

Main differences between 5.2.0 and 5.2.5 web filtering and advice on migrating to the new filtering system

Summary of document:

- The main differences in 5.2.5
- What will happen once you upgrade to 5.2.5 and any actions you need to take
- How to block a web site using the new system

What you need:

- Knowledge of the current URL filtering system used by Pilot.

Software Revision Required:

- Applicable to software revision 5.2.5 > on Pilots

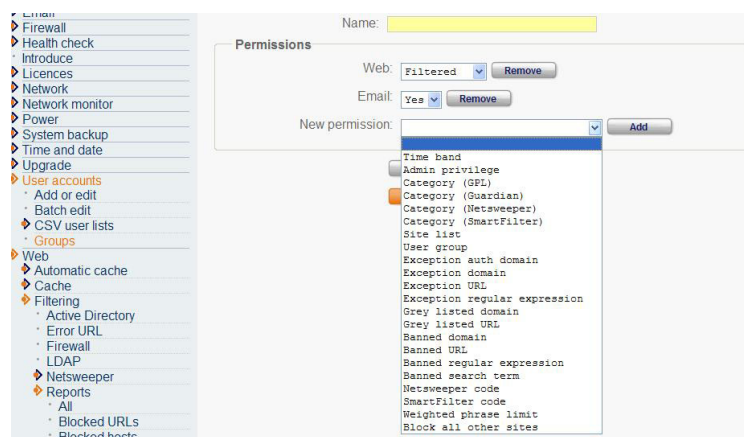
Main differences in 5.2.5

The main differences in the new system are:

- Admin permissions are now granted to a user by their membership of a group using the "User Accounts - Groups" page, rather than on a per-user basis using the "Site admin" page (which has been removed). There are three new groups ("admin", "admin site" and "admin cache"), corresponding to the old admin levels on the "Site admin" page.



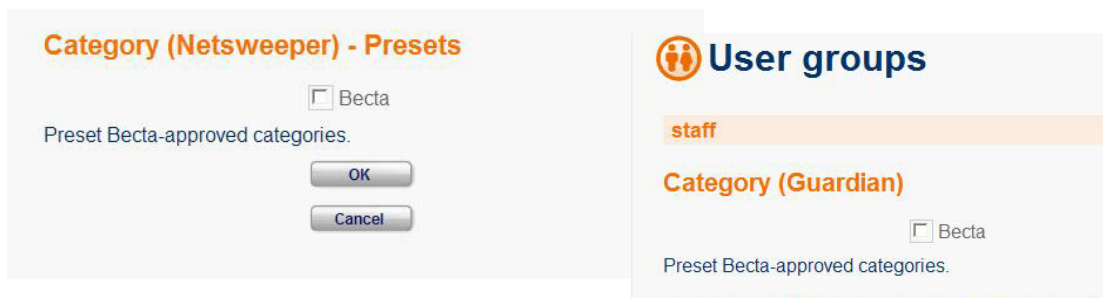
- User groups can specify web filter rules directly. Previously, web filter rules had to be in a site list and a user group then had to refer to a site list. That usually meant having to make a new site list for every new user group with different rules (you can still do that if you want, but it's not necessary).



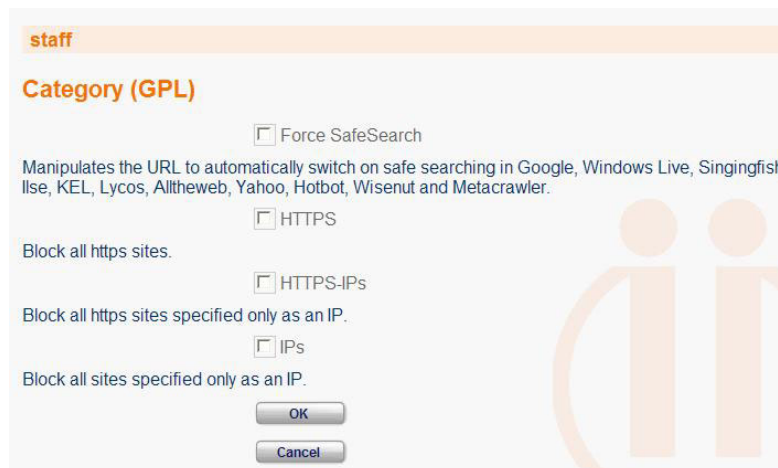
This makes it so much easier to express what you want for a new group therefore we have removed many of the pre-defined groups and site lists we used to include. You now get only "open" and "controlled", which differ only in the behaviour for sites not listed ("open" defaults to allow, "controlled" defaults to "block").



- **The priority of filtering rules now depends on the type of the rule, regardless of the group or site list it comes from.** This means that all the exceptions apply first, then any grey lists, and lastly the banned sites. Previously, white and black rules applied strictly in the order they were mentioned in the global group, then in the order mentioned in the user group; this meant a user group couldn't grant an exception to something blocked by the global group.
- BECTA approved filtering services SmoothWall Guardian and Netsweeper offer now a BECTA category in the 'Category' permissions, which automatically activates all categories required for BECTA approval.

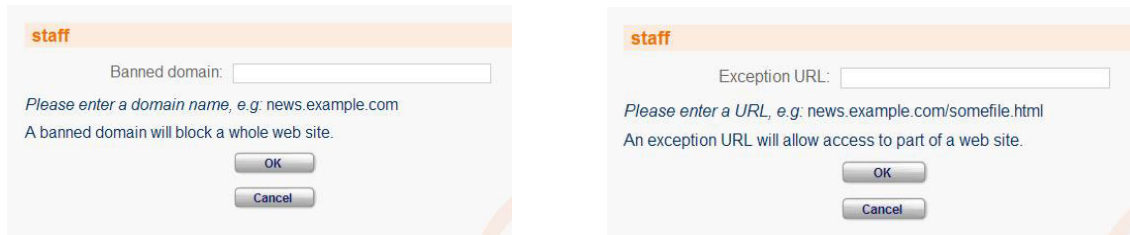


- New "Force SafeSearch" category. This ensures that any web search automatically activates the safe search feature built in to all the major web search engines. The closest equivalent in previous versions was a complicated method we documented to block unsafe Google searches. This involved a lengthy sequence of whitelist and blacklist patterns in a specific order. The new way of sorting patterns by types means this method doesn't work any more, so if you have used this method, we suggest removing the relevant rules and simply using the new category instead.

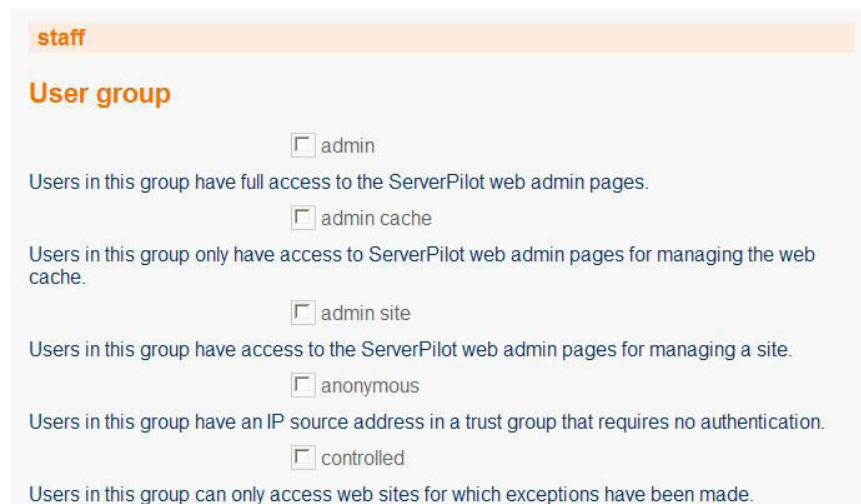


- Active Directory users who don't belong to any Active Directory Group known to Pilot are now handled by the new "no profile" group, instead of being treated the same as anonymous users.
- Previously you could add "regular expression" patterns, which were very powerful but hard to use correctly. Now you can also use "domain" and "URL" patterns, which

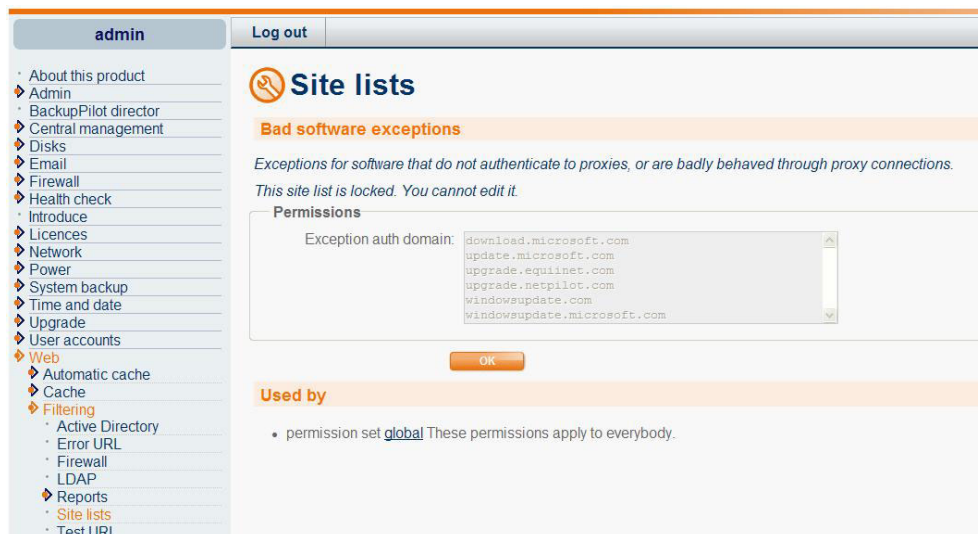
work faster, and you don't need to use the fiddly regular expression syntax. You can still use the regex syntax in 'regular expression' patterns.



- One user group can act like another user group with the addition of its own allow or deny rules. This makes it possible to construct chains, such as saying group "Year 9" uses the rules from "Year 10" plus some extra restrictions appropriate to the younger age-group. This was only possible before by using of lots of site lists.



- It is now possible to see the built-in "Bad software exceptions" site list, which is used to identify programs which don't work well with web proxies. This list existed previously but couldn't be seen or changed. You still can't change it directly, but you can now create your own equivalent list using the "exception auth domain" permission.



- Time bands are now set in the site list they apply to. Previously, the time band was set in the user group separately from the site list it applied to.

staff

Time band:

If you add a time band, all other rules for this group will only take effect when in time band. One time band can be added per group.

For those with SmoothWall Guardian web filtering, many more features are configurable:

- Previously you could only add "regular expression" patterns, which were very powerful but hard to use correctly. Now you can also use "domain" and "URL" patterns, which work faster, and you don't need to use the fiddly regular expression syntax. You can still use the regex syntax in 'regular expression' patterns.

staff

Banned domain:

Please enter a domain name, e.g. news.example.com
A banned domain will block a whole web site.

staff

Exception URL:

Please enter a URL, e.g. news.example.com/somefile.html
An exception URL will allow access to part of a web site.

- You can now make "grey list" domain and URL exceptions; these are exempt from being banned by category but still subject to content filtering (this was partly implemented before as "grey" site lists).

staff

Grey listed domain:

Please enter a domain name, e.g. news.example.com
A grey listed domain allows a whole web site to be accessed without disabling content filtering.

staff

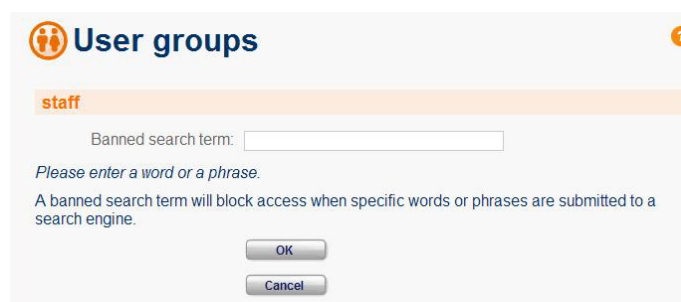
Grey listed URL:

Please enter a URL, e.g. news.example.com/somefile.html
A grey listed URL allows part of a web site to be accessed without disabling content filtering.


- It is now possible to change the strictness of the content filtering system's "weighted phrase limit": there are several levels ranging from "young children" to "older children", "young adults" and beyond. Previously this was always set to "young children".



- You can now block "search terms"; these are recognised for all the major search engines.



Changes following upgrade to 5.2.5

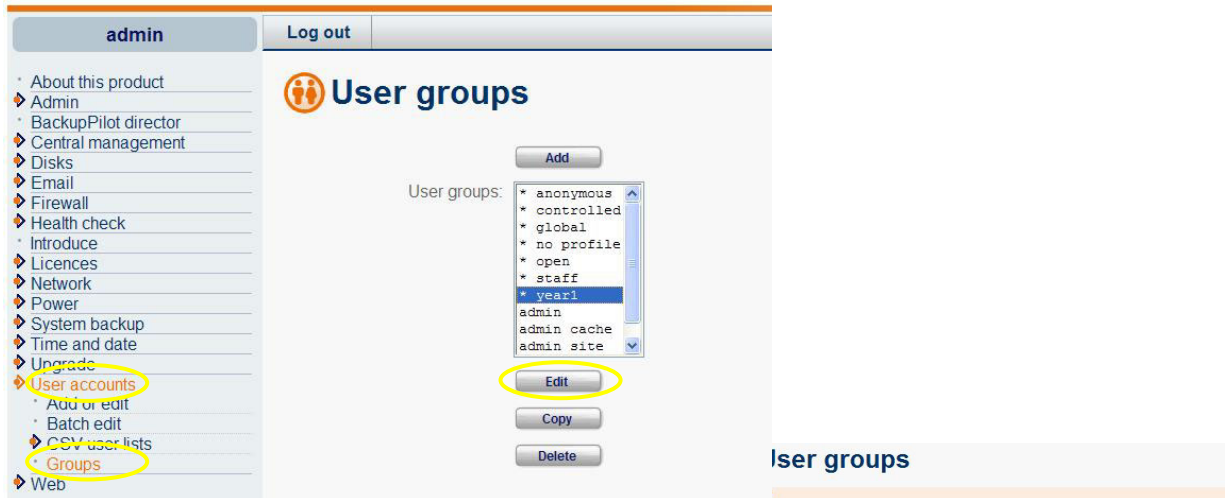
 Automatic changes which will happen once you have upgraded (or restored from an old backup) and actions you might want to take as a result of the upgrade

- When migrating from earlier code, changes are made automatically which try to preserve the behaviour of user groups and site lists, while taking advantage of some of the new features. User groups will be preserved, however where a user group uses a site list that isn't used for any other purpose, the contents of the site list will be moved to the user group and the site list will be removed. This applies to groups you created and to groups that came with the product, so you should see the old 'global permitted sites', 'global manipulated sites' and 'global forbidden sites' site lists will disappear and be merged into the 'global' group. Site lists used by more than one group or those with an associated time band are preserved.
- Inside a site list, you may notice that what used to be a single list of patterns has been split up in to two or more separate sections. Patterns which only matched hostnames or parts of a domain name (domain patterns) are grouped separately from those matching fixed parts of URLs (URL patterns), which are grouped separately from patterns using the extra features of regular expressions (regular expression patterns). This is done primarily to improve the efficiency of the web filter, since hostname and URL types of pattern can be matched much faster than the regular expression type.

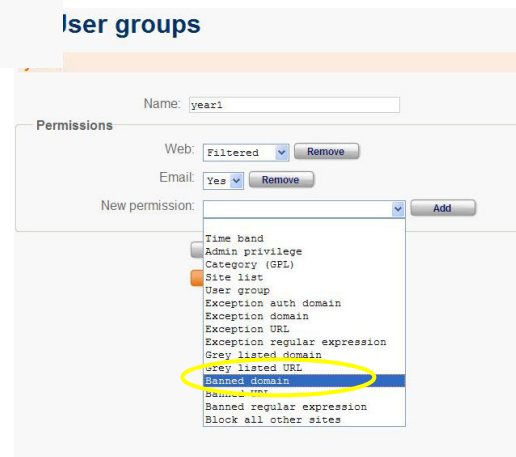
- You might like to check anything that has been placed in the "regular expression" patterns to see if that was what you intended, or whether the same effect could now be achieved by moving the pattern to be one of the more efficient types.
- If the upgrade detects the patterns we previously suggested for blocking unsafe Google images searches, it will remove those patterns and activate the new "Force SafeSearch" category.
 - If you have experimented with this kind of blocking yourself rather than following our instructions, it is likely that the upgrade will not be able to make the conversion automatically. In that case, please delete the old site list rules you have added and activate the "Force SafeSearch" category manually.
- The old filtering system allowed users to combine white (allow) and black (block) as rules in 'User groups'. When filtering occurred first the allow and block lists of the global group and then later if no match was found the rules of the user's group were interrogated. In the new system all rules of the same type are applied first with the specific group rules taking precedence over the more general global rules.
 - Normally you should see no difference in your browsing. The new way of filtering however adds additional ways in which web access can be affected. For example if you blocked the category 'Weapons' in global, and later you created a white list including the site www.knives.com and added it to a group, your change would not have any effect using the old filtering whereas it would work using the new system.
- The changes to the filtering also have implications for logging. The log file format has now been updated. Whereas originally log entries referred to black, white, grey or red site lists as reasons for allowing or blocking a specific website, the new filtering system logs the type of permission used to grant or disallow access.
 - If you have customised the message appearing when a website is blocked using cgi, you should contact Equinet for advice on how the upgraded will affect your block message and how it can be adapted to work with the new filtering.
- After the upgrade the 'no profile' group (used for Active Directory users not included in AD groups on the Pilot) is set to behave the same as 'anonymous' so as to exactly preserve the previous behaviour.
 - However, when starting from fresh, 'no profile' is set to block access; we recommend changing the 'no profile' setting back to "block" on an upgraded unit if you don't need this feature.

How to block a website in 5.2.5 using group rules

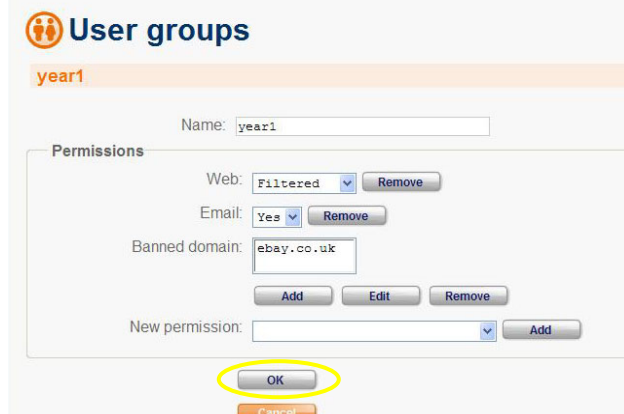
① Firstly select the group for which you want the website to be blocked. Go to **User accounts > Groups**, make your selection and click on **'Edit'**.



Next from the drop down menu for **'New permission'** select **'Banned domain'** and click on **'Add'**.



In the next screen enter the domain you want to block and click **'OK'**.




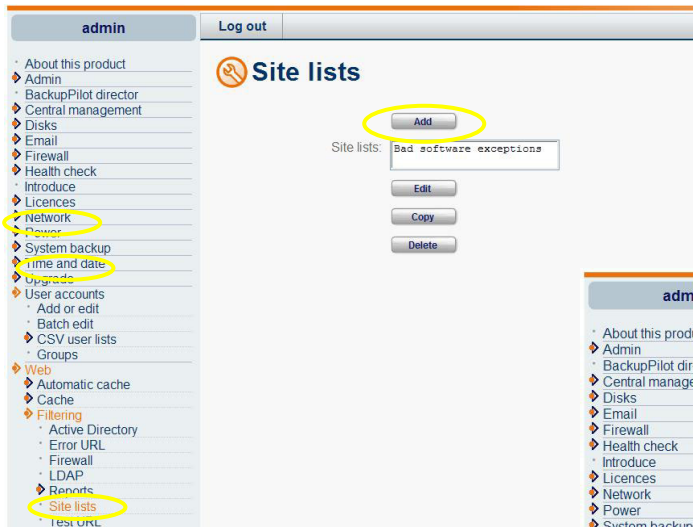
In the main **'User group'** screen you can see that the website has been added and from now on it will be blocked for that specific group. Click **'OK'** again and again to reconfirm the change.



① If you want to allow a website follow the above steps but select **'Exception domain'** instead of **'Banned domain'**.

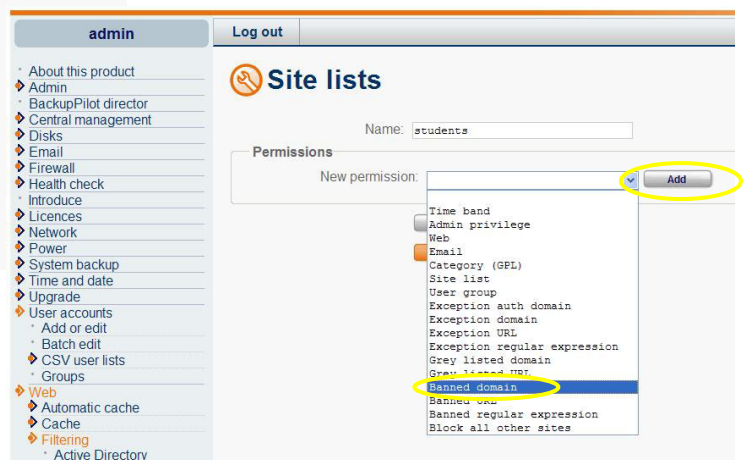
How to block a website in 5.2.5 using a site list

 You can also block a website using 'Site lists' as shown next. They are primarily useful where rules applying to some set of web pages needs to be used by more than one group, or when using time bands. If a time band permission is used in a group the time rules will apply to all other permissions used in that group. However if a time band permission is used within a site list the time restrictions will apply to the rules of that site list not the group in which it will be used. That way if required, it is easy to set the permissions which apply all the time on the group, with the extra permissions for the time band in the site list.

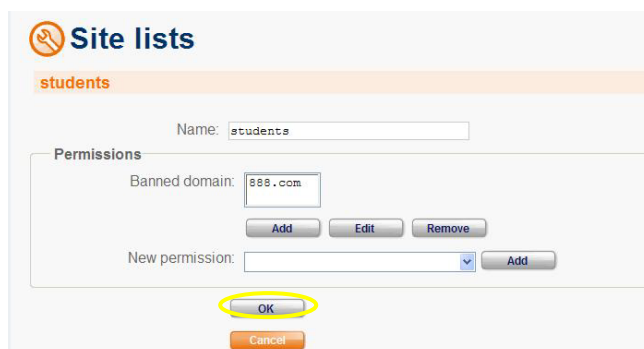


To create a site list go to **Web > Filtering > Site lists** and select 'Add'.

Next enter the name of the site list and from the drop down menu under 'New permission' select 'Banned domain'.

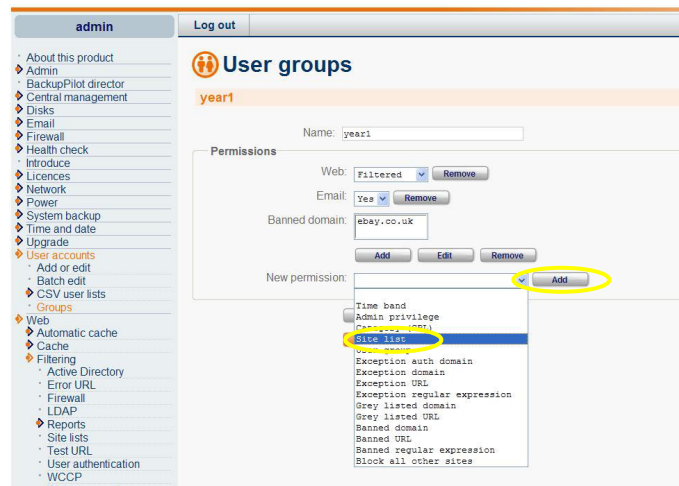


Next enter the domain you want to block and click 'OK'. Once you are back in the main 'Site list' screen click 'OK' again and again to reconfirm the change.

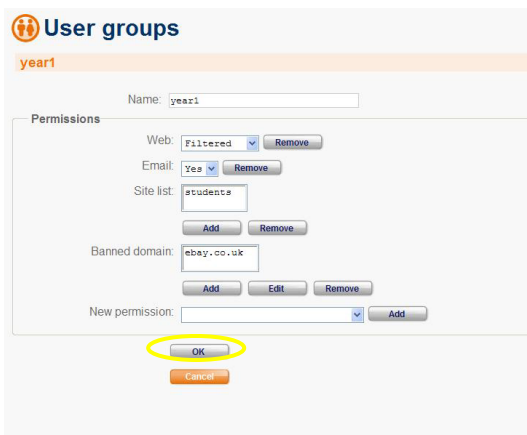


Next go to **User accounts > Groups**
select the group to which you want to
add the site list and click on **'Edit'**

From the drop down menu under **'New permission'** select the option **'Site list'** and click on **'Add'**.



Tick the box next to your newly create site list and click on **'OK'**.



Back in the main screen you can see that the site list has been added and you just need to click on **'OK'** to reconfirm the changes to your group.

i The permission rules of the site list will apply to the group and any other group to which you might add the site list in the future.

