbrella Finish

Lets start by describing your new profile.

Profile name: Staff

Profile description: The staff filtering profile

Start Next

The profile creation wizard makes adding profiles simple, starting by asking you to provide a profile name and optionally a description. In our example we are calling this new profile 'Staff'.

2.

Create new Profile

Info Matching Policy Umbrella Finish

Now that we've given it a name, We need to know how we'll match on this profile.

Profiles can be matched in four different ways:

☐ External IP
☐ Internal IP
☐ Username
☒ Group Name

Group: Group

Start Previous Next

After that you choose how requests will be matched against this profile. In our example we are creating a profile which will match the SSO groupname 'Staff'.

Note: Matching against Internal IPs, SSO usernames and SSO groupnames does require using certain SurfProtect setups which give SurfProtect access to that data. See the section on SSO integrations for more information on these solutions.

3.

Create new Profile

Info Matching Policy Umbrella Finish

The last thing we need to do is set up the filtering that will be applied to this profile.

Allowed URLs: Create New List Staff

Blocked URLs: Create New List Staff

Banned categories: Create New List Staff

Blocked search terms: Create New List Staff

Start Previous Next Finish

The next step is selecting which existing policy lists to apply to the new profile. By default when creating a new profile the Wizard will attempt to create a new set of lists with names matching the new profile, however you can choose to use already existing lists by selecting them from the dropdown boxes next to each list type.

These list choices can be updated within the profile later if you change your mind.

4.

Create new Profile

Info Matching Policy Umbrella Finish

The last thing we need to do is set up the filtering that will be applied to this profile.

Allowed URLs: Create New List Staff

Blocked URLs: Create New List Staff

Banned categories: Create New List Staff

Blocked search terms: Create New List Staff

Start Previous Next Finish

The final section of the Wizard is the Umbrella behaviours. A number of these behaviours are recommended and selected by default, however you can select any of the Umbrella behaviours you want to be applied to the new profile.

5.

Create new Profile

Info Matching Policy Umbrella Finish

Lets start by describing your new profile.

Profile name: Staff









Profile description: The staff filtering profile

Start Next

That's it, you can now click finish to finalise and create the profile.

Working with Overriding profiles

After creating an overriding profile you will be able to see it listed when viewing a location.

Filtering profiles			
Tailored filtering for matched users and machines. Ordered in matching priority from top to bottom.			
Name	Description	Profile Type	Internal
Users profile	Matches specific users	User Name	 
Groups profile	Matches specific groups	Group Name	 
Internal IP profile	Matches specific internal IPs	Internal IP	 
External IP profile	Matches specific external IPs	External IP	 
Staff	The staff filtering profile	Group Name	 

Each overriding profile has two options; selecting the eye will let you view and manage that profile and its policies. Selecting the bin icon will delete the profile.

The list of overriding profiles is hierarchical, when SurfProtect is matching a request against the currently defined profiles it will work through the available overriding profiles from top-to-bottom and try to match against the rules for each one. This order can be changed at any time by dragging a profile up, or down, into the desired position.

A newly created overriding profile is placed at the bottom of the list of overriding profiles.

For example, in the picture above, you would only match against the Staff profile if the request did not match the users in the user's profile, the groups in the groups profile, etc. If none of the matching rules are matched then the request will fall into the filtering provided by the default profile.

SurfProtect / Demo SurfProtect / Staff - Internal

Matching rules

Type


Group Name

Group Name


staff

Policy for profile: Staff


Control profile filtering rules.




Categories
Staff




Umbrella Behaviours




Allowed URLs
Staff




Blocked URLs
Staff




Restricted Search Terms
Staff




Search Engine Settings



Video site settings



Content Types



HTTPS Bypasses
No Filtering

Advanced Policy Settings

When viewing an overriding profile you will be presented with the same view as when viewing the default profile for a location. The only difference is the matching rules which allow requests to be matched against the given profile.

SurfProtect History

When any action is performed on your SurfProtect service we record it, along with all the information we have at the time such as the affected Location name or affected profile.

This information is visible from the History page, under the customer tools section of the left hand menu.

Each recorded action is shown like the example below:

Time	Action	Performer	Location	Profile	Component	Expiry Date	
2020-05-12 10:39:49	Category list: Add category	Exa Networks	-	-	Category list	-	
2020-05-12 10:39:49	Category list: Update category priority	Exa Networks	-	-	Category List	-	
2020-05-12 10:39:53	Category list: Update category state	Exa Networks	-	-	Category List	-	

This overview of historical actions is broken down into:

Time: The date and time the action occurred

Action: A short description of the action that was performed. The first item in our example affected a Category list and added a category to it.

Performer: This is the username which carried out the action.

Location: This is the name of the SurfProtect location in which the action was performed. If this is blank then the action was performed outside of a location or was not specific to being in a Location.

Profile: This is the name of the SurfProtect profile in which the action was performed. If the Profile name is available then the Location it is part of will also be available. If this is blank then the action was performed at the location level, outside of a Profile or was not specific to being in a Location.

Component: This is the specific feature of your SurfProtect service that was affected, in our example the affected components were all Category lists. This will be blank if nothing was affected, such as when creating new lists, locations, assigning lists to profiles, etc.

Detailed View

If you want to know more about a specific historical action, you can click on the view (eye icon) button at the end of the row, this will pop up the detailed view for that specific action.

History Detail

Action Info

Timestamp

2020-05-12 10:39:49

Action

Category list: Add category

Performer

Exa Networks

Change Info

Location

N/A

Profile

N/A

Component

Category list

Data Changed

List name

defaultbannedcatslist

Category Enabled

['news']

Category State

block

This detail view shows a historical action in three sections:

Action info

This section contains the date and time, the action description, and who performed the action.

Change info

This section contains the Location name, Profile name and affected component of your filtering service. As previously mentioned some or all of these may be blank depending on the action that was performed.

Data changed

This section contains the actual data related to the action performed. In the example given we can see that the Category list which was changed was the 'defaultbannedcatlist', the category affected was the 'News' category, and that category had its state set to the 'Block' state.

SurfProtect History

These tools allow for you to get an overview of the web activity that your SurfProtect service has filtered.

Website Analytics

The Website Analytics provides an overview of all web requests made within a queried time period, providing information about when it happened, who did it, what they did and what the filtering decision was.

This is broken down into a number of easier to digest sections:

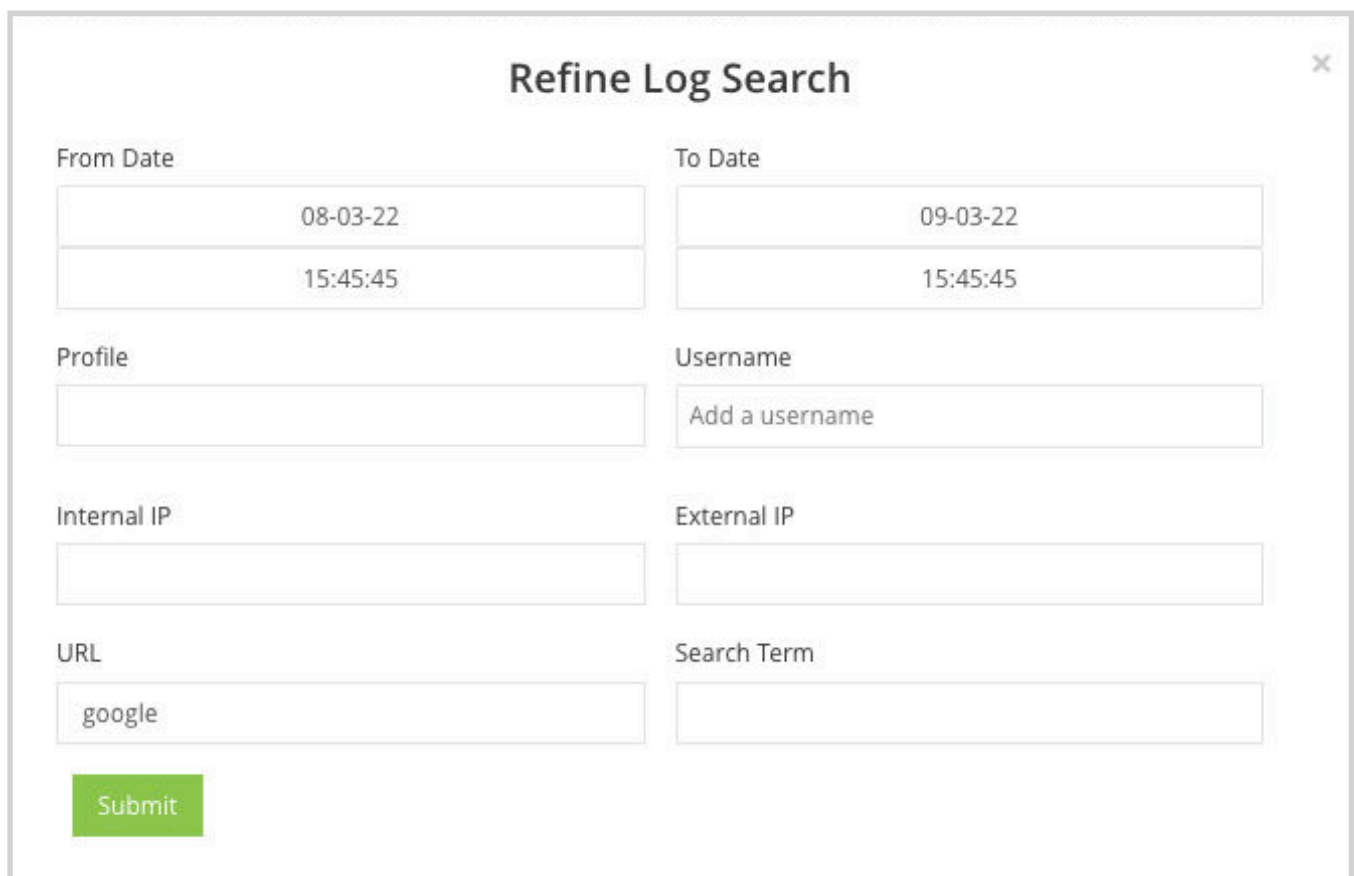
Query Options

These options allow you to filter the Analytics results to a more limited set of results.

A horizontal filter bar with four buttons: 'Permit', 'All', 'Reject', and a search icon. The 'All' button is highlighted in blue, while the others are light gray. The search icon is a magnifying glass.

The first three of these options are broad, quick filters which can be applied to the displayed results. By default, the 'All' filter is selected, which shows every request that has been filtered. Switching to the 'Permit' or 'Reject' filters shows only results which either have a Permitted or Rejected status.

The final option, the search icon, allows you to filter results in a much more granular way.

A 'Refine Log Search' dialog box with a close button (X) in the top right corner. It contains several input fields for refining search results:

- From Date:** A date field with '08-03-22' and a time field with '15:45:45'.
- To Date:** A date field with '09-03-22' and a time field with '15:45:45'.
- Profile:** An empty text input field.
- Username:** A text input field with the placeholder text 'Add a username'.
- Internal IP:** An empty text input field.
- External IP:** An empty text input field.
- URL:** A text input field with the text 'google'.
- Search Term:** An empty text input field.

A green 'Submit' button is located at the bottom left of the dialog.

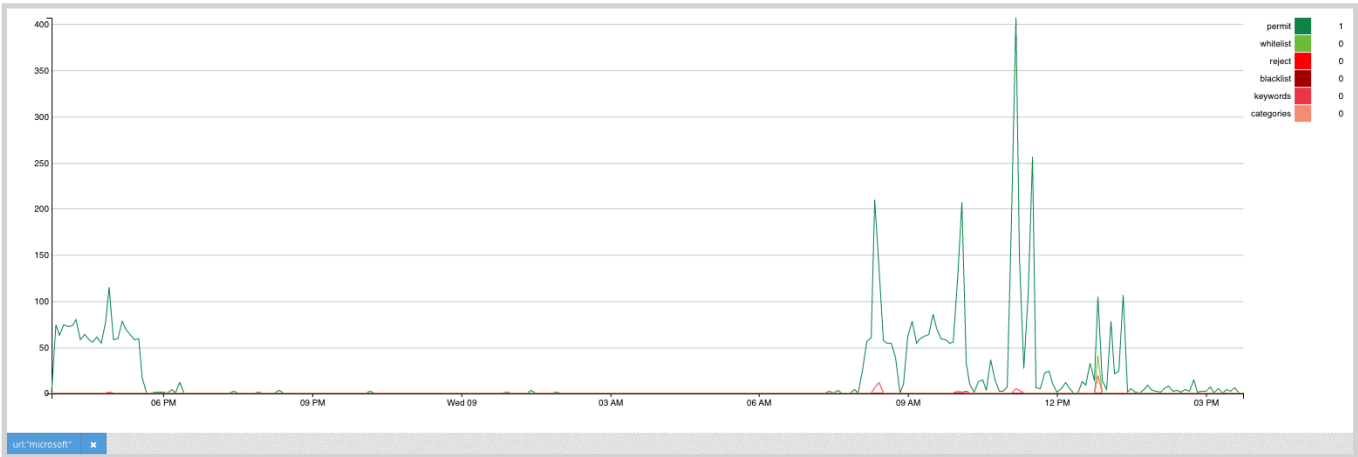
This allows you to filter results down to specific time periods, internal or external ips, users, etc. The 'All', 'Permit' and 'Reject' options can be enabled, which will limit the results further to these specific statuses.

When these more advanced filters have been set, you can see them listed beneath the activity graph.

Activity Graph

This graph shows the rate of filtered requests over the queried time period. Requests are grouped into five-minute intervals so that the volume of traffic being generated over these time periods can be more easily visualised at high resolution.

The data in this graph shows permitted and rejected requests independently, however currently it is not possible to filter these results further and will not update to match the filters that are set.



Activity Log

The final section of this page is the Activity logs themselves, which show data about every filtered web request that has been handled by your SurfProtect service. These logs are split into four tabs of data:

566 Activities		74 Unique Activities		0 Searches		0 Unique Searches	
Time	Username	External/Internal IPs	Status	URL	Profile	Decision Match	Decision Item
09-03-22 15:44:52		82.219.212.5 0.0.0.0	permit	http://detectportal.firefox.com/success.txt?pv4	Default Profile		
09-03-22 15:44:52		82.219.212.5 0.0.0.0	permit	http://detectportal.firefox.com/canonical.html	Default Profile		
09-03-22 15:44:52		82.219.212.5 0.0.0.0	permit	http://detectportal.firefox.com/success.txt?pv4	Default Profile		
09-03-22 15:44:46		82.219.212.5 0.0.0.0	permit	http://settings-win.data.microsoft.com/	Default Profile		
09-03-22 15:42:29	support	82.219.212.5 10.12.33.4	permit	http://edge.microsoft.com/	Default Profile		

Activities

This is the most granular set of logs, showing every request in the order it happened during the queried time period, limited to the query filters set by the user.

Unique Activities

This is an alternative view of the Activities logs. In this view you can see all of the unique activities, how many times each has happened, when it first occurred and when it last occurred within the queried time period. Some information is not shown here, like usernames, as this view is focused on the number of occurrences rather than the specific logs.

Searches

This is a view of all the requests seen by the filtering where an identifiable search query was found, again limited to the queried time period and query filters.

Unique Searches

This is an alternative view of the Searches logs. In this view you can see all of the unique searches which were performed, how many times each has happened, when it first occurred and when it last occurred within the queried time period. Some information is not shown here, like usernames, as this view is focused on the number of occurrences rather than the specific logs.

Customer Tools

Profile Overview

Located in the customer tools section of the left hand navigation menu, the Profile overview tool is accessible from any page within a SurfProtect location. This tool directly compares your settings across the current location, comparing all overriding profiles and the Default Profile to each other.

In the image below, we have the Comparison mode active, which aids you by highlighting differing settings. The mouse is on the External IP Profile column and Violence row - showing an Active status. The contrasting results (Inactive) are highlighted in red for you.

Profiles overview						
Here you can view the policy overview for the current location and its child profiles in one go						
Comparison mode						
<input checked="" type="checkbox"/> Enabled <input type="checkbox"/>						
Turning on comparison mode allowed you to either:						
• Mouse over the location / profile names to see where the location / other profiles differ from the currently hovered one.						
• Mouse over a policy component, the Allowed URLs, Banned categories, to see where the location / other profiles have different setting or no filtering.						
	Default Profile	User Name Users profile	Group Name Groups profile	Internal IP Internal IP profile	External IP External IP profile	Group Name Staff
Policies						
Allowed URLs	defaultallowedlist	Users profile	Groups profile	Internal IP profile	defaultallowedlist	Staff
Blocked URLs	defaultblockedlist	Users profile	Groups profile	Internal IP profile	External IP profile	Staff
Banned Categories						
Blocked Search Terms	defaultblockedwords	Users profile	Groups profile	Internal IP profile	External IP profile	Staff
Behaviors						
Adult	Active	Active	Active	Active	Active	Active
Drugs	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive
Hate And Intolerance	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive
Prevent	Active	Active	Active	Active	Active	Active
Proxy Filtering	Active	Active	Active	Active	Active	Active
Violence	Active	Inactive	Inactive	Inactive	Active	Inactive
Wall of Garden	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive
Youtube settings						
Youtube For Schools ID						
Safe Search	True	True	True	True	True	True
Search settings						
Safe Search	Active	Active	Active	Active	Active	Active
Preferred Search Engine						

Application Controls

Located in the customer tools section of the left hand navigation menu, the Application controls tool is accessible from any page within a SurfProtect location. This tool contains a number of known applications / services which do not always function correctly when being filtered by SurfProtect, and allows you to enable a control which applies known 'fixes' to the application / service.

SurfProtect / Demo SurfProtect / Application control

Application Control

This page allows for the management of applications which do not function correctly when used within a filtered environment.

These issues can happen for a number of reasons, for example:

- Certificates not being trusted
- TLS errors

The following application controls can be used to make these applications work, however doing so may affect filtering for the application. More details on what may be affected can be found on each application control.

Application Name	Application Description	Enable / Disable Control
Anti-Virus & Security		
Sophos		<input checked="" type="checkbox"/>
Google Services		
Google Earth	Bypasses authentication and TLS decryption for some backend google services. Also affects: maps.google.com	<input type="checkbox"/>
Googlevoice	Bypasses authentication and TLS decryption for some backend google services. Bypasses TLS decryption for www.google.com	<input type="checkbox"/>
IM & Messaging		
Skype	Bypasses authentication for related services accessed over HTTP	<input type="checkbox"/>
Slackapp	Bypasses authentication and TLS decryption for backend services.	<input type="checkbox"/>
Microsoft Services		
Iamcloud		<input type="checkbox"/>
Microsoftstore		<input type="checkbox"/>
Misc Services		
Bathspavle		<input type="checkbox"/>
Doodlemaths		<input type="checkbox"/>
Envoyapp		<input type="checkbox"/>

List Overview

Earlier in this guide it was mentioned that policy lists, such as Allowed URLs, are independent from Profiles and Locations.

Located in the customer tools section of the left hand navigation menu, the list overview allows you to manage your existing lists, or create new ones. New lists can be created using the plus icon at the top of the relevant section. This page does not allow you to assign lists to profiles, to do that you will need to navigate to the profile itself.


SurfProtect / List Overview

Allowed Lists		Blocked Lists	
Name	Description	Name	Description
defaultallowedlist		defaultblockedlist	
Users profile		Users profile	
Groups profile		Groups profile	
External IP profile		External IP profile	
Internal IP profile		Internal IP profile	
Staff		Staff	
Category Lists		Search Term Lists	
Name	Description	Name	Description
defaultbannedcatslist		defaultblockedwords	Default list of blocked search words
Users profile		Users profile	
Groups profile		Groups profile	
External IP profile		External IP profile	
Internal IP profile		Internal IP profile	
Staff		Staff	

Customer Reclassification

Located in the customer tools section of the left hand navigation menu, the Customer Reclassification tool allows you to set your own URL classifications or update existing reclassifications you have already made.

SurfProtect / Reclassifications	
Customer reclassifications	
Domain	Customer Classification
www.exa.net.uk	ISP/Network Infrastructure


For existing reclassifications, clicking on the edit (pencil) icon will allow you to change the classification for the chosen URL. Clicking the delete  button will remove the reclassification.

Add Domain Classification

Domain:

Category:

Please select a classification

For existing reclassifications, clicking on the edit (pencil) icon will allow you to change the classification for the chosen URL. Clicking the delete  button will remove the reclassification.

To view the existing classification for a URL, you will need to use the Domain Classification tool.

Diagnostic Tools

Domain Classification

Accessible on any page, this pop-up allows for you to check a domain's classification.

View domain classification

Domain:

SurfProtect default

Category: Computing / Internet, ISP/Network Infrastructure

Matching Domain: www.exa.net.uk

SurfProtect Solutions

A number of solutions exist for SurfProtect, the features of each solution are listed and compared below. Below is an example URL, and a breakdown of it, to help explain the abilities of each SurfProtect solution.

http://www.exa.net.uk/example_url?query=exa

Scheme: <http://>
Hostname: www.exa.net.uk
Path: [/example_url](http://www.exa.net.uk/example_url)
Querystring: [?query=exa](http://www.exa.net.uk/example_url?query=exa)

Quantum

The primary Surfprotect offering. This solution provides all standard SurfProtect filtering features.

As long as HTTPS decryption has not been disabled then both HTTP and HTTPS traffic will be filtered using the entire URL, hostname + path. With full HTTPS decryption SurfProtect is also able to extract search terms from the Querystring of the URL.

Quantum+

The upgraded version of the SurfProtect Quantum solution. This provides a number of additional features over the standard Quantum solution, including Captive Portal, VPN and SurfProtect Anywhere.

One key difference is that External IP matching does not happen if using the VPN feature, which allows SurfProtect to always know what internal IP address a request originated from.

SurfProtect SSO Integration

When using the SurfProtect Quantum and Quantum+ solutions a number of options are available to integrate SSO with SurfProtect.

Active Directory

Allows for integration with an Active Directory service.

This requires installation on the AD server itself and the use of the SurfProtect AD proxy.

The details for this setup can be found in the [AD setup guide](#).

Captive Portal

Requires SurfProtect Quantum+

Allows for integration with Active Directory, Google SSO and Azure Active Directory.

This requires installation on the AD server itself for AD integration, and setup on the SurfProtect panel to integrate with Google SSO and Azure AD.

The details for setting up Captive Portal for AD can be found in the [AD setup guide](#).

Notes...

Notes...





Exa Networks, Exa Education and SurfProtect are registered trademarks of Exa Networks Limited.

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