

Syslog Integration with Barracuda Content Shield

<https://campus.barracuda.com/doc/92766352/>

You can export log information from your **BCS Plus** account to your custom logging server using the Syslog feature as described below. Syslog data is available for the following traffic:

- **Web Filtering Component (WFC) log:** Web traffic logs generated by the BCS agent Web Filtering Component (WFC), or when the Barracuda Web Security Gateway is integrated with BCS.
- **Chromebook**
- **DNS proxy**
- **ATP**

Configure Your On-Site Syslog Server and Firewall

On your syslog server, configure the following:

- Default port is 6514, or whatever port your administrator decides to use
- TLS mode

On your firewall, make sure that traffic from the following IP addresses, depending on your region, are allowed to access the configured port on your syslog server:

- AWS East Region: 18.211.131.227 and 18.211.158.158
- AWS EU Region: 108.128.34.0 and 63.32.36.170

Configure the BCS Syslog Feature

1. Log into your BCS account and go to the **ACCOUNT SETTINGS** page.
2. On the lower right of the screen, click **Configure Syslog**.
3. In the Configure Syslog pop-up window:
 1. Set **Enable Syslog** to *ON*.
 2. Enter the **Server Address** and **Port** of your syslog server.
 3. Click **Save**.

Syslog Configuration

Enable Syslog

☐ OFF

Server Address and Port

12.12.12.12

514

?

CANCEL

SAVE

To edit the above values after you save them, click **EDIT SYSLOG CONFIGURATION**.

When BCS connects with your syslog server, the page displays this message:

Syslog Configuration

Export logs to your custom logging server

✓

Active (100.102.48.100)
Last synced August 8th, 2019 8:32 AM

EDIT SYSLOG CONFIGURATION

REMOVE SYSLOG

If BCS cannot connect to your syslog server, the page displays this message:

Syslog Configuration

Export logs to your custom logging server

!

Failed to connect (100.102.48.100)

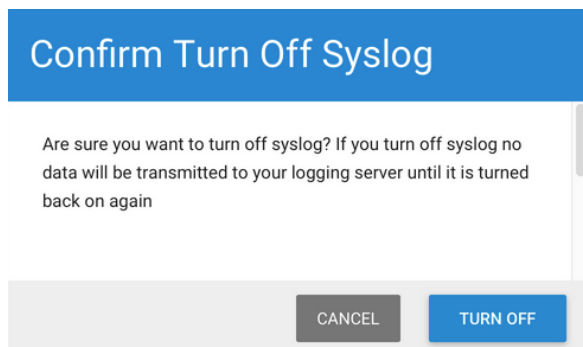
EDIT SYSLOG CONFIGURATION

REMOVE SYSLOG

Turn off Syslog

To stop BCS from sending syslog data to your syslog server:


1. On the ACCOUNT SETTINGS page, click **EDIT SYSLOG CONFIGURATION**.
2. In the confirmation pop-up window, click **TURN OFF**. You can turn syslogs back on later by reversing the procedure.



After you turn off Syslog, the following message is displayed on the page:

Syslog Configuration

Export logs to your syslog server

 **Inactive (12.12.12.12)**

Last Synced Unknown

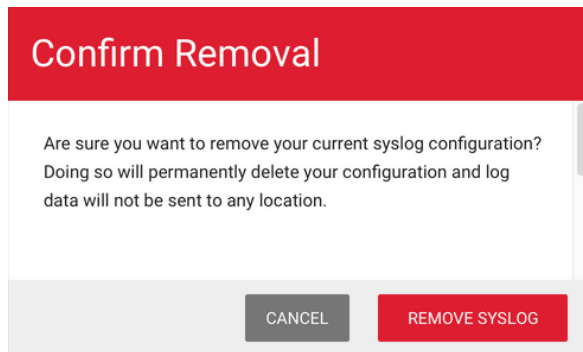
EDIT SYSLOG CONFIGURATION

[REMOVE SYSLOG](#)

Disconnect BCS From Your Syslog Server

1. On the ACCOUNT SETTINGS page, click **REMOVE SYSLOG**.
2. In the confirmation pop-up window, click **REMOVE SYSLOG**.

If you want to connect with your syslog server at a later time, you will need to follow instructions to **Configure Syslog** as described above.



Logs and Data Formats

Web Access Logs

Web access logs are generated either by the BCS agent Web Filtering Component (WFC), Chromebooks, DNS Proxy traffic, or the Barracuda Web Security Gateway when integrated with BCS. Examples of each type of log entry follows. This log data has the following format:

Header Format:

```
bcs-remote <traffic-log>[]:
```

In this header, traffic-log type can be any of:

- wca-logs (for WFC traffic)
- wsg-logs (for traffic when the Barracuda Web Security Gateway is integrated with BCS)
- chromebook-logs
- dns-logs (for DNS Proxy traffic)

Data Format:

```
<timestamp> <src_ip> <host/name> <username> <dst_ip> <action> <url>  
<::categories> <::supercategories> <content_type> <referrer>
```

Sample log output for each traffic type:

```
Jun 23 21:28:01 bcs-remote wca-logs[]: 2020-06-23T21:28:01.707Z 10.1.2.214  
wfdev-PC6 [wfdev] 198.185.159.176 ALLOWED  
http://www.tekdefense.com/universal/images/overlay-arrow-left.png [Computing
```

```
& Internet] [Technology] http://www.tekdefense.com/downloads/
Jun 23 21:26:48 bcs-remote wsg-logs[]: 2020-06-23T21:31:15.193Z 10.42.246.146
cuda229.wfdev.barracuda.com [anonymous] 10.42.246.146 ALLOWED
https://data.cnn.com/ [News] [News and Information] -

Jul 8 18:11:21 bcs-remote chromebook-logs[]: 2020-07-08T18:10:43+00:00
172.13.185.58 - [jdoe@gmail.com] 23.205.64.7 ALLOWED
http://news.mit.edu/sites/mit.edu.newsoffice/files/styles/article_cover_image
_small/public/images/2020/MIT-Brain-Electro-01_1.jpg?itok=mpB048Fm
[Educational Reference] [Education] http://news.mit.edu
Jun 19 18:16:29 bcs-remote dns-logs[]: 2020-06-19T14:20:35+00:00
198.35.20.112 - [-] - DENIED poker.com [Gambling in General] [Adult
Recreation or Illegal] -
```

These sample logs are described below:

Sample BCS WFC agent log output: The 'wca-logs' in the header portion in the first line signifies log data from the BCS WFC agent.

- Source IP address = 10.1.2.214
- Host/name = wfdev-PC6
- Username = wfdev
- Destination IP address = 198.185.159.176
- Action = ALLOWED
- URL = http://www.tekdefense.com/universal/images/overlay-arrow-left.png
- Category = Computing & Internet
- Supercategory = Technology
- Referrer = http://www.tekdefense.com/downloads/

Sample BCS with Barracuda Web Security Gateway log output: The 'wsg-logs' in the header portion in the second line signifies log data from [Barracuda Content Shield Integrated With the Web Security Gateway](#).

- Source IP address = 10.42.246.146
- Host/name = cuda229.wfdev.barracuda.com
- Username = anonymous
- Destination IP address = 10.42.246.146
- Action = ALLOWED
- URL = https://data.cnn.com/
- Category = News
- Supercategory = News and Information
- Referrer = [none]

Sample Chromebook log output: The 'chromebook-logs' in the header portion in the third line

signifies log data from Chromebook traffic.

- Source IP address = 172.13.185.58
- Host/name = empty (no value, indicated by a dash '-')
- Username = jdoe@gmail.com
- Destination IP address = 23.205.64.7
- Action = ALLOWED
- URL =
http://news.mit.edu/sites/mit.edu.newsoffice/files/styles/article_cover_image_small/public/images/2020/MIT-Brain-Electro-01_1.jpg?itok=mpBO48Fm
- Category = Educational Reference
- Supercategory = Education
- Referrer = http://news.mit.edu

Sample DNS Proxy log output: The 'dns-logs' in the header portion in the fourth line signifies log data from DNS proxy traffic.

- Source IP address = 198.35.20.112
- Host/name = [this field will be empty or populated with a '-']
- Username = [this field will be empty or populated with a '-']
- Destination IP address = [this field will be empty or populated with a '-']
- Action = DENIED
- URL = poker.com
- Category = Gambling in General
- Supercategory = Adult Recreation or Illegal
- Referrer = - (none listed)

ATP Log: This threat log data comes from the ATP virus scanner and has the following format:

Header Format:

```
bcs-remote atp-logs[]:
```

Data Format:

```
<timestamp> <hardware_uuid> <user> <action> <scan_path> <scan_filename>  
<scan_file_type> <threat_policy> <threat_info> <threat_type>
```

Sample ATP log output:

```
Jun 23 23:39:32 bcs-remote atp-logs[]: 2020-06-23T22:59:30.866Z wfdev-PC6  
[wfdev] malicious [C:\Users\wfdev\AppData\Local\Google\Chrome\User  
Data\Default\Cache\f_0005a5] [f_0005a5] application/zip quarantine VIRUS  
[Heuristics score 100]  
Jun 23 23:39:32 bcs-remote atp-logs[]: 2020-06-23T22:25:54.909Z wfdev-PC6  
[wfdev] malicious [C:\Users\wfdev\Downloads\Google_Adobe_FlashPlayer.exe.zip]
```

[Google_Adobe_FlashPlayer.exe.zip] application/zip quarantine VIRUS
[Heuristics score 100]

First line:

- Hardware_uuid = wfdev-PC6
- User = wfdev
- Action = malicious
- Scan path = C:\Users\wfdev\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0005a5
- Scan filename = f_0005a5
- Scan file type = application/zip
- Threat policy = quarantine
- Threat type = VIRUS
- Threat info = Heuristics score 100

Second line:

- Hardware_uuid = wfdev-PC6
- User = wfdev
- Action = maliciouse
- Scan path = C:\Users\wfdev\Downloads\Google_Adobe_FlashPlayer.exe.zip
- Scan filename = Google_Adobe_FlashPlayer.exe.zip
- Scan file type = application/zip
- Threat policy = quarantine
- Threat type = VIRUS
- Threat info = Heuristics score 100

Figures

1. SyslogServerEnable.png
2. SyslogActive.png
3. SyslogFailedToConnect.png
4. SyslogConfirmTurnOff.png
5. SyslogInactive.png
6. SyslogConfirmRemoval.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.