

The attached tip sheet presents the most common Search bar entries, regular expression filters and queries used in creating reports.

Example of Search bar entries	Result
IP Address:	
192.168.127.1	A single IP address 192.168.127.1
192.168.127.0/24	All IP addresses in the range 192.168.127.1 to 192.168.127.254
192.168.127.1,192.168.127.2	The IP addresses 192.168.127.1 and 192.168.127.2
192.168.127.0/24,192.168.128.0/24	All IP addresses in the range 192.168.127.1 to 192.168.127.254 and 192.168.128.1 to 192.168.128.254
192.168.0.0/16,!192.168.127.0/24	All IP addresses in the range 192.168.0.1 to 192.168.127.254 but excludes IP addresses in the range 192.168.127.1 to 192.168.127.254
Report variables can be used in place of IPs/Ports/Subnets	
Dublin (or displayed as \$Dublin in the filter field)	A single IP which matches the report variable "Dublin". Filter box will autofill on typing.
Dublin,NewYork,Berlin	The IP addresses which correspond to the report variables (subnets) "Dublin" and "NewYork" and "Berlin" separated by a comma. You will need to type in the report variable name after you select the first one or create one report variable, which encompasses all subnets.
User Name	
laura.ashton with the option 'Contains'	Returns the user "laura.ashton" only
laura.ashton robert.schmidt with the option 'Matches regexp'	Returns "laura.ashton" and "robert.schmidt" only
laura.ashton robert.schmidt with the option 'Does not match regexp option'	To exclude "laura.ashton" and "Robert.schmidt" from the results use
File or Folder Name	
sales	All filenames or directory names that contain "sales"
Website	
youtube.com with the option 'Contains'	Web activity associated with youtube.com only
Face with the option 'Contains'	Web activity associated with any website that contains "Face" in the URL
youtube.com googlevideo.com with the option 'Matches regexp'	Websites that contain "youtube.com" or "googlevideo.com" in the URLs
youtube.com googlevideo.com with the option 'Does not matche regexp'	Websites that do not contain "youtube.com" or "googlevideo.com" in the URLs

Example Regular Expression (rexep)	Result
Website Domain Name Field using "Matches regexp"	e.g. Web :: Top Website Domains report
windows	Websites that contain "windows" in their URL
^windows	Websites that have URLs starting with "windows"
windows.com\$	Websites that have URLs ending with "windows.com"
^windows.com\$	Websites that exactly match "windows.com"
Logon Name Field using "Matches regexp" or "Does not match regexp"	e.g. Identity :: Directory Logins report
laura.ashton	The user "laura.ashton"
laura.ashton robert.schmidt	The users "laura.ashton" and "robert.schmidt"
File/Folder Name Field	"Matches regexp"
sales profit loss	All filenames or directory names that contain "sales", "profit", or "loss"
\\.mdb\$	All file activity involving .mdb files
\\.docx\$ \\.xlsx\$	All file activity involving Microsoft Word or Excel files
\\.wnry \\.zip	All file activity involving file extensions .wnry and .zip
\\Documents\\	All file activity involving a directory named "Documents"

Logging in with the rescue account	Details:
rescue credentials	Login: rescue Password: netfortaccess

BPF traffic filter for IDS and for the Traffic Monitor	BPF filter explained
Ignore traffic from a network range and a few singular hosts.	not net xx.xx.xx.0/20 and not host x.x.x.x and not host x.x.x.x
To exclude one host:	not host xx.xx.xx.xx
To exclude multiple hosts:	not host xx.xx.xx.xx and not host xx.xx.xx.xx and not host xx.xx.xx.xx
To exclude one port:	not port xx

Protocols	Using the Protocol filter menu
Include	From the Include Protocol filter menu e.g. Applications in Use report, select single or multiple protocols to include in the results
Exclude	From the exclude Protocol filter menu e.g. Applications in Use report, select single or multiple protocols to omit from the results

If you have any queries regarding regular expressions and queries used in the creating report and running search queries, please contact the NetFort support team who will be delighted to assist you <https://www.netfort.com/about-netfort/contact/>