New in v5.4 - two new fields in E2guardian log formats 7 & 8. (revised for v5.5)

searchterms and extflags

Searchterms has the searchterms used in a search that has been detected. This to make it easier to report on searchterms used. Since most users launching point is via a search engine, this is likely be the most useful thing to indicate trends in users' browsing.

Extflags (extension flags)

Prior to v5.4 the e2guardian access.log has not held the listening port, information on whether the request was proxied or transparent, or an indication of how the 'user' and 'group' has been arrived at.

To add all this information in the normal way would require the addition of at least 4 fields to the log, so to avoid this and keep the log as compact as possible a single 'extflags' field is added in the following format:-

listening_port:flags([P|T|I|L][|E][H|S|M]):user_source:group_source

where:-

listening_port is the port number e2g was listening on.

flags are:-

first character:
P – proxy request
T – Transparent request
I – ICAP request
L – tLs proxy request (Secure proxy)

optional middle character (requires addECHtoFlags to be set in e2guardian.conf)
E – Encrypted Client Hello (ECH) detected

final character
H – HTTP request
S - SSL (HTTPS) request
M – request within MITM

so:- 'PH' standard proxy http request
'PS' proxy https request (no MITM)
'PM' request within MITM session over proxied session
'TH' transparent http request
'TS' transparent https request (no MITM)
'TES' transparent https request with ECH
'TM' request within MITM session over transparent session

user_source is the authentication method source for the 'user' field
dnsa – dnsauth
port – port based auth
ip – ip auth
bearer_b – bearer basic auth
header – header auth
ident – ident auth
pf_basic – ProxyFirstBasic auth

group_source is the source for the filter group

This may be hard coded

dnsa – from dnsauth record

def - default

or the name of the maplist (or ipmaplist) defined in e2guardian.conf where a match has been found for the user. These are mapped to an authentication plug-in with the appropriate auth_* function in preauth.story

e.g.

defaultusermap,

ipmap,

portmap.

Examples	
8443:TS:dnsa:dnsa	listening on transparent https port 8443, transparent https, user and group from dns record
8443:TM:ip:ipmap	listening on transparent https port 8443, transparent MITM, user (ip) and group from ipmap
8080:PH:dnsa:dnsa	listening on proxy http port 8080, explicit proxy http, user and group from dns record
8080:PM:dnsa:dnsa	listening on http port 8080, transparent http, user and group from dns record
8080:TH:dnsa:dnsa	listening on http port 8080, transparent http, user and group from dns record
8080:TH::def	listening on http port 8080, transparent http, no auth matched, default group
8084:PH:port:portmap	listening on port 8084, explicit proxy http, user is port and group from portmap
8084:PH:ip:ipmap	listening on port 8084, explicit proxy http, user is ip and group from ipmap

Note that in v5.6 onwards the logformats are replaced by a more flexible templating system, which allows each of the fields above to be split out into separate log fields if required. But as default a format that is the same as logformat 7 is deployed which includes the ExtFlags composite field as described above.

Revised 9 April 2025