

## Secure Connector Logging

<https://campus.barracuda.com/doc/96026770/>

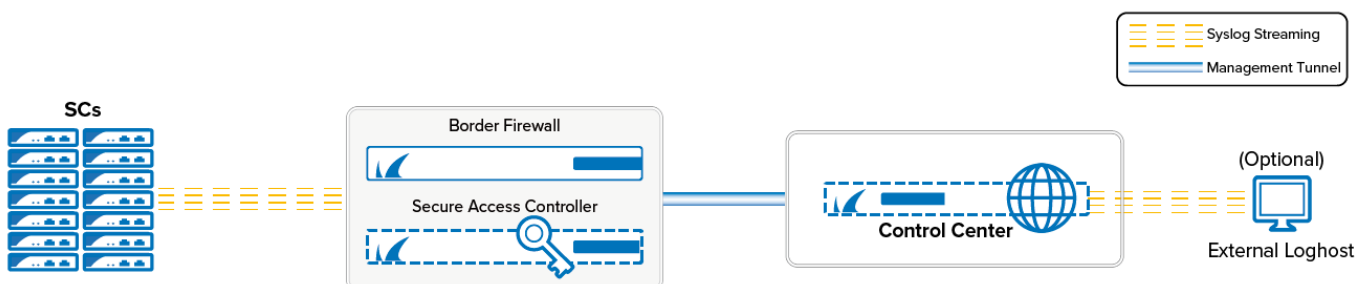
The Secure Connector creates logs for all system processes. By default, all log files on the Secure Connector are written to a temporary partition in volatile memory that is reset every time the device is rebooted. You can also configure the Secure Connector to stream the logs to the Control Center syslog server. For troubleshooting purposes, you can enable persistent logging directly to the SD card of the Secure Connector. Enabling persistent logging is not recommended because it decreases the lifetime of the SD card.

- **/var/phion/logs/c3c.log** – Log file for the communication between Secure Connectors and the Control Center.
- **/var/phion/logs/cudavpn.log** – Secure Connector VPN service log file.
- **/var/phion/logs/scactl.log** – Web UI log file
- **/var/phion/logs/shorewall/shorewall.log** – Logs connections denied by the Secure Connector Firewall service.
- **/var/phion/logs/shorewall/shorewall-init.log** – Log file containing firewall activation logs.

## Syslog Streaming

Syslog streaming to the Control Center allows you to process the log files using the Control Center syslog service. Syslog streaming allows you to store log files directly on the Control Center. The Secure Connector streams over UDP port 5144. The port can be changed if an external syslog server is used as the streaming target. The following log files are streamed:

- c3c.log
- controld.log
- scactl.log
- scad.log
- cudavpn.log
- UMTS.log

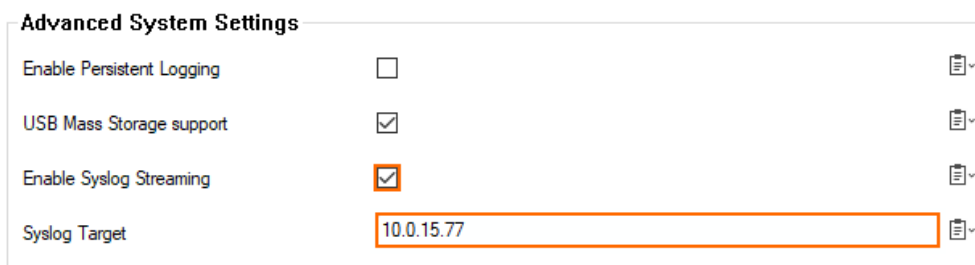


## Before You Begin

Configure the **Control Center Syslog Service** on the Control Center. For more information, see [Control Center Syslog Service](#).

## Configure Syslog Streaming on the Secure Connector

1. Go to **your cluster > Cluster Settings > Secure Connector Editor**.
2. Click **Lock**.
3. Double-click to edit the device or template.
4. In the left menu, click **Advanced**.
5. Select the **Enable Syslog Streaming** check box.
6. Enter the **Syslog Target** address and, optionally, port in the following format: IP address : port If the port is not specified, the default port 5144 is used.



**Advanced System Settings**

Enable Persistent Logging	<input type="checkbox"/>	
USB Mass Storage support	<input checked="" type="checkbox"/>	
Enable Syslog Streaming	<input checked="" type="checkbox"/>	
Syslog Target	10.0.15.77	

7. Click **OK** and **Activate**.

The logs are now streamed to your Control Center and stored in the **/phion0/mlogs/** directory. For more information, see [Control Center Syslog Service](#).

```
[root@cc620-216-227:/phion0/mlogs]# ls
c3c.Fri.00.log  c3c.Fri.11.log  c3c.Fri.22.log  c3c.Mon.09.log  c3c.Sat.07.log
c3c.Fri.01.log  c3c.Fri.12.log  c3c.Fri.23.log  c3c.Mon.10.log  c3c.Sat.08.log
c3c.Fri.02.log  c3c.Fri.13.log  c3c.Mon.00.log  c3c.Mon.11.log  c3c.Sat.09.log
c3c.Fri.03.log  c3c.Fri.14.log  c3c.Mon.01.log  c3c.Mon.12.log  c3c.Sat.10.log
c3c.Fri.04.log  c3c.Fri.15.log  c3c.Mon.02.log  c3c.Sat.00.log  c3c.Sat.11.log
c3c.Fri.05.log  c3c.Fri.16.log  c3c.Mon.03.log  c3c.Sat.01.log  c3c.Sat.12.log
c3c.Fri.06.log  c3c.Fri.17.log  c3c.Mon.04.log  c3c.Sat.02.log  c3c.Sat.13.log
c3c.Fri.07.log  c3c.Fri.18.log  c3c.Mon.05.log  c3c.Sat.03.log  c3c.Sat.14.log
c3c.Fri.08.log  c3c.Fri.19.log  c3c.Mon.06.log  c3c.Sat.04.log  c3c.Sat.15.log
c3c.Fri.09.log  c3c.Fri.20.log  c3c.Mon.07.log  c3c.Sat.05.log  c3c.Sat.16.log
c3c.Fri.10.log  c3c.Fri.21.log  c3c.Mon.08.log  c3c.Sat.06.log  c3c.Sat.17.log
[2015-11-30 12:39 CET] [-root shell-] [-Barracuda Networks-]
[root@cc620-216-227:/phion0/mlogs]#
```

## Web Interface Log File Viewer

Use the web interface to view the log files on the Secure Connector:

1. Log into the web interface.
2. Click the **Log** tab.

3. From the **Log file** drop-down list, select the log file.

Logs RETRIEVE LOCK

Log file Authentication





Number lines 50

```
2019 12 04 14:58:13 notice *00:00 sudo: www-data : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/opt/phon/bin/scctl --getconfigstate
2019 12 04 14:58:13 info *00:00 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
2019 12 04 14:58:14 info *00:00 sudo: pam_unix(sudo:session): session closed for user root
2019 12 04 14:58:20 notice *00:00 sudo: www-data : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/opt/phon/bin/scctl --getconfigstate
2019 12 04 14:58:20 info *00:00 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
2019 12 04 14:58:20 info *00:00 sudo: pam_unix(sudo:session): session closed for user root
2019 12 04 14:58:20 notice *00:00 sudo: www-data : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/opt/phon/bin/scctl --getconfigstate
2019 12 04 14:58:20 info *00:00 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
2019 12 04 14:58:28 info *00:00 sudo: pam_unix(sudo:session): session closed for user root
2019 12 04 14:58:28 info *00:00 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
2019 12 04 14:58:35 notice *00:00 sudo: www-data : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/opt/phon/bin/scctl --getconfigstate
2019 12 04 14:58:35 info *00:00 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
2019 12 04 14:58:35 info *00:00 sudo: pam_unix(sudo:session): session closed for user root
```

## Enable Persistent Logging

1. Go to **your cluster** > **Cluster Settings** > **Secure Connector Editor**.
2. Click **Lock**.
3. Double-click to edit the device or Secure Connector template.
4. In the left menu, click **Advanced**.
5. (Template only) Enable **Advanced Settings**.
6. Select **Enable Persistent Logging**.

**Advanced System Settings**

Enable Persistent Logging	<input checked="" type="checkbox"/>	
USB Mass Storage support	<input checked="" type="checkbox"/>	
Enable Syslog Streaming	<input type="checkbox"/>	
Syslog Target	<input type="text"/>	

7. Click **OK** and **Activate**.

## Figures

1. sc\_syslog\_streaming.png
2. sc\_syslog\_streaming01.png
3. sca\_Syslog\_Streaming\_03.png
4. logs\_select.png
5. sc\_logging01.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.