



Talk-101 User Guides
Web Content Filter Administration

Contents

Contents	2
Accessing the Control Panel	3
Proxy User Management.....	4
Adding a new Proxy User	5
Modifying an existing Proxy User	5
Deleting an existing Proxy User	5
Managing Filters.....	6
Creating a new custom Filter.....	6
Modifying an existing Filter	8
Deleting an existing Filter	8
Managing Custom Categories.....	9
Adding a Custom Category	9
Custom Category Guidelines	10
General Guidelines.....	10
Syntax for entering Web sites, file types and keywords	11
Managing Filter Schedules	13
Reporting	14
Viewing Reports	14
IMPORTANT NOTES	16

Accessing the Control Panel

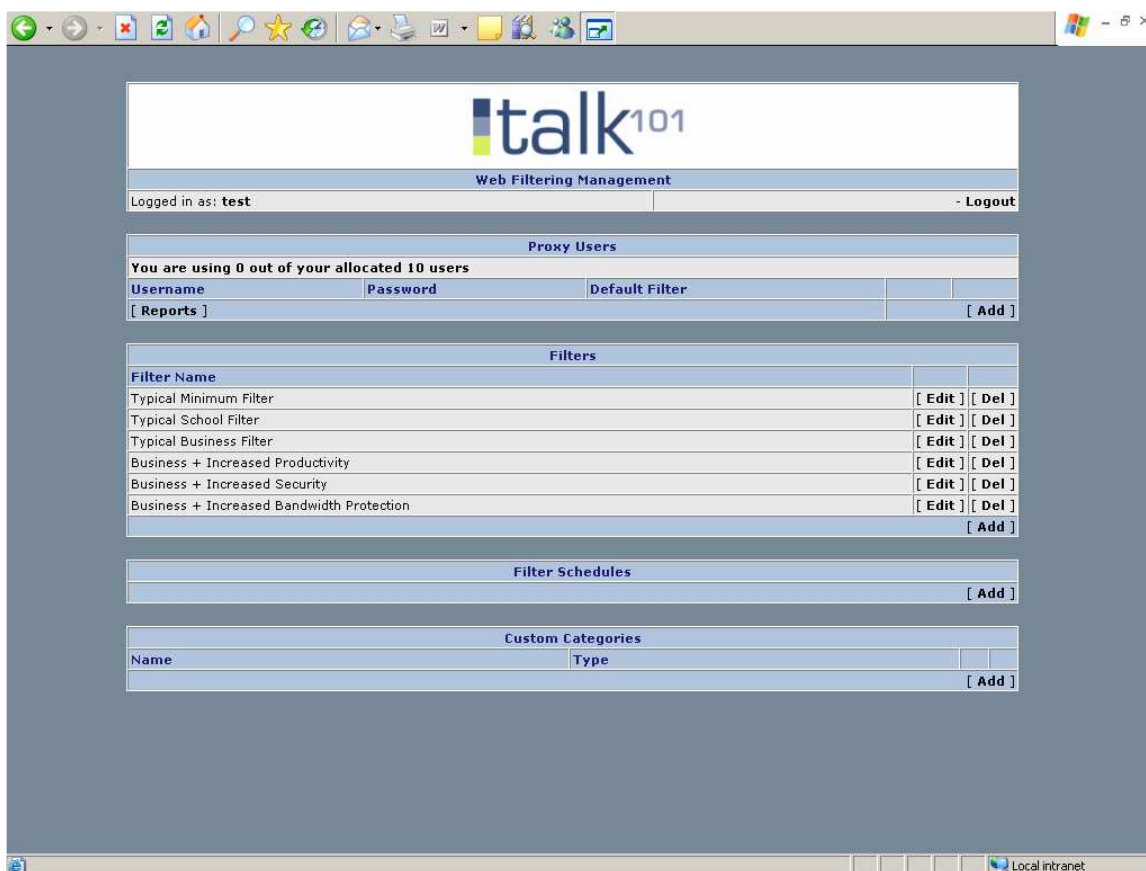
To log in to the Web Filtering Control Panel, you need to use a web browser and go to the following URL:

<http://filter.talk-101.com/>

You will be asked to provide your Administrator Username and Password which you should have been provided with.

Enter this information, and then click the 'Login' button.

You should now see a Customer Menu:



This is the menu from which you will make any changes to your web filtering accounts.

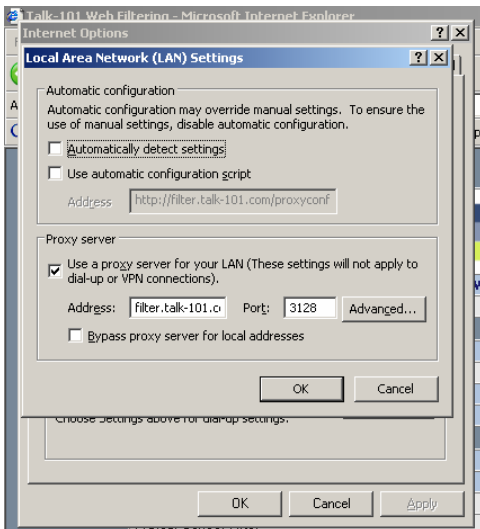
Proxy User Management

Proxy Users are the 'actual' users being filtered.

For filtering occur, they must have a username and password, and have their web browser settings changed to use the filtering server as a proxy server.

To change the browser settings in Internet Explorer do the following:

- In the menu click 'Tools' and choose 'Internet Options'
- Click the tab labelled 'Connections'
- Click the button 'LAN Settings...'
- Under 'Proxy Server', tick the box next to "Use a proxy server for your LAN" and enter the following information
- Address: filter.talk-101.com
- Port: 3128.

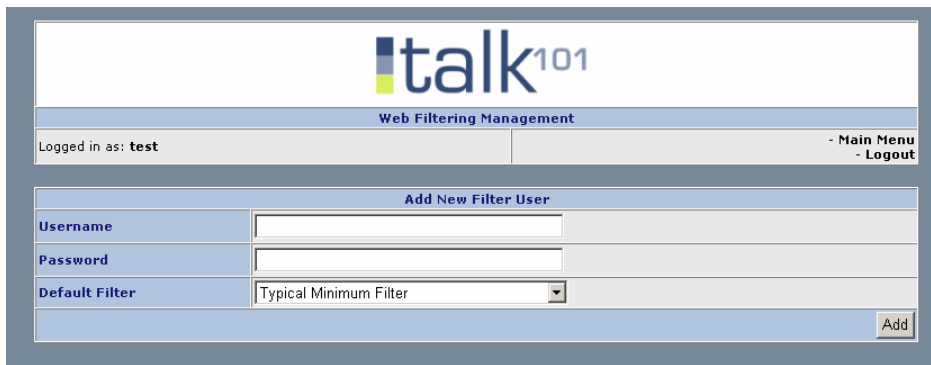


Alternatively, you can use an automatic configuration script using the address: <http://filter.talk-101.com/proxyconfig.pac> in the 'Automatic Configuration Script' settings (found above the Proxy Server Settings).

Adding a new Proxy User

To add a new proxy user to the interface, do the following:

- Under 'Proxy Users' click the 'Add' link in the bottom right-hand of the table.
- You will be asked to provide a Username, Password and Default Filter for the new user. Enter this information and click 'Add'.



The screenshot shows the 'Add New Filter User' form within the 'Web Filtering Management' interface. The form includes the following fields:

Add New Filter User	
Username	<input type="text"/>
Password	<input type="password"/>
Default Filter	<input type="text" value="Typical Minimum Filter"/>
<input type="button" value="Add"/>	

Hint: Try to use the users 'email address' as the username. This keeps the name unique and individual; allowing for better tracking from reports.

Modifying an existing Proxy User

To modify an existing proxy user, click the 'Edit' link next to the user in the 'Proxy User' table. You will be able to modify the Password and Default Filter fields; however will not be able to modify the username.

If you require a change of username, you will need to delete and recreate the user.

Deleting an existing Proxy User

To delete an existing Proxy User, click the 'Del' link next to the user. You will be asked to confirm the deletion. Click 'OK' to confirm, or 'Cancel'.

Note: If you delete a user, schedule filters attached to that user will also be removed. You will also no longer be able to view the reporting data for that username without re-creating the user.

Note: Any changes made to settings on the filtering interface may take upto 2 minutes to take effect.

Managing Filters

When you first login to the Web Filter administration, you will already have set a number of pre-defined filters. These consist of typical filters for minimal filtering, school and business filtering; with some extra business filters for increased productivity, security, and bandwidth protection.

These pre-defined filters are useful if you wish for your filtering to remain simple; however there may be times when these filters do not suffice. The solution is to add your own filtering rules, whereby you specify a rule on a per-category basis; as well as specifying rules for your own custom categories.

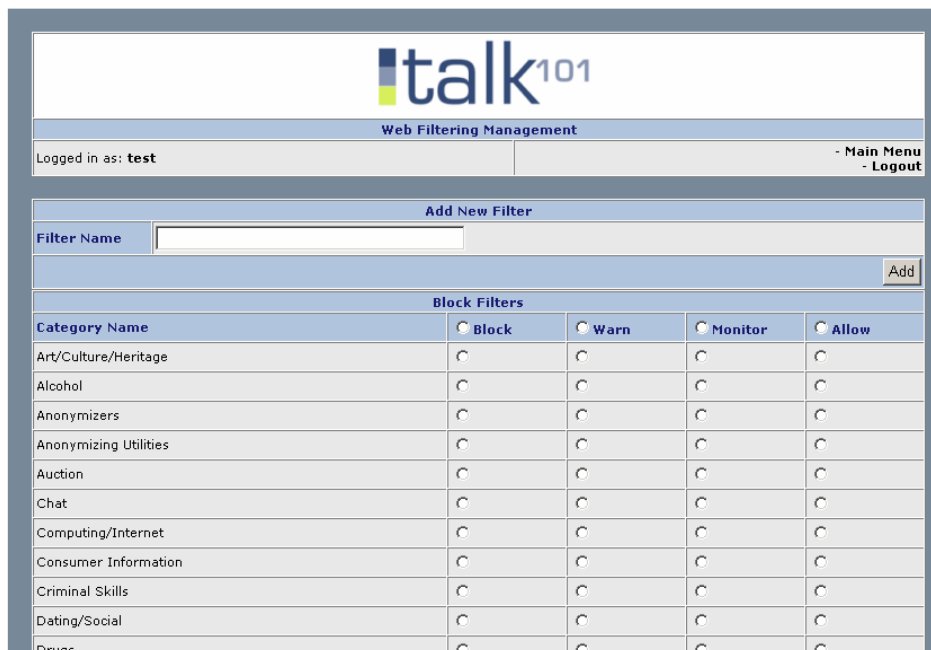
(For example, you may wish to block online news sites, but allow the Financial Times Online).

The filter interface will allow you to add your own filtering rules and custom categories, and these can be modified at any time.

Creating a new custom Filter

To create a new filter, do the following:

- Under the 'Filter' table, click the 'Add' link.
- Enter a Name for your custom filter.
- You will be presented with two lists of categories. The first, 'Block Filters' will be listed, and you will be given four options for each of the categories.



The screenshot shows the 'Web Filtering Management' interface. At the top, there is a header with the 'talk101' logo and the text 'Web Filtering Management'. Below this, it shows 'Logged in as: test' and links for 'Main Menu' and 'Logout'. The main content area is titled 'Add New Filter' and contains a 'Filter Name' input field and an 'Add' button. Below the input field is a table titled 'Block Filters' with the following structure:

Category Name	<input type="radio"/> Block	<input type="radio"/> Warn	<input type="radio"/> Monitor	<input type="radio"/> Allow
Art/Culture/Heritage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Alcohol	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anonymizers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anonymizing Utilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Auction	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Chat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Computing/Internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Consumer Information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Criminal Skills	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dating/Social	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Drugs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The four options for each of the 'Block Filter' categories are:

- Block
 - This option blocks any of the websites listed under that category.
- Warn
 - This option will present a warning page to any user that has this filter set. To bypass the warning page, they must click a link on the warning page, accepting that they are aware of the content categorisation they wish to view.
- Monitor

- This option, at present, will log the category separate from an accepted URL. Further monitoring options, such as notification by email, will be made at a later date.
- Allow
 - This option allows access to any of the sites listed under this category.
- For each of these categories, choose the option you wish to apply.
- You will also be presented with a list of the 'Exception Filters'; these are separate categories, such as 'Business' related websites, which may lie under the one of the categories already listed above.
You are presented with the option to allow these categories as an exception. If you do so, any websites listed under the exception category; regardless of the previous rules applied to them above, will be allowed access.
- Once you have have finished choosing options for each of the categories, click the 'Add' button.

Note: If you fail to choose an option for any of the categories, it will default to 'Allow' (in the case of 'Block Filters') or 'Don't allow as an exception (in the case of 'Exception Filters').

Note: Any changes made to settings on the filtering interface may take upto 2 minutes to take effect.

Modifying an existing Filter

To modify a filter, click the 'Edit' link next to filter in the Filters table. Options are the same as adding a new custom filter.

Deleting an existing Filter

To delete a filter, click the 'Delete' link next to the filter you wish to delete, in the Filters table.

Managing Custom Categories

It is likely that you will find some sites that are not currently classified by the Web Filtering system, or have sites internally with which you wish to restrict your user's access. To allow for this, you are able to add 'Custom Categories' to the web filtering system.

Adding a Custom Category

To add a custom category, you must first set up the name, category type and URL/keyword list.

First you are asked to give your custom category a name.

Next you are asked to choose a category type, these are explained below.

- 'Block'
The 'Block' type is a list of sites to Block, Warn, Monitor or Allow. Use this type for sites you wish to apply any of these rules to.
Please do not assume that setting category type to Block will cause sites to be instantly blocked without editing any filters. **Filters need to be modified to apply the rules for custom categories.**
- 'Exception'
The 'Exception' type allows you to list URLs that can be an exception to existing rules. For example, to allow the BBC news website, but block websites in the News category.

Note: You must edit filters to choose the options for custom categories. By default filters will ignore or allow any sites listed in a category that does not have

Next you are asked to provide a list of sites you wish to block.
Please follow the guidelines on the following pages:

Custom Category Guidelines

When you create a custom category, you specify the Web addresses (sites, folders, and pages), file types, and keywords to block or allow. To ensure that filtering works as expected, review the guidelines and syntax examples on the following pages before adding items to a custom category.

General Guidelines

- To avoid overblocking or overallowing Web content, be as specific as possible when creating your custom categories.
- The filter supports all protocols (including HTTP, HTTPS, and FTP).
- For HTTPS address, the filter can only base filtering on the hostname. Thus, you can block or allow an entire HTTPS site, but no specific sections or pages within an HTTPS site or file types from HTTPS sources.
- The filter supports two wildcard characters: '*' matches zero or more characters; '?' matches any character, but there must be a character present.
Note: It's recommended that you minimise wildcard usage in the custom categories. Wildcard entries slow filtering performance.
- You can enter URLs in uppercase or lowercase. However, the filter automatically converts to lowercase all URLs included as part of a custom category.

Syntax for entering Web sites, file types and keywords

Use the following syntax guidelines when adding items to a custom category.

To block or allow	Type	Notes
An entire Web site	<protocol>://<host name> e.g. http://www.talk-101.com	For greater flexibility, just type the site's domain: site.com. This blocks or allows the site under HTTP, HTTPS, and FTP, as well as any host (such as www).
An entire Web site (Including it's associated IP addresses)	[ipmap] <protocol>://<host name> e.g. [ipmap] http://www.talk-101.com/	Typing [ipmap] before the URL blocks or allows all sites hosted on the same server as the URL. So other sites sharing the same IP address/es are also blocked or allowed. Be selective when typing [ipmap] before a URL: typing [ipmap] before a URL will also block or allow URLs matching the entry on this virtual host.
Particular sections of a Web site (HTTP only)	<a href="http://<host name>/<path>">http://<host name>/<path> e.g. http://www.talk-101.com/partners/	Use paths to block or allow specific sections or pages within an HTTP site. If you don't specify a path, the entire site is blocked or allowed.
Particular pages in a Web site (HTTP only)	<a href="http://<host name>/<path>/<page>">http://<host name>/<path>/<page> e.g. http://www.talk-101.com/html/jobs.html	You can block a page within an allowed path, and vice versa. For example you can allow http://www.talk-101.com/html/jobs.html even if you've blocked http://www.talk-101.com/html/ .
An IP address	<a href="http://<ip address>">http://<ip address> e.g. http://195.8.181.10/	Only the IP address you specify is blocked or allowed. It is not mapped to a specific URL or another IP address.
A file type (from any HTTP source)	[ftype] <file extension> e.g. [ftype] exe	Note: The filter doesn't support wildcards as part of the file extension. So if you want to block or allow both mp3 and mpeg, type [ftype] mp3 and [ftype] mpeg on separate lines.

To block or allow	Type	Notes
A file type (from a particular HTTP location)	http://<host name>/*.<file extension> e.g. http://www.google.com/images/*.jpg	
URLs that contain a particular keyword or phrase anywhere in the URL	[keyurl] <word> e.g. [keyurl] travel vacation e.g. [keyurl] stocks	
URLs that contain a particular keyword in the CGI portion of the URL	[keycgi] <word> e.g. [keycgi] stocks e.g. [keycgi] sexyphotos	Use [keycgi] to block or allow particular keywords when used for Web searches.
A URL that contains '*' or '?' characters that are not used as wildcards	http://www.dictionary.com/search/?q=*	If a '?' or '*' appears in a URL, and you don't want to treat the characters as a wildcard, precede the '?' or '*' with a backslash. (This may be necessary to block or allow URLs that contain parameters).

Managing Filter Schedules

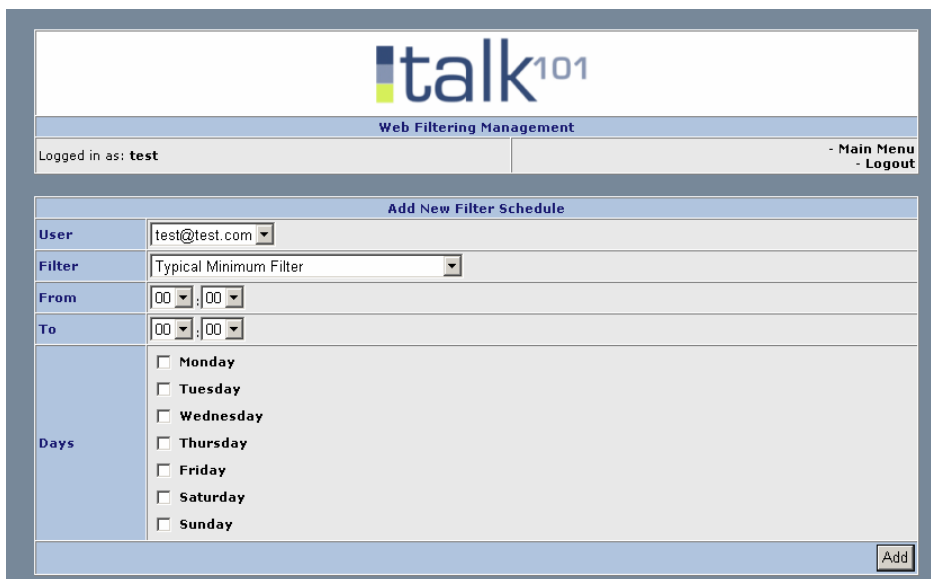
Filter schedules allow you to apply filters to a particular user at a specific time of day.

For example, you may wish to allow your employees to browse websites during their lunch hour, which you would not otherwise allow them during business hours.

Note: Filter schedules can only be applied on a per-person basis.

Adding a new Filter Schedule

To add a new filter schedule, click the 'Add' link in the bottom right-hand of the Filter Schedule table.



You will be asked to provide the User, Filter, Start and End times, and the Days that you wish the filter to be applied.

Important Note: You are unable to overlap times in filter schedules (e.g. Filter 1 between 12pm and 1pm and Filter 2 between 12.30pm and 1.30pm). You need to separate such overlaps into different sections (e.g. Filter 1 between 12pm and 12.30pm, Filter 3 between 12.30pm and 13.30pm).

Attempts to overlap times will result failing.

Note: Due to limitations beyond our control, you can not schedule filters past midnight in a single rule. (e.g. Monday 8:30pm – Tuesday 4:30am). Instead you need to create 2 rules. The first on Day 1 (e.g. Monday 8:30pm-11:59pm), the second on Day 2 (e.g. Tuesday 0:00am - 4:30am).

Reporting

Whilst blocking categorised sites may be useful, another feature of the filtering system is its reporting abilities. From the Control Panel you are able to see breakdowns on the usage by your employees/users. You are also able to download the reporting data into a CSV format for use in a spreadsheet to produce your own reports.

Viewing Reports

To view the reports area, click the 'Reports Link', located in the bottom left-hand of the Proxy Users.

You will be asked to provide the following:

- Report Type
 - o This is the type of report, which can be either 'All Visited Websites' or 'Blocked Websites'.
- User
 - o You can use this option to specify the report to contain only data for a particular user, or all users.

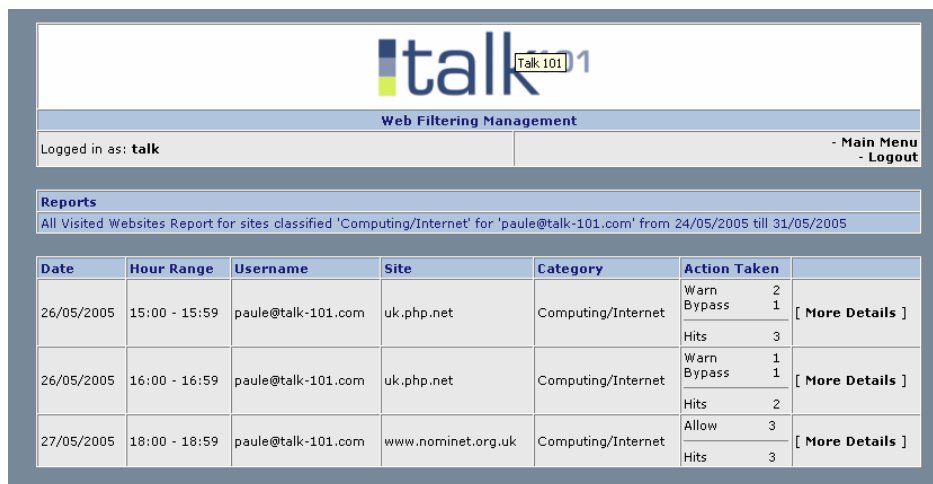
- o **Note:** If you delete a user from the Proxy Users, you will not be able to view reports for the user.

- Category
 - o This option allows you to filter the report by a particular category.
- Date Range
 - o This option allows you to specify a particular date range for the report data.

- o **Note:** Report data is retained for 90 days.

Once you have selected your report options, you can choose either:

- Show Report
 - o This will display the report on-screen in your web browser window.
- Download CSV Report
 - o This will generate the report, and give you a link from which you will be able to download the report data.



Date	Hour Range	Username	Site	Category	Action Taken	
26/05/2005	15:00 - 15:59	paule@talk-101.com	uk.php.net	Computing/Internet	Warn	2
					Bypass	1
					Hits	3
26/05/2005	16:00 - 16:59	paule@talk-101.com	uk.php.net	Computing/Internet	Warn	1
					Bypass	1
					Hits	2
27/05/2005	18:00 - 18:59	paule@talk-101.com	www.nominet.org.uk	Computing/Internet	Allow	3
					Hits	3

If you choose to display the report on screen, you will be given a page that looks similar to the above.

You will be given details of the site, time, username, category and action taken for each entry. Multiple site entries, which contain the same username and site, are grouped for each hour. Action Taken displays one or more of the following:

- Allow
 - o The user has been allowed to access the site or a page/path within the site.
- Warn
 - o The user has been shown a warning page, explaining that the content in the URL is classified as (category).
- Bypass
 - o The user has 'accepted' and bypassed the warning page above.
- Monitor
 - o The user has visited a URL that has been set to monitor within the Filter preferences.
- Blocked
 - o The user has attempted, and been blocked from visiting a URL.

IMPORTANT NOTES

- Changes made take up to 2 minutes to take effect.

- Reporting may be behind on the summary reports by up to 1 hour during busy periods. This is due to the volume of data being processed and summarised.

- Whilst Talk-101 has made every effort possible to ensure this service works as perfectly as possible, this service is by no means a guarantee of protection from any of the categorised content.

- Also, there may be circumstances whereby a website URL has yet to be classified by the filter system. We update our filter lists regularly, and should you find any sites that are unclassified, we will be happy to forward this information on to the developers to include these sites in the lists.