Software Version 5.9.2: Release Notes

Orolia (Spectracom) released a software update for NetClock 9400 Series Products. Customers can download this software update at no charge from the Orolia website (see How to download and install the new SW.) This software update will upgrade the unit's system software to **Version 5.9.2**.

This update provides added benefits through new features, enhancements to existing functionality, as well as software fixes and security updates, as described in this document.

For your convenience, older 5.x legacy releases are also described in this document, while release notes for 4.x releases are described in the document *Release Notes for SecureSync System software updates up to and including Version 4.8.9*, which is available on the Orolia website.

***Note**: If the System Software running on your unit is older than **Version 5.0.2**, the upgrade to the latest Version may require additional steps – for details, see the **Upgrade Instructions** (> How to download and install the new SW).*

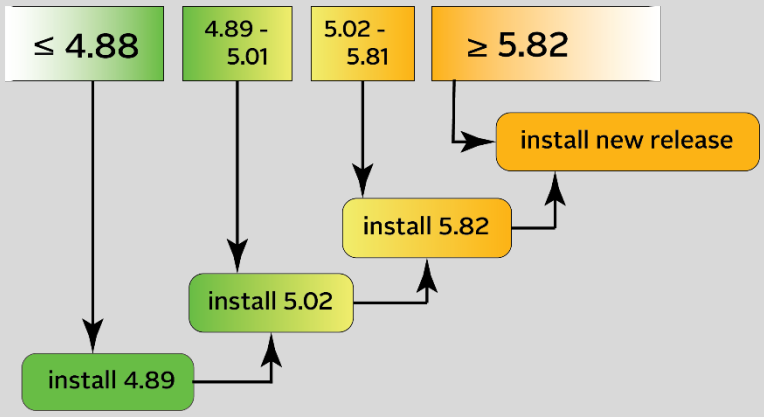

Table of Contents

Version 5.9.2

Enhancements and fixes

The following defects were corrected:

- Fixed the ZDA NMEA format to allow it to be used as valid reference.
- Fixed a Known Issue (v5.9.1) where `ping` and `arping` were unavailable to customers. The `arping` command now requires *sudo* permission.
- Repaired the calibrate button on the Oscillator Disciplining page of the Web UI.

Security enhancements and fixes

- Corrected a CSRF vulnerability found in the Web UI.

Known Issues

In this software version as well as the previous version (5.9.1), the recommended Upgrade Path has changed

Version 5.9.1

Enhancements and fixes

The following defects were corrected:

- Fixed a Known Issue from the previous release: the “Clean and Halt” command does not function properly when logged into SSH.
  This issue was found to extend to the `clean` as well as `clean and halt` commands and is not related to an SSH login. The issue caused them to intermittently not fully reboot or halt when issued through the CLI, Web UI, or front panel.

Known Issues

- Due to security policy changes in the Linux system, the `ping` and `arping` commands are currently not able to be executed by customers. This will be corrected in a subsequent release.

BroadShield customer note: The installation patch released in software version 5.9.0 does NOT persist across upgrades. If you have a BroadShield patch installed, you will need to re-apply that patch after upgrading to restore functionality.

All current BroadShield customers will require the new patch (BroadShield version 5.7.6) when installing 5.9.0 or higher. The old BroadShield patch (BroadShield version 5.2.2) is not compatible with software beyond this point.
BroadShield licenses are not affected by software upgrades.

Version 5.9.0

Newly released features

- Release 5.9.0 provides the ability to manage independently a license for jamming detection and/or a license for both jamming and spoofing detection (as part of Orolia's Interference Detection and Mitigation Suite) in support of various commercial offers.

Enhancements and fixes

The following improvements were applied to existing features and functions:

- Enacted security improvements, including upgrading several packages:
  - Upgraded NTP to 4.2.8p14
  - Upgraded PHP to 7.4.6
  - Upgraded Apache to version 2.4.41
  - Upgraded OpenSSL to version 1.0.2u.
  - Upgraded Broadshield to version 5.7.6
- Added a No Privacy option to SNMPv3 settings.
- Removed support of the Classic Web UI to increase security.

The following defects were corrected:

- Fixed errors in the loading of the journal log when configuring the unit via the front panel.
- Aligned all changes in the Web UI to look identical in journal log entries.
- Added a Quick Align option to automatically restart tracking when the unit enters holdover.
- Repaired password reuse limitation to cap reuse failures at 10 attempts
- Limited public key creation in SSH to each user, in order to increase security
- Created hard-coded SSH timeout, set to 60 minutes (previous timeout was nonfunctional).
- Fixed an issue in which Remote Logging could not be disabled.
- Corrected a Known Issue in software version 5.8.9 with saved configurations not being restored following updates.
- Enabled NTP to add an IPv6 address
- Repaired NMEA GGA zero-fill messages to ensure HDOP values are filled with 0.00 when a GPS reference is not present, rather than an arbitrary value
- Fixed a visual bug within the graphs in the Web UI page on Ethernet Monitoring.
- Corrected an inconsistency with NTP dir permissions between an upgrade and a fresh install

Security enhancements and fixes

Upgrades of multiple packages resulted in the following resolved security vulnerabilities:

Apache was updated to 2.4.41, resolving:

- CVE-2014-3581, CVE-2014-3583, CVE-2015-3183, CVE-2016-0736, CVE-2016-1546, CVE-2016-2161, CVE-2016-4979, CVE-2016-5387, CVE-2016-8740, CVE-2016-8743, CVE-2018-17189, CVE-2018-17190, CVE-2018-17199, CVE-2019-0190, CVE-2019-0211, CVE-2019-9517, CVE-2019-10081, CVE-2019-10082, CVE-2019-10092, CVE-2019-10098, CVE-2019-10097

Open SSL was updated to 1.0.2u correcting the following:

- CVE-2018-0732, CVE-2018-5407, CVE-2019-1547, CVE-2019-1559, CVE-2019-1563, CVE-2019-1551, CVE-2020-1967

Open SSH was updated to 8.1p1 correcting the following:

- CVE-2018-15473, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111

PHP was updated to 7.4.6, correcting the following:

- CVE-2018-10545, CVE-2018-10546, CVE-2018-10548, CVE-2018-10549, CVE-2018-17082, CVE-2019-11043

Option Card enhancements and fixes

- 1204-32 Gb PTP Master Card had several improvements with the updated version 1.31 firmware
  - fixed inoperability with devices that use non-standard values for the PTP transportSpecific field
  - resolved an issue with PTP packets being broadcast before the unit is fully synchronized
  - changed generation of clockAccuracy parameter to reduce unnecessary transitions between Best Masters
  - fixed configuration of TTL value on PTP multicast announce packets
  - corrected the MAC address in Layer 2 PTP packets.
- Upgraded option cards for improved system reliability:
  1204-3E to 1.02 firmware,
  1204-14 to version 1.02,
  1204-15 to version 1.12,
  1204-1B to version 1.04,
  1204-1E to version 1.03,
  1204-22 to version 1.03,
  1204-28 to version 1.02,
  1204-2A to version 1.03, and
  1204-34 to version 1.01.

Known Issues

- DHCPv6 subnet prefixes are currently limited to 64.

- The “Clean and Halt” command does not function properly when logged into SSH
- OpenSSL version 1.0.2u has a few known CVE security vulnerabilities (CVE-2019-1551, CVE-2000-1967).

Version 5.8.9

Newly released features

- Added IRIG-H output support for option card 1204-15 (formats H122 and H002).
- Added hardware and software watchdogs to control behavior and prevent lockup in the rare event of a unit failure

Enhancements and fixes

The following defects were corrected:

- Updated memory controller configuration to improve reliability on 32-bit systems.
- Fixed issue with the log file lastlog becoming too large within the configuration bundle.
- Repaired TACACS+ username functionality to allow the "_" character
- Corrected NMEA-GGA output decimal length.

Known Issues

In this software version as well as the previous version (5.8.8), certain customer configurations are known to fail to transfer when updating to this version. The known failures include saved local clock settings (which can occasionally result in timing error), custom web banners, and saved syslog server settings.

To avoid this issue, the customer is recommended to make a backup of their current configuration prior to updating to this version. This saved configuration bundle can then be used to restore saved settings.

See the user manual page on customer configuration bundles for more information: *http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/ConfFilesBckpRest.htm*

Version 5.8.8

Enhancements and fixes

The following improvements were applied to existing features and functions:

- Updated the FPGA versions of the following option cards to increase communication reliability: 1204-01, 1204-02, 1204-03, 1204-04, 1204-05, 1204-15, 1204-1F, and 1204-23.

Version 5.8.7

Newly released features

- Added support for option cards 1204-4C and 1204-53, which both provide (4) E1/T1 outputs.

Enhancements and fixes

The following improvements were applied to existing features and functions:

- Improved FPGAs for the IRIG-AM option cards 1204-05, 1205-15, 1204-1F.
- Released new FPGAs for 1204-01 and 1204-03
- Added Geoid Height to the NMEA GGA output of SAASM GPS.

The following defects were corrected:

- Upgraded software on the 1204-3B option card. This upgrade repairs the following issues: a problem changing the MTU, and issue when setting bad network parameters, and an issue where SSH and FTP Server weren't disabled before the release to the customer.
- Fixed an issue with TACACS+ and RADIUS not ignoring local users before checking against the remote server, and allowed both TACACS+ and RADIUS users to issue CLI commands.
- Corrected a bug with IRIG AM output phase adjustment at 100 Hz.
- Repaired a reporting error of the CPU utilization in the system monitor being averaged across entire uptime of the device.
- Fixed GPS Antenna Sense on SAASM MPE-S returning OK after antenna was removed.
- Resolved issue with saved config file not zeroing out the domain server.

Version 5.8.6

Newly released features

- Added 1/8 Hz pulse output for use on the 1204-17 option card.

Enhancements and fixes

The following improvements were applied to existing features and functions:

- Updated NTP to 4.2.8p13.
- Updated Trimble firmware to 1.10.

The following defects were corrected:

- Corrected problem with LDAP Groups used with SSH.
- Fixed an issue with TACACS+ and RADIUS causing kernel lockup, to improve responsiveness for SSH users.

Version 5.8.5

Enhancements and fixes

The following improvements were applied to existing features and functions:

- Added a Disk Healthcheck feature to the Web UI under **TOOLS** > **Upgrade/Backup**, which reports the approximate remaining life of the CF card and provides instruction to take action if necessary.
- Improved security of the Web UI by preventing simultaneous login from multiple locations, preventing Cross Site Request Forgery (CSRF), and reducing access to the factory account.
- Updated Broadshield support to version 5.2.2
- Added the geoid height to the NMEA GGA output message.

The following defects were corrected:

- Corrected behavior of SNMP in order to retain engine IDs on each startup.
- Fixed a minor issue with errors from the STL front panel status display.
- Modified Rubidium disciplining support to prevent breaking from the warm-up state early.

Option Card enhancements and fixes

- 1204-32 Gb PTP Master Card had several improvements: updated firmware, repaired functionality when in slot 4, corrected a control field value, corrected the output time until the first PPS, and fixed a bug when switching between masters.
- Added support of the 1204-50 option card.
- 1204-3C performance enhancements.

Version 5.8.4

Enhancements and fixes

The following defects were corrected:

- Fixed a problem with the u-blox receiver upgrade procedure, which failed to restart the receiver.

Version 5.8.3

Enhancements and fixes

The following improvements were applied to existing features and functions:

- GGA Fix Quality field is now based on overall sync state—not solely on GPS sync
- Increased SAASM functionality with ASCII Output mode visibility
- Added support for STANAG 4430 (Extended HaveQuick Edition 1)
- Reduced the CF disc size
- Increased responsiveness of content on small screens
- Improved the reliability of u-blox receiver firmware updates
- Updated Broadshield to version 5.1.1
- Created opportunity for customers with admin privileges to run traceroute with the TCP option
- Enabled full ASCII offset range, both positive and negative
- Added verification of presence of SGPS receiver

The following defects were corrected:

- Corrected ICMP redirects, eliminating potential security vulnerability
- Increased security on terminal connections
- Fixed configuration issues with the IPv6 Transfer Engine
- Fixed an issue with file limits in IPv6 setups
- Repaired intermittent issue with DHCP addresses being obtained despite static settings
- Fixed an error in the manifest file if no GPS is found by system
- Fixed an issue with NMEA messages transitioning to empty fields
- Fixed an issue in which clean updates wouldn't allow TACACS+ access through http

Security enhancements and fixes

NTP was updated to 4.2.8_p12, resolving:

CVE2018-12327

Option Card enhancements and fixes

- 1204-43 and 1204-44 upgrade bundles created
- Option card 1204-4A is changed to 1204-50.

Version 5.8.2

Enhancements and fixes

The following defects were corrected:

- Repaired an issue with faulty log rotation.
- Improved data logging to prolong compact flash longevity
- Fixed issue where TACACS+, RADIUS, and LDAP were not configurable following a clean update.

Version 5.8.1

Enhancements and fixes

The following defects were corrected:

- Fixed a DHCP failure in release 5.8.0 due to a race condition at startup.

Option Card enhancements and fixes

The following defects were corrected:

- 1204-32 PTP Option Card no longer displays incorrect IP addresses and other values. The communication speed was slowed down to prevent corruption.

Version 5.8.0

Newly released features

- Added support for 1204-3E-STL option card
- Added support for 1204-40 Low Phase Noise 100MHz Output option card
- Added support for 1204-43 Single GNSS option card
- Added support for 1204-44 Dual GNSS option card

Enhancements and fixes

The following improvements were applied to existing features and functions:

- Updated Linux kernel from 4.4.87 to 4.14.34 to improve system stability and functionality
- A-GNSS Server RINEX3 and Almanac file creation now supports GLONASS
- Added HTTPS certificate support of SANS fields for Common Names.

The following defects were corrected:

- Corrected support of 6 1204-12 PTP 10/100 cards with u-blox M8T receiver
- Removed command line access to the password command, requiring users to change user passwords from Web UI only
- Added code to help recover from database stuck issue on update and database maintenance

Security enhancements and fixes

Kernel was updated to 4.14.34 resolving Spectre vulnerabilities (System is not vulnerable to Meltdown CVE-2017-5754)

- CVE-2017-5715, CVE-2017-5753

NTP was updated to 4.2.8p11 correcting the following:

- CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185

OpenSSL was updated to 1.0.2n correcting the following:

- CVE-2018-0739

Apache was updated to 2.2.34 correcting the following:

- CVE-2017-3167, CVE-2017-3169, CVE-2017-7668, CVE-2017-7679

glibc was updated to 2.25-r12 correcting the following:

- CVE-2017-14062, CVE-2017-15670, CVE-2017-15671, CVE-2017-15804, CVE-2017-16997, CVE-2018-1000001, CVE-2018-6485, CVE-2018-6551

Quagga was updated to 1.2.4 correcting the following:

- CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

ncurses was updated to 6.1 correcting the following:

- CVE-2017-10684, CVE-2017-10685, CVE-2017-11112, CVE-2017-11113, CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734, CVE-2017-16879

DHCP was updated to 4.3.6p1 correcting the following:

- CVE-2018-5732

Option Card enhancements and fixes

The following defects were corrected:

- 1204-2F Programmable Frequency Card no longer disables all outputs
- 1204-17 Square Wave Option Card can now disable direct outputs after being enabled

Version 5.7.3

Newly released features

- Added capability to enable/disable link auto-negotiation and set individual network port speed/duplex settings
- Updated IPv6 networking support to more closely match IPv4 networking. Added additional routing tables per network port with individual IPv6 default gateways. Static IPv6 routes can be applied per network port.

Enhancements and fixes

The following improvements were applied to existing features and functions:

- Updated Linux kernel from 4.4.26 to 4.4.87 to improve system stability and functionality
- Updated disciplining algorithms to improve short term stability and increase the maximum of the dynamic loop constants
- Changed Rubidium disciplining to operate using common disciplining algorithm with other oscillators for new and existing fielded units. In order to downgrade SW, existing Rubidium units will need to be patched back to previous disciplining mode.

The following defects were corrected:

- Corrected bug in enabling/disabling IPv6 SLAAC

Security enhancements and fixes

Kernel was updated to 4.4.87

- The following CVEs were corrected related to the stack clash vulnerabilities: CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-1000379

OpenSSL was updated to 1.0.2n correcting the following:

- CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738

tcpdump was updated to 4.9.2 to resolve many vulnerabilities:

- CVE-2017-11108, CVE-2017-(11541-11544), CVE-2017-(12893-12902), CVE-2017-(12985-13055), CVE-2017-(13687-13690), CVE-2017-13725

Option Card enhancements and fixes

The following defects were corrected:

- n/a

Version 5.7.2

Newly released features

- n/a

Enhancements and fixes

The following improvements were applied to existing features and functions:

- n/a

The following defects were corrected:

- Fixed defect in live application of a user set Link Local IPv6 gateway address

***Security** enhancements and fixes*

- n/a

***Option Card** enhancements and fixes*

The following defects were corrected:

- n/a

Version 5.7.1

- AMENDMENT to the previous release, Version 5.7.0:
  Software release 5.7.0 contains Linux Kernel 4.4.26 which fixes CVE-2016-5195 “Dirty Cow”.

Newly released features

- Introduced Talen-X **BroadShield** feature requiring license SS-OPT-BSH. This optional functionality offers spoofing and jamming protection and can be added to existing units with u-blox M8T receivers.
- Added a SecureSync/Netclock 94XX Manifest file in `/home/spectracom/config/manifest.conf`, and a Manifest Log in `/home/spectracom/log/manifest.log`.
  The config file contains the current software/fpga/firmware versions, option cards and licenses installed. The Log shows these as they change each reboot.
- Added link to Spectracom Orolia USA online user documentation manuals.spectracom.com
- Update process improved to reduce disk space utilized.
- NOTE: Unlike **Standard Mode**, **Single Satellite Mode** requires position to be deleted if the user relocates the device. This is required because users often handset position when using **Single Satellite Mode**.
- Syslog Port Number can now be changed in the Web UI.

Enhancements and fixes

The following improvements were applied to existing features and functions:

- n/a

The following defects were corrected:

- Corrected error in system log relating to temperature logging.
- Update with Clean operation no longer backs-up SQLITE database. Now it is simply cleared.
- Corrected failover kernel update process bug.
- Corrected 100-150 µsec NTP Offset reported by SSS-313 by adjusting 1204-06 Gigabit Ethernet Port rx-µsecs value set in start up script.
- Added ability to set a Link Local IPv6 gateway address
- Corrected ability to restore Syslog to default configuration
- Corrected Security issues by updating packages to correct CVEs, and corrected various file permissions errors.

Security enhancements and fixes

- glibc package was updated due to:

  CVE-2014-9761, CVE-2015-5277, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2016-1234, CVE-2016-3075, CVE-2015-5180, CVE-2016-6323, CVE-2017-1000366

- libpcre package was updated due to:

  CVE-2017-6004

- libevent package was updated due to:

  CVE-2016-10195, CVE-2016-10196, CVE-2016-10197

- sudo package was updated due to:

  CVE-2017-1000367

- shadow package was updated due to:

  CVE-2016-6252, CVE-2017-2616

- wgetpackage was updated due to:

  CVE-2017-6508

- vim and gvim packages were updated due to:

  CVE-2017-5953, CVE-2017-6349, CVE-2017-6350

- nettle package was updated due to:

  CVE-2016-6489

OpenSSH:

- OpenSSH was updated to openssh 7.5_p1

  The following CVEs were corrected:
  CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012

Option Card enhancements and fixes

The following defects were corrected:

- Option Card 1204-12 PTP 10/100 Card intermittently failed to complete an update. A 25-minute timeout now exists. If it fails to update, and 25 minutes pass, the update fails and the update process moves to the next option card.

Version 5.7.0

Newly released features

- Multi-GNSS reception is now a standard feature (no longer an option), defaulting to GPS + GAL.
- Phase monitoring now includes phase validation, causing the unit to flywheel if a threshold value is exceeded.

Enhancements and fixes

The following improvements were applied to existing features and functions:

- Updated Linux kernel from 4.0.5 to 4.4.26 to improve system stability and functionality
- Fixed Kernel errors caused by, inter alia, i2C temperature sensor readouts: Changed LM90 SMBUS clock speed to a valid range, and applied Realtek *8139too* patch.
- SNMP Trap Port restriction was modified from 0-1023 to 0-65535.

The following defects were corrected:

- GNSS Receiver Satellite Data Tab now will be populated with data
- A unit equipped with a Trimble RES-SMT-GG receiver now will resurvey automatically on reboot after it has been moved.

Security enhancements and fixes

- CVE-2014-2830

OpenSSL was updated due to:

- CVE-2016-7055, CVE-2017-3730, CVE-2017-3731, CVE-2017-3732

net-misc/quagga was updated due to:

- CVE-2016-1245, CVE-2016-4049

NTP was updated to NTP 4.2.8_p10 (released on 21 March 2017). For more information, see http://support.ntp.org/bin/view/Main/SecurityNotice#March_2017_ntp_4_2_8p10_NTP_Secu

- CVE-2017-6464: NTP-01-016 NTP: Denial of Service via Malformed Config (Pentest report 01.2017)

- CVE-2017-6462: NTP-01-014 NTP: Buffer Overflow in DPTS Clock (Pentest report 01.2017)
- CVE-2017-6463: NTP-01-012 NTP: Authenticated DoS via Malicious Config Option (Pentest report 01.2017)
- Sec 3386: NTP-01-011 NTP: ntpq_stripquotes() returns incorrect Value (Pentest report 01.2017)
- Sec 3385: NTP-01-010 NTP: ereallocarray()/eallocarray() underused (Pentest report 01.2017)
- CVE-2017-6455: NTP-01-009 NTP: Windows: Privileged execution of User Library code (Pentest report 01.2017)
- CVE-2017-6452: NTP-01-008 NTP: Windows Installer: Stack Buffer Overflow from Command Line (Pentest report 01.2017)
- CVE-2017-6459: NTP-01-007 NTP: Windows Installer: Data Structure terminated insufficiently (Pentest report 01.2017)
- Sec 3381: NTP-01-006 NTP: Copious amounts of Unused Code (Pentest report 01.2017)
- Sec 3380: NTP-01-005 NTP: Off-by-one in Oncore GPS Receiver (Pentest report 01.2017)
- CVE-2017-6458: NTP-01-004 NTP: Potential Overflows in ctl_put() functions (Pentest report 01.2017)
- CVE-2017-6451: NTP-01-003 Improper use of snprintf() in mx4200_send() (Pentest report 01.2017)
- CVE-2017-6460: NTP-01-002 Buffer Overflow in ntpq when fetching reslist (Pentest report 01.2017)
- Sec 3376: NTP-01-001 Makefile does not enforce Security Flags (Pentest report 01.2017)
- CVE-2016-9042: Origin

net-fs/cifs-utils was updated due to CVE-2014-2830

- AMENDED at the time of publishing Release Notes for Version 5.7.1:
  Software release 5.7.0 contains Linux Kernel 4.4.26 which fixes CVE-2016-5195 Dirty Cow.

Option Card enhancements and fixes

- 1204-34: Frequency Monitor reports error "Error: Sum of Period is NULL from FM"

Version 5.6.0

Newly released features

- Added support for u-blox M8T **receiver firmware** update to Release 3.01 TIM 1.10 which provides performance improvements and use of the **Galileo** constellation.
- Added support for loading **x509 PEM CA chain certificates**.

Enhancements and fixes

The following improvements were applied to existing features and functions:

- The HTTPS setup window now requires the user to first check the **Enable** checkbox.
- Upon saving the **log bundle**, the contents of the `/var/log` log folder are now included in the downloaded log bundle.
- **Radius and TACACS+** now provide login user authentication support for protocols other than HTTP/HTTPS such as ssh, telnet and FTP.
- Resolved issues generating **A-GPS** and **A-GNSS** using the u-blox receiver. Added generation of RINEX and Almanac for GPS, Galileo, and BeiDou constellations. Note: A-GNSS server functionality for GLONASS is not yet supported (known issue – scheduled to be fixed in next release.)
- The **update process** can now program BIOS changes.

The following defects were corrected:

- Clock Service now can convert from **TAI or GPS timescales to UTC** (used for inputs like ASCII)
- Default UTC/GPS and UTC/TAI **offsets** were updated to 18 and 37 seconds, respectively.
- TimeKeeper can no longer be set to an **NTP rate of 0**.

***Security** enhancements and fixes*

- **Apache http headers** HTML text no longer contain version information to improve security: The raw HTML returned from the Apache web server it will no longer display the Apache version information.
- The creation of a default certificate and public/private key pairs now defaults to using a **SHA-256** digest. However, this digest is NOT supported by Internet Explorer version 8 and below, i.e. users of release 5.6.0 and higher will not be able to login with HTTP/HTTPS using a SHA-256 digest (use default certificate creation with user specified digest such as SHA1 instead [defcert command]).

- The **LDAP validation criteria** will now appropriately check for a correct Distinguished Name (DN), and bind DN/Password before allowing the enabling of the configuration. In addition to that, all servers in the setup will now be checked, as opposed to just one server, to make sure the DN is valid for all servers listed.

Option Card enhancements and fixes

- The **SNMP MIBs** now provide read-only support for PTP variables from the 1204-32 Gigabit PTP Option Card.
- Square Wave Output features now include an added **5MPPS/1PPS** preset.
- **Gigabit Ethernet option card** 1204-06: **eth1 - eth3** now allows user to enable/disable individual ports from the Front Panel.

Version 5.5.0

Newly released features

- Added **TACACS+** for user authentication
- Added ability to enable and disable **Classic Web UI** via command line
- Improved Web UI for **HTTPS** Certificate generation
- Support u-blox GNSS receiver model **LEA-M8T firmware** version 3.01 TIM 1.10
- Added support for **Galileo** Constellation, using LEA-M8T firmware version 3.01 TIM 1.10
- Updated the Web UI to provide current Spectracom **contact information** and emails

Enhancements and fixes

The following defects were corrected:

- SQLite Database for NTP Statistics and Reference Monitor **Statistics graphs** grow without limit until the graphs stop updating.
- SNMP always reports **NTP Jitter measurement** as 4.000
- Require **GPS to be enabled** if user selects GLONASS or QZSS and the SecureSync unit has a Trimble RES-SMT-GG GNSS receiver
- Corrected defects in **LDAP Security** configuration in Web UI and in Classic Web UI.
- Improved code to provide more consistent **error codes**
- Provided **E-Loran** protocol fix
- Updated to **NTP 4.2.8_p9** (NTP Autokey authentication is now supported again)
- Corrected system log error indicating current **Leap Indicator bits** are empty string from NTP on startup.

Security enhancements and fixes

- **libgcrypt:** Multiple vulnerability fixes (dev-libs/libgcrypt-1.6.3-r4) CVE-2014-3591, CVE-2015-0837, CVE-2015-7511, CVE-2016-6313

- **GNU Wget:** Multiple vulnerabilities (net-misc/wget-1.16.3-r1) CVE-2016-4971
- **UnZip:** Multiple vulnerabilities (app-arch/unzip-6.0-r3) CVE-2014-8139, CVE-2014-8140, CVE-2014-8141, CVE-2014-9636
- **libpng:** Multiple vulnerabilities (media-libs/libpng-1.6.19) CVE-2015-7981, CVE-2015-8126
- **MIT Kerberos 5:** Multiple vulnerabilities (app-crypt/mit-krb5-1.13.2) CVE-2015-2695, CVE-2015-2696, CVE-2015-2697
- **Tar:** Extract pathname bypass (app-arch/tar-1.27.1-r2) CVE-2016-6321

- **glibc:** Update to 2.22-r4 (CVE-2016-5417)

OpenSSH 7.3p1: Fixes CVE-2015-8325, CVE-2016-6210, CVE-2016-8858

OpenSSL 1.0.2j:

- **Bug 581234** (CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176)
- CVE-2016-6309, CVE-2016-7052, CVE-2016-6304, CVE-2016-6306, CVE-2016-6303, CVE-2016-6302, CVE-2016-2179, CVE-2016-2181, CVE-2016-2182, CVE-2016-2180, CVE-2016-2178, CVE-2016-2177

Apache 2.2.31: CVE-2016-5387

NTP 4.2.8p9: Bug 600430 (CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311, CVE-2016-9312)

Option Card enhancements and fixes

- Bug fix, addressing ASCII RS-232 outputs not always responding to request characters:
  - **1204-02** ASCII RS-232 Option Card FPGA update to version 1.16
  - **1204-1F** NENA Card FPGA update to version 1.03

- **1204-12** 10/100 PTP Card update to firmware version T159:
  - When the Slave is configured in Minicast mode, the delay request is now sent to the Master in Unicast even if no contract has been established.
  - The Slave now accepts the delay response even if it is configured for Unicast, and it received the delay response in Multicast.
  - Now handles IGMP join requests in Minicast mode.

Version 5.4.5

Newly released features

- Reference Monitoring – Allows comparison of filtered phase offsets between Input References.
- ASCII Format 9S – New variation of ASCII Format 9 with Sysplex compatible fields.
- Update to NTP 4.2.8p8
- Added user selectable High and Medium level HTTPS Security settings
- U-blox type receivers will now resurvey on reboot. The user may select the resurvey mode by selecting Standard Mode and Land Dynamics to request a resurvey on reboot, or No Resurvey on Reboot if Standard Mode Stationary Dynamics has been selected.
- For GNSS receiver models Trimble Resolution-T and u-blox M8T, the user can now choose between Mobile Dynamics Land, Sea, Air, and Stationary Dynamics.
- Host disciplining defaults to disabled, but can be enabled by the user.
- Classic Web UI is now disabled by default. The user can enable Classic Web UI from Network General Setup Web page.

Enhancements and fixes

- Removed logging of invalid text on user entry of default gateway.
- Changed Web UI **MANAGEMENT** dropdown menu to increase user visibility of **Network Setup** selection.
- Reboot and Halt from Command line now journal the log user who issues them.
- Anycast configuration changes are now journal the log user who issues them.
- Temperature Alarm mask configuration and other notification changes are logged in plain English.
- Registration reminder now is no longer repeatedly asserted.
- Clear All Logs command now removes Auth and NTP Logs.
- NTP Broadcast now correctly accepts address input without error.
- System Monitor page corrected for user group members.
- Command line command `gettemp` allows reading of temperatures.
- Ethernet Monitor now correctly downloads graph in Excel spreadsheet file.
- The command line `tcpdump` and `iptables` can now be run by spadmin group users.
- Adding and deleting of NTP Peer and Server addresses are now logged.
- Corrected update/add/delete NTP Peer/Server line error
- SNMP web page is now only accessible by spadmin group members
- Improved Time Manipulation Library functions to take into account UTC-GPS Offset
- Corrected KHTD defect which caused delay when time stepped backwards
- Modification to StatusD to support ntpq commands being issued on a single thread at a time.

- Simplified IPv6 Gateway main gateway input
- Updated Trimble RES-SMT-GG to version 1.9
- Updated to 0.9.88 version of “8139too” Ethernet Eth0 10/100 driver
- Improved Update Process to more safely format and partition CompactFlash
- Corrected Epsilon TOD 1 format issue
- Added support for OpenSSH use of ED25519 keys
- Disabled Web UI caching
- Reduced Apache error logging level to reduce amount of logging
- Corrected Timing System software initialization error in GP Outputs
- Corrected ASCII Input Auto-Detect mode to display auto-detect rather than E-Loran format when format is being discovered automatically.
- Corrected Timing System to schedule leap seconds in the 24 hours prior to the leap second.
- Corrected File permissions for some Web UI modified files.
- Changed “Time Scale” to “Timescale” in Web UI
- Improved Error Logging in Timing System library for commands issued from Web UI or command line.
- Improved data storage and organization of Network Monitor data in SQL database
- Changed Web UI access to “Network Setup” menu.
- ASCII Formats for BBC EBU LTC outputs now support Local Clocks.
- Anycast daemons failure to start from Web UI has been corrected. (Note that the Enable status checkbox may not display as checked after startup. To verify the Enable state after startup, close Anycast dialog and reopen it.)

Security enhancements and fixes

- Updated Quagga, OpenSSL, OpenSSH, PHP, and others for security vulnerabilities:

Quagga CVE:

- Bug 577156 (CVE-2016-2342) - <net-misc/quagga-1.0.20160315: Buffer overflow in bgpd (CVE-2016-2342)
- Bug 581526 (CVE-2016-4049) - net-misc/quagga: denial of service vulnerability in BGP routing daemon

OpenSSH (7.2p2):

- CVE-2016-3115
- CVE-2016-3115 (not vulnerable)

PHP, and other libraries:

- **PHP:** Multiple vulnerabilities (dev-lang/php-5.5.37 dev-lang/php-5.6.17) CVE-2013-6501,CVE-2014-9705,CVE-2014-9709,CVE-2015-0231,CVE-2015-0273,CVE-2015-1351,CVE-2015-1352,CVE-2015-2301,CVE-2015-2348,CVE-2015-2783,CVE-2015-2787,CVE-2015-3329,CVE-2015-3330,CVE-2015-4021,CVE-2015-4022,CVE-2015-4025,CVE-2015-4026,CVE-2015-4147,CVE-2015-4148,CVE-2015-4642,CVE-2015-4643,CVE-2015-4644,CVE-2015-6831,CVE-

2015-6832,CVE-2015-6833,CVE-2015-6834,CVE-2015-6835,CVE-2015-6836,CVE-2015-6837,CVE-2015-6838,CVE-2015-7803,CVE-2015-7804, 201607-02 [N] [remote]

- : Multiple Vulnerabilities (dev-libs/libpcre-8.36) CVE-2014-8964,CVE-2014-8964,CVE-2015-5073,CVE-2015-5073,CVE-2015-5073,CVE-2015-8380,CVE-2015-8381,CVE-2015-8383,CVE-2015-8384,CVE-2015-8385,CVE-2015-8386,CVE-2015-8387,CVE-2015-8388,CVE-2015-8389,CVE-2015-8390,CVE-2015-8391,CVE-2015-8392,CVE-2015-8393,CVE-2015-8394,CVE-2015-8395,CVE-2016-1283,CVE-2016-1283, 201607-04 [N] [remote]
- **GD**: Multiple vulnerabilities (media-libs/gd-2.0.35-r4) CVE-2016-3074

OpenSSL (1.0.2h):

CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-2176, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800

NTP:

- **ntp-4.2.8p8**: CVE-2016-4957 / VU#321640: Crypto-NAK crash; CVE-2016-4953 / VU#321640: Bad authentication demobilizes ephemeral associations; CVE-2016-4954 / VU#321640: Processing spoofed server packets; CVE-2016-4955 / VU#321640: Autokey association reset; CVE-2016-4956 / VU#321640: Broadcast interleave
- **ntp-4.2.8p7**: CVE-2016-1551: Refclock impersonation vulnerability, AKA: refclock-peering; CVE-2016-1549: Sybil vulnerability: ephemeral association attack, AKA: ntp-sybil - MITIGATION ONLY; CVE-2016-2516: Duplicate IPs on unconfig directives will cause an assertion botch; CVE-2016-2517: Remote configuration trustedkey/requestkey values are not properly validated; CVE-2016-2518: Crafted addpeer with hmode > 7 causes array wraparound with MATCH_ASSOC; CVE-2016-2519: `ctl_getitem()` return value not always checked; CVE-2016-1547: Validate crypto-NAKs, AKA: nak-dos; CVE-2016-1548: Interleave-pivot - MITIGATION ONLY; CVE-2015-7704: KoD fix: peer associations were broken by the fix for NtpBug2901, AKA: Symmetric active/passive mode is broken; CVE-2015-8138: Zero Origin Timestamp Bypass, AKA: Additional KoD Checks; CVE-2016-1550: Improve NTP security against buffer comparison timing attacks, authdecrypt-timing, AKA: authdecrypt-timing

Option Card enhancements and fixes

- Option Card 1204-12 10/100 PTP Option Card firmware updated to version T156

Version 5.4.1

Release features

- n/a

Enhancements and fixes

- Fixed Anycast configuration defect occurring in release 5.4.0.
- Corrects a defect in release 5.4.0 in which log rotation fails to occur, resulting in disk utilization issues.

***Security** enhancements and fixes*

- n/a

***Option Card** enhancements and fixes*

- n/a

Version 5.4.0

Release features

- NetClock now supports u-blox LEA-M8T GNSS receiver boards. Trimble receivers continue to be supported, as well.
- Under Network Web Interface settings, it is now possible to set a Login timeout. This timeout is a limit on how long a user can stay logged on, regardless of activity.
- Ethernet monitoring functionality has been added, allowing a user to observe network traffic on all Ethernet ports.
- It is now possible to prefer certain NTP Peers.
- Support of iptables allows for customizable access restrictions.
- Language preferences set by the user will now be maintained across logins.

Enhancements and fixes

- Linux Kernel 4.0.5 configuration has been changed to NO preemption.
- Processor BIOS update supported.
- Refactored software to improve software CPU cycle usage.
- Disciplining improvements have been applied.
- NTP Autokey is NOT supported in Spectracom Release 5.4.0 NTP 4.2.8_p6, due to a patch to fix a recent CVE related to Symmetric keys which broke the Autokey feature (for more information, see http://bugs.ntp.org/show_bug.cgi?id=3005).
- Anycast over the BGP protocol has been added. Note: BGP will be disabled if the user updates to Release 5.4.0 or restores an older configuration file after updating to Release 5.4.0. The user must enable Anycast BGP if so desired.
- The LDAP authentication setup window now displays only necessary fields, based on Server Type.
- It is now possible for the user to enter special characters into the SNMP location string such as "!@#$%^ words 1234 _[]~"
- Notifications will be sent based on SAASM events e.g., Key expiration or Keys becoming valid.
- Static routes will now be restored in the course of a configuration update or an upgrade and on reboot.
- Spelling of SNMP MIB variables has been corrected.
- It is now permissible to load an HTTPS Certificate.
- The log history will not be cut off any more, i.e. the entire log history will be displayed in the Web UI.
- The GPS Signal strength web pages have been corrected in the Classic Web UI.
- Corrected the averaging of samples in NTP graphs.
- Restored the ability to input a Syslog Server IP address in the Web UI.

Security enhancements and fixes

- Updated from version NTP 4.2.8_p3 to **NTP 4.2.8_p6** (for more information, see http://nwtime.org/ntf-releases-ntp-4-2-8p6-security-patch/)
    - CVE-2015-8158: Potential Infinite Loop in ntpq
    - CVE-2015-8140: Ntpq vulnerable to replay attacks
    - CVE-2015-8139: Origin Leak: ntpq and ntpdc, disclose origin
    - CVE-2015-8138: origin: Zero Origin Timestamp Bypass
    - CVE-2015-7979: Off-path Denial of Service (DoS) attack on authenticated broadcast mode
    - CVE-2015-7978: Stack exhaustion in recursive traversal of restriction list
    - CVE-2015-7977: reslist NULL pointer dereference
    - CVE-2015-7976: ntpq saveconfigcommand allows dangerous characters in filenames
    - CVE-2015-7975: nextvar()missing length check
    - CVE-2015-7974: Skeleton Key: Missing key check allows impersonation between authenticated peers
    - CVE-2015-7973: Deja Vu: Replay attack on authenticated broadcast mode

- Updated **OpenSSL** from version 1.0.1p to **1.0.2f** (for more information, see https://www.openssl.org/news/openssl-1.0.2-notes.html)
    - CVE-2016-0800
    - CVE-2016-0705
    - CVE-2016-0798
    - CVE-2016-0797
    - CVE-2016-0799
    - CVE-2016-0702
    - CVE-2015-3197

- Updated **OpenSSH** from version 6.9p1 to **7.1p2** (for more information, see http://www.openssh.com/txt/release-7.2)
    - CVE-2016-0777
    - CVE-2016-0778.

- Updated **GNU** C Library GLIBC 2.21-r2 (for more information, see https://sourceware.org/ml/libc-alpha/2016-02/msg00416.html)
    - CVE-2015-7547 --- glibc getaddrinfo() stack-based buffer overflow

- Updated to MPFR 3.1.3_p4; **Gentoo** recommended update.
    - CVE-2009-075

Version 5.3.1

Release features

- **Enhanced fan control** for units equipped with *Front Panel Fan Modification*, offering the choice between “Always On” and “User Defined”. The latter can be used to define a temperature window.
- **Temperature Monitoring Alarms/Clears** can now be set by the user: **Major** and **minor** alarms can be generated and delivered via SNMP and Email, and are logged in Alarm and Event logs. A retry value can be set to determine for how long the measured temperature must remain above the threshold value before an alarm is triggered.
- A new **System Status** page consolidates key temperature and hardware utilization graphs
- Two **NTP traffic graphs**, plus peak traffic information have been added to the NTP Setup page. The graphs can be saved and downloaded. Currently supported for NTP only (not TimeKeeper).
- All **graphs** now offer a user-friendly way to **delete** the logged data. Most graphs can be **downloaded** (satellite data, disciplining and temperature data, NTP throughput statistics).
- **New SNMP MIB variables** to read oscillator, board and CPU temperatures, including four new temperature monitoring traps (cf. above).
- The **Front Panel** is designed to continue **enabling the fan** as it did in the past, but additionally accepts input control from the SecureSync Software/FPGA logic to either enable the Fan all the time, or to control the fans enable state via user-defined min./max. temperatures to keep the CPU temperature within the user defined band.
- The **mysql database** is converted to a sqlite database which is returned in the `spectracom.log` file when saved.

Enhancements and fixes

- A CLI Command "**reboot hard**" has been provided to force a restart of SecureSync. This command is de facto a power cycle.
- The most current **Apache2 Error Log** is now returned in the SecureSync log bundle.
- Changed the **Frequency Error threshold** for TCXO units to $1x10^{-6}$ or 1PPM, to avoid immediately generating frequency alarms when SecureSync exits time synchronization, due to a loss of a valid reference, e.g. caused by loss of GPS reception.
- Improvements to oscillator disciplining (not applicable to Rubidium oscillators), including phase noise improvements during synchronization.
- Several changes to how **processes** are **launched, detected** and **runtime status** is **collected** have been made to improve efficiency, reduce memory usage.
- The **build scripts** were improved to detect failures and warnings during build and install.
- **Apache2 error logs** including the most recent one are now included in the Spectracom Log bundle.
- UI names for temperature graphs were changed to **CPU, Board** and **Oscillator temperatures**.

- GNSS licensing error with Multi-GNSS feature was corrected.
- Corrected setting of **Static Routes** so user can set them and ensured they are preserved across a software update.
- **Netmask "0"** in Access Restriction is no longer accepted, thus avoiding Apache crash.
- Added an end-of-year happy **new year** message. Note this message is logged when the year changes so it is also an indicator that a problem exists such as the Processor BIOS does not have the correct year set, e.g. when the battery backing up the BIOS settings has discharged.
- The SNMP **MIB** `SPECTRACOM-SECURE-SYNC-MIB.mib` was changed to add new Oscillator, Board, and CPU Temperature values. Also, four new SNMP Traps were added to indicate Major/Minor Temperature Alarms/Clears based on temperature thresholds and number of reads (user-definable).

Security enhancements and fixes

- Corrected security vulnerability **CVE-2012-2141** by applying the recommended patch to SecureSync version of NET-SNMP.

Option Card enhancements and fixes

- The 1204-06 Gigabit Ethernet card EEPROM used to configure the Intel MAC chip was corrected to fix known issues and errata published by **Intel**.

Version 5.3.0

Release features

- Support of Anycast over IPv6 utilizing OSPF
- Host disciplining: Linux kernel time set by NTP or PTP can now also be utilized to discipline the oscillator in the timing system. (Rubidium oscillators not supported)

Enhancements and fixes

- NetClock 9483 now displays option cards installed in slots 1-6 (was 1-4).
- Upgrade to GPS receiver firmware version 1.8, allowing QZSS Constellation support and improved performance
- RES-SMT-GG GNSS receiver update firmware was improved to avoid intermittent update failures.
- Updated TimeKeeper to version 7.0.6
- Enhanced temperature monitoring, adding processor board and CPU temperature graphs provided under the **Management** > **Disciplining** Menu.
- Fixed issue caused by NTP monitor Daemon NTPMOND, trying to stop NTP when the Timing System and Linux kernel time differ by more than 1 sec
- Software version of GNSS Receiver is no longer displayed when not present.
- LDAP can no longer be enabled with empty input, causing inability to login.
- Display of software versions are corrected on update page
- Web UI message for tcpdump changed from ON/OFF to “Permanently disabled”.
- Clear Logs and Statistics operation corrected to work from Web UI.
- Fixed error with creation of HTTPS certificate request and public/private key pair when entering common name
- Fixed an error causing Radius authentication to fail because the NAS address is being output as 127.0.0.1
- Updated IRIG control field format, Spectracom IEEE C37, to control sync state passed in control fields via signature control settings
- Corrected DOW (Day-of-Week) range in the BBC message 4 format
- Corrected Low Phase Noise Rubidium DAC value to remain constant when time is set by user
- Corrected Web UI to allow update of Main Default Gateway
- Updated translation of Web UI into French
- Improved Username management during upgrade

Security *enhancements and fixes*

- **Net-SNMP** 5.6.2.1 has been updated with a security patch to correct CVE-2015-5621
- **Open SSH** has been updated to version 6.9.
- Updated **OpenSSL** from 1.0.1m to **1.0.1p**.
  Among other things, the following vulnerabilities have been addressed:
  CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792, CVE-2015-1793, CVE-2015-4000, CVE-2014-8176
- Updated **NTP version** from 4.2.8p2 to 4.2.8p3 to address CVE-2015-5146.
  (NTP CVE-2014-9295 was fixed in 5.2.1 by updating to 4.2.8p2).
- **NTP** – Corrected GUI to avoid issue with allowing exploit of vulnerability CVE-2014-9295
- **Apache** CIPHERS were strengthened to remove weak ciphers, and Apache timeouts were adjusted to improve transfer of update images via web browser.
  (Apache was updated to 2.2.29 in 5.2.1)

Option Card enhancements and fixes

- Model 1204-06, Gigabit Ethernet Option Card: Updated Gigabit Ethernet driver to version 3.1.0.2

Version 5.2.1

Release features

- Added **tcpdump** functionality, with the ability to delete tcpdump, if so desired
- Added **Assisted GPS Rinex server license**, and improved A-GPS functionality
- Added **IRIG** control field format, Spectracom IEEE C37, to extend **leap second notification** to a month
- Added NTP throughput statistics logging

Enhancements and fixes

- Updated **Linux kernel** from 3.17.7 to 3.18.11 to improve system stability and functionality
- Improved how **Radius** detects and fills in NAS-IP address in its packets
- Improved **local clock** functionality: When a local clock has been modified by the user, features that the clock is applied to will be updated automatically.
- Added ability to pull **serial number** from **SNMP**
- Added ability to pull system **memory**, **CPU**, and CF card **disk usage** information from **SNMP**
- Updated **SNMP trap username** min/max length to 1 and 31 respectively
- Improved SNMP stability
- Extended the scope of journal **logging** of Web UI configuration settings
- Fixed issue with submitting **NTP stratum 1 configuration**
- Updated **Show Clock page** to improve clock and system status info displays
- Fixed issue when attempting to **clear** a scheduled **leap second**
- Software version and model and serial number will be logged in the **system log** on startup
- Improved internal **network configuration** for added stability
- Fixed issue where **Radius/LDAP** could be turned on after an update
- Fixed issue reporting **negative phase error** numbers via SNMP ssSysStaEstPhaseError OID
- Fixed issue where disabling an **AM IRIG output** would not disable the associated AM carrier
- Front panel **ResetPW** command now disables **Radius/LDAP** when resetting spadmin password

Security enhancements and fixes

- Updated **NTP version** from 4.2.6p5 to 4.2.8p2
- Updated **OpenSSL** from 1.0.1k to 1.0.1m
- Updated **ciphers** for **SSL and SSH** to address RC4/ARC4 issue

Version 5.2.0

Release features

- A **phase error limit field** was added to the Edit window of the Disciplining page allowing for an automatic disciplining tracking restart, once the phase error limit is exceeded, thus avoiding manual intervention.
- Added **static IPv6 routing** capability by allowing manual configuration of IPv6 routes via the SecureSync CLI.
- The System Status panel on the Web UI home page now includes a **temperature readout** for enhanced oscillator disciplining monitoring. The data can also be readout as a temperature-over-time graph in the Web UI, and is logged in the SecureSync log files.
- Added **Anycast** routing functionality for NTP.
  For more information on this subject, see the Tech Brief publication “NTP over Anycast”, which is located here.
- To facilitate diagnostics, **version numbers** of software components, option cards and GPS receiver are now displayed on the Upgrade/Backup page of the Web UI.
  Timing system and software version number have also been added to the system log.
- The **disk/memory status** is now displayed on the Upgrade/Backup page
- Added the ability to **re-calibrate oscillator control parameters** for non-standard rubidium oscillators.
- A note was added to the login page of the Web UI, to inform the user that **cookies** need to be enabled in browser.

Enhancements and fixes

- Implementation of a software fix to resolve an issue where **Linux processes** could become frozen and not processed.
- Added the **Linux kernel map** for improved diagnostic purposes.
- Improvements to **LDAP group authentication**, addressing reported login issue.
- Removed **password expired message** (LDAP/RADIUS only) that was displayed when logging in as a remote user.
- Improved **LDAP configuration status reporting** in the Web UI, as well as add/delete functionality.
- Improved the software **update patching process**, addressing patching configuration issue when upgrading from older revisions.
- Implemented a fix, now correctly displaying the **NetClock SW version number** when obtaining it via SNMP.
- Fixed issue, now correctly **applying DST rules** to the local time display in the Web UI.
- Fixed **submission error** on the GNSS Edit page on systems equipped without a GNSS license.

***Security** enhancements and fixes*

- Upgraded **Net-SNMP** software package from Version 5.6.1 to Version 5.6.2.1.
- Updated **OpenSSL** package from Version 1.0.1j to 1.0.1k, thus closing a reported security vulnerability.
- Updated **GLIBC** package from version 2.15 to 2.19 (addressing "**GHOST**" vulnerability, among other things)

Options enhancements and fixes

- Implemented a fix in FPGA to **improve 1PPS signal** to option cards, including IRIG, and addressing possible 5-ns **1PPS signal jump**. Previously occurring in SecureSync units equipped with a standard rubidium oscillator.
- Implemented a fix addressing an issue with how **local clock** settings had been applied to an **output**.

Version 5.1.7

Release features

- No new features added

Enhancements and fixes

- Fixed validation rules for SNMP V1/V2 IP address settings to allow set from returned value of “default” for the IP address
- Disciplining updates with phase error limiting to reduce transient phase error effects.
- Resolved an Apache web browser configuration issue in the 5.1.6 release
- Upgrading from software versions 5.1.4 or below to version 5.1.6 caused the web browser to become inaccessible. The fix to restore the web browser was to upload a clean config backup file.
- Includes firmware version 1.0.7 update for the Trimble RES-SMT-GG GNSS receiver (commercial GPS receiver installed in units that shipped after April 1, 2014. Not applicable to SAASM GPS receivers.)
- Fixes erroneous GPS time offset corrections potentially being applied.
- Fixes erroneous leap second notifications potentially being asserted.

Version 5.1.6

Release features

- No new features added

Security enhancements and fixes

- Bash update to version 4.2.53, in order to patch the “ShellShock” vulnerability.
  - Addresses potential vulnerabilities CVE 2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186 and CVE-2014-7187.
- Updated OpenSSL to Version 1.0.1i
  - Addresses potential vulnerabilities such as the following: CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3509, CVE-2014-3510, CVE-2014-3511, CVE-2014-3512 and CVE-2014-5139.

Version 5.1.5

Release features

- Software in the newer “RES SMT-GG” GNSS receiver can now be updated via NetClock’s Web UI.
- RES-SMT-GG GNSS receivers started shipping in NetClocks on April 1, 2014 (see also Release Notes for Version 5.1.7 above).

Enhancements and fixes

- Added prevention of erroneous timescale offset information
- (Applicable only to NetClocks with a Rubidium oscillator installed) Fixed an intermittent, potential issue affecting output references’ 1PPS.
- This potential 1PPS issue only affects installed Option Cards (not the outputs on the chassis) and operation changes on a power cycle.
- Enhanced front panel LCD display indications of the shutdown sequence status
- “Stopping System” is now displayed for several seconds before “Power off system” is displayed.
- Fixed a minor issue with LDAP and Radius authentication which required a user account be created, if the time server had been “cleaned”.
- NTP broadcast address is now user-configurable instead of being a static factory default value.
- Prevented a potential one second time error adjustment during operation, when synced to NTP for the Time reference and to an external 1PPS input for the PPS reference.
- When creating a Local Clock, manually configured DST rules can now be saved.
- Telnet and SSH login no longer prompts twice for a password.
- Management -> SNMP page of the browser now allows SNMPv1 and v2 configurations to be deleted.
- “SysObjID” in the Management -> SNMP page of the browser can now be edited.
- Optional Login banner will now be preserved during software updates.
- Improved operation of MySQL database (MySQL database is used with the new Web UI).
- Improved the "Scaled DAC Value" graph's scaling/display in the Management -> disciplining page of the browser.
- Configuration changes made to the User-defined Minor and Major alarms are now logged in the Journal log.
- Addressed an error with Oscillator log entries reporting all negative frequency error values as “0.00e-16”.
- Interface -> Main page of the Web UI (for configuring the GNSS receiver and A-GPS) and the Management -> Reference Priority table were not operating correctly with certain web browsers.

Security enhancements and fixes

- Updated OpenSSL to Version 1.0.1h
- Addresses potential vulnerabilities such as the following: CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224 and CVE-2014-3470.
- Updated Apache to Version 2.2.27.
- Web browser Login password is now cleared after each login attempt.
- Validation of passwords in the Management -> HTTPS page of the browser now allows all ASCII characters, but doesn't allow any spaces.

Version 5.1.4

Release features

- Added ability to configure the MTU (Maximum Transmission Unit) for each installed Ethernet Interface
  - The MTU value for each Ethernet interface can be displayed/configured via the **Management** -> **Network** page of the browser.

Enhancements and fixes

- Fixed settings validation issues related to SNMP configuration.
- Resolved an error message being displayed when trying to delete SNMPv1 or v2 access configurations.
- Addresses an issue with "Assisted GPS" ("A-GPS") always running/asserting "Rinex server" log entries in the System log each hour (if the time server does not have access to the Internet).
- Fixes an issue with certain erratic System log entries being asserted.
- Changed the scale value of the "Y" Axis of the "NTP Status Summary" graphs to "(Seconds)".
- Fixed an issue with the front panel display trying to display a Serial Number for the GPS receiver (Applicable only to units with no GPS receiver installed.)
- Main default gateway port number was not being displayed as the same value in both the web browser and the "gw4get" CLI command.

Security enhancements and fixes

- Updated OpenSSL to Version 1.0.1g to address CVE-2014-0160 ("Heartbleed").
- Updated OpenSSH to Version 6.6p1.
- Addresses potential vulnerabilities such as CVE-2014-2532 and CVE-2014-5107
- Updated PHP to Version 5.3.28.
- Addresses potential vulnerabilities such as CVE-2013-6420, CVE-2013-4113 and CVE-2013-2110
- Prevents ability to login to the web browser again, if the "Log Out" button wasn't pressed before closing the browser.
- Added ability to disable the "Classic Interface" web browser (Port 8080).
- Can be disabled via the **Management** -> **Network** page of the Web UI

Version 5.1.3

Release features

(Models 1204-13, 1204-30 and 1204-2F Programmable Frequency Option Cards)

- Released support for new Programmable Frequency output Option Cards, Models 1204-13, 1204-30 and 1204-2F.

(Models 1204-10, 1204-11, 1204-25 and 1204-1B HaveQuick/Stanag Output Option Cards, if installed):

- Added support for additional formats
- Added DOD-STD-1399 BCD Time Code to HAVE QUICK / STANAG option cards
- Added ICD-GPS-060A BCD Time Code to HAVE QUICK only option cards
- Added STANAG 4430 STM to HAVE QUICK only option cards

(All Models):

- Added "A-GPS" (Assisted-GPS) capability for enhanced "Skylight" indoor antenna operation/weak GPS reception

Enhancements and fixes

- Fixed SNMP enterprises.18837.3.3.2.1 MIB (ntpSysStaCurrentMode) from causing SNMP to potentially halt/crash.
- Added ability for hostname to accept either dashes or capital letters.
- Corrected an issue that was preventing users from logging into the new browser, with user rights, via LDAP or Radius. Users that can authenticate will now be logged in with admin rights.
- Fixed an issue that prevented the **Tools** -> **Upgrade/Backup** page from reporting the GPS receiver had been replaced by a GNSS (GPS + Glonass) receiver.
- Added an indication of "completion" when a software upgrade or license file has finished being installed.
- Fixed an issue preventing files from being able to be scp transferred into the SecureSync.
- Removed a "-4" from the ntp.conf file for NTP restrictions that was being added during software updates from previous versions of software.
- The "-4" being in the file was preventing NTP Symmetric key from working, after updating to software version 5.1.2.

Option Card enhancement and fixes

(Option 16: Multi-port Ethernet module, if installed):

- Implemented a fix to a potential, but seldom observed, condition which could cause received packets to be dropped.
- Added ability to re-disable Ethernet interfaces Eth1, Eth2 and/or Eth3, if they have since been enabled.
- Added network configuration qualification checking based on Ethernet port status/state.
- Gb Ethernet ports settings can only be changed if the port has been enabled.
- Fixed a broken link in the new web browser that resulted in an error message when clicked.

Security enhancements and fixes

- Added ability for SNMP passwords to be able to include “{ }” characters.

Version 5.1.2

Release features

- Implemented a new design of the web browser interface.
  - To help with the transition between the earlier and new web browser designs, the previous web browser design is still currently available, via the "**Classic Interface**" button in the top-right corner of the new web browser. (Note that a future software update will remove the ability to switch between the two web browser designs).
  - Please note the new web browser design removes the IPSec functionality (this function is still available via the "Classic Interface" web browser).
- New web browser design implements the ability to view NTP clients that are requesting time from the time server.
  - The "**Management**" -> "**NTP Setup**" page of the new web browser has a "**View NTP Clients**" button, which opens a table of the last 600 NTP clients that the time server received NTP requests from, including the average duration (in seconds) between the NTP requests from that client and how long ago (in seconds) the time server last received a NTP request from each client.
- Auth (Authentication) log entries can now be sent to Syslog server(s), as desired.
- Added Ethernet interface enabling/disabling (applicable to the Model 1204-06: Gigabit Ethernet Option Card, if installed- All three Ethernet connectors on this module are disabled by factory default).
- Added support for IPv6 DHCP functionality and SLAAC addresses.
- Added graphs to the GPS Status page of the new web browser to show number of satellites tracked over time and the signal strength of each receiver channel.
- Released support for new option card, model 1204-32: 1GB PTP Master Option Card

Enhancement and fixes

- Corrected an issue that was preventing NTP from correcting the time with more than a one second time error.
- Corrected the operation of NTP to allow NTP to be able to initially sync (or subsequently resync) if the System Time is manually set, or if an input reference changes by greater than 1000 seconds.
- Moved NTP to a slightly higher system priority
  - Addresses a condition which was causing NTP to periodically take 1 to 2 milliseconds to respond to NTP time requests, instead of it responding right away.
- Addressed an issue with the NTP log rotation.
- Users who can successfully login using LDAP or Radius will now have administrative privileges (fields will no longer be grayed-out after logging into the web browser).
- Fcron scheduler is now restarted if the System Time/date is manually set to values in the past.

- SNMP traps associated with the available User-defined Major/Minor alarms for GPS thresholds were switched.
- Fixed an issue that could potentially cause the Compact Flash card with Archive versions 5.0.0 through 5.0.2 installed to become full of data.
    - After a very long period of time, time servers with Archive software versions 5.0.0 to 5.0.2 installed could potentially become full of file snippets. This was related to the email functionality.
- SNMP MIB 1.3.6.1.4.1.18837.3.3.2.1.0, ("NTP_CURRENT_MODE") now reports 0 or 3 to avoid sluggish SNMP performance
    - Response times for SNMP Gets of this particular MIB were about 6 seconds or so, far longer than all other MIBs (due to how this status information is obtained from NTP). This potentially required SNMP script time-outs to need to be lengthened to account for the delayed responses from this MIB.

Option enhancements and fixes

(Models 1204-14, Simulcast CTSSS Option Card if installed):

- Alarm outputs will transition away from NC/NO/Alarm state when set to "None".
- Addressed an anomaly that was occurring with the 9600 baud output
- Once-per-second, a stray signal was being added to the 9600 baud output (if this signal was configured to be outputted).

Version 5.0.2

Release features

- Added an RFC 2783 interface for our timing system to source a 1PPS signal to NTP, to discipline the Operating System

Enhancements and fixes

- Strengthened the upgrade process to prevent loss of configuration information in systems with large accumulated NTP statistics and log files.
  - NTP statistics are not preserved and large log files are truncated
- Revised thread priorities.

Version 5.0.1

Option Card release features

- Added logging of Input Reference changes to the Event log
  - When an Input Reference change occurs, a log entry is asserted to indicate what the newly selected “Time” and/or “1PPS” input reference has been selected.

Enhancements and fixes

- Resolved an issue with setting/displaying the main network gateway on the front panel
  - This issue introduced in the version 5.0.0 software upgrade caused characters for the gateway address to run off the edge of the LCD display and also caused difficulty setting this value using the keypad.
- Fixed an issue (introduced in the version 5.0.0 software upgrade) that was causing about a 30 second delay while connecting to SSH, Telnet or FTP.
- Added the ability to view the Authentication (Auth) log via the web browser (Tools -> Logs page).
- “Reference Change” log entries are now being sent to the Event log.
- Changes associated with a user either creating or updating a Local Clock are now logged in the Journal log.
- Resolved an issue with certain Journal log entries being sent to the wrong log.
  - Log entries for a user enabling/disabling Services (such as HTTP, Telnet and FTP) and the IPv4 Gateway were being sent to the Timing log instead of the Journal log.
- Differentiated the reporting of Rubidium oscillator error messages.
- Improved switching between GPS Modes (Standard, Mobile and Single Satellite)
  - Previous software versions periodically required a Mode selection change be submitted more than once for the change to occur.
- Fixed an issue with the propagation of the Local System Clock, if a previously created Local Clock was modified.
  - If a previously created Local Clock was edited, the output ports using that Local Clock would no longer be configured to use a Local Clock.

Security enhancements and fixes

- Removed the “arcfour” (ARC4, RC4) cipher from SSH.
- Reduced the SSH tryouts to 3.

Option Card enhancements and fixes

- (Option 16: Multi-port Ethernet module, if installed)
  - Added monitoring of the Multi-port Ethernet module’s three network interfaces.

- (Option 04: Rubidium Oscillator, if installed)
    - Differentiated the reporting of Rubidium oscillator error messages.

Version 5.0.0

Release features

- No new features added

Enhancements and fixes

- Upgraded the Operating System to a newer version in order to address a memory consumption condition
- Earlier versions of software could potentially consume too much memory, rendering the web browser inaccessible, until a reboot/power cycle was performed.
- Upgraded NTP to a newer version
- NTP was upgraded to version 4.2.6p5.
- Resolves potential “buffer overflow” messages from being asserted in the NTP log.
- Mitigates potential vulnerabilities associated with NTPQ/NTPDC.
- Removed the GPS Dynamics code for the GPS receiver mode selection
- The GPS Dynamics code (Stationary, Land, Sea, Air) for mobile operation is no longer necessary.
- Removed this configuration from the Setup -> Inputs -> Onboard GPS receiver page of the browser.
- The Dynamics code is no longer displayed on the front panel when GPS information is selected to be displayed or with the CLI interface commands associated with GPS Mode.
- IPv4 main default gateway is now tied to the default gateway of a specified interface rather than as an independent setting.
- Removed the NTP Local Clock Reference selection from the Network -> NTP Setup page of the browser, NTP servers tab
- In earlier versions, if a Stratum 1 reference had excessive 1PPS jitter (such as an unsynchronized IRIG generator), NTP could potentially resonate back and forth between selecting the Stratum 1 server and its own internal reference. A better method of going to Stratum 16 when no NTP servers are present, without needing to use the NTP Local Clock driver, was implemented.

Security enhancements and fixes

- Upgraded SSL to version 1.0.1e to mitigate potential vulnerabilities
- (CVE-2013-0169) “Lucky Thirteen” issue mitigated. TLS protocols 1.1 and 1.2 as well as DTLS protocols 1.0 and 1.2 can allow remote attackers to conduct distinguishing attacks and plain-text recovery attacks.
- Disabled SSL compression to mitigate potential vulnerabilities
- (CVE-2012-4929 and CVE-2012-4930) SSL/TLS CRIME attack against HTTPS mitigated.

- A few configuration fields in the “Network” Setup pages of the web browser were changed from text fields to “password” fields to prevent credentials from being in “plain sight” to users.
  These fields include the following in the “NETWORK” pages -> tabs:
- HTTPS/SSH SETUP, -> HTTPS tab: “Private Key Passphrase” and “Challenge Password”
- NTP SETUP -> Autokey tab: “Passphrase”
- LDAP SETUP, LDAP -> Servers Configuration tab: “Credential to Bind Server with”
- RADIUS SETUP -> Server Configurations tab: “Secret Keys”
- IPSEC SETUP -> SA Manual Configuration tab – all “Key” fields
- SNMP SETUP -> Notifications and Users tabs: “Auth Passphrases” and “Priv Passphrases”

Version 4.x

Release notes for NetClock software versions 4.x are available upon request. Please contact Technical Support, or your local Sales representative.

Which SW version is installed on my SecureSync?

To determine the software version currently installed on your unit:

A) **Using the new Web UI (Software versions 5.1.0 and above)**
Log in to the unit's Web UI. Click on "**Tools**", then "**Upgrade/Backup**". The "System Configuration" table on this page contains a "System" field. The number next to this is the current Archive software version:

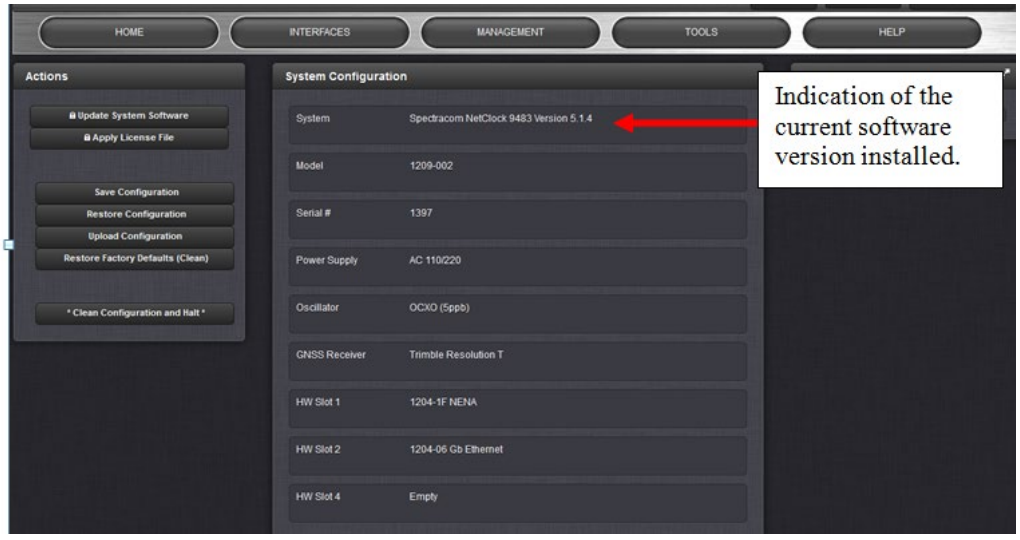

Figure 1: Software revision reported in the **Tools -> Upgrade/Backup** Page

B) **Using the "Classic Interface" (Software versions 5.0.2 and below)**
Log in to the unit's Web UI. Click on **"Tools"**, then "**Versions**". The "**System Version**" table on this page contains a field named "**Archive version**". The number next to this is the current Archive software version:

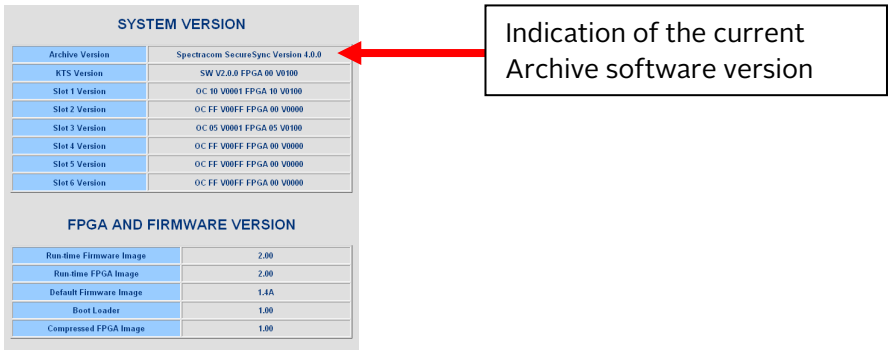

Figure 2: Archive software revision reported in the **Tools -> Versions** Page

How to download and install the new SW

Downloading the Software Update

The latest NetClock software update can be downloaded from the Orolia website under:
https://www.orolia.com/support/timing/securesync-netclock-9400

On this page, navigate to:

Installing the Software Update

Instructions on how to install the new software update can be found in the **NetClock Upgrade Instructions:**

This document is also available under the link provided above.

NOTE: The most current version of the main **User Manual** can be found under manuals.spectracom.com.

Hard copies of this User Manual may be purchased from the Orolia Sales department at US +1.585.321.5800.

How to contact Orolia Technical Support

Should you have any questions or comments regarding any of the above-mentioned features or fixes, please contact Technical Support:

https://www.orolia.com/support/orolia

- End of document -