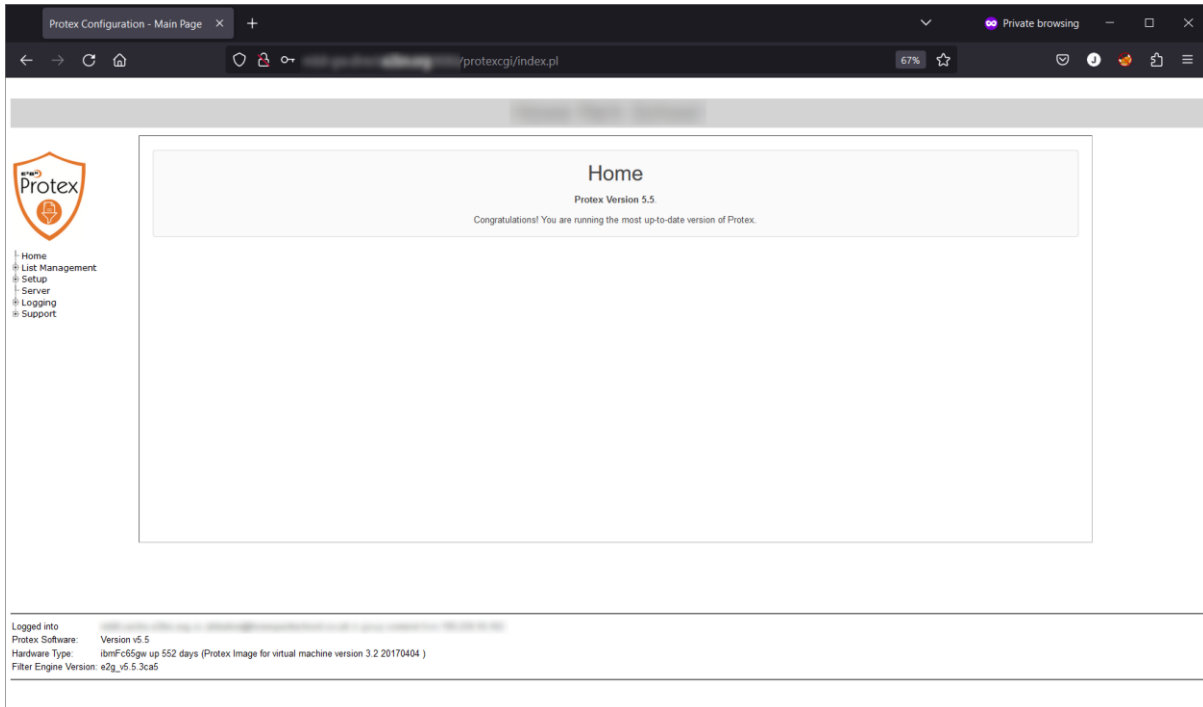
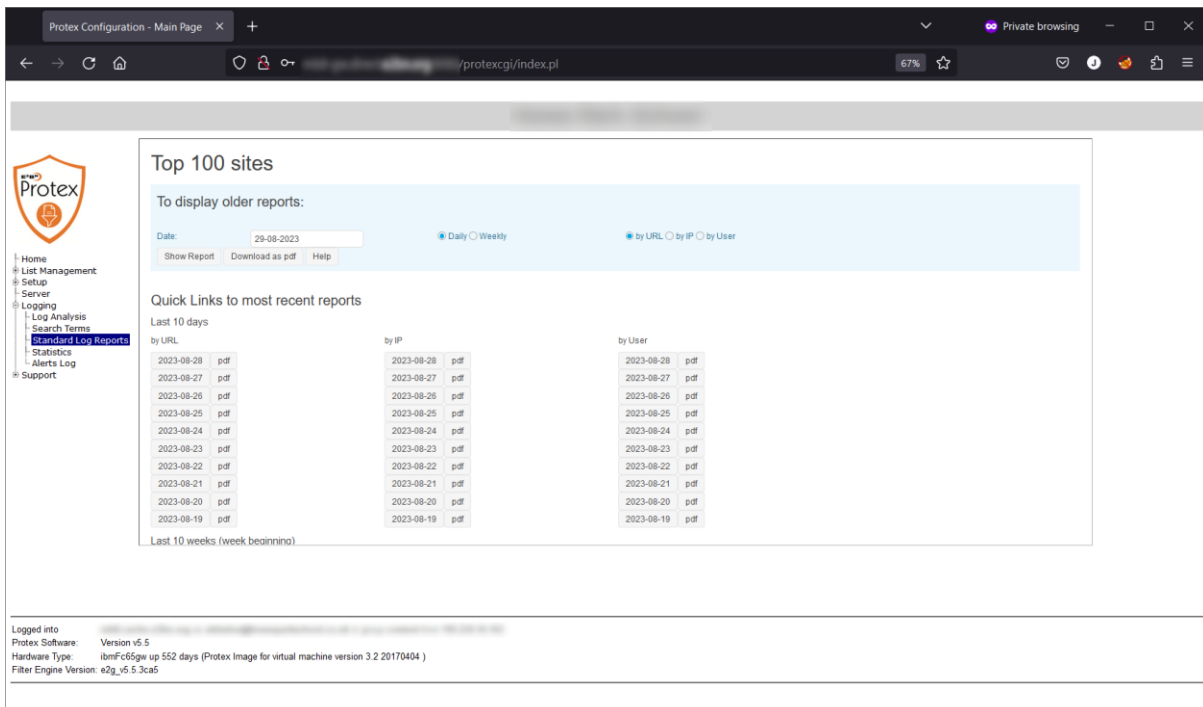


PROTEX – HOW TO ANALYSE AND ACCESS LOGS

1st Step: Logon on to Protex, <http://xxx.xxx.xxx.xxx> – xxx.xxx.xxx.xxx it the Protex’s LAN interface.



2nd Step: Expand Logging and select Standard Log Reports...



Standard Log Reports shows 100 Top Sites in the last 10 days, and by scrolling down, in the last 10 weeks. Reports are available on html format (left button with date) or PDF format (right button).

The screenshot shows the Protex Configuration interface. On the left is a navigation menu with options: Home, List Management, Setup, Server, Logging, Log Analysis (selected), Search Terms, Statistics, Alerts Log, and Support. The main content area is titled 'Standard Log Reports' and contains three columns of PDF report links. The first column is for 'Last 10 days', the second for 'Last 10 weeks (week beginning)', and the third for 'by User'. Each link includes a date and a 'pdf' label. At the bottom, there is a 'Logged into' section with system information: Protex Software: Version v5.5, Hardware Type: ibmF65gw up 552 days (Protex Image for virtual machine version 3.2 20170404), and Filter Engine Version: e2g_v5.5.3ca5.

Note: by user reports are only available if AD connection is working or devices are using Protex4Remote Google Chrome extension.

3rd Step: If it is necessary to look in depth the Protex logs, Log Analysis must be clicked:

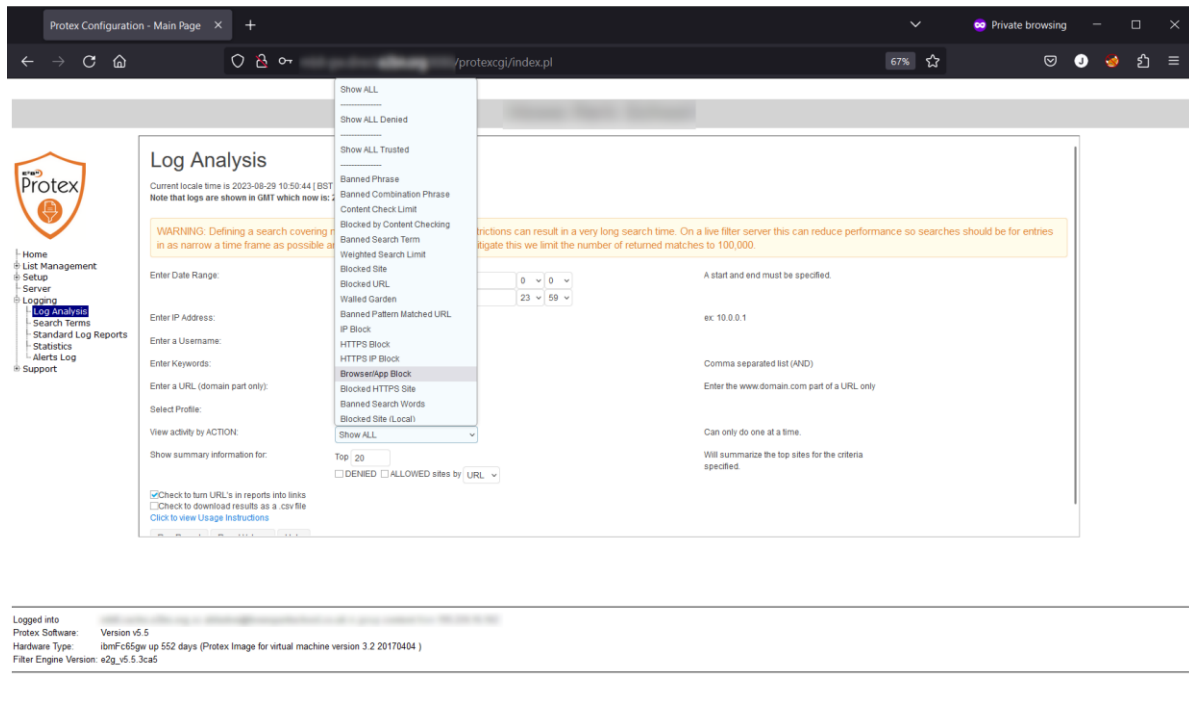
The screenshot shows the Protex Configuration interface with the 'Log Analysis' section active. The left navigation menu is the same as in the previous screenshot. The main content area is titled 'Log Analysis' and includes a warning message: 'WARNING: Defining a search covering multiple days or with no other restrictions can result in a very long search time. On a live filter server this can reduce performance so searches should be for entries in as narrow a time frame as possible and with some other criteria. To mitigate this we limit the number of returned matches to 100,000.' Below the warning are several input fields for search criteria: 'Enter Date Range' (Start Date: 29-08-2023, End Date: 29-08-2023), 'Enter IP Address' (ALL), 'Enter a Username' (ALL), 'Enter Keywords' (ALL), 'Enter a URL (domain part only)' (ALL), 'Select Profile' (dropdown menu with options: ALL, E2BN Middle, E2BN Primary, E2BN Secondary, E2BN Staff, m08 Staffnomadm), and 'View activity by ACTION' (dropdown menu). There are also checkboxes for 'Check to turn URL's in reports into links' and 'Check to download results as a csv file'. At the bottom, the same 'Logged into' section with system information is visible.

Log Analysis can filter results by date and hour, narrowing down the scope of data which needs to be obtained.

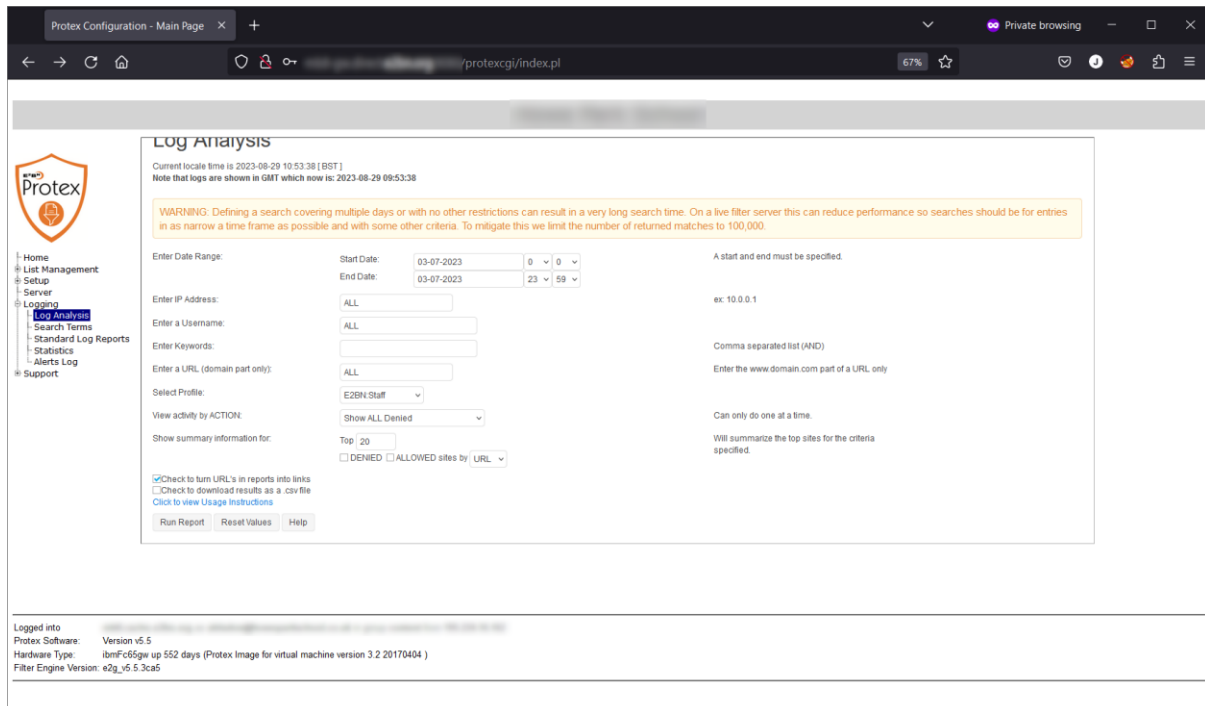
If the device's IP address is known, results can be filtered to only match that device's IP address.

URL's keyword or URL's domain can be used to filter results as well.

It is possible to filter results by profile and by classification:



In the following example, it is shown denied access on the Staff Profile on the 3rd of July:



Click on “Run Report” button to run the report...

Protex Configuration - Main Page

Protex

Log Analysis

Current locale time is 2023-08-29 10:54:30 [BST]
 Note that logs are shown in GMT which now is: 2023-08-29 09:54:30

WARNING: Defining a search covering multiple days or with no other restrictions can result in a very long search time. On a live filter server this can reduce performance so searches should be for entries in as narrow a time frame as possible and with some other criteria. To mitigate this we limit the number of returned matches to 100,000.

Refresh Report

Report information for:
 Start Date: 2023-07-03 00:00:00 | End Date: 2023-07-03 23:59:59 | Username: ALL | IP: ALL | LogDir: /home/ldlog/1/ | Action: denAll | URL: ALL

| | | | |
|---------------------------------------|------------------------------------|---------------------------------|---|
| 2023-07-03 06:49:30 10.01.129.5 8084 | SES-Staff-LTS1.howepk.school.local | E2BN Staff | https://howepk.school.co.uk/443 |
| 2023-07-03 07:03:24 10.01.129.80 8084 | E2BN Staff | https://88.221.41.37-443 | SSL SITE : *DENIED* Certificate supplied by server was not valid: hostname mismatch |
| 2023-07-03 07:05:54 10.01.129.5 8084 | E2BN Staff | https://plug.chartbeat.net/zing | PROXY : *DENIED* blocked site: plug.chartbeat.net |
| 2023-07-03 07:06:09 10.01.129.5 8084 | E2BN Staff | https://plug.chartbeat.net/zing | PROXY : *DENIED* blocked site: plug.chartbeat.net |
| 2023-07-03 07:06:24 10.01.129.5 8084 | E2BN Staff | https://plug.chartbeat.net/zing | PROXY : *DENIED* blocked site: plug.chartbeat.net |
| 2023-07-03 07:10:04 10.01.129.5 8084 | E2BN Staff | | |

Logged into
 Protex Software: Version v5.5
 Hardware Type: ibmF65gw up 552 days (Protex Image for virtual machine version 3.2 20170404)
 Filter Engine Version: e2g_v5.5.3ca5

Optionally, if the denied box is ticked...

Protex Configuration - Main Page

Protex

Log Analysis

Current locale time is 2023-08-29 10:55:15 [BST]
 Note that logs are shown in GMT which now is: 2023-08-29 09:55:15

WARNING: Defining a search covering multiple days or with no other restrictions can result in a very long search time. On a live filter server this can reduce performance so searches should be for entries in as narrow a time frame as possible and with some other criteria. To mitigate this we limit the number of returned matches to 100,000.

Enter Date Range: Start Date: 03-07-2023 0 0 End Date: 03-07-2023 23 59

Enter IP Address: ALL

Enter a Username: ALL

Enter Keywords: ALL

Enter a URL (domain part only): ALL

Select Profile: E2BN Staff

View activity by ACTION: Show ALL Denied

Show summary information for: Top 20 DENIED ALLOWED sites by URL

Check to turn URL's in reports into links
 Check to download results as a csv file
[Click to view Usage Instructions](#)

Run Report Reset Values Help

Logged into
 Protex Software: Version v5.5
 Hardware Type: ibmF65gw up 552 days (Protex Image for virtual machine version 3.2 20170404)
 Filter Engine Version: e2g_v5.5.3ca5

The following results will be available:

Log Analysis

Current locale time is 2023-08-29 10:55:51 [BST]
 Note that logs are shown in GMT which now is: 2023-08-29 09:55:51

WARNING: Defining a search covering multiple days or with no other restrictions can result in a very long search time. On a live filter server this can reduce performance so searches should be for entries in as narrow a time frame as possible and with some other criteria. To mitigate this we limit the number of returned matches to 100,000.

Refresh Report

Report information for:
 Start Date: 2023-07-03 00:00:00 | End Date: 2023-07-03 23:59:59 | Username: ALL | IP: ALL | LogDir: /home/dlog11/ | Action: denAll | URL: ALL

| Rank | URL | Hits | % DENIED | % of Total Requests |
|------|----------------------------|------|----------|---------------------|
| 1 | ping.chartbeat.net | 19 | 20.00 | 20.00 |
| 2 | 17.57.163.28 | 15 | 15.79 | 15.79 |
| 3 | c.apple.news | 10 | 10.53 | 10.53 |
| 4 | geo.yahoo.com | 9 | 9.47 | 9.47 |
| 5 | pages.blackhawknetwork.com | 8 | 8.42 | 8.42 |
| 6 | howeparkschool.co.uk | 7 | 7.37 | 7.37 |
| 7 | guroc.eath.com | 4 | 4.21 | 4.21 |
| 8 | 23.206.147.40 | 3 | 3.16 | 3.16 |
| 9 | ssc-cms.3sacross.com | 2 | 2.11 | 2.11 |
| 10 | sds.pltagrounds.pl | 2 | 2.11 | 2.11 |
| 11 | encyclofedia0.gastatic.com | 2 | 2.11 | 2.11 |
| 12 | cdn-ol.immworldwide.com | 2 | 2.11 | 2.11 |

Logged into: [redacted]
 Protex Software: Version v5.5
 Hardware Type: ibmF65gw up 552 days (Protex Image for virtual machine version 3.2 20170404)
 Filter Engine Version: e2g_v5.5.3ca5

PROTEX – HOW TO ANALYSE AND SEARCH TERMS

1st step: select “Search Terms” and on Search Terms Analysis, you can perform searches by date interval, classification, by search engine, etc.

Search Term Analysis

This screen allows you to interrogate the search terms used. You can select either **allowed**, **blocked**, or **all** searches. The results can be ranked either by **search term**, or by total number of searches via each **search engine** and displayed **alphabetically** or **numerically** and the results for each listed engine may be displayed individually.

Multiple logs can be selected from the list (Ctrl-click on windows, cmd-click on Mac). If none are selected the current access log is used.

Start Date:

End Date:

Select: All Allowed Blocked

Rank: by search term by search engine

Order: Alphabetical Numerical

Engines: All Google Bing DuckDuckGo Qwant YouTube Yahoo
 Answers Other...
 Check to download results as a .csv file

2nd step: click on “Submit” button to see all the search terms that were performed on the 12th of September of 2023:

The screenshot shows a web browser window with the URL `mb8-gw.direct.e2bn.org:9080/protexcgi/index.pl`. The left sidebar contains a navigation menu with the following items: Home, List Management, Setup, Server, Logging, Log Analysis, Search Terms (highlighted), Standard Log Reports, Statistics, Alerts Log, and Support. The main content area is titled "Results:" and features a "Download as pdf" button. Below the button is a list of search terms with their respective counts:

| Count | Search Term |
|-------|--------------------------|
| 3 | active+music+digital |
| 2 | active+music |
| 1 | amazon |
| 2 | best+practise |
| 2 | callum+turner |
| 3 | callump |
| 9 | callum |
| 1 | currys+business |
| 1 | developing+experts+login |
| 2 | duplo+amusement+park |
| 1 | duplo+amusment+park |

At the bottom of the page, it says "Logged into" followed by a blurred username and password field.

3rd step: search for blocked search terms. The time interval was increased to pick up more easily blocked search terms:

The screenshot shows the same web browser window, but now displaying a search filter interface. The URL is `9080/protexcgi/index.pl`. The left sidebar is identical to the previous screenshot. The main content area contains a yellow informational box with the following text:

This screen allows you to interrogate the search terms used. You can select either **allowed**, **blocked**, or **all** searches. The results can be ranked either by **search term**, or by total number of searches via each **search engine** and displayed **alphabetically or numerically** and the results for each listed engine may be displayed individually.

Multiple logs can be selected from the list (Ctrl-click on windows, cmd-click on Mac). If none are selected the current access log is used.

The search filters are as follows:

- Start Date: 01-09-2023
- End Date: 08-09-2023
- Select: All Allowed Blocked
- Rank: by search term by search engine
- Order: Alphabetical Numerical
- Engines: All Google Bing DuckDuckGo Qwant YouTube Yahoo Answers Other...
- Check to download results as a .csv file

Buttons for "Submit" and "Help" are visible. Below the filters, the "Results:" section shows a "Download as pdf" button and a single search term:

| Count | Search Term |
|-------|-----------------------------------|
| 1 | e2bn+content+blocking+test+protex |

4th step: pick up the result and copy totally or partially the result onto Log Analysis “Enter Keywords” and run a report...

The screenshot shows the 'Log Analysis' search form in the Protex Configuration web interface. The form includes the following fields and options:

- Enter Date Range:** Start Date: 01-09-2023 00:00, End Date: 12-09-2023 23:59. A note states: "A start and end must be specified."
- Enter IP Address:** ALL. Example: 10.0.0.1
- Enter a Username:** ALL
- Enter Keywords:** E2bn content. Note: "Comma separated list (AND)"
- Enter a URL (domain part only):** ALL. Note: "Enter the www.domain.com part of a URL only"
- Select Profile:** ALL
- View activity by ACTION:** Show ALL. Note: "Can only do one at a time."
- Show summary information for:** Top 20. Note: "Will summarize the top sites for the criteria specified." Includes checkboxes for DENIED and ALLOWED sites by URL.
- Check to turn URL's in reports into links
- Check to download results as a .csv file
- [Click to view Usage Instructions](#)
- Buttons: Run Report, Reset Values, Help

... the result shows time of access, device IP Address, computer name and profile in use.

The screenshot shows the search results page in the Protex Configuration web interface. It includes the following information:

- Note that logs are shown in GMT which now is: 2023-09-12 15:07:39**
- WARNING:** Defining a search covering multiple days or with no other restrictions can result in a very long search time. On a live filter server this can reduce performance so searches should be for entries in as narrow a time frame as possible and with some other criteria. To mitigate this we limit the number of returned matches to 100,000.
- Refresh Report** button
- Report information for:** Start Date: 2023-09-01 00:00:00 | End Date: 2023-09-12 23:59:59 | Username : ALL | IP: ALL | Logdir : /home/dg/log/i1/ Action: All | URL: ALL
- Log Entry:** 2023-09-06 13:26:16 10.28.8084 - school.local E2BN:Staff
<https://www.google.com/search>
 ILLEGALHACKING : *URLMOD* *DENIED* Banned Search Words: blocking+content+e2bn+protex+test
- Total matches: 1 | Query Time: 3 seconds**