

# SURFPROTECT

## 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.

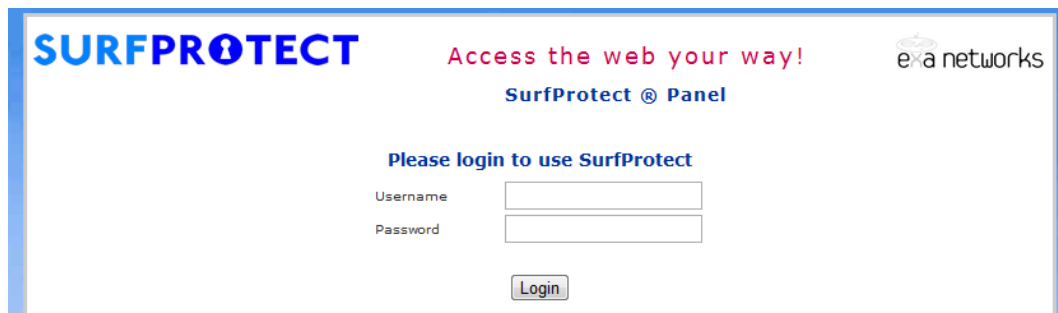
By default, SurfProtect® automatically limits access to a reasonable standard; you may not need to change anything. However, if you want that extra control, you can.

### SurfProtect® Control Panel

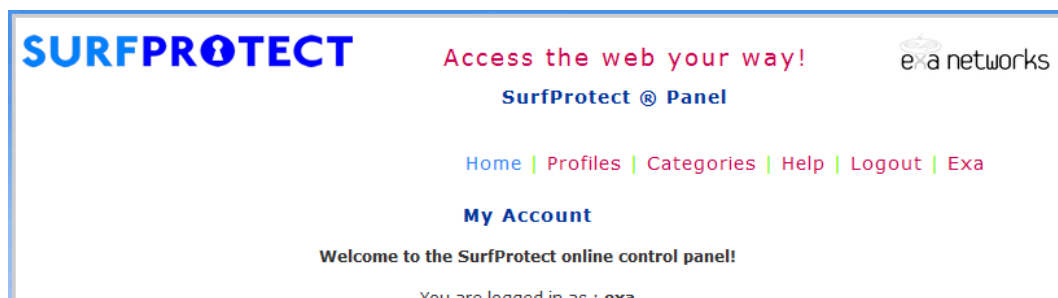
In order to tailor your service to your access requirements, the first step required is to login to the SurfProtect® control panel. You can access the login panel by clicking here: [Click Here](#) - [panel.surfprotect.co.uk](#).

You will be presented with a login screen 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**.



Setup of SurfProtect® is controlled by the menu which is shown at the top of the browser after logging in.



# SURFPROTECT

## 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 two, one for each of the following areas: Staff and Pupil Networks

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.

The screenshot shows the SurfProtect web interface. At the top left is the SurfProtect logo, and at the top right is the Exa Networks logo. The main heading is "Web Filtering Profiles". Below this, there is a text block explaining that web filtering profiles are the first step to configuring SurfProtect. A form with a text input field containing "<profile name>" and a "Create New Profile" button is visible. Below the form is a table with the following data:

Profile Name	Internal IP Range (Enabled)	Options
Pupil	Yes	<a href="#">Edit</a> <a href="#">Delete</a>
Staff	No	<a href="#">Edit</a> <a href="#">Delete</a>

The profile selection screen indicates if you have included any internal address ranges against a particular profile – this indicates that you are using the Internet Content Adaptation Protocol (ICAP) option with SurfProtect®.

The ICAP option enables SurfProtect® to apply settings to individual private range addresses from the customer's network.

## Profile Administration

<< back

Edit Profile

Profile Name : Staff

Change Profile Name

Update

Public Address Ranges

Start IP	End IP	
82.219.205.104	82.219.205.111	Delete
82.219.211.40	82.219.211.40	Delete

Add New IP Range

Public Policy List Settings

Banned Categories	staffBCats	Activate	Edit	Delete	New
Blocked List	StaffBlockedList	Activate	Edit	Delete	New
Allowed List	StaffAllowedList	Activate	Edit	Delete	New

Internal Address Ranges

Start IP	End IP	
10.0.0.1	10.0.0.50	Delete

Add New IP Range

Valid Private Network IP Address Ranges

10.0.0.0 - 10.255.255.255  
172.16.0.0 - 172.31.255.255  
192.168.0.0 - 192.168.255.255

Internal Policy List Settings

Banned Categories	staffBCats	Activate	Edit	Delete	New
Blocked List	StaffBlockedList	Activate	Edit	Delete	New
Allowed List	StaffAllowedList	Activate	Edit	Delete	New

The profile administration screen is split into three sections.

The first section allows you to adjust the name for the profile you are editing. Simply type the new name and select the 'Update' button to save the change.

The second section, allows you to specify the Public IP Address Ranges that you want to be affected by your chosen profile.

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

Below the Public IP Ranges are the options to configure the filtering to apply to the listed Public addresses

Banned Categories	The Automatically Banned Sites based on Classification Settings
Blocked Lists	Your specific list of Banned Sites
Allowed 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 Allowed and Blocked Lists provide you with the ability to grant or deny access to sites, this overrides the default behaviour of SurfProtect® for the defined sites.

**After you have selected a list from any of the drop down lists – please remember to select the 'Activate' link to make that list live before you leave the Edit Profile web page.**

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.

# SURFPROTECT

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

Below the 'Public Address Ranges' section is the 'Internal Address Ranges' section which should only be configured if you are using our ICAP option with SurfProtect®.

Please consult Exa Networks to check if this is the case.

If you are using this option it will be possible to better control your web traffic by internal network IP addresses.

In the example screen shot on the previous page the user has indicated that any web activity requests from the internal network for the range 10.0.0.1 – 10.0.0.50 will apply the selected 'Staff' based lists rather than the Public IP Range lists referred to as 'default.'

Now to control the Pupil access we would create a similar profile as shown below which has 2 differences to the previous profile – different Internal Address Ranges and different internal lists selected.

If you are using a non-standard internal IP range – the IP address will be displayed in red to bring it to your attention.

[<< back](#)

**Edit Profile**

Profile Name : Pupils

**Change Profile Name**

**Public Address Ranges**

Start IP 82.219.211.40	End IP 82.219.211.40	<a href="#">Delete</a>
82.219.205.104	82.219.205.111	<a href="#">Delete</a>

**Public Policy List Settings**

Banned Categories	<input type="text" value="pupilBCats"/>	<a href="#">Activate</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">New</a>
Blocked List	<input type="text" value="PupilBlockedList"/>	<a href="#">Activate</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">New</a>
Allowed List	<input type="text" value="PupilAllowedList"/>	<a href="#">Activate</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">New</a>

**Internal Address Ranges**

Start IP 10.0.0.51	End IP 10.0.0.100	<a href="#">Delete</a>
-----------------------	----------------------	------------------------

**Valid Private Network IP Address Ranges**

10.0.0.0 - 10.255.255.255  
172.16.0.0 - 172.31.255.255  
192.168.0.0 - 192.168.255.255

**Internal Policy List Settings**

Banned Categories	<input type="text" value="pupilBCats"/>	<a href="#">Activate</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">New</a>
Blocked List	<input type="text" value="PupilBlockedList"/>	<a href="#">Activate</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">New</a>
Allowed List	<input type="text" value="PupilAllowedList"/>	<a href="#">Activate</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">New</a>

If for any reason you have internet access from your network that is not providing an internal IP address to SurfProtect®, the Public Address Ranges Policy lists will still be in force as a safe guard.

Any internal IP presented to SurfProtect® that is NOT against a profile will have the recommended banned categories applied as a safe guard – these categories are shown in the next section on Category Lists.

# SURFPROTECT

## Category Lists

The category administration page shows two lists 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®.

There are two lists – “Recommended Banned Categories” and “Other Categories”. The first section of categories are more commonly used and so there are two buttons to aide in selection of these categories – ‘Select All’ and ‘Deselect All’. The categories in this section are the default categories used when you have a profile and have not selected ANY categories to ban. These categories will be applied by default for your protection. A note at the top of the screen has been added to remind customers of this fact.

**Edit Category List**

List Name : pupilBCats

Please select the site categories you would like to block.  
Access to any site classified under the following categories will be restricted until this section is configured with at least one category to block.

**Please note that when you have created a profile and have selected no categories, the items shown in the Recommended Banned Categories section will apply.**

Blocked Categories

**Recommended Banned Categories**

<input checked="" type="checkbox"/> Adult / Sexually Explicit	<input checked="" type="checkbox"/> Advertisements Or Pop-Ups
<input checked="" type="checkbox"/> Alcohol & Tobacco	<input checked="" type="checkbox"/> Criminal Activity
<input checked="" type="checkbox"/> Gambling	<input checked="" type="checkbox"/> Hacking
<input checked="" type="checkbox"/> Illegal Filesharing	<input checked="" type="checkbox"/> Intimate Apparel / Swimwear
<input checked="" type="checkbox"/> Peer To Peer	<input checked="" type="checkbox"/> Personals & Dating
<input checked="" type="checkbox"/> Ringtones / Mobile Downloads	<input checked="" type="checkbox"/> Social Networking
<input checked="" type="checkbox"/> Spam URLs	<input checked="" type="checkbox"/> Tasteless & Offensive
<input checked="" type="checkbox"/> Violence	<input checked="" type="checkbox"/> Weapons
<input checked="" type="checkbox"/> Google (and others) Safe Search	<input checked="" type="checkbox"/> Block Proxy Scripts
<input checked="" type="checkbox"/> Communication Url Rewriting	<input checked="" type="checkbox"/> Illegal Drugs
<input checked="" type="checkbox"/> Intolerance & Hate	<input checked="" type="checkbox"/> Phishing / Online Fraud
<input checked="" type="checkbox"/> Proxies / Translators	<input checked="" type="checkbox"/> Spyware
<input checked="" type="checkbox"/> Virus Worm Infected	

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.

**Other Categories**

<input type="checkbox"/> No Classification	<input type="checkbox"/> Arts
<input type="checkbox"/> Forums Or Blogs	<input type="checkbox"/> Business
<input type="checkbox"/> Chat	<input type="checkbox"/> Computing / Internet
<input type="checkbox"/> Downloads	<input type="checkbox"/> Education
<input type="checkbox"/> Entertainment	<input type="checkbox"/> Fashion & Beauty
<input type="checkbox"/> Finance & Investments	<input type="checkbox"/> Food & Dining
<input checked="" type="checkbox"/> Games	<input type="checkbox"/> Government
<input type="checkbox"/> Health & Medicine	<input type="checkbox"/> Hobbies / Recreation
<input type="checkbox"/> Hosting Sites	<input type="checkbox"/> ISP/Network Infrastructure
<input type="checkbox"/> Job Search / Career Development	<input type="checkbox"/> Kid's Sites
<input type="checkbox"/> Motor Vehicles	<input type="checkbox"/> News
<input type="checkbox"/> Professional Organisations	<input type="checkbox"/> Photo Searches
<input type="checkbox"/> Politics	<input type="checkbox"/> Real Estate
<input type="checkbox"/> Reference	<input type="checkbox"/> Religion
<input type="checkbox"/> Search Engines	<input type="checkbox"/> Sex Education
<input checked="" type="checkbox"/> Shopping	<input type="checkbox"/> Society & Culture
<input type="checkbox"/> Sports	<input checked="" type="checkbox"/> Streaming Media
<input type="checkbox"/> Travel	<input type="checkbox"/> Web Based Email
<input type="checkbox"/> Online Software Update	

# SURFPROTECT

## Allowed and Blocked Lists

The Allowed and Blocked lists, provide you with more control than the website automatic categorisation of permitted sites.

The Public or Internal Section you are editing the Allowed or Blocked for will be shown to remind you which area of the profile this list applies.

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

The screenshot shows a web interface titled "Edit URL List". Below the title, it says "List Name : PupilBlockedList". A message reads: "Please enter a list of sites you would like to block, one per line (without http://)". Below this is a text area labeled "Internal Blocked List" containing the text ".somedomain.com". At the bottom of the text area is a "Save List" button.

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

# SURFPROTECT

## 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 you 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.