

SecureSync NTP Peering Tech Note

This document contains supplemental information regarding the NTP Peer and Server modes of operation for the Spectracom SecureSync.

Section 1: Description of NTP Peering	2
Section 2: Configuring a SecureSync with either NTP Peers or NTP Servers (such as Internet Time servers)	4
Configuring the Default Port and Default Gateway address be able to sync to NTP time servers not on an immediate subnet.	6
Section 2A: NTP Peer/Server mode configuration “Use Case” examples:	22
Section 3: NTP Stratum Level reported to the network clients	40
Section 4: NTP Input and Output Status	42
A) NTP Input Status	42
B) NTP Output Status	44
Section 5: System’s 1PPS/on-time point and internal 10 MHz Oscillator disciplining when syncing via NTP input	52
Section 6: Troubleshooting	53
Spectracom Technical Support	62

Section 1: Description of NTP Peering

The Spectracom SecureSync contains two available modes of operation for synchronizing the SecureSync with other NTP servers on the same network. These two modes are called “NTP Peer” (Also called “Symmetric Active” mode) and “NTP Server” (Also called “Symmetric Passive” mode). The two modes are somewhat similar and are described herein.

These two modes of NTP operation allow other NTP time servers on the same network as the Spectracom SecureSync to be “Time” and “PPS input references for the SecureSync to synchronize with. The SecureSyncs have the ability to be “Peered” to other SecureSyncs as well as to other Spectracom Model 9200 and 9300 series time servers (or other NTP Time servers) available on the same network (NTP servers on separate/isolated networks can’t be “peered” together).

The other NTP servers desired to be a time reference to the SecureSync must be reachable on the network and must also support NTP peering capability. With NTP peering, one NTP server is pointed to the IP address (or host name) of other NTP servers for its NTP time reference. NTP Peer mode can be used as a back-up to the primary reference input(s) of GPS, IRIG input, ASCII data input, etc for NTP synchronization. Or, if GPS, IRIG input, ASCII data input, etc is unavailable or not valid, NTP Peering can also be the primary input for NTP synchronization to allow an NTP server to be a dedicated Stratum 2 time server, for example.

Note: The earlier (discontinued) Spectracom Model 9100 series NTP servers do not support NTP peering. So the SecureSync cannot be peered to a Model 9100 series NTP server and vice-versa. Windows PCs are not NTP servers either, so these NTP servers can’t be peered with Windows PCs and vice-versa.

Below is a description of the “Symmetric active” (NTP Peer) and the “Symmetric Passive” (NTP Server) modes.

In summary of the two modes:

NTP Peer mode (“Symmetric Active”) can be considered a *push-pull* mode of NTP operation whereas SecureSync can either *pull* time from any other NTP server that is configured to be an NTP Peer with it OR it can also *push* time out to any other NTP server that is configured in its internal list of NTP Peers with its IP address or its host name (The NTP time servers that it can either push NTP time to or pull NTP time from are configured in the NTP Peers tab of the Network/NTP Setup page of the browser).

NTP Peer Mode is typically used among:

Groups of NTP time servers located on the same network that all normally have other external and accurate references connected (such as GPS, IRIG or ASCII timecode, for example). But, in case the SecureSync was to lose all its available accurate inputs, it's desired for this SecureSync to be able to pull time from another SecureSync in the group of other accurately synchronized NTP time server for it to continue providing NTP time to its clients. And, if another NTP server in the group was to lose its references, it's also desired for this SecureSync to provide time to the other NTP servers, so it can continue to provide time to its clients. Each Stratum 1 server is listed in each other's list of available NTP Peers.

NTP Server mode (“Symmetric Passive”) can be considered a *pull* mode only of NTP whereas SecureSync can only *pull* time from any its other NTP servers that are configured to be an NTP Peer with it BUT it cannot *push* time out to any other NTP server. This mode indicates single direction synchronization only. (The NTP time servers that it can pull NTP time from are configured in the NTP Servers tab of the “Network / NTP Setup” page of the browser).

NTP Server Mode is typically used when:

SecureSync will have no other external and accurate reference connected (such as GPS, IRIG or ASCII timecode) besides other NTP Servers, so it's only selected input reference will be one of the other listed NTP servers that is residing on the same network as SecureSync (It's desired for SecureSync to receive time from an Internet time server. SecureSync can get time from an Internet time server, but an Internet Time server will not get time from the SecureSync).

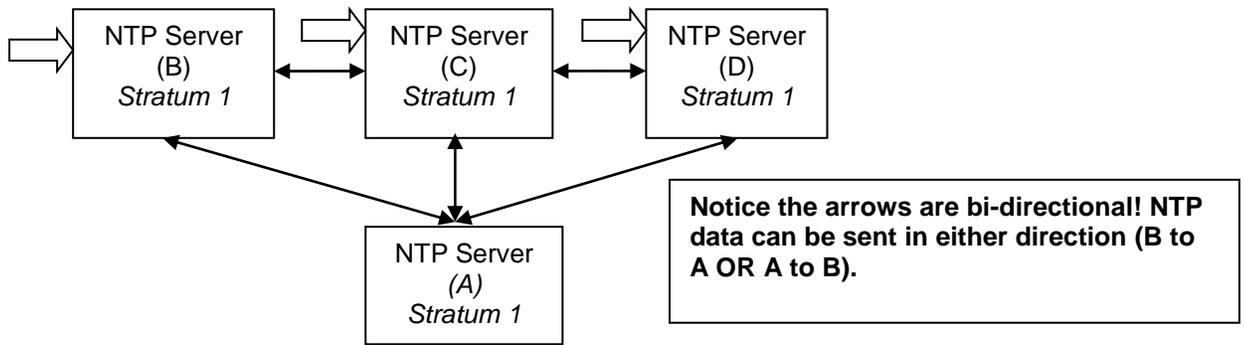
Note: In order for SecureSync to be able to sync to an Internet time server, SecureSync has to have access to the Internet from its network and port 123 must remain open to the Internet at all times.

The following is a more in-depth description of the two modes of NTP operation.

NTP Peer (“Symmetric Active”) mode:

In the NTP Peer mode (“Symmetric Active”) one NTP time server (A) can obtain time from one or more other NTP time servers (B, C, D, etc) that are at the same Stratum level (A) is at. And the other NTP servers (B, C, D, etc) in return can also obtain time from (A). Symmetric Active mode is used with a group of same Stratum level NTP servers to ensure all can have an NTP time reference available.

In the NTP Peer mode, the SecureSync is typically a Stratum 1 server, synced to one or more primary reference inputs (such as such as GPS, IRIG or ASCII time code). However, if all of its references are lost, SecureSync will then sync to one of its peers and will drop to one less Stratum than its peers (Typically, it will become a Stratum 2 NTP server).



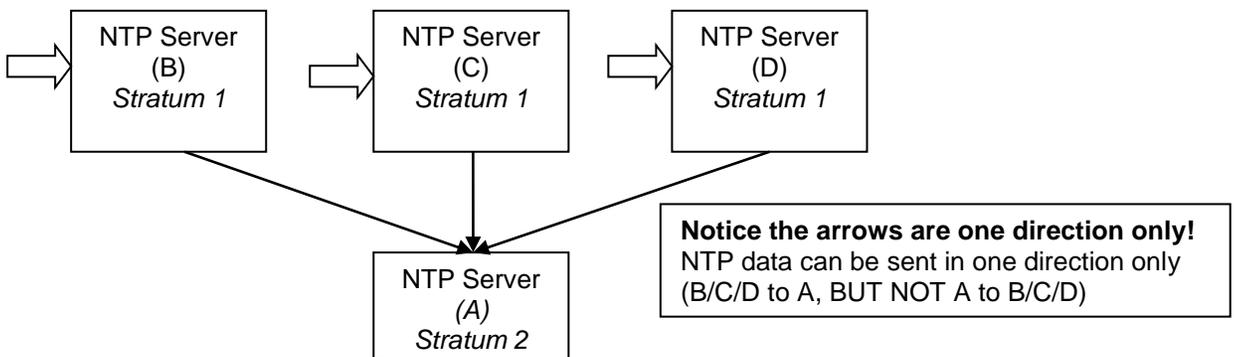
⇒ (= Primary input reference available, such as GPS, IRIG or ASCII time code for Stratum 1 synchronization)

Figure 1: “NTP Symmetric Active” mode of operation

NTP Server (“Symmetric Passive”) mode:

In NTP Server mode (“Symmetric Passive”), the main difference is the NTP server (A) can get time other NTP time servers (B, C, D, etc), but (A) can’t be a reference to any other NTP Time Server (B, C, D, etc). NTP Server mode is typically used when it is desired to have the time server (A) at a lower Stratum (like Stratum 2) than the ones that it is getting time from (B, C, D, etc) which are typically Stratum 1 time servers. It is also used when using Internet NTP time servers as a time reference to (A). In NTP Server mode, (B, C, D, etc) are Stratum 1 time servers and (A) is desired to be a Stratum 2 time server instead of a Stratum 1 server. Because an Internet NTP time server won’t ever reference SecureSync for its time, the Internet time server is configured as an NTP Server instead of as an NTP Peer.

In the NTP Server mode, the SecureSync is typically a Stratum 2 server, synced only to one or more other Stratum 1 NTP servers on the same network.



⇒ (= Primary input reference available, such as GPS, IRIG or ASCII time code for Stratum 1 synchronization)

Figure 2: “NTP Server” mode of operation

In both Symmetric Active and Symmetric Passive modes, the NTP Service in the time server obtains the time data from other NTP servers by configuring it in the Network/ NTP Setup page of the web browser with the IP address/host name of the other available NTP time server(s).

Refer to [Section 3](#) for information on reported Stratum levels when using NTP peering.

Section 2: Configuring a SecureSync with either NTP Peers or NTP Servers (such as Internet Time servers)

Important note: NTP peering is not intended/recommended to be used with SecureSyncs in simulcast radio applications. Please contact Tech Support for more information.

Note: Archive software update version 5.1.2 implemented a new design of the web browser interface. This document provides information for both the “classic interface” (white background) applicable to Archive software versions 5.0.2 and below, as well as the newer design (black/charcoal background) in versions 5.1.2 or higher.

If you aren’t sure what version of software is currently installed:

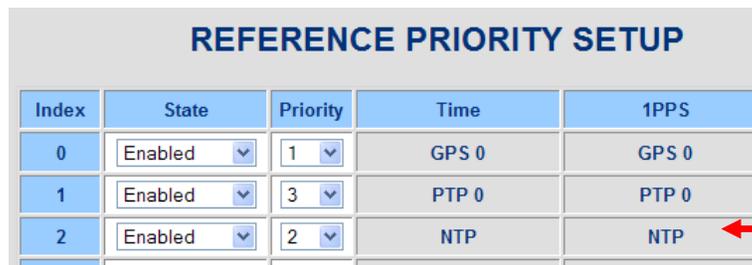
- In software versions 5.1.2 and above, it’s the “**System**” version reported near the top of the **Tools -> Upgrade/Backup** page of the browser (under “System Configuration”).
- In software versions 5.0.2 and below, it’s the “**Archive**” version reported near the top of the **Tools -> Versions** page of the browser (under “System Version”).

With SecureSyncs, other NTP time servers can be a primary time reference for SecureSync. As configured in the “**Reference Priority Setup**” table located in the **Management -> Reference Priority** page (or the “classic interface” browser – located in the **Setup -> Reference Priority** page) “NTP” needs to be listed and enabled as both an input “Time” and “1PPS” reference (as shown below). With NTP/NTP enabled, if another NTP server is the only available time reference connected, or if no other higher priority inputs are currently present and valid, the selected NTP peer will be the selected primary time reference for all SecureSync outputs.



Priority	Time	1PPS	Enabled
1	GPS 0	GPS 0	<input checked="" type="checkbox"/>
2	NTP 1	NTP 1	<input checked="" type="checkbox"/>
3	User 0	User 0	<input checked="" type="checkbox"/>

Figure 3: Reference Priority table (Versions 5.1.2 and above)



Index	State	Priority	Time	1PPS
0	Enabled	1	GPS 0	GPS 0
1	Enabled	3	PTP 0	PTP 0
2	Enabled	2	NTP	NTP

Figure 4: Reference Priority table (Versions 5.0.2 and below)

Adding either an NTP Peer or NTP Server to SecureSync is the same process, with the exception of which table the NTP reference is added to in the NTP setup page. Whether to add another NTP server as a Peer or as a Server is a decision that is made, based on whether it's desired for this SecureSync to be able to provide NTP time data to other NTP servers. It's also dependent on whether the other reference NTP servers(s) are internet time servers.

Note about firewall ports: In any of the following scenarios, network **NTP port 123** needs to be continuously left open on any firewalls between the NTP servers, in order for one NTP server to be able to get time from another NTP server.

- A) If this SecureSync normally has an accurate external input (such as GPS, IRIG or ASCII time code) it is likely to be a good reference for the network and therefore should be considered as an NTP peer in this unit as well as others in a similar input configuration. In this case, list its other available NTP references in the NTP Peers table and include this SecureSync in the NTP Peers configuration of the other NTP servers in a similar input configuration. This is the "push-pull" configuration.
- B) However, if this SecureSync is normally synchronized to only other NTP servers (such as it being a dedicated Stratum 2 time server, for example) it's likely not desired for it to be a time reference to any other NTP servers. In this case, list its references in the NTP Servers table instead and do not add this SecureSync to the Peers table of other NTP servers. If desired, this SecureSync can still be added to the NTP Servers table as a reference to other NTP servers. In this particular configuration, other NTP servers that get time from this one will be no higher than Stratum 3. This is the "pull" configuration.
- C) When syncing the NTP server to Internet time server(s), the Internet time servers are configured as "NTP Servers" (not as "NTP Peers"). This is also the "pull" configuration.

Notes about using Internet Time Servers for input synchronization

- 1) If you wish to use one or more Internet time servers as a time reference to the NTP time server, refer to sites such as <http://tf.nist.gov/tf-cgi/servers.cgi> or <http://support.ntp.org/bin/view/Servers/StratumOneTimeServer> for lists of IP addresses/Host names of available Internet NTP Time Servers.

Many countries provide NTP servers for use. Examples of "local" NTP servers may include:

- A) **nets.org.sg** located in **Singapore** (refer to http://www.singaporestandardtime.org.sg/nets_home.htm)
- B) **ntp.nict.jp** located in **Japan** (refer to <http://www2.nict.go.jp/w/w114/tsp/PubNtp/index-e.html>).

Restrictions on use of free Internet NTP servers: Be aware that some free Internet time servers have special rules/restrictions on their use, such as:

- A) How often NTP clients can query/poll them (a factor of the server's minpoll interval, as configured in the **Management -> NTP Setup** page of the browser) the minpoll interval for that particular NTP server may need to be increased to prevent the SecureSync from polling it too often.
- B) Limitations on what geographical areas are allowed to use this particular NTP server.

Refer to the applicable websites for the NTP servers to see if they have any restrictions in place for their use.

- 2) Decreasing the number of network hops between the NTP server and the Internet time servers will improve the NTP performance. Select NTP servers that are near your region for optimum NTP performance.
- 3) The network that SecureSync is connected to must have continuous **UDP port 123** access to the Internet to use an Internet NTP Time Server as a time reference. This may require UDP port 123 currently closed on any firewall(s) to the Internet be opened.

Configuring SecureSync with an NTP Peer is performed in the web browser for the NTP server. As shown below, the Peers and Servers tables are accessed via the **Management** -> **NTP Setup** page of the browser, then clicking on the “+” sign in the applicable “**NTP Peers**” or “**NTP Servers**” section (or in the classic web browser, the **Network** -> **NTP Setup** page of the browser, in the applicable “**NTP Peers**” or “**NTP Servers**” tabs).

Note: Adding either an NTP Peer or NTP Server is the same process, with the exception of which table the NTP reference is added to in the NTP Setup page.

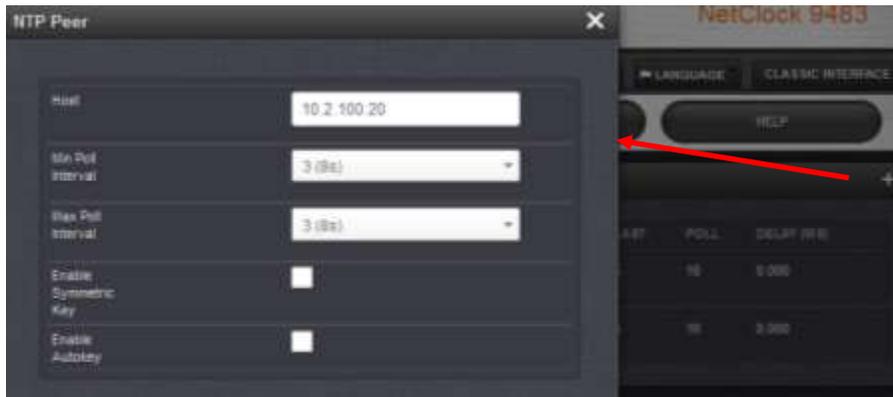


Figure 5: NTP Peers configuration (versions 5.1.2 and below)



Figure 6: NTP Peers configuration (versions 5.0.2 and below)

Configuring the Default Port and Default Gateway address be able to sync to NTP time servers not on an immediate subnet.

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 sync the SecureSync to other NTP time servers not on an immediate subnet of the SecureSync (not directly connected). As the NTP time stamps to sync to the Internet time servers are originating from within the SecureSync, the route for the time stamps to take in order to reach the Internet time server(s) needs to be defined, via the Default 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 Internet also needs to be selected (known as the “Default Port”).

If NTP packets aren’t able to reach an NTP Peer/Server after initially starting up NTP (such as default gateway configuration or firewall port 123 issues), the NTP “Ref ID” field for the unreachable NTP server will be reported as “.INIT” and its reach value will remain “0”. The reach value normally increments to “377” when the other NTP server is reachable.

Now refer to:

[Section "A\)"](#) for Archive software versions 5.1.2 and above (using the newer web browser)

[Section "B\)"](#) further below for Archive software versions between 5.0.2 and 5.1.2

[Section "C\)"](#) further below for Archive Software Versions 4.8.6 to 5.0.2

[Section "D\)"](#) further below for Archive Software versions 4.8.5 and below:

A) Archive software versions 5.1.2 and above (black/charcoal web browser)

To configure this NTP time server with other NTP Peers or NTP Servers, first login to the main page of the web browser and navigate to the **“Management”** -> **“NTP Setup”** page. Press the **“Gear”** box on the right-side of either **“NTP Peers”** (to define available NTP Peers) or on the right-side of **“NTP Servers”** (to define other NTP Servers) and enter the desired IP address for each of the other desired NTP servers that this NTP server can obtain time from. Then hit the Submit button.

Note: The grids on the NTP Peers and Servers tabs allow the user to define, by IP address or hostname, the locations of other NTP servers to use as time references (instead of, or in addition to, the configured SecureSync’s primary reference) and the locations of other NTP servers to use as peers. The maximum number of Peers allowed is twelve (12).

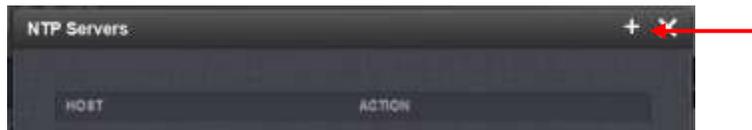
Notice about using DNS hostnames: When listing DNS hostnames (instead of IP addresses) to peer NTP servers together, the FQDN (Fully Qualified Domain Name) may need to be used, especially when the devices are not on the same domain. Or, setup the domain name on the network interface setup page (**Network** -> **Interfaces** page of the web browser) for each port, which should allow the single name rather than needing to use the FQDN.

A) To add a new NTP Server (versions 5.1.2 and above)

- 1) Navigate to the **Management** -> **NTP Setup** page of the browser.
- 2) Click on the **“gear box”** ICON to the right of **“NTP Servers”**

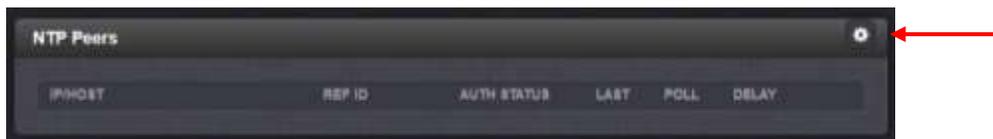


- 3) Click on the **“+”** to the right of **“NTP Servers”**

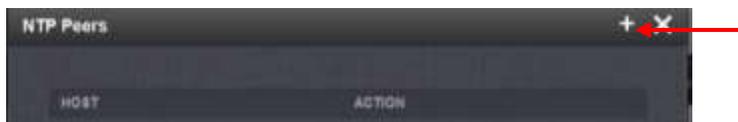


B) To add a new NTP Peer (versions 5.1.2 and above)

- 1) Navigate to the **Management** -> **NTP Setup** page of the browser.
- 2) Click on the **“gear box”** ICON to the right of **“NTP Peers”**



- 3) Click on the **“+”** to the right of **“NTP Peers”**



“NTP Peer” entry table:

Enter the IP addresses or Hostnames for the other, same Stratum NTP server(s) that this unit can use as a time reference.

Also enter this time server’s IP address/host name in the NTP Peers table of all of the other NTP servers that are referenced here.

“Min Poll” field:

Leave this value set to “3 (8s)” for each listed NTP sever to allow NTP to be able to sync faster.

“Enable Symmetric key” field:

Select if it’s desired to use NTP symmetric key authentication with this peer.

“Enable Autokey” field:

Select if it’s desired to use NTP Autokey with this peer.

Figure 7: “NTP Peers” table (versions 5.1.2 or higher)

“NTP Server” entry table:

Enter the IP addresses or Hostnames for the other, same Stratum NTP server(s) that this unit can use as a time reference.

Also enter this time server’s IP address/host name in the NTP Peers table of all of the other NTP servers that are referenced here.

“Min Poll” field:

Leave this value set to “3 (8s)” for each listed NTP sever to allow NTP to be able to sync faster.

“Enable Symmetric key” field:

Select if it’s desired to use NTP symmetric key authentication with this peer.

“Enable Autokey key” field:

Select if it’s desired to use NTP Autokey with this peer.

“Enable burst” mode field:

Select if it’s desired to send a burst of 8 packets when NTP is started up (helps NTP sync faster)

“Enable iburst” mode field:

Select if it’s desired to send a burst of 8 packets when NTP is started up (helps NTP sync faster)

“Mark as Preferred” field:

Select if it’s desired to provide additional weight to this one particular server, to help NTP likely select it as its reference.

Figure 8: “NTP Servers” table (versions 5.1.2 or higher)

Edit NTP Services (“Timing System Reference”, “Preferred” and “Timing System 1PPS Reference” fields):

Unlike Archive versions prior to version 5.1.2, which have additional configurations for NTP Peers and Servers in the same pages as these two tables, versions beyond 5.0.2 have additional configurations associated with NTP Peering in a different location of the browser.

The “Timing System Reference”, “Preferred” and “Timing System 1PPS Reference” fields also need to be configured. To configure these fields, in the **Management -> NTP Setup** page, click on the “gear” symbol on the right side of **“NTP Services”** (as shown below). Then select the **“Stratum 1”** tab.



Figure 9: “Edit NTP Services” (versions 5.1.2 and higher)

Note: “Timing System” refers to available and accurate external time and 1PPS input references for SecureSync (such as GPS, IRIG, ASCII timecode, etc.) or hand-set time (User mode). The Timing System’s time can be viewed in the **Management -> Time Management** page of the web browser)

If desired, the “Time” and “PPS” References for the NTP Service (such as GPS, IRIG, ASCII timecode, User set time, etc.) which are input to the Timing System can be enabled or disabled and when enabled, configured as “Preferred”. As these inputs are usually much more accurate than NTP data, “Prefer” provides additional “weighting” to these particular NTP input references while NTP is selecting which reference it should select as its time source. Though “prefer” does not guarantee that reference will become the selected reference, it can help it be selected.

- The **“Enable Stratum 1 Operation”** field is used to either allow or prevent the ability for NTP to select the SecureSync’s “System Time” as its time source.
 - **When enabled:** NTP can select the “System Time” reference as its time source. The System Time is synced via external references (such as GPS, NTP IRIG, Havequick, etc.) or hand-set by a user.
 - **When disabled:** When this field is disabled, NTP cannot select the System Time as its reference and therefore it can only sync to other NTP servers.
 - **Disable this checkbox** if the only input reference available is other NTP servers
- The **“Prefer Stratum 1”** checkbox (for the Timing System reference) configures NTP to “weight” the Timing System input heavier than inputs from other NTP servers for its reference selection (The Timing System inputs are normally more accurate than other NTP time servers, so it’s likely beneficial to select this box- unless NTP is the only input reference available).
 - **Enable this checkbox** if there are other external input references present/enabled (such as GPS, IRIG or external 1PPS input, for examples).
 - **Disable this checkbox** if NTP is the only external input reference available (no GPS or IRIG input, for examples).

- The “**Enable Stratum 1 1PPS**” checkbox determines whether NTP uses the 1PPS input from the Timing System. The 1PPS input to NTP needs to correlate with its “Time” input. If the Time and PPS inputs are originating from the same source, they will be correlated. However, if the time is originating from another NTP server, but the 1PPS is being derived by the Timing System, the two inputs may not always correlate. Without this correlation, NTP performance will be degraded. In this scenario, it is best not to use the System Time’s 1PPS as a reference.
 - **Disable this checkbox** whenever one or more NTP peers or servers on the network have been configured to allow NTP synchronization of this time server. It should not be selected if this time server can get NTP time stamps from another time server on the network.

Configuring the Default Port and Default Gateway address in order to be able to sync to Internet time servers

As these NTP time stamps originate from the SecureSync (not sent to the SecureSync), the SecureSync needs to know how to route the timestamps to the Internet. So the default gateway address (and which Ethernet interface to user, if the Gigabit 3 port Option Card is installed), needs to first be defined. Then once NTP has been restarted, the NTP time stamps can be routed to the Internet time servers.

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.

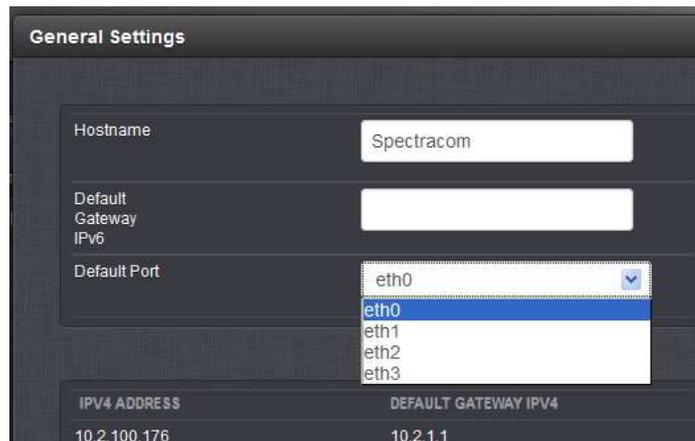


Figure 10: Configuring the Default Port (versions 5.1.2 and higher)

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.

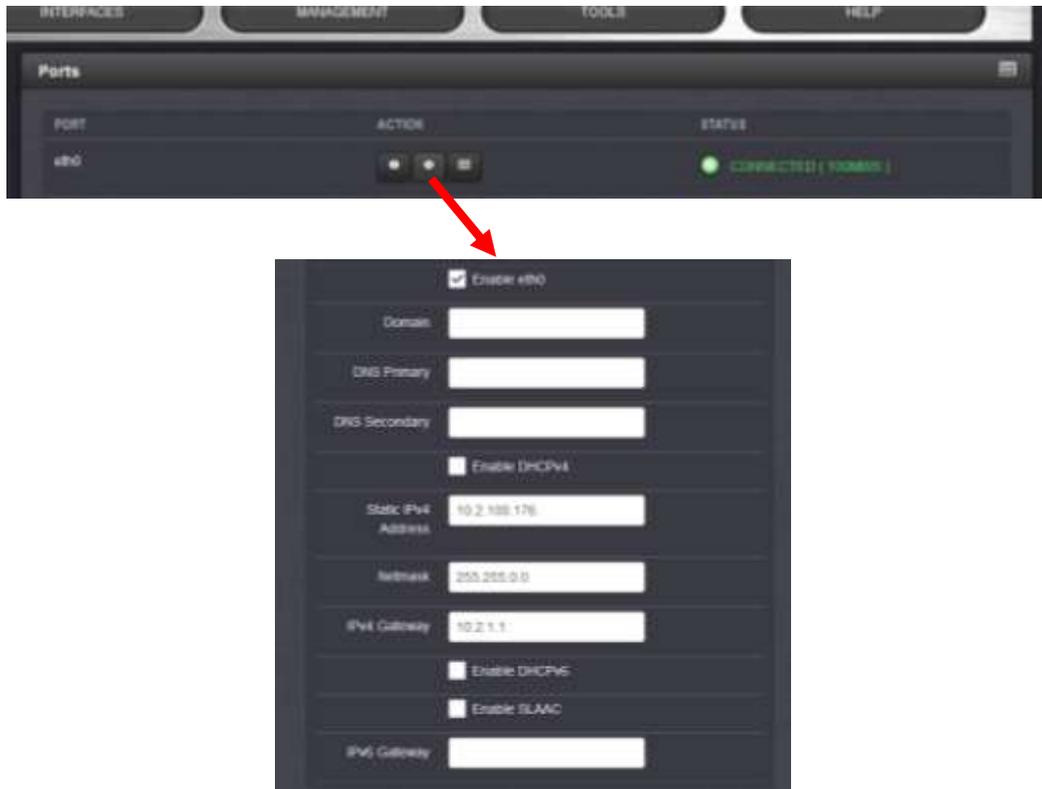


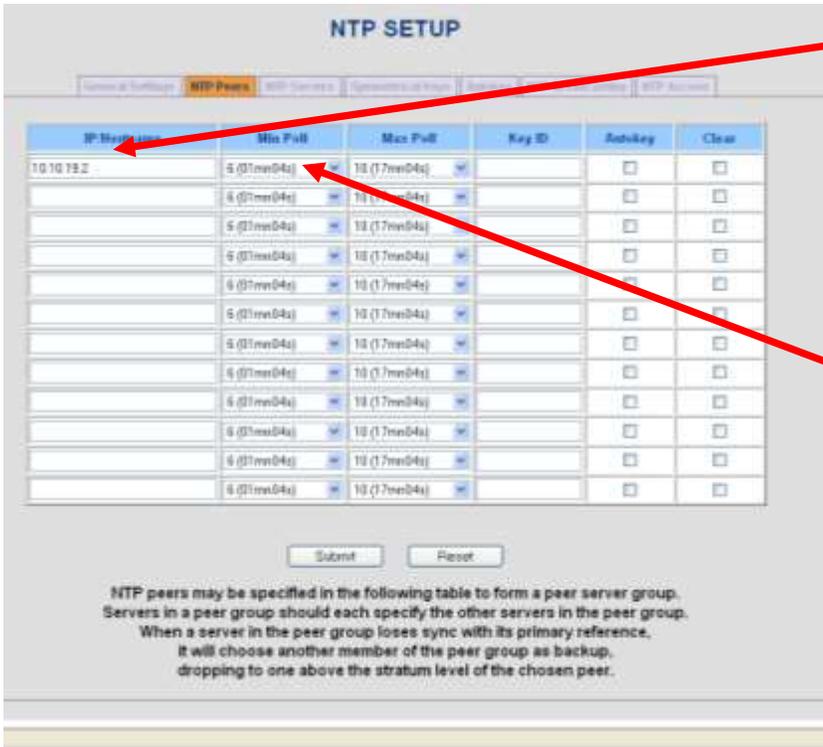
Figure 11: Configuring the default gateway (versions 5.1.2 and higher)

B) Archive software versions between 5.0.2 and 5.1.2

To configure this NTP time server with other NTP Peers or NTP Servers, first login to the main page of the web browser for the NTP server and navigate to the “Network/NTP Setup” page. Select either the “NTP Peers” tab (to define available NTP Peers) or the “NTP Servers” tab (to define other NTP Servers) and enter the desired IP address for each of the other desired NTP servers that this NTP server can obtain time from.. Then hit the Submit button.

Note: The grids on the NTP Peers and Servers tabs allow the user to define, by IP address or hostname, the locations of other NTP servers to use as time references (instead of, or in addition to, the configured SecureSync’s primary reference) and the locations of other NTP servers to use as peers. The maximum number of Peers allowed is twelve (12).

Notice about using DNS hostnames: When listing DNS hostnames (instead of IP addresses) to peer NTP servers together, the FQDN (Fully Qualified Domain Name) may need to be used, especially when the devices are not on the same domain. Or, setup the domain name on the network interface setup page (**Network -> Interfaces** page of the web browser) for each port, which should allow the single name rather than needing to use the FQDN.



“NTP Peers” table:

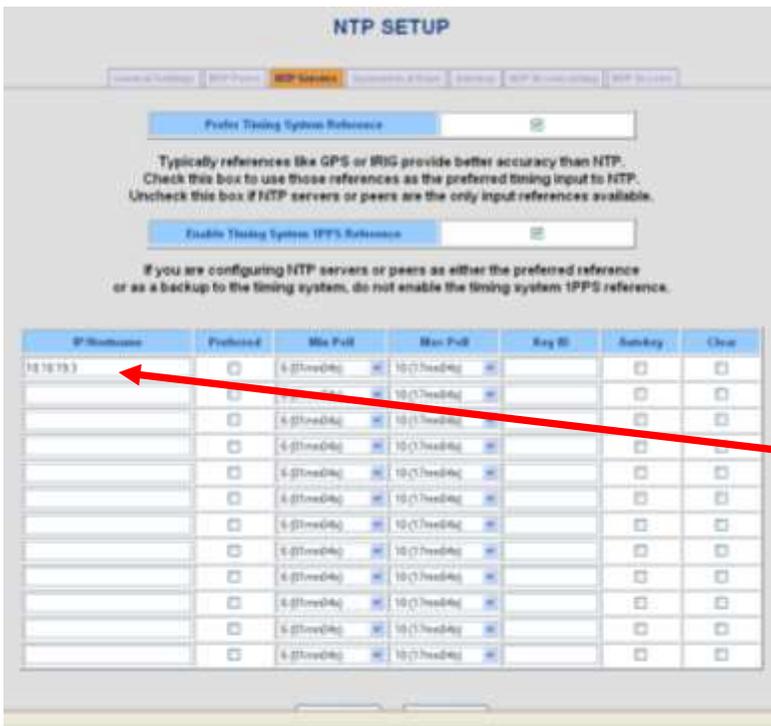
Enter the IP addresses or Hostnames for the other, same Stratum NTP server(s) that this unit can use as a time reference.

Also enter this time server’s IP address/hostname in the NTP Peers table of all of the other NTP servers that are referenced here.

“Min Poll” field:

Change this drop-down value to “4 (16s)” for each listed NTP sever to allow NTP to be able to sync faster.

Figure 12: “NTP Peers” table



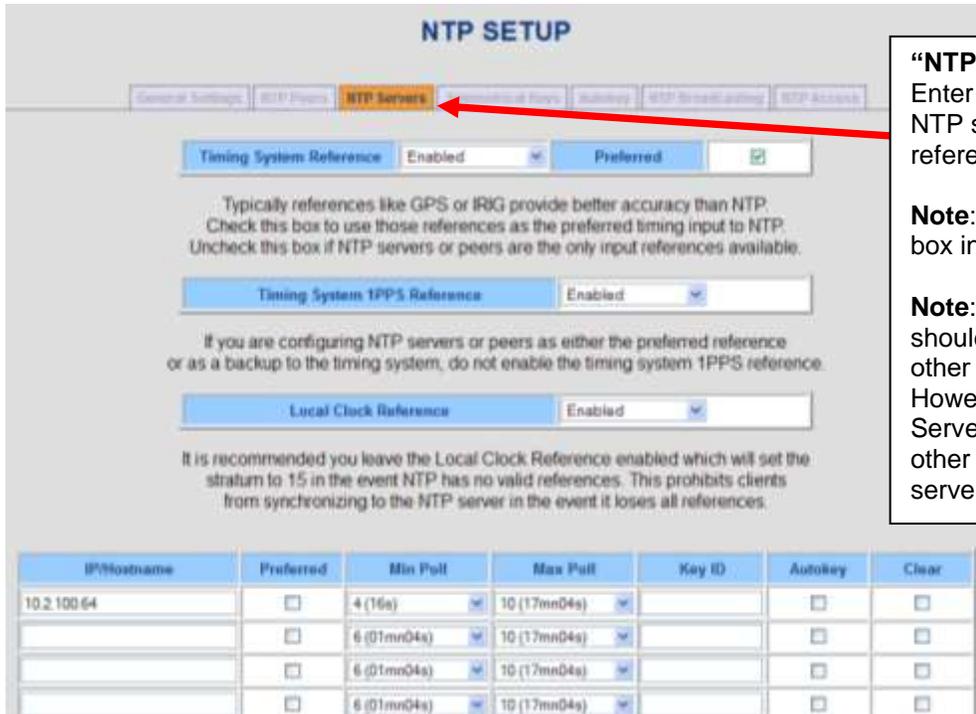
“NTP Servers” tab

Enter the IP addresses/hostnames for the other NTP server(s) that this unit can use as a time reference.

Note: Make sure to select the “Preferred” checkbox in one of these listed NTP servers.

Note: In NTP Server mode, this SecureSync should not be configured as an NTP peer in any other networked NTP server’s configuration. However, if desired, it can be listed as an NTP Server to another NTP time server (making the other NTP server no higher than a Stratum 3 server).

Figure 13: “NTP Servers” tab (Archive software versions 4.8.5 and below)



“NTP Servers” tab
 Enter the IP addresses/hostnames for the other NTP server(s) that this unit can use as a time reference.

Note: Make sure to select the “Preferred” checkbox in one of these listed NTP servers.

Note: In NTP Server mode, this SecureSync should not be configured as an NTP peer in any other networked NTP server’s configuration. However, if desired, it can be listed as an NTP Server to another NTP time server (making the other NTP server no higher than a Stratum 3 server).

Figure 14: “NTP Servers” tab (Archive software versions 4.8.6 and above)

Description of the NTP Peers and Servers table fields:

Note: Archive Software version 4.8.6 (June 2012) incorporated changes to the NTP Servers tab (Both Versions 4.8.5 and below as well as versions 4.8.6 and above are discussed herein).

IP/hostname: Enter either the IP address or DNS hostname of the desired NTP time server to peer with or sync to.

Preferred: Provides this NTP input reference with additional weighting for the NTP’s selection of its input reference. In the NTP Servers tab, this field needs to be selected in one of the listed NTP references. In the NTP peers table, the System reference is preferred over the list of NTP servers.

Min poll and Max poll: provide the NTP daemon with a range in which to poll the configured NTP server as determined by the daemon. The default values for these two fields are usually OK as-is and do not normally need to be reconfigured (Note: changing these values may impact the optimum operation of NTP).

Trusted Sym Key ID field- When using MD5 authentication (the NTP server being peered with must also support MD5 operation to use MD5), in the drop-down, select the desired key ID number to use to authenticate with the other NTP server (as defined in the NTP/Symmetric key table in this NTP server as well as the same MD5 key value in the other NTP server as well. The key strings have to be the same in both NTP servers in order for MD5 authentication to be successful.

Autokey field: Select Autokey if using the NTP Autokey feature in all NTP servers and clients.

Clear: Select this button to remove the entire row from the table. After hitting Submit, the entry will disappear.

C) Archive Software Versions 4.8.6 to 5.0.2:

Refer to [Section 2A: "Use Case" examples](#) for recommended NTP Server mode configurations.

"Timing System Reference", "Preferred" and "Timing System 1PPS Reference" fields:

Note: "Timing System" refers to available and accurate external time and 1PPS input references for SecureSync (such as GPS, IRIG, ASCII timecode, etc.) or hand-set time (User mode). The Timing System's time can be viewed in the **Setup -> Time Management** page of the web browser

If desired, the "Time" and "PPS" References for the NTP Service (such as GPS, IRIG, ASCII timecode, User set time, etc.) which are input to the Timing System can be enabled or disabled and when enabled, configured as "Preferred". As these inputs are usually much more accurate than NTP data, "Prefer" provides additional "weighting" to these particular NTP input references while NTP is selecting which reference it should select as its time source. Though "prefer" does not guarantee that reference will become the selected reference, it can help it be selected.

- The "**Timing System Reference**" Enable/Disable field is used to either allow or prevent the ability for NTP to select the SecureSync's "System Time" as its time source.
 - **When enabled:** NTP can select the "System Time" reference as its time source. The System Time is synced via external references (such as GPS, NTP IRIG, Havequick, etc.) or hand-set by a user.
 - **When disabled:** When this field is disabled, NTP cannot select the System Time as its reference and therefore it can only sync to other NTP servers.

Note: When NTP is only synced to other NTP servers (no other references available), having this field enabled allows NTP output to have Holdover capability, in case the configured NTP servers become unavailable (NTP syncs the System time. System Time has Holdover capability). If this field is disabled, NTP will have no Holdover capability and will go to Stratum 16 very shortly upon loss of connectivity with its configured NTP servers.

- The "**Preferred**" checkbox (for the Timing System reference) configures NTP to "weight" the Timing System input heavier than inputs from other NTP servers for its reference selection (The Timing System inputs are normally more accurate than other NTP time servers, so it's likely beneficial to select this box- unless NTP is the only input reference available).
 - **Enable this checkbox** if there are other external input references present/enabled (such as GPS, IRIG or external 1PPS input, for examples).
 - **Disable this checkbox** if NTP is the only external input reference available (no GPS or IRIG input, for examples).

- The "**Timing System 1PPS Reference**" checkbox determines whether or not NTP uses the 1PPS input from the Timing System. The 1PPS input to NTP needs to correlate with its "Time" input. If the Time and PPS inputs are originating from the same source, they will be correlated. However, if the time is originating from another NTP server, but the 1PPS is being derived by the Timing System, the two inputs may not always correlate. Without this correlation, NTP performance will be degraded. In this scenario, it is best not to use the System Time's 1PPS as a reference.

- The "**Local Clock Reference**" (Enable/Disable field):

Starting in Archive software version 4.8.6, a new Enable/Disable field has been added, in order to disable NTP's local clock reference (if needed or desired). Disabling this checkbox may help improve NTP operation when NTP's input reference(s) are not very stable or are periodically being lost.

The "Local Clock Reference" enable option determines whether NTP uses its Local Clock Reference as its selected reference, in the event all other references are lost or not selected due to stability, reliability or jitter. The Local Clock Reference degrades the NTP stratum to 16 by default when selected, so an NTP server without references cannot synchronize a timing chain of NTP servers.

When NTP selects the Local Clock Reference over any other external reference(s), NTP will go to Stratum 16 (by default). If NTP's inputs are not very stable (jittery) or are periodically not present, NTP may switch back and forth between Stratum 1 (or Stratum 2, for instance) and Stratum 16. While at Stratum 16, NTP will be ignored by the network clients. When it switches back to Stratum 1 or 2 again, it is considered a valid reference. An example where NTP may switch between an external reference and the Local Clock Reference is syncing SecureSync to an IRIG generator that is not externally synced to GPS, for instance. The IRIG input will not be jittery, resulting in NTP periodically selecting the Local Clock Reference over the IRIG generator, because the internal clock is more stable than the IRIG generator.

The Local Clock Reference can be disabled if the user does not desire this feature or to avoid switching between a reference and the Local Clock driver when the reference is intermittently reachable or less stable than the Local Clock. The Local Clock stratum can be adjusted to values other than 15 by using NTP Expert Mode.

Note: If the "Local Clock Reference" checkbox has been disabled in the web browser and if NTP has no other input references (such as GPS, IRIG, other NTP servers, etc) that it can sync with, the following entry will be asserted into the SecureSync's NTP Log file: "**no servers reachable**". While in this state, NTP will not be able to indicate its Stratum 16, so NTP clients will still sync to the NTP sever. It is typically recommended that the "**Local Clock Reference**" checkbox be enabled, to prevent this condition from occurring.

D) Archive Software versions 4.8.5 and below:

Refer to [Section 2A: "Use Case" examples](#) for recommended NTP Server mode configurations.

- **Prefer Timing System Reference** and **Enable Timing System 1PPS Reference** fields:

The "NTP Servers" tab on the **Network -> NTP Setup** page of the web browser contains two checkboxes, "Prefer Timing System Reference" and "Enable Timing System 1PPS Reference". These two boxes are described below:

Note: "Timing System" refers to available and accurate external time and 1PPS input references for SecureSync (such as GPS, IRIG, ASCII timecode, etc) or hand-set time (User).

If desired, the "Time" and "PPS" References for the NTP Service (such as GPS, IRIG, ASCII timecode, User set time, etc) which are input to the Timing System can be configured as "Preferred". As these inputs are usually much more accurate than NTP data, "Prefer" provides additional "weighting" to these particular NTP inputs references during the selection process, while NTP is deciding which reference it should select as its source (though "prefer" does not guarantee that reference will become the selected reference).

- The "**Prefer Timing System Reference**" checkbox configures NTP to "weight" the Timing system input heavier than input from other NTP servers for its selection (The Timing System inputs are normally more accurate than other NTP servers). However, if the Timing System inputs are not normally available (such as with intermittent GPS reception or no other inputs other than NTP input are available), it may be desired not to prefer the Timing System over an NTP reference, in which case this box should not be checked.
- The "**Enable Timing System 1PPS Reference**" checkbox determines whether or not NTP uses the 1PPS input from the Timing System. The 1PPS input to NTP needs to correlate with its "Time" input. If the Time and PPS inputs are originating from the same source, they will be correlated. However, if the time is originating from another NTP server, but the 1PPS is being derived by the Timing System, the two inputs may not always correlate. Without this correlation, NTP performance will be degraded. In this scenario, it is best not to use the System Time's 1PPS as a reference.

When to enable these boxes/fields and when to disable them:

Normally, the NTP service will obtain its Time and PPS reference inputs from the Timing System (The Timing System is the time, as derived from the GPS, IRIG, ASCII data input and NTP, etc). However, if desired, NTP can also obtain time from other NTP server(s).

NTP can either sync to other NTP servers directly (bypassing “System Time”), or it can sync to the “System Time” and then NTP can sync to the System Time. This later method provides Holdover capability, in case the other configured NTP servers become unavailable as reference(s).

Note: Refer to the Use Cases in [Section 2A](#) for specific examples.

- When the Timing System reference(s) (such as GPS, IRIG, Havequick, etc) are normally available to SecureSync, both the “Timing System Reference” and the “Timing System 1PPS Reference” should be selected/enabled.
- In the case of dedicated Stratum synchronization (syncing SecureSync to one or more other NTP servers on the network - instead of using the Timing System - so that it can operate as a dedicated Stratum 2 time server, for example), the Timing System inputs are not going to be available, as the only available input will be other configured NTP servers.
 - Enable the “Timing System Reference” (and the “Preferred” checkbox in versions 4.8.6 and higher) if you wish to have a Holdover period to be available upon loss of all NTP servers, before NTP goes to Stratum 16.
 - Disable the “Timing System Reference” (and the “Preferred” checkbox in versions 4.8.6 and higher) if you want NTP to go directly to Stratum 16 (causing the clients to ignore the SecureSync as a time reference) upon loss of all configured NTP servers (no Holdover capability).
- It may be desired to primarily sync the SecureSync to the Timing System (The System Time input from GPS, IRIG input, Stanag, as examples) and to also have one or more other NTP servers on the network be a backup, in case the primary reference is lost or not valid. If the primary reference is lost (and after Holdover mode has expired) it can operate as a Stratum 2 time server until the Primary time reference is available again.

In this scenario, it is best to check only the box at the top of the page so that the Timing System is preferred over a configured NTP server and unselect the bottom box to keep the Timing System’s 1PPS from affecting the operation of NTP.

- If NTP is being used only for SecureSync’s input synchronization (NTP isn’t being used as an output to sync any network NTP clients or other lower stratum NTP time servers) enable the “Timing System Reference” and disable the Timing System 1PPS Reference”.

In summary:

“Timing System Reference” (System Time)

- ✓ Select/Enable this box/field when using **any** input reference, unless NTP is the only input AND it’s desired for NTP to have Holdover capability upon loss of all listed NTP servers.
- ✓ Unselect/Disable this box/field when using **only** other NTP servers as the input reference for NTP AND there is no desire for NTP to have any Holdover capability upon loss of all listed NTP servers. NTP will go directly to Stratum 16 upon loss of all configured NTP servers.

“Preferred” checkbox (Archive versions 4.8.6 and above)

- ✓ Select this box if there are other input references (such as GPS, IRIG or external 1PPS enabled/available)
- ✓ Unselect this box if NTP is the only available external input reference available.

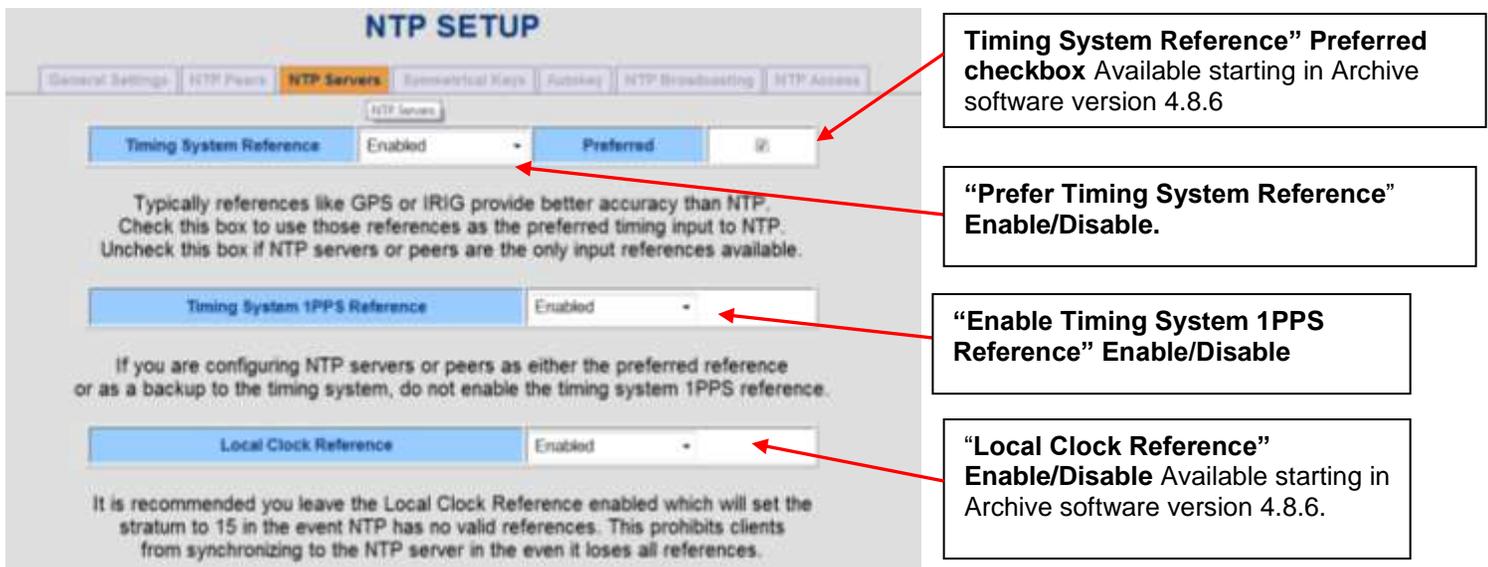
Note: When this “Preferred” checkbox is not selected, the “Preferred” checkbox next to **one** configured NTP server in the list of NTP Servers (the table below these fields) should be selected as being the preferred NTP reference.

“Timing System 1PPS Reference” checkbox

- ✓ Select/Enable this box when there are **no other NTP servers** being used as an input reference (there are no listed NTP servers in either the “NTP Servers” or “NTP Peers” tabs of the Setup/NTP Setup page of the browser).
- ✓ Unselect/Disable this box if using **any other NTP servers** as an input reference as a primary reference or as a backup to System Time references (such as GPS or IRIG, for examples). In this particular scenario, there will be at least one listed NTP server in either the “NTP Servers” or “NTP Peers” tabs of the Setup/NTP Setup page of the browser.

“Enable Local Clock Reference” checkbox (Archive versions 4.8.6 and above)

- ✓ Select this box when NTP is being provided stable input references (such as GPS, IRIG from an IRIG generator that is synced to GPS, or NTP from another stable NTP server). NTP will select these as its reference and will remain at a high Stratum (such as Stratum 1 or 2). However, if those references are lost, NTP can go to Stratum 16 until they are restored. While at Stratum 16, NTP will be ignored by the NTP clients on the network.
- ✓ Unselect this box when NTP is being provided unstable inputs (such as IRIG from an IRIG generator that is not synced to GPS or NTP from another unstable NTP server- like a Stratum 2 time server, for instance). NTP won’t select the “Local Clock Reference” and won’t go to Stratum 16, even though its reference(s) may either have marginal performance or may even periodically not be present. NTP will continue to be a useable time reference for the NTP clients (the SecureSync will never be ignored by the network clients, no matter the status of the input references).



The screenshot shows the 'NTP SETUP' page with the 'NTP Servers' tab selected. Three callout boxes point to specific settings:

- “Timing System Reference” Preferred checkbox** Available starting in Archive software version 4.8.6. This points to the 'Preferred' checkbox in the 'Timing System Reference' section.
- “Prefer Timing System Reference” Enable/Disable.** This points to the 'Enabled' dropdown menu in the 'Timing System Reference' section.
- “Enable Timing System 1PPS Reference” Enable/Disable** This points to the 'Enabled' dropdown menu in the 'Timing System 1PPS Reference' section.
- “Local Clock Reference” Enable/Disable** Available starting in Archive software version 4.8.6. This points to the 'Enabled' dropdown menu in the 'Local Clock Reference' section.

Figure 15: “NTP Servers” tab (Archive software versions 4.8.6 and above)

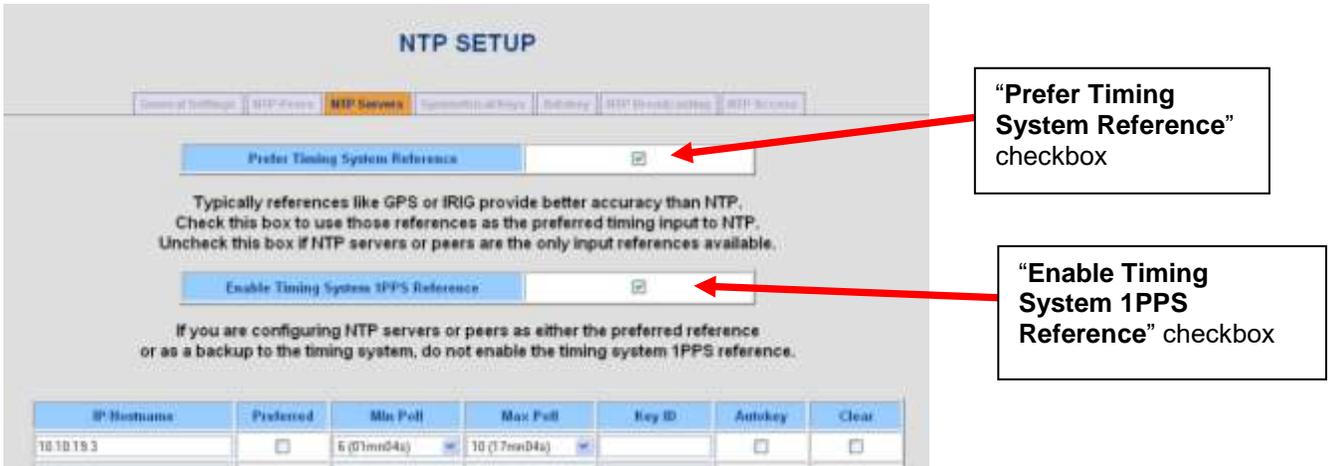


Figure 16: “Prefer Timing System” and “Enable Timing System” checkboxes (Archive software versions 4.8.5 and below)

Note: Only one NTP server in the “NTP Servers” tab can be selected as “Preferred” (and should only be selected if the “Prefer Timing System Reference” box is not selected).

“Antenna Problem” and “Frequency” alarms asserted when using “NTP Servers” mode (only syncing the SecureSync to other NTP servers).

Please note that when SecureSyncs, with a GPS receiver installed, are configured to be dedicated Stratum 2 NTP servers (only syncing to other NTP servers) and therefore don't have a GPS antenna attached to the SecureSync, the “Antenna Problem” alarm (classified as a Minor alarm condition) will remain asserted. Also, as the SecureSync cannot discipline its 10 MHz oscillator to other NTP servers, with no other input references present and selected, the Frequency alarm (classified as a Major alarm condition) will remain asserted.

Archive software version 4.8.7 (and above) provides the ability to override these, and other undesired alarm conditions. These alarm conditions can be overridden in the **Management -> Notifications** page (or in the classic browser, **Tools -> Notification** page).

- The “**Antenna Problem**” alarm mask (and associated clear mask) is in the **GPS** tab.
- The “**Frequency Error**” alarm mask (and associated clear mask) is in the **Timing** tab.

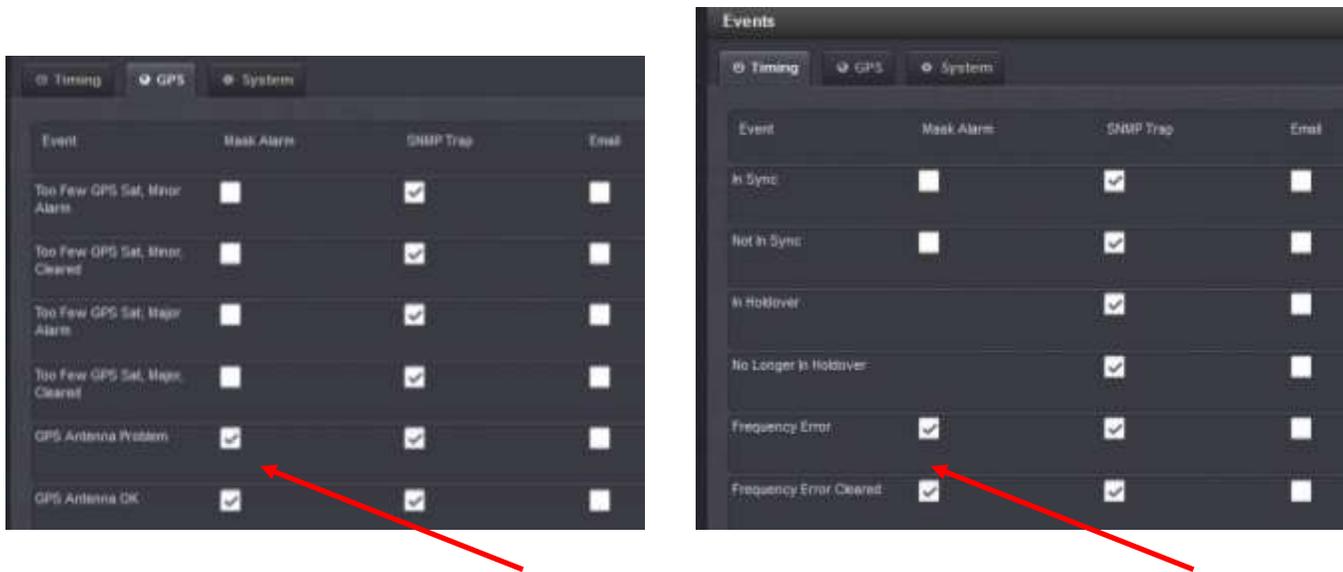


Figure 17: Mask undesired alarms (Archive versions 5.1.2 and above)

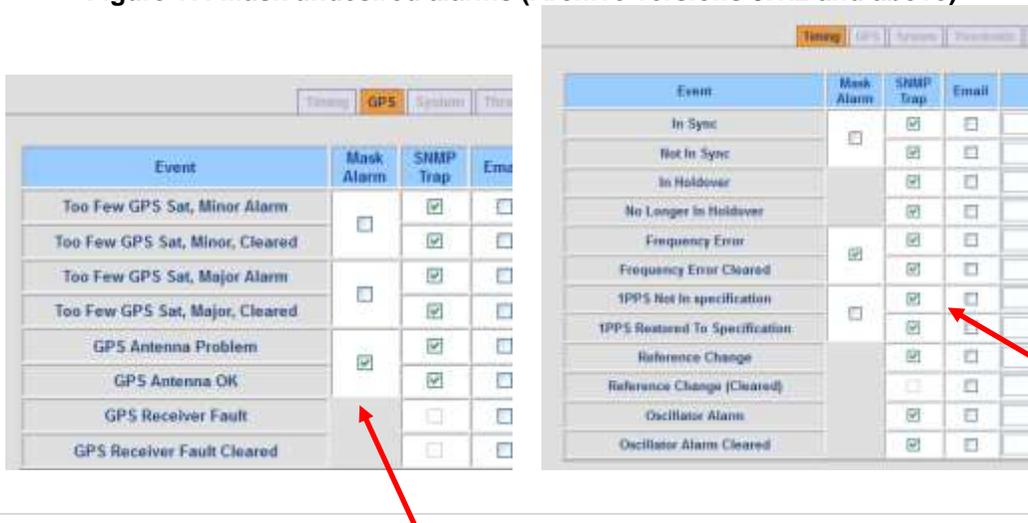


Figure 18: Mask undesired alarms (Archive versions 5.0.2 to 4.8.7)

Archive versions prior to version 4.8.7

With earlier versions of Archive software installed, the “Antenna Problem” alarm can be cleared by adding a 200 ohm resistor across the rear panel GPS connector. Version 4.8.7 (and above) software alleviates the need to add a resistor to the GPS antenna connector in order to clear the Antenna Problem alarm, as this alarm can now be overridden via software configuration. The Frequency alarm cannot be cleared in software versions prior to version 4.8.7, without another external input reference besides NTP selected.

Section 2A: NTP Peer/Server mode configuration “Use Case” examples:

This section provides a few example “use case” scenarios of how to configure NTP in SecureSync:

- Example A:** This is the **factory default NTP settings** when no other NTP Servers are configured or available to be input references for SecureSync to sync with. The SecureSync is not syncing any other NTP servers on the network.
- Example B:** This example shows NTP configuration **if other references (such as GPS or IRIG) are the primary input to NTP while one or more other NTP servers (at the same stratum level) are available on the network to be a backup reference.** For instance, this SecureSync is typically a Stratum 1 time server, along with one or more other Stratum 1 servers on the same network. But if the primary references are lost, NTP can go to Stratum 2 for instance (instead of going to Stratum 16). This is referred to as the “NTP Peering” mode.
- Example C:** This example shows NTP configuration **if no other references (such as GPS or IRIG) are available** for the SecureSync to sync with. However, **one or more other NTP servers on the same network are available** to provide the SecureSync with both the required “Time” and “1PPS” references that it needs for synchronization. In this example, SecureSync is normally one Stratum level lower than its configured references (Examples include: this SecureSync is normally a Stratum 2 server which is syncing to one or more Stratum 1 servers. Or it’s normally a Stratum 3 time server, syncing to Stratum 2 time servers).
- Example D:** This example shows NTP configuration **if no other references (such as GPS or IRIG) are available** for NTP to sync with. However, **one or more other NTP servers on the same network are available to provide with the required Time input.** In addition to having NTP servers to sync with, in this particular example, **the System Time is also being provided with an external 1PPS input signal,** which is used to discipline the SecureSync’s oscillator and control the on-time point of the SecureSync’s output (such as an external Rubidium oscillator, for example).

The external 1PPS replaces the 1PPS that is normally generated by the oscillator inside of SecureSync. As the internal oscillator cannot be disciplined when syncing only to NTP, this external 1PPS reference input may provide better stability of the SecureSync’s outputs than the unit’s internal oscillator.

Note: In this configuration, the stability/accuracy of the SecureSync’s outputs (such as PTP for example) will be based on the stability/accuracy of this 1PPS input signal (the outputs will follow the external 1PPS input as the internal oscillator disciplines to the external 1PPS input), instead of being based on the free-run characteristics of the internal oscillator.

If this external 1PPS is not very stable, the SecureSync’s outputs may be adversely affected. In this case, it may be more beneficial to use the internal 1PPS as the selected reference, instead of an external 1PPS reference.

Note: As noted in these scenario sections, disable and then re-enable the NTP Service after making any NTP configuration changes in SecureSync (**Network -> NTP Setup** page of the browser, “**General Settings**” tab). Disable NTP and then re-enable NTP. NTP will be in sync a few minutes later.

Example A) Factory default NTP configuration:

By factory default, SecureSync is configured for NTP to prefer and sync with the **System Time** and **System 1PPS**. System Time and System 1PPS are typically synced to one or more external time references (such as GPS, IRIG, ASCII data, Stanag. Or the time can be manually set).

The default configuration is to have no NTP servers listed in either the “NTP Servers” or the “NTP Peers tab”. Both the “Prefer Timing System Reference” and “Enable Timing System 1PPS Reference” checkboxes/fields are selected/enabled, as shown in the following two screenshots.



Figure 19: “Edit NTP Services, Stratum 1 tab (versions 5.1.2 and above)



Figure 20: “NTP Servers” tab (versions 4.8.6 and above)



Figure 21: “NTP Servers” tab (versions 4.8.5 and below)

Operation of this example configuration:

- 1) Initially, NTP will be synced to the System Time Reference(s) (i.e. GPS, IRIG, Stanag, Havequick, etc) and will report to the network clients that it's a Stratum 1 time server.
- 2) If all the System Time's input references (i.e. GPS, IRIG, etc) are lost or becomes not valid, the SecureSync will go into Holdover mode. NTP will remain at Stratum 1 during the Holdover period.
- 3) If the System Time's input reference is regained or declared valid again, before the "Holdover Timeout" period expires, as configured (in seconds) before the SecureSync goes back into full time sync and NTP remains at Stratum 1. The allotted Holdover period is 2 hours by factory default and can be configured in:
 - A) *Newer web browser:* **Management -> Disciplining** page of the browser (click on the gear box next to "Status" on the left side of the page)
 - B) *Classic interface:* **Setup -> Disciplining** page of the browser
- 4) However, if the System Time's input references aren't regained, or not declared valid again, before the Holdover period expires, SecureSync will then switch from Holdover to "Not in Sync" state, causing NTP to then switch to Stratum 16.

Note: If the "Local Clock Reference" field (Archive versions 4.8.6 and higher) has been changed to "Disabled", NTP will remain at Stratum 1 and will continue to be a useable time reference for the network. NTP will not be able to go to Stratum 16.
- 5) When the System Time's input reference is regained or declared valid again, NTP will then switch back to Stratum 1 again (NTP will be using the "System Time" and "System PPS" as its references again).

Example B) “NTP Peering mode”: System Time is normally synced to one or more primary input references (such as GPS or IRIG) and it’s also desired to have one or more other “same Stratum” NTP servers on the network be a backup to the System Time reference.

In this example, the SecureSync is typically a Stratum 1 time server, along with one or more other Stratum 1 servers on the same network. If System Time is lost, NTP can get time from another same Stratum time server. This is referred to as the “NTP Peering” mode.

Note: Example B discusses NTP having Holdover capability, upon loss of the System Time references and upon the loss of all NTP servers (this is typically the preferred operation). Contact Tech Support if it’s desired for NTP to go directly to Stratum 16 (no Holdover capability) upon the loss of all external references.

The SecureSync can be configured to have NTP still prefer the System Time and System 1PPS references, when they are present and valid. However, NTP can still select its input from other same Stratum level NTP servers, if the primary input is lost or becomes not valid.

In this configuration, the Reference Priority table, located in:

- A) *Newer web browser:* **Management** -> **Reference Priority** page of the browser
- B) *Classic interface:* **Setup** -> **Reference Priority** page of the browser

will have an “Enabled” row in this table that lists “NTP” in the “Time” column and “NTP” in the “1PPS” column. This entry in the table will be assigned a lower priority than other input references (such as GNSS, IRIG, ASCII data, etc).

Priority	Time	1PPS	Enabled	Action
1	GNSS 0	GNSS 0	<input checked="" type="checkbox"/>	Delete
2	PTP 0	PTP 0	<input checked="" type="checkbox"/>	Delete
3	NTP 1	NTP 1	<input checked="" type="checkbox"/>	Delete

Figure 22: “Reference Priority Setup” table (versions 5.1.2 and above)

Index	State	Priority	Time	1PPS	Delete
0	Enabled	1	GPS 0	GPS 0	<input type="checkbox"/>
1	Enabled	2	IRIG 0	IRIG 0	<input type="checkbox"/>
2	Enabled	3	NTP	NTP	<input type="checkbox"/>

Figure 23: “Reference Priority Setup” table (versions 5.0.2 and below)

When its desired to have NTP prefer the primary System Time and System 1PPS references (such as GPS or IRIG), and its desired to have one or more other NTP servers be a backup to the primary input(s), the desired NTP server(s) are also listed in the “NTP Peers” table.

In this example configuration, the other Stratum 1 NTP time servers (on the same network) that you wish for this SecureSync to be able to sync with are listed in the NTP Peers table (not in the “NTP Servers” tab). The “NTP Peers” table is located in the:

- A) Newer web browser: **Management** -> **NTP Setup** page of the browser
- B) Classic interface: **Network** -> **NTP Setup** page of the browser, “**NTP Peers**” tab.

Note: As shown below, we also recommend configuring the corresponding “Min Poll” interval drop-down field for each listed NTP time server be changed to “4 (16s)” in versions 4.8.9 and below, or to “3 (8s)” in versions 5.0.0 and above. This will help speed-up the time for initial NTP synchronization to occur.



Figure 24: “NTP Peers” table (versions 5.1.2 and above)

IP/Hostname	Min Poll	Max Poll	Key ID	Autokey	Clear
10.10.10.2	4 (16s)	10 (17mn04s)		<input type="checkbox"/>	<input type="checkbox"/>
10.10.10.3	4 (16s)	10 (17mn04s)		<input type="checkbox"/>	<input type="checkbox"/>
	6 (01mn04s)	10 (17mn04s)		<input type="checkbox"/>	<input type="checkbox"/>

Figure 25: “NTP Peers” table (versions 5.0.2 to 4.8.7)

Configure GPS to be primary input for NTP selection/synchronization, NTP as backup

A) Black/charcoal background web browser (versions 5.1.2 and above)

In this particular configuration of GPS as primary NTP sync and NTP as backup sync, the “**Enable Stratum 1 Operation**” and “**Prefer Stratum 1**” checkboxes should still be selected. However, the “**Enable Stratum 1 1PPS**” checkbox should be unselected (this checkbox is selected by factory default), as shown in the following screenshot. The screenshot below depicts this recommended configuration.

1. Click on the “gear” icon to the right of “**NTP Services**” (located on the left side of the **Management** -> **NTP Setup** page, just above the NTP ON/OFF slider switch) to open a pop-up window.
2. In the pop-up window, select the “**Stratum 1**” tab.
3. As shown in the screenshot further below:
 - Leave the “**Enable Stratum 1 Operation**” checkbox selected (this allows System holdover if GPS and the NTP servers happen to become unavailable for a period of time).
 - Leave the “**Prefer Stratum 1**” checkbox selected (this gives GPS additional “weight” for NTP to select GPS input over other NTP Servers).
 - Unselect the “**Enable Stratum 1 1PPS**” checkbox.



4. Press Submit

B) Classic interface web browser

In this particular configuration, the “**Prefer Timing System Reference**” checkbox/field should still be selected/enabled. However, the “**Timing System 1PPS Reference**” checkbox should not be selected/enabled, as shown in the following screenshot. The screenshot below depicts this recommended configuration.



Figure 26: “NTP Servers” tab (versions 4.8.6 to 5.0.1)

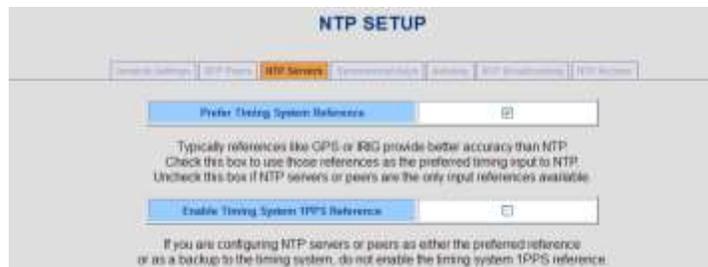


Figure 27: “NTP Servers” tab (versions 4.8.5 and below)

Note: With this “NTP Peering” mode (unlike the “NTP Servers” mode), this same configuration can be performed in other NTP servers on the same network, so that they can reference this SecureSync, if that other NTP server loses its primary System Time reference (In the “NTP Servers” mode, NTP synchronization is available in one direction only).

Operation of this configuration:

- 1) Initially, NTP will be synced to the System Time Reference(s) (i.e. GPS, IRIG, etc.) and will report it's at Stratum 1.
- 2) If all of the System Time's input references (i.e. GPS, IRIG, etc.) are lost or become not valid, the SecureSync will select a listed NTP Peer to be its selected Reference. NTP will report to its NTP clients that it's one Stratum level less than its selected NTP Peer (typically, the NTP Peer is Stratum 1, so this SecureSync will go to Stratum 2).
- 3) If the System Time's input reference is regained or declared valid again, before the "Holdover Timeout period expires, as configured (in seconds) before the SecureSync goes back into full time sync and NTP remains at Stratum 1. The allotted Holdover period is 2 hours by factory default and can be configured in:
 - A) *Newer web browser:* **Management -> Disciplining** page of the browser (click on the gear box next to "Status" on the left side of the page)
 - B) *Classic interface:* **Setup -> Disciplining** page of the browser
- 4) However, if the System Time's input references aren't regained or not declared valid again, before the Holdover period expires, SecureSync will then switch from Holdover to "Not in sync" state, causing NTP to then switch to Stratum 2 (using a listed NTP Peer as its reference).
- 5) When the System Time's input reference is regained or declared valid again, NTP will then switch back to Stratum 1 again (using the "System Time" and "System PPS" again as its selected references).
- 6) However, if the System Time's input reference is not regained, or not declared valid again, before the Holdover period expires (as configured in the **Setup -> Disciplining** page of the browser), SecureSync will then switch from Holdover to "Not in Sync" state, causing NTP to then switch to Stratum 16.

Note: If the "Local Clock Reference" field (Archive versions 4.8.6 and higher) has been changed to "Disabled", NTP will remain at Stratum 1 and will continue to be a useable time reference for the network. NTP will not be able to go to Stratum 16.
- 7) When the System Time's input reference is regained or declared valid again, NTP will then switch back to Stratum 1 again (NTP will be using the "System Time" and "System PPS" as its references again).

Note: if one or more NTP Peers or Servers reports it's "unreachable", refer to: [Section 6: Troubleshooting](#)

Example C) One or more other NTP time servers on the network are the only “Time” and “1PPS” input references to SecureSync. Also, it’s desired for NTP to have Holdover capability, in case the configured NTP servers become unreachable/unavailable for synchronization)

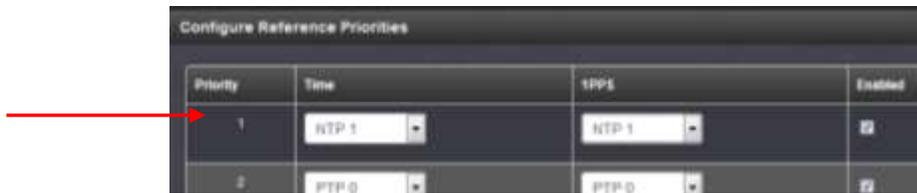
Note: Example C discusses NTP having Holdover capability, upon loss of the System Time references and upon the loss of all NTP servers (this is typically the preferred operation). Contact Tech Support if it’s desired for NTP to go directly to Stratum 16 (no Holdover capability) upon the loss of all external references.

SecureSync can be configured for one or more other NTP time servers to be the only references to provide the required Time input for NTP synchronization. In this example, NTP has no available inputs from System Time.

In this configuration, the Reference Priority table will have an “**Enabled**” row in this table that lists “**NTP**” in the “**Time**” column and “**NTP**” in the “**1PPS**” column. (Other enabled input references can be listed in this table without affecting this operation, since no other inputs are present in this example configuration).

The Reference Priority table is located in:

A) **Newer web browser:** Management -> Reference Priority page of the browser



B) **Classic interface:** Setup -> Reference Priority page



Figure 28: “Reference Priority Setup” table

In this particular example:

- The “**Timing System Reference** (or “**Prefer Timing System Reference**”) fields should be disabled/unchecked.
- The “**Preferred**” checkbox (versions 4.8.6 and above) should not be checked.
- The “**Timing System 1PPS Reference**” (or “**Enable Timing System 1PPS Reference**”) checkboxes/fields should be disabled/unchecked.
- The other NTP servers on the network for the SecureSync to sync with should be listed in either the “NTP Servers” section of **Management** -> **NTP Setup** page of the browser. OR in the “NTP Servers” tab of the classic interface browser.

Note: One of listed NTP servers in the “NTP Servers tab” should have the corresponding “Preferred” checkbox selected (if only one NTP server is listed, select the “Preferred” box for that NTP server).

The screenshots below depict this recommended configuration.

Note: We also recommend configuring the corresponding “Min Poll” interval drop-down field for each listed NTP server be changed to “4(16s)”. This will help speed-up the time for initial NTP synchronization to occur.

A) Newer web browser (versions 5.1.2 and above)

Add desired server(s) in the Management -> NTP Setup page of the browser

1. Click on the “gear” icon to the right of “NTP Servers” to open a pop-up window.
2. In the pop-up window, click the “+” sign.
3. Enter the address of an NTP server you wish for this time server to sync with, set the “**Min Poll Interval**” to “**3 (8s)**” and select the “Mark as Preferred” checkbox (as shown below) Note the “Max Poll Interval” can be set as desired. Setting it to “3 (8s)” also will cause NTP to poll this time server every 8 seconds.

Figure 29: “NTP Servers” tab (versions 4.8.6 and above)

4. Press Submit.
5. Repeat this process for each additional NTP Server you wish this time server to be able to sync with, if more than one NTP time server is available for its synchronization (NTP in this time server will then decide and select for its sync the one that it thinks is the best time server).

Now edit “NTP Services” for “NTP input only”

1. Click on the “gear” icon to the right of “NTP Services” (located on the left side of the **Management** -> **NTP Setup** page, just above the NTP ON/OFF slider switch) to open a pop-up window.
2. In the pop-up window, select the “Stratum 1” tab.
3. As shown below, leave the “**Enable Stratum 1 operation**” checkbox selected (this allows System holdover if the NTP servers become unavailable for a period of time). Unselect the other two checkboxes below it (“**Prefer Stratum 1**” and “**Enable Stratum 1 1PPS**”).



Figure 30: “NTP Servers” tab (versions 4.8.6 and above)

4. Press Submit

B) Classic interface web browser



Figure 31: “NTP Servers” tab (versions 4.8.6 and above)



Figure 32: “NTP Servers” tab (versions 4.8.5 and below)

Note: If it's desired for NTP to go to Stratum 16 very shortly after all configured NTP servers become unreachable/unavailable for synchronization (instead of having an allotted amount of Holdover to allow one or more configured NTP servers to be made available again before NTP goes to Stratum 16), disable the “Prefer Timing System Reference” and “Enable the Timing System Reference”. Also select the “Preferred” checkbox next to one of the NTP servers listed in the table below these checkboxes.

Operation of this example configuration:

- 1) Initially, NTP will be synced to one of the NTP Servers listed in the “NTP Servers” tab (note that the selected NTP server may, or may not, be the “Preferred” NTP Server - though NTP is more likely to select the preferred reference). NTP will report to its clients that it’s one Stratum level less than its selected NTP server (it’s Stratum 2, when synced to a Stratum 1 server).
- 2) If the selected NTP server is unreachable or not useable as reference for an extended period time, and as long as there is more than one NTP server listed, NTP will eventually switch (after a few bad polls of that reference, so this period of time will vary) to another NTP server as its selected reference. NTP will remain one less Stratum than its selected NTP server.
- 3) If the NTP input reference is regained or declared valid again, before the “Holdover Timeout period expires, as configured (in seconds) before the SecureSync goes back into full time sync and NTP remains at Stratum 1. The allotted Holdover period is 2 hours by factory default and can be configured in:
 - A) **Newer web browser: Management -> Disciplining** page of the browser (click on the gear box next to “Status” on the left side of the page)
 - B) **Classic interface: Setup -> Disciplining** page of the browser
- 4) If one or more other NTP servers are regained or declared valid again, before the holdover period expires, SecureSync goes back into full time sync and NTP goes back to reporting its Stratum level is one less than its selected reference.
- 5) However, if the NTP server is not regained, or not declared valid again (and there are no other useable time servers on the network) before the Holdover period expires
- 6) (as configured in the **Setup -> Disciplining** page of the browser), SecureSync will then switch from Holdover to “Not in Sync” state, causing NTP to then switch to Stratum 16.
- 7) SecureSync will then switch from Holdover to “Not in Sync” state, causing NTP to then switch to Stratum 16.

Note: If the “Local Clock Reference” field (Archive versions 4.8.6 and higher) has been changed to “Disabled”, NTP will remain at Stratum 1 and will continue to be a useable time reference for the network. NTP will not be able to go to Stratum 16.
- 8) When one or more other NTP servers are regained or declared valid again, NTP will then switch back to one less Stratum than its selected reference.

Note: if one or more NTP Peers or Servers reports it’s “unreachable”, refer to: [Section 6: Troubleshooting](#)

Example D) NTP is the only enabled “Time” input reference, combined with an external 1PPS input being supplied to discipline the internal oscillator and align the SecureSync’s outputs (such as its PTP Master’s outputs, for instance)

Notes about this configuration:

- 1) This configuration requires an available 1PPS input Option Card be installed in the SecureSync (such as the Models 1204-01 or 1204-28). The 1PPS input is connected to this Option Card.
- 2) Normally, the oscillator is in free-run mode when using NTP as the only input reference. When providing an external 1PPS input signal which is used to discipline the oscillator. Therefore, the System PPS and its on-time point will follow the external 1PPS input. So, if the external PPS is not stable or the 1PPS generator is not being disciplined to an external source, the SecureSync’s outputs may also waver, in unison with the external 1PPS input reference.
- 3) This configuration requires NTP Expert mode be enabled, in order to manually edit the ntp.conf file directly.

In this configuration, the Reference Priority table will have an “Enabled” row in this table that lists “NTP” in the “Time” column and “PPS Input 0” (or “EPP 0” for the Classic interface browser) in the “1PPS” column.

The Reference Priority table is located in:

A) **Newer web browser:** Management -> Reference Priority page of the browser



B) **Classic interface:** Setup -> Reference Priority page



Figure 33: “Reference Priority table

A) Newer web browser (versions 5.1.2 and above)

Configure NTP Services for “NTP and external 1PPS input”

1. Click on the “gear” icon to the right of “NTP Services” (located on the left side of the **Management** -> **NTP Setup** page, just above the NTP slider switch) to open a pop-up window.
2. In the pop-up window, select the “**Stratum 1**” tab.
3. As shown below, leave the “**Enable Stratum 1 operation**” and “**Enable Stratum 1 1PPS**” checkboxes selected. Unselect the “**Prefer Stratum 1**” checkbox



Figure 34: “NTP Servers” tab (versions 4.8.6 and above)

4. Press Submit

Add at least two desired server(s) in the Management -> NTP Setup page of the browser

1. Click on the “gear” icon to the right of “NTP Servers” to open a pop-up window.
2. In the pop-up window, click the “+” sign.
3. As shown below, enter the address of an NTP server you wish for this time server to sync with, set the “**Min Poll Interval**” to “**3 (8s)**” and select the “**Mark as Preferred**” checkbox (on only ONE of the NTP servers being added)

Note the “Max Poll Interval” can be set as desired. Setting it to “3 (8s)” also will cause NTP to poll this time server every 8 seconds.



Figure 35: “NTP Servers” tab (versions 4.8.6 and above)

4. Press Submit.
5. Repeat this process for each additional NTP Server you wish this time server to be able to sync with, if more than one NTP time server is available for its synchronization (NTP in this time server will then decide and select for its sync the one that it thinks is the best time server).

B) Classic interface web browser

Configure NTP (in the “NTP Servers” Tab) as shown in Figure 36

- a. Enable **Timing System Reference**, but do NOT check prefer.
- b. Enable **Timing System 1PPS Reference**
- c. Enable **Local Clock Reference**
- d. Configure at least 2 IP addresses on the NTP server page (see **Notes** below):
 - i. **Prefer** a single Stratum 1 server, based on network configuration or quality.
 - ii. Set the **Min Poll** interval to “**4 (16 seconds)**”.
- e. Press Submit

Notes:

- 1) In this configuration, at least one of the listed NTP servers should be selected as “Preferred”. The “Prefer Timing System Reference” and “Enable Timing System 1PPS Reference” checkboxes should not be selected.
- 2) We also recommend configuring the corresponding “Min Poll” interval drop-down field for each listed NTP server be changed to “4(16s)”. This will help speed-up the time for initial NTP synchronization to occur.
- 3) We highly recommend adding at least (2) two Stratum 1 servers in the table, in order to prevent a potential condition which might cause NTP to periodically switch between the Stratum 2 server, the System PPS and the System Time as its selected reference (System Time may periodically go into the Holdover mode, making the System Time a valid input to NTP). Listing more than one Stratum 1 server gives the Stratum 1 servers more “weight” so that NTP can always select one of the Stratum 1 servers

If this occurs, the Alarms logs will show periodic Holdover alarms occurring, and the NTP log will show the NTP daemon periodically switching between “TSync 0” (System Time), “PPS 0” (System PPS) and one or more Stratum 1 servers.



Figure 36: “NTP Servers” tab (versions 4.8.5 and below)

- Edit the NTP Configuration file to change the PPS Clock Discipline driver to default to **Stratum 1** rather than **Stratum 0** and Submit. This ensures NTP Stratum remains at Stratum 2.

To edit the ntp.conf file, navigate to the **Network -> NTP Setup** page of the browser, “**General Settings**” tab. Enable “Expert Mode” and then switch to the “**Expert Mode**” tab. Edit the Stratum value (as shown in Figure 37) and then press Submit.

Edit this line to become “fudge 127.127.22.0 stratum 1”

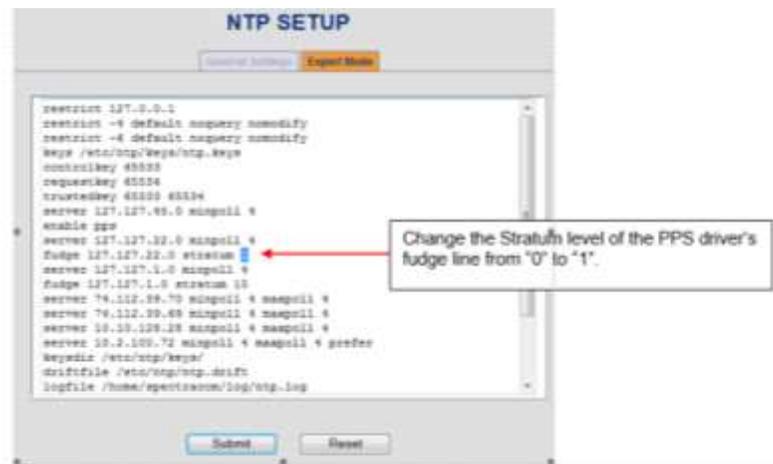


Figure 37: Edit Expert mode

Go to **Status -> NTP** page of the browser and wait for NTP Synchronization. The PPS Driver may be selected and deselected a few times as time goes on. It should remain the selected reference unless the NTP Stratum 2 reference selected changes from the Preferred to another one.

Note: NTP expert mode needs to remain enabled, once it's been manually edited. Disabling NTP Expert mode will reset any changes to the ntp.conf file that were made while in Expert Mode.

NTP INPUT STATUS

System	Selected Reference	Stratum	LI	Drift (ppm)	Offset (ppm)	Other (ppm)
Yes	System PPS	2	00	0.000	-0.073	0.000

NTP Selected Reference Status

System	Host	Ref ID	Stratum	Mode	Type	Auth. Source	Link (Host)	Peer Interval (Sec)	Reach	Offset (ppm)	Other (ppm)	TFOM (ppm)	
✓	System PPS	1-00-01-0	1	00	Client	Local	None	1	16	17	0.000	-0.073	0.000

NTP Reference Status

System	Host	Ref ID	Stratum	Mode	Type	Auth. Source	Link (Host)	Peer Interval (Sec)	Reach	Offset (ppm)	Other (ppm)	TFOM (ppm)	
---	System Time	PPS	16	00	Client	Local	None	2	16	177	0.000	4.543	0.000
✓	System PPS	1-00-01-0	1	00	Client	Local	None	2	16	17	0.000	-0.073	0.000
---	193.127.1.6	2-00-01-00	10	00	Client	Local	None	4	16	207	0.000	0.000	0.000
---	193.112.25.10	-GPS-	0	00	Client	External	None	0	16	207	0.000	-1.120	-1.910
---	193.112.25.10	-GPS-	0	00	Client	External	None	2	16	207	0.000	0.000	-1.120
---	193.112.25.10	-GPS-	0	00	Client	External	None	16	16	177	0.000	0.000	0.000
---	193.112.25.12	-GPS-	0	00	Client	External	None	2	16	207	0.000	0.000	0.000
---	Other	---	15	11	Master	Local	None	0	0	0	0.000	0.000	0.000

Figure 38: Status -> NTP page

- Navigate to the **Tools -> Logs** page of the browser and select the “NTP” log. **Error! Reference source not found.** shows an example of what you should observe if the above changes worked properly.

LOG FILES

Timestamps are in system time scale (UTC)

Time	Message
17 Jul 18 31:12:04	kernel time sync: enabled 0001
17 Jul 18 31:12:04	sync'ed to PPS01, stratum=1
17 Jul 18 30:12:04	sync'ed to 193.127.1.6, stratum=10
17 Jul 18 30:08:04	sync'ed to 193.112.25.10, stratum=0
17 Jul 18 30:07:04	kernel time sync: disabled 0001
17 Jul 18 30:07:04	sync'ed to LOCAL05, stratum=15
17 Jul 18 27:29:04	ppm exiting on signal %
17 Jul 18 25:52:04	sync'ed to PPS02, stratum=0
17 Jul 18 24:48:04	sync'ed to PPS01, stratum=1
17 Jul 18 22:53:04	kernel time sync: enabled 0001
17 Jul 18 21:48:04	kernel time sync: disabled 0001
17 Jul 18 21:48:04	sync'ed to LOCAL05, stratum=15

Figure 39: NTP log

Operation of this particular configuration:

With the exception of the information below, the operation of this example is the same as the operation listed in Example C.

In this configuration, the SecureSync’s internal oscillator will discipline to the external 1PPS input. The disciplining of the oscillator will cause the SecureSync’s output to follow the 1PPS input.

The alignment of the system 1PPS to this external input can be determined by the reported “TFOM” and “Phase Accuracy Error” values in the **Status /Time and Frequency** page of the browser. The lower these two values, the more closely aligned the System 1PPS is to the external 1PPS input. The following is a sample of these two values being reported:

TIME AND FREQUENCY STATUS	
Selected Time Reference Source	GPS 0
Selected 1PPS Reference Source	GPS 0
Synchronization	OK
Holdover	Not In Holdover
TFOM	3
Estimated Time Error (ETE)	10 ns < ETE <= 100 ns
Timescale Reference	UTC
Oscillator Type	OXC0 (1ppb)
Oscillator State	Lock
Phase Accuracy Error (ns)	5
Frequency Accuracy Error (Hz)	0.000200

Current TFOM value

Current Phase Accuracy Error

Figure 40: “Time and Frequency” page

Stopping and restarting NTP (Versions 4.8.9 and below)

Note: In software versions 5.0.0 and above, NTP automatically restarts after making changes to NTP configurations. It doesn’t need to be manually restarted for the changes to take effect.

With software versions 4.8.9 and below, in order for NTP to start using the configured NTP servers, NTP has to be manually stopped and restarted (or the unit rebooted). To stop and restart NTP, navigate to the **“General Settings”** tab on the **Network -> NTP Setup** page of the browser. Change the **“NTP Service”** drop-down to “Disabled” and hit Submit. Then, go back to the same tab and change the “NTP Service” drop-down to “Enabled” and hit Submit. NTP will now restart and will be re-synchronized within a few minutes.

Note: if one or more NTP Peers or Servers reports it’s “unreachable”, refer to: [Section 6: Troubleshooting](#)

Section 3: NTP Stratum Level reported to the network clients

SecureSync reports its current NTP Stratum level to its clients that are synchronizing to the SecureSync. When NTP has selected a Timing System input (such as GPS, IRIG or ASCII timecode) for it to synchronize with, SecureSync will indicate it's currently a Stratum 1 NTP time server. If instead, NTP has selected another NTP server to be its current reference, it will always report that it is one less Stratum level than the one NTP server it has selected for synchronization.

For example, GPS is the highest priority input to SecureSync and GPS is valid, SecureSync will report it is a Stratum 1 time server. If GPS or any other primary Timing System reference is not valid or not available, it can select another NTP server to be its time reference. If the NTP server it selects for its synchronization is another SecureSync that is synced to GPS, IRIG, ASCII time-code, etc. for example, this other NTP server will report to this SecureSync that it's Stratum 1, so this SecureSync will then report to its clients that it's a Stratum 2 NTP time server.

If the only available Time input reference is NTP, once NTP has been configured with other NTP servers (in the NTP servers tab) and has been restarted, the NTP Status page will indicate NTP is currently one less Stratum than its selected reference NTP server. Typically, the SecureSync is configured to sync to one or more other Stratum 1 NTP servers. In this configuration, the Status/ NTP page will indicate the SecureSync is a Stratum 2 time server, as shown below:

The current NTP Stratum is reported in:

- A) **Newer web browser:** Lower-left corner of the "Management" -> "NTP Setup" page (in the "NTP Status Summary" table).

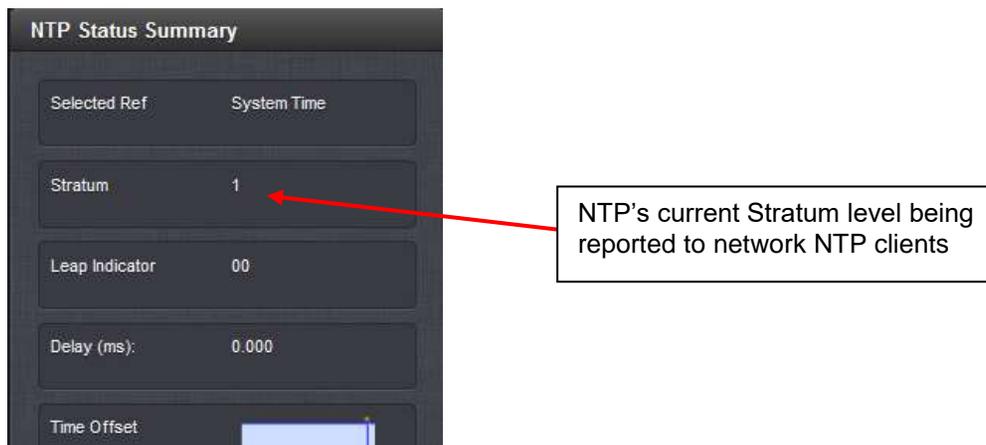


Figure 41: Management -> NTP Setup page (Archive versions 5.1.2 and above)

- B) **Classic interface:** Top of the Status -> NTP page. Note that it takes a few seconds for the NTP status data to be displayed"



Figure 42: Status -> NTP page (Archive versions 5.0.2 and below)

Note: If a SecureSync is configured to receive Time from only other NTP servers (“Host” is not enabled for manually set time and no valid inputs from GPS, IRIG, ASCII timecode, etc. are available), the highest NTP Stratum level it can ever be, is a Stratum 2 NTP time server.

Note: if one or more NTP Peers or Servers reports it’s “unreachable”, refer to: [Section 6: Troubleshooting](#)

Section 4: NTP Input and Output Status

Once other NTP time servers have been added to the NTP Peers or Servers tables and after NTP has been restarted, all of the configured NTP Peers and Servers can be viewed and the synchronization status of all of the configured time servers can be monitored.

A) NTP Input Status

SecureSync's System Time and NTP can be synced by many types of input references, including NTP from other NTP servers on the network, as desired.

The **“Reference Status”** table of the web browser will display all possible input references to System Time (including NTP input from other NTP servers) and the validity of each input reference.

1. Newer web browser (Archive Versions 5.1.2 and above)

The input Status table is located at the top right-side of the **“Home”** page of the browser.

REFERENCE	PRIORITY	STATUS	
GNSS 0	1	TIME (Green)	PPS (Green)
IRIG Input 0	2	TIME (Red)	PPS (Red)
Local System / PPS Input 0	3	TIME (Green)	PPS (Red)
Local System / Freq Input 0	4	TIME (Green)	PPS (Red)
NTP 1	5	TIME (Red)	PPS (Red)

Figure 43: Reference Status table (Home page)

Indication of whether NTP from one or more other time servers is valid and selected input to sync System Time.

- **“Time” and “PPS” both green** = NTP input from another NTP server is currently selected as the input reference to sync the System Time (note that NTP only remains “OK” when NTP is selected as the input for syncing System Time).
- **“Time” and/or “PPS” both red** = NTP input from another NTP server is not currently selected as the input reference to sync System Time (note that “Not Valid” does not necessarily indicate that other NTP servers aren't available for selection. “NTP” only remains “OK” when NTP is the selected input reference).

2. Classic web browser (Versions 5.0.2 and below)

The input Status table is located at the bottom of the **Status -> Time and Frequency**

Navigate to the **Status -> Time and Frequency** page of the web browser to access the “**Reference Status**” table (as shown below):

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

Indication of whether NTP from one or more other time servers is valid and selected input to sync System Time.

“**OK**” = NTP input from another NTP server is currently selected as the input reference to sync the System Time (note that NTP only remains “OK” when NTP is selected as the input for syncing System Time).

“**Not Valid**” = NTP input from another NTP server is not currently selected as the input reference to sync System Time (note that “Not Valid” does not necessarily indicate that other NTP servers aren’t available for selection. “NTP” only remains “OK” | when NTP is the selected input reference).

Figure 44: Reference Status table (“Status” -> “Time and Frequency” page)

NTP input validity

“NTP” (as well as “User”) is a unique input reference. Unlike other input references that provide data every second (such as GPS, IRIG, Stanag, etc), NTP only periodically obtains data from other configured NTP servers (based on the poll interval selected by NTP). Also, NTP can be both an input reference for System Time synchronization and an output to network NTP clients (However, it cannot be both an input and an output at the same time). NTP toggles between being an input reference for System Time synchronization and an output time reference for network synchronization.

In the Reference Status table, as long as other NTP servers are present and reachable, “NTP” validity will blink green for one second, every 60 seconds. Otherwise, it remains “Not Valid”, even if one or more other NTP servers are being successfully polled by NTP, unless NTP is selected as the input reference for syncing System Time. When other input references (such as GPS) are selected as the input reference, NTP Reference status will remain “Not Valid”.

Once NTP has been selected as the input reference for System Time synchronization (as configured in the Reference Priority table) and as long as at least one other NTP server is available on the network, the “NTP” Reference Status will switch from “Not Valid” to “OK”. It will then remain “OK”, unless a higher priority input reference becomes available. Then, it will go back to Not Valid” again.

Even though NTP is normally displayed as “Not Valid”, NTP inputs from other NTP servers are checked for validity once each minute, allowing NTP to become the selected reference, if all higher priority references are lost (it doesn’t have to wait to be re-qualified, when all other higher priority references are lost. Instead, it can switch over to NTP as the selected reference “right away”).

Note: NTP may periodically and temporarily select an NTP server (before switching back to the System Time reference, for example). In this scenario, “NTP” in the Reference Status table will momentarily be “OK” and then switch back to “Not Valid” again, because NTP is no longer synced to another NTP server.

B) NTP Output Status

The NTP Status of the web browser will display all available inputs to NTP and the status of its synchronization with each configured reference.

1. Newer web browser (Archive Versions 5.1.2 and above)

Navigate to the **Management -> NTP Status** page of the black/charcoal browser to view the **NTP Status Summary table**.

This table is in the lower-left corner of the page. The top of the table indicates the NTP Stratum value and LI bits being provided to the NTP clients and also reports the NTP offset and jitter within the time server.

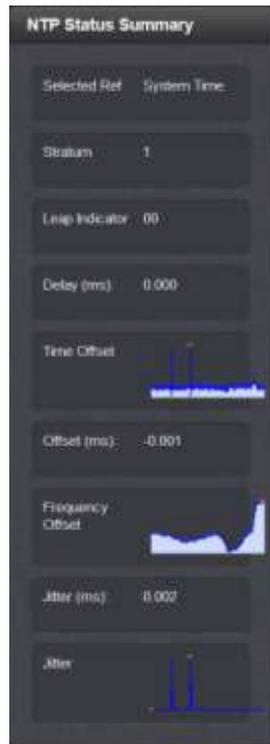


Figure 45: NTP Input/Output Status page (Versions 5.1.2 and above)

Status of all NTP's configured Peers and Servers

NTP can be provided a list of other NTP servers that it can sync to, but it can only choose one as its current selected reference. The NTP status page displays current information about the selected NTP server and the other configured NTP Peers and servers (such as reported Stratum level, sync status, jitter, offset, poll interval, etc) for any other configured NTP Peers and/or Servers that can be used as input time references for System Time synchronization.

In addition to the NTP Status Summary table the Setup page also consists of the **NTP Servers** and **NTP Peers** sections:

NTP Servers: A list of all configured references that SecureSync can sync with (such as the System Time and/or other NTP servers).

Note about listed NTP references in the Servers table

In addition to other NTP servers, you may notice other values also listed. Below is a list of values you may see listed in the NTP Servers table:

Reference clock driver (“127.127.45.0”): This NTP reference is a time input to NTP from NetClock’s System Time (as synced by external time references (such as GPS, IRIG havequick for examples). In Holdover mode, this time is being derived from the oscillator. This reference is only listed if the “Prefer Timing System Reference” checkbox (in the **Network / NTP** page of the browser, “**NTP Servers**” tab) is selected.

Atom clock/System PPS driver (“127.127.22.0”): This NTP reference is a 1PPS input to NTP, from NetClock’s System 1PPS (as synced by external 1PPS references, such as GPS, IRIG havequick or from an external 1PPS input signal for examples). This reference is only listed if the “Enable Timing System 1PPS Reference” checkbox (in the **Network / NTP** page of the browser, “**NTP Servers**” tab) is selected.

Local clock driver “127.127.1.0”: This NTP reference is the internal local clock, based on the OS kernel time. Having this clock driver enabled allows NTP to be able to go to Stratum 16 when NTP has no valid input to select. Stratum 16 keeps the network NTP clients from using it as a time reference.

NTP Peers: A list of all configured NTP servers that SecureSync can sync with.

Both the NTP Peers and NTP Servers sections consist of the following fields:

Ref ID: NTP Reference ID of the Reference/NTP server

Auth Status: Indicates if the selected reference is using MD5 authentication (“**None**” indicates authentication is not being used)

Last: The number of seconds it’s been since this reference was last polled for its time.

Poll: The interval (in seconds) that NTP is polling this reference.

Delay: The delay (in seconds) that it takes for the NTP packet to reach this reference.

Using several algorithms, NTP selects one of all of its available references to be its selected reference (factoring in items such as the current Stratum level of the input references, amount of jitter and offset for each reference, type of reference it is, etc),

Each of the listed references/NTP servers in these two tables have “color-coded lettering and are labeled” (in parenthesis) with their current status. Both the color-coding and labeling are based on a tally code that NTP applies to each reference depending on its algorithms and the reach value for each reference.

Color-coding of text

Please Note: NTP continues to monitor and evaluate each of its references and updates of each as it feels best. A reference in red at this moment may turn green at any time, if NTP determines it’s now a better reference than one that is currently green. Red does not indicate it won’t ever be selected for synchronization. Red just indicates NTP algorithms indicate the references in green are better at this particular moment.

Up two four references (NTP Servers and NTP peers combined) will be green at any given time. The rest will be inherently red. References that are “preferred are more likely to be green than those that are not “preferred”.

- A) **Green lettering:** Indicates NTP is receiving responses from this reference and it has passed all NTP algorithms needed for its selection. Any references in green can be selected for NTP’s synchronization.
- B) **Red lettering:** Indicates NTP is receiving at least some responses from this reference, but the reference has been currently ruled out for selection by NTP’s algorithms. Any references in red won’t currently be selected for NTP’s synchronization.

- C) **Yellow lettering:** Indicates NTP is not receiving any, or not all, responses from this NTP server, each time NTP polls this reference. Any references in yellow won't currently be selected for NTP's synchronization.

Note: If the entry continues to remain yellow after NTP has started, a network reach issue likely exists.

Labeling of each reference (value in parenthesis)

- A) **(Sync):** Indicates a reference that NTP can currently select for its synchronization.
- B) **(Not Sync):** Indicates a reference that is responding to polls, but NTP's algorithms have currently ruled out syncing with, as better references (in green text) are currently available. Note these references can become "Sync" at any time, as NTP continues to evaluate all of its available references.
- C) **(Initializing):** Indicates a reference that has a "reach" value of "0" because the reference has not yet responded to any polls. This reference may not be reachable on the network or may not be a useable reference.
- D) **(limited reach):** Indicates a reference that has a "reach" value of greater than "0" but less than "377" because some, but not all, of the polls of this reference have been successful. NTP packets may be colliding with others, the reference may be too busy at times which is preventing it from always being able to respond, or the time server may have recently become not reachable on the network.

2. Classic web browser (Versions 5.0.2 and below)

Click on the **Status -> NTP** page of the browser to access the NTP Status page.



Figure 46: NTP Input/Output Status page (Versions 5.0.2 and below)

Status of NTP's Peers and Servers

NTP can be provided a list of other NTP servers that it can sync to, but it can only choose one as its current selected reference. The NTP status page displays current information about the selected NTP server and the other configured NTP Peers and servers (such as reported Stratum level, sync status, jitter, offset, poll interval, etc.) for any other configured NTP Peers and/or Servers that can be used as input time references for System Time synchronization.

The NTP Status page consists of the following three sections:

NTP Status: The current status of SecureSync's NTP functionality.

NTP Selected Reference Status: Information about the reference that NTP has selected for its synchronization (The selected reference can be either SecureSync itself or another NTP server).

NTP Reference Status: Information on all available references that NTP can choose from for its synchronization (whether the reference is selected for synchronization, not currently selected, but is available for synchronization or has been disqualified for its synchronization).

“NTP Status” (Top section): Displays SecureSync’s current NTP status, including whether or not NTP is in sync, the current Stratum level being reported to the network, as well as its Delay, Offset and Jitter values (as compared to its selected input references). This section consists of the following fields:

Sync: Indicates if SecureSync is reporting to the network that NTP is in sync.

Selected Reference: Indicates what NTP is synchronized with for its reference. If NTP is internally synced to SecureSync’s internal System information “System Time” will initially be displayed and then it will switch to “System PPS” being displayed in this field. Otherwise, an IP address will be displayed in this field if NTP is synced with another NTP server instead.

Stratum: The NTP Stratum level being reported to the network. This value indicates “NTP hierarchy” and also determines if the network can use the NTP packets supplied by SecureSync for its synchronization.

- 1) When SecureSync is currently synced with its NTP input reference selected (or went into Holdover mode after losing its NTP reference), this value will be one less than SecureSync’s NTP reference. The clients on the network can use the SecureSync’s NTP packets for its synchronization.
- 2) When SecureSync is currently synced with any other reference selected (besides the NTP input reference) or SecureSync has since lost the reference and has gone into the Holdover mode, this value will indicate Stratum 1. The clients on the network can use the SecureSync’s NTP packets for synchronization.
- 3) When SecureSync is currently not synced with any of its input references and is not currently in Holdover mode, this value will indicate Stratum 16. Stratum 16 will cause the NTP clients to ignore the SecureSync’s NTP packets.

Delay: the measured one-way path delay (in milliseconds) between NTP and its selected reference (i.e. System Time).

Offset: The measured time difference (in milliseconds) between NTP and its selected reference (i.e. System Time).

Jitter: Variance (in milliseconds) occurring in the reference input time (from one poll to the next).

“NTP Selected Reference Status” (Middle section): Using several algorithms, NTP selects one of all of its available references to be its selected reference (factoring in items such as the current Stratum level of the input references, amount of jitter and offset for each reference, type of reference it is, etc).

Note: Each NTP server’s status line listed in this section of the Status page contains a “Reach” octal counter. The Reach Interval counter will start increasing in value each time SecureSync is able to contact and receive time data from that configured NTP Peer/Server. This number increasing to a max value of 377 indicates the other NTP server is reachable. After several minutes, if the NTP Peers or Servers Reach field remains a “0”, this configured NTP Peer is either unreachable or not available for NTP synchronization (It’s not on the same network, a firewall is blocking port 123, the other time reference isn’t really an NTP time server, the other NTP server is not in sync, etc).

This section displays information about the selected NTP Peer or Server that NTP is using as its reference, including the following fields:

Sync (“Tally Code”): a symbol that indicates if the listed reference is available for selection as a reference. The following table indicates the symbols and their meanings.

Symbol (Tally code)	Indication
*	The Selected Time reference
o	The Selected PPS reference
+	A high quality candidate for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected)
x	“ Falseticker ” Listed NTP Peer was discarded from selection (NTP won’t select this peer as its reference).
-	“ Outlier ” Listed NTP Peer was discarded from selection (NTP won’t select this peer as its reference).
(blank)	Source discarded: Failed Sanity check

Table 1: Sync column symbols

Host: Indicates what the selected NTP reference is synchronized with for its reference. If NTP is internally synced to SecureSync’s internal System information “System Time” or “System PPS” will be displayed in this field. Otherwise, an IP address will be displayed in this field if the NTP reference is synced with another NTP server.

Ref ID: The type of input reference (For example “GPS” indicates the reference can use GPS for its synchronization).

LOCL (Local): Listed reference is currently synced to itself (the listed reference has not yet synced to its reference yet).

GPS: The listed reference is a GPS-based type reference (such as another SecureSync).

PPS: The listed reference is a PPS (not a Time) reference for NTP.

STC (Serial Time Code): The listed reference is an ASCII data reference.

Stratum: The Stratum level of the selected input reference.

Mode: The mode of NTP operation, where:

Client: Indicates a Client/Server relation used when communicating with another reference that is configured as a “Server”.

INIT: Indicates the NTP mode of the reference has not yet been identified.

STEP: Indicates an initial time correction has been applied.

Symmetric Active: Indicates the listed reference is configured in SecureSync as an “NTP Peer”

Symmetric Passive: Indicates the listed reference is configured in SecureSync as an “NTP”.

DROP: The Reference identifier shows the word “**DROP**” in a “Peer” status. This occurs when two SecureSyncs are configured as NTP Peers, but when NTP started up on this SecureSync, only one of the two SecureSyncs was in sync while the other was not in sync. If both SecureSyncs don’t start out at the same stratum value (such as Stratum 1), peering doesn’t work.

If the GPS antenna or other input reference is not connected for instance and it’s not synced, do not configure each other as peers. Instead, list the one that is synced as a NTP server in the “Servers” table of the other unit that is not synced to a reference. Then

restart NTP. Example below:

Site A (GPS Antenna attached)

NTP Reference Status:

Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (mS)	Offset (mS)	Jitter (mS)
*	Spectracom	GPS	0	Client	local	none	65	64	377	0.000	0.003	0.002
	172.20.75.10	LCL	16	Symmetric Active	unicast	none	12	128	0	0.000	0.000	4000.000

Site B (No GPS Antenna)

NTP Reference Status:

Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (mS)	Offset (mS)	Jitter (mS)
	Spectracom	LCL	0	Client	local	none	0	16	0	0.000	0.000	4000.000
	172.23.75.10	DROP	16	Symmetric Active	unicast	none	0	16	0	0.000	0.000	4000.000

Figure 47: “DROP” Ref ID

Type: “local” indicates NTP generated internal to SecureSync. “Unicast” indicates NTP received over the network.

Auth Status: Indicates if the selected reference is using MD5 authentication. “None” indicates authentication not being used.

Last: The number of seconds it’s been since this reference was last polled for its time.

Poll Interval: How often SecureSync is polling this NTP reference for its time.

Reach: An octal counter that indicates how many of the last eight polls of the NTP server were successful (A reach value of “377” indicates all eight of the last eight polls were successful).

Note: If the Reach value remains at “0” for a longer duration than the displayed “Poll Interval”, NTP may not be running in SecureSync, there may be a network issue between SecureSync and the other NTP reference or the configured reference is not able to provide NTP packets to SecureSync.

Delay: The measured one-way delay between SecureSync and its selected reference.

Offset: The measured time difference between SecureSync and its selected reference.

Jitter: Variance in the reference inputs time from one poll to the next.

“NTP Reference Status” (Bottom section):

This table provides all of the same information as the Selected Reference Status table, but in addition to the selected reference, it also lists all internal references and of the other configured Peers and Servers that that NTP has available to choose from, as its selected input reference for synchronization.

Notes about listed NTP references:

If any other NTP servers on the network have been listed in either the NTP Servers or NTP Peers tabs (**Network / NTP setup** page of the browser) they will be listed in this table. In addition to these other NTP servers, you may notice other values also listed. Below is a list of values you may see (as indicated, not all of these values will always be displayed). Some of these are based on how NTP has been configured in the **Network / NTP setup** page of the browser.

Reference clock driver (“127.127.45.0”): This NTP reference is a time input to NTP from SecureSync’s System Time (as synced by external time references (such as GPS, IRIG havequick for examples). In Holdover mode, this time is being derived from the oscillator. This reference is only listed if the “Prefer Timing System Reference” checkbox (in the **Network / NTP** page of the browser, “**NTP Servers**” tab) is selected.

Atom clock/System PPS driver (“127.127.22.0”): This NTP reference is a 1PPS input to NTP, from SecureSync’s System 1PPS (as synced by external 1PPS references, such as GPS, IRIG havequick or from an external 1PPS input signal for examples). This reference is only listed if the “Enable Timing System 1PPS Reference” checkbox (in the **Network / NTP** page of the browser, “**NTP Servers**” tab) is selected.

Local clock driver “127.127.1.0”: This NTP reference is the internal local clock, based on the OS kernel time. Having this clock driver enabled allows NTP to be able to go to Stratum 16 when NTP has no valid input to select. Stratum 16 keeps the network clients from using it as a time reference.

For more information on NTP peering or NTP operation in general, please refer to the NTP website of <http://www.ntp.org/>.

NTP graphs (Applicable to software versions 5.1.2 and above only)

Note Clicking on the small graphs in the NTP Status Summary section will cause the graph to expand in a new window (as shown below). This allows the ability to examine the NTP graphs in greater detail.



Figure 48: Expanded NTP graph (Versions 5.1.2 and above)

Vertical scale of NTP graph (nanoseconds)

The vertical scale varies depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as 2e-06).

The scientific breakdown is as follows:

1e-09	=	1 ns	(or 0.000000001 seconds)
1e-08	=	10 ns	(or 0.00000001 seconds)
1e-07	=	100 ns	(or 0.0000001 seconds)
1e-06	=	1 microsecond	(or 0.000001 seconds)
1e-05	=	10 microseconds	(or 0.00001 seconds)
1e-04	=	100 microseconds	(or 0.001 seconds)
1e-03	=	1 millisecond	(or 0.001 seconds)
1e-02	=	10 milliseconds	(or 0.01 seconds)
1e-01	=	100 milliseconds	(or 0.1 seconds)
1e+00	=	1 second	(or 1.000 seconds)
1e+01	=	10 Seconds	(or 10.000 seconds)
1e+02	=	100 Seconds	(or 100.000 seconds)
1e+03	=	1000 Seconds	(or 1000.000 seconds)

Note: If the first digit isn't a "1", multiply the first digit by the "time" value in the table above

Examples

2e-05= 20 microseconds or 0000.000020000 ("2" times "10 microseconds" is 20 microseconds)

5e-06= 5 microseconds or 0000.000050000 ("5" times "1 microsecond" is 5 microseconds)

Section 5: System's 1PPS/on-time point and internal 10 MHz Oscillator disciplining when syncing via NTP input

A) The System Time/on-time point when syncing SecureSync via NTP

When syncing the SecureSync via NTP, keep in mind that the SecureSync's on-time point will be offset from the on-time point of its selected NTP server. The SecureSync's 1PPS output (the base unit's 1PPS output and/or installed Option Card 1PPS outputs) as well as the on-time point for the SecureSync's outputs (such as NTP, ASCII outputs, IRIG outputs, etc) will be offset from the 1PPS on-time point of its selected NTP reference. The actual amount of offset between the SecureSync and its selected NTP server will be based on network topography plus inherent internal NTP synchronization processing delays.

NTP does not have an accuracy specification. However, the offset between an NTP server and NTP client on the same subnet is typically 1 to 10 milliseconds. There are many factors that can affect how accurately an NTP server can sync its NTP clients (such as the SecureSync when it's synced to another NTP server) and therefore the time offset between them. One of the biggest factors of this time offset is the number of network hops between the NTP server and its NTP clients. The more hops in between, the more likely there will be a larger offset between the NTP server and its clients.

The processing delay for NTP synchronization in this SecureSync is approximately 1 millisecond. This is the minimum offset between this NTP server and its selected NTP server, when syncing it via NTP. The actual offset will be this processing delay plus the offset based on performance of NTP on this particular network. (Note that NTP in networks with many hops located between the NTP server and its NTP clients can be measured in the tens of milliseconds).

To minimize the time offsets and on-time points between the SecureSync and its selected NTP server, we recommend the NTP server be located on the subnet as the SecureSync (thus minimizing the number of network hops in between).

B) 10MHz output disciplining

Unlike input references such as either GPS or IRIG, NTP (as well as manually set time) cannot provide the SecureSync with a very stable 1PPS that can be used to discipline its internal oscillator. When syncing the SecureSync via NTP (NTP Peering mode), the internal oscillator will remain in the oscillator free-run mode.

The System Time/System on-time point will be maintained by the NTP input. However, the oscillator's 10 MHz output will not be disciplined to the NTP input. If the oscillator was being disciplined by another input reference (such as GPS or IRIG input, for instance) but the Reference Priority table has since selected NTP as the input reference because the other reference(s) have been lost or declared not valid, the internal oscillator will begin to drift from the last known D/A value. It will not be steered to the desired 10MHz frequency again, until another input reference (other than NTP or manually set time) has been re-selected. Then, the oscillator disciplining will resume.

If the oscillator wasn't being disciplined by another input reference (such as GPS or IRIG input, for instance) since it was last powered-up the internal oscillator will begin to drift without ever being disciplined to 10MHz. The internal oscillator will not be steered to the desired 10MHz frequency, until another higher priority input reference (other than NTP or manually set time) has been selected.

This is only a factor when it's desired to use the 10 MHz output from the base unit, or from an installed Option Card. When it's desired to provide a very stable and accurate 10 MHz output to other equipment, the SecureSync should not be synced to NTP (or the time just manually set with no other references such as GPS or IRIG being available).

If it's desired to use NTP as the Time input and still be able to provide a disciplined 10 MHz output, the NTP Time input should preferably be combined with an external 1PPS input from an external reference. Refer to [Section 2A](#) (Example Use Case "D") for more information on this scenario. Note that a 1PPS input Option Card may be required for this particular application.

Section 6: Troubleshooting

Troubleshooting NTP conditions which may occur:

1) NTP peering with other NTP servers /NTP synchronization with NTP clients work fine without Symmetric Key authentication enabled, but not working with Symmetric Key enabled

- Make sure all Symmetric keys (in NTP servers and NT clients) have been annotated as “Trusted” keys

A) NTP Authentication failures (“bad” or “none” instead of “ok”)



IP/HOST	REF ID	AUTH STATUS	LAST
10.133.12.150 (NOT IN SYNC)	172.30.133.149	ok	1
172.30.170.150 (NOT IN SYNC)	172.30.133.149	bad	6

“Auth Status”

Note: “Auth Status” is only updated when NTP first starts-up.

- “**none**”: Indicates authentication is not being used (no key has been specified in the specified peer/server in **Management** -> **NTP Setup** page)
- “**bad**”: Indicates authentication is being used, but the authentication failed when NTP last started-up
- Either no key ID or the wrong key ID may have been specified in the specified peer/server in Management -> NTP Setup page of one or more units.
- The selected key may not have been selected as “**trusted**” in the “Symmetric Keys” table
- The selected key in the “Symmetric Keys” table may not match the same key in the other’s ntp.keys table.

Troubleshooting Auth failures

- With the original web browser design (versions prior to 5.1.0) do not use characters such as a “\$” (dollar sign). MD5 won’t work. (See note further below)
 1. Get the logs and especially the config files from both units.
 2. View the **ntp.conf** file from both units:

A) Make sure the selected key is trusted on both units (as specified next to “trustedkey”)

Example: trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534

- 1) Make sure a key for each other (peers or servers) is selected and it’s the same number specified on both units.

Specific example below of where the customer only specified a key on one but not the other (notice the second red line does not contain the word “key” so the key hadn’t been specified in the Management->NTP Setup page. I had verified from both configs that both are supposed to be using key 2

```
mantp
trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534
```

```
peer 10.133.12.150 key 2 minpoll 3 maxpoll 3
peer 172.30.170.150 key 2 minpoll 3 maxpoll 3 (auth was reported as "bad")
server 172.18.33.191 key 2 minpoll 3 maxpoll 3
server 172.22.115.45 key 2 minpoll 3 maxpoll 3
server 10.153.36.191 key 2 minpoll 3 maxpoll 3
server 172.30.133.149 key 2 minpoll 3 maxpoll 3
keysdir /etc/ntp/keys/
```

sdcntp201

```
trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534
peer 10.133.12.150 key 2 minpoll 3 maxpoll 3
server 172.18.33.191 key 2 minpoll 3 maxpoll 3
server 172.22.115.45 key 2 minpoll 3 maxpoll 3
server 10.153.36.191 key 2 minpoll 3 maxpoll 3
server 172.30.133.149 key 2 minpoll 3 maxpoll 3
peer 10.133.10.150 minpoll 3 maxpoll 3 (auth was reported as "none") (notice the phrase "key 2" is
missing from this line)
```

- 2) View the **ntp.keys** file in both config files to make sure the specified key matches verbatim the key of the other unit,

A) Issue with MD5 authentication not working with clients after updating from version 4.8.9 (NTP version 4.2.0) to versions 5.x.x (NTP version 4.2.6p5)

- Refer to Mantis case 2756 (http://cvsmantis.int.rolia.com/mantis/view_all_bug_page.php)
- Also refer to Salesforce case 13501 for Paul Lindblad.
- Internal Knowledge article: <https://na8.salesforce.com/ka0C0000000L6H1>.
- He needed to edit Management -> NTP Setup, "Access Restrictions" after updating to archive version 5.x.x.

Our clients are now seeing the upgraded NTP server. I went to management /NTP setup/Access restrictions It seemed to be messed up. When I looked at it in the classic interface it looked OK. On the new GUI interface in the IP address column there were "-4"s I decided to change the IP in one column. When I did, all columns changed to that IP address. Then I tried to change the mask in one column. All columns changed to that mask. So I just deleted them all and manually typed the correct info in, one by one. This worked OK except for the fact that the IP version column kept wanting to say IPv6. I had to change this back to IPv4 on several of them. It seems stable now and the clients are seeing the NTP server.

B) MD5 authentication not working with non-ASCII characters (Applicable to classic web browser design only, versions 5.0.2 and below)

Note: Update to at least version 5.1.2 (new browser) for non-ASCII characters.

In classic interface web browser- Do not use symbols such as the "\$" (dollar sign). The browser will accept the characters but it will prevent authentication from working at all. This is a limitation of the browser and not a limitation of NTP/MD5. Engineering believes the new web browser handles all characters correctly

2) NTP Servers and/or NTP Peers tables (Management -> NTP Setup page) is not reporting/displaying NTP server(s) which have already been added to/configured in these tables.

For simplicity of the status info in the NTP Setup page of the browser, the “NTP Servers” and the “NTP Peers” status tables don’t display other NTP servers which have not yet been reachable over the network (their “Reach” value is still “0”).

If one or more servers have been added/configured, but aren’t being displayed in the status tables:

- 1) Very recently (within the last couple minutes or so) NTP was just restarted/the unit just rebooted.
- 2) The server(s) not being displayed in the table aren’t reachable over the network.
- 3) The server(s) not being displayed in the table is reachable over the network, but is not currently able to provide useable time data (its NTP may be at Stratum 16, for instance)

If the server(s) not being displayed are Internet NTP Time servers, there may be network/routing issues, or **UDP port 123** may be closed to the Internet (not allowing NTP packets through).

See info further below on using the CLI interface commands **ntpq -p** and **traceroute** to help troubleshoot this condition.

3) NTP Peer or NTP Server is “unreachable”

If one or more NTP Peers or NTP servers isn’t reachable by the SecureSync through the network, this indicates the configured main default port/default gateway (such as either eth0 or eth1 for examples) in the SecureSync may not be configured correctly, or there may a network issue likely occurring between the two NTP time servers. In the case of free Internet time servers, it can also indicate there may be restrictions in place on using this time server.

Restrictions on use of free Internet NTP servers: Be aware that NTP time servers on the Internet may have special rules/restrictions on their use, such as:

- A) How often NTP clients can query/poll them (a factor of the server’s minpoll interval, as configured in the **Management -> NTP Setup** page of the browser). The minpoll interval for that particular NTP server may need to be increased to prevent the SecureSync from polling it too often.
- B) Limitations on what geographical areas are allowed to use this particular NTP server.

These restrictions may potentially cause periodic or complete loss of its NTP time stamps. Refer to any applicable websites for the Internet NTP servers to see if they have any restrictions in place for their use.

Note that the main default port/gateway address needs to be configured as the correct ethernet interface and the associated proper gateway address that the NTP packets need to go through to reach the subnet this TP peer is on. If eth0 is connected to the router that the packets need to go through to get to this other subnet, the main default interface needs to be configured as eth0. For more info on configuring the main default port/gateway address, refer to: [Configuring the Default Port and Default Gateway address](#)

If you need additional assistance confirming there is an issue with the network (external to the SecureSync), please perform network packet captures (performed on the same side of the switch) for every network connection between the SecureSync and your network. If you would like to minimize the number of packets in each capture, filter each capture for it to show all packets on port 123. Make sure to run the packet capture for several minutes,

To analyze the packet captures, verify there are NTP packets with a destination address of the unreachable NTP peer being sent every few seconds (likely every 8 seconds) on one of the ethernet interfaces connected to your network. If the subnets this unreachable NTP peer is on, is an immediate subnet (connected directly to the SecureSync), this is the port which should show NTP packets being sent to that address every few seconds.

But if the subnet the unreachable NTP peer/server is connected with, is not on an immediate subnet that the SecureSync is directly connected with, the NTP packets having the destination address of the unreachable peer will be

in the capture on the default port (as discussed above). After confirming the NTP packets (port 123) are being sent out the SecureSync, verify the network routing of port 123 from there to the unreachable NTP peer.

Note that in lieu of performing Wireshark packet captures on each network connection from the SecureSync, you can optionally perform tcpdump captures for port 123 for each interface, via the SecureSync's CLI interface (filtered for port 123). See info further below pertaining to performing tcpdump.

Steps to help Troubleshoot NTP issues

A) “`ntpq -p / ntpq -pn`” and `traceroute` CLI commands

NTP has an available query tool (called `ntpq`) which allows status info of NTPs time references/time servers to be reported.

After logging into the CLI interface (via a telnet/ssh session) type `ntpq -p`<enter> (or `ntpq -pn`<enter>). As shown below, the response will list all configured NTP Servers and NTP peers, along with info on each Server/Peer:

```
spectracom NetOS version 3.0.0
spadmin@Spectracom ~ $ ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
-----
*PCI_TSYNC(0)       .GPS.         0 1  2   8  377   0.000  -0.024  0.004
bPPS(0)            .GPS.         0 1  1   8  377   0.000  -0.038  0.004
+128.252.19.1       .GPS.         1 u  5   8  377  30.850  3.854  0.324
+193.170.62.252    131.188.3.220 2 u  5   8  377 104.458 -1.662  0.360
spadmin@Spectracom ~ $
```

Except for the first couple minutes after NTP is restarted/the unit booted-up, the “**reach**” column (red circle above) value for each NTP server should normally be “**377**”, indicating that of the last eight polls/time requests sent to that server, successful time stamps were received back for all eight requests. Reach values “**376**” or below indicate at least one of the last eight time requests did not result in a response being received back from that server. A Reach value of “**0**” indicates none of the last eight time requests sent resulted in a response back to this unit.

Reach values **between** “**376**” (one missed response) and “**0**” (all eight last responses missed) indicate the NTP sever at this address may be too busy to respond to all the requests its receiving (a common occurrence with Internet time servers), or the server at this address is not reachable over the network from this unit.

Use the `traceroute` cli command to see if/where NTP requests/responses may not be getting through the network.

Traceroute cli command

at the CLO prompt. type: `traceroute -p 123 xxxx` (where “`-p 123`” defines NTP port of port 123, and where “`xxxx`” is the IP/hostname of the peer/server). The command should respond with list of nodes all the way to the peer/server

Example:

`traceroute -p 123 time.spectracomcorp.com` As shown below, verify the last value is **74.112.39.70** is followed by “**reached**” at the end of the line:

```
Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
1?: [LOCALHOST] pmtu 1500
1: 10.2.1.1 2.353ms
1: 10.2.1.1 2.239ms
2: 74.112.39.70 2.165ms reached
Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $
```

Example of a destination address not being available via port 123 (“send failed” to a bad address)

```
spadmin@Spectracom ~ $ tracepath -p 123 10.1.2.8
1: send failed
Resume: pmtu 65535
spadmin@Spectracom ~ $
```

If the “refID” field for a particular peer/server is remaining “.init” (and its “Reach” remains “0”)

```

address      ref clock      st  when  poll reach  delay  offset
10.164.60.200 .INIT.         16   -    1024    0  0.000  0.000
167.164.200.11 167.164.171.152 2    874  1024  377  0.000 -0.748
167.164.200.12 157.154.12.10  2    754  1024  377  1.000 -0.852
  
```

- Indicates the NTP mode of the particular peer/server has not yet been identified
- Indicates NTP is trying to reach the reference for the first time, but can't initiate communications with this reference.
- The refID should only remain “.INIT” until after the initial NTP packet is received from the configured peer/server

Most likely causes for the refID value not to change from “INIT”

- The default gateway/port is not configured or not configured correctly (if the optional Model 1204-06 GB ethernet Option Card is installed)
- There is a network issue with UDP port 123 being closed on a firewall
- **NTP Access restriction** has been configured (in this SecureSync and/or its applicable peer/server) to restrict NTP from providing NTP packets to certain NTP nodes on the network.
- **NTP symmetric key is being enforced**, but not correctly configured in all associated NTP devices (preventing authentication from being successful, so NTP packets can't be exchanged)

To troubleshoot “.init” refID not changing shortly after NTP has started

3. Verify the peer/server is a valid NTP server that is known to be up and running.
4. Is the “INIT” peer/server able to sync any other NTP clients on its immediate subnet?
5. Does the “INIT” peer/server respond to ping?
6. is **UDP port 123** open on any/all firewalls in between the NTP devices
7. Perform a **tracert -p 123 xxx.xxx.xxx** CLI command from this time server to the “INIT” peer/server
8. Check if optional NTP Restriction has been configured

Note: For more info on NTP Access Restriction, refer to the online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_AccsRestrict.htm

9. Check if **NTP Symmetric key authentication** is being enforced in either SecureSync

Note: For more info on NTP Symmetric key authentication and its configuration, refer to the online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/NTP_ConfSymmKeys.htm and <http://manuals.spectracom.com/SS/Content/Global/Topics/NTP/ConfNTPsymmKeys.htm>

in summary of the online user guide, to determine if a SecureSync requires successful symmetric key authentication, on the left side of the **Management** -> **NTP Setup** page of the browser, click the “**Access Restrictions**” button. In the pop-up window, see if there is a “1” in the first row (for “IP4”), for the “Auth **Only**” column (as shown below)



Details of verifying NTP symmetric key authentication (especially if network issues have been ruled-out)

If a peer/server is remaining "INIT" and its reach is remaining "0" (and network port 123 is port is open) there is likely a symmetric key configuration mis-match between this SecureSync and its peer/server remaining "INIT".

If this SecureSync has been configured to require NTP authentication (not the factory default state), and its peer(s) is not configured with an identical keystring, this will prevent the time servers from peering to each other, as being observed.

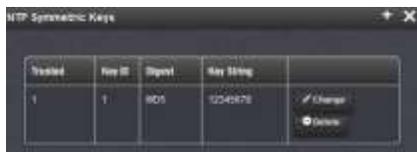
To determine if a SecureSync and/or its peer requires successful symmetric key authentication, on the left side of the **Management -> NTP Setup** page of the browser, click the **"Access Restrictions"** button. In the pop-up window, see if there is a **"1"** in the first row (for "IP4"), for the **"Auth Only"** column (as shown below):



Type	IP Version	IP	IP Mask	Auth Only	Control Query	
Allow	IPv4	default		1		Change Submit
Allow	IPv6	default				Change Submit

If this "Auth Only" field is blank, this SecureSync doesn't require successful authentication in order to exchange NTP packets with other NTP clients/other SecureSyncs. But if there is a "1" in the field (as shown above) symmetric key is being enforced and so it will only exchange NTP packets with other devices which are configured with an identical keystring.

Next, to see what trusted symmetric keys, if any, have been added to this SecureSync and other NTP servers/peers desired to be peered together (make sure to also verify the NTP auth key in every NTP client you wish to sync to the SecureSync or it won't be able to sync to this SecureSync), click the **"Symmetric Key"** button, also on the left side of the **Management -> NTP setup** page. The pop-up table will be empty if there are no keys configured. Or it will list a key ID, digest and a keystring, for each configured key



Trusted	Key ID	Digest	Key String	
<input checked="" type="checkbox"/>	1	MD5	12345678	Change Submit

For authentication to be successful between an NTP server requiring authentication and another NTP device, the Key IDs don't have to match (they can, though it's not necessary), but:

the keystring on both NTP devices HAVE to be IDENTICAL

the Trusted checkbox needs to be selected (which will place a "1" in the Trusted field for each key listed in the SecureSync)

if the Keys table for the SecureSync requiring auth has at least one key in it and its marked as Trusted, but the other NTP server has no keys listed, none of the keystrings is identical and/or a key with a matching string isn't marked as trusted, this is the problem. You will need to either create a new key having the trusted box selected and a matching keystring, or edit an existing incorrect key to make it a trusted/matching key.

To add a new Symmetric key to the SecureSync, press the **"+"** sign in the upper-right corner of the "symmetric key table" (after pressing the **Symmetric keys** button on the left side of the NTP Setup page). The pop-up will initially look like the following screenshot.

Select the Trusted box, enter an arbitrary Key ID Number (such as 45 for example), match the Digest Scheme selected in all the other servers/peers, and enter the identical key string entered in the desired peer/server. Then press Submit. Note more than one Symmetric key, with different digests/key strings can be added).



Note that many Cisco switches use MD5 for the Message Digest, but SecureSyncs also optionally support several other digests, also (such as SHA and SHA1 for examples)

B) `tcpdump` for NTP packets on each interface of the SecureSync

Login to the CLI interface using a telnet/ssh session.

Notes:

- 1) If the SecureSync's software version (use the `version` CLI command to check the current version installed) is version 5.4.1 or below, also type "`sudo`" in front of every '`tcpdump`' command referenced below: (such as "`sudo tcpdump`"). For versions 5.4.5 and above, there is no need to type 'sudo' before each command.
- 2) Use **CTRL + C** to stop a capture in progress
- 3) The 'letter' after "`tcpdump`" in each command below is a lower-case letter 'l' (as in "eye". It's not the letter L)

Type the following command (substitute the letter '`x`' with the desired SecureSync port/ethernet interface number) to start showing NTP packets to and from this interface.

`tcpdump -i ethx port 123` <enter> (where "`x`" is the ethernet interface to perform the capture of, such as "0" for eth0)

Specific examples, type or copy/paste the commands below in green:

Type: `tcpdump -i eth0 port 123`<enter> to see all NTP packets on **eth0** (**CTRL + C** to stop a capture in progress)

```

spadmin@Spectracom ~ $ tcpdump -i eth0 port 123
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:53:40.486808 IP 10.2.192.226.ntp > 10.2.192.227.ntp: NTPv4, symmetric active,
length 48
20:53:40.829681 IP 10.2.192.231.ntp > 10.2.192.226.ntp: NTPv3, Client, length 48
20:53:40.830646 IP 10.2.192.226.ntp > 10.2.192.231.ntp: NTPv3, Server, length 48
20:53:40.881542 IP 10.2.192.231.ntp > 10.2.192.226.ntp: NTPv3, Client, length 48
20:53:40.881940 IP 10.2.192.226.ntp > 10.2.192.231.ntp: NTPv3, Server, length 48
20:53:42.097529 IP 10.2.192.231.ntp > 10.2.192.226.ntp: NTPv3, Client, length 48
20:53:42.097966 IP 10.2.192.226.ntp > 10.2.192.231.ntp: NTPv3, Server, length 48
20:53:42.149526 IP 10.2.192.231.ntp > 10.2.192.226.ntp: NTPv3, Client, length 48
20:53:42.149849 IP 10.2.192.226.ntp > 10.2.192.231.ntp: NTPv3, Server, length 48
20:53:43.071812 IP 10.2.192.227.ntp > 10.2.192.226.ntp: NTPv4, symmetric active,
length 48
20:53:43.285031 IP 10.2.192.231.ntp > 10.2.192.226.ntp: NTPv3, Client, length 48
20:53:43.285438 IP 10.2.192.226.ntp > 10.2.192.231.ntp: NTPv3, Server, length 48
20:53:43.335701 IP 10.2.192.231.ntp > 10.2.192.226.ntp: NTPv3, Client, length 48
20:53:43.336095 IP 10.2.192.226.ntp > 10.2.192.231.ntp: NTPv3, Server, length 48
^C
14 packets captured
16 packets received by filter
0 packets dropped by kernel
spadmin@Spectracom ~ $

```

Type: `tcpdump -i eth1 port 123`<enter> to see all NTP packets on **eth1** (**CTRL + C** to stop a capture in progress)

Type: `tcpdump -i eth2 port 123`<enter> to see all NTP packets on **eth2** (**CTRL + C** to stop a capture in progress)

Type: `tcpdump -i eth3 port 123`<enter> to see all NTP packets on **eth3** (**CTRL + C** to stop a capture in progress)

Please confirm that you see NTP packets to the IP address of the unreachable host, in one of the four commands performed above. The port number they are observed on will let you know the start of the NTP packets being present out of the time server. the port 1234 packets are then likely being lost somewhere between that connection and the unreachable NTP time server.

For more information on NTP peering or NTP operation in general, please refer to the NTP website of <http://www.ntp.org/>.

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