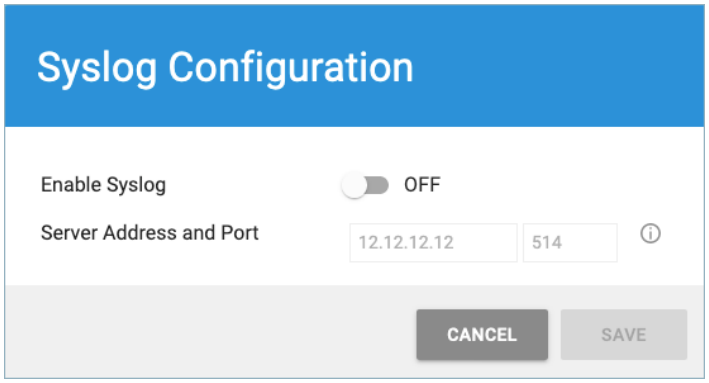
Syslog Integration with Barracuda Content Shield

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.

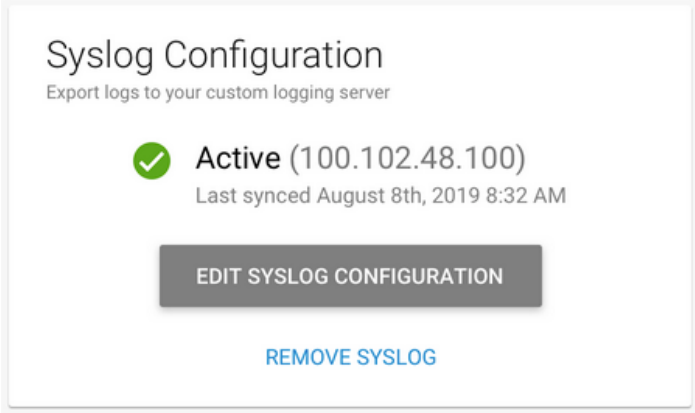
Configure Syslog

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**.

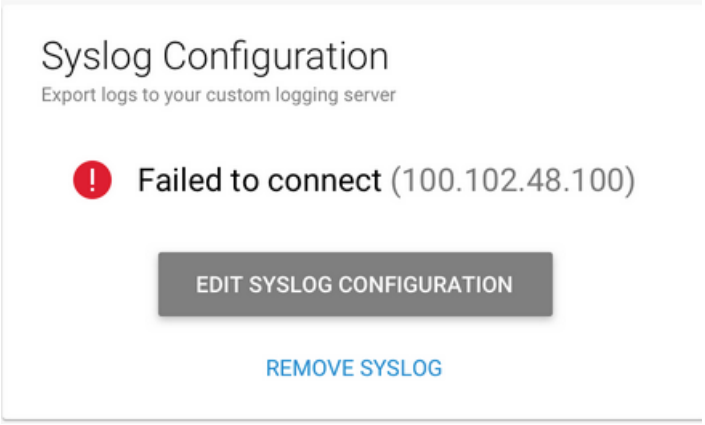


To edit the above values after you save them, click **EDIT SYSLOG CONFIGURATION**.

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



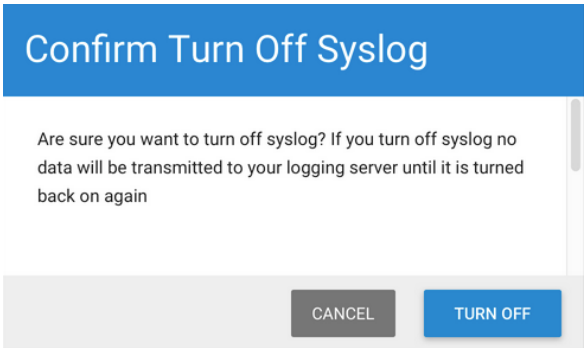
If BCS cannot connect to your syslog server, the page displays this message:



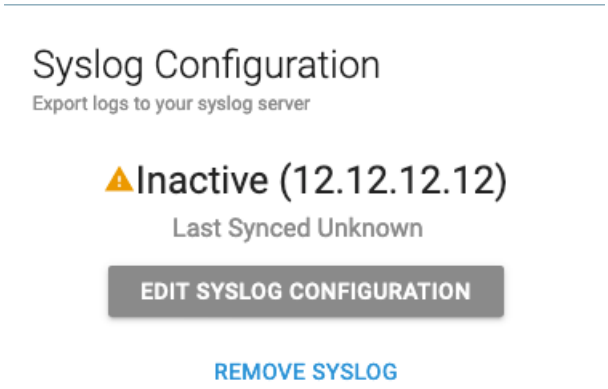
Turn off Syslogs

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.



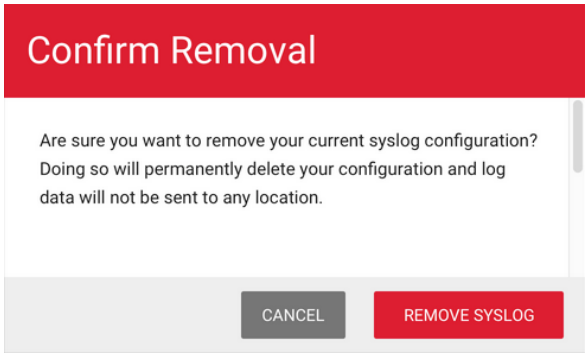
After you turn off Syslog, the following message is displayed on the page:



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

Header Format:

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

Data Format:

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

Sample log output:

```
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] -
```

In this example:

First line: 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/`

Second line: The 'wsg-logs' in the header portion of the second line signifies log data from the Barracuda Web Security Gateway when it has been integrated with BCS.

- 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]

ATP Log. This 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 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. SylogServerEnable.png
2. SyslogActive.png
3. SyslogFailedToConnect.png
4. SyslogConfirmTurnOff.png
5. SyslogInactive.png
6. SyslogConfirmRemoval.png