

Syslog and Log configuration

Purpose: The purpose of this document is to provide supplemental information regarding syslog configuration for the Spectracom SecureSync.

Table of Contents

Section 1: Syslog configuration.....	2
Section 2: Facility/Severity code combination for each log type.....	7
Section 3: Troubleshooting Syslog not working.....	8
Section 4: SecureSync software changes associated with Syslog.....	14
Section 5: Spectracom Tech Support	14

Section 1: Syslog configuration

The SecureSync can be configured to send either certain, or all, its log file entries from each of its log “types” (such as its Authentication log, Alarms log, Qual log, etc.) to a selected syslog server. A list of one or more syslog servers available on the network is first created and then one of these servers in the list can then be selected to send each of that log type’s entries to.

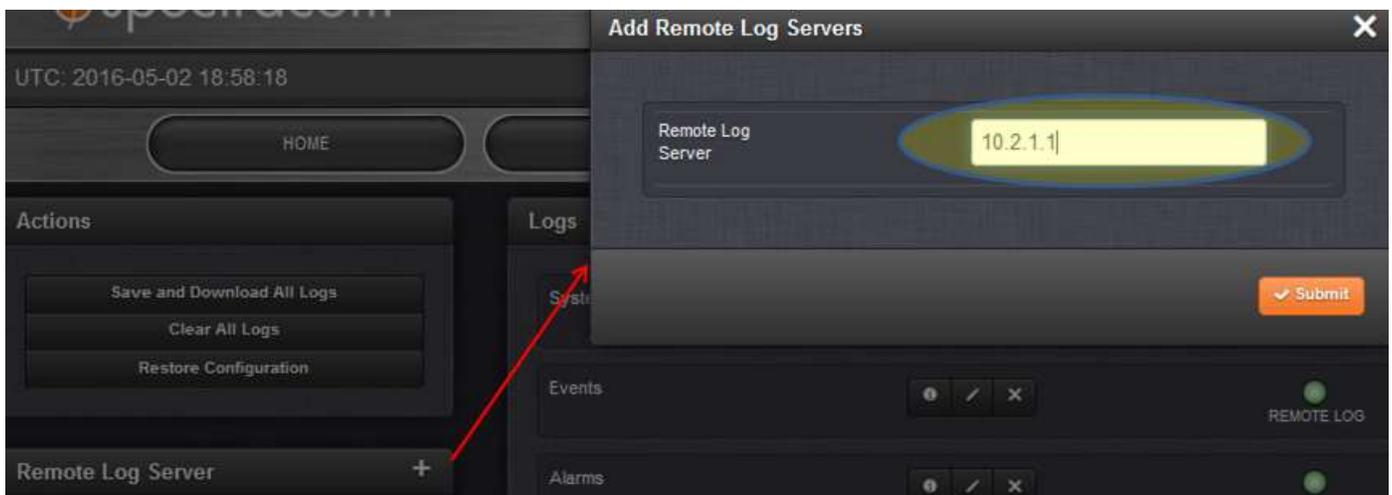
In order for the SecureSync to send all of its log entries from each log type to a syslog server, “**Remote Log**” needs to be enabled for each log type and the desired syslog server for that log type needs to be specified from the list of available servers (only one syslog server can be selected for each log type, but varying syslog servers can be selected to have each log type sent to a different syslog server -not all log entries have to go to the same syslog server, if desired).

By factory default, logs are sent to the selected/configured syslog server(s) on **port 514**. Software version 5.7.1 and above now allow the ability to optionally change/custom-configure this port number to use a number other than port 514.

As shown in the screenshot below, “**Remote Log Server**” (on the left side of the **Management -> Log Configuration** page of the browser) is a list of all syslog servers that can be chosen from, for each log type to be sent to. But just having one or more syslog servers listed here is not quite enough configuration to have any logs sent to these syslog servers.

First, add the desired syslog server(s) to the list of available syslog servers that each log type can be individually configured to be sent to (overall, multiple syslog servers can be listed, with each log file type being able to be sent to any one of the servers in this list).

On the left side of the **Management -> Log Configuration** page of the browser, press the “+” sign to the right of “**Remote Log Server**”. In the pop-up window that opens, enter the IP address or DNS name of a desired syslog server on the network and press Submit. Repeat as desired to enter any additional syslog servers you wish to be available for selection for individual logs to be sent to.



Note: Software versions 5.7.1 and above allow the Syslog port to be changed from the factory default port number “514” to a user-defined value. Verify if the Syslog port has been changed from “514” to a different number via the **Management -> Log Configuration** page of the browser (then click the “+” just to the right of “**Remote Log Server**” to open a pop-up window, as shown below):



Each log type that you wish to send its logs to a syslog server still needs to be defined and Remote logging enabled (its “Remote log” checkbox to the right of its three icons, if its syslogging is enabled).

Clicking on the middle of the three icons (the pencil) for a particular log type (such as the Timing log for example, as shown with the yellow circle below), will either display what syslog server its log entries will be sent to, or will allow you to choose which syslog server listed under “**Remote Log server**” that this log type should send its logs to- this selection is via a drop-down list of the syslog servers that have been added under “**Remote Log Server**”.

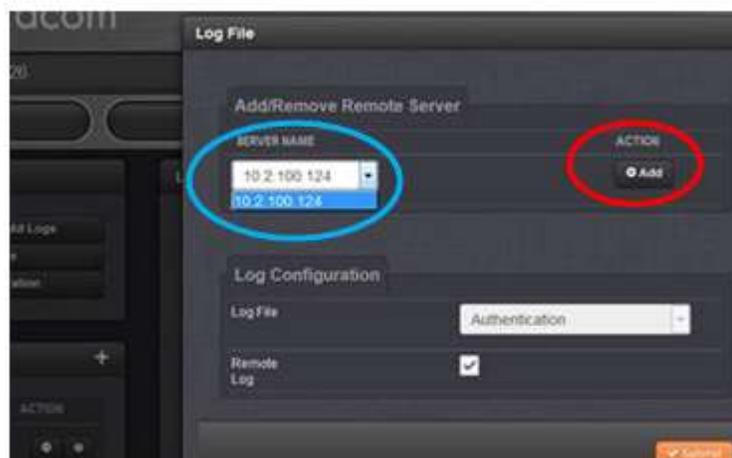


If there is a drop-down list present when pressing the middle icon, this particular log type has not yet been configured to send its log entries to a syslog server. Select the desired syslog server in the drop-down list (and verify the Remote log checkbox is selected). Then press the **Add** button.

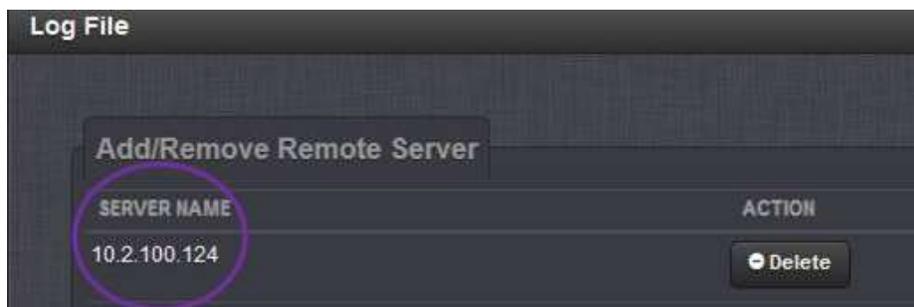
Because the log files can be individually configured as to which remote server it’s entries are sent to, each log file type (such as the System Log for example) needs to be individually configured to be sent to the desired remote server, before its logs will be sent to any remote server. You need to add (select) a Remote server from the list of previously added to “Remote Log servers” (on the left side of Log Configuration page).

To configure a “**Remote Server**” to each log type (this can’t be done as a single global setting for all its log files), press the middle icon (**Management -> Log configuration** page of the browser) for each log type you wish to send to a remote server.

Each log type of the SecureSync has its own “remote log” enable checkbox that also needs to be selected, if you desire for that file’s log entries to be sent to a specified syslog server. The “remote log” enable for each log file/type (such as the “Qualification” log for instance) is in the **Management -> Log configuration** page of the browser. For each log file that you wish for its logs to be sent to remote servers, click the middle of the three ICONS (the pencil ICON) for that log file. In the **server name**” drop-down of the pop-up window, select the particular syslog server you wish to send this log file to and then press the **Add** button.



Note the “**Server name**” drop-down field and the **Add** button will vanish after pressing the **Add** button:



Log entries for each log file can be stored internally, sent to a syslog server, or both (depending on the state of the “Local” and “Remote” log checkboxes for each log file)

Make sure the “**Remote Log**” checkbox is selected to be able to send associated log entries to a remote server (it is selected for all log files by Factory default”. But if it’s been since unchecked, its log entries won’t be able to be sent to a remote server).

“**Local log**”: When selected, this causes all log entries for this log file to be stored internal to the time server. If this checkbox is unselected, logs for this file will not be stored within the time server.



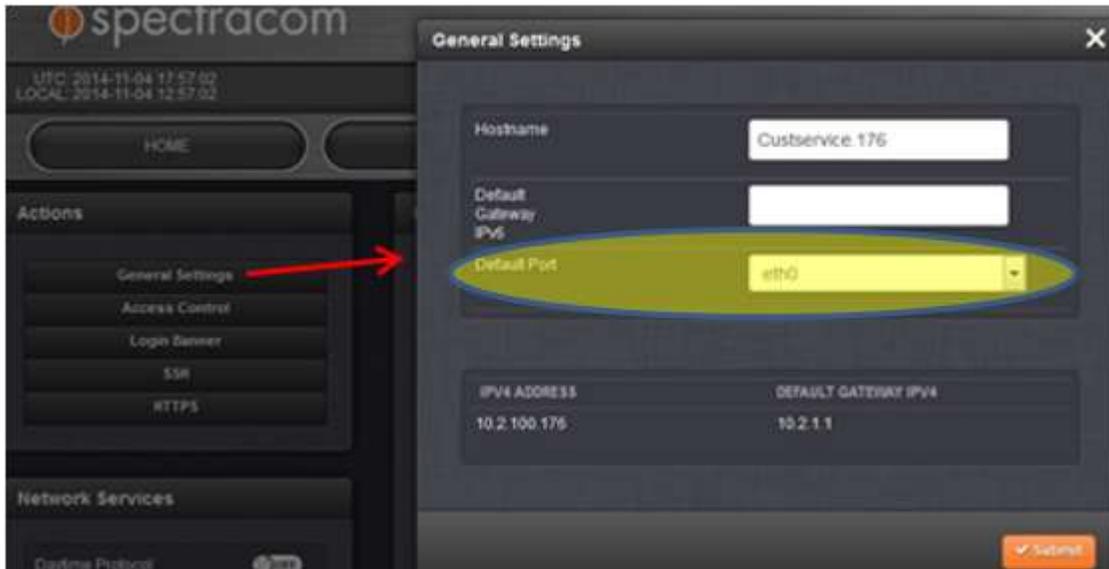
(Note about Facility/Priority Codes) Changing either/both the Facility and Priority codes for each log file will cause the associated log entries to be mapped/stored in the wrong internal log files (or possibly not stored internally at all). Refer to [Section 2](#) for more info.

Notice: Repeat this same process of selecting the desired syslog server, for each log file type you wish to send its log entries to a syslog server (Selecting a syslog server for one log file will not cause any other log files to have its logs also sent to a syslog server).

Main default port/default gateway configuration

With each log type having Remote Log enabled, the desired syslog server selected for each log file (and having the main default port/default gateway configured correctly, if the optional Model 1204-06 Gb Ethernet Option Card is installed) so that the SecureSync's log entries can be routed to the Syslog server.

The configuration for the default port/gateway is in the **Management -> Network Setup** page of the browser, **General Settings** button (as shown below), the SecureSync can now send its log entries to the configured syslog server. Any log entries sent to the local log will also be sent to this syslog server.



Section 2: Facility/Severity code combination for each log type

Important Note: Please be aware that the specific combination of the **Facility** and **Severity** codes for each log file (as also configured in the same pop-up window mentioned above) define which Log File (such as the Alarms Log, System Log, etc.) the Log entries are actually sent to in the SecureSync/syslog server.

Changing any of these two codes (Facility and/or Severity) for a Log File will prevent the associated Log entries from being stored in its coinciding Log File.

- Changing either or both codes for any Log File (having it match the same combination of another Log file) will result in the associated log entries that are supposed to be sent to that Log file actually being sent to/stored in another Log file. So, log files can become inter-mixed inside the SecureSync (Alarms log entries may be mixed in with the hourly GPS Qualification log entries. for instance), making it nearly impossible to review the logs in the browser, via the CLI. or if the logs bundle is downloaded from the unit and sent to Spectracom for review.
- Changing either or both codes for each Log File (and if the new combination doesn't apply to any available Log File) will result in all associated log entries destined to the original Log File (such as all System logs, or All Alarms logs for examples) not being stored at all within the time server (these entries will be lost)

For these reasons (unless it's desired not to store any log entries inside the time server) we do not recommend any of the Facility and/or Severity codes in the **Log Configuration** page be changed from the default settings.

Just in case either or both the two codes may have already changed. for any of the Log Files, below are the factory default values for each of the log file types:

Logtab	Facility code	Priority code
System	Local Use 7	Emergency
Events	Local Use 7	Alert
Alarms	Local Use 7	Critical
Timing	Local Use 7	Error
GPS Qual (Qualification)	Local Use 7	Warning
Oscillator	Local Use 7	Debug
Journal	Local Use 7	Notice
Update	Local Use 7	Information
Authentication	N/A	N/A

Note these values can be manually changed by a user back to their factory default settings. Or with software **versions 5.7.1 or above** installed, simply press the “**Restore Configuration**” button in the upper-left corner of the **Management -> Log configuration** page of the browser, as shown below, to restore all the Log configurations on this web page back to their default states.



Section 3: Troubleshooting Syslog not working

As for troubleshooting issues with Syslog, there is a **QPS Qualification log** entry asserted at the top of each hour (as confirmed/viewed in the **Tools-> Qualification log** page of the browser). With the log configuration for the Qual log having a desired Syslog server selected, and with its remote logging enabled (as described further above in [Section 1: Syslog configuration](#)), a new log entry should be sent to the one selected syslog server as well, at the top of each hour.

If this entry is sent to the Syslog server, the syslog function is working. But if the new log entry is sent to the Qual log inside the SecureSync, but not sent to the selected Syslog server, there is an issue with the syslog function (it could be an issue be with internal configuration, or external to the SecureSync).

A) Error message “500: Interval Server Error” reported when trying to enter a syslog server to the list of remote servers. Version 5.3.1 software is installed in the tine server.

- Upgrade the time server’s software to a version beyond version 5.3.1. Contact Tech Support for info on downloading and applying the latest version of software. Refer to [Section 5](#) for contact info.

B) SecureSync’s logs are not present in the syslog server (general syslog function troubleshooting)

Note: Temporarily disconnecting the GPS antenna (for even just a moment) on the rear panel is a good way to intentionally assert a Minor alarm (“GPS Antenna Problem”) for the Alarms log, to force a new log entry to be sent to the selected/configured Syslog server assigned to the Alarms log. If this intentional entry is sent to the configured syslog server, the SecureSync’s Syslog is operating normally (at least the Alarms log is configured correctly in the Syslog configs). The unit will continue to be useable time server while the antenna is being disconnected and reconnected.

Verify the SecureSync’s **syslog configs** are correct (**Management -> Log Configuration** page of the black/charcoal background web browser).

For each Log File type desiring to have its log entries sent to the selected syslog server:

- 1) Each listed Log File type (such as the System Log, Events Log, Alarms log, etc.,) on this page should have its “Remote log” checkbox selected

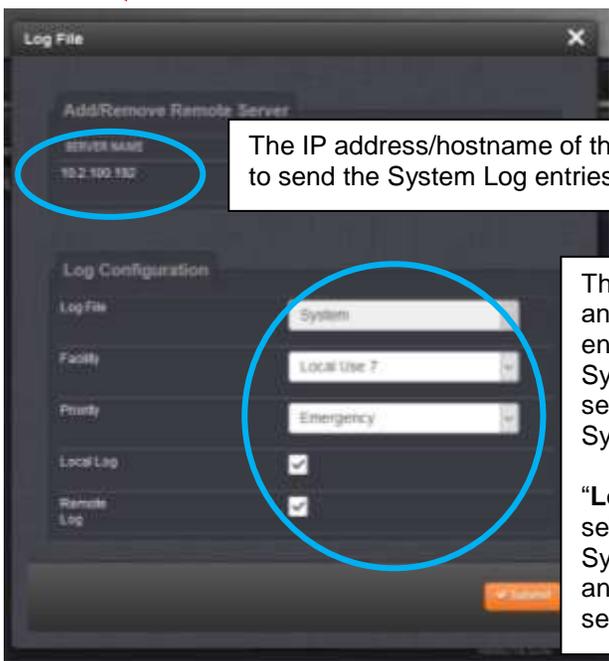


- 2) Each listed Log File type on this page needs the selected DNS name/IP address of the desired syslog server to send log entries to (click the middle of the three icons for each Log file)

Below is an example of the **System Log File** properly configured to send all System Log entries to the Syslog server at the address of **10.2.100.192** (and also storing System logs inside the SecureSync, in its **System Log file**)



Both **“Remote Log”** (for System log entries to be sent to Syslog) and **“Local Log”** (for internal storage of System log entries) are green/enabled



The IP address/hostname of the desired Syslog server to send the System Log entries to has been selected.

The specific combination of **“Local Use 7”** and **“Emergency”** routes all **System** log entries to the **System Log** file, so the System log entries can be sent to the selected Syslog sever and to the internal System Log file.

“Local Log” and **“Remote Log”** are both selected/enabled here, allowing the System Log entries to be stored internally and also sent to the selected Syslog server.

- If the Model 1204-06 Gb Ethernet Option Card (which adds three additional network interfaces to the rear panel) is installed in the back of the time server, and especially if the Syslog server(s) is not on the immediate subnet as the SecureSync, check the **main default port/gateway** is correct (**Management -> General Setup** page of the black/charcoal background web browser) as shown below.

The correct ethernet interface (and therefore the correct main default gateway) needs to be selected here, so that the time server’s log entries can be successfully routed to the syslog server, via its correct ethernet interface.



- If **“ping”** capability has not been disabled in the Syslog server(s), login to SecureSync’s cli interface (via a telnet or ssh session) and try pinging out to the syslog server’s address (there could be a network issue preventing the syslog server from being reachable).
- If listing syslog server(s) with its **DNS name (instead of IP address)** at least temporarily add a syslog server using its IP address. Then select this server for the logs to be sent to. If log entries start to be sent to this

syslog server, there is likely a problem associated with DNS configuration in the time server, or a network-related DNS issue occurring.

Note the **Primary and Secondary DNS servers** are configured in the **Management -> Network Setup** page of the web browser. Then click the middle of the three icons (the gear icon) for the applicable network interface (such as eth0 for instance).

- Perform a **tracpath** CLI command on the default syslog port 514 to see if there is a network routing issue between the SecureSync and the Syslog server.

Note: Software versions 5.7.1 and above allow the default syslog port number to be changed from port “514” to a user-defined value. Refer to the **Management -> Log configuration** page of the browser to see if the Syslog port has been changed to a different number.

Type: **tracpath -p 514 xxxx** (where **-p 514** defines the syslog port- “514” is the factory default syslog port- and where **xxxx** is the IP/hostname of the Syslog server).

This command should respond with a list, and the number of, network nodes between the SecureSync and the Syslog server (indicating “reached”)

Note: Software versions 5.7.1 and above allow the Syslog port to be changed from the factory default port number “514” to a user-defined value. Verify if the Syslog port has been changed from “514” to a different number via the **Management -> Log Configuration** page of the browser (then click the “+” just to the right of “Remote Log Server” to open a pop-up window, as shown below):



(Example tracpath command via CLI interface)

```

0 packets dropped by kernel
spadmin@Spectracom ~ $ tracpath -p 514 10.2.100.192
 1?: [LOCALHOST]                               pmtu 1500
 1: 10.2.100.192                               1.113ms reached
Resume: pmtu 1500 hops 1 back 128
spadmin@Spectracom ~ $

```

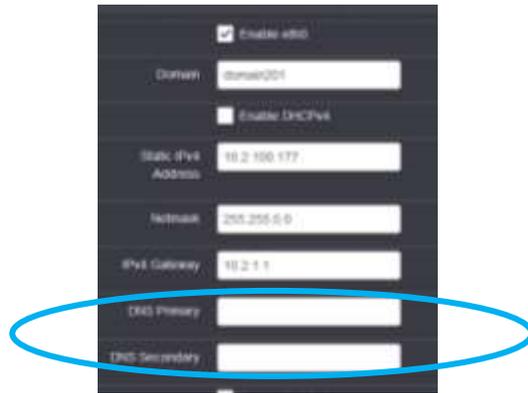
If the Syslog server not reachable using its DNS hostname

If the response indicates the Syslog server is not reachable, and you used its DNS hostname (instead of its IP address), perform the same command again, this time using the Syslog’s IP address. If its reachable with its IP address but not reachable using its hostname, there is an issue with DNS (either on the time server or on the network).

To quickly check the DNS configuration of the time server using the CLI interface, type **DNS4get X** (where X is the ethernet interface (such as 0, 1, 2 or 3) rotatable to the DNS server on the network. If the command responds no Domain Name Servers were found, DNS is not configured for the correct interface, or the Primary and Secondary DNS Servers for this interface have not yet been configured.

To verify, or configure, DNS via the web browser, navigate to the **Management -> Network Setup** page. Then press the center of the three icons (the gear icon) for the interface which is routable to the network’s

DNS server (such as eth0 for instance). Verify the configuration of the DNS servers in the pop-up window:



- **Perform a tcpdump/Windows Wireshark packet capture** on the same side of the switch as the time server (or use tcpdump in the time server itself (software versions 5.2.1 and above only), to see if log entries are being sent out the time server (and on the correct Ethernet interface, which is routable to the syslog server).

Optionally filter the packet capture for packets originating from the time server on the configured syslog port - default value of 514 (or with software versions 5.7.1 and above, the user-defined port number if it's been changed), to confirm if each log entry is sent (while also confirming it was inserted into the appropriate internal log file to know it should have been sent out and present in the packet capture).

Performing a tcpdump on the time server itself

As long as 'tcpdump' has not yet been deleted/removed by a user, tcpdump can be performed on the time server to see if log entries are being sent out to the syslog server. To see if tcpdump is still enabled/available for use, open a cli (telnet or ssh session) connection to the SecureSync. At the command prompt, type: `tcpdump` <enter>.

If the tcpdump command responds with a password prompt (as shown below), tcpdump has since been removed from the system by a user, and is therefore no longer available.

```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.7.1
spadmin@Spectracom ~ $ tcpdump
Password: █
```

Re-enabling tcpdump requires performing a full software "upgrade" / "restore to factory defaults process (the unit can be updated to a newer version of software at the same time, or it can remain at the current version). Contact Tech Support for additional assistance restoring tcpdump

If tcpdump has not been disabled type, type at the **command prompt** `tcpdump port 514` <enter> (where 514 is the factory default syslog port - Note this value can be optionally changed in software versions 5.7.1 and above). This command will listen on ethernet interface **eth0** only for any log entries being sent.

Notes:

- 1) With software versions 5.4.1 or below installed, add the word **sudo** to the beginning of all tcpdump commands,
- 2) Use **Ctrl + C** keys to stop a packet capture in progress.
- 3) Add **-i any** at the end of the tcpdump commands to have tcpdump listen to all ethernet interfaces on the time server (especially if the syslog server is not routable from ethernet interface eth0 (which is the only interface tcpdump listens to, unless specifying it to listen to a different interface/all interfaces).

Below is an example screenshot of tcpdump inside the time server capturing **System** Log entries successfully being sent to the desired Syslog server (in this example, the SecureSync is at **10.2.100.177** and the Syslog server is at **10.2.100.192**) based on the specific Facility/Severity code combination of **“Local Use 7”** and **“Emergency”**.

```

tcpdump: syntax error
spadmin@Spectracom ~ $ tcpdump port 514 -i any
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
14:25:39.734536 IP 10.2.100.177.syslog > 10.2.100.192.syslog: SYSLOG local7.emer
gency, length: 62
14:25:52.396384 IP 10.2.100.177.syslog > 10.2.100.192.syslog: SYSLOG local7.emer
gency, length: 62
14:26:24.389285 IP 10.2.100.177.syslog > 10.2.100.192.syslog: SYSLOG local7.emer
gency, length: 64
14:28:30.992446 IP 10.2.100.177.syslog > 10.2.100.192.syslog: SYSLOG local7.alert, length: 10

```

Verify the main default port/default gateway configuration (if the Syslog server is not on the immediate subnet of any of the time server’s interfaces

If the Syslog server is not on the immediate subnet of any of its available four ethernet interfaces, to go one step further and verify using the CLI interface, the Log entry was sent out the correct interface (via its main default port/gateway) to be able to reach the Syslog server, perform the following CLI command: **gw4get**<enter>. The response will report the default gateway address and which ethernet interface (such as eth0) the log entries will go out to reach the syslog server (in this example, the entries will be sent via ethernet interface “eth0”:

```

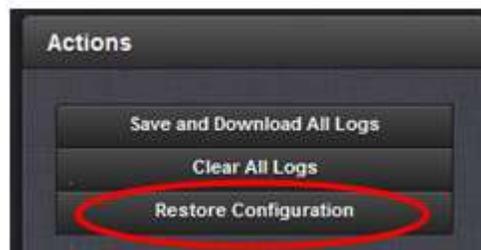
eth0 default gateway: 0.0.0.0
spadmin@Spectracom ~ $ gw4get
Main IPv4 default gateway (eth0): 10.2.1.1
eth0 default gateway: 10.2.1.1
eth1 default gateway: 0.0.0.0
eth2 default gateway: 0.0.0.0
eth3 default gateway: 0.0.0.0
spadmin@Spectracom ~ $

```

Reset the Syslog configs back to factory default

After going through this troubleshooting section (such as verifying the syslog server’s network port is accessible from the SecureSync and that each log file in the SecureSync have a selected syslog server configured), If the syslog server is still not receiving any new log entries as they are being generated within the SecureSync, reset the Syslog configuration back to factory default settings. Then restore the syslog settings again, as applicable.

Note that Software update version **5.7.1** Added a **“Restore Configuration”** button to the left side of the **Management -> Log Configuration** page of the web browser (as shown below) to be able to reset just the Log Configurations.



Section 4: SecureSync software changes associated with Syslog

Spectracom may periodically incorporate software changes to SecureSync's syslog functionality via software update. Below are software changes associated with syslog functionality.

1) Version 5.7.1 software update

- Added ability to change the default Syslog port number to a user-defined value
- Added a “**Restore Configuration**” button to the **Management** -> **Log Configuration** page of the web browser to be able to reset just the Log Configurations.

2) Version 5.4.0 software update

- Fixed an issue affecting either new time servers shipped with software version 5.3.1 installed, or “fielded” time servers that were updated to version 5.3.1 and then subsequently “cleaned. When trying to add a new syslog server, reports error message “**500: Interval Server Error**”.

Section 5: Spectracom Tech Support

Please contact one of the global Spectracom Technical Support centers for assistance:

USA www.spectracomcorp.com | techsupport@spectracomcorp.com |
1565 Jefferson Rd. | Rochester, NY 14623 | +1.585.321.5800

FRANCE www.spectracom.fr | techsupport@spectracom.fr |
3 Avenue du Canada | 91974 Les Ulis, Cedex | +33 (0)1 64 53 39 80