SPECTRACOM

Technical Note: SecureSync

Monitoring- SNMP/Email alert operation of the Spectracom SecureSync

Purpose: The purpose of this document is to provide supplemental information regarding monitoring (SNMP and Email alert operation) of the Spectracom SecureSync.

Table of Contents

Section 1: SecureSync SNMP

Spectracom SecureSync has two types of notifications available. One is SNMP (via SNMP traps) and the other is via Email alerts. To provide the SNMP traps, SecureSync has SNMP (Simple Network Management Protocol) capability. The primary function of SNMP is to send SNMP Traps which remotely alert to specific conditions occurring in SecureSync (such as loss of time sync status or problems with the GPS antenna cable, for examples). Any network with one or more available SNMP Managers in operation can utilize the SNMP capabilities of SecureSync.

By factory default, SNMP is disabled in SecureSync. After enabling SNMP, if the network has one or more SNMP Managers, SNMP can be configured and enabled to provide remote monitoring capability via SNMP Traps (The time servers can support up to five different SNMP Managers).

All Spectracom SecureSyncs have at least three ASCII text MIB (Management Information Base) files contained in the time server ("**Home/Spectracom/mibs**" directory). These MIB files can either be retrieved using an FTP/SFTP/SCP connection to the SecureSync, or they can also be emailed to you, as desired, upon request. The MIB files are often Application software version specific, so we will need to know the current "Archive Version" of the Application software contained in the unit. This information can be found on either the **Tools -> Upgrade/Backup** page of the newer black/charcoal browser, or in the "**Tools**" -> "**Versions**" page of the earlier white background web browser (referred to as the "classic interface"), in the "**System Version**" table. Contact Spectracom Tech Support to obtain the MIB files via email.

The MIB files are a database of objects that can be monitored by a network management system (SNMP Manager). The MIB files define the available SNMP Traps and the OID numbers (object identifiers) of all of the objects. These MIB files need to be compiled into the SNMP Manager(s):

- General information such as the Model information is located in the "**SPECTRACOM-GLOBAL-MIB.mib**" file.
- The list of all of SNMP Traps (Notifications) supported by the time servers can be found at the bottom of the "**Spectracom-Secure-Sync-MIB.mib**" file.
- Information regarding the SNMP functionality of NTP (Network Time Protocol) can be found in the "**SPECTRACOM-NTP-v4-MIB.mib**" file.

In order for SecureSync to utilize the SNMP functionality, the SNMP agent has to be configured and enabled via the web browser. SecureSync supports three versions of SNMP (SNMPv1, SNMPv2c and SNMPv3). SNMPv1 is the least secure method, SNMPv2C is a more secure method, while SNMPv3 is the most secure method. SNMPv1 and SNMPv2C use a passphrase sent "in the clear" for Authentication only (no encryption of the packets can occur). SNMPv3 uses authentication as well as encryption algorithms to scramble the SNMP communication between the SecureSync and the SNMP Manager(s). In order to use SNMPv3, the SNMP Manager must also support SNMPv3 functionality.

SecureSyncs also have the ability to automatically send an Email (Email alerts) to a specified email address when certain conditions (events) occur.

Note: Software update version 5.1.2 introduced a new web browser design which has a black/charcoal background instead of a white background (the earlier white background web browser is now referred to as the “Classic interface”**)**. Both interfaces are discussed herein.

Section 2: SNMP Management software

In case you don't already have at least one SNMP Manager on the network to interface with the SecureSync and would like to obtain one, many SNMP Manager programs are available for both Linux and Windows Operating Systems. Some are freeware/open-source programs while others are shareware/payware programs.

SNMP for Linux

For Linux-based machines, we recommend using Net-SNMP software (http://www.net-snmp.org/). This program is free and open-source code.

SNMP for Windows

There are many SNMP Manager programs available for Windows. Below is a list of some of examples:

1. ManageEngine software (http://www.manageengine.com/products/mibbrowser-free-tool/download.html) (freeware)

    Note: This SNMP software supports v1, v2c and v3 SNMP traps

2. iReasoning software (www.ireasoning.com) (freeware)

3. Castle Rock SNMPc (http://www.castlerock.com/) (Cost involved)

2. WhatsUP Gold (http://www.ipswitch.com/Products/WhatsUp/pricing.html) (Cost involved)

3. SNMP Manager from BTT Software (http://www.bttsoftware.co.uk/) (I believe it is free)

4. SNMP Trap Watcher from BTT Software (http://www.bttsoftware.co.uk/) (I believe it is free)

5. MG-Soft SNMP Software (http://www.mg-soft.com/) (Various packages and pricing available)

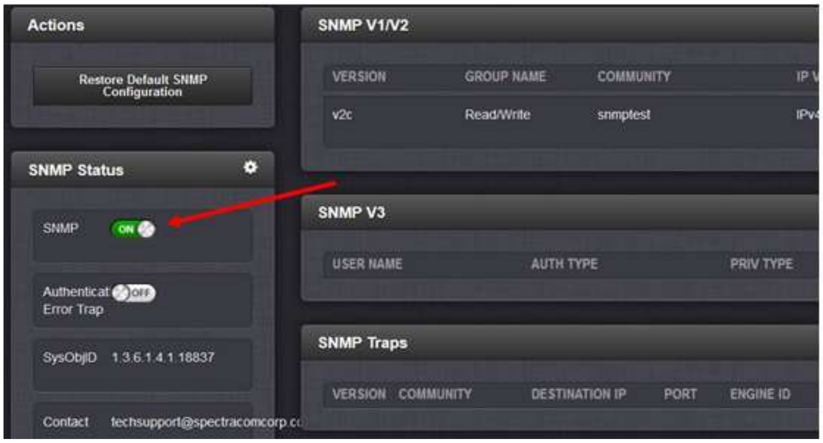
6. IBM Trivoli Software Package (http://www.tivoli.com/products/) (Cost involved)

7. HP OpenView software http://www8.hp.com/us/en/software/enterprise-software.html (Cost involved)

Section 3: Turning SNMP ON or OFF in SecureSync

A) Newer web browser (Software versions 5.12 and above)

SNMP can be turned on (Enabled) or off (Disabled) as desired, using the slider bar on the left side of the "**Management**" -> "**SNMP Setup**" page of the web browser. Refer to Figure 2.



SNMP: ON

Authentication Error Trap: OFF

SysObjID 1.3.6.1.4.1.18837

Contact techsupport@spectracomcorp.c

VERSION	GROUP NAME	COMMUNITY	IP V
v2c	Read/Write	snmptest	IPv

USER NAME	AUTH TYPE	PRIV TYPE

VERSION	COMMUNITY	DESTINATION IP	PORT	ENGINE ID

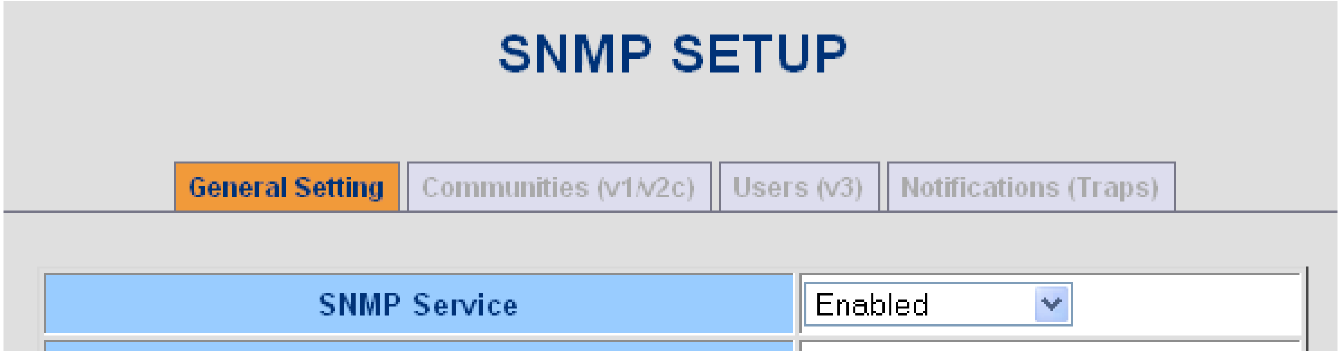
Figure 1: Enabling or Disabling SNMP in the "Management" -> "SNMP Setup" page

SNMP can be also be turned on (Enabled) or off (Disabled) as desired via CLI interface command (using Services such as telnet or SSH). The CLI command to determine if SNMP is currently running is **servget**. The CLI command to stop or start SNMP is **servset**.

When "SNMP Service" is set to "Disabled", the SNMP Port (Port 162) is closed. When "SNMP Service" is set to "Enabled", the SNMP Port (Port 162) is opened.

B) "Classic Interface" (Software versions 5.0.2 and below)

SNMP can be turned on (Enabled) or off (Disabled) as desired in the "**General Settings**" tab of the "**Network**" -> "**SNMP Setup**" page of the web browser. Refer to Figure 2.



SNMP Service: Enabled

Figure 2: Enabling or Disabling SNMP via the "General Setting" tab of the "Network" -> "SNMP Setup" page

SNMP can be also be turned on (Enabled) or off (Disabled) as desired via CLI interface command (using Services such as telnet or SSH). The CLI command to determine if SNMP is currently running is **servget**. The CLI command to stop or start SNMP is **servset**.

When “SNMP Service” is set to “Disabled”, the SNMP Port (Port 162) is closed. When “SNMP Service” is set to “Enabled”, the SNMP Port (Port 162) is opened.

Section 4: Configuring SNMP (Software versions 5.1.2 and above)

The configuration of SNMPv1, SNMPv2c and SNMPv3 is located on the “**Management**” -> “**SNMP Setup**” page of the browser.

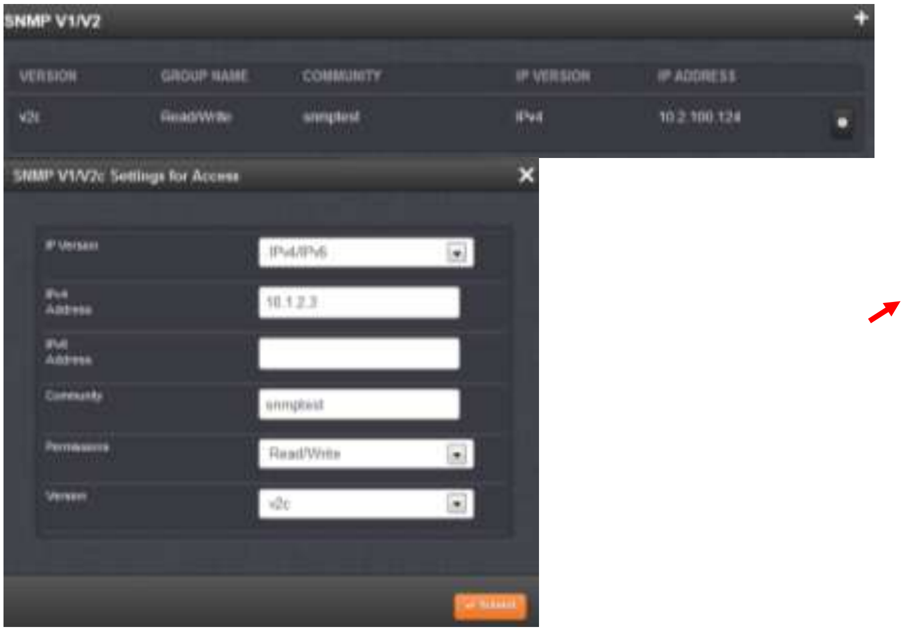
SNMPv1 and v2c do not authenticate or encrypt the SNMP packets that are exchanged between SecureSync and the SNMP Manager(s). The packets are sent out in the clear. However, SNMPv3 provides the ability to add authentication and/or encryption to the SNMP packets that are exchanged between SecureSync and the SNMP Manager(s).

> **Note:** The SNMP Manager(s) must be able to support SNMPv3 in order to use this enhanced SNMP functionality in SecureSync.

- Refer to **Section 4A** below for **SNMPv1/SNMPv2c** configuration.
- Refer to **Section 4B** below for **SNMPv3** configuration.

Section 4A: SNMPv1 and SNMPv2c configuration

The “SNMP V1/V2” section of the “**Management**” -> “**SNMP Setup**” page of the web browser is used to list and add up to more than 5 available SNMP Managers that can communicate with SecureSync.



SNMP V1/V2

VERSION	GROUP NAME	COMMUNITY	IP VERSION	IP ADDRESS
v2c	Read/Write	snmptest	IPv4	10.2.100.124

SNMP V1/V2c Settings for Access

IP Version	IPv4/IPv6
IPv4 Address	10.1.2.3
IPv6 Address	
Community	snmptest
Permissions	Read/Write
Version	v2c

Figure 3: “SNMP V1/V2” section of the “SNMP Setup” web page

To add a SNMP V1 or V2 users, click on the “+” sign in the upper-right corner of this section. Or, to view the current setting of a previously created user, click on the “gear” ICON in the lower-right corner of this section.

Configure the fields in this pop-up window (as configured in the SNMP Manager). Then press Submit.

IP Version: Select the appropriate box for the IP addressing of the SNMP Manager.

IPv4 Address / IPv6 Address: Used to restrict SecureSync access to a single network (or to a single PC). Enter the network address and the subnet mask in the format of “xxx.xxx.xxx.xxx/yy” (where x is the only network allowed access to the time server and yy is the number of bits in the subnet mask (example: 10.20.200.0/16). Enter “default” to not restrict SNMP access to SecureSync.

Community (“Community name”): Enter the desired community name as configured in the SNMP Manager (such as “public” for example).

Notes about the Community Name string

- The Community Name is a clear-text string that is used as a password.
- Starting in software version 5.2.1, the string can be 1 to 31 characters in length.
- If more than one user is added, the Community Name field must be unique. There can’t be any duplicates of the same name.

Permissions: Select the permission as either ”Read only” or “Read/Write” as desired (where “ Read” will only allow values to be retrieved from the time server and “Read/Write” allows values to be retrieved or configured in the time server).

Version: Select either v1 or v2c as desired for communications between the SNMP Manager and the time server (as also configured in the SNMP manager).

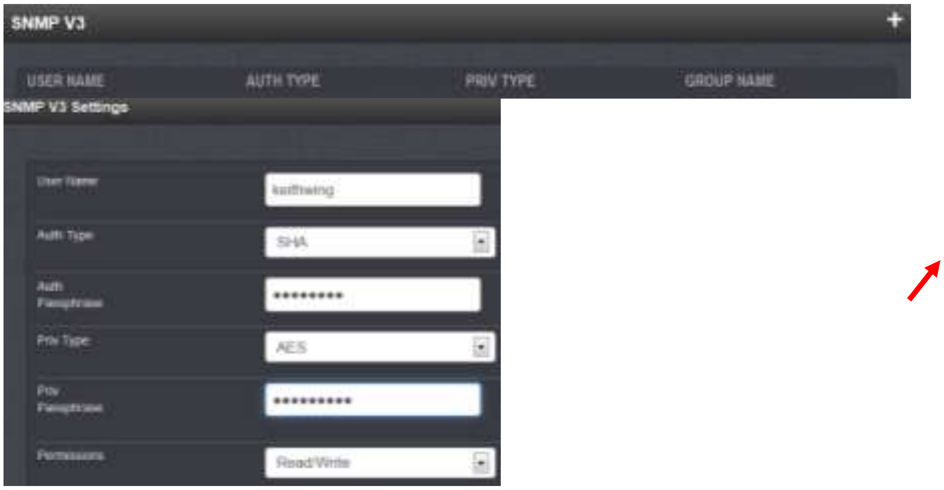
Section 4B: SNMPv3 configuration

Unlike SNMPv1 and v2c, SNMPv3 provides secure SNMP access to devices by using a combination of message integrity, authentication and encryption (privacy).

By utilizing one of two selected authentication algorithms and/or one of two encryption algorithms, SNMPv3 provides the following:

1) Message integrity to ensure the message packets haven’t been tampered with in-route.
2) Authentication (abbreviated as “Auth”) to verify the packets came from a valid source.
3) Encryption (abbreviated as “Priv” for “Privacy”) to scramble the SNMP packet contents to prevent it from being viewed by unauthorized users.

The SNMPv3 section of the “**Management**” -> “**SNMP Setup**” page is used to list and add up to 5 available SNMP Managers that can communicate with SecureSync using SNMPv3.



User Name: keithwing
Auth Type: SHA
Auth Passphrase: *********
Priv Type: AES
Priv Passphrase: **********
Permissions: Read/Write

Figure 4: “SNMP v3 Users” section of the “SNMP Security” web page

To add a SNMP V3 users, click on the “+” sign in the upper-right corner of this section. Or, to view the current setting of a previously created user, click on the “gear” ICON in the lower-right corner of this section.

Configure the fields in this pop-up window (as also configured in the SNMP Manager). Then press Submit.

User name: Enter the 8-32 character user (principal) on whose behalf the message is being exchanged.

Authentication configuration: (Provides ability to use a “hash” to ensure the SNMP packets originated from the SecureSync or from a valid SNMP Manager)**.**

(Where: “MD5” stands for “Message Digest” and “SHA” stands for “Secure Hash Algorithm”).

Note: SHA is considered a stronger authentication algorithm than MD5.

Auth type: To enable authentication, select the desired authentication algorithm as either “MD5” or “SHA” (as also configured in the SNMP Manager(s).

Auth Passphrase: Configure the authentication passphrase (as shared by the NTP server and SNMP Manager)

SNMPv3 Privacy (data encryption) configuration: (Provides ability to scrambles the SNMP data so that it can only be read by the SecureSync and a valid SNMP Manager)

Priv Type: To enable encryption, **s**elect the desired encryption algorithm as either “DES” or “AES”

(Where: “DES” stands for “Data Encryption Standard” and “AES” stands for “Advanced Encryption Standard”).

Priv Passphrase: Enter an 8-32 character passphrase for encryption.

Permission: Select the permission as either “read” or “read/write” as desired (where “ read” will only allow values to be retrieved from SecureSync and “read/write” allows values to be retrieved or configured in SecureSync.

Section 5: Configuring SNMP (Software versions 5.0.2 and below)

The configuration of SNMPv1, SNMPv2c and SNMPv3 is located on the “**Network**” -> ”**SNMP Setup**” page of the browser, The “**Communities (v1/v2c)”** tab is for SNMPv1 and v2c configuration, while the “**Users (v3)**” tab is for SNMPv3 configuration.

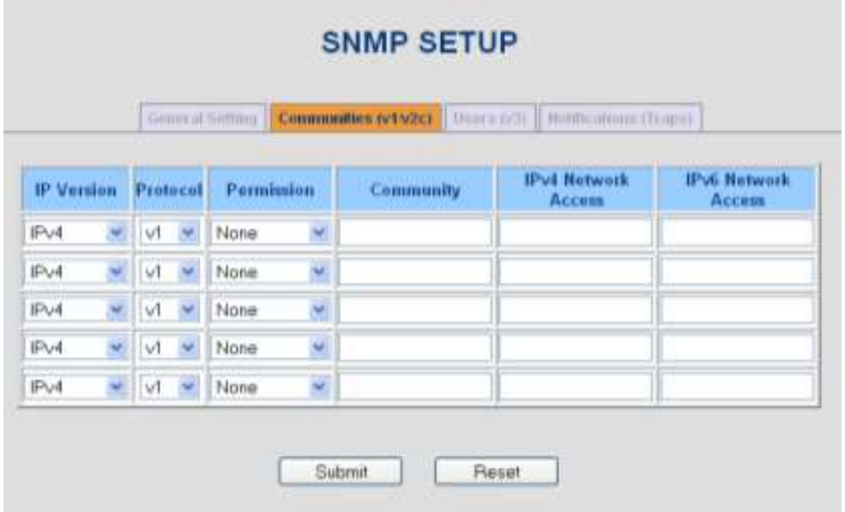
SNMPv1 and v2c do not authenticate or encrypt the SNMP packets that are exchanged between SecureSync and the SNMP Manager(s). The packets are sent out in the clear. However, SNMPv3 provides the ability to add authentication and/or encryption to the SNMP packets that are exchanged between SecureSync and the SNMP Manager(s).

Note: The SNMP Manager(s) must be able to support SNMPv3 in order to use this enhanced SNMP functionality in SecureSync.

Refer to **Section 5A** for **SNMPv1/SNMPv2c** configuration or to **Section 5B** for **SNMPv3** configuration.

Section 5A: SNMPv1 and SNMPv2c configuration

The “Communities (v1/v2c)” tab of the “**Network**” -> “**SNMP Setup**” page of the web browser is used to list up to 5 available SNMP Managers that can communicate with SecureSync.



SNMP SETUP

IP Version	Protocol	Permission	Community	IPv4 Network Access	IPv6 Network Access
IPv4	v1	None			
IPv4	v1	None			
IPv4	v1	None			
IPv4	v1	None			
IPv4	v1	None			

Figure 5: SNMP v1/v2c Users” section of the “SNMP Setup” web page

IP Version: Select the appropriate box for the IP addressing of the SNMP Manager(s) (Note that up to five SNMP Manager IP addresses can be listed in this table).

Protocol: Select either v1 or v2c as desired for communications between the SNMP Manager and the time server (as also configured in the SNMP manager).

Permission: Select the permission as either "Read" or "Read/Write" as desired (where " Read" will only allow values to be retrieved from the appliance and "Read/Write" allows values to be retrieved or configured in the appliance).

3B of "None" will delete the user you are trying to create. If it's set to "None" before hitting Submit, the changes that were made will be lost. Refreshing this page will show all values erased.

Community ("Community name"): Enter the desired community name as configured in the SNMP Manager (such as "public"). **Note:** The Community Name is a clear-text string that is used as a password.

IPv4 Network Access/ IPv6 Network Access: Used to restrict SecureSync access to a single network (or to a single PC). Enter the network address and the subnet mask in the format of "xxx.xxx.xxx.xxx/yy" (where x is the only network allowed access to the time server and yy is the number of bits in the subnet mask (example: 10.20.200.0/16). Enter "default" to not restrict SNMP access to SecureSync.

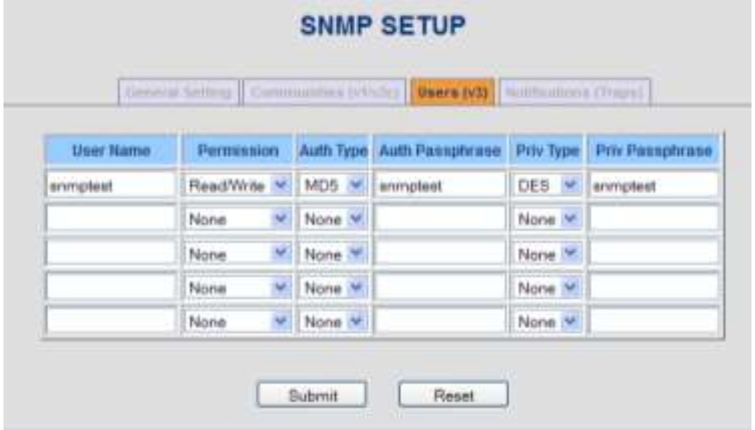
Section 5B: SNMPv3 configuration

Unlike SNMPv1 and v2c, SNMPv3 provides secure SNMP access to devices by using a combination of message integrity, authentication and encryption (privacy).

By utilizing one of two selected authentication algorithms and/or one of two encryption algorithms, SNMPv3 provides the following:

4) Message integrity to ensure the message packets haven't been tampered with in-route.
5) Authentication (abbreviated as "Auth") to verify the packets came from a valid source.
6) Encryption (abbreviated as "Priv" for "Privacy") to scramble the SNMP packet contents to prevent it from being viewed by unauthorized users.

The "**Users (v3)**" tab of the "**Network**" -> "**SNMP Setup**" page of the web browser is used to list up to 5 available SNMP Managers that can communicate with SecureSync using a secure connection to the appliance



User Name	Permission	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
snmptest	Read/Write	MD5	snmptest	DES	snmptest
	None	None		None	
	None	None		None	
	None	None		None	
	None	None		None	

Figure 6: "SNMP v3 Users" section of the "SNMP Security" web page

Configure the fields in this menu (as configured in the SNMP Manager):

User name: Enter the 8-32 character user (principal) on whose behalf the message is being exchanged.

Permission: Select the permission as either “read” or “read/write” as desired (where “ read” will only allow values to be retrieved from SecureSync and “read/write” allows values to be retrieved or configured in SecureSync.

Authentication configuration: (Provides ability to use a “hash” to ensure the SNMP packets originated from the SecureSync or from a valid SNMP Manager)**.**

(Where: “MD5” stands for “Message Digest” and “SHA” stands for “Secure Hash Algorithm”).
Note: SHA is considered a stronger authentication algorithm than MD5.

Auth type: To enable authentication, select the desired authentication algorithm as either “MD5” or “SHA” (as also configured in the SNMP Manager(s).

Auth Passphrase: Configure the authentication passphrase (as shared by the NTP server and SNMP Manager)

SNMPv3 Privacy (data encryption) configuration: (Provides ability to scrambles the SNMP data so that it can only be read by the SecureSync and a valid SNMP Manager)

Priv Type: To enable encryption, **s**elect the desired encryption algorithm as either “DES” or “AES”

(Where: “DES” stands for “Data Encryption Standard” and “AES” stands for “Advanced Encryption Standard”).

Priv Passphrase: Enter an 8-32 character passphrase for encryption.

Section 6: SNMP OIDs, sets, gets and Reboot

Important Notice: the SNMP objects associated with NTP (object names that begin with "ntp", such as "ntpSysStaStratum", instead of "ss", such as "ssGpsRefTimeValid") require several seconds of additional time to respond to individual SNMP polls or walks. An NTP query needs to be performed to obtain the requested NTP information, before the SecureSync can respond to the SNMP Manager with this information. This query adds about 6 to 7 seconds of delay in each poll of NTP associated objects.

To account for this additional time needed for SecureSync to respond to NTP objects, the SNMP Manager's timeout period (this configuration is in the SNMP Manager or linux machine and not in the SecureSync itself) needs to be configured for a minimum of about 7 seconds, to allot enough time for the SecureSync to finish responding to each NTP object, before the SNMP Manager times-out and proceeds to the next poll in the list. Extending the timeout even longer than about 7 seconds will not cause the polls or walks to take longer. It will just ensure the SecureSync has enough time to be able to respond before the time-out occurs. If the SNMP Manager times-out before the SecureSync can respond to the poll, the data will not be able to be returned to the SNMP Manger.

OIDs (Object IDs) associated with the SecureSync SNMP functionality

There are actually three unique sets of SNMP OIDs/Object Numbers for the SecureSyncs. SecureSync run Net- SNMP software for its SNMP functionality. Net-SNMP has its own set of SNMP objects. A second set of objects is for the Spectracom-specific objects (such as the majority of the available SNMP traps are Spectracom-specific, for example). The Authorization trap is a Net-SNMP trap instead of a Spectracom-specific trap. SecureSync SNMP also supports the generic RFC-1213 MIB file, which also has its own OID numbers associated with it.

In summary:

- The SNMP object numbers of "**.1.3.6.1.4.1.18837.**" are for Spectracom-specific objects.
- The SNMP object numbers of "**.1.3.6.1.4.1.8072.**" are objects associated with Net-SNMP.
- The SNMP object numbers of "**.1.3.6.1.4.1.2.1**" are objects associated with RFC-1213.

SNMP gets and sets

The SecureSync has the capability to perform many SNMP "gets" (to poll for data/status via SNMP), as well the ability to perform a limited number of SNMP "sets" (to be able to change configurations via SNMP).

The Spectracom MIB files define all of the available "gets" and "sets" that are available via SNMP.

For each item listed in the mib files, the "**MAX-ACCESS**" field defines if each item (OID) is an SNMP get only, if it's available as either an SNMP get or a set, or if it's not accessible as either a SNMP get or set.

- If the OID is listed as “**read only**” it’s available only as an SNMP get.
- If the OID is listed as “**read-write**”, it’s available as either an SNMP get or set.
- If the OID is listed as “**not accessible**”, it’s not available as either an SNMP get or as an SNMP set (**Note**: These “not accessible” OIDs/items are typically used to build a table).

file provides information on what its specific function is. Below is a list of the available SNMP MIB files and their primary functions:

1) **SPECTRACOM-NTP-V4-MIB.mib**
This MIB defines the NTPv4 MIB for the private Spectracom MIB.

2) **SPECTRACOM-PTP-V4-MIB.mib**
This MIB defines the PTP MIB for the private Spectracom MIB (This MIB file is only applicable if the available SecureSync PTP Option Card, Model 1204-12) is installed.

3) **SPECTRACOM-SECURE-SYNC-MIB.mib**
This MIB defines the SecureSync product module for the private Spectracom MIB.

4) **NET-SNMP-AGENT-MIB.mib**
This MIB defines control and monitoring structures for the Net-SNMP agent.

5) **NET-SNMP-MIB.mib**
Top-level infrastructure of the Net-SNMP project enterprise MIB tree

6) **SPECTRACOM-GLOBAL-MIB.mib**
This MIB defines the global registration module for the private Spectracom MIB (defines the product is a Spectracom SecureSync and not a Model 9383 NetClock, for example).

Performing SNMP gets with all of the available SNMP traps
SNMP traps (Notifications) just define alerts that can be automatically sent when a specific event occurs. Traps and the variables they report cannot be polled using an SNMP Get. However, there may be another object available that reports the current status that is associated with that particular trap. For example, the "Time Synchronization" trap is sent when loss of sync occurs. An SNMP Get of the trap can't be performed. But there may be an associated object available that can be polled for the current sync status.

The table below lists all of the traps that have an associated OID that can be obtained via an SNMP get.

SNMP Trap	OID Number	Indicates	OID (if one is available) to perform an SNMPGet for this associated current status
"Time Synchronization"	1.3.6.1.4.1.18837.3.1.3.0.2	The unit has either entered or left the synchronized state	**Sync Status** **.1.3.6.1.4.1.18837.3.2.2.1.5**
"Holdover"	1.3.6.1.4.1.18837.3.2.3.0.2	The unit has either entered or left the holdover state.	**Holdover Mode** **.1.3.6.1.4.1.18837.3.2.2.1.6**
"UserMinorAlarm"	1.3.6.1.4.1.18837.3.2.3.0.5	The user-programmable minor alarm timeout has been asserted.	**# Satellites being tracked** : **.1.3.6.1.4.1.18837.3.2.2.2.1.1.8**
"UserMajorAlarm"	1.3.6.1.4.1.18837.3.2.3.0.7	The user-programmable major alarm timeout has been asserted.	**# Satellites being tracked** **.1.3.6.1.4.1.18837.3.2.2.2.1.1.8**
"GpsAntenna"	1.3.6.1.4.1.18837.3.2.3.0.9	The GPS antenna state has changed (antenna is disconnected, short or open occurring in the antenna cable).	**Antenna Sense** **.1.3.6.1.4.1.18837.3.2.2.2.1.1.17**
"MinorAlarm"	1.3.6.1.4.1.18837.3.2.3.0.10	The system Minor alarm has changed state.	**Minor Alarm** **.1.3.6.1.4.1.18837.3.2.2.1.13**
"MajorAlarm"	1.3.6.1.4.1.18837.3.2.3.0.11	The system Major alarm has changed state.	**Major Alarm** **.1.3.6.1.4.1.18837.3.2.2.1.14**

Alarms in the table above (such as Holdover, Time Sync, GPS antenna and the Major alarm - which is asserted when an event classified as a Major alarm occur) are typically caused by issues with GPS reception and/or antenna cabling issues. For assistance with troubleshooting these SNMP traps, please refer to the "**SecureSync GPS reception troubleshooting**" document on our website at the following link:
http://spectracom.com/Support/HowCanWeHelpYou/Library/tabid/59/Default.aspx?EntryId=315

For example, this troubleshooting document discusses the GPS Antenna Sense indicator, which can alert to an open or short being detected in the antenna cable. If this happens, the SecureSync will first go into Holdover mode. If the reception issue isn't fixed before this mode expires (two hours by factory default), the Time Sync alarm and associated Major alarm will be asserted. This document discusses how to help locate the open or short in the antenna cable so that it can be fixed.

SNMP Sets/Reboot

SNMP "sets" can be used to either reconfigure entries in the "Reference Priority" table or to perform software updates (instead of using the web browser to perform updates)

Note: With the exception of the Model 1204-12 PTP Option Card, there are no SNMP "gets" or "sets" available for any of the Option Card(s) that may be installed in the rear panel Option Bays. The PTP Option Card does have several available SNMP "gets" for values such as its configurations for the network port, delay mechanism, Master/Slave mode, One Step/Two Step mode, etc.

SNMP Reboot (Applicable to software versions 4.8.8 and above)

In addition to being used to perform software updates, the *ssSysCtrlCommand* Object can also be used to reboot the time server via SNMP. This Object was added in Archive software version 4.8.8.

OID	**NAME**	**FUNCTION**	**VALUE TO "SET"**
18837.3.2.2.5.1	ssSysCtrlCommand	Either Reboot or apply remote software updates	"4" to reboot (SNMP Get will normally return "idle (1)". Values 2 and 3 are for performing software updates)

SNMP Gets (SNMP Polls)

SNMP "gets" (polls) can be used to read many different values, such as the Sync status indications, NTP data, or configured values.

Note about SNMP Gets for NTP information

Polls for NTP data take a few seconds longer than polls for other information about the system. The reason for this slight delay is because unlike other system data, the NTP data isn't "tabled before-hand", resulting in "stale", outdated information about NTP. Instead, the SNMP polls for NTP information cause NTP to be queried at that particular moment and then the data obtained from NTP can be returned. This "on demand" querying is to provide the most recent data about NTP when it's polled. The short delay in the SNMP Get is a factor of NTP being queried and the data being passed to SNMP.

Section 6A: Examples of suggested gets that may be desired to perform in order to monitor SecureSync via SNMP

Tables 1, 2 and 3: System level OIDs (CPU, Memory and Disk usage)

Note: These system MIBs are only available with SecureSync software versions 5.2.1 and higher installed

TABLE 1: CPU USAGE	
OID	**FUNCTION**
.1.3.6.1.4.1.2021.11.9.0	Percentage of user CPU time
.1.3.6.1.4.1.2021.11.50.0	Raw user CPU time
.1.3.6.1.4.1.2021.11.10.0	Percentages of system CPU time
.1.3.6.1.4.1.2021.11.52.0	Raw system CPU time
.1.3.6.1.4.1.2021.11.11.0	Percentages of idle CPU time
.1.3.6.1.4.1.2021.11.53.0	raw idle CPU time
.1.3.6.1.4.1.2021.11.51.0	raw nice CPU time

TABLE 2: MEMORY USAGE	
OID	**FUNCTION**
.1.3.6.1.4.1.2021.4.3.0	Total Swap Size
.1.3.6.1.4.1.2021.4.4.0	Available Swap Space
.1.3.6.1.4.1.2021.4.5.0	Total RAM in machine
.1.3.6.1.4.1.2021.4.6.0	Total RAM used
.1.3.6.1.4.1.2021.4.11.0	Total RAM Free
.1.3.6.1.4.1.2021.4.13.0	Total RAM Shared
.1.3.6.1.4.1.2021.4.14.0	Total RAM Buffered
.1.3.6.1.4.1.2021.4.15.0	Total Cached Memory

TABLE 3: DISK USAGE	
OID	**FUNCTION**
.1.3.6.1.4.1.2021.9.1.2.1	Path where the disk is mounted
.1.3.6.1.4.1.2021.9.1.3.1	Path of the device for the partition
.1.3.6.1.4.1.2021.9.1.6.1	Total size of the disk/partition (kBytes)
.1.3.6.1.4.1.2021.9.1.7.1	Available space on the disk
.1.3.6.1.4.1.2021.9.1.8.1	Used space on the disk
.1.3.6.1.4.1.2021.9.1.9.1	Percentage of space used on disk
.1.3.6.1.4.1.2021.9.1.10.1	Percentage of inodes used on disk

Please note that Spectracom doesn’t have any suggested max thresholds for CPU or Memory usage. And other than when applying a software update to the SecureSync, we don’t have any suggested max thresholds for disk usage, either.

Disk usage needs to be less than about 72% when applying a software update (in order for there to be enough space to be able upload the upgrade file into the SecureSync and for the file to have enough space available to be able to extract this file). During operation, as long is its memory usage is less than 100%, it will continue to operate normally.

Note that CPU usage threshold needs to be set very high, as its CPU usage (for the outer processor that can be monitored) normally runs at about 90% or higher. For more information about this, please refer to the knowledge base article on our website at: http://support.spectracomcorp.com/articles/FAQ/Reported-CPU-usage?q=cpu&

As for memory usage, much of the memory is claimed by the Operating System, which allocates this memory as necessary and then takes it back when it's done being used. This will cause the amount of free memory to be reported as a very low number, such as around 40 to 60MB. For more information on memory usage reporting, please refer to the knowledge base article on our website at: http://support.spectracomcorp.com/articles/FAQ/free-cpu-memory?q=cpu&.

Table A: General status (Input power / Selected Time and PPS references / Sync Status / TFOM / Alarms)

OID	NAME	FUNCTION
18837.3.2.2.1.1.0	ssSysStaPowerAC	Status of the AC power input
18837.3.2.2.1.2.0	ssSysStaPowerDC	Status of the DC power input
18837.3.2.2.1.3.0	ssSysStaTimeReference	Selected “Time” reference
18837.3.2.2.1.4.0	ssSysSta1PPSReference	Selected “PPS” reference
18837.3.2.2.1.5.0	ssSysStaSyncState	Status of the unit's synchronization with its selected Time/1PPS references
18837.3.2.2.1.6.0	ssSysStaHoldoverState	Holdover status (loss of all input references)
18837.3.2.2.1.7.0	ssSysStaTfom	Current TFOM (Estimated accuracy of System Time)
18837.3.2.2.1.13.0	ssSysStaMinorAlarm	Indicates whether or not a Minor alarm is currently active.
18837.3.2.2.1.14.0	ssSysStaMajorAlarm	Indicates whether or not a Major alarm is currently active
18837.3.2.2.1.15.0	ssSysStaDateTime	Indicates current System Date and Time

Table B: GPS input status (If GPS is being used as an input reference)

OID	Name	Function
18837.3.2.2.2.4	ssGpsRefTimeValid	Indicates whether GPS can provide valid “Time (Needed for GPS to be a valid reference)
18837.3.2.2.2.5	ssGpsRef1ppsValid	Indicates whether GPS can provide valid PPS. (Needed for GPS to be a valid reference)
18837.3.2.2.2.8	ssGpsRefNumSats	Number of satellites currently used in calculating position and time
18837.3.2.2.2.17	ssGpsRefAntennaState	Detects opens or shorts in the antenna cable

Table C: NTP OUTPUT STATUS

OID	Name	Function
18837.3.3.2.1.0	ntpSysStaCurrentMode	Current Sync status of NTP
18837.3.3.2.2.0	ntpSysStaStratum	Current NTP Stratum level (As reported to the NTP Clients). Stratum 16 indicates NTP clients will likely ignore the NTP packets from the NTP server

Table D: Oscillator Phase and Frequency Error (as compared to selected 1PPS input reference)

OID	Name	Function
18837.3.2.2.1.8.0	ssSysStaEstPhaseError	The estimated phase error (magnitude) of the unit's internal 1PPS with respect to the selected 1pps reference
18837.3.3.2.1.9.0	ssSysStaEstFreqError	The estimated frequency error (magnitude) of the unit's internal 10 MHz oscillator with respect to the selected 1PPS reference.

Section 6B: Desire to use SNMP sets to remotely disable or enable Input References (such as GPS, or IRIG input)

If it's desired to "remove" Input References (such as GPS, IRIG, havequick, etc), references can be remotely disabled, alleviating the need to physically disconnect input cables. Input References can be remotely enabled or disabled as desired, using SNMP, the web browser or via CLI commands (serial connection, telnet or ssh).

The Reference Priority table contains rows of Input References and the associated priority value for each reference. Each row of this table also contains a "State" field that allows that particular row of the table to be either Enabled or Disabled. When a row of the table is "disabled", the input reference is declared "not valid", (even if the signal is being applied to the SecureSync). If there are lower priority input references present/valid when a particular reference is disabled, the next lower priority reference will be selected for synchronization. However, if no other references are present/valid when a reference is disabled, the SecureSync will then go into Holdover mode, until a reference becomes available.

With GPS input, the GPS receiver will continue to track GPS satellites while it's disabled in the Reference Priority table. But GPS won't be selected for synchronization, until this reference has been re-enabled. With other Input References (such as IRIG or Havequick for examples) being disabled, the signal may still be present at the input connector. Because the GPS receiver continues to track GPS satellites while GPS is disabled and because other signals remain present on the input connection, when the reference is re-enabled, it's able to be declared valid almost immediately thereafter. If the re-enabled reference signal is still present, and it's the highest priority reference listed in the Priority table, it will become the selected reference for synchronization as soon as its "State" field is changed to "Enabled". If it was in Holdover mode, Holdover mode ends when Synchronization occurs.

For the SNMP gets and sets used to remotely read and set the fields of the Reference Priority table, refer to the "**ssReferenceMgmtObjs"** objects in the **SPECTRACOM-SECURE-SYNC-MIB.mib** file. Specifically, "**ssRefMgmtState**" is used to configure the "State" field of the Reference Priority table to either enable or disable input references.

Section 7: Configuring the Reference Priority setup table via SNMP

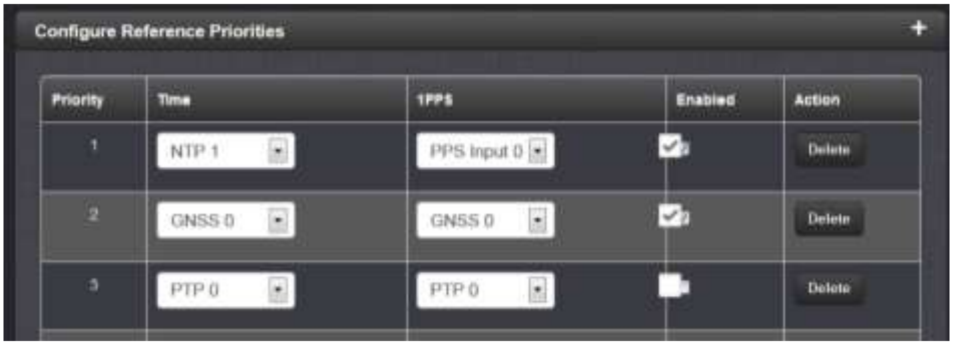
The “Enable/Disable” and “Priority” fields of the “Reference Priority Setup” can be configured via the SecureSync’s web browser or with SNMP “Sets”. The “SPECTRACOM-SECURE-SYNC-MIB.mib” file contains the applicable values for configuring this table via SNMP. Refer to “**ssReferenceMgmtObjs Objects [enterprises.18837.3.2.2.4.x]**” in this MIB file for a list of all of the values associated with this table. Refer to the SecureSync user manual for additional information on the “Reference Priority Setup” table.

Note: SNMP provides the ability to “get” the entire Reference Priority table, but only provides the ability to “set” the “State” field (Enable or Disable input references) and the “Priority” of the reference. SNMP does not allow entries to be added or deleted from the Reference Priority table.

Section 7A: Newer web browser (Software versions 5.1.2 and above)

Starting in SecureSync Archive software version 4.5.0, the ability to remotely configure the SecureSync’s input “Reference Priority Setup” table using SNMP sets (in addition to being able to configure it via the web browser) is available.

The “Reference Priority Setup” table (“**Management**” -> “**Reference Priority**” page of the SecureSync’s web browser) lists all available input references and their associated priorities. This table also allows each input reference to be individually enabled or disabled, as desired. When an input reference (such as GPS, for example) has been disabled, it will no longer be used as an input reference, even if it’s present and valid.



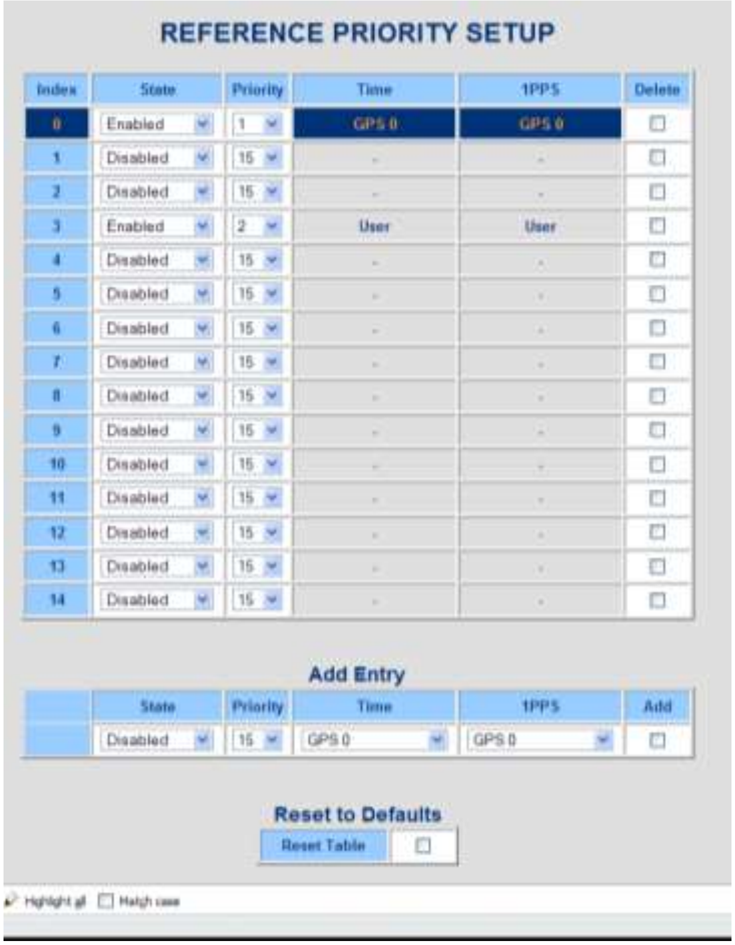
Priority	Time	1PPS	Enabled	Action
1	NTP 1	PPS Input 0	☑	Delete
2	GNSS 0	GNSS 0	☑	Delete
3	PTP 0	PTP 0	□	Delete

Figure 7: Reference Priority Setup table

Section 7B: “Classic interface web browser” (Software versions 5.0.2 and below)

Starting in SecureSync Archive software version 4.5.0, the ability to remotely configure the SecureSync’s input “Reference Priority Setup” table using SNMP sets (in addition to being able to configure it via the web browser) is available.

The “Reference Priority Setup” table (“**Setup**” -> “**Reference Priority**” page of the SecureSync’s web browser) lists all available input references and their associated priorities. This table also allows each input reference to be individually enabled or disabled, as desired. When an input reference (such as GPS, for example) has been disabled, it will no longer be used as an input reference, even if it’s present and valid.



REFERENCE PRIORITY SETUP

Index	State	Priority	Time	1PPS	Delete
0	Enabled	1	GPS 0	GPS 0	□
1	Disabled	15	-	-	□
2	Disabled	15	-	-	□
3	Enabled	2	User	User	□
4	Disabled	15	-	-	□
5	Disabled	15	-	-	□
6	Disabled	15	-	-	□
7	Disabled	15	-	-	□
8	Disabled	15	-	-	□
9	Disabled	15	-	-	□
10	Disabled	15	-	-	□
11	Disabled	15	-	-	□
12	Disabled	15	-	-	□
13	Disabled	15	-	-	□
14	Disabled	15	-	-	□

Add Entry

	State	Priority	Time	1PPS	Add
	Disabled	15	GPS 0	GPS 0	□

Reset to Defaults

Figure 8: Reference Priority Setup table

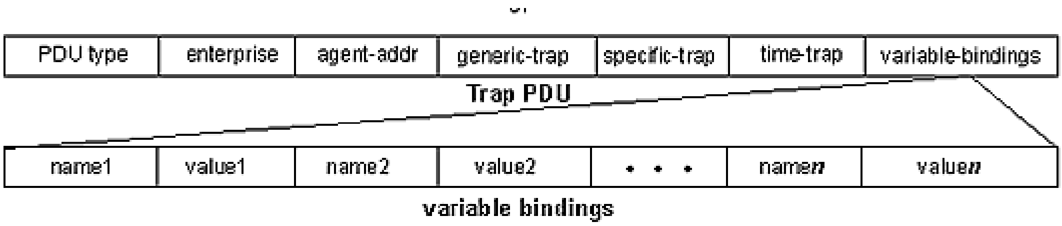
Section 8: SNMP Traps (Notifications) (Software versions 5.1.2 and above only)

The Spectracom SecureSync has the ability to automatically send SNMP Traps and/or Email alerts when certain SecureSync conditions (events) occur. These SNMP Traps are received by one or more SNMP Managers, and with the SNMP MIB files compiled into the SNMP Manager, the SNMP Manager can be configured as desired to react to a received SNMP Trap.

To begin, from Wikipedia:
Trap
Asynchronous notification from agent to manager. Includes current sysUpTime value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed SNMPv2-Trap.

SNMP traps are a one-way only transmission of a network packet (From SecureSync to SNMP Managers on the network) that occurs each time specific events occur and when they clear. Note that not all events actually "clear", so just one trap is sent when that particular type of event occurs (such as switching from one input reference to another).

Below is the packet structure of an SNMP trap. The second line breaks down the optional "Variable-bindings (also known as the "varbind") field. "Varbinds" can provide the SNMP Manager with additional specific information about the trap.



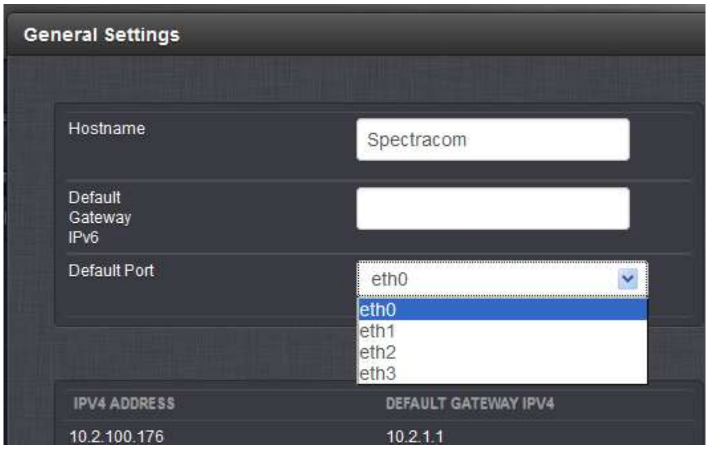
SecureSync traps
SecureSync SNMP traps are not solicited by the SNMP Manager(s) on the network. The SecureSync just sends out a trap (also referred to as a "notification") using a defined OID number in an SNMP packet when specific events occur. When the SNMP Manager receives the trap packet, it looks up the particular OID number in the MIB files that have been compiled into the SNMP Manager software. It determines what the particular OID number means and based on how you have set up the SNMP Manager, you can have it perform different things when a trap from the SecureSync is received.

Most, but not all, SecureSync conditions (events) consist of two related events. One is the "On" event which occurs when and event first happens and the other is the "Off" event which occurs later, when the condition clears. However, a few conditions consist of only one event occurring, as these conditions may be a one-time occurrence that doesn't actually "clear". An example of a condition that doesn't "clear" is when SecureSync switches from one input reference to lower priority input reference. Only one "event" occurs in this particular situation, when SecureSync switches to using a different input reference. If it subsequently changes back to the original input reference, the same one-time event occurs again.

Section 8A: Configuring the Default Port and "Global" Default Gateway

When it's desired to send SNMP traps, the default Gateway Address needs to be properly configured in the SecureSync. As the SNMP traps are originating from within the SecureSync (they are unsolicited packets), the route for the traps to take in order to reach the configured SNMP Manager(s) needs to be defined, via the Default Global Gateway. Also, if the Model 1204-06 Gigabit Ethernet Option card is installed (to add three additional Ethernet interfaces), the Ethernet interface that can route the time stamps to the SNMP Manager(s) also needs to be selected (known as the "Default Port").

With software versions 5.1.2 or higher installed, and if the Model 1204-06 Gigabit Ethernet Option Card is installed, the Ethernet Interface to route the packets to the Internet is configured in the **Management** -> **Network** page of the browser, "**General Settings**" button which is located in the upper-left corner of the browser. This interface is defined in the "**Default port**" field.



General Settings

Hostname	Spectracom
Default Gateway IPv6	
Default Port	eth0

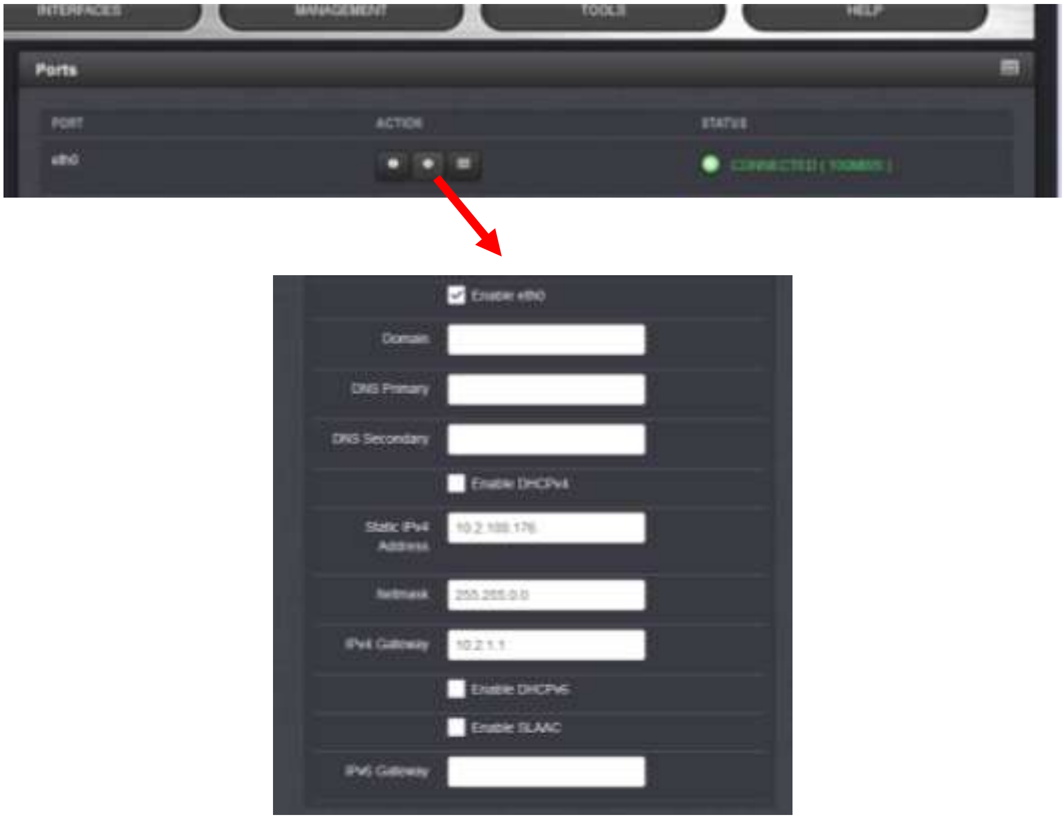
IPV4 ADDRESS	DEFAULT GATEWAY IPV4
10.2.100.176	10.2.1.1

Figure 9: Configuring the Default Port (versions 5.1.2 and higher)

The default gateway address for the selected Ethernet Interface ("default port") is configured in the "**Ports**" section of the **Management** -> **Network page** of the browser.

To configure the default gateway address, first press the "gear" box (center of the three boxes in the row for the Default port (such as "Eth 0" for example). This will open a new window. If the "**Enable DHCPv4**" checkbox is not selected, the default gateway address can be defined in the "**IPv4 Gateway**" field). If the "**Enable DHCPv4**" checkbox is selected, the default gateway address should be automatically configured via the DHCP server (when this checkbox is selected, the "**IPv4 Gateway**" field won't be displayed in this window.

> **Note**: The same info applies if you are using an IPv6 network, except the associated fields for IPv6 networks are the "**Enable DHCPv6"** checkbox and the "**IPv6 Gateway**" field.



PORT	ACTION	STATUS
eth0		CONNECTED (100MB/S)

☑ Enable eth0

Domain:

DNS Primary:

DNS Secondary:

□ Enable DHCPv4

Static IPv4 Address: 10.2.100.176

Netmask: 255.255.0.0

IPv4 Gateway: 10.2.1.1

□ Enable DHCPv6

□ Enable SLAAC

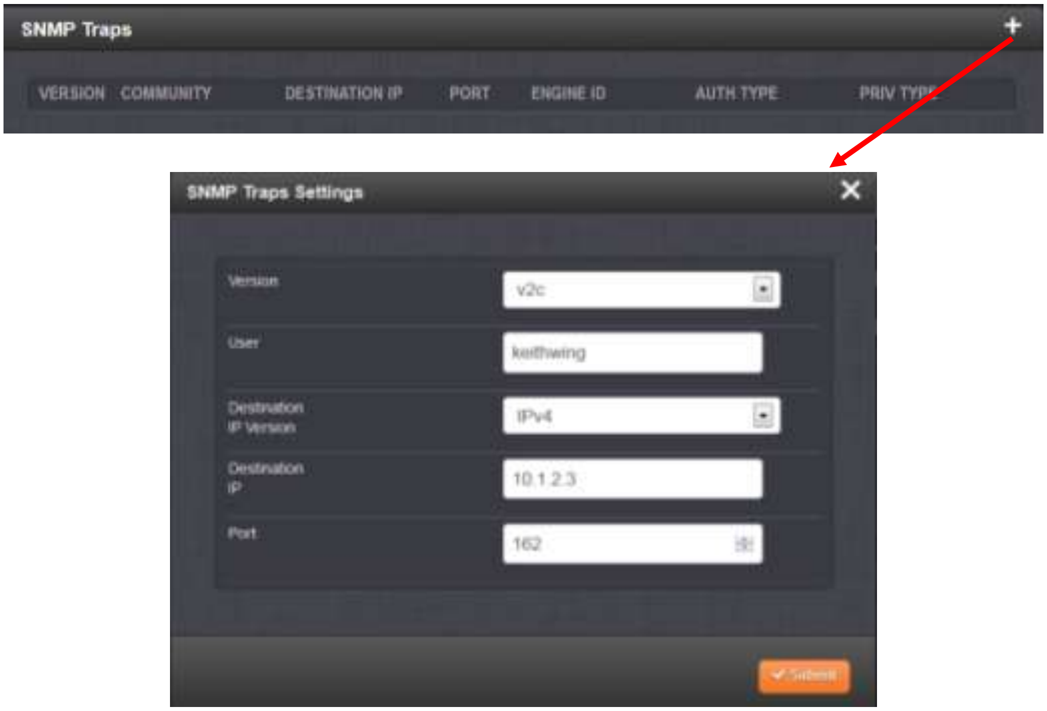
IPv6 Gateway:

Figure 10: Configuring the default gateway (versions 5.1.2 and higher)

- Now refer to **Section 8B** below for **SNMPv1/SNMPv2c** Trap configuration.
- Now refer to **Section 8C** below for **SNMPv3** Trap configuration.

Section 8B: Enabling/Disabling and configuring SNMP V1/SNMPV2 Trap generation

With SNMP enabled and the Global default Gateway configured, SNMP traps can be sent to up to five different SNMP Managers on the network, as configured in the "**SNMP Traps**" section of the "**Management**" -> "**SNMP Setup**" page of the browser.



SNMP Traps

VERSION	COMMUNITY	DESTINATION IP	PORT	ENGINE ID	AUTH TYPE	PRIV TYPE

SNMP Traps Settings

Version	v2c
User	keithwing
Destination IP Version	IPv4
Destination IP	10.1.2.3
Port	162

Figure 11: "Notifications (Traps)" tab of the "SNMP Setup" web page

Fill out this section of the "Notifications (Traps)" tab (refer to Figure 22) to enable SNMP Traps to be sent from the SecureSync to the SNMP Manager(s) on the network. Traps that are individually enabled will be automatically sent if and when the specific condition (event) occurs.

Version: Select v1, v2c or v3 as desired for the Traps to be sent from the time server to the SNMP Manager.

> **Note**: The SNMP Manager must support SNMPv3 functionality in order to send encrypted SNMP Traps to the SNMP Manager.

Type: Select either "Trap" to enable SNMP Traps to be sent to the SNMP Manager or "None" to disable Traps.

User/Community: Enter the community name for SNMP as configured in the SNMP Manager (such as "public").

Dest IP version: Select either "IPv4" or "IPv6" as appropriate for the SNMP Manager's IP addressing.

Destination IP: Enter the appropriate box for the IP address of the desired SNMP Manager(s).

> **Note:** This list is limited to five SNMP Manager IP addresses.

> **Important Note:** When entering any other values in this same row, the Destination IP address field is a required field. With software versions 5.0.0, 5.0.1 or 5.0.2 installed, this field needs a value entered in it before pressing Submit. Leaving this field blank when pressing Submit

with these version of software installed will result in the web browser displaying an error message and requires a **clean** command be performed to reset the unit's configurations back to their factory default settings. This issue was addressed in the version 5.1.0 software update.

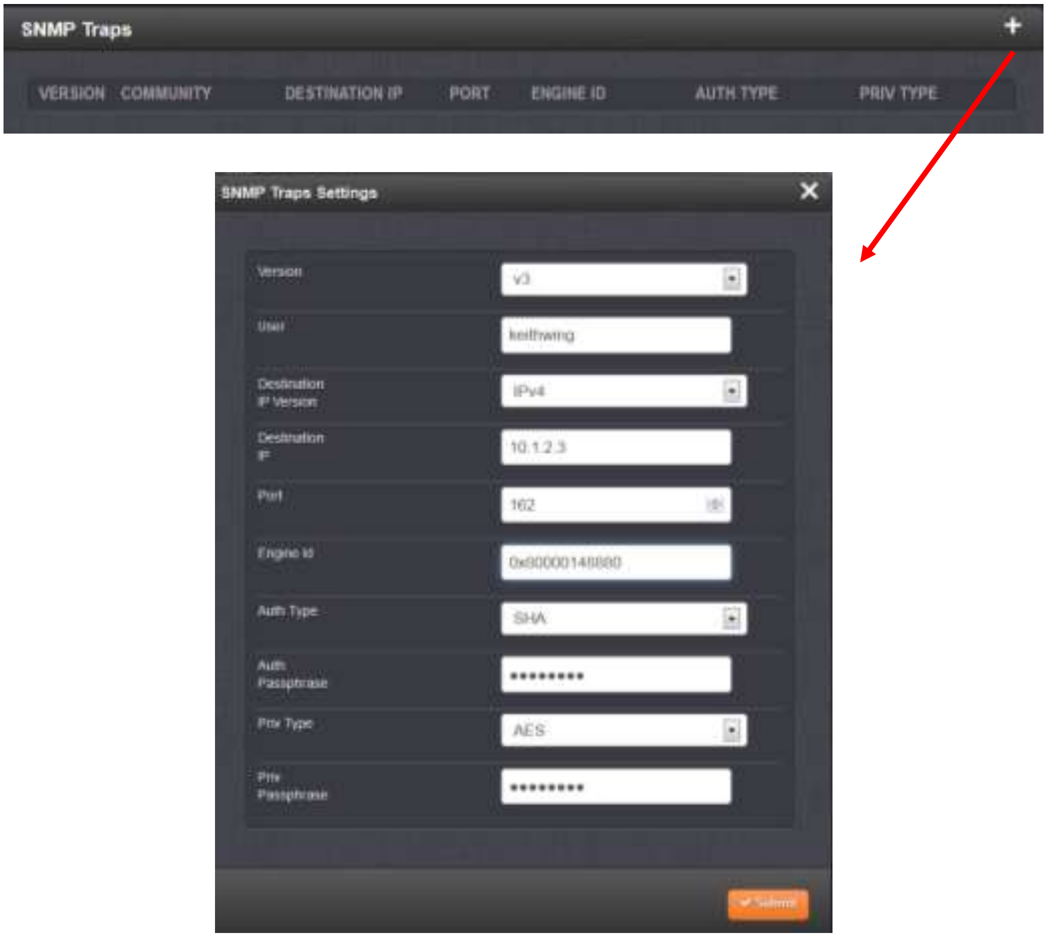
Port #: Enter the desired SNMP port value. The default port setting for SNMP is Port 162, but the time server allows configuration to another assigned port number as desired/required by the network.

Note: The remaining configurations in this particular section are only needed when using SNMPv3 SNMP Manager (they aren't required when using SNMPv1/SNMPv2c sets, gets and Traps).

Section 8C: Enabling/Disabling and configuring SNMPv3 Trap generation

With SNMP enabled, SNMP traps can be sent to up to five different SNMP Managers on the network, as configured in the "**Notifications (Traps)**" tab on the "**Network**" -> "**SNMP Setup**" page of the browser.

"**Notifications (Traps)**" tab



Version	v3
User	keithwing
Destination IP Version	IPv4
Destination IP	10.1.2.3
Port	162
Engine Id	0x80000148880
Auth Type	SHA
Auth Passphrase	*********
Priv Type	AES
Priv Passphrase	*********

Figure 12: "Notifications (Traps)" tab of the "SNMP Setup" web page

Fill out this section of the "Notifications (Traps)" tab (refer to Figure 22) to enable SNMP Traps to be sent from the SecureSync to the SNMP Manager(s) on the network. Traps that are individually enabled will be automatically sent if and when the specific condition (event) occurs.

Version: Select v1, v2c or v3 as desired for the Traps to be sent from the time server to the SNMP Manager.

> **Note**: The SNMP Manager must support SNMPv3 functionality in order to send encrypted SNMP Traps to the SNMP Manager.

Type: Select either "Trap" to enable SNMP Traps to be sent to the SNMP Manager or "None" to disable Traps.

User/Community: Enter the community name for SNMP as configured in the SNMP Manager (such as "public").

Dest IP version: Select either "IPv4" or "IPv6" as appropriate for the SNMP Manager's IP addressing.

Destination IP: Enter the appropriate box for the IP address of the desired SNMP Manager(s).

Note: This list is limited to five SNMP Manager IP addresses.

Port #: Enter the desired SNMP port value. The default port setting for SNMP is Port 162, but the time server allows configuration to another assigned port number as desired/required by the network.

Note: The following configurations in this particular section are only needed when sending SNMPv3 Traps to the time server (they aren't required when using SNMPv1/SNMPv2c).

Engine ID (SNMPv3): Enter the SNMP EngineID of the authoritative SNMP engine involved in the exchange of this message.

Note: The Engine ID is a 12 octet, hexadecimal value that needs to be externally created by a user and then entered into the SecureSync's web browser. This value needs to begin with a "0x". If this field is left blank, its defaults to "0x01". If your SNMP Manager/MIB browser generates a hex "Content ID" value, this value can be used as the Engine ID.

Note: Archive software version 4.8.9 extends the allowable number of characters that can be entered into this field. Archive software versions 4.8.9 and above can have up to 50 characters in this field, while earlier versions of software limited this field to 32 characters.

Auth type: Select the desired authentication algorithm as either "MD5" or "SHA".

Auth Passphrase: Enter an 8-32 character passphrase for authentication.

Priv Type: Select the desired encryption algorithm as "None", "DES" or "AES"

Priv Passphrase: Enter an 8-32 character passphrase for encryption.

Section 9: SNMP Traps (Notifications) (Software versions 5.0.2 and below only)

The Spectracom SecureSync has the ability to automatically send SNMP Traps and/or Email alerts when certain SecureSync conditions (events) occur. These SNMP Traps are received by one or more SNMP Managers, and with the SNMP MIB files compiled into the SNMP Manager, the SNMP Manager can be configured as desired to react to a received SNMP Trap.

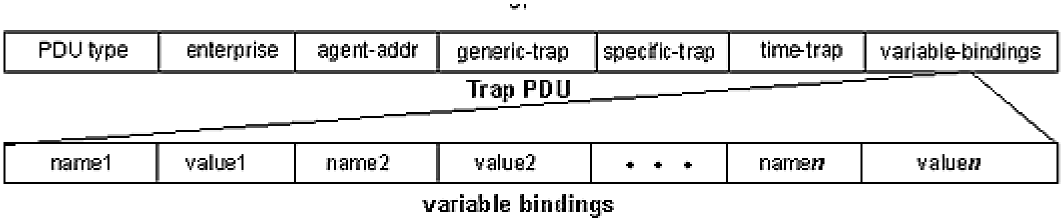
To begin, from Wikipedia:

Trap

Asynchronous notification from agent to manager. Includes current sysUpTime value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed SNMPv2-Trap.

SNMP traps are a one-way only transmission of a network packet (From SecureSync to SNMP Managers on the network) that occurs each time specific events occur and when they clear. Note that not all events actually “clear”, so just one trap is sent when that particular type of event occurs (such as switching from one input reference to another).

Below is the packet structure of an SNMP trap. The second line breaks down the optional “Variable-bindings (also known as the “varbind”) field. “Varbinds” can provide the SNMP Manager with additional specific information about the trap.



SecureSync traps

SecureSync SNMP traps are not solicited by the SNMP Manager(s) on the network. The SecureSync just sends out a trap (also referred to as a “notification”) using a defined OID number in an SNMP packet when specific events occur. When the SNMP Manager receives the trap packet, it looks up the particular OID number in the MIB files that have been compiled into the SNMP Manager software. It determines what the particular OID number means and based on how you have set up the SNMP Manager, you can have it perform different things when a trap from the SecureSync is received.

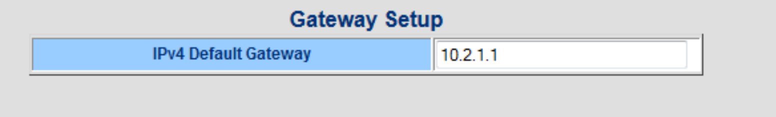
Most, but not all, SecureSync conditions (events) consist of two related events. One is the “On” event which occurs when and event first happens and the other is the “Off” event which occurs later, when the condition clears. However, a few conditions consist of only one event occurring, as these conditions may be a one-time occurrence that doesn’t actually “clear”. An example of a condition that doesn’t “clear” is when SecureSync switches from one input reference to lower priority input reference. Only one “event” occurs in this particular situation, when SecureSync switches to using a different input reference. If it subsequently changes back to the original input reference, the same one-time event occurs again.

Section 9A: Configuring the Default Port and "Global" Default Gateway

As described in more detail in each of the two follows sections below, the default Gateway Address needs to be properly configured in the SecureSync, when it's desired to send SNMP traps. As the SNMP traps are originating from within the SecureSync (they are unsolicited packets), the route for the traps to take in order to reach the configured SNMP Manager(s) needs to be defined, via the Default (Global) Gateway address. A

Also, if the Model 1204-06 Gigabit Ethernet Option card is installed (to add three additional Ethernet interfaces), the Ethernet interface that needs to route the SNMP traps to the SNMP Manager(s) also needs to be selected (this is known as the "Default Port").

The default gateway for each network interface is configured in the **Network** -> **Interfaces** page of the browser. A tab for each network interface installed will be displayed (only "eth0" is shown, if the Model 1204-06 Option Card is not installed). Select the network interface tab that the SNMP packets need to go through to reach the SNMP Manager (such as "eth0" for example). Scroll down and verify the IPv4 (or IPv6) Gateway address is configured appropriately for the network this port is connected with. The IPv4 Gateway address is configured/displayed in the "Gateway Setup field".

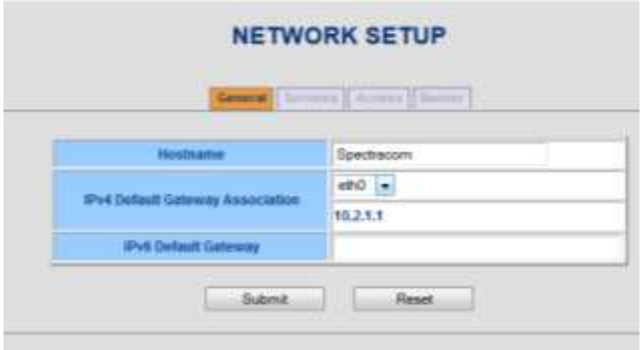


Gateway Setup

IPv4 Default Gateway	10.2.1.1

Figure 13: Configuring the Default gateway (versions 5.0.2 and below)

If the Model 1204-06 Gigabit Ethernet Option Card is installed, which Ethernet Interface port to route the SNMP traps to the SNMP Manager needs to be selected, this port is selected via a drop-down in the **Network** -> **General Setup** page of the browser, "**General**" tab. This interface port is referred to as the "**Default port**" and is selected in the "**IPv4 Default Gateway Association**" field. If using IPv6, enter the IPv6 address in the "IPv6 Default Gateway" field. The configured global gateway address for the selected port will be displayed in the field below the drop-down.



NETWORK SETUP

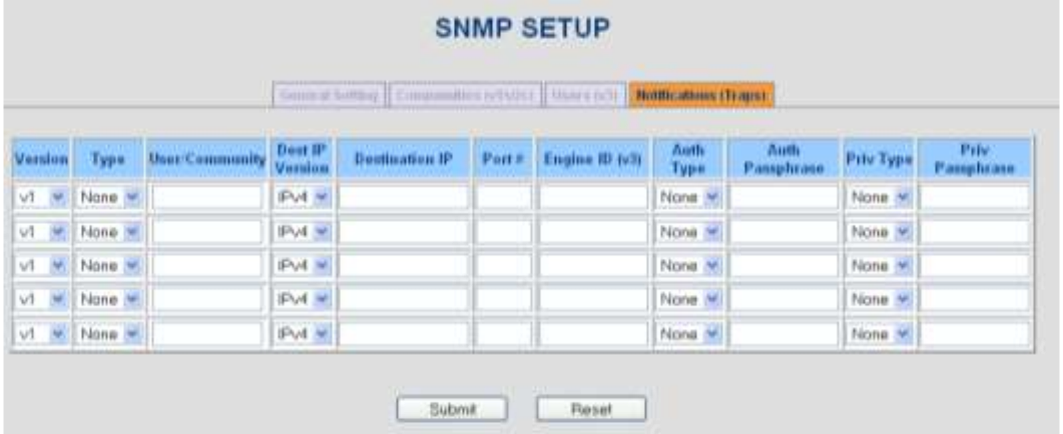
Hostname	Spectracom
IPv4 Default Gateway Association	eth0 10.2.1.1
IPv6 Default Gateway	

Figure 14: Configuring the Default Port (versions 5.0.2 and below)

- Now refer to **Section 9B** below for **SNMPv1/SNMPv2c** Trap configuration.
- Now refer to **Section 9C** below for **SNMPv3** Trap configuration.

Section 9B: Enabling/Disabling and configuring SNMP V1/SNMPV2 Trap generation

With SNMP enabled and the Global default Gateway configured, SNMP traps can be sent to up to five different SNMP Managers on the network, as configured in the “**Notifications (Traps)**” tab on the “**Network**” -> “**SNMP Setup**” page of the browser.



SNMP SETUP

Version	Type	User/Community	Dest IP Version	Destination IP	Port #	Engine ID (v3)	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
v1	None		IPv4				None		None	
v1	None		IPv4				None		None	
v1	None		IPv4				None		None	
v1	None		IPv4				None		None	
v1	None		IPv4				None		None	

Figure 15: “Notifications (Traps)” tab of the “SNMP Setup” web page

Fill out this section of the “Notifications (Traps)” tab (refer to Figure 22) to enable SNMP Traps to be sent from the SecureSync to the SNMP Manager(s) on the network. Traps that are individually enabled will be automatically sent if and when the specific condition (event) occurs.

Version: Select v1, v2c or v3 as desired for the Traps to be sent from the time server to the SNMP Manager.

> **Note**: The SNMP Manager must support SNMPv3 functionality in order to send encrypted SNMP Traps to the SNMP Manager.

Type: Select either “Trap” to enable SNMP Traps to be sent to the SNMP Manager or “None” to disable Traps.

User/Community: Enter the community name for SNMP as configured in the SNMP Manager (such as “public”).

Dest IP version: Select either “IPv4” or “IPv6” as appropriate for the SNMP Manager’s IP addressing.

Destination IP: Enter the appropriate box for the IP address of the desired SNMP Manager(s).

> **Note:** This list is limited to five SNMP Manager IP addresses.
>
> **Important Note:** When entering any other values in this same row, the Destination IP address field is a required field. With Archive software versions 5.0.0, 5.0.1 or 5.0.2 installed, this field needs a value entered in it before pressing Submit. Leaving this field blank when pressing Submit with these version of software installed will result in the web browser displaying an error message and requires a **clean** command be performed to reset the unit’s configurations back to their factory default settings. This issue was addressed in the version 5.1.0 software update.

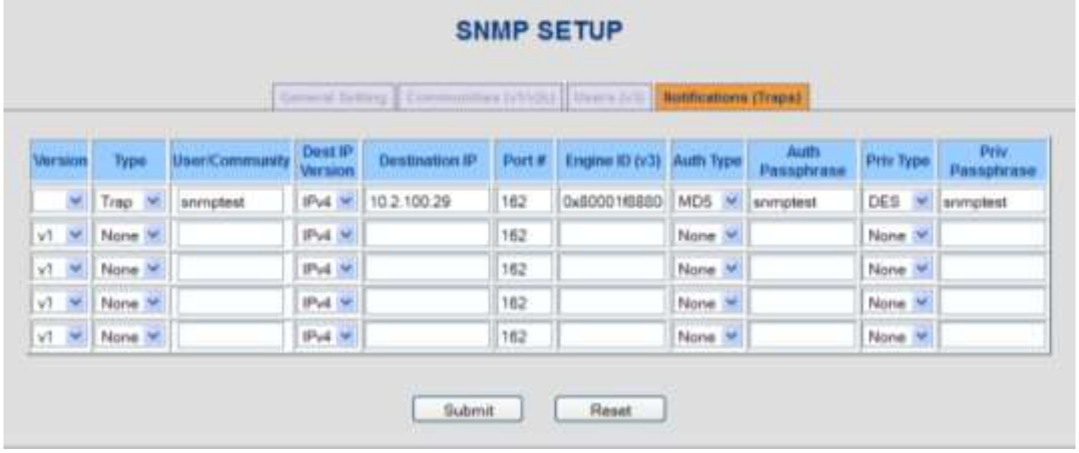
Port #: Enter the desired SNMP port value. The default port setting for SNMP is Port 162, but the time server allows configuration to another assigned port number as desired/required by the network.

Note: The remaining configurations in this particular section are only needed when using SNMPv3 SNMP Manager (they aren't required when using SNMPv1/SNMPv2c sets, gets and Traps).

Section 9C: Enabling/Disabling and configuring trap generation (SNMPv3 Traps only)

With SNMP enabled and the Global default Gateway configured, SNMP traps can be sent to up to five different SNMP Managers on the network, as configured in the "**Notifications (Traps)**" tab on the "**Network**" -> "**SNMP Setup**" page of the browser.

"**Notifications (Traps)**" tab



Version	Type	User/Community	Dest IP Version	Destination IP	Port #	Engine ID (v3)	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
	Trap	snmptest	IPv4	10.2.100.29	162	0x80001f8880	MD5	snmptest	DES	snmptest
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	

Figure 16: "Notifications (Traps)" tab of the "SNMP Setup" web page

Fill out this section of the "Notifications (Traps)" tab (refer to Figure 22) to enable SNMP Traps to be sent from the SecureSync to the SNMP Manager(s) on the network. Traps that are individually enabled will be automatically sent if and when the specific condition (event) occurs.

Version: Select v1, v2c or v3 as desired for the Traps to be sent from the time server to the SNMP Manager.

Note: The SNMP Manager must support SNMPv3 functionality in order to send encrypted SNMP Traps to the SNMP Manager.

Type: Select either "Trap" to enable SNMP Traps to be sent to the SNMP Manager or "None" to disable Traps.

User/Community: Enter the community name for SNMP as configured in the SNMP Manager (such as "public").

Dest IP version: Select either "IPv4" or "IPv6" as appropriate for the SNMP Manager's IP addressing.

Destination IP: Enter the appropriate box for the IP address of the desired SNMP Manager(s).

Note: This list is limited to five SNMP Manager IP addresses.

Port #: Enter the desired SNMP port value. The default port setting for SNMP is Port 162, but the time server allows configuration to another assigned port number as desired/required by the network.

Note: The following configurations in this particular section are only needed when sending SNMPv3 Traps to the time server (they aren't required when using SNMPv1/SNMPv2c).

Engine ID (SNMPv3): Enter the SNMP EngineID of the authoritative SNMP engine involved in the exchange of this message.

Note: The Engine ID is a 12 octet, hexadecimal value that needs to be externally created by a user and then entered into the SecureSync's web browser. This value needs to begin with a "0x". If this field is left blank, its defaults to "0x01". If your SNMP Manager/MIB browser generates a hex "Content ID" value, this value can be used as the Engine ID.

Note: Archive software version 4.8.9 extends the allowable number of characters that can be entered into this field. Archive software versions 4.8.9 and above can have up to 50 characters in this field, while earlier versions of software limited this field to 32 characters.

Auth type: Select the desired authentication algorithm as either "MD5" or "SHA".

Auth Passphrase: Enter an 8-32 character passphrase for authentication.

Priv Type: Select the desired encryption algorithm as "None", "DES" or "AES"

Priv Passphrase: Enter an 8-32 character passphrase for encryption.

Section 10: Authentication Error Trap and System SNMP Information fields

The Auth (Authentication) trap is an SNMPv2-generic trap (not a Spectracom-specific trap) that occurs each time an incorrect SNMP login attempt occurs (for example, the SNMP v2 community name is configured as “public123” but a user tries using an SNMP login value of “public”, instead. This failed login attempt will send this generic SNMP trap.

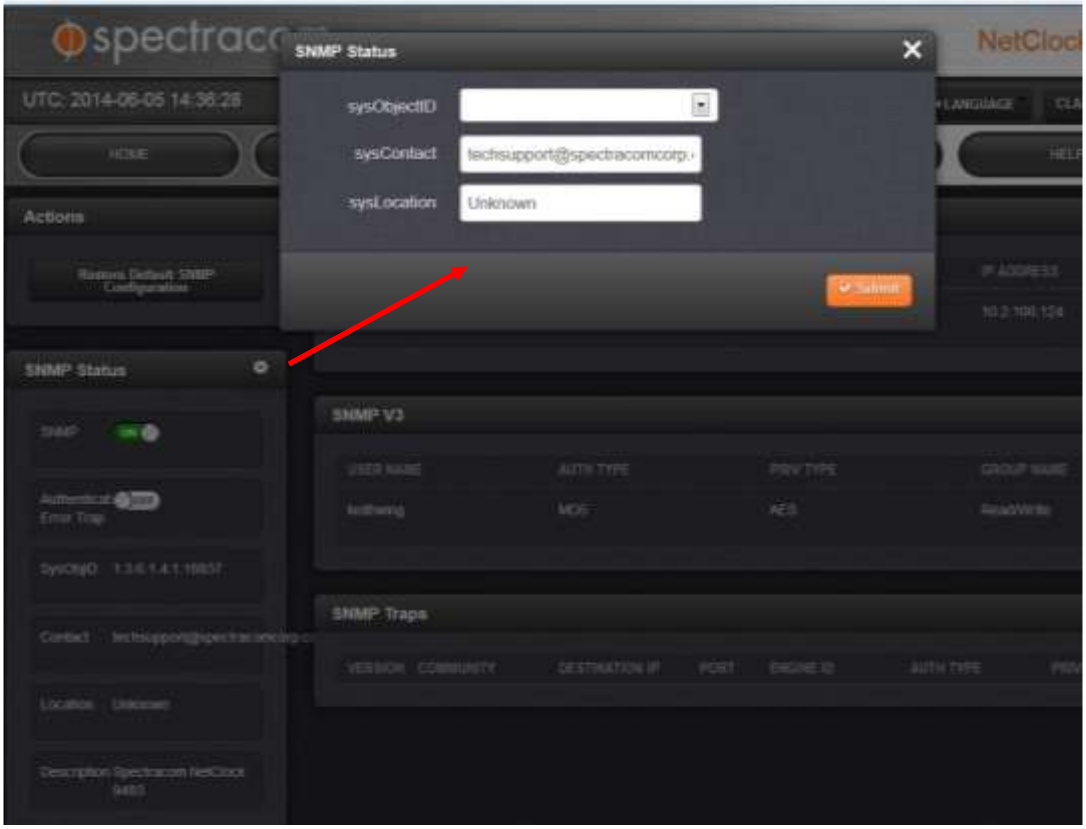
From the SNMPv2 MIB file:
"An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated."

A) Software versions 5.1.2 and above only

Besides providing the ability to either Enable or Disable SNMP, the “**SNMP Status** ” section on the left side of the “**Management**” -> “**SNMP Setup**” page also provides the ability to either enable or disable the “Authentication Error Trap (also referred to as the “Auth” trap). Refer to Figure 17.

Note: The generic SNMPv2 MIB file must be compiled in order to define this generic trap. This generic SNMP MIB file can be pre-compiled onto SNMP Managers (it is not included with the SecureSync’s MIB files). If the SNMPv2 MIB file is not pre-complied onto your SNMP Manager, this MIB file may be able to be downloaded from the Internet (refer to sites such as: http://www.net-snmp.org/docs/mibs/).

The **SNMP Status**” section also allows the reported System Information for SNMP to be individually configured, via the three available “Sys…” fields (consisting of “sysObjectID”, “sysContac” and “sysLocation”).



SNMP Status

sysObjectID

sysContact techsupport@spectracomcorp.

sysLocation Unknown

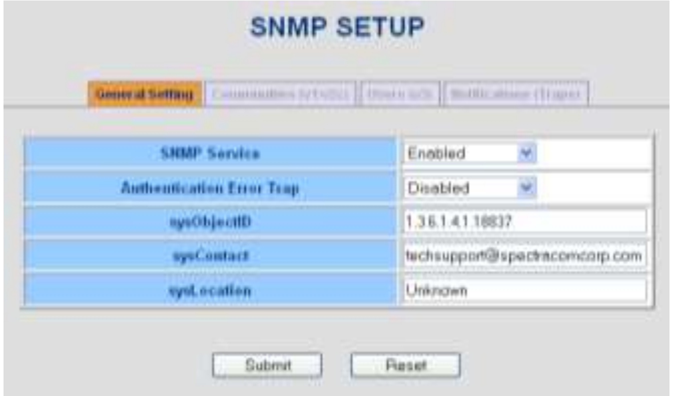
Figure 17: "Authentication Error Trap" and System SNMP Information

B) Software versions 5.0.2 and below

Besides providing the ability to either Enable or Disable SNMP, the "**General Settings**" tab of the "**Network**" -> "**SNMP Setup**" page also provides the ability to either enable or disable the "Authentication Error Trap (also referred to as the "Auth" trap). Refer to Figure 25.

Note: The generic SNMPv2 MIB file must be compiled in order to define this generic trap. This generic SNMP MIB file can be pre-compiled onto SNMP Managers (it is not included with the SecureSync's MIB files). If the SNMPv2 MIB file is not pre-complied onto your SNMP Manager, this MIB file may be able to be downloaded from the Internet (refer to sites such as: http://www.net-snmp.org/docs/mibs/).

The "General Setting" tab also allows the reported System Information for SNMP to be individually configured, via the three available "Sys…" fields (consisting of "sysObjectID", "sysContac" and "sysLocation").



SNMP SETUP

SNMP Service	Enabled
Authentication Error Trap	Disabled
sysObjectID	1.3.6.1.4.1.18837
sysContact	techsupport@spectracomcorp.com
sysLocation	Unknown

Figure 18: "Authentication Error Trap" and System SNMP Information

Section 11: Descriptions of the available generic SNMP traps (Non-Spectracom specific SNMP traps)

The SecureSync automatically sends three generic SNMPv2 traps when the SNMP agent in the SecureSync changes states. These generic SNMPv2 traps (SNMP Start, SNMP Shutdown and SNMP Restart) are defined in the Net-SNMP-Agent-MIB.mib file (as also defined below):

NotifyStart: “An indication that the agent has started running.” (Such as enabling SNMP)

NotifyShutdown: “An indication that the agent is in the process of being shut down.” (Such as disabling SNMP)

NotifyRestart: “An indication that the agent has been restarted. This does not imply anything about whether the configuration has changed or not (unlike the standard coldStart or warmStart traps).”

Note: Unlike the available Spectracom-specific SNMP traps, these generic SNMP traps do not have the ability to be disabled or to send email alerts when they occur.

Section 12: Ability to “Mask” (override/squelch) undesired alarms

In some SecureSync configurations, there may be one or more alarm conditions that will remain always asserted, so the associated alarm(s) may need to remain active. This results in the front panel “Fault” LED remaining lit. Starting in Archive software version 4.8.7, undesired “Spectracom-specific” alarms can be “masked” (squelched) to prevent undesired alarms from being continuously asserted.

Log entries are still inserted for masked alarm conditions, but traps and emails aren’t sent for masked alarm conditions. And masking undesired alarm conditions can allow the front panel “Fault” LED to clear when all other “non-masked” alarm conditions have cleared.

Examples of desired SecureSync configurations that may warrant the desire to mask alarms include:

1) When syncing the SecureSync to itself (user mode) or to only other NTP servers (no GPS input), it may be desired to mask both the “Antenna Problem” alarm (that is normally asserted when the GPS antenna is disconnected) and the Frequency alarm which is asserted because the 10 MHz oscillator cannot be disciplined to NTP input or to user set time.

2) When the SecureSync was purchased with a GPS receiver installed, but it’s currently desired to sync it via IRIG input only (the GPS antenna is not currently connected). If a GPS antenna is not connected, the Antenna Problem alarm will always be active. Since this is an expected alarm condition which will prevent the Fault LED from clearing, it may be desired to mask the Antenna Problem alarm.

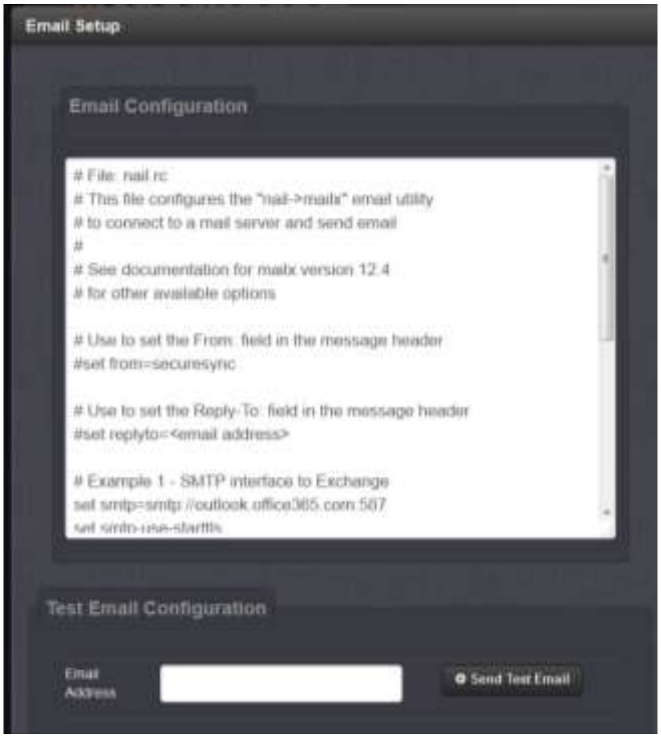
Note: Alarms are “Masked” by selecting the “Mask Alarm” checkbox, as mentioned in the next Section.

Section 13: Email Alerts/ Descriptions of the available Spectracom-specific SNMP traps

In addition to generic SNMP traps, the SecureSync also has the ability to send several individual, Spectracom-specific SNMP traps, as desired. Configuring "Email alerts" to be able to generate automatic Emails when certain events occur, in order for SecureSync to be able to be able to automatically send an Email alert each time certain events occur, SecureSync has to be properly configured to send Email, as applicable to your specific email requirements.

A) Newer web browser (Software versions 5.1.2 and above)

To setup Email capability, navigate to the "**Management**" -> "**Notifications**" page of the browser and click on the "**Edit Setup"** button located on the left side of the page. Section 4 discusses how to simulate events in order to test Email alert functionality.



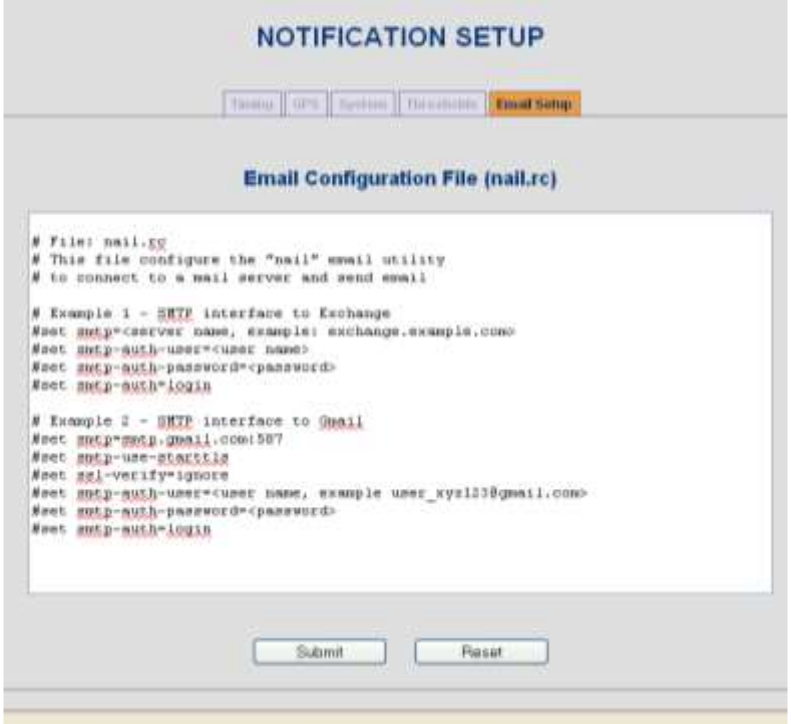
```
# File: nail.rc
# This file configures the "nail->mailx" email utility
# to connect to a mail server and send email
#
# See documentation for mailx version 12.4
# for other available options

# Use to set the From: field in the message header
#set from=securesync

# Use to set the Reply-To: field in the message header
#set replyto=<email address>

# Example 1 - SMTP interface to Exchange
set smtp=smtp://outlook.office365.com:587
set smtp-use-starttls
```

Figure 19: Email alert configuration (newer browser)

Note: Refer to the SecureSync instruction manual for information on editing the "Email Configuration File" as applicable to your specific Email server's requirements.

B) Classic Interface browser (Software versions 5.0.2 and below)

To setup Email capability, navigate to the "**Tools**" -> "**Notification**" page of the browser and click on the "**Email Setup**" tab. Section 4 discusses how to simulate events in order to test Email alert functionality.



```
# File: nail.rc
# This file configure the "nail" email utility
# to connect to a mail server and send email

# Example 1 - SMTP interface to Exchange
#set smtp=<server name, example: exchange.example.com>
#set smtp-auth-user=<user name>
#set smtp-auth-password=<password>
#set smtp-auth=login

# Example 2 - SMTP interface to Gmail
#set smtp=smtp.gmail.com:587
#set smtp-use-starttls
#set ssl-verify=ignore
#set smtp-auth-user=<user name, example user_xyz123@gmail.com>
#set smtp-auth-password=<password>
#set smtp-auth=login
```

Figure 20: Email alert configuration (classic interface)

Note: Refer to the SecureSync instruction manual for information on editing the "Email Configuration File" as applicable to your specific Email server's requirements.

Enabling and disabling each individual trap/email alert (Events)

Each available SNMP Trap and Email alert can individually be either enabled or disabled, as desired. With the exception of the generic "Authorization Error Trap" (which is enabled elsewhere in SecureSync, as previously described) the list of all other "Spectracom-specific" available traps and the enable/disable check box for each trap is located in either the "**Management**" **->** "**Notifications**" page of the classic interface browser or the "**Tools**" -> "**Notification Setup**" page of the "classic interface" browser.

Three of the tabs located on this page ("Timing", "GPS" and "System") contain the lists of all available traps and email alerts that can be sent (separated into the three tabs by their function within the system), below is a lists and descriptions of currently available traps that can be enabled or disabled in each of these tabs. Note that only one email address can be entered in each event field.

Note: The list of available SNMP Traps may be software version specific so the list below may not be the same in all versions of SecureSync software.

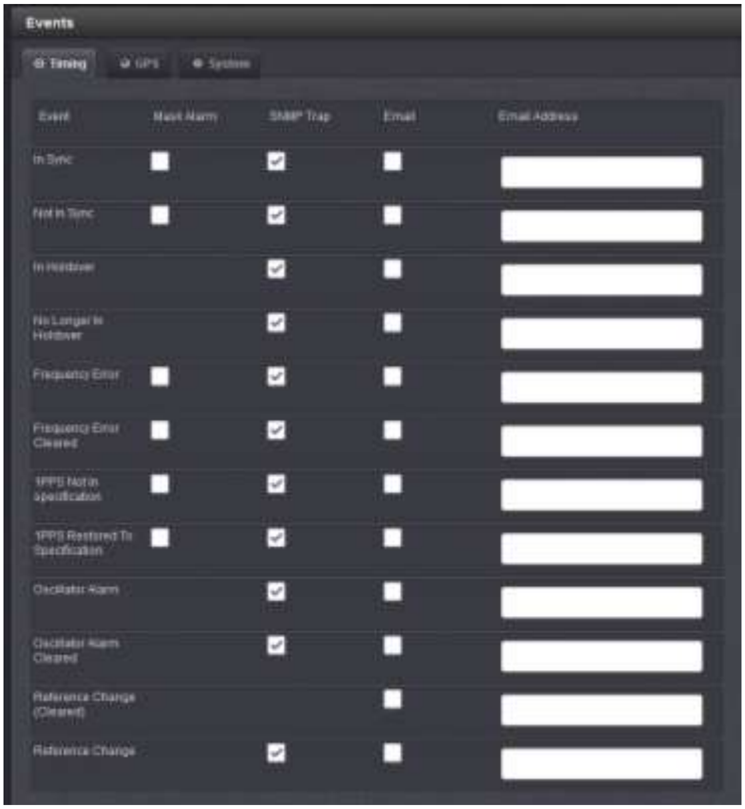
Spectracom-specific SNMP trap OID Numbers

SNMP Trap name	Corresponding OID Number	Indicates	Associated "Integer" values reported in each trap
ssEvtV2TimeSync	1.3.6.1.4.1.18837.3.2.3.0.1	The unit has either entered or left the synchronized state.	Reports either of the following: "**sync (1)**" if unit currently in Sync "**nosync (2)**" if unit not currently in Sync
ssEvtV2Holdover	1.3.6.1.4.1.18837.3.2.3.0.2	The unit has either entered or left the holdover state.	Reports either of the following: "**inHoldover (1)**" if unit currently in Holdover "**notInHoldover (2)** " If unit not currently in Holdover mode
ssEvtV2FrequencyError	1.3.6.1.4.1.18837.3.2.3.0.3	The frequency output error exceeds specifications.	Reports the currently measured Fractional Frequency Error (as also indicated in the Oscillator log) (can be a positive or negative value)
ssEvtV2FrequencyOK	1.3.6.1.4.1.18837.3.2.3.0.4	The frequency output error meets specifications.	Reports the currently measured Fractional Frequency Error (as also indicated in the Oscillator log) (can be a positive or negative value)
ssEvtV2UserMinorAlarm	1.3.6.1.4.1.18837.3.2.3.0.5	The user-programmable minor alarm timeout has been asserted.	Reports the number of satellites currently being tracked by the receiver
ssEvtV2UserMinorClear	1.3.6.1.4.1.18837.3.2.3.0.6	The user-programmable minor alarm timeout has been reset.	Reports the number of satellites currently being tracked by the receiver
ssEvtV2UserMajorAlarm	1.3.6.1.4.1.18837.3.2.3.0.7	The user-programmable major alarm timeout has been asserted.	Reports the number of satellites currently being tracked by the receiver
ssEvtV2UserMajorClear	1.3.6.1.4.1.18837.3.2.3.0.8	The user-programmable major alarm timeout has been reset.	Reports the number of satellites currently being tracked by the receiver
ssEvtV2GpsAntenna	1.3.6.1.4.1.18837.3.2.3.0.9	The GPS antenna state has changed (antenna is disconnected, short or open occurring in the antenna cable)	Will report one of the following four values depending on the current antenna cable state **Ok (1)** (good connection to antenna) **Short (2)** (short detected in cable) **Open (3)** (open detected in cable) **Unknown (4)** (receiver may have been damaged by a power surge)
ssEvtV2MinorAlarm	1.3.6.1.4.1.18837.3.2.3.0.10	The system minor alarm has changed state.	Will report one of the following two values **Pending (1)** (Minor alarm is currently active) **Clear (2)** (Minor alarm is currently not active)
ssEvtV2MajorAlarm	1.3.6.1.4.1.18837.3.2.3.0.11	The system major alarm has changed state.	Will report one of the following two values **Pending (1)** if Major alarm is currently active **Clear (2)** if Major alarm is currently not active
ssEvtV2RefChange	1.3.6.1.4.1.18837.3.2.3.0.12	The selected time reference has changed.	Reports the currently selected Time and 1PPS references (such as GPS , IRIG, NTP, etc)

ssEvtV21ppsError	1.3.6.1.4.1.18837.3.2.3.0.13	The 1PPS output error exceeds specifications.	Reports the currently selected Time and 1PPS references (such as GPS , IRIG, NTP, etc)
ssEvtV21ppsOK	1.3.6.1.4.1.18837.3.2.3.0.14	The 1PPS output error meets specifications.	Reports the currently selected Time and 1PPS references (such as GPS , IRIG, NTP, etc)
ssEvtV2HWError	1.3.6.1.4.1.18837.3.2.3.0.15	The timing system hardware is impaired.	Reports the currently selected Time and 1PPS references (such as GPS , IRIG, NTP, etc)
ssEvtV2OscillatorAlarm	1.3.6.1.4.1.18837.3.2.3.0.16	The oscillator is requires maintenance. This typically indicates that the oscillator is within 10% of the edge its adjustable range (TCXO and OCXO) or the oscillator module lamp needs service (Rubidium).	Reports the currently measured Fractional Frequency Error (can be a positive or negative value)
ssEvtV2OscillatorOK	1.3.6.1.4.1.18837.3.2.3.0.17	The oscillator no longer requires maintenance. This typically indicates that the oscillator adjustment value has changed and is now greater than 10% from the edge of its adjustable range.	Reports the currently measured Fractional Frequency Error(can be a positive or negative value)
ssEvtV2Reboot	1.3.6.1.4.1.18837.3.2.3.0.18	The system has rebooted.	No integer values reported

Table 2: Spectracom-specific SNMP trap OID Numbers

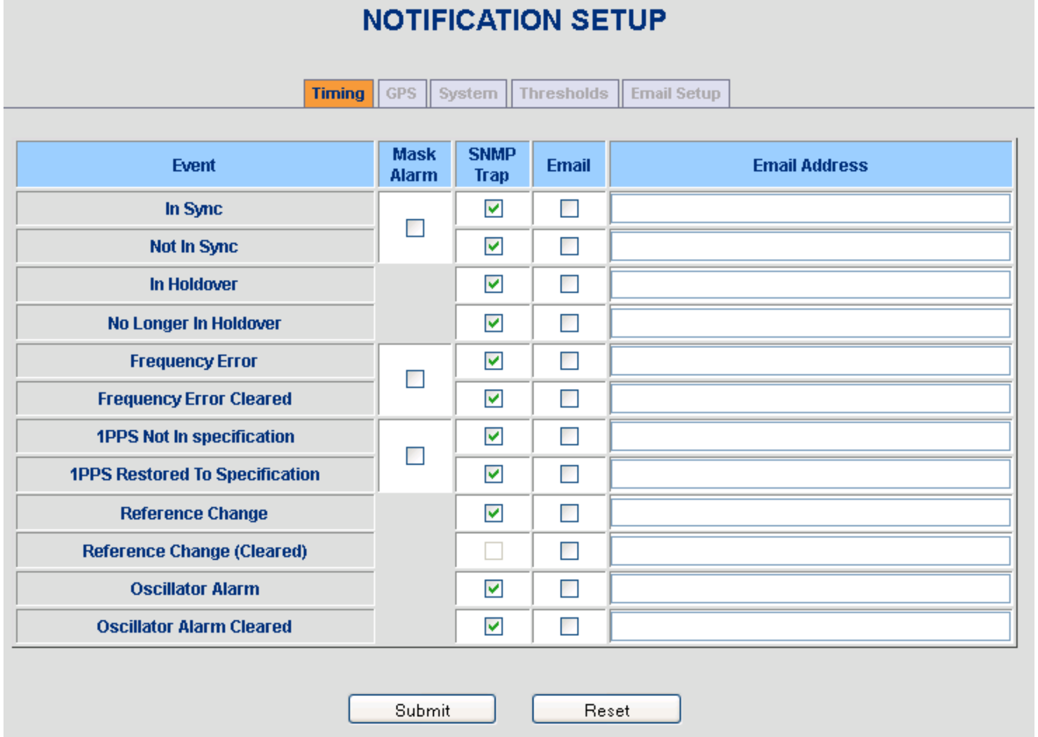
"Timing" related traps/ Email alerts



Events

Event	Mask Alarm	SNMP Trap	Email	Email Address
In Sync	□	☑	□	
Not In Sync	□	☑	□	
In Holdover		☑	□	
No Longer In Holdover		☑	□	
Frequency Error	□	☑	□	
Frequency Error Cleared	□	☑	□	
1PPS Not in specification	□	☑	□	
1PPS Restored To Specification	□	☑	□	
Oscillator Alarm		☑	□	
Oscillator Alarm Cleared		☑	□	
Reference Change (Cleared)			□	
Reference Change		☑	□	

Figure 21: list of available "Timing" related traps/Email alerts (versions 5.1.2 and above)



NOTIFICATION SETUP

Event	Mask Alarm	SNMP Trap	Email	Email Address
In Sync	□	☑	□	
Not In Sync		☑	□	
In Holdover		☑	□	
No Longer In Holdover		☑	□	
Frequency Error	□	☑	□	
Frequency Error Cleared		☑	□	
1PPS Not In specification	□	☑	□	
1PPS Restored To Specification		☑	□	
Reference Change		☑	□	
Reference Change (Cleared)		□	□	
Oscillator Alarm		☑	□	
Oscillator Alarm Cleared		☑	□	

Figure 22: list of available "Timing" related traps/Email alerts (versions 5.0.2 and below)

Description of the available "Timing" Traps and Email alerts

In Sync/Not In Sync: Traps/Emails that can be sent when SecureSync enters or exits "In Sync" status (In Sync indicates that at least one valid time and 1PPS input is present/valid and SecureSync is aligned with these references).

In Holdover/No Longer In Holdover: Traps/Emails that can be sent when SecureSync enters or exits the Holdover mode (Holdover mode occurs when all configured Input references are no longer available or are considered invalid).

Frequency Error/ Frequency Error Cleared: Traps/Emails that can be sent if a Frequency alarm (associated with the oscillator or when SecureSync reboots) occurs and then clears.

1PPS Not In Specification/1PPS Restored To Specification: Traps/Emails that can be sent each time the Maximum TFOM value has been exceeded (The Maximum TFOM value is configured in the "**Setup"/ "Disciplining"** page of the browser) and then also when TFOM has returned to being a value less than the Maximum TFOM value.

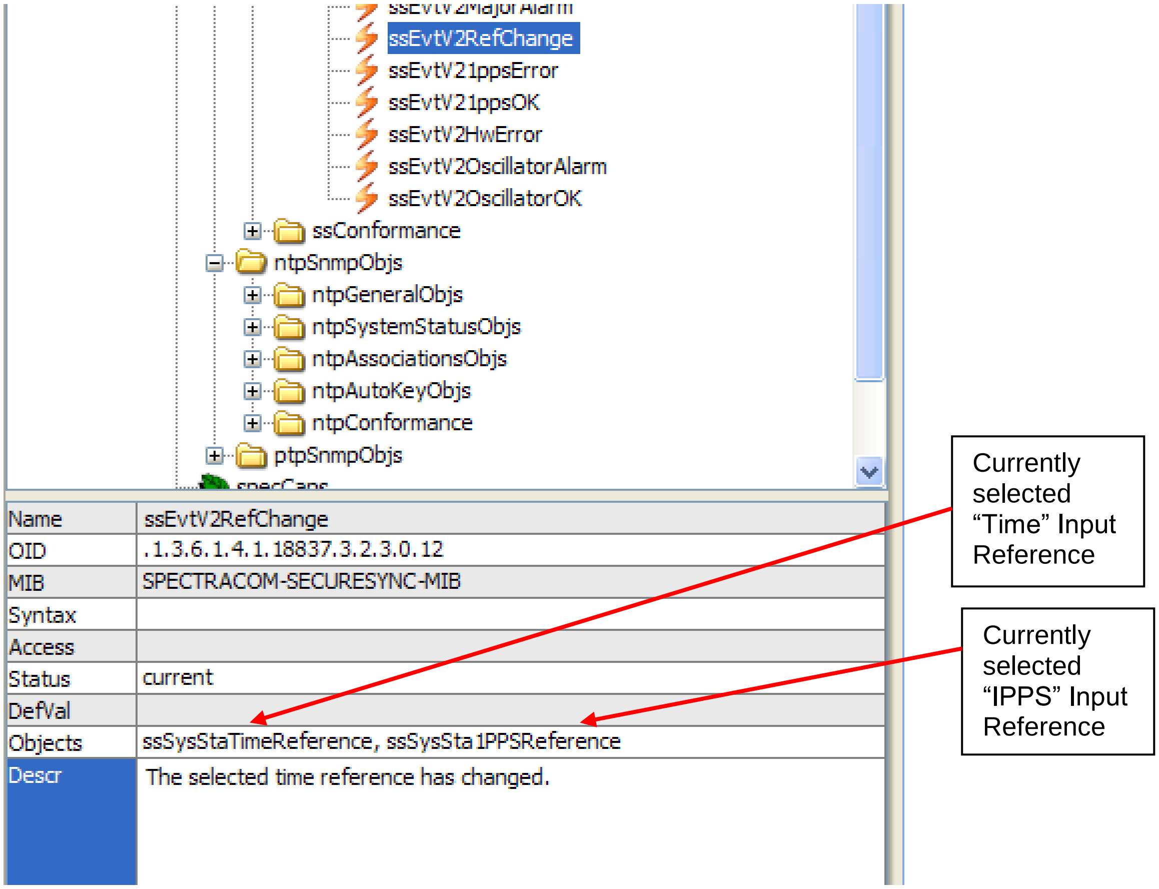
With the Maximum TFOM value set to the default value of "15" (the highest possible value), the "1PPS Not In Specification" alarm will not be asserted, so this trap won't be generated with this TFOM value. In order for the 1PPS to be considered out of specification and therefore this condition to occur, the TFOM value needs to be changed to a lower-value than 15. The Typical expected TFOM values when tracking GPS satellites are 3 and 4. Changing the TFOM value to a 1 or a 2 would cause this condition to occur, even when tracking GPS. Input References other than GPS would likely cause higher TFOM values to be calculated.

Reference Change/Reference Change (Cleared): "Reference Change" Trap/ Email can be sent each time SecureSync switches to a different available Input Reference.

Note: "**Reference Change (Cleared**)" is not a condition/trap, because input Reference changes consist of only event each time it occurs. There is no need for a "clearing" of a Reference Change.

Note that the "Reference Change trap reports what the newly selected "Time" and "1PPS " input references have been changed to, each time an input reference change has occurred:

As shown below, the "Objects" field located in Varbind (Variable Binding) section of the "Reference Change" trap reports both the currently selected "Time" and "1PPS" input references (what input references are selected, after the reference change has occurred).



ssEvtV2MajorAlarm
ssEvtV2RefChange
ssEvtV21ppsError
ssEvtV21ppsOK
ssEvtV2HwError
ssEvtV2OscillatorAlarm
ssEvtV2OscillatorOK
ssConformance
ntpSnmpObjs
ntpGeneralObjs
ntpSystemStatusObjs
ntpAssociationsObjs
ntpAutoKeyObjs
ntpConformance
ptpSnmpObjs
specCaps

Name	ssEvtV2RefChange
OID	.1.3.6.1.4.1.18837.3.2.3.0.12
MIB	SPECTRACOM-SECURESYNC-MIB
Syntax	
Access	
Status	current
DefVal	
Objects	ssSysStaTimeReference, ssSysSta1PPSReference
Descr	The selected time reference has changed.

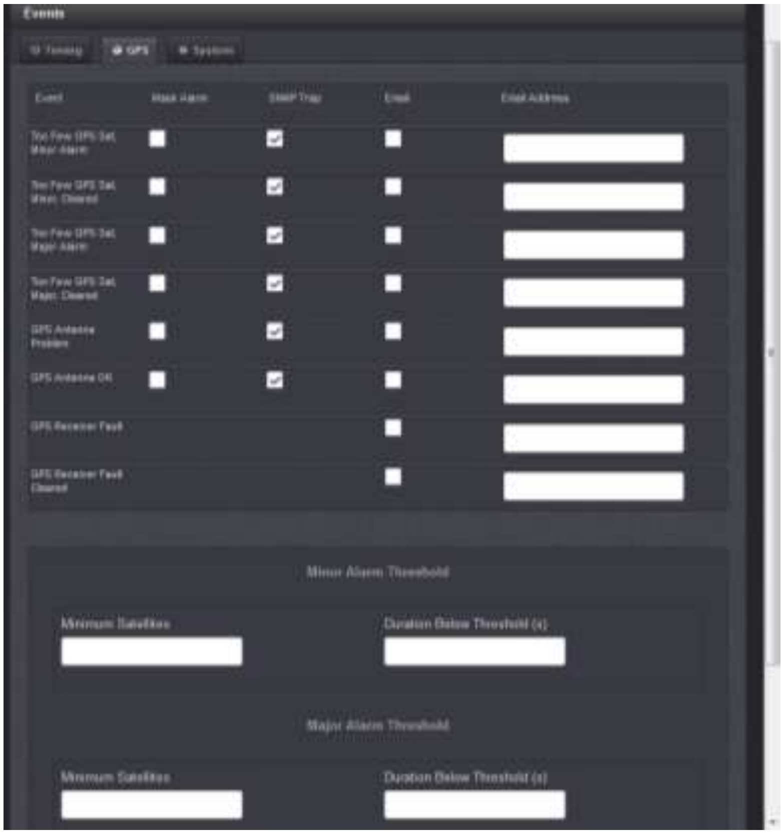
Currently selected “Time” Input Reference

Currently selected “IPPS” Input Reference

Figure 23: Reference Change trap showing newly selected input references

Oscillator Alarm/Oscillator Alarm Cleared: Traps/Emails that can be sent if an Oscillator alarm occurs and when this alarm clears (Oscillator alarm indicates a large frequency error has been detected).

"GPS" related traps/Email alerts



Events

Event	Mask Alarm	SNMP Trap	Email	Email Address
Too Few GPS Sat, Minor Alarm	□	☑	□	
Too Few GPS Sat, Minor, Cleared	□	☑	□	
Too Few GPS Sat, Major Alarm	□	☑	□	
Too Few GPS Sat, Major, Cleared	□	☑	□	
GPS Antenna Problem	□	☑	□	
GPS Antenna OK	□	☑	□	
GPS Receiver Fault			□	
GPS Receiver Fault Cleared			□	

Minor Alarm Threshold

Minimum Satellites

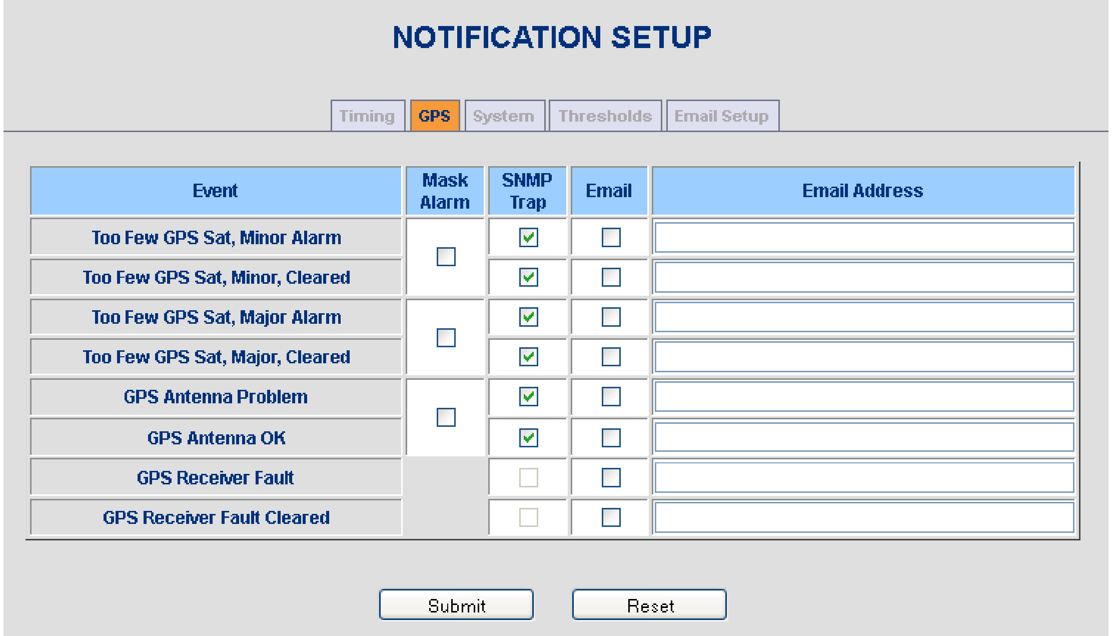
Duration Below Threshold (s)

Major Alarm Threshold

Minimum Satellites

Duration Below Threshold (s)

Figure 24: list of available "GPS" related traps/Email alerts (versions 5.1.2 and above)



NOTIFICATION SETUP

Event	Mask Alarm	SNMP Trap	Email	Email Address
Too Few GPS Sat, Minor Alarm	□	☑	□	
Too Few GPS Sat, Minor, Cleared		☑	□	
Too Few GPS Sat, Major Alarm	□	☑	□	
Too Few GPS Sat, Major, Cleared		☑	□	
GPS Antenna Problem	□	☑	□	
GPS Antenna OK		☑	□	
GPS Receiver Fault		□	□	
GPS Receiver Fault Cleared		□	□	

Figure 25: list of available "GPS" related traps/Email alerts (versions 5.0.2 and below)

Description of the available "GPS" Traps and Email alerts:

Too Few GPS Sat, Minor alarm/Too Few GPS Sat, Minor alarm, cleared: Traps/Emails that can be sent if a Minor alarm has been asserted/cleared because the GPS receiver has dropped below a user-defined minimum number of satellites.

Note: The Minimum number of satellites required by SecureSync is tracking four satellites at all times in order to have GPS considered as a valid input reference. However, a user can also define when a Minor alarm is asserted if SecureSync is initially tracking greater than the user-configured minimum number of satellites but then drops below the user-configured minimum number of satellites. The user-defined minimum number of satellites to assert the Minor alarm is configured in the **"Tools**"/"**Notification**" page of the browser and click on the "**Thresholds**" tab.

Too Few GPS Sat, Major alarm/Too Few GPS Sat, Major alarm, cleared: Traps/Emails that can be sent if a Major alarm has been asserted/cleared because the GPS receiver has dropped below the user-defined minimum number of satellites.

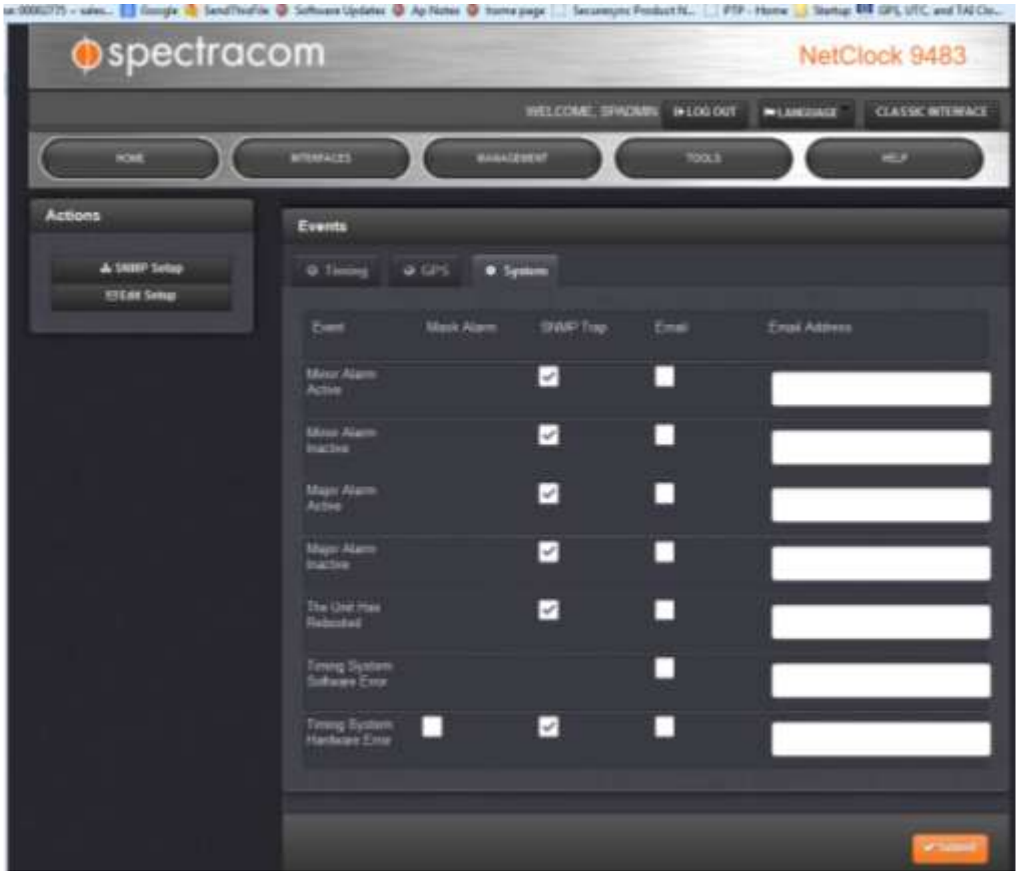
Note: The Minimum number of satellites required by SecureSync is tracking four satellites at all times in order to have GPS considered as a valid input reference. However, a user can also define when a Major alarm is asserted if SecureSync is initially tracking greater than the user-configured minimum number of satellites but then drops below the user-configured minimum number of satellites. The user-defined minimum number of satellites to assert the Major alarm is configured in the **"Tools**"/"**Notification**" page of the browser and click on the "**Thresholds**" tab.

GPS Antenna Problem/GPS Antenna OK: Traps/Emails that can be sent if an open or short has been detected in the GPS antenna cable (or if the GPS antenna is not connected to SecureSync). These conditions will trigger the "GPS Antenna Problem" alert. "GPS Antenna OK" indicates the GPS receiver has detected the GPS antenna is connected to SecureSync and no shorts or opens are being detected in the GPS antenna coax cable.

GPS Receiver Fault Problem/GPS Receiver Fault Cleared: Emails that can be sent if the GPS Receiver Fault alarm is asserted or clears. A GPS Receiver Fault alarm indicates a loss of communication between SecureSync and its GPS receiver (if installed).

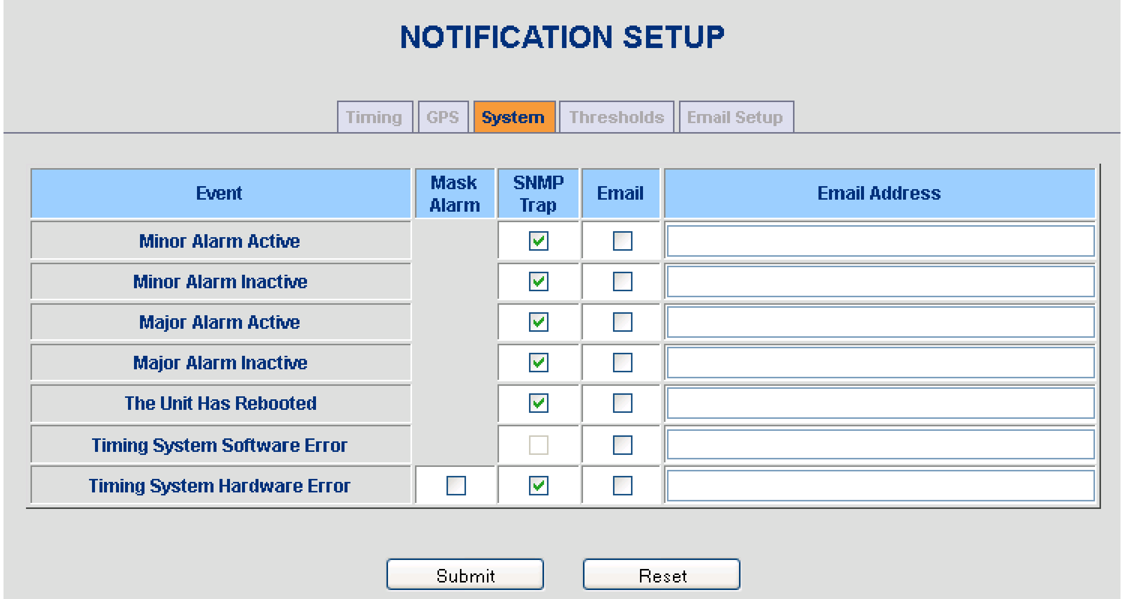
Note there are no SNMP Traps or OIDs associated with these two conditions. However, if the GPS Antenna Problem OID/trap reports "Unknown" state, this also indicates the GPS receiver is not communicating with the SecureSync.

“System” traps/Email alerts



Event	Mask Alarm	SNMP Trap	Email	Email Address
Minor Alarm Active		☑	□	
Minor Alarm Inactive		☑	□	
Major Alarm Active		☑	□	
Major Alarm Inactive		☑	□	
The Unit Has Rebooted		☑	□	
Timing System Software Error			□	
Timing System Hardware Error	□	☑	□	

Figure 26: list of available “System” related traps/Email alerts (versions 5.1.2 and above)



Event	Mask Alarm	SNMP Trap	Email	Email Address
Minor Alarm Active		☑	□	
Minor Alarm Inactive		☑	□	
Major Alarm Active		☑	□	
Major Alarm Inactive		☑	□	
The Unit Has Rebooted		☑	□	
Timing System Software Error		□	□	
Timing System Hardware Error	□	☑	□	

Figure 27: list of available “System” related traps/Email alerts (versions 5.0.2 and below)

Description of the available “System” Traps and Email alerts:

Minor Alarm Active/ Minor Alarm Inactive: Traps/Emails that can be sent each time a Minor alarm is asserted or clears.

Major Alarm Active/ Major Alarm Inactive: Traps/Emails that can be sent each time a Major alarm is asserted or clears.

The Unit Has Rebooted: Trap/Email that can be sent each time SecureSync is rebooted (or power cycled).

***Timing System Software Error:** Emails that can be sent if a Timing System (also referred to as “KTS” or “Kramden Timing System”) software error has been detected or cleared. Note there is no trap/OID associated with this event.

“Timing System Software Errors” are a generic software “or else” condition alarm that is generated if an abnormal/highly unlikely operational event was to occur in the timing system software (KTS) that was not able to be handled by any other specific alarm condition.

***Timing System Hardware Error:** Emails that can be sent if a Timing System (also referred to as “KTS” or “Kramden Timing System”) hardware error has been detected or cleared.

“Timing System Hardware Errors” are a generic software “or else” condition alarm that is generated if an abnormal/highly unlikely operational event was to occur in the timing system hardware (KTS) that was not able to be handled by any other specific alarm condition.

* **Denotes an event that shouldn’t ever occur during normal operation**

Section 14: Verifying SNMPv1/v2c/v3 Trap operation

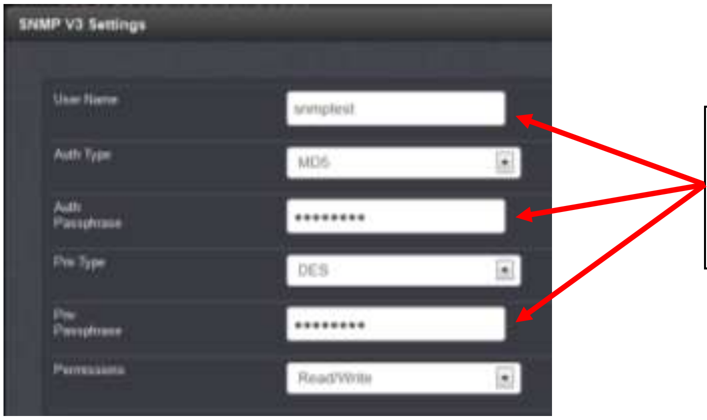
Once SecureSync has been configured with the appropriate settings for the desired SNMP Manager(s) on the network, SNMP has been enabled and with SNMP traps enabled, SecureSync can then start sending SNMP TRAPS to the SNMP Manager(s) when certain conditions (events) occur. If more than one SNMP Manager has been configured in SecureSync, the trap messages will be sent to every SNMP Manager listed (as long as there is network connectivity available to each SNMP Manager).

It may be desired to test SNMP trap generation in order to verify inter-operability with the SNMP Manager. In SecureSync's with software versions 4.5.0 and higher installed (as displayed in the "Archive Version" field of the Tools / Versions page of the browser), SNMP traps can be tested without the need to manually perform events to trigger associated traps.

In order to receive SNMPv3 Notifications (Traps) from the SecureSync, the SNMP Manager needs to support SNMPv3 Traps (not all SNMP Manager programs support Version 3 Traps). If your SNMP Manager software does not support V3 traps (or if it does not appear to be receiving any SNMPv3 traps from a SecureSync, which is properly configured to send SNMP3 traps), an example of a freeware SNMP Manager program that supports SNMPv3 traps is called "**ManageEngine**" software (http://www.manageengine.com/products/mibbrowser-free-tool/download.html).

Below are screenshots and additional information for configuring the "ManageEngine" software for receiving version 3 traps from the SecureSync. Though you may be using other SNMP Manager software from another vendor, this information may also help you configure your SNMP software to be able to receive version 3 traps from the SecureSync (as the SNMP version 3 functionality will be similar across SNMP Managers).

A) Example configured screenshot of the **Management -> SNMP Setup** page, "**SNMP v3**" section of the SecureSync (software versions 5.1.2 and above)



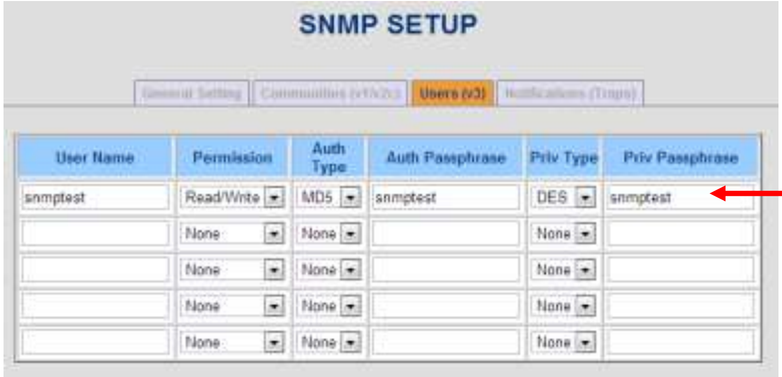
SNMP V3 Settings

User Name	snmptest
Auth Type	MD5
Auth Passphrase	********
Priv Type	DES
Priv Passphrase	********
Permissions	Read/Write

As configured in the SNMP Manager (example being used herein is "**snmptest**")

Figure 28: Create a new SNMPV3 user

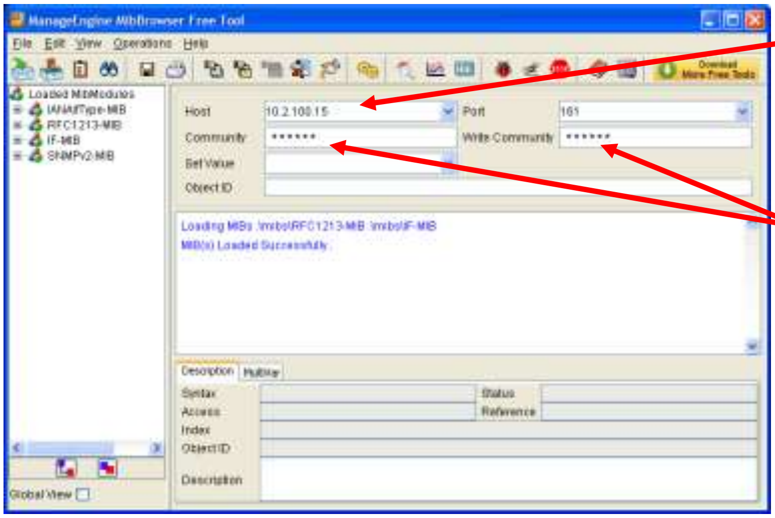
B) Example configured screenshot of the **Network -> SNMP Setup** page, "**Users**" tab in SecureSync (software versions 5.0.2 and below)



User Name	Permission	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
snmptest	Read/Write	MD5	snmptest	DES	snmptest
	None	None		None	
	None	None		None	
	None	None		None	
	None	None		None	

As configured in the SNMP Manager (example being used herein is "**snmptest**")

Main page of the "ManageEngine" software



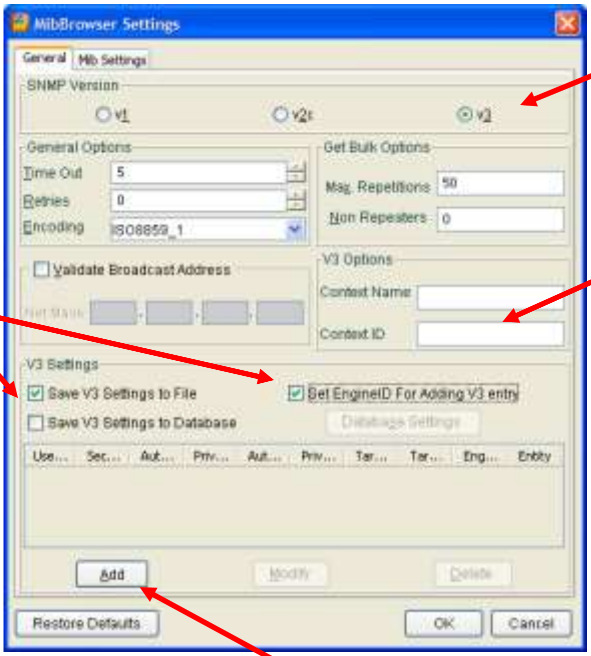
Host: 10.2.100.15
Port: 161
Community: ******
Write Community: ******
Set Value:
Object ID:

Loading MIBs .\mibs\RFC1213-MIB .\mibs\IF-MIB
MIB(s) Loaded Successfully .

Enter IP address of NTP server

As configured in NTP server (in this example both fields are set to "**public**").

Edit -> **Settings** page of the “ManageEngine” software



SNMP Version: ○ v1 ○ v2c ● v3

General Options: Time Out 5; Retries 0; Encoding ISO8859_1

Get Bulk Options: Max Repetitions 50; Non Repeaters 0

□ Validate Broadcast Address

Net Mask

V3 Options: Context Name; Context ID

V3 Settings:

☑ Save V3 Settings to File

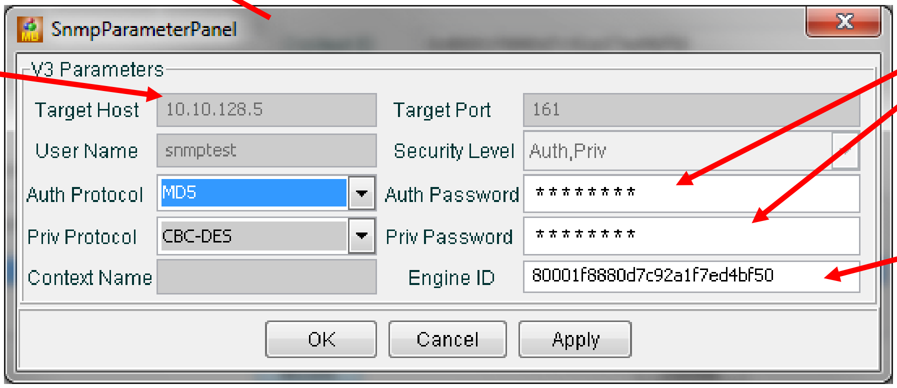
☑ Set EngineID For Adding V3 entry

□ Save V3 Settings to Database

Select “**v3**”

Use the Context ID field as the EngineID field in this software and in the SecureSync’s SNMP configurations.

Select both: “Save v3 settings to File” and “Set EngineID for adding v3



V3 Parameters

Target Host	10.10.128.5	Target Port	161
User Name	snmptest	Security Level	Auth,Priv
Auth Protocol	MD5	Auth Password	********
Priv Protocol	CBC-DES	Priv Password	********
Context Name		Engine ID	80001f8880d7c92a1f7ed4bf50

IP address of the NTP server

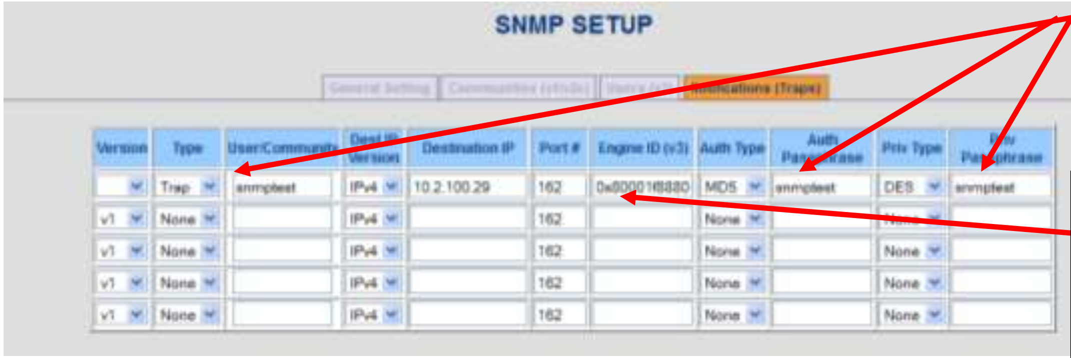
“**snmptest** “ (for example)

Engine ID (copy/paste the Context field) into this field.

Note: The Context ID field in the “General” tab isn’t entered until the “SNMP Parameters” window has been created. Once it’s been created, the “Modify” button will be available. Select “Modify to copy/paste the “Context ID” field into the “Engine ID” field and then hit “Apply”

Screenshot of the **Network -> SNMP Setup** page, “**Users**” tab in the SecureSync

“**snmptest** “ (for example)



SNMP SETUP

Version	Type	User/Community	Dest IP Version	Destination IP	Port #	Engine ID (v3)	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
	Trap	snmptest	IPv4	10.2.100.29	162	0x80001f8880	MD5	snmptest	DES	snmptest
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	
v1	None		IPv4		162		None		None	

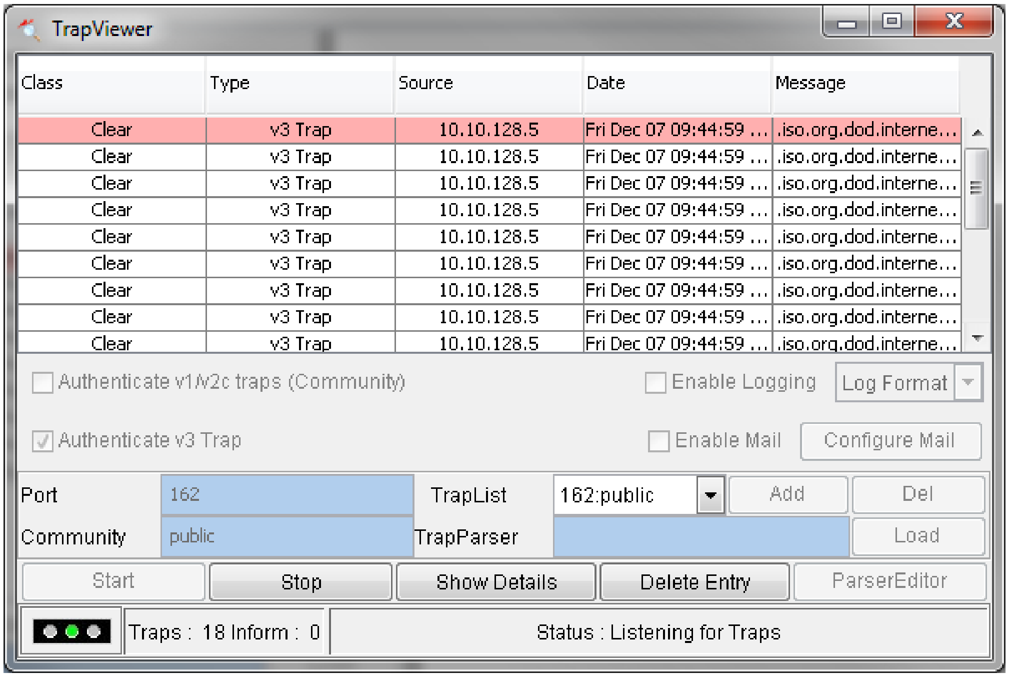
EngineID (copy/paste the Context field here)

Note (Archive software versions 4.8.8 and below): The "Version" field will go to a blank after hitting Submit. This does not affect the SNMP operation. This issue is addressed with Archive software version 4.8.9 (or above) installed.

View -> **Trap Viewer** menu of the "ManageEngine" software

Screenshot of "ManageEngine" **TrapViewer showing SNMP version 3 traps being received**

Examples of SNMPv3 traps that were sent from the SecureSync to the SNMP Manager



TrapViewer

Class	Type	Source	Date	Message
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...
Clear	v3 Trap	10.10.128.5	Fri Dec 07 09:44:59 ...	.iso.org.dod.interne...

□ Authenticate v1/v2c traps (Community)

□ Enable Logging

☑ Authenticate v3 Trap

□ Enable Mail

Port: 162

Community: public

TrapList: 162:public

TrapParser:

Traps : 18 Inform : 0

Status : Listening for Traps

SNMP Notifications in the SecureSync MIB files

All of the available SecureSync notifications are contained in the "**SPECTRACOM-SECURE-SYNC-MIB.mib**" file. Refer to "**ssEventsV2 [enterprises.18837.3.2.3.x]**" for the list of all available notifications.

- Refer to Section 7A below for more information on testing traps (notifications) with software versions 4.5.0 and higher installed.
- Refer to Section 7Bv below for more information on testing traps with a software version prior to version 4.5.0 installed.

Section 7A: Testing SNMP traps in Archive versions 4.5.0 and above

Versions 4.5.0 and above have an available "**testevent**" command that can be issued in the command line interface (CLI) in order to send test SNMP traps. The CLI is accessible via the front panel Serial port, telnet or SSH). Individual notifications can be sent one-by-one or all notifications can be sent simultaneously, as desired.

Note: The "**testevent**" only sends test SNMP Traps (Notifications). It does not send the associated email alerts and the "event" will not be shown in any of the logs.

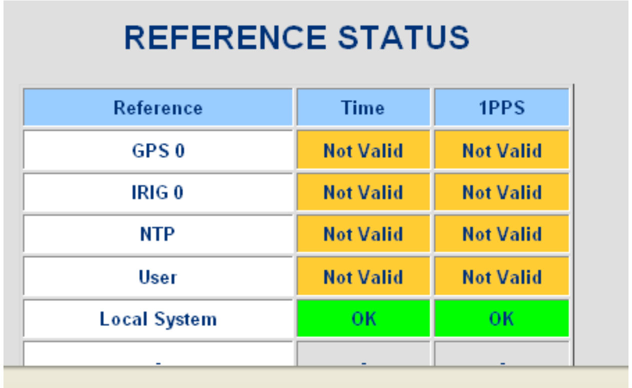
When using the "testevent" command to generate test SNMP traps, the applied event doesn't actually occur. Besides the associated notification(s) being sent, there will no other indication that the event occurred (no new log entries will be asserted, the front panel status LEDs won't change, the web browser status pages will not display the status change, etc).

To test generate notifications, open a CLI connection with the SecureSync's command line interface, using telnet, SSH or via the front panel Serial port. Once the connection has been established, type: testevent <enter> for a list of all available events that can be asserted. To send all available notifications at the same time, type **testevent all** <enter>. Or, to test SNMP traps individually, type: **testevent**, followed by the number of the desired SNMP trap to test (such as testevent 2 <enter> in order to send the Holdover trap).

Section 7B: Testing SNMP traps/Email alerts in versions prior to version 4.5.0

To verify SNMP trap operation and/or email alerts without affecting Time Sync status of the SecureSync (with loss of Time Sync, other devices will likely ignore the appliance) the best and easiest way to generate a test trap/test email is to momentarily disconnect the GPS antenna from the rear panel of SecureSync. Disconnecting the GPS antenna will generate a "GPS Antenna Problem" alarm. If GPS input is the only available and valid Input Reference, removing the GPS antenna will also cause SecureSync to go into the Holdover mode, as well. To verify if GPS is currently the only valid Input Reference, navigate to the "**Status**" -> "**Time and Frequency**" page of the browser. The "Reference Status" table on this page will indicate "OK" for each input reference that is available and valid, as shown below

Note: In some versions of software, if an input reference is not considered valid, it will be displayed as "Alarm" instead of "Not Valid", as shown in this figure (In this particular example, GPS is not valid so SecureSync is not synced to GPS).



REFERENCE STATUS

Reference	Time	1PPS
GPS 0	Not Valid	Not Valid
IRIG 0	Not Valid	Not Valid
NTP	Not Valid	Not Valid
User	Not Valid	Not Valid
Local System	OK	OK
-	-	-

Figure 29: list of all available input references

If GPS indicates “OK” in both columns and all other listed references indicate either “Alarm” or ‘Not Valid”, GPS is the only current input reference that is available and valid.

Both the GPS Antenna and Holdover alarms are trap/email conditions that are enabled by default. To verify both of these traps are still enabled, go to the “T**o**ols” -> “**Notification Setup**” page of the browser and click on the “GPS” tab. Verify the following Events have “SNMP” and or “Email” selected (as desired).

“GPS Antenna Problem”
“GPS Antenna OK”
“In Holdover”
“No Longer In Holdover”

With GPS being the only input reference connected to SecureSync, temporarily disconnect the GPS antenna from SecureSync. Once the GPS antenna has been disconnected, the unit will stop tracking satellites and will go into the Holdover mode. This test will cause SecureSync to send both a “GPS Antenna Problem” trap and a “In Holdover” trap to the SNMP Manager(s) as configured in the Notifications (Traps)” tab on the “**Network**” -> “**SNMP Setup**” page of the browser. If these traps are received by the Manager(s), SNMP trap operation has been successfully configured in the SecureSync appliance.

After reconnecting the GPS antenna, the Antenna problem alarm will clear and SecureSync will exit the Holdover mode. These will cause additional SNMP traps to be sent. If “Email” has also been enabled for these events, an email will be automatically sent to the email address listed in the “Email address” field for each of these Events.

Testing other SNMP trap generation (not already previously tested)

TESTING THE AUTHENTICATION TRAP

When the generic Authentication trap is enabled, a trap will be sent to the configured SNMP Manager(s) each time a user enters an invalid password when trying to login to SecureSync (unsuccessful login).

To test this trap, after enabling it in the “**General Settings**” tab of the “**Network**” -> “**SNMP Setup**” page of the browser (note that this trap is disabled by default), open the web browser, but enter an incorrect login password, such as just the word “admin” (instead of the default password of “admin123, for example). This condition will assert an Authentication failure entry in the “Authentication” log (as viewed in the “**Tools” -> “Logs”** page of the browser) and because the trap is enabled, an Authentication trap will also be sent.

TESTING THE TIMING TRAPS

In Sync/Not In Sync: "Not in Sync" occurs if the Holdover period expires with no valid input references becoming present again before the holdover period expires. It also occurs at power-up.

To test this trap, power cycle SecureSync. The Time Sync alarm/trap will occur shortly after power-up. "In Sync" occurs when at least one input reference is declared valid. With the GPS antenna connected and able to track satellites, SecureSync will go back into sync a few minutes after power-up.

Besides power cycling SecureSync, these traps can also be tested by temporarily disconnecting all input references (such as GPS) and waiting for the Holdover period to expire. With this method, it may be desired to temporarily shorten the Holdover period to shorten the length of time before this alarm is asserted. The Holdover period (configured in number of seconds of Holdover) is configured in the "Holdover Timeout" field located in the "**Setup**" -> "**Disciplining**" page of the browser. The minimum Holdover period is one second(one second after all input references have been removed or classified as not valid, SecureSync will go out of Sync).

Reconnect at least one input reference (such as GPS) and shortly thereafter, SecureSync should be tracking at least four satellites. It will then be back in Sync and the "In Sync" condition will be triggered.

Frequency Error/ Frequency Error Cleared: "Frequency Error" occurs if a large oscillator output frequency error has been measured. It also occurs at SecureSync power-up.

To test this trap, power cycle (or reboot) SecureSync. SecureSync can be remotely rebooted via the "**Tools" -> "Reboot/Halt**" page of the browser.

The "Frequency Error" condition will occur shortly after power-up.

With GPS (or other input reference) present and considered valid, a short time later the Frequency Error condition should clear, triggering the "Frequency Error cleared" condition.

Self reference only/Reference Other than Self: Traps/Emails that are reserved for future use. These reserved traps will not be generated in SecureSync.

1PPS Not In Specification/1PPS Restored To Specification:

Traps/Emails that can be sent each time the Maximum TFOM value has been exceeded (The Maximum TFOM value is configured in the Setup/disciplining page of the browser) and then also when TFOM has returned to being a value less than the Max TFOM value.

To test this trap, with SecureSync connected and synced to GPS, in the Setup/ Disciplining page of the web browser, change the Maximum TFOM value to a value of "1". As the expected TFOM values with GPS present are typically in the 3-4 value range, setting the Maximum TFOM value to 1 will trigger this condition as soon as the TFOM is measured as a value of 2 or higher (TFOM with a SecureSync housing a Rubidium oscillator is calculated and updated about once-per-second. With an OCXO oscillator installed, the TFOM is recalculated about every 10 seconds). The calculated TFOM should exceed the maximum threshold within just a few seconds.

To test the "1PPS Restored to Specification" condition, reset the Maximum TFOM value to a higher value (such as the default value of 15). Within just a few moments, the calculated TFOM will no longer exceed the Maximum TFOM value and the condition will clear.

Reference Change/Reference Change Cleared: "Reference Change" Trap/ Email can be sent each time SecureSync switches to a different available Input Reference.

"Reference Change Cleared" is a condition/trap reserved for future used. This condition cannot be generated.

To test the "Reference Change" trap/email condition, it will be necessary for SecureSync to have two different valid inputs. Removing the higher priority reference (as defined in the "Reference Priority Setup" table) will cause SecureSync to switch to the next lower priority input reference.

Depending on the configuration of SecureSync and its installed Option Cards, available SecureSync input reference include (but are not limited to) GPS, IRIG, ASCII data and manually setting the time.

If GPS is the only available external reference, use "manually set time" as the second lower-priority input. If the Reference Priority table has not yet been configured to be able to manually set the time, go to the "**Setup**" -> "**Reference Priority**" page of the browser. In the Reference Priority Setup table, see if an Index exists with both the "Time" and "1PPS" columns indicate "User". If not, add a new entry to this table.

In the "Add Entry" table, Enable a "Priority 2" entry that uses "Host" for both references and also select the "Add" checkbox. Press Submit and a new entry will be located in the table (verify the GPS/GPS" index indicates this index is Priority 1.

To manually set the time, go to the "**Setup**" -> "**Time Management**" page and just press the Submit button (you can first manually change the Date and Time first, if desired). Next, go to the "**Status" -> "Time and Frequency**" page and in the Reference Status table, make sure both User and GPS both indicate "OK".

Now, disconnect the GPS antenna cable from SecureSync. Moments later, the GPS receiver will drop to tracking 0 satellites and because the GPS will no longer be valid, it will switch to the user set time as its input reference. This condition will cause a "Reference Change" entry to be added to the Event log and will also trigger an SNMP trap to be sent.

Oscillator Alarm/Oscillator Alarm Cleared: Traps/Emails that can be sent if an Oscillator alarm occurs and when this alarm clears (Oscillator alarm indicates a large frequency error has been detected).

These traps cannot be simulated for test purposes.

TESTING THE GPS TRAPS

Too Few GPS Sat, Minor alarm/ Too Few GPS Sat, Minor alarm, cleared: Traps/Emails that can be sent if a Minor alarm has been asserted/cleared because the GPS receiver has dropped below the minimum number of satellites specified by a user .

To test this trap, navigate to the **"Tools**"/"**Notification**" page of the browser and click on the "**Thresholds**" tab. Under "Minor Alarm Threshold" set the Minimum Satellites field to a value of

"3" (Leave the Duration field set to "0)". With SecureSync tracking at least four satellites, as reported on the Status/Inputs/GPS page of the browser, disconnect the GPS antenna cable from SecureSync. This will cause the GPS receiver to suddenly drop to tracking 0 satellites, thereby triggering this trap to occur.

Too Few GPS Sat, Major alarm/ Too Few GPS Sat, Major alarm, cleared: Traps/Emails that can be sent if a Major alarm has been asserted/cleared because the GPS receiver has dropped below the minimum number of satellites specified by a user.

To test this trap, navigate to the **"Tools**"/"**Notification**" page of the browser and click on the "**Thresholds**" tab. Under "Major Alarm Threshold" set the Minimum Satellites field to a value of "3" (Leave the Duration field set to "0"). With SecureSync tracking at least four satellites, as reported on the Status/Inputs/GPS page of the browser, disconnect the GPS antenna cable from SecureSync. This will cause the GPS receiver to suddenly drop to tracking 0 satellites, thereby triggering this trap to occur.

GPS Receiver Fault Problem/ GPS Receiver Fault Cleared: Traps/Emails that can be sent if the GPS Receiver Fault alarm is asserted or clears. A GPS Receiver Fault alarm indicates a loss of communication between SecureSync and its GPS receiver (if installed).

These traps can only be generated by powering down SecureSync, removing the top cover and then removing the GPS receiver daughterboard from the motherboard. Then power it back-up. Because there will be a loss of communication with the GPS receiver, this condition will cause the alarm/trap to be asserted. Reinstalling the GPS receiver board will clear this condition.

Because the GPS receiver board needs to be removed to generate this trap, we do not recommend testing this trap.

TESTING THE SYSTEM TRAPS

Minor Alarm Active/ Minor Alarm Inactive: Traps/Emails that can be sent each time a Minor alarm is asserted or when it clears (as indicated in the "Alarms" log located on the "**Tools**" -> "**Log**" page of the browser).

To test these two traps, with the GPS antenna initially connected to SecureSync (so that SecureSync is tracking at least four satellites) verify the front panel Sync light is solid green and the front panel Fault light is not lit. Then, disconnect the GPS antenna cable from SecureSync. This will cause the "Antenna Problem" alarm (which is classified as a Minor alarm condition) to trigger the "Minor Alarm Active" trap.

Next, reconnect the GPS antenna cable to SecureSync. This will clear the "GPS Antenna Problem" alarm and the associated Minor alarm, triggering the "Minor Alarm Inactive" trap to occur.

Major Alarm Active/ Major Alarm Inactive: Traps/Emails that can be sent each time a Major alarm is asserted or clears (as indicated in the "Alarms" log located on the "**Tools**" -> "**Log**" page of the browser).

To test these two traps, disconnect the GPS antenna from SecureSync and then power cycle SecureSync. When the unit powers back up, the Time Sync (classified as a Major alarm) is asserted and a trap is sent.

Reconnect the GPS antenna and after a few minutes, SecureSync will go back into Sync, clearing the major alarm and therefore, sending the "major Alarm Inactive" trap.

The Unit Has Rebooted: A trap that can be sent each time SecureSync is rebooted (or power cycled).

To test this trap, reboot the SecureSync. This trap should be sent shortly after SecureSync has powered back up.

Timing System Software Error/ Timing System Software Error (Cleared): Emails that can be sent if a Timing System (also referred to as "KTS" or "Kramden Timing System") error has been detected or cleared. Note there are no SNMP traps or OID numbers associated with these two conditions.

The "Timing System Software Error" and "Timing System Software Error (Cleared)" conditions cannot be simulated for testing purposes.

*__Software Error/ Software Error (Cleared):__ Emails that can be sent if a Software Error has been detected or when it clears.

Software Errors are a "generic bucket alarm" that is generated if an abnormal operational event was to occur in the software but outside of the timing system software (KTS).

"The Software Error" condition cannot be simulated for testing purposes. The Software Error (Cleared)" trap is reserved for future use only. This particular trap will not be generated by SecureSync.

***Unrecognized Option Card/Unrecognized Option Card (Cleared):** Traps/Emails that can be sent if SecureSync detects an Option Card has been installed, but it doesn't recognize this card as one that it is compatible with.

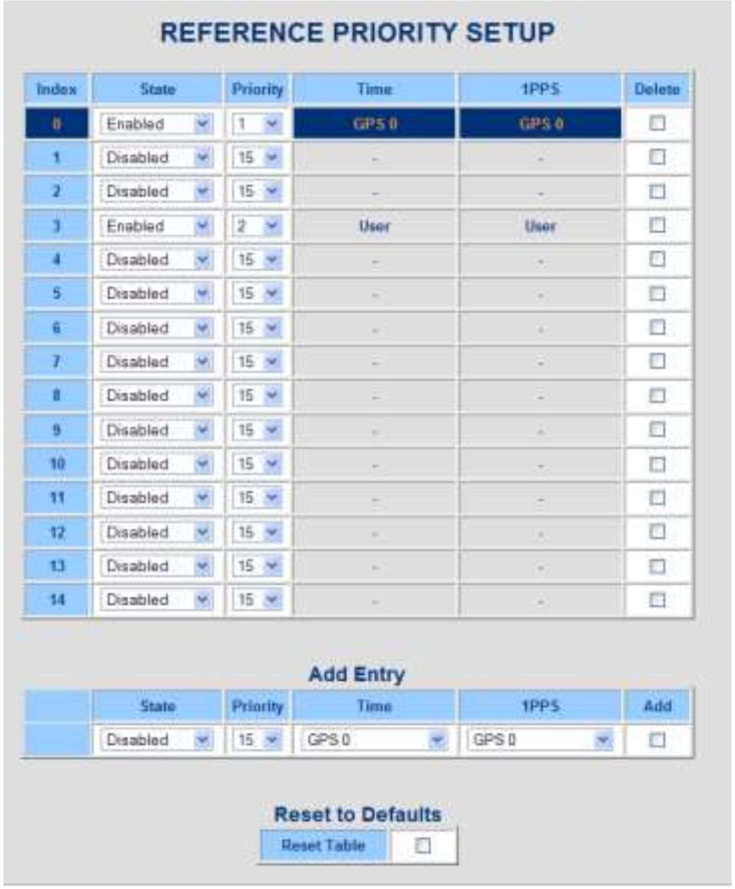
This trap condition can only be tested if an earlier version of software was installed prior to installing a new Option Card that is not compatible with the earlier version of software.

Section 15: Specific SNMP usage examples

A) Configuring the Reference Priority table via SNMP

Starting in Archive software version 4.5.0, the ability to remotely configure the SecureSync's input "Reference Priority Setup" table using SNMP sets (in addition to being able to configure it via the web browser) is available.

The "Reference Priority Setup" table ("**Setup**" -> "**Reference Priority**" page of the SecureSync's web browser) lists all available input references and their associated priorities. This table also allows each input reference to be individually enabled or disabled, as desired. When an input reference (such as GPS, for example) has been disabled, it will no longer be used as an input reference, even if it's present and valid.



REFERENCE PRIORITY SETUP

Index	State	Priority	Time	1PPS	Delete
0	Enabled	1	GPS 0	GPS 0	□
1	Disabled	15	-	-	□
2	Disabled	15	-	-	□
3	Enabled	2	User	User	□
4	Disabled	15	-	-	□
5	Disabled	15	-	-	□
6	Disabled	15	-	-	□
7	Disabled	15	-	-	□
8	Disabled	15	-	-	□
9	Disabled	15	-	-	□
10	Disabled	15	-	-	□
11	Disabled	15	-	-	□
12	Disabled	15	-	-	□
13	Disabled	15	-	-	□
14	Disabled	15	-	-	□

Add Entry

	State	Priority	Time	1PPS	Add
	Disabled	15	GPS 0	GPS 0	□

Reset to Defaults

Reset Table	□

Figure 30: Reference Priority Setup table

The "Enable/Disable" and "Priority" fields of the "Reference Priority Setup" can be configured via the SecureSync's web browser or with SNMP "Sets". The "SPECTRACOM-SECURE-SYNC-MIB.mib" file contains the applicable values for configuring this table via SNMP. Refer to "**ssReferenceMgmtObjs Objects [enterprises.18837.3.2.2.4.x]**" in this MIB file for a list of all of the values associated with this table. Refer to the SecureSync user manual for additional information on the "Reference Priority Setup" table.

Note: SNMP provides the ability to "get" the entire Reference Priority table, but only provides the ability to "set" the "State" field (Enable or Disable input references) and the "Priority" of the reference. SNMP does not allow entries to be added or deleted from the Reference Priority table.

B) Desire to remotely monitor the current TFOM/ETE value (as also reported in the Status -> Time and Frequency page of the web browser, or with the 'tfomget' CLI command) via SNMP

Besides being able to read the current TFOM value reported in the web browser, or with the '**tfomget'** CLI interface command, there are a couple of ways to also remotely monitor the SecureSync's current TFOM value via SNMP.

There is no SNMP trap (or email alert) directly associated with the TFOM value. However, there is an SNMP trap that can be sent to alert to the TFOM exceeding the user-configurable MaxTFOM value. If the TFOM is ever higher than the MaxTFOM value, the "1PPS Not in Specification" alarm is asserted (the alarm clears when TFOM becomes either the same value or lower than the configured MaxTFOM value). This alarm condition has two associated SNMP traps (and/or Email alerts) that can be sent when these alarms occur. These are the "**1PPS Not in Specification**" trap and/or email that is sent when MaxTFOM is exceeded and the "**1PPS Restored to Specification**" trap and/or when TFOM no longer exceeds the MaxTFOM.

These two traps/emails can be enabled or disabled via the **Management** -> **Notifications** page of the newer browser (or the **Tools** -> **Notifications** page of the "Classic Interface" browser), **Timing** tab (they are enabled by default). To generate an email alert, enter an email address in the associated field. If you haven't already configured email alerts, the email configuration for your particular email exchange server is on the same page of the browser, in the **Edit Setup** button.

The current TFOM value can also be read using an SNMP Get. With the MIB files compiled in the SNMP Manager, the SNMP Manager can poll the TFOM value. There may be a way to configure the SNMP Manager to automatically poll the value and alert to the value exceeding a specified value. Refer to '**ssSysStaTfom**' in the SPECTRACOM-SECURESYNC-MIB.mib file.

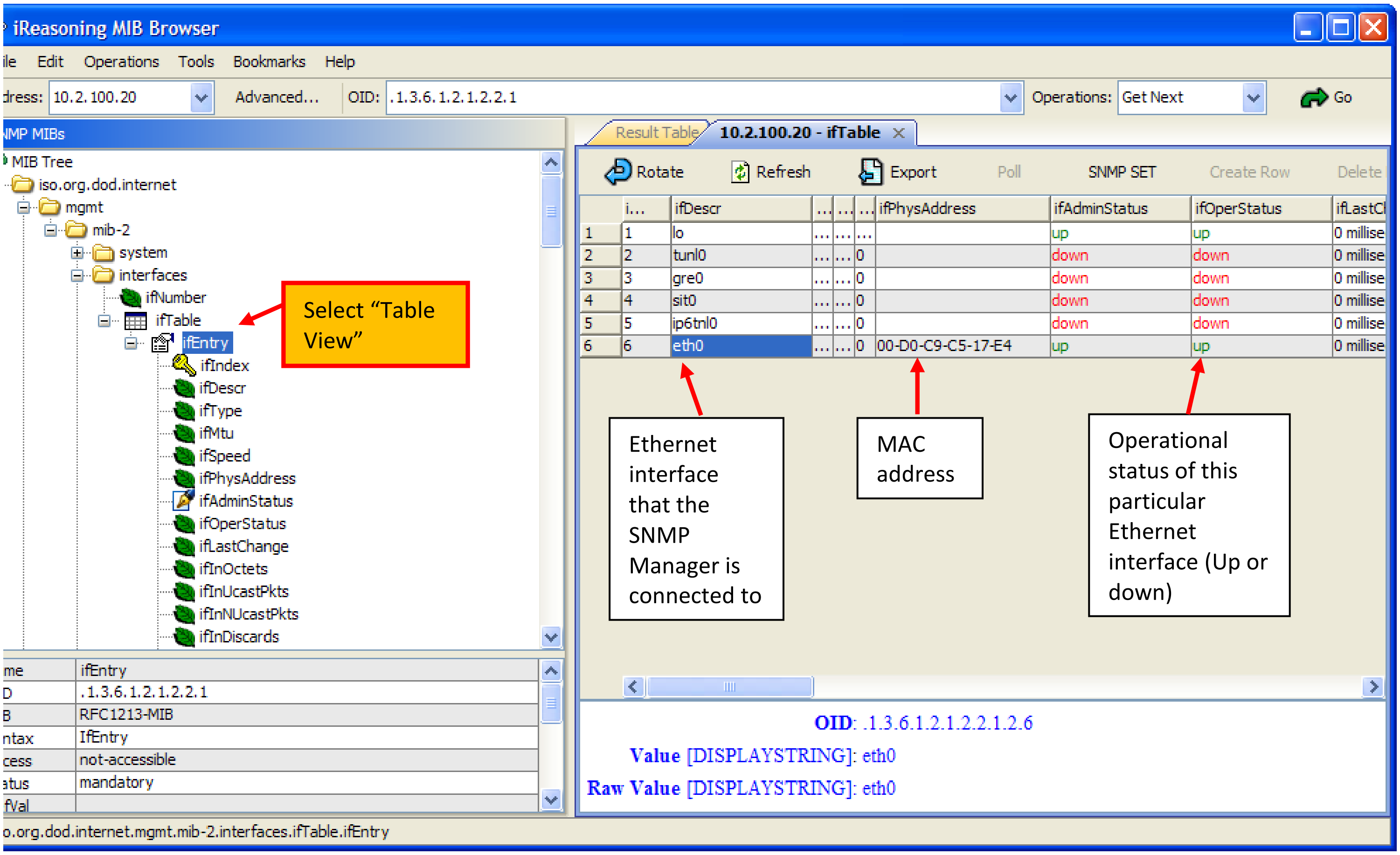
Section 16: RFC 1213 / Desire to remotely monitor SecureSync's network interface status

It may be desired to monitor the status of the Ethernet interface (to determine if the interface is currently up or down). This can be done using SNMP in conjunction with a generic SNMP MIB file not included in the SecureSync, the RFC 1213 MIB file.

SecureSync supports the SNMP Gets (read-only) functionality of the generic RFC 1213 MIB file, which includes the ability to read the current operational status of a network interface. This MIB file can be freely downloaded from websites such as http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=RFC1213-MIB. For more information on this MIB file, refer to RFC 1213 (http://www.ietf.org/rfc/rfc1213.txt).

The RFC 1213 MIB file contains an "**ifTable**" (Interface table). The read-only "ifOperStatus" (Operational Status) field in this table reports if the particular network interface that the SNMP Manager is connected to is currently up or down. Note this interface status is not available as an SNMP trap (if the interface goes down for instance) but the current state can be read using this table. The variables for this field are as follows:

```
        up(1),      -- ready to pass packets
          down(2),
          testing(3),   -- in some test mode
          unknown(4),
          dormant(5)
```



dress: 10.2.100.20 OID: .1.3.6.1.2.1.2.2.1 Operations: Get Next

Select "Table View"

	i...	ifDescr	...	...	...	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastCl
1	1	lo	...	...	...		up	up	0 millise
2	2	tunl0	...	...	0		down	down	0 millise
3	3	gre0	...	...	0		down	down	0 millise
4	4	sit0	...	...	0		down	down	0 millise
5	5	ip6tnl0	...	...	0		down	down	0 millise
6	6	eth0	...	...	0	00-D0-C9-C5-17-E4	up	up	0 millise

Ethernet interface that the SNMP Manager is connected to

MAC address

Operational status of this particular Ethernet interface (Up or down)

me	ifEntry
D	.1.3.6.1.2.1.2.2.1
B	RFC1213-MIB
ntax	IfEntry
cess	not-accessible
atus	mandatory
fVal	

o.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry

OID: .1.3.6.1.2.1.2.2.1.2.6

Value [DISPLAYSTRING]: eth0

Raw Value [DISPLAYSTRING]: eth0

Other values listed in the IfEntry table:

A) **IfSpeed**

Here is a description of ifSpeed:

ifSpeed OBJECT-TYPE
SYNTAX Gauge
ACCESS read-only
STATUS mandatory
DESCRIPTION
"An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth."::= { ifEntry 5 }

"An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and if High Speed must be used to report the interface’s speed. For a sub-layer which has no concept of bandwidth, this object should be zero."

In the SecureSync we do not report bandwidth, so this value is always a “0”.

Section 17: Monitoring NTP

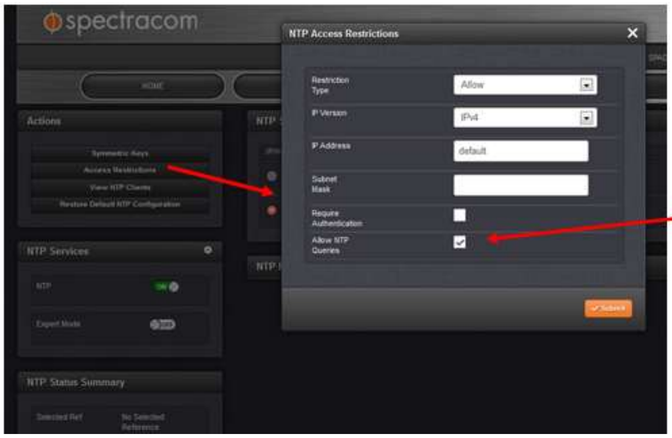
NTP software can also be used for monitoring the NTP performance of the SecureSync(s) on the network.

Here is a link to the NTP website regarding monitoring NTP:
http://support.ntp.org/bin/view/Support/MonitoringAndControllingNTP#Monitoring_NTP

In addition, the Spectracom-supplied NTP MIB file ("SPECTRACOM-NTP-V4-MIB.mib") also provides the ability to monitor NTP. This NTP MIB file, supplied with the other MIB files, provides the ability to poll for NTP sync status and Stratum level. It also provides the ability to monitor configured NTP Peers or Servers. To monitor NTP status using this file, compile it into the SNMP Manager(s) along with the other MIB files.

A) Newer web browser (Software versions 5.1.2 and above)

Note: In order to use NTPQ to monitor NTP, it needs to be enabled in the **Management** ->**NTP Setup** page of the browser (click on **Access Restrictions** on the left side of the page. As shown below, the checkbox for "**Allow NTP queries"** in the **"IP V4"** and/or **"IP V6" rows** (as applicable) needs to be selected (press "Change" on the right side of each row to access the pop-up window and this checkbox).



NTP Access Restrictions

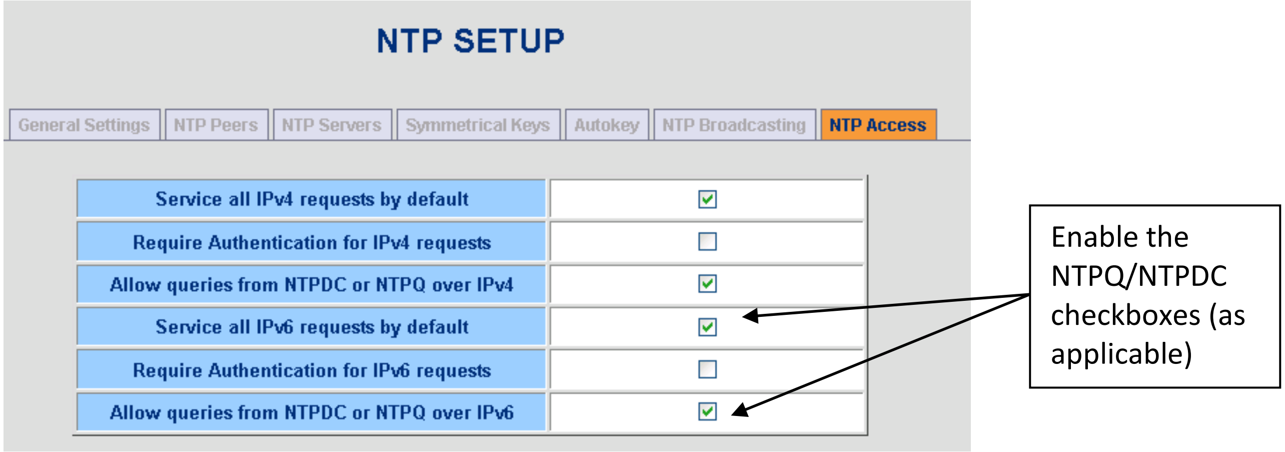
Restriction Type: Allow
IP Version: IPv4
IP Address: default
Subnet Mask:
Require Authentication: □
Allow NTP Queries: ☑

Enable the "Allow NTP Queries" checkbox

Figure 31: "Allow NTP queries" checkbox

B) "Classic Interface" (Software versions 5.0.2 and below)

Note: In order to use NTPQ to monitor NTP, it needs to be enabled in the **Network** ->**NTP Setup** page of the browser, NTP Access tab. As shown below, the checkboxes for "**Allow queries from NTPDC or NTPQ over IPv4**" and/or "**Allow queries from NTPDC or NTPQ over IPv6**" (as applicable) needs to be selected.



NTP SETUP

Service all IPv4 requests by default	☑
Require Authentication for IPv4 requests	□
Allow queries from NTPDC or NTPQ over IPv4	☑
Service all IPv6 requests by default	☑
Require Authentication for IPv6 requests	□
Allow queries from NTPDC or NTPQ over IPv6	☑

Enable the NTPQ/NTPDC checkboxes (as applicable)

Figure 32: “Allow queries” checkboxes

Section 18: SNMP MIB file changes/SecureSync software changes associated with SNMP

Spectracom periodically incorporates changes to SecureSync's SNMP functionality via software update, which may change the supplied SecureSync SNMP MIB files. In order for newer SNMP features to be available for use, the newer versions of the supplied SNMP MIB files need to be loaded into the SNMP Manager(s) on the network.

Below is a list of SNMP changes (latest to earliest) that have been incorporated that affect the SecureSync's SNMP configuration, MIB files or other SNMP functionality:

1) **Version 5.3.0 software update**
   - No changes incorporated with SNMPD or the SNMP MIB files.

2) **Version 5.2.1 software update**

   SNMP Setup page of the web browser
   - Changed the SNMPv1 and v2c Community Name requirements to allow a string of 1 to 31 characters.
   - Editing the **SNMPSysObject ID** field in the SNMP Setup page of the web browser wasn't propagating through to the SNMP operation.

   Other SNMP changes incorporated
   - Enabled several new system level MIBs for obtaining Memory and Disk usage, and well as CPU stats.
   - Added a new OID to be able to get the unit's Serial Number via SNMP
   - Fixed an issue with **ssSysStaEstPhaseError** reporting an erratic value, when the phase value was a negative number.

3) **Version 5.2.0 software update**

   Updated Net-SNMP to a newer version of software.

4) **Version 5.1.7 software update**

   Fixed validation rules for SNMP V1/V2 IP address settings to allow set from returned value of "default" for the IP address.

5) **Version 5.1.5 software update**

   The version 5.1.5 software update now allows the "SysObjID" field in the **Management** -> **SNMP** page of the browser to be edited, as desired.

6) **Version 5.1.4 software update**

   The version 5.1.4 software update fixed a few settings validation issues. This update also resolved an error message being displayed when trying to delete SNMPv1 or v2 access configurations.

7) **Version 5.1.3 software update**

   The version 5.1.3 software update did not incorporate any changes to the MIB files. However, this update incorporated one change associated with SNMP in the SecureSync's internal firmware:

   A) SNMP MIB "1.3.6.1.4.1.18837.3.3.2.1.0", ("NTP_CURRENT_MODE") restored Integers 3 and 4 which were temporarily disabled in version 5.1.2 due to delayed response time for this particular OID. The response time for this OID was able to be increased in this update.

8) **Version 5.1.2 software update**

The version 5.1.2 software update did not incorporate any changes to the MIB files. However, this update incorporated two changes associated with SNMP in the SecureSync's internal firmware:

A) Instead of the "User-defined Major" trap being sent when the User-defined Major alarm was asserted, the standard "Major alarm" trap and associated clear trap were inadvertently being sent.

B) SNMP MIB "1.3.6.1.4.1.18837.3.3.2.1.0", ("NTP_CURRENT_MODE") now reports an integer of either 1 or 2 to avoid sluggish SNMP performance (Integers 3 and 4 are temporarily disabled).

   - Response times for SNMP Gets of this particular MIB were about 6 seconds or so, far longer than all other MIBs (due to how this status information is obtained from NTP). This potentially required SNMP script time-outs to need to be lengthened to account for the delayed responses for this MIB.

9) Version 5.0.0 software update

The version 5.0.0 software update made very minor changes to the MIB files, where a value "number" was being indicated, instead of the corresponding text for that particular value.

This software update also changed the "Auth Passphrases" and "Priv Passphrases" fields (SNMP SETUP page of the browser -> Notifications and Users tabs) to "password" fields so that these values are no longer displayed as clear text.

10) Version 4.8.9 software update

Extended the SNMPv3 "EngineID" field to support more than 32 characters (it now supports up to 50 characters). There were no SNMP MIB file changes incorporated in this software upgrade.

11) Version 4.8.7 software update

The version 4.8.7 software update added the ability to "mask" (override) undesired alarms (via the **Tools** -> **Notifications** page of the browser) such as the Antenna Problem or Frequency alarms, for example. There were no SNMP MIB file changes incorporated in this software upgrade.

12) Version 4.8.6 software update

The version 4.8.6 software update implemented one minor change to just one of the MIB files (the Global MIB file). The Global MIB file was updated to reflect Spectracom address and organizational changes. In most cases, recompiling the MIB file for these minor edits isn't necessary.

13) Version 4.8.2 software update

The version 4.8.2 software update incorporated the ability to read the System Time via SNMP. For more information on this capability, refer to "**ssSysStaDateTime**" in the SPECTRACOM-SECURE-SYNC-MIB.mib file.

14) Version 4.8.0 software update

The 4.8.0 software update added a new reboot trap that can be sent each time the NTP server is rebooted/power cycled.

15) Version 4.5.0 software update

The version 4.5.0 software:

- Added a new mib file to support generic start, restart and shut-down traps.
- Added the ability to configure/control the Input Reference Priority table via SNMP (Refer to section 5 of this document for more information on this change).
- Added the ability to send test traps to the SNMP Manager(s).

- In the “SPECTRACOM-SECURE-SYNC-MIB.mib” file, modified the two integer values for “sync” and “nosync” in “**ssSysStaSyncState**” (Sync status).

16) Version 4.1.0 software update

- Added a web browser Notification page to configure whether each SecureSync event that may occur (such as loss of Time Sync, going into or out of the Holdover mode, etc) will trigger an SNMP trap or an email (or both) to be sent out to a desired email recipient.
- Two SNMP traps were available, the Time Sync trap and the Holdover trap.
- Version 4.1.0 also adds several new available traps, such as a minimum satellites trap, frequency alarm traps, etc. Each SNMP trap can be either selected or de-selected, as desired.

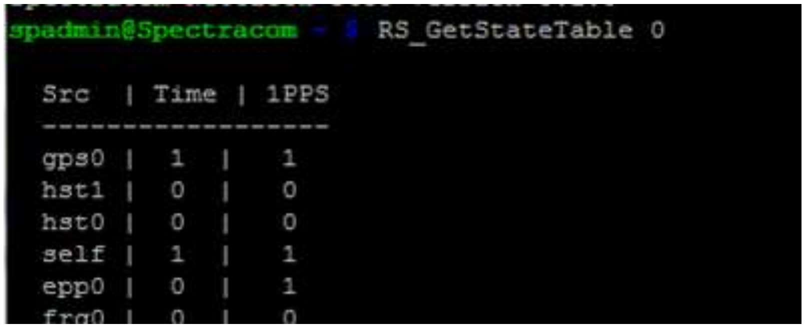
Section 19: Frequently Asked Questions regarding SecureSync SNMP

Input Reference Status/ Reference Status table

Q. Can I query the validity/presence of the individual input references that are listed in the "**Reference Status**" table of the time server's web browser (such as GPS input, havequick input, IRIG input, external 1PPS input, etc)?

A. With the exception of the GPS input reference, the validity/presence of other input references cannot be directly obtained via SNMP. However, at least one Time and 1PPS reference needs to be present/valid in order to prevent the time server from going into Holdover mode. The Holdover (and Sync) status can be queried using SNMP.

Note: Though the Reference Status for all inputs is not available via SNMP, it is available via the web browser or a CLI command. The **RS_GetStateTable 0** command will respond with a table of all references listed in the Reference Priority table and whether or not they are a valid input ("0" indicates not valid and "1" indicates valid. In order for a reference to be selectable, both The Time and 1PPS columns need to be a "1"). An example of this command is shown below:



```
spadmin@Spectracom ~ $ RS_GetStateTable 0

  Src   | Time | 1PPS
  ------------------
  gps0 |  1   |   1
  hst1 |  0   |   0
  hst0 |  0   |   0
  self |  1   |   1
  epp0 |  0   |   1
  frq0 |  0   |   0
```

Q. Is there a way to obtain via SNMP the Signal Strengths of each received GPS satellite?

A. As of at least Archive software version 5.0.2, Signal Strengths for each channel of the GPS receiver are not available via SNMP. The GPS Signal Strengths can only be obtained via the web browser or via a CLI command (**GR_GetSatData 0 0**).

SNMP traps

Q. A few of the SNMP traps listed in SecureSync's web browser are grayed out, not allowing the user to select these specific traps. What are these traps?

A. The SecureSync uses a Spectracom timing system that is shared amongst other Spectracom products (such as the Spectracom TSync-PCIe bus-level timing boards). These traps that are specific to the other Spectracom products won't likely ever be added to SecureSync specifically, because they don't really apply to this product. It is intended to remove these from the web browser in a future software update).

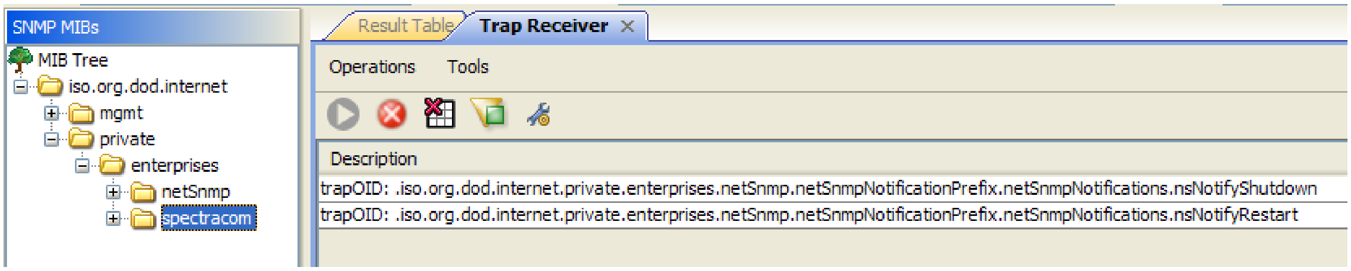
Q. Besides all the traps events listed and checked in the “Tools/Notification” page of the web browser, what other “System” traps (that not listed) will the SecureSync will be sending out to the SNMP Manager?

A. The SNMP traps that are listed in the SecureSync’s web browser are the Spectracom-specific traps. The SNMP daemon (NET-SNMP) in the SecureSync also provides a few “generic” SNMP traps, as well. These generic traps include the authentication trap as well as the “ColdStart trap” and “WarmStart” trap (which occur after each reboot/power cycle of the SecureSync). It also includes the “NotifyRestart” which is generated each time SNMP in SecureSync is restarted.

The SNMP agent also sends SNMP traps when SNMP is either disabled or enabled (restarted) in the SecureSync. From the NTP-SNMP-AGENT-MIB.mib file:

```
nsNotifyStart       NOTIFICATION-TYPE
    STATUS        current
    DESCRIPTION
            "An indication that the agent has started running."
    ::= { netSnmpNotifications 1 }

nsNotifyShutdown    NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
            "An indication that the agent is in the process of being shut down."
    ::= { netSnmpNotifications 2 }

nsNotifyRestart     NOTIFICATION-TYPE
    STATUS        current
    DESCRIPTION
            "An indication that the agent has been restarted.
             This does not imply anything about whether the configuration has
             changed or not (unlike the standard coldStart or warmStart traps)"
        ::= { netSnmpNotifications 3 }
```

Example traps after stopping and restarting SNMP in the SecureSync (showing the SNMP agent was stopped and then restarted):



```
Description
trapOID: .iso.org.dod.internet.private.enterprises.netSnmp.netSnmpNotificationPrefix.netSnmpNotifications.nsNotifyShutdown
trapOID: .iso.org.dod.internet.private.enterprises.netSnmp.netSnmpNotificationPrefix.netSnmpNotifications.nsNotifyRestart
```

MIB Files

Q. Why are there 6 different MIB files for the SecureSync? What is the primary purpose of each of these files?

A. The SNMP functionality in SecureSyncs encompasses a few different primary functions of the SecureSync. Instead of one very large MIB file, the SNMP MIBs files are instead broken down to smaller, individual MIB files. Not all of the files apply to all SecureSyncs, so not all files necessarily need to be compiled onto the network SNMP Managers.

The Spectracom SecureSync MIB files consist of the following six files (the purpose of each MIB is stated at the top of each of the MIB file, but is also stated below for your convenience) As noted below, some of the following MIB files help define information for other MIB files (Not all of the MIB files are stand-alone files. The PTP "Precision Time Protocol" MIB file is an example of a stand-alone MB file. The NET-SNMP files are an example of files that work together to provide a SecureSync function).

Note: The two NTP-SNTP files (NET-SNMP-AGENT-MIB.mib and NET-SNMP-MIB.mib) are common, generic MIB files that may not needed to be compiled into the SNMP Manager. These files may already be pre-compiled into the SNMP Manager software. If they are, they don't need to be loaded again.

1) SPECTRACOM-NTP-V4-MIB.mib
This MIB defines the NTPv4 MIB for the private Spectracom MIB.

2) SPECTRACOM-PTP-V4-MIB.mib
This MIB defines the PTP MIB for the private Spectracom MIB (This MIB file is only applicable if the available SecureSync PTP Option Card, Model 1204-12) is installed.

3) SPECTRACOM-SECURE-SYNC-MIB.mib
This MIB defines the SecureSync product module for the private Spectracom MIB.

4) NET-SNMP-AGENT-MIB.mib
This MIB defines control and monitoring structures for the Net-SNMP agent.

5) NET-SNMP-MIB.mib
Top-level infrastructure of the Net-SNMP project enterprise MIB tree

6) SPECTRACOM-GLOBAL-MIB.mib
This MIB defines the global registration module for the private Spectracom MIB (defines the product is a Spectracom SecureSync and not a Model 9383 NetClock, for example).

SNMP Manager

Q. If the SNMP manager happens to be down during a SecureSync event and then back up again during this event, how does it catch the current alarm condition of the SecureSync?

A. The SecureSync only sends a trap once when an event initially occurs (and in most cases, once when the event clears – some events, like the "Reference Change" trap don't have a clear trap associated with that particular event so only one trap is generated). Likely similar with most other SNMP-capable devices, if an SNMP Manager happens to be down while an event initially occurs, that particular SNMP Manager will not be aware it's in that state.

For this reason, SecureSync supports the ability to send the SNMP traps to up to five different SNMP Managers on the network. If one SNMP Manager happens to be down, four other Managers are also capable of receiving the same traps that the down SNMP Manager would have received, if it had been operational, when the event trap was sent from the SecureSync.

Section 20: Spectracom Technical 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

UK www.spectracom.co.uk | techsupport@spectracom.co.uk |
6A Beechwood | Chineham Park | Basingstoke, Hampshire, RG24 8WA |
44 (0)1256 303630