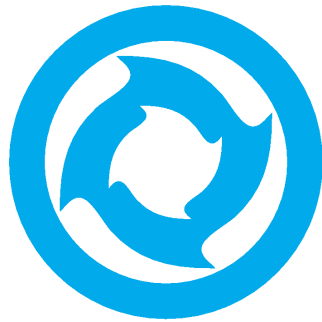


# Reporting log format



**CYan**

**NETWORK SECURITY**

---

# Table of Contents

1. Introduction .....	1
1.1. About CYAN Secure Web Appliance .....	1
1.2. About this Manual .....	1
1.2.1. Document Conventions .....	1
2. Log format .....	2
2.1. Categories details .....	3
2.2. Categories from IBM Content Security SDK .....	4
2.3. Application details .....	6
2.4. Restriction details .....	6
2.5. Blocking reason details .....	6
2.6. YouTube category details .....	7
A. Contact data .....	8
A.1. How to contact our sales department .....	8
A.2. How to contact our support department .....	8
A.2.1. Getting Support .....	8

---

# List of Figures

A.1. Version information of the Secure Web ..... 8  
A.2. Version information of the Reporting System ..... 8  
A.3. Support Package ..... 9

---

# 1. Introduction

## 1.1. About CYAN Secure Web Appliance

The all-in-one appliance hardware solution developed by CYAN Networks is an optimal customized platform that makes the deployment of Secure Web very easy. The Appliance includes a complete pre-installed Secure Web, as well as a Web Admin Interface used for the configuration of the entire machine. The product can easily be integrated into the already existing infrastructures. The configuration and other operating tasks are done with your favorite web browser, thus no knowledge about the integrated operating system is required.

## 1.2. About this Manual

This manual covers the format of the reporting log files. These log files are located in a log directory of the CYAN Secure Web installation (*/opt/cyan/sweb/logs/*). By default, the log files are named *sweb.reporting.log.<number>*. The *.<number>* part represents number of seconds since the epoch (1.1.1970) and it is not present in the most recent log file name. The log files are a good way to see what is happening on the Secure Web Proxy and it may help with debugging of traffic related issues.



The reporting log files are used internally and they are not intended to be a source of debugging information. They are deleted as soon as they are no longer needed by the internal processes. For safe manual inspection, however, can be additional reporting targets configured in the Reporting Web Admin Interface.

For a quick overview about the basic appliance setup, please see the documentation "CYAN Secure Web Appliance Getting Started Guide".

This manual is to be used with a Secure Web appliance with version 2.1.9 and above.

For additional documentation, please see our document repository on <http://www.cyan-networks.com/documentation>

### 1.2.1. Document Conventions



Indicates a potentially risky situation, leaving the appliance in an unusable state.



Indicates a potentially risky situation, causing malfunction of the solutions.



Indicates information that is substantial for successfully configuring and using the product.



Provides helpful information for the process of configuring and using the product.



Provides additional information about typical scenarios and best practices.

---

## 2. Log format

The reporting log file consists of lines where each line represents a set of fields separated by a semicolon (also known as the CSV format). A semicolon is used just for separating the fields. Any field that might contain an arbitrary semicolon is URL encoded (meaning that for example the semicolon character ";" will be represented as "%3B").

Some of the field are optional and must be manually turned on in the Web Admin Interface prior receiving any information related to these fields. They will remain empty until you do so. Each of the following fields having this necessity has a note about it in its description. Fields *Authentication instance*, *Authentication container*, and *Authentication credential* will also by default remain empty when an authentication attempt is not completely successful. This behavior can be again changed in the Web Admin Interface.

1. **Format ID** - determines what format is used in the current line. Currently, the highest format number is 1006.
2. **Date and time** - when was the record created, in ISO representation. ("2013-12-24 17:42:08.635+01:00")
3. **Request method** - URL encoded, examples: "GET", "PUT", "CONNECT".
4. **Request protocol** - URL encoded, example: "http".
5. **Host name** - URL encoded, example: "www.news.com".
6. **Path and file name of the requested file** - URL encoded, example: "/index.html".
7. **Web server response code** - example: "200" (OK), "0" (blocked request)
8. **Content length** - numeric value representing length of the requested file in bytes.
9. **MIME type** - URL encoded type of the requested file, example: "text/html", empty for blocked requests.
10. **Category number** - numeric identifier of the request's category. See [Section 2.1, "Categories details"](#) for the complete list of possible values. User defined categories (in menu *Services / Proxy Settings / URL Filter*) have numbers starting from 30000 in order they have been defined. Categories from IBM Content Security SDK have numbers starting from 40000 and there may be more that one category present if these categories are used. For the complete list of category number values please see [Section 2.2, "Categories from IBM Content Security SDK"](#).
11. **Application type** - Application type of the request. See [Section 2.3, "Application details"](#) for the complete list of possible values.
12. **Category name** - Name user-defined category if any matched at all (otherwise this field remains empty).
13. **User Agent** - User-Agent string from the request, for example "Mozilla/5.0 (X11; Linux x86\_64; rv:12.0) Gecko/20100101 Firefox/12.0". This field is optional.
14. **Referer** - The address of the previous web page from which a link to the currently requested page was followed. This field is optional.
15. **Client IP address**
16. **Server IP address**
17. **Number of bytes received from client** - numeric value.
18. **Number of bytes sent to client** - numeric value.

19. **Number of bytes received from server** - numeric value.
20. **Number of bytes sent to server** - numeric value.
21. **Connection duration** - Numeric value representing the duration of the connection in milliseconds.
22. **Cache hit** - value "cached" if the file was served from cache, empty otherwise.
23. **Restriction** - Blocking status of the connection. See [Section 2.4, "Restriction details"](#) for a complete list of possible values.
24. **Blocking reason** - Numeric value representing the reason for blocking the current connection. See [Section 2.5, "Blocking reason details"](#) for the complete list of possible values.
25. **Virus name** - virus name string, empty string if no virus found or virus name is not known.
26. **Authentication instance** - Name of the authentication instance through which the request was authenticated.
27. **Authentication container** - Name of an authentication container (e.g. group).
28. **Authentication credential** - Name of an authentication credential (e.g. user name).
29. **Connection filter** - Name of a filter applied to this connection.
30. **Web 2.0 site ID** - ID of a particular site in the list present in menu *Services / Profile tree / <profile> / Web 2.0 / Web 2.0 Policy* in the top level (list is grouped by site) or second level (list is grouped by usage) of the hierarchy. What kind of grouping is being used can be viewed and changed in menu *Services / Proxy Settings / Web 2.0 / Web 2.0 Policy*.
31. **Web 2.0 usage ID** - When grouping by usage is active (see previous item), this field matches the top level items in the list in *Services / Profile tree / <profile> / Web 2.0 / Web 2.0 Policy*.
32. **Web 2.0 control ID** - When grouping by site is active (see previous item), this field matches the second level items in the list in *Services / Profile tree / <profile> / Web 2.0 / Web 2.0 Policy*.
33. **YouTube ID** - Numeric representation of category under which was a request categorized. These categories can be found in menu *Services / Profile tree / <profile> / Web 2.0 / YouTube Categories*. See [Section 2.6, "YouTube category details"](#) for the complete list of possible values.
34. **S2C bandwidth bucket ID** - ID of bandwidth profile used for downstream connection. List of these profiles can be found in menu *Services / Proxy Settings / Bandwidth Management*.
35. **C2S bandwidth bucket ID** - ID of bandwidth profile used for upstream directed connection. List of these profiles can be found in menu *Services / Proxy Settings / Bandwidth Management*.
36. **Port** - Port number used in URL of a request. If no port is specified, the default value will be used. An example: `http://www.google.com` will the standard HTTP port 80 assigned, `localhost:9992/sweb` will have port number 9992 assigned.

## 2.1. Categories details

Category numbers resolve to the following list:

0	None		
1	Pornography	17	Education
2	Gambling	18	Games
3	Violence	19	Webmail

4	Drugs	20	Ads
5	Military & Weapons	21	Shopping
6	Sport	22	Jobs
7	News	23	Downloads
8	Finance	24	Phishing/Spyware/Virus/Proxies
9	Travel	25	Streaming Media
10	Religion	26	Communities
11	Government	28	Hosting
12	Real Estate	30	Health care
13	Mobile Phones	31	Humor
14	Dating	32	Search Engines/Directories
15	Vehicles	33	Pharmacies
16	Alcohol & Tobacco	34	Resources

## 2.2. Categories from IBM Content Security SDK

Category numbers resolve to the following list:

- 40000 Pornography
- 40001 Erotic / Sex
- 40002 Swimwear / Lingerie
- 40003 Shopping
- 40004 Auctions / Classified Ads
- 40005 Governmental Organisations
- 40006 Non-Governmental Organisations
- 40007 Cities / Regions / Countries
- 40008 Education
- 40009 Political Parties
- 40010 Religion
- 40011 Sects
- 40012 Illegal Activities
- 40013 Computer Crime / Hacking
- 40014 Political Extreme / Hate / Discrimination
- 40015 Warez / Software Piracy
- 40016 Violence / Extreme
- 40017 Gambling / Lottery
- 40018 Computer Games
- 40019 Toys
- 40020 Cinema / Television
- 40021 Recreational Facilities / Theme Parks
- 40022 Arts / Museums / Theatres
- 40023 Music / Radio Broadcast
- 40024 Literature / Books
- 40025 Humour / Cartoons

40026 News / Magazines  
40027 Webmail / Unified Messaging  
40028 Chat  
40029 Blogs / Bulletin Boards  
40030 Mobile Telephony  
40031 Digital Postcards  
40032 Search Engines / Web Catalogues / Portals  
40033 Software / Hardware  
40034 Communication Services  
40035 IT Security / IT Information  
40036 Web Site Translation  
40037 Anonymous Proxies  
40038 Illegal Drugs  
40039 Alcohol  
40040 Tobacco  
40041 Self-Help / Addiction  
40042 Dating  
40043 Restaurants / Entertainment Venues  
40044 Travel  
40045 Fashion / Cosmetics / Jewellery  
40046 Sports  
40047 Architecture / Construction / Furniture  
40048 Environment / Climate / Pets  
40049 Personal Web Sites  
40050 Job Search  
40051 Brokers / Stock Exchange  
40052 Financial Services / Insurance / Real Estate  
40053 Banking  
40054 Vehicles  
40055 Weapons / Military  
40056 Health  
40057 Abortion  
40059 Spam URLs  
40060 Malware  
40061 Phishing URLs  
40062 Instant Messaging  
40066 General Business  
40073 Banner Advertisements  
40076 Social Networking  
40077 Business Networking  
40078 Social Media  
40079 Web Storage



40080 Category 80

## 2.3. Application details

Currently supported applications:

0	Unknown/Untested		
1	Audio/Video	10	PDF file
2	Image	12	Messenger applications
3	Archive	13	Web Proxy
4	Executable	14	Skype
5	Binary file	15	Remote management tools
6	Office application		
7	Java or ActiveX content	97	Tunnels
8	iTunes request	98	Trusted
9	Flash animation	99	Text

## 2.4. Restriction details

These values show the status of the connection:

0	Connection allowed
1	Connection denied
2	Connection allowed because of SUP policy override

## 2.5. Blocking reason details

Reason why the connection was blocked:

407	Request not authenticated
1001	Method not allowed
1002	Protocol not allowed
1003	Proxy request not allowed
1004	Host request not allowed
1005	IP request not allowed
1006	Non-SSL tunneling not allowed through HTTPS proxy
1007	Non-HTTP requests not allowed through HTTPS proxy
1008	SSL Certificate error
2001	URL category denied
3001	Application denied
3101	Content (MIME) type denied
3201	File extension denied
3301	Request to localhost not allowed
3401	Blocked by Web 2.0 filter
3501	Blocked by YouTube filter
4001	Virus detected

- 4002 Error during virus scanning
- 4003 Invalid license for virus scanning
- 5001 Deep Archive Inspection error

## 2.6. YouTube category details

Values of all the YouTube categories:

- |    |                  |    |                           |
|----|------------------|----|---------------------------|
| 0  | Unknown          | 17 | Science & Technology      |
| 1  | Film & Animation | 18 | Movies - Anime/Animation  |
| 2  | Autos & Vehicles | 19 | Movies                    |
| 3  | Music            | 20 | Movies - Comedy           |
| 4  | Pets & Animals   | 21 | Movies - Documentary      |
| 5  | Sports           | 22 | Movies - Action/Adventure |
| 6  | Travel & Events  | 23 | Movies - Classics         |
| 7  | Short movies     | 24 | Movies - Foreign          |
| 8  | Videoblogging    | 25 | Movies - Horror           |
| 9  | Gaming           | 26 | Movies - Drama            |
| 10 | Comedy           | 27 | Movies - Family           |
| 11 | People & Blogs   | 28 | Movies - Shorts           |
| 12 | News & Politics  | 29 | Shows                     |
| 13 | Entertainment    | 30 | Movies - SciFi/Fantasy    |
| 14 | Education        | 31 | Movies - Thriller         |
| 15 | Howto & Style    | 32 | Trailers                  |
| 16 | Nonprofits       |    |                           |

---

## Appendix A. Contact data

### A.1. How to contact our sales department

Tel.: +43 (1) 33933-0  
Email: [sales@cyan-networks.com](mailto:sales@cyan-networks.com)

### A.2. How to contact our support department

Tel.: +43 (1) 33933-333  
Email: [support@cyan-networks.com](mailto:support@cyan-networks.com)

#### A.2.1. Getting Support

In case you should have any technical problems, or questions and would like to get support from our team, we kindly ask you to provide us with the following information:

- Description of your question or problem
- The version information of the product:
  - The version information of Secure Web can be found after logging into the Web Admin Interface in the top part of the screen:



Figure A.1. Version information of the Secure Web

- The version information of the Reporting System can be found after login in the top part of the screen of the Web Admin Interface:



Figure A.2. Version information of the Reporting System

- All the information contained in the screen found in menu *Services / Services / Overview*
- In the case authentication is activated, provide us with the method in place (via Windows Agent, via Linux Agent, etc.)
- The deployment method of the Appliance (Out-of-line, In-Line, DMZ)
- The operation mode of the Appliance (dedicated mode, transparent mode)

- Information about the environment (proxy cascades that are used, firewalls and gateways involved in the infrastructure that are of relevance to the Appliance)

The appliance interface provides the possibility to create a support package that includes the configuration and log files of the system. This package can help us to track down the issue easier and faster. Please attach this package to your e-mail.

In order to create a support pack, navigate to menu *Appliances / Maintenance / Support* and click on the *Download* button. You may select the files you want to provide to our support team and then download a package, which we kindly ask you to send to our support email address.

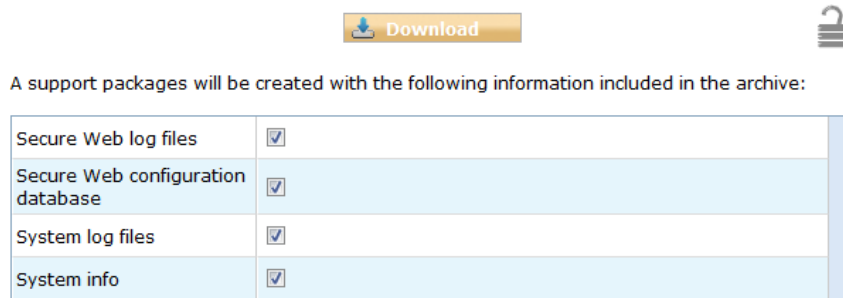


Figure A.3. Support Package

Further documentation about the product as well as technical white papers that describe certain use cases can be found in our documentation repository on our homepage:

<http://www.cyan-networks.com/documentation>