



User Guide

Overview

SurfProtect™ is a real-time web-site filtering system designed to adapt to your particular needs.

SurfProtect's main advantage over many rivals is its unique architecture that provides real-time classification of any unknown site, ensuring a safe and responsive browsing experience.

The experience can be further improved by making use of the website classification procedure which allows you to select the type of websites you want to block and which ones you want to continue having access to.

By default, SurfProtect™ automatically limits access to a reasonable standard; you may not need to change anything. However, if you want that extra control, you can.

SurfProtect™ Control Panel

In order to tailor your service to your access requirements, the first step required is to login to the SurfProtect™ control panel. You can access the login panel by clicking here: [Click Here - panel.surfprotect.co.uk](http://panel.surfprotect.co.uk).

You will be presented with a login facility which will ask you for your username and password.

These details should have been given to you already by your sales contact, if you do not have them please contact our sales or technical team on 0845 145 1234.

The SurfProtect™ setup is controlled by the menu which is shown at the top of the browser.

A screenshot of the SurfProtect login interface. It features the SurfProtect logo on the left and the Exa Networks logo on the right. The text reads: 'Access the web your way!', 'SurfProtect™, a centralised web content filtering solution', and 'Please login to use surfprotect'. Below this is a form with 'Username' and 'Password' labels, two input fields, and a 'Login' button.

Access the web your way!

SurfProtect™, a centralised web content filtering solution

Please login to use surfprotect

Username

Password

Login



Profiles

To change the default configuration, the first step is to set up a number of profiles. One profile for each different filter configuration.

e.g. You may require for example three, one for each of the following areas: Main School, Nursery, Staff Network

The configuration of each profile allows you to define a specific range; or ranges, of IP addresses that will then have each profiles filtering options. This allows you to enforce the policies as required. e.g. on a site by site basis or based on job function.



To create a new profile name, type a unique name into the empty box and click on the 'Create New Profile' button. Once you have created a new profile, it will be visible in the list.

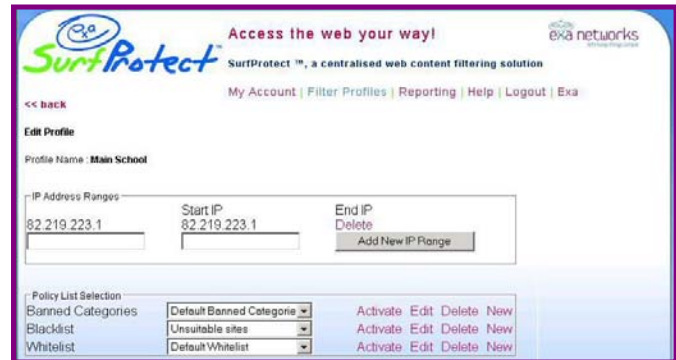
You can then select the 'Edit' link to administer each profile. Alternatively if you have entered the profile name incorrectly or it is no longer required, you can select the 'Delete' link to remove the item from the list.

Profile Administration

The profile administration screen is split into two sections.

The first section, allows you to specify the IP addresses that you want to be affected by your chosen profile.

You are only permitted to enter IP's within your own IP address ranges. If you have difficulty adding IP addresses please contact Exa Networks and we will resolve your problem.



In the second section, the profiles splits into three categories:

- | | |
|-------------------|---|
| Banned Categories | The Automatically Banned Sites based on Classification Settings |
| Black Lists | Your specific list of Banned Sites |
| White Lists | Your specific list of Permitted Sites |

One of the benefits of SurfProtect™ is that when a web page is requested page is classified automatically. Since the categorisation of certain types of content as either good or bad can be extremely subjective, it may be dependant on the particular user or group accessing it. The Black and White Lists provide you with the ability to grant or deny access to sites, this overrides the default behaviour of SurfProtect™ for the defined sites.

There is no limit to the number of lists you can create with the 'Create New List' button, but only one of each type can be active on a profile at any one time.

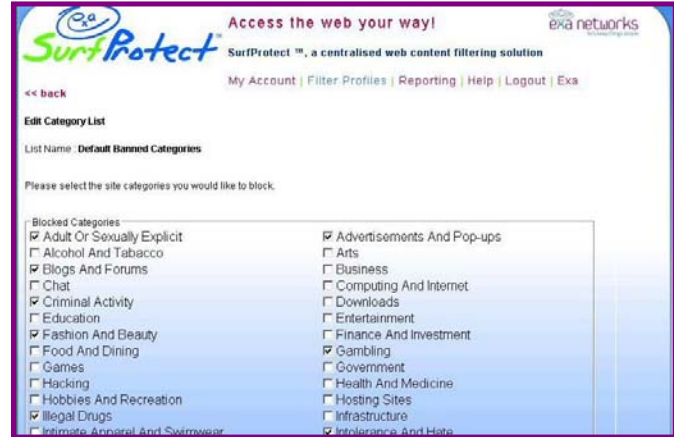
You can apply the same list simultaneously to as many profiles as you wish.



Category Lists

The category administration page shows a list of the current categories that can be selected or not. If a category has a tick next to its name, that category of sites will be blocked by SurfProtect™.

To change the current list of sites that are banned, please select or deselect each of the relevant tick boxes and then press the 'Save Categories' button.



Black and White Lists

As mentioned above, the Black and White lists, provide you with more control control than the website automatic categorisation of permitted sites.

Adding a website URL to an active White List will override the normal categorisation rules and permit access to the site. Alternatively adding to the Black List will deny access to the site.

Any existing websites will appear in the list, you can then add and remove websites from the list as you require.

Each website URL must appear on a separate line.

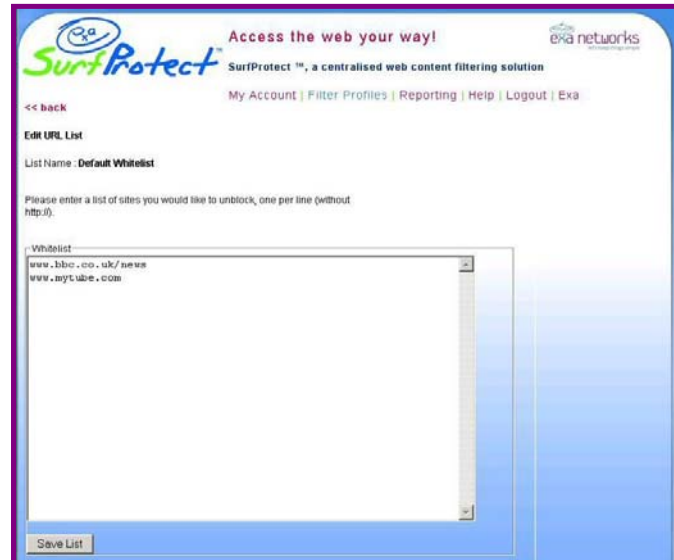
Also, blocking a higher level domain will automatically block the lower levels.
e.g.

somedomain.com

will also block:

images.somedomain.com
graphics.somedomain.com

Clicking on the 'Save List' button will store any changes you have made.





Proxy Support

One of the most attractive properties of SurfProtect™ is its plug and play nature. Sitting in between your internet connection and the remote web server, it can protect every host on your network without the need for any extra configuration on your behalf.

More important than the obvious convenience provided is the added security this introduces; there are no configuration options or software to be installed on your hardware.

There may, however, be situations where you would like the benefits of SurfProtect™ but you are not on a connection purchased through Exa Networks.

For such a scenario, we have a HTTP proxy server which any popular web browser or proxy can be configured to use to request its web pages. Please talk to us if this is something you think you may want to use.