

Chapter Twelve (a): General Information on Site Lists for Smartfilter & Netsweeper

Summary of Chapter:

- General Information on Site Lists and how Site Lists are connected to User Groups.
- How to check if individual URLs are being categorised correctly by the 'User Groups' you have created.

What you need:

- Knowledge of Admin user account and valid password for your Pilot.
- A UTM PoP code. NetPilot users can purchase this from the following address: <http://www.equinet.com/ordering/default.asp>, CachePilot users please contact Equinet for a quote.

Software Revision Required:

- Applicable to software revision 5.2.0 > Net/CachePilots

(Net/CachePilot will be referred to as 'Pilot'. All image examples are of a NetPilot.)



Site Lists are part of 'Web access rules' which are applied when editing or adding 'User Groups' in the User Accounts / Groups section.

Site Lists:

- Log on to the Pilot as shown in Chapter One (b).
- From the left-hand side of the screen, select 'Web', then 'Filtering' and then 'Site lists'. (All links are highlighted below).

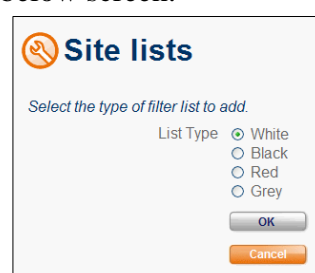



- The default Site Lists are highlighted left.

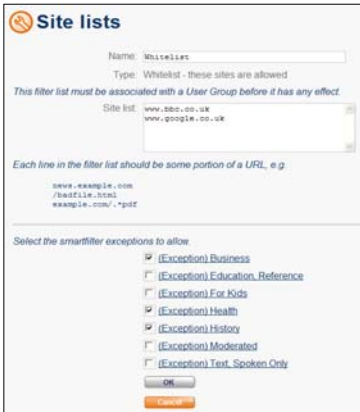


These Site Lists are blank as default, until you edit them.

- To edit any Site Lists, select the Site List you want and then select the 'Edit' button.
- In addition to the default Site Lists, you can create your own. Select the 'Add' button and you will be presented with the below screen:



 Here is more information about the different site lists you can create:



Site lists

Name:

Type: Whitelist - these sites are allowed

This filter list must be associated with a User Group before it has any effect.

Site list:

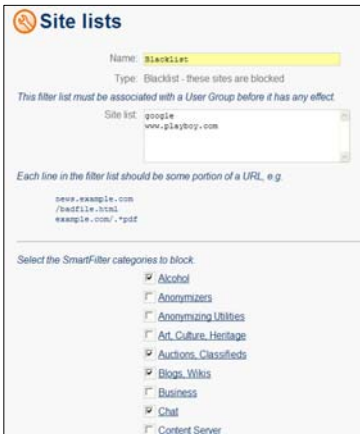
Each line in the filter list should be some portion of a URL, e.g.

`www.example.com`
`/badfile.html`
`example.com/*.pdf`

Select the smartfilter exceptions to allow:

(Exception) Business
 (Exception) Education, Reference
 (Exception) For Kids
 (Exception) Health
 (Exception) History
 (Exception) Moderated
 (Exception) Text, Spoken Only

White – Whitelists can override blacklists and redlists. They will only allow the sites which have been entered into the ‘Site List:’ text box and the exceptions which are provided by Smartfilter or Netsweeper.



Site lists

Name:

Type: Blacklist - these sites are blocked

This filter list must be associated with a User Group before it has any effect.

Site list:

Each line in the filter list should be some portion of a URL, e.g.

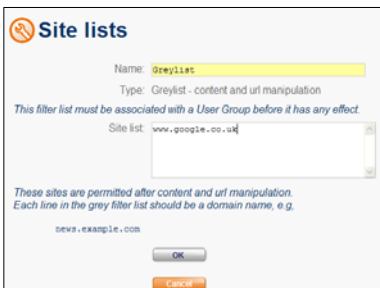
`www.example.com`
`/badfile.html`
`example.com/*.pdf`

Select the SmartFilter categories to block:

Alcohol
 Anonymizers
 Anonymizing Utilities
 Art, Culture, Heritage
 Auctions, Classifieds
 Blogs, Wikis
 Business
 Chat
 Content Server

Black – Blacklists block specific sites. They will block sites entered into the ‘Site List:’ text box and selected categories of sites, which are provided by Smartfilter or Netsweeper.

Red – Redlists are similar to blacklists. They are block lists which can be used for more severe block categories than the standard blacklists. A suitable error.cgi script can be setup to react to red list block messages and if necessary send an email when triggered. (This is also true of all block messages).



Site lists

Name:

Type: Greylist - content and url manipulation

This filter list must be associated with a User Group before it has any effect.

Site list:

These sites are permitted after content and url manipulation.
Each line in the grey filter list should be a domain name, e.g.

`www.example.com`

Grey – Greylists allow access to URLs, like Whitelists. They are only for use with a filter service called Guardian.



Tip! If you would like further information on Guardian, please see Chapter 12 (b) and 12 (h).



Information Be careful not to exceed the character size limit of 10,000 characters for each of the Site Lists text box, in which you can enter URLs.


Site Lists & User Groups:



Information User Groups use Site Lists to implement browsing controls. Listed below are standard User Groups with the Site Lists they contain. As default the Site Lists are blank and have no URLs or categories selected.

 **Controlled:**


 Allow Permitted sites

 Filters for Anonymous user (this group applies if the firewall does not require users to log in before using the web proxy):


 This contains no Site Lists as default.

 Global: this group applies to all users
 Allow Global Permitted sites
 Allow Global manipulated sites

 Block Global Forbidden sites

 Limited:

 Block and report restricted sites

 Block forbidden sites during work hours

 Open:

 This contains no Site Lists as default.


Smartfilter:

Alongside our simple text / URL Site Lists you can use Smartfilter. When a URL is checked it will go to an external server is contacted to find out which category the requested URL is classified in. Equinet customers can run their own servers offering the URL category checking service or check against hosted servers e.g. Brightfilter service. Smartfilter's database has over 15 million URLs, which are divided into over ninety categories and growing. The administrator of the local Equinet unit defines which users may view which categories. Therefore local flexible controls are available, which is often a key requirement. This technology is Becta approved for education users.



 To see the latest definition of Smartfilter's categories, please see:
<http://www.securecomputing.com/index.cfm?skey=86>

 To check whether a particular site is categorised by Smartfilter and to which category it falls into. Please see: <http://www.trustedsource.org/en/feedback/url> select 'Smartfilter XL'

 If you find a URL that is not categorised by Smartfilter and feel it should be, please see check it on the above URL first. Once you've done this you will have the option to choose which categories it should appear in.



For further information on Smartfilter please see Chapter 12 and 13.

Netsweeper:

Alongside our simple text / URL Site Lists you can use Netsweeper. Netsweeper also has a large database of many millions of URLs. In addition, it attempts to categorise URLs in real-time if they are not present in its database. Equinet customers can run their own servers offering the URL category checking service or check against Netsweeper hosted CNS servers. The administrator of the local Equinet unit define which users may view which categories. Therefore local flexible controls are available, which is often a key requirement. This technology is Becta approved for education users.



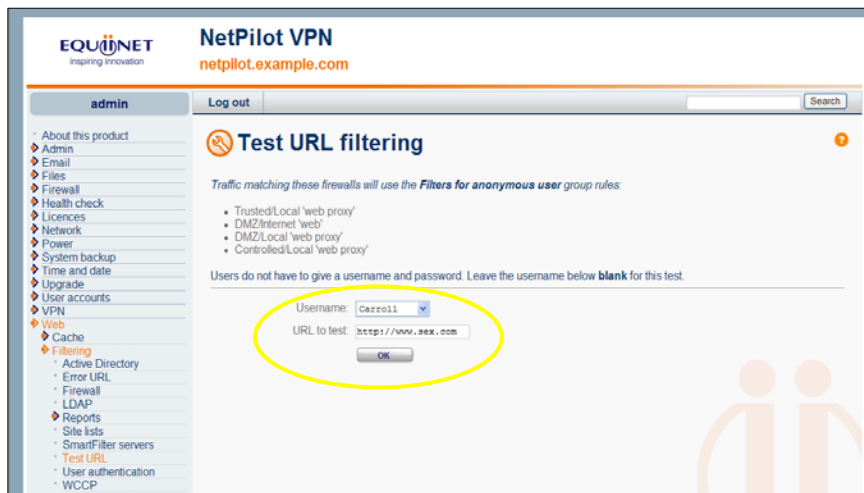
 To check whether a particular site is categorised by Netsweeper and to which category it falls into. Please see: <http://www.netsweeper.com/Support/Test+A+Site>



For further information on Netsweeper please see Chapter 12 and 13.

Test URL-Filtering:

🛠 From the left-hand side of the screen, select 'Web', then 'Filtering' and then 'Test URL'. (All links are highlighted below).



🛠 In the drop down list select a User you wish to test.

🛠 In the text box enter a URL you wish to test. You must manually enter the syntax 'http://' or 'https://' or 'ftp://' etc before the 'www.sitename.com'.

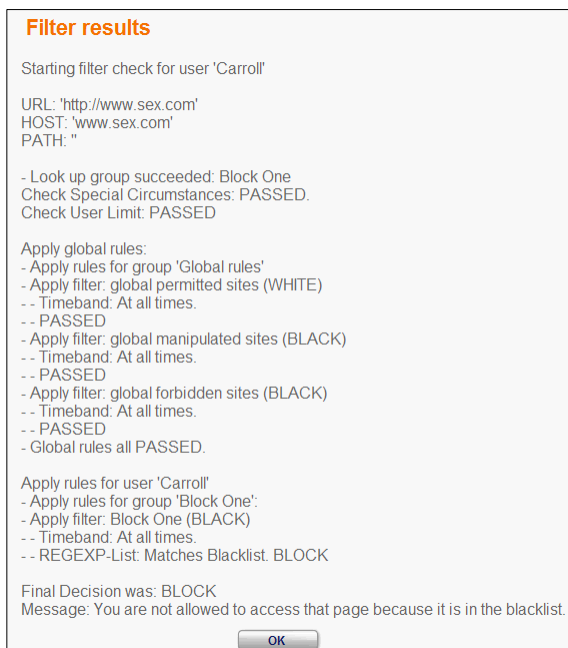
🛠 Select 'OK'.

🛠 The Pilot will then display the filter results after going through a process of checking the following:

- 🛠 Timeband controls
- 🛠 Global filtering controls
- 🛠 Blacklist/Whitelist controls depending on the User Group (which contains the filtering controls) that is assigned to the User.

🛠 In the below example,

🛠 The user is 'Carroll' who is in the 'block_one' group.



🛠 The Pilot will check 'Special Circumstances' this is to constantly allow Admin to Bypass Site Lists and always allow Equinet's websites.

🛠 The Global Rules are applied first.

🛠 In this default User Groups Whitelists are applied first before Blacklists.

🛠 In the Global Site Lists there is no match to the URL entered.

🛠 The filter will continue on to the Users' 'User Group' which contains more Site Lists.

🛠 In the User Group 'block_one' the URL was matched.

🛠 The final decision is 'Block'.

```

Filter results

Starting filter check for user 'Carroll'


URL: 'http://www.sex.com'
HOST: 'www.sex.com'
PATH: ''


- Look up group succeeded: Block One
Check Special Circumstances: PASSED.
Check User Limit: PASSED


Apply global rules:
- Apply rules for group 'Global rules'
- Apply filter: global permitted sites (WHITE)
-- Timeband: At all times.
-- PASSED
- Apply filter: global manipulated sites (BLACK)
-- Timeband: At all times.
-- PASSED
- Apply filter: global forbidden sites (BLACK)
-- Timeband: At all times.
-- REGEXP-List: Matches Blacklist. BLOCK


Final Decision was: BLOCK
Message: You are not allowed to access that page because it is in the blacklist.
  
```

In this example,

 The Pilot will check 'Special Circumstances' this is to constantly allow Admin to Bypass Site Lists and always allow Equinet websites.

 Then the Global Forbidden Site List matches the URL.

 As soon as there is a 'Block' match in the Global rules, the URL is blocked.

 The Filter results will not continue to look into the Users individual Site Lists, as shown in the example above.



When URL filtering is applied to Users' browsing, 'Global rules' are always implemented first. If users are accessing the Internet anonymously, without having to authenticate with the unit, 'Filters for anonymous user' will be applied after the Global Groups.



For more information on Sites Lists please see the other sections of this chapter.