Calnex
Insight and Innovation

User Guide
Sentinel Sync Analyser

Table of Contents

Sentinel Sync Analyser

1.1 Introduction

Calnex Sentinel is the all-in-one Synchronisation tester for testing both the legacy PDH/SDH networks and the newer SyncE, PTP (IEEE1588v2), NTP IP/Ethernet networks for mobile backhaul, data center, financial trading venues, power utility systems and, indeed, any network requiring Frequency, Phase or Time Synchronisation.

Sentinel measures PTP or clock Time Error (TE) 5G NR or 4G LTE networks that use either ITU-T G.8275.1 Full on Path support, or ITU-T G.8275.2 Assisted Partial Timing Support (APTS)/Partial Timing Support (PTS), as well as TE measurements over the air (OTA) by examining the timing signals within the NR or LTE transmission.

Sentinel is of modular design to allow for flexible configuration and easy future upgrade. It contains three slots where measurement modules can be fitted. Newer revisions (serial number 400XXX) of Sentinel come with two licensable PTP measurement channels built in, leaving the other slots free for clock measurement and OTA modules

Sentinel is designed to simultaneously measure any combination of SyncE, PTP/NTP, E1/T1, 10MHz, 1 PPS, RF air interface phase and user defined clocks to multiple industry and standards masks.

There are four different measurements module types available.

Clock module

- For Recovered clock measurement
- Provides two ports for Frequency, E1/T1 and 1 PPS measurement and analysis.

Packet module

- Emulates one PTP Slave clock on each packet module (maximum of two modules can be fitted)
- Transport protocol level for PTP measurement: UDP/IPv4, UDP/IPv6 or Ethernet
- PTP Multicast and Unicast supported
- PTP message rates up to 128 messages/sec
- PTP packet by packet capture, measurement and analysis of PDV and TE
- PTP TE and PDV measurements based on PTP event message timestamps
- NTP packet by packet capture, measurement and analysis of PDV and TE
- Emulated NTP Client on each module
- SyncE wander generation and measurements to G.8262
- Simultaneous measurement of SyncE and PTP/NTP for measuring Hybrid networks
- 1 Ethernet port supporting 100 M / 1GbE interface rates

Packet module (10GbE)

- Identical functionality to packet module
- Maximum of two Ethernet ports supporting 100M / 1GbE / 10GbE interface rates

Over the Air (OTA) module

- Determine absolute timing accuracy of 5G NR gNodeB or 4G LTE eNodeB RF interface
- Frequency range from 350 MHz to 6GHz

Sentinel supports real-time measurements and metric analysis of SyncE and clock TIE/MTIE/TDEV metrics and Packet PDV, FPP, Packet Distribution, 2 Way TE and 1 PPS TE. Additionally, it supports the measurement of Max |TE|, cTE and dTE to G.8271.1 and pktSelected 2 Way TE for G.8271.2 APTS/PTS networks.

Sentinel has a built-in high-quality Rubidium clock which can be trained by GNSS (GPS, GLONASS, Galileo, Beidou and QZSS) or external 1 PPS (Rb- or Cs-Quality). The Rubidium is battery backed up to allow it to be held in holdover >3 hours, so that Time can be maintained while travelling to the test site.

It is equipped with a large 8.4" colour LCD touch screen, clearly showing graphs of Wander TIE/MTIE/TDEV and PTP/NTP PDV, Time Error, FPP, MAFE, Packet Distribution and other ITU-T metrics in real time during a measurement. With an intuitive graphical interface, Sentinel is a user-friendly instrument.

1.2 Description

Front panel
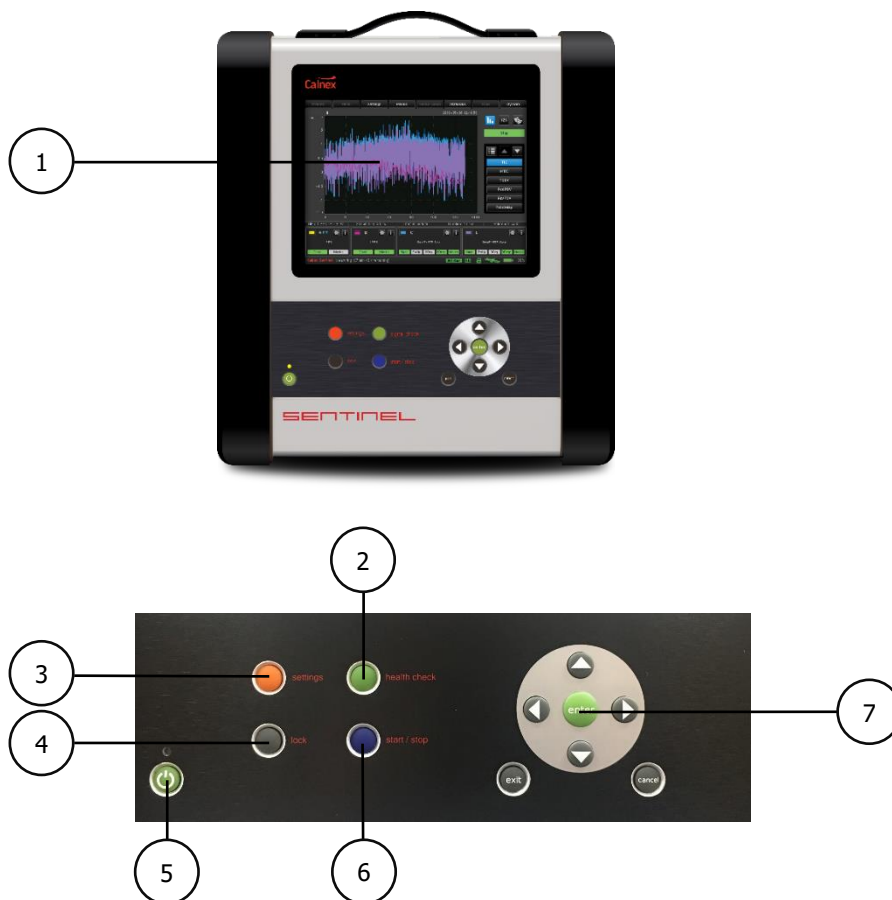
1		Colour LCD touch screen
2		Health Check Opens the Health Check menu.
3		Settings Opens the Settings menu
4		Lock Lock/Unlock the touch screen
5		Power Instrument power on/off button. Press to switch on and to switch off the instrument. In the Stand-by mode, power is maintained for the internal rubidium timebase, as long as the mains cable is connected to the mains outlet.
6		Start/Stop Measurement start/stop button
7		Keypad Buttons for navigation in the menus displayed on the screen [Enter] Confirm

[Exit] Exit from the menu, save the selection, and return to the previous page
[Cancel]

Right Panel

8	Clock module 2 channels per module, BNC connectors
9	Packet Module 1 channel per module, RJ45 or SFP connector

Left Panel

10	Main connection Power Supply

11	Antenna	GNSS antenna connector
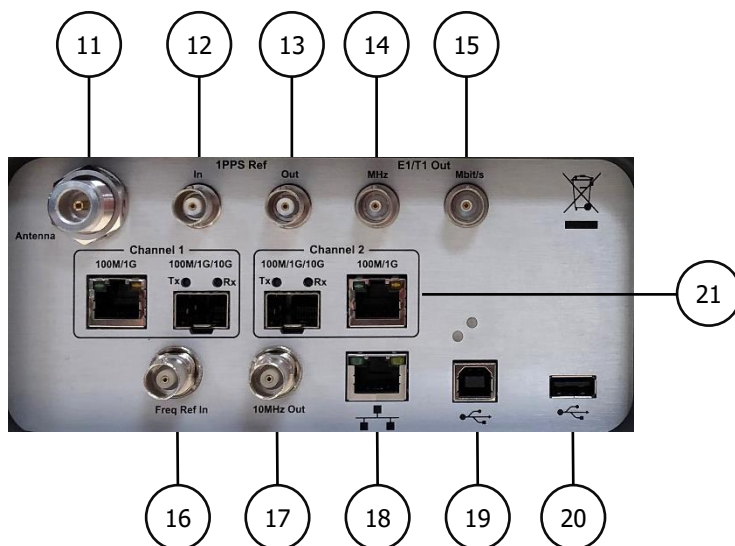
11 Antenna
GNSS antenna connector

12 1 PPS in – TTL / 50Ω
External 1 PPS phase reference input.

13 1 PPS out – TTL / 50Ω
Internal 1 PPS timing output from Rubidium oscillator.

14 E1/T1 clock output (MHz)
User settable E1 or T1 clock output, BNC 75Ω.

15 E1/T1 framed output (Mbit/s)
User settable E1 or T1 framed output, isolated BNC 75Ω.

16 External reference
Input for precision external reference (1, 5 or 10MHz clock).

17 Reference signal output
10MHz frequency from the internal reference or the external reference (if selected).

18 Ethernet network connector
Standard RJ45 connector for connecting the instrument to a PC or LAN using the 10/100BASE-T protocol, enabling remote control over Ethernet.

19 USB type B connector (for future use)
USB Device port

20 USB type A connector
USB Host port

21 10GbE packet module
Up to 2 channels per module, RJ45 or SFP connectors

Accessories delivered with the instrument

- Line power cord
- GNSS Antenna and 20m cable
- User Guide & CAT Analysis software on USB stick

1.3 Specifications

General Specifications

Power Supply

- Line Voltage: 100-240V~, 50-60Hz, <150W

Environmental Data

- Temperature: Operating: 0°C to 40°C
- Safety: EN 61010-1:2010, CAT II, Pollution degree 2, Measuring category I, CE
- EMC: EN61326-1:2013

Mechanical Data

- Fold-out stand; Shock resistant cabinet
- Dimensions (w x h x d): 320 x 388 x 126 mm (12.6" x 15.3" x 5")
- Weight: Net <7kg (15lb); Shipping with transport case < 16kg (35lb)

Platform Specifications

- Reference Clock: Built-in Rubidium reference or external reference input 1, 5 or 10MHz
- Display: Colour TFT, 8.4", 800x600 pixels
- Internal Memory: sufficient for > 3 days measurement

Internal Time Base Stability (hold-over)

- Stability Versus Temperature: 20 to 26 °C: <1x10-11 (typ.), -20 to +65°C: <$1x10^{-10}$ baseplate
- Ageing Rate per 24 h: <$5x10^{-11}$ per month); <$5x10^{-10}$ (yearly)
- Warm-up Stability: 12 min to <$1x10^{-9}$
- Allan Variance: <$2x10^{-11}$ (1s); <$1x10^{-11}$ (10s); <$2x10^{-12}$ (100s)

GNSS disciplining

- Built-in GNSS module: 12 channels, TRAIM GNSS receiver, high sensitivity
- Supported constellations: GPS, GLONASS, Galileo, Beidou and QZSS
- Frequency accuracy: $2x10^{-12}$ averaged over 24 hours

Input Modules

Clock module

- Number of channels: 2 per module
- Connector: BNC, unbalanced
- Frequency: 1 PPS/2s to 200MHz
- Impedance: 75Ω or 1MΩ selectable
- Voltage Range: from -5V to +5V
- Sensitivity: 60mVpp
- Signal Type: Symmetrical pulse (Clock signal), Unsymmetrical repetitive pulse (Clock signal), HDB3-coded data (Data signal), AMI B8ZS, B3ZS (Data signal)

Packet module

- Connectors: RJ45 for 10/100/1000BASE-T, SFP 100M/1GbE
- Number of channels: 1 per module
- SyncE Wander measurement Accuracy: 1ns
- PDV measurement accuracy: 5ns
- Time Error Accuracy: +/-75ns with reference to GNSS

10GbE Packet module

- Connectors: RJ45 for 10/100/1000BASE-T, SFP(+) 100M/1GbE/10GbE
- Number of channels: up to 2 per module
- SyncE Wander measurement Accuracy: 1ns
- PDV measurement accuracy: 5ns
- Time Error Accuracy: +/-75ns with reference to GNSS

OTA module

- Connectors: SMA connector for RF antenna

- Number of channels: 1 per module
- Time Error Accuracy: +/-100ns with reference to GNSS

External References

Frequency Reference Input

- Input Frequency: 1MHz, 5MHz or 10MHz
- Voltage Range: 0.1Vrms to 5Vrms
- Impedance: approx. 50Ω

External 1 PPS Timing Input

- Voltage range: 0V to 0.8V (Low), 2V to 3.3V (High) into 50Ω
- Required accuracy: ± 100ns to UTC

GNSS Timing Reference

- Antenna input: N-type connector
- DC-feed: +5V on centre pin to active antenna

Output References

Frequency Reference Output

- Ref. Frequency: 10MHz sine-wave
- Output Levels: 1Vrms in 50Ω

1 PPS Output

- Source: Internal Rubidium oscillator
- Output Level: TTL levels in 50Ω

E1/T1 Output

- Connector: Clock: BNC; Data: isolated BNC
- Frequency: 1.544/2.048MHz, 1.544/2.048Mb/s
- Output Level: Acc. to G703:10; ±1.2V ±10% in 75Ω

Interfaces

USB Device port

- Connector: USB type B
- USB version: 2.0

USB Host port

- Connector: USB type A
- Max supply current: 400mA
- USB version: 2.0

Ethernet

- Communication port: RJ45, 10/100BASE-T
- Protocol: DHCP and FTP server, VNC

Safety Instructions

2.1 Introduction

Read this page carefully before you install and use the instrument.

This instrument has been designed and tested according to safety Class1 requirements of standard IEC/EN 61010-1 and has been supplied in a safe condition. The user of this instrument must have the required knowledge of it. This knowledge can be gained by thoroughly studying this manual.

This instrument is designed to be used by trained personnel only. The cover of the instrument must only be removed for repair by Calnex personnel who are aware of the hazards involved. There are no user-serviceable parts inside the instrument.

If the surface of the Sentinel becomes dirty, remove the AC power and clean with a soft lint-free cloth. Never use flammable liquids to clean the device.

2.2 Safety Precautions

To ensure the correct and safe operation of this instrument, it is essential that you follow generally accepted safety procedures in addition to the safety precautions specified in this manual.

Use of this equipment in a manner not specified by Calnex, may impair the protection provided by the equipment.

This equipment is portable and should be lifted and carried by handle only, never use the tilt bail to lift the unit.

In normal operation the openings in the chassis should be not be blocked, to allow for cooling of the internal components.

Always operate the equipment with unrestricted access to the AC power connector.

Caution and Warning statements

CAUTION:	**WARNING**:
Shows where incorrect procedures can cause damage to, or destruction of equipment or other property.	Shows a potential danger that requires correct procedures or practices to prevent personal injury.

Symbols

Indicates that the user should consult the manual.

Shows where the protective ground terminal is connected inside the instrument. Never remove or loosen this screw.

If in doubt about Safety

Whenever you suspect that it is unsafe to use the instrument, you must make it inoperative as follows:

- Disconnect the mains cable.
- Clearly mark the instrument to prevent its further operation.
- Contact Calnex customer service.

For example, the instrument is likely to be unsafe if it is visibly damaged.

2.3 Grounding

Whenever an instrument is connected to the mains voltage, any grounding fault will make it potentially dangerous. Before connecting any unit to the mains supply, you must make sure that the protective ground functions correctly. Only then can a unit be connected to the mains supply and only by using a three-wire mains cable. No other method of grounding is permitted. Extension cords must always have a protective ground conductor.

A power supply cord is supplied with the equipment. If the user is obtaining a pluggable power cord for use with their local power connection the power cord must meet all local safety requirements, have an integrated safety ground wire and be rated for the power requirements of the Sentinel.

WARNING:

If a unit is moved from a cold to a warm environment, condensation may cause a shock hazard. Ensure that the grounding requirements are strictly met.

WARNING:

Never interrupt the grounding cable. Any interruption of the protective ground connection inside or outside the instrument or disconnection of the protective ground terminal is likely to make the instrument dangerous.

2.4 Power Switch

This instrument is equipped with a secondary power switch. It disconnects the main power-consuming circuits on the secondary side of the power supply. Mains voltage is always present on the primary side.

WARNING:

Always consider the instrument active as soon as it is connected to the primary AC power source with a mains cable. Disconnection of the mains cable completely cuts off the power supply to the instrument.

2.5 Disposal of Hazardous Material

This instrument uses a 3V lithium cell to power a Real Time Clock. It is placed in a holder and can be replaced by qualified personnel who are aware of the hazards involved.

> **WARNING**:
>
> Disposal of lithium cells requires special attention. Do not expose them to heat or to excessive pressure, which may cause the cells to explode. Make sure they are recycled according to local regulations.

2.6 GNSS Antenna Installation

This instrument is equipped with GNSS receiver which requires GNSS antenna input. This input should be connected properly and safely to the external GNSS antenna.

> **WARNING**:
>
> For permanent installation, the GNSS antenna and associated cables require an EMP Protector to be fitted for safety reasons. The EMP Protector should be professionally fitted as per the manufacturer's instructions. These instructions come with the EMP Protector.
>
> Observe all local regulations on the fitting, grounding and specification of lightning or surge arrestors on the antenna cable.
>
> Disconnect or switch off in-line equipment when installing, checking, disconnecting and connecting EMP protectors. This includes also the exchange of gas discharge tubes. Keep back from such activities during thunderstorms. Be aware that only a complete protection system according to IEC 62305-1 can protect your equipment and personnel against the impact of lightning.
>
> This includes an external lightning protection system with air terminal, down conductor and grounding system and bonding of all incoming and outgoing lines (e.g. protectors for mains, data and telephone lines) - not RF lines only.
>
> With gas discharge tube protectors take care that the GDT has been properly installed before putting the equipment into operation.

Using Sentinel

3.1 General Operation

Set-Up

Connect the source(s) under test to the inputs on the Clock or Packet modules

By default, the frequency reference to use is automatically selected. The Rubidium reference is used, unless a valid external reference is connected to the external reference **Freq In** connector.

Connect the instrument to the mains supply and turn on the power switch: the instrument switches on automatically.

An identification screen is displayed, then the main instrument software starts up.

On completion of start-up, the following screen is displayed, with the message **Ready** at bottom-left of the screen; the instrument is ready for use (in case of a cold start the message will be **Warming Up...** and the Rubidium icon on bottom-right will be yellow).
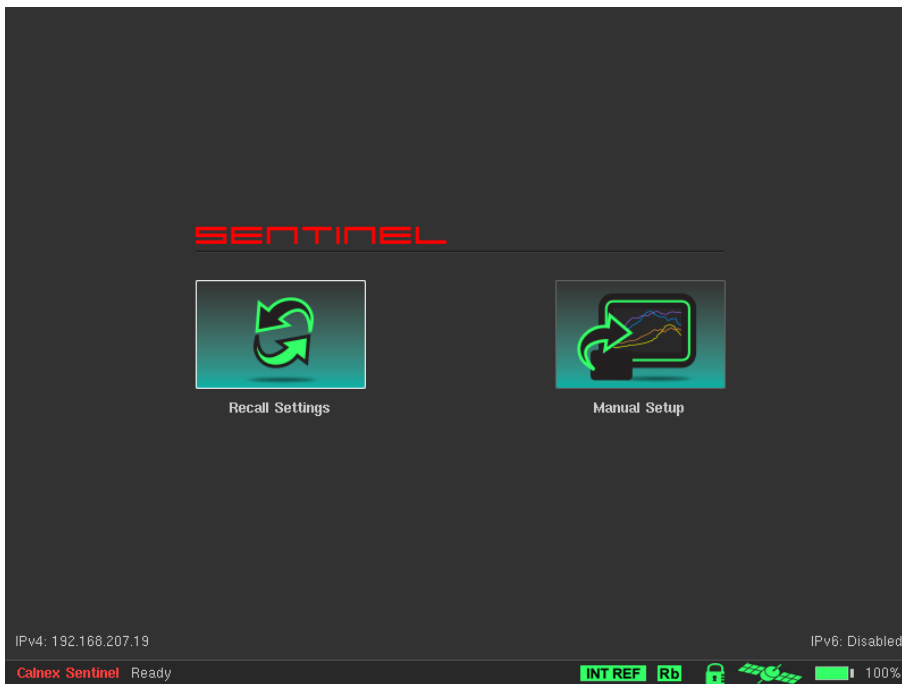
The **Recall Settings** option allows previously saved configuration files to be re-loaded, automatically setting up Sentinel to the state defined in the preset file and then displaying the main operating screen. Selecting the **Manual Setup** option moves directly to the main operating screen.


Battery Option

If the **Battery Option** is present, it can be used for providing power to the internal Rubidium oscillator during transport to site (**Transport Mode**). Information about installed options is available in the **About** page of the **System** menu. Also, when the **Battery Option** is present the corresponding icon in status bar will display battery charge percentage:

If the **Battery Option** is installed then upon switching off the instrument, the user is asked if **Transport Mode** should be turned on. In **Transport Mode**, Sentinel will use the battery to keep the internal Rubidium oscillator powered for up to 3 hours when mains supply is not present.
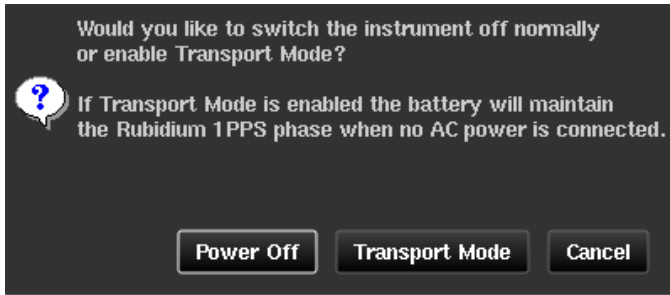
Note: When in **Transport Mode**, the battery will not be charged. The battery is only charged when Sentinel is powered on and running.

Switching off

The instrument is switched off by pressing the button ⏻ on the front panel. When the indicator light turns on red the instrument is switched off.

As long as the instrument is connected to the mains supply, the internal Rubidium oscillator is powered up and retains its characteristics.

Disconnection of the mains cable completely cuts off the power supply to the instrument unless the **Battery Option** is installed, in which case only the Rubidium oscillator remains powered.

3.2 Controls

The main screen contains controls to allow simple, ordered **Configuration (1)** and **Operation (2)** of Sentinel. Navigation buttons allow movement between each **Measurement Result Graph (3)** and change the mode of **Viewing Results (4)**. The status of the measurement sub system is shown in **Widgets and Icons (5)** at the bottom of the screen.

These will be described in detail in the following chapters of the user guide.

Configuration settings

Manual configuration of Sentinel is simply a process of working through the tabs on the main screen as detailed below.

| Presets | Mode | Settings | Masks | Health Check | Data | System |

4.1 Presets

Measurement settings can be saved and reloaded later. The user can choose the filename and current Settings will be saved in a **.preset** file. This function is especially useful for fast setup in the field.

Factory default settings can be restored using the **Restore to Defaults** button.
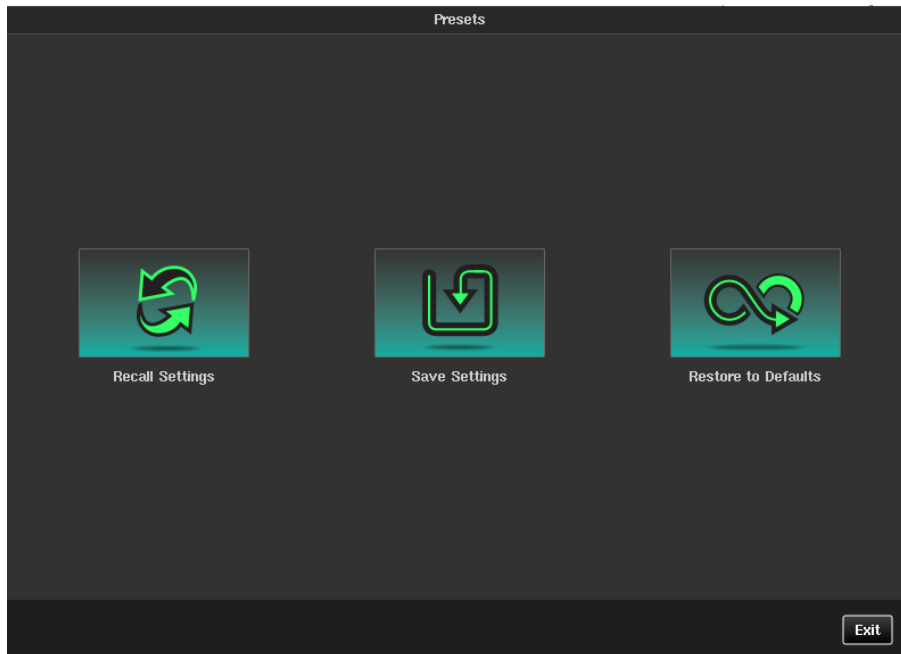
4.2 Mode

The **Mode** screen allows the Sentinel measurement subsystem to be configured as required for the type of testing being performed. Sentinel expansion slot channels are labelled A – F and the 10 GbE module is labelled 1 – 2. This screen will reflect which modules are installed in Sentinel. The example below shows that one Clock module, an OTA module and the 10GbE packet module with 2 channels are installed. The user can enabled/disable channels on this screen according to requirements. **Monitor Mode** can also be selected through this screen (two packet ports need to be installed and **PDV option** needs to be enabled for this option to be available). Note that for the 4G/5G OTA module, only one OTA measurement type may be selected at a time. For the 4G OTA module, only **OTA-LTE** is present.
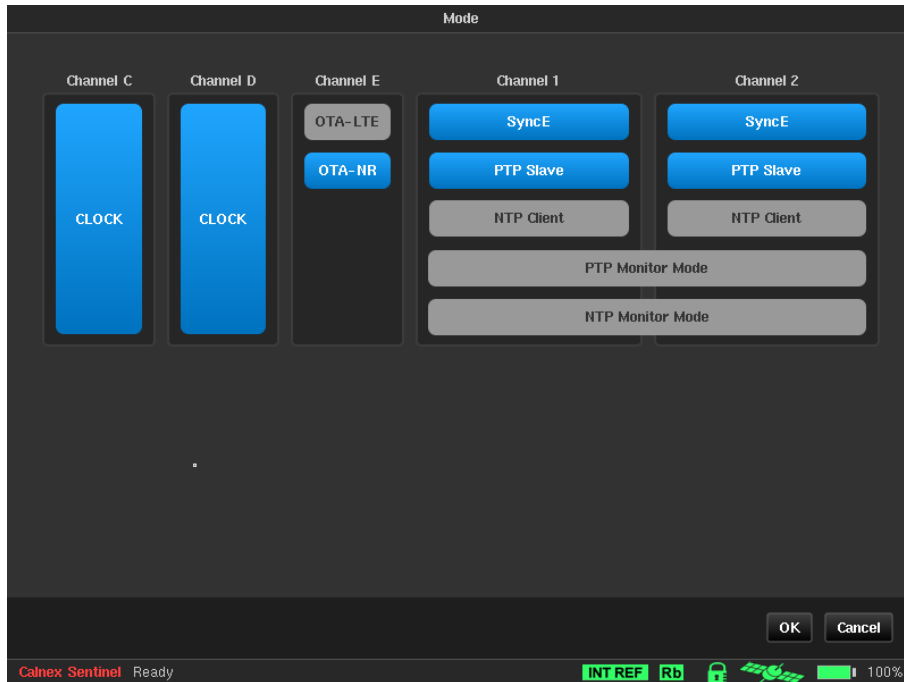
If a channel is disabled on the **Mode** screen, this will be reflected in the corresponding **Widget** on the main screen. Disabling unused channels simplifies configuration and result viewing by removing these channels from the configuration and results screen.
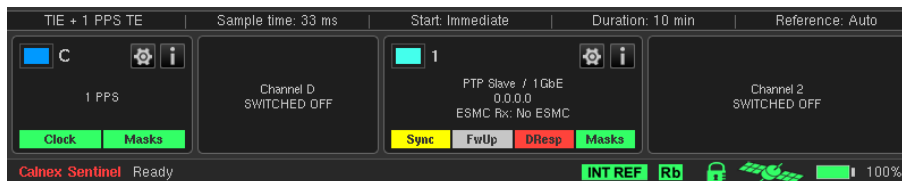
4.3 Settings

The settings area contains multiple tabs to configure all the relevant measurement subsystems selected through the mode screen and some options that are common to all measurement types.

A common set of buttons are displayed permanently on each of the **Settings** screens. The buttons always have the following functionality:

OK Apply all the settings changes that have been made whilst in the settings screens. When applied return to the main display

Cancel Cancel all settings changes that have been made to date within the exception of any that have already been applied using the **Apply** button

Apply Apply all settings changes that have been made and remain in the settings screen
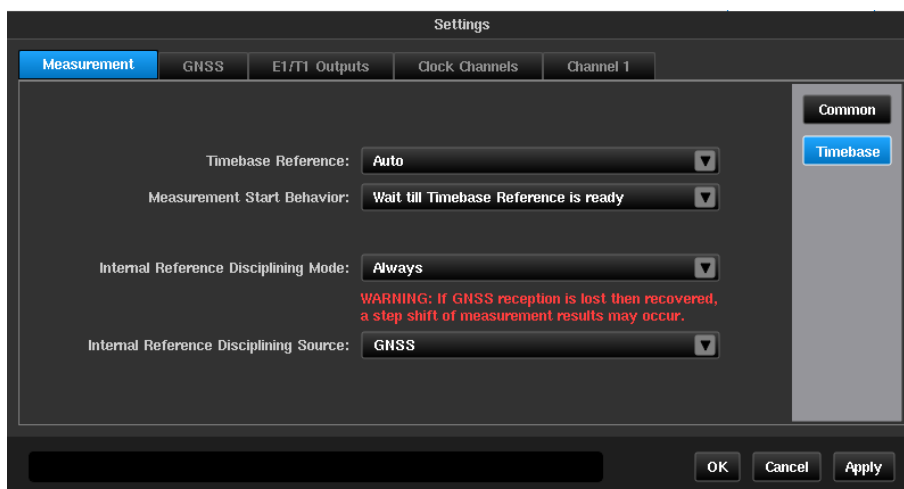
Measurement

Common

The **Common** page is used to define the general characteristics of the measurement.

Start	Defines when the measurement should start and allows the following options
Immediate	Start the measurement as soon as the **Start** button is pressed
Timer	Start the measurement at the specified time
Start time	Defines start time when **Start** mode is *Timer*
Continuous Measurement	Defines whether the measurement when started should run on a continuous basis. This results in a series of 24 hours measurements being made. A new measurement is started each time 00:00 UTC is reached. The last 7 days of measurement data is retained in the folder named *continuous* within the internal storage. Each day of data is stored in a folder within the *continuous* folder with a name indicating the day the measurement started based on UTC time.
	Whilst running in this mode it is not possible to measure any metrics e.g. TDEV, MTIE.
	No masks will be checked whilst continuous mode is enabled.
Metrics	This disables metric calculation (e.g. TDEV, MTIE) and mask checking during measurement.
	If this option has been selected and metrics are required after a measurement has been completed, this can be achieved using the Calnex Analysis Tool (CAT) which is supplied with Sentinel.
Duration	Duration of the measurement. The measurement duration is defined either by the time entered in the **Duration** field or by the stop time entered in the **Stop time** field. If a duration is entered, the **Stop time** is updated accordingly, and if a stop time and date are entered, the measurement duration is updated accordingly
Stop time	Defines stop time when **Start** mode is *Timer*
Estimated Data size	Displays estimated size of file for measurement data. Depending on the configuration, if the duration exceeds a certain length, the instrument enters **Long Term mode**. In **Long Term mode** only some of the available graphs are displayed and no metrics are calculated
Sample time	Measurement interval. Signal measurements are made point by point at regular intervals defined by entry using the virtual keyboard. *33ms* is the default setting to provide 30 TIE samples per second in accordance with the recommendations for wander measurement equipment in ITU-T O.172
Auto-Restart	The user can define if they want the measurement to restart should there be a power interruption during the measurement
TIE Mode	This parameter allows the selection of the following measurement modes
TIE	General TIE measurement for every enabled input channel

TIE + 1 PPS TE	All connected 1 PPS signals will measure absolute differential TIE relative to the signal connected to the reference channel. All other signals measure normal TIE relative to the selected timebase
TE	This performs the same measurement as *TIE*, but the initial phase offset of each signal is not compensated for
Diff TIE	All connected signals (including SyncE) will measure differential TIE relative to the signal connected to the reference channel. See **Diff TIE Reference** setting
Diff TE	This performs the same measurement as *Diff TIE*, but the initial phase offset of each signal is not compensated for
Diff T(I)E reference	Drop-down list for selection of the input channel or internal reference to be used as reference when **TIE Mode** is *Diff TIE, Diff TE* or *TIE + 1 PPS TE*
G.8271.1 TE Mask Value	Sets the absolute value for the G.8271.1 Max|TE| mask. This is user defined and configures the Pass/Fail limit for TE measurements when that mask is selected

Note: In all cases, even a delayed start, the measurement is not made until the **Start** button is pressed.

Timebase

The **Timebase** page provides the following settings:

Timebase Reference

Internal	Use the internal Rubidium as the reference for measurements
External	Use an external reference for measurements
Auto	Use an external reference if connected to the **Freq In** connector and if not use the internal Rubidium reference.

Measurement Start Behavior

Start even if Timebase Reference is not ready	This will start a measurement even if the internal Rubidium reference is not fully warmed up
Wait till Timebase Reference is ready	The measurement will wait until the reference is fully ready and warmed
Abort if Timebase Reference is not ready	The measurement will fail if the reference is not ready to proceed

Internal Reference Disciplining Mode

Never	Disable disciplining. The internal Rubidium will remain in free running mode and will never discipline to GNSS or an external reference even if available.
Not during measurement	Enable disciplining, but do not use it during measurement
Always	Enable disciplining always, the Rubidium reference will not discipline if a suitable reference is not available.

Internal Reference Disciplining Source

GNSS	Use internal GNSS receiver.

|	
	If the last disciplining was less than 1 week ago, Sentinel should be disciplined for at least 6 hours, otherwise Sentinel should be disciplined for at least 12 hours
Ext 1 PPS (GPS/Rb Quality Source)	Use 1 PPS signal from external GPS receiver or external Rb quality atomic clock
Ext 1 PPS (Cs Quality Source)	Use 1 PPS signal from external Cs quality atomic clock

Note: Sentinel will only discipline if the disciplining source selected is producing a valid disciplining output and so **Internal Reference Disciplining Mode** can be left to *Always* even if the source is not available. If the source is re-connected during a measurement, then there may be a phase shift in the timebase reference.

GNSS

This page allows selection of GNSS constellation and displays general GNSS information received: position, altitude, number of satellites that receiver is locked to, antenna status and signal levels for all visible satellites.
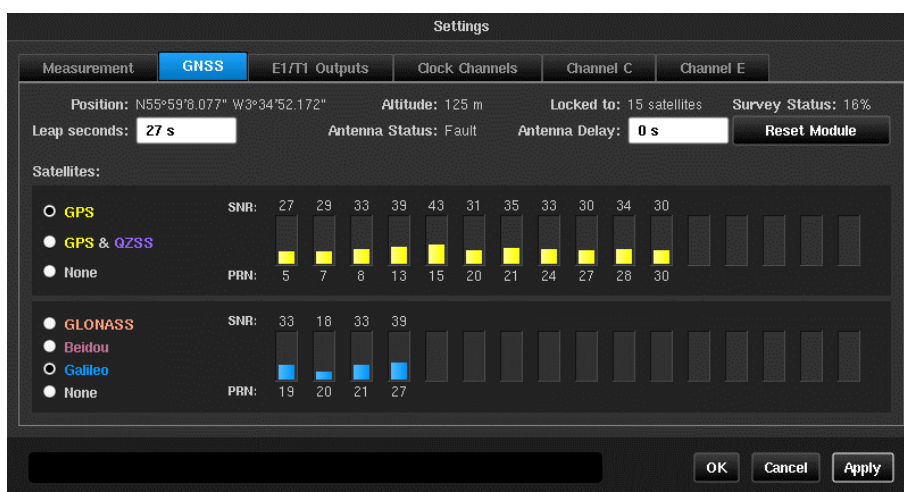
The top constellation selection determines whether GPS is used and if GPS is selected, whether QZSS is also used. If GPS is not selected, a constellation must be selected in the lower selection area. For multi-constellation operation, select GPS or GPS and QZSS and a secondary constellation.

Press **Apply**. This will cause the GNSS module to reset and begin a new site survey using the new constellation(s).

NOTE: Changing constellations will cause the Rb timebase to unlock and it may experience a step input from the GNSS 1 PPS output. It is recommended that Sentinel remains disciplining to GNSS for at least 6 hours after changing constellations. This period should be at least 12 hours if Sentinel has not been disciplined for more than a week.

Satellite SNR status is shown in the same colour as the text in the constellation name. The **Locked to** status displays the total number of locked satellites over all selected constellations.

GPS, Galileo and Beidou satellites transmit information that allows Sentinel to calculate the number of leap seconds that have occurred, and this is used to determine the offset between TAI and UTC. The **Leap seconds** value is updated automatically whenever this information is received.

GLONASS does not transmit leap second information and the Leap seconds must be manually entered if the current value is not correct. PTP uses TAI as the time base for its timestamps and if **the Leap seconds** value is incorrect it will show as whole seconds of offset in the FwdPDV, RevPDV and 2WayTE graphs.

Survey status shows progress of the GNSS receiver site survey.

Reset Module allows the GNSS receiver to be reset.

Antenna Delay setting is used to compensate for antenna cable length.

NOTE: Support for multiple GNSS constellations is dependent on the correct revision of GNSS module hardware being fitted. If, after installing R9.1, no additional constellations can be configured then please submit a problem report to support@calnexsol.com requesting information on whether multi-constellation operation can be added.

The following table shows valid GNSS configurations

GPS	GLONASS	Galileo	Beidou	QZSS
✓				
	✓			
		✓		
			✓	
✓	✓			
✓		✓		
✓			✓	
✓				✓
✓	✓			✓
✓		✓		✓
✓			✓	✓

E1/T1 Outputs

This page defines parameters of the signals generated by **E1/T1 out** ports. Various options are available to specify the type of signal that will be output on the **E1/T1 out** port

Clock Channels

Channels

The **Channels** settings are used to define the characteristics of the input channels. The displayed values are those identified by the **Signal check**, if the check has been carried out.

Each installed channel (**A** to **F** depending on modules fitted) is displayed on a line with the following columns:

Signal type[1]   Drop-down list for selection of the type of input signal, including:

- Standard signal types predefined in the instrument
- Signal types defined manually (refer to the "Signals" menu below).

Trigger level   Within the limit ± 5V

Cable comp.[2]   Value up to 1000ns to compensate for delay introduced by the length of cable. (1 PPS signal only)

1 PPS converter[2]   Drop down list to select if Calnex converter box is being used to convert balanced 1 PPS to single ended 1 PPS. When enabled, this will automatically compensate for the delays introduced by that device.

Slope   Drop-down list defining the trigger slope: Positive or Negative

Impedance   Drop-down list defining the channel impedance, 75Ω or 1MΩ

Filter   Drop-down list (*ON/OFF*) for application of a predefined RC-type analogue LP filter with a cut-off frequency of approximately 10kHz and signal rejection of 13dB at 1MHz. This filter is used to suppress noise on 1 PPS signal measurements

Signals

The **Signals** screen is used to define the input signals not included in the predefined list in the instrument. Only clock type signals can be defined in this menu.
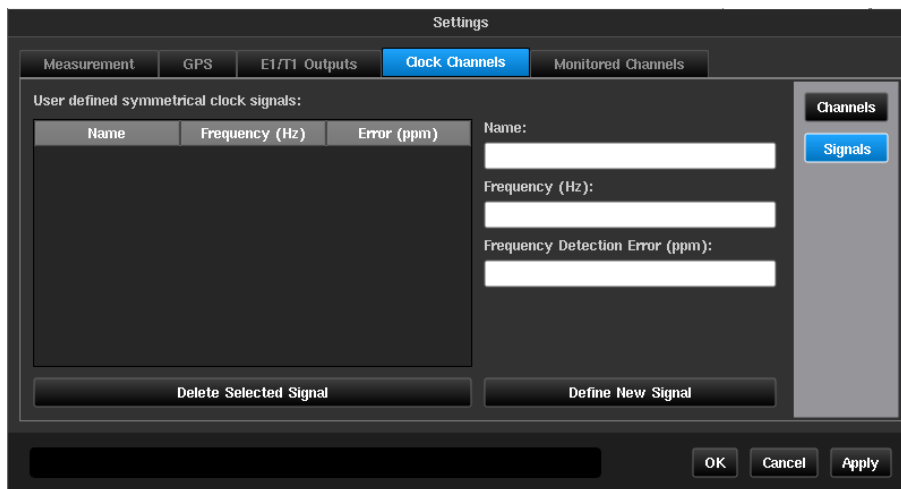
On the left the signals already defined manually are listed. A signal can be deleted by selecting it (highlighted) then pressing the **Delete selected signal** button.

The fields on the right are used to define a new signal type, by entry using the virtual keyboard.

Name   Entry of the signal name

Frequency   The accepted values are those measurable by the instrument, i.e. 1 PPS/2s to 200MHz

Frequency Detection Error   Tolerance in ppm on the frequency detected by the system during the signal check. If the measured signal is out of tolerance, a **signal unknown** message is displayed as result of the signal check
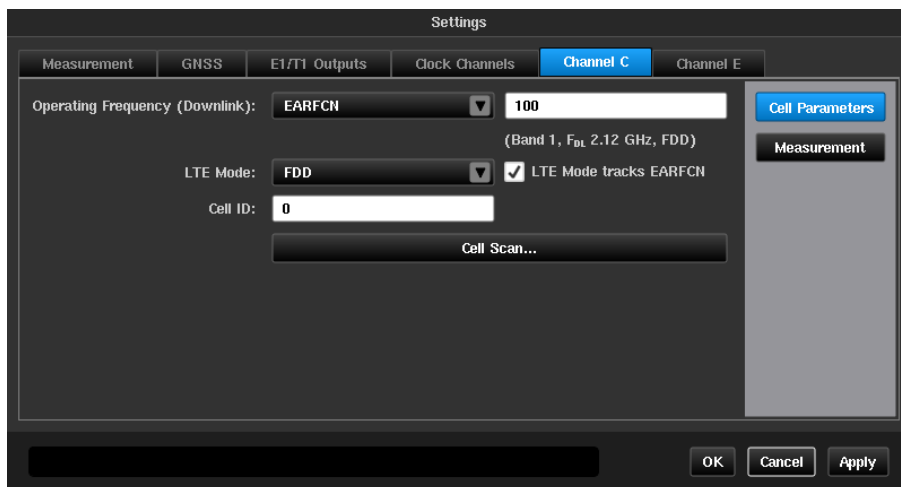
---

[1] Signal types shown in Appendix A

[2] These items will be greyed out if **Settings->Measurement->Common TIE Mode** is not set to *TIE + 1 PPS TE* or the signal type is not **1 PPS**

Channel *X* (OTA-LTE)

Selecting **OTA-LTE** in the **Mode** screen will enable a **Channel *X*** tab to be presented in the Settings screen.

Cell Parameters

| Operating Frequency (Downlink)	This allows the frequency of the LTE RF signal to be entered, either as the EARFCN or directly as an absolute frequency. Valid range is 350 MHz to 6 GHz or an EARFCN defined in TS 36.521 Table 5.4.4-1
LTE Mode	Selects whether LTE is Frequency Division Duplex (FDD) or Time Division Duplex (TDD)
LTE Mode tracks EARFCN	Selects whether LTE mode is automatically set based on the EARFCN chosen
Cell ID	Identifies which cell in the LTE frequency band is to be used as the source of the measurement.
Cell Scan	Pressing this button will cause each Cell ID within the selected frequency band to be displayed along with a confidence level indicating the quality of the decoded result.

Cell Scan

The Cell Scan feature simplifies cell parameter filling by giving the user the option to select desired Cell IDs from a list. After pressing the **Cell Scan...** button, a scan of the selected frequency is performed, and the list of possible Cell IDs for OTA-LTE measuring is displayed.
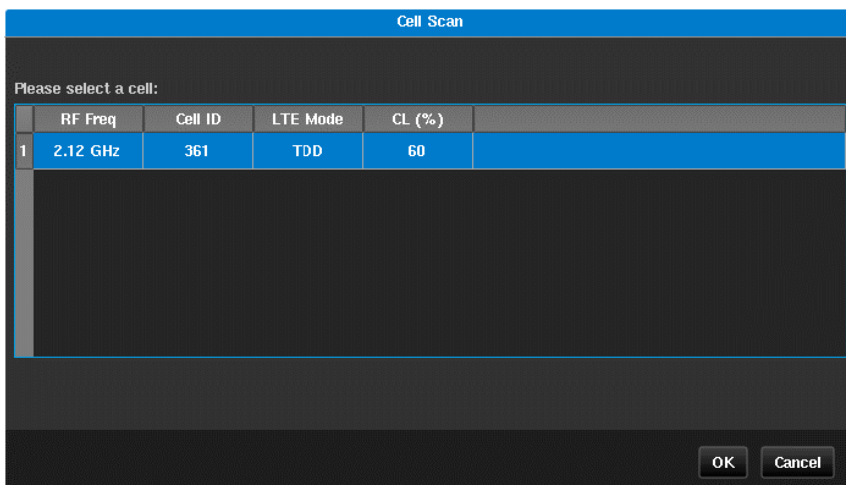
After the user selects a row in the table and presses the **OK** button, the corresponding fields in the cell parameters configuration page are automatically filled.
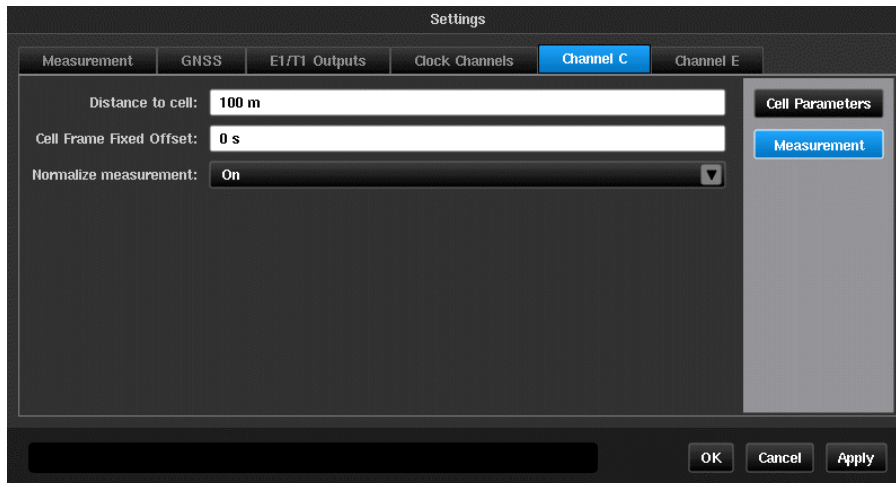
Measurement

| Distance to cell	Compensates for the time of flight of the RF signal to the test site
Cell Frame Fixed Offset	Compensates for any known offset of timing pulses from start of cell
Normalize measurement	When set to *On*, TE samples are normalised relative to the first sample i.e., the value of the first TE sample is zero. In this mode TE variation is displayed on the TIE graph. When set to *Off*, no TE normalization is applied i.e., the TE graph displays absolute delays (including propagation delay, time offset between Master and Sentinel, and other time inaccuracies in the system).

Channel *X* (OTA-NR)

Selecting **OTA-NR** in the **Mode** screen will enable a **Channel *X*** tab to be presented in the Settings screen.

Cell Parameters
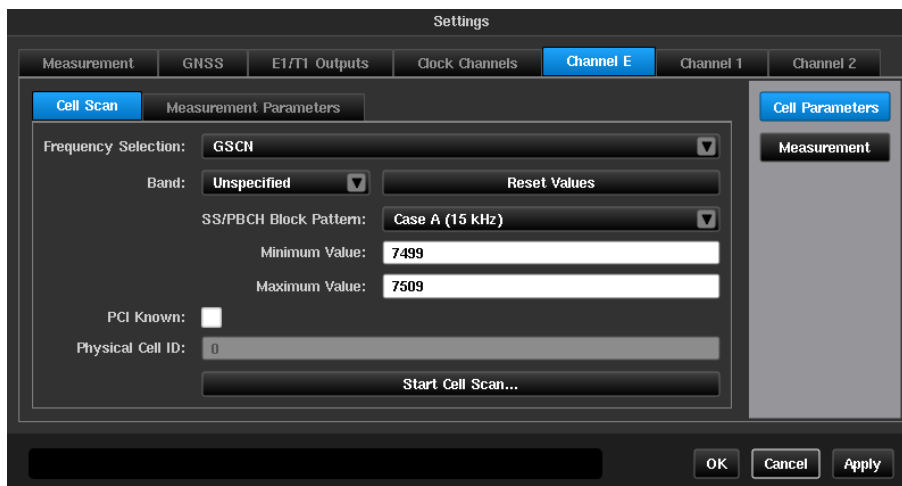
Cell Scan

Frequency Selection	This allows the frequency of the NR RF signal to be entered, either as the GSCN or nrARFCN or directly as an absolute frequency. Valid range is 350 MHz to 6 GHz.

Band	Selects the NR frequency band if GSCN or nrARFCN Frequency Selection is used.
SS/PBCH Block Pattern	Selects which subcarrier spacing pattern is used by the signal to allow Sentinel to detect and decode the Synchronisation Signal Block.
PCI Known	Enables option to enter Physical Cell ID, if known. If not known, cell scan will return a list of all detected PCIs.
Physical Cell ID	Identifies which physical cell in the configured NR frequency range is to be used as the source of the measurement. Valid range is 0 to 1007.
Start Cell Scan	See **Cell Scan** section below for details.

Measurement Parameters

Signal parameters can be manually entered on this page, if known, without a cell scan being required. If manually entering parameters, only one of the three frequency parameters is required – **SSB Downlink**, **GSCN** or **ARFCN**. When one of these is entered, the other two will automatically populate. Alongside one frequency parameter, **PCI** (Physical Cell ID) and **SS/PBCH Block Pattern** are required fields.

Cell Scan

The Cell Scan feature simplifies entering cell parameters by giving the user the option to select the desired Cell ID from a list. After pressing the **Start Cell Scan...** button, a scan of the selected frequency is performed, and the list of possible Cell IDs for OTA-NR measuring is displayed. If PCI value is configured, only that Cell ID will show.
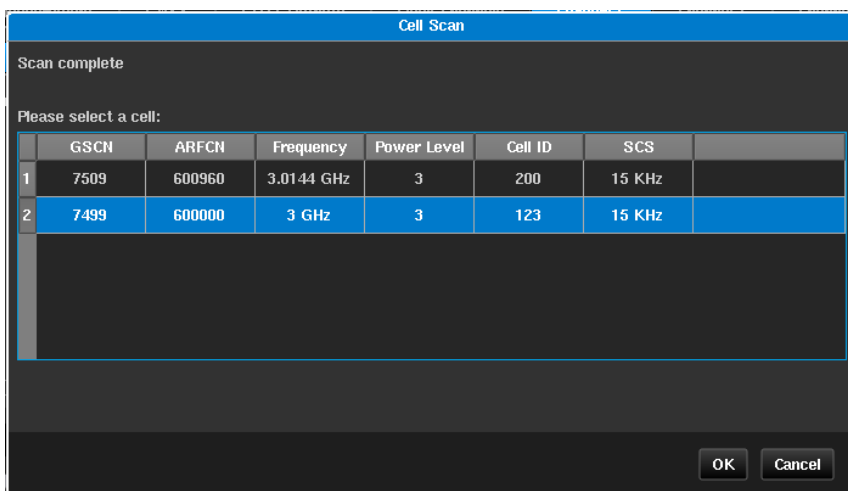
After the user selects a row in the table and presses the **OK** button, the corresponding fields in the **Measurement Parameters** configuration page are automatically filled.

Measurement

Distance to cell	Compensates for the time of flight of the RF signal to the test site
Cell Frame Fixed Offset	Compensates for any known offset of timing pulses from start of cell
Normalize measurement	When set to *On*, TE samples are normalised relative to the first sample i.e., the value of the first TE sample is zero. In this mode TE variation is displayed on the TIE graph. When set to *Off*, no TE normalization is applied i.e., the TE graph displays absolute delays (including propagation delay, time offset between Master and Sentinel, and other time inaccuracies in the system).

Channel *X* (PTP / NTP)

The channel used for the PTP or NTP connection is selected by the **Mode** screen, as mentioned earlier, and a **Channel *X*** tab will be present for each PTP or NTP connection chosen.

Some of the menus such as PTP or NTP and Selection appear only when the **PDV Option** is enabled. This tab allows the user to change parameters related to Sync and PTP or NTP.

Ethernet

Note: These settings are applied only for PDV measurements in **Pseudo-slave/Pseudo-Client** mode. When **Monitor mode** is enabled these settings are not applied and a **Monitored Channels** tab will be available.

Auto-Negotiation   This allows auto-negotiation to be *Enabled* or *Disabled*

When *Enabled*, Sentinel auto-negotiates the line rate with the other device

When *Disabled*, the user must select the media type from the Ethernet Media drop down menu

Ethernet Media   Select media type for when Auto-negotiation is *Disabled*. Choose from *100BASE-T*, *1000BASE-T*, *100BASE-FX* and *1000BASE-FX 10G*

VLAN 802.1Q   Turn *On* /*Off* VLAN Ethernet packets tagging according to 802.1Q specification

VLAN ID   VLAN identifier

VLAN Priority   VLAN priority setting, range 0 to 7

DHCP   Turn on/off using DHCP server for automatic IP allocation

IP Address   IP-address to assign for module if DHCP is *Off*, the address entered should be in IPv4 or IPv6 format depending on the option chosen for PTP/NTP. Sentinel NTP client on units with serial numbers below 400000 only supports IPv4 unicast mode. Selecting IPv6 will result in no measurement data being recorded.

Mask   Network mask, IPv4 or IPv6 format

Gateway   IP-address of the gateway in the network; IPv4 or IPv6 format

The **Ping** button allows the user to ping the gateway address currently specified

MAC Address   Read-only. Displays MAC Address of corresponding Packet module.

Wander Generator

This page contains parameters related to Wander Generation for Synchronous Ethernet.

Note: These parameters are applied only when Packet module is configured as SyncE Master (see **SyncE** page for further details). When the Packet module is acting as *Master* and Wander Generation is *Enabled*, Sentinel will generate sine wander according to parameters specified on this page. Wander Generation is not supported by 10G modules.

SyncE

This window contains parameters related to the Packet module in Synchronous Ethernet.

Mode	Packet module can function in two modes – *Master* or *Slave*. In *Master* mode the Packet module is SyncE master in the connected network segment. It is source of synchronization clock signal and it can send ESMC messages over the network in accordance to specified scenario. In *Slave* mode the Packet module can measure TIE of extracted synchronization signal and it can receive ESMC messages
ESMC Generation	This parameter enables or disables ESMC messages generation scenario. Works only in *Master* mode
ESMC Transition	This parameter enables or disables periodic ESMC transition
Initial SSM	Specifies initial SSM in scenario
Alternate SSM	Specifies alternate SSM in scenario
Transition Start	Time from starting measurement when first transition occurs
Transition Period	Period between two adjacent ESMC transitions

PTP

This page will only be available if the **PDV Option** is enabled on the Sentinel. This window contains all parameters related to PTP stack behaviour in pseudo-slave mode.
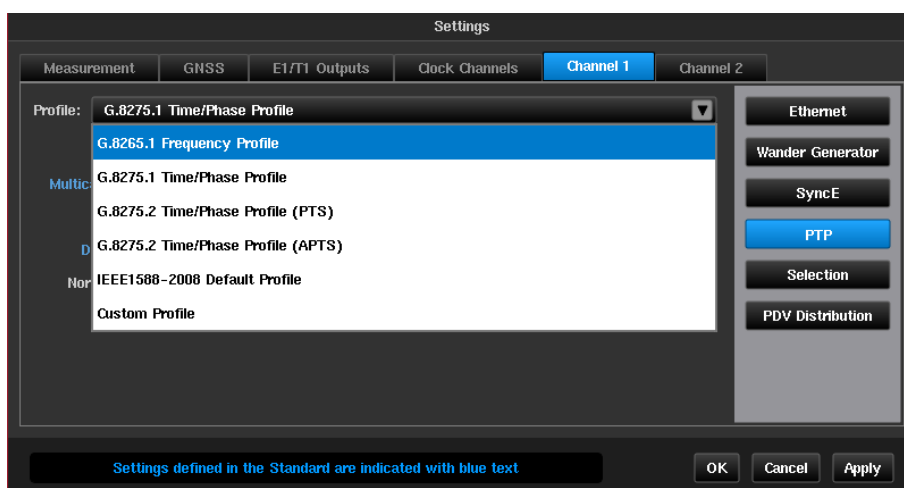

The PTP transport protocol and relevant settings can be pre-set to values according to the ITU-T standard related to the test being performed via the **Profile** selection.

Available profiles are:

- *G.8265.1 Frequency Profile*
- *G.8275.1 Time/Phase Profile*
- *G.8275.2 Time/Phase Profile (PTS)*
- *G.8275.2 Time/Phase Profile (APTS)*
- *IEEE1588-2008 Default Profile*

When a standard profile is chosen, only relevant fields are displayed and are populated with values from the ITU-T profile or the IEEE1588-2008 standard. Fields that are defined for this profile are highlighted in blue text. Clicking on a particular entry will detail what the IEEE1588 valid range is and what the range specified by the ITU-T profile is e.g. for ITU-T G.8275.1 testing the PTP Domain field has a specified range of 24 to 43, while the IEEE1588 valid range is 0 to 255.
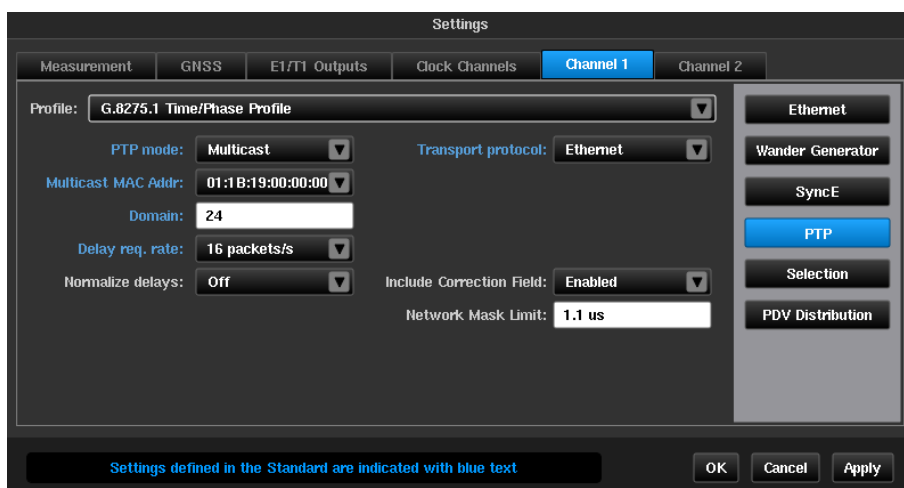
Any profile can be changed to any value, however, changing values in a standard profile that is outside the range for the profile will cause the profile to change to *Custom Profile*.

PTP mode	PTP protocol mode: *Unicast* or *Multicast*. This setting should be set accordingly to the PTP master configuration.
Transport protocol	Protocol level for PTP measurement: *UDP/IPv4*, *UDP/IPv6* or *Ethernet*
Multicast MAC Addr	Select Multicast MAC Address – forwardable or non-forwardable; applies in *Ethernet* mode only
TTL	IP header Time To Live value when *UDP/IPv4 Multicast* is selected
Hop Limit	IP header Hop Limit value when *UDP/IPv6 Multicast* is selected

IPv6 Multicast Scope	Applies in *UDP/IPv6 Multicast* mode only. Values are: *Interface – Local, Link – local, Realm – local, Admin – local, Site – local, Organisation – local* or *Global*.
DSCP	IP header DSCP setting, range 0 to 63; default 46
Unicast Neg	Determines whether negotiation is enabled or disabled in Unicast mode
Master address	IP address of PTP master. The **Ping** button allows user to ping the master address
Domain	PTP domain which PTP Master is configured to work in.
Announce rate	Number of Announce messages to be sent per second
Sync rate	Requested number of Sync messages to be sent per second (by the PTP Master)
Delay req. rate	Number of Delay Request messages to be sent per second
Contract duration	Requested PTP contract duration
Include correction field	Allows the correction field to be included in the PDV measurement; default enabled
Normalize delays	When *On* - PDV samples are normalized relative to first delay sample so that first PDV sample has zero value. In this mode delay variations are displayed on PDV graphs.
	When *Off* - no PDV normalization is done, so PDV graphs display absolute delays (including propagation delay, time offset between Master and Sentinel, and other time inaccuracies in the system). PTP 2 Way TE will be calculated when **Normalize delays** is *Off*
Network Mask Limit	User defined 2way Time Error mask value

When in Pseudo-slave mode, the Packet module acts as a PTP slave, however the internal 1 PPS is kept constant for the measurement and is not adjusted according to the PTP master. This allows measurement of PDV on Master to Pseudo-slave network path.

NTP

This page will only be available if the **PDV Option** is enabled on the Sentinel and **NTP Client** has been selected in the Mode page. This window contains all parameters related to NTP stack behaviour in pseudo-client mode.

NTP mode	Unicast
Transport protocol	Protocol level for NTP measurement: *UDP/IPv4, UDP/IPv6*.
	Note: On Sentinels with serial numbers below 400000 NTP client only supports UDP/IPv4. Selecting UDP/IPv6 will result in no measurement data being recorded.
Server address	IP address of NTP server. The **Ping** button allows user to ping the server address

Poll	Poll rate selection. The poll rate can be configured as 1 packet every 2^n seconds, where n=0 to 17. This gives a max poll rate of 1 packet per second and a minimum poll rate of 1 packet every 36.4 hours.
Version	NTP version. Sentinel supports versions 1 through 4.
Normalize delays	When *On* PDV samples are normalized relative to first delay sample so that first PDV sample has zero value. In this mode delay variations are displayed on PDV graphs.
	When *Off* – no PDV normalization is done, so PDV graphs display absolute delays (including propagation delay, time offset between Server and Sentinel, and other time inaccuracies in the system). NTP 2 Way TE will be calculated when **Normalize delays** is *Off*
Network Mask Limit	User defined 2way Time Error mask value

Selection
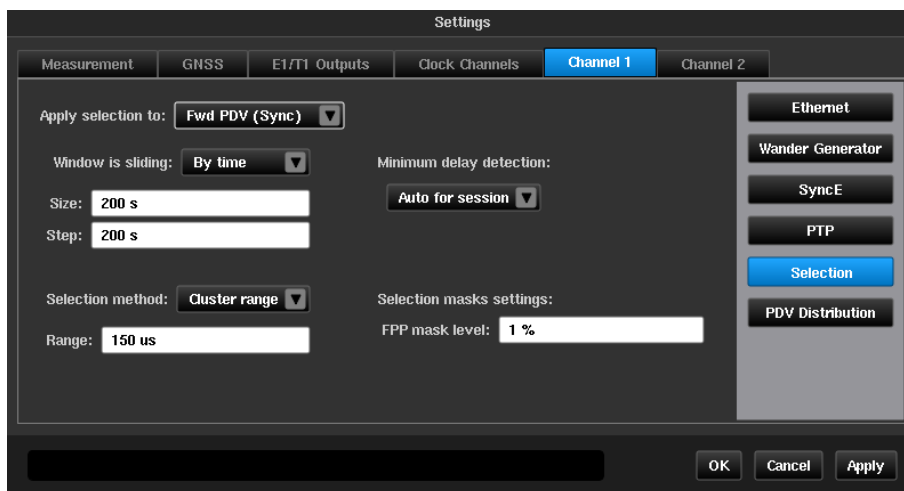
This window will appear only when the **PDV Option** is enabled. For each installed Packet module, a selection algorithm can be applied to only one type of packet delays (FWD/REV/PD - Forward, Reverse or Path Delay) or to none.

Selection algorithm contains three components which can be set up independently.

By default, the settings are for ITU-T G.8261.1 FPP testing.

Window parameters

The user can choose one type of window: **window sliding by** samples or window sliding by time.

When the **Window is sliding** by samples, it always consists of a constant number of samples but time interval between first and last sample in the window is varying. Window size and step are defined in terms of samples number.

When the **Window is sliding** by time, it contains set of samples in which time difference between last and first samples is not greater than given window size; Window step is also given in terms of time.

Window step to window size ratio determine overlapping rate. Normally, window step should not be greater than window size.
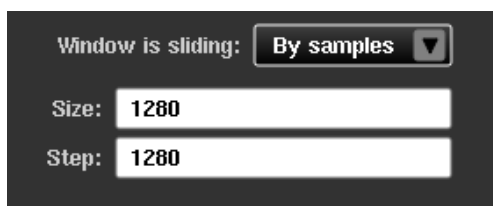
Selection method

Selection is a procedure of picking packets from a window which conforms to a given constraint. The user can select one of two possible selection types which determine constraints being used: *Band* selection and *Cluster range*.

Band selection is a selection of packets which are inside a range (defined by percentiles) of window packets sorted out by delay value. For example, range 0%-25% means selection of quarter of fastest packets (with lowest delay values).

Selection method:	Band ▼
a:	0 %
b:	50 %

Cluster range selection method is a selection of packets which are inside a range of current minimum delay parameter to current minimum delay + given range. Range value is given by user and is constant during the measurement. Current minimum delay is determined depending of settings of **Minimum delay detection** component.

Selection method:	Cluster range ▼
Range:	150 us

Minimum delay detection

Minimum delay detection:	
Custom ▼	0 s

Minimum delay detection parameter affects lower edge of cluster range interval and can be one of the following:

Custom	Constant minimum delay entered by user is used
Auto for last	Minimum delay is automatically determined by packet delays received for last given amount of time
Auto for session	Minimum delay is automatically determined as lowest delay packet ever received during measurement

Selection masks settings

User can enter FPP mask level. FPP mask for a particular Packet module is considered failed if at least one of FPP sample is below mask level. Otherwise it is considered a pass.

PDV Distribution

Different PTP slave vendors have their own specification for PDV distributions for their PTP slave to work correctly. This PDV distribution function allows the user to set a vendor specific specification so that Sentinel can be used to compare the measurement results against vendor specification for pass/fail test.

Settings						
Measurement	GNSS	E1/T1 Outputs	Clock Channels	**Channel 1**	Channel 2	

Mask Type:	Range ▼		Ethernet
Min:	0 s		Wander Generator
Max:	0 s		SyncE
Nominal:	0 s	Please note! Normalization by minimum delay is applied after PDV normalization if enabled in the 'PTP' settings page or the 'Monitor Mode' page.	PTP
Below:	30 %		Selection
Above:	30 %		**PDV Distribution**
Pass Criteria:	90 %		
Normalize by min delay:	On ▼		

OK Cancel Apply

Mask Type	Different ways to define the mask, either by range or by tolerance. When *Range* is selected, it is possible to set the required mask by min/max delay values. When *Tolerance* is selected, the mask can be set around a nominal value

Min	The minimum delay of the requested range
Max	The maximum delay of the requested range
Nominal	The requested nominal delay
Below	The percentage below the nominal delay
Above	The percentage above the nominal delay
Pass Criteria	The percentage of packets which fall in the defined delay range

Normalize by min delay

| *ON* | The delay measurement references to the luckiest packet (packet with the minimum delay) |
| *OFF* | The delay measurement references to the first packet |

Monitor Mode

Monitor Mode is selected via the **Mode** page as earlier described. When this is mode is selected a new tab, **Monitored Channels**, will be available in the **Settings** pages.

All parameters on this page correspond to PDV measurement performed in **Monitor Mode**.

Note: An external network Test Access Point (TAP) or optical splitter is needed to be able to measure PDV in Monitor Mode.

When operating in **Monitor Mode**, Sentinel "sniffs" for PTP or NTP packets between two nodes. By monitoring the traffic between the two nodes available via the TAP, Sentinel can measure PDV between channels.

Settings				
Measurement	GNSS	E1/T1 Outputs	Clock Channels	**Monitored Channels**

Protocol Level: UDP/IPv4   Include Correction Field: Enabled   **Monitor Mode**

Normalize delays: On   **Selection**

Network Mask Limit: 1.1 us   **PDV Distribution**

Discover...

VLAN (802.1Q): Off   VLAN ID: 2   **Channel 1 / Ethernet**

Monitored Domain: 0   Monitored Mode: Multicast

Monitored Master IP: 10.32.1.163   ...

Monitored Slave IP: 10.32.1.168   **Channel 2 / Ethernet**

OK   Cancel   Apply

Protocol Level	Protocol level for PTP measurement: *UDP/IPv4*, *UDP/IPv6* or *Ethernet*;
Normalize delays	When *On* PDV samples are relative to first delay sample so that first PDV sample has zero value;
	When *Off* true Fwd/Rev/PD delays are shown;
Include correction field	Allows the correction field to be included in the PDV measurement; default enabled
Network Mask Limit	Value of TE mask
Discover...	Allows auto-fill of setting fields below based on network traffic analysis and auto-detection of all possible nodes which could be used for measuring PDV in monitor mode. See detailed description below.
VLAN (802.1Q)	Specifies if VLAN packets are captured;
VLAN ID	Specifies VLAN identifier when VLAN packets capturing is enabled. See **VLAN (802.1Q)** setting
Monitored domain	PTP domain which is monitored; This setting is not available for NTP protocol.
Monitored mode	Specifies which type of traffic is monitored: *Unicast* or *Multicast*. This setting is not available for NTP protocol.
Monitored Master IP / **Monitored Slave IP**	IP addresses of two PTP or NTP nodes which are monitored. This setting is not available for *Ethernet* protocol level.
Monitored Master MAC / **Monitored Slave MAC**	MAC addresses of two PTP nodes which are monitored. This setting is not available for NTP protocol or *UDP/IP* protocol level.

Discovery

The Discovery feature simplifies network node parameter filling by giving the user the option to select desired node pairs from a list. After pressing the **Discover...** button, network traffic analysis is performed and the list of possible nodes for PDV measuring is displayed.
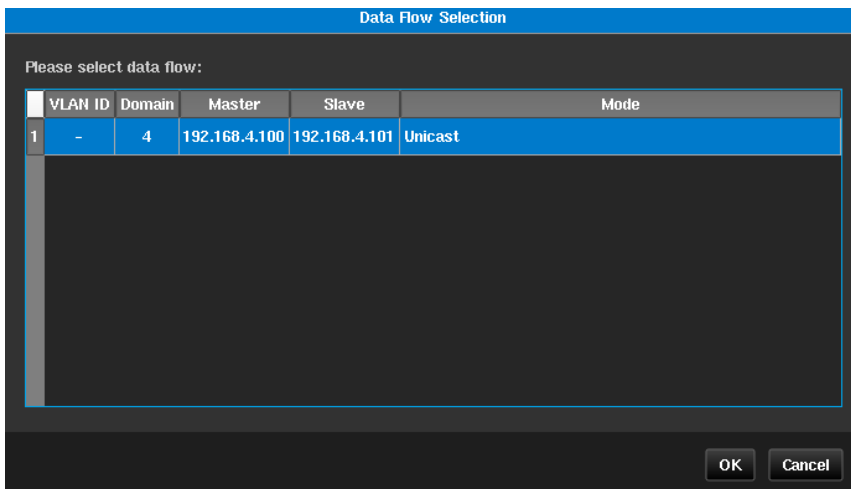
After the user selects a row in the table and presses **OK** button, the corresponding fields in the monitor mode configuration page are automatically filled.

When using **Monitor Mode**, the channel widget is combined for the two PTP channels as shown below:
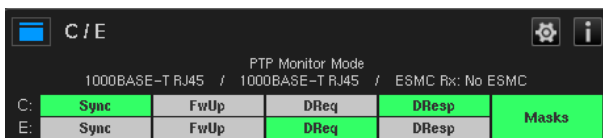
4.4 Masks

Sentinel provides various predefined masks to be applied to TE, TIE, MTIE and TDEV graphs - six can be selected and displayed on main screen at the same time. The **Masks** screen is used to select which masks are displayed on the main screen and can be overlaid on the measurement curves.

On the left all the available masks within Sentinel are listed.

On the right the masks to be displayed on the measurement page are listed.

The **Add** button is used to add the mask currently selected in the **Available masks** list to the Selected masks list. The **Remove** button is used to remove the mask selected in the Selected masks list, from the masks to be displayed.

For a full list of available masks see Appendix C
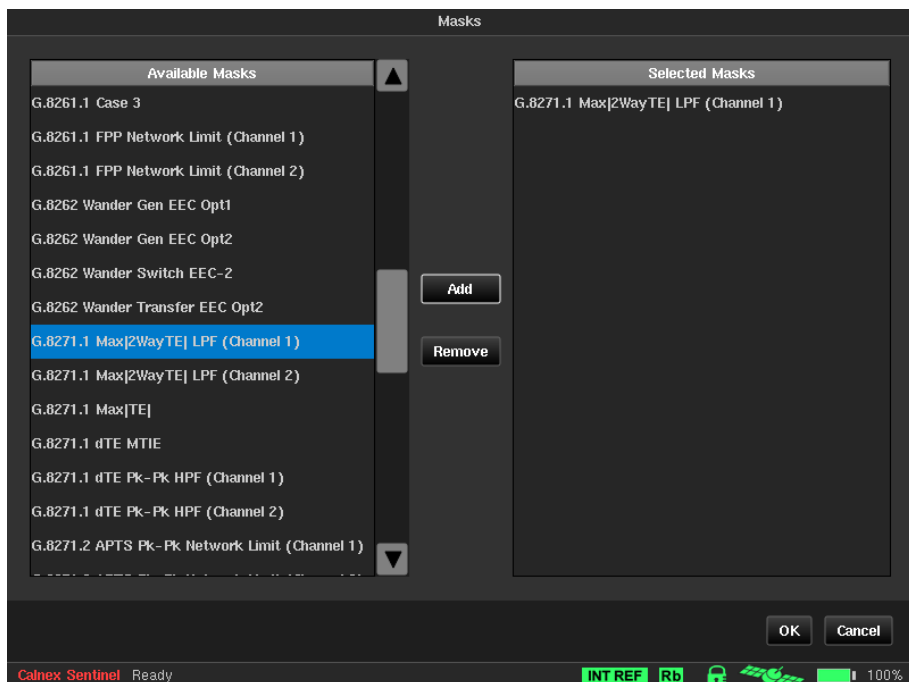
4.5 Health Check

The Health Check screen contains three utilities to automatically setup measurement inputs and to debug the setup of PTP measurements.
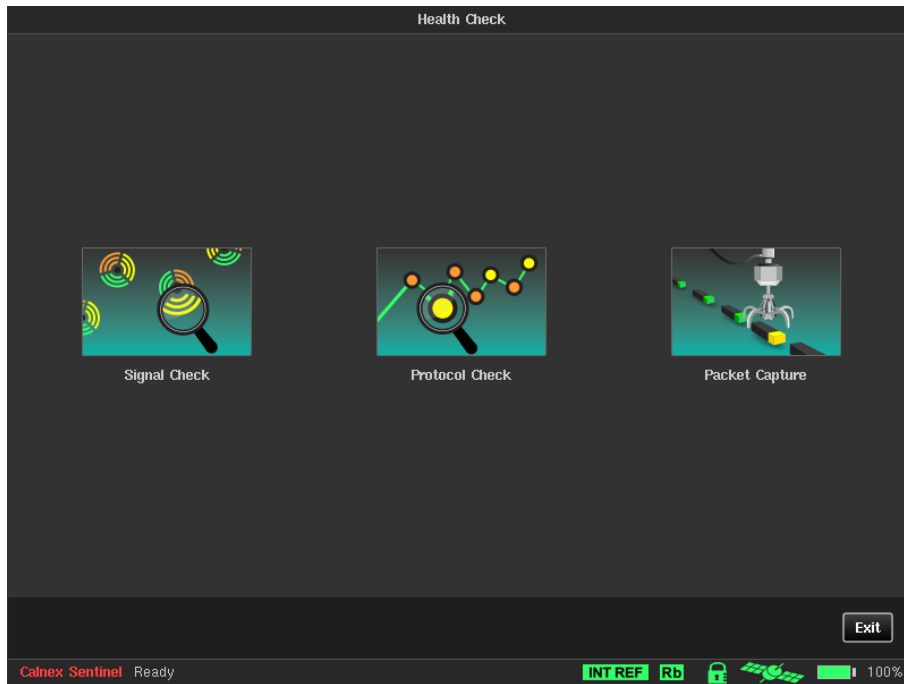
Signal Check

Running **Signal Check** will detect all clocks that are connected to Sentinel and set up the measurement subsystem. If a signal check is not performed then TIE measurements may display erroneous data.
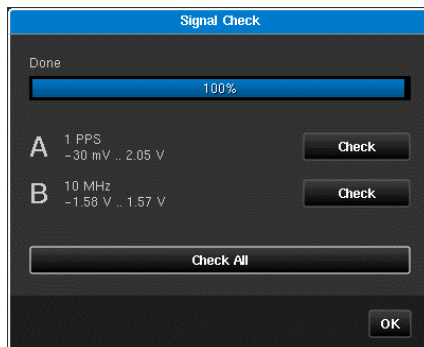
Protocol Check

The **Protocol Check** is used to check that the PTP protocol is working as expected for the PTP profile being used by identifying and highlight any issues. When running a PTP measurement the validity of Sentinel and GM settings can be checked using the protocol check procedure.

When selecting the **Protocol Check** button, the protocol check window will open and Sentinel will start to look for PTP messages based on the PTP or Monitor Mode Settings.

Fields are populated as they are discovered by protocol check. The message rates are checked against their advertised values.
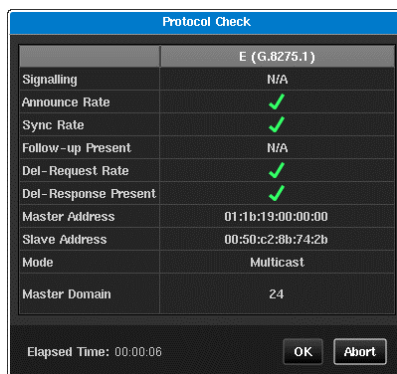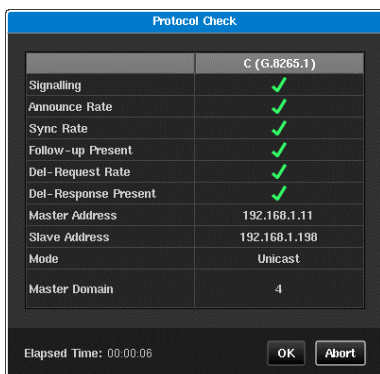
Fields that are not relevant to the operating mode are marked as N/A e.g. **Signalling** in Multicast mode or **Follow-up** messages in 1-step mode.

Master Address and Slave Address will be populated with the GM and T-TSC MAC addresses in *Ethernet* mode or IP addresses in *IPv4 / IPv6* mode. Mode will be either *Multicast* or *Unicast* and the Master Domain will show the value used by the GM. If the Master Domain differs from the value configured by Sentinel then it will be highlighted in red text.

A clock displays the time since protocol check was started.

If a message type is present and passes its rate check then a **√** will be displayed. If the message type is not present or the message rate is incorrect a **X** will be displayed and the message rate if appropriate.

The protocol check will complete automatically if all PTP channels have successfully been analysed. If this does not occur, then the check can be terminated by pressing the abort button.

Packet Capture

This option captures the Ethernet flow on each PTP card to allow analysis of the packets to validate the exchange of PTP traffic between the GMC and Sentinel.

Packet Capture is accessed by pressing the **Packet Capture** button on the **Health Check** screen.
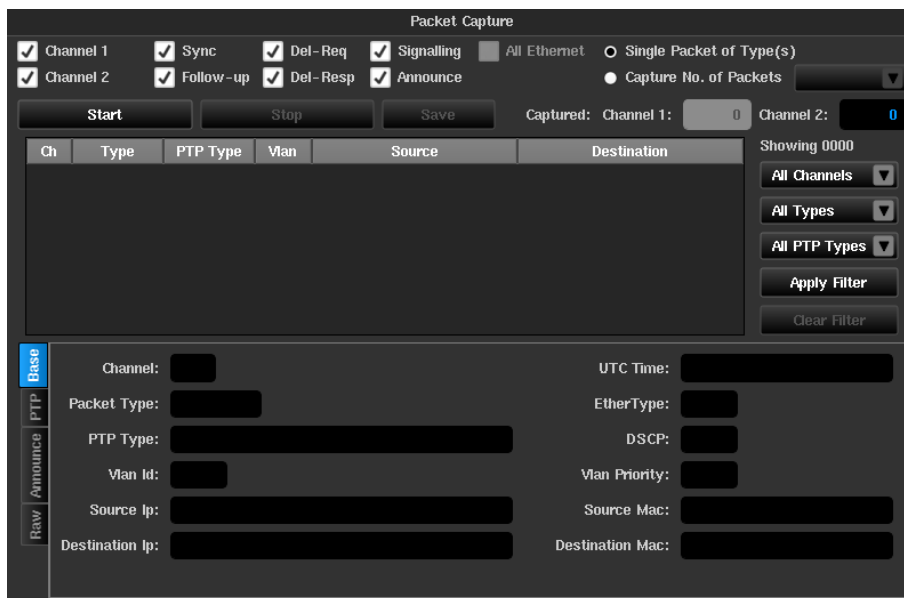
The following check boxes configure which PTP ports will be used and which types of Ethernet packets will be captured:

Capture Slot **x** (x = 1, 2, C or E)	Selects which PTP ports will be used to capture packets
Sync, **Follow-up**, **Del-Req**, **Del-Resp**, **Signalling** and **Announce**	Selects which type of PTP messages are captured
All Ethernet	Captures all Ethernet packets

Capture can be configured to capture a single packet of each PTP message type, selected by the check boxes, or to capture a specific number of packets.

The packet capture can be run by pressing the **Start** button. The number of packets captured on each PTP card is displayed.

If **Single Packet of Type(s)** is selected the capture will end when a single packet of each of the types selected has been captured. If **Capture Number of Packets** is selected the capture will end when the specified number of packets of the specified types has been captured for each channel selected.

In either case the capture can be stopped by pressing the **Stop** button.

The previous example shows packet capture configured to capture one Sync, Delay Request, Delay Response and Announce message using the PTP card in slot 1. 4 packets are indicated as being captured on Channel 1 and Channel 2 is disabled so no packets have been captured.

Results can be filtered using the **Channel**, **Type** and **PTP Type** dropdown boxes to the right of the results window.

Channel	_1, 2, C_ or _E_ selects which PTP card is the source of the capture
Type	_PTP-UDP, PTP-ETH, ETH, IPv4, IPv6 or UDP_ selects the type of packet to be displayed
PTP Type	_Sync, Delay_Req, Delay_Resp, Follow_Up, Announce, Signalling, Management, Pdelay_Req_ or _Pdelay_Resp_ selects the type of PTP message to be displayed

Results are filtered by pressing the **Apply Filter** button. Filtering of results can be removed by pressing the **Clear Filter** button. There are also options to select all types or all channels for each of the filters.

Filtering can be a combination of one or more of the dropdown boxes e.g., the following example shows filtering for Delay Request messages from slot 1.
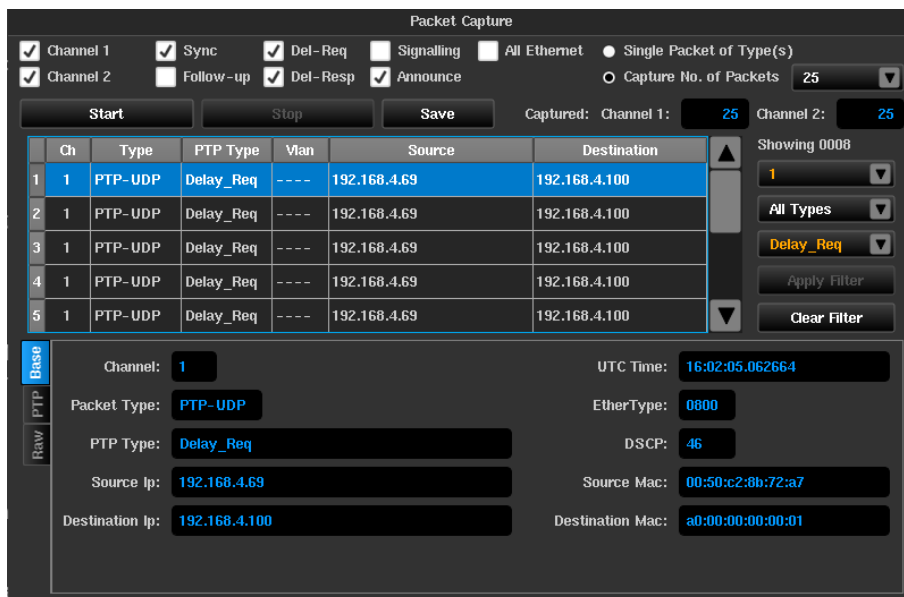
The bottom portion of the packet capture screen shows context sensitive decode of the packet highlighted in the results window.

Various levels of decode will take place depending on the types of pacture captured. There will be up to four tabs displayed for each message selected and these will be as follows.
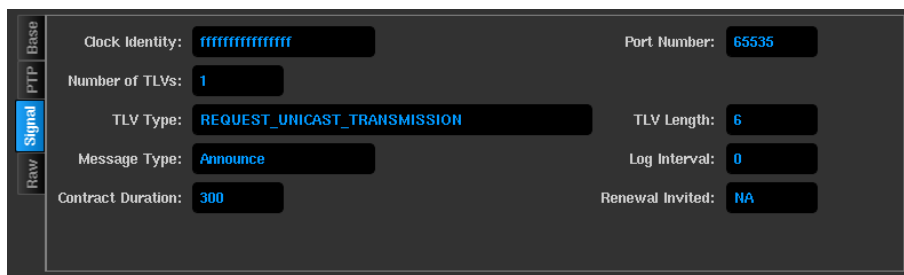
Base – Decode of packet transport header fields (MAC, VLAN, IP). All packets will have this tab.
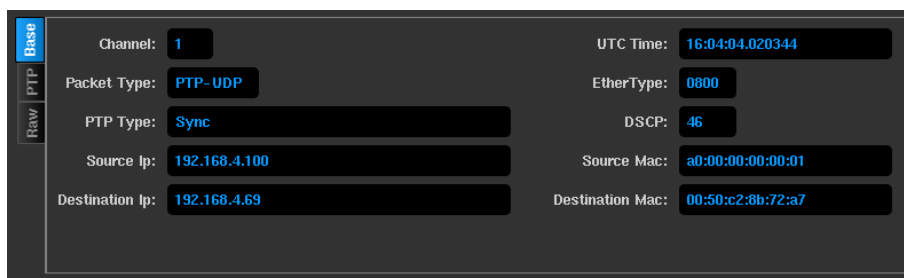
PTP – Decode of significant PTP header fields. Only packet types PTP-UDP and PTP-ETH packets will have this tab.

Signal / Announce – Decode of the fields contained within a PTP Signalling or Announce message Only PTP-UDP and PTP-ETH Signalling / Announce packets will have this tab.

Raw – Hexadecimal and Ascii display of the captured packet. All packets will have this tab

Captured packets can be saved using the save button on the Packet Capture screen. The saved files will be in **PCAP** format. The captured packets are saved together in a single .pcapng file and as separate .pcap files for each PTP channel to the name and location specified during the save operation. These file can be transferred from the Sentinel and analysed further using Calnex PTP Field Verifier (PFV) or other tools e.g. WireShark

4.6 Data

The Data screen allows the user to reload previous measurements or to Export the data in a CSV format.
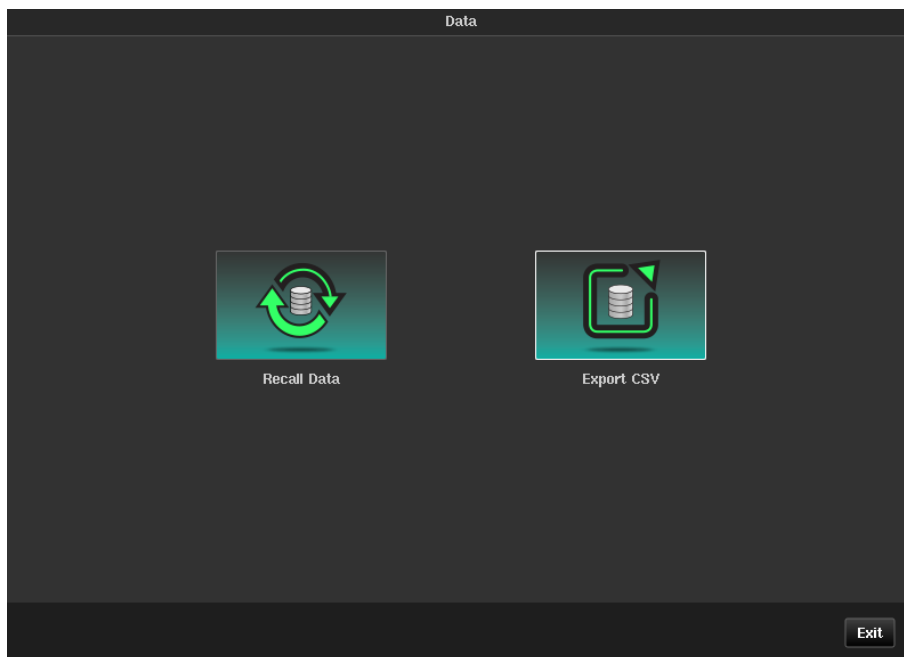
NOTE: Sentinel measurement files can be directly read into the Calnex Analysis Tool for in depth analysis and report generation. If the files are in Sentinel internal storage, then they can be copied either using an ftp client or by copying to a USB stick. See File Management section.

4.7 System

The System screen gives access to a number of other screens as shown below:
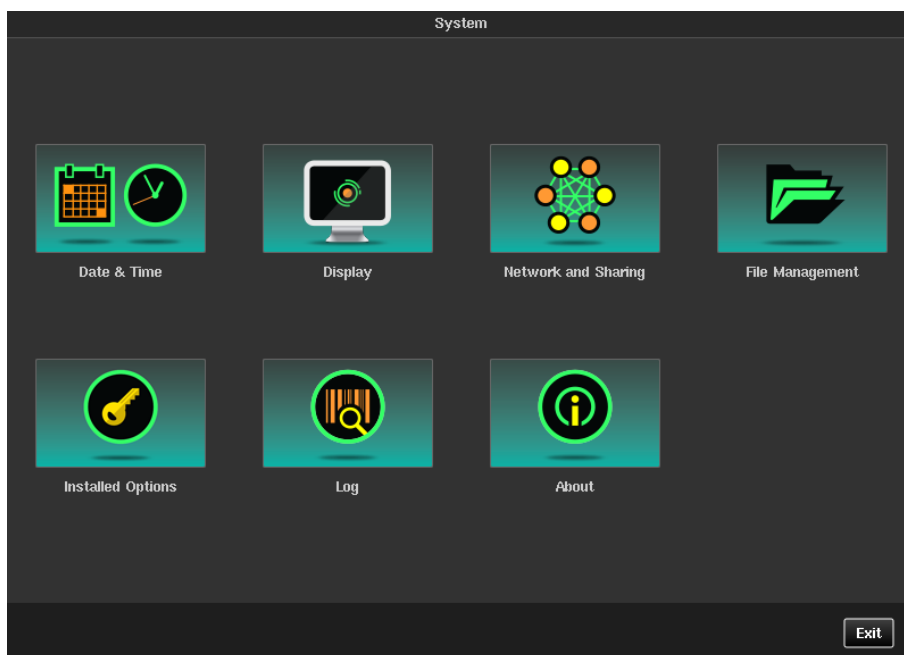
Date & Time
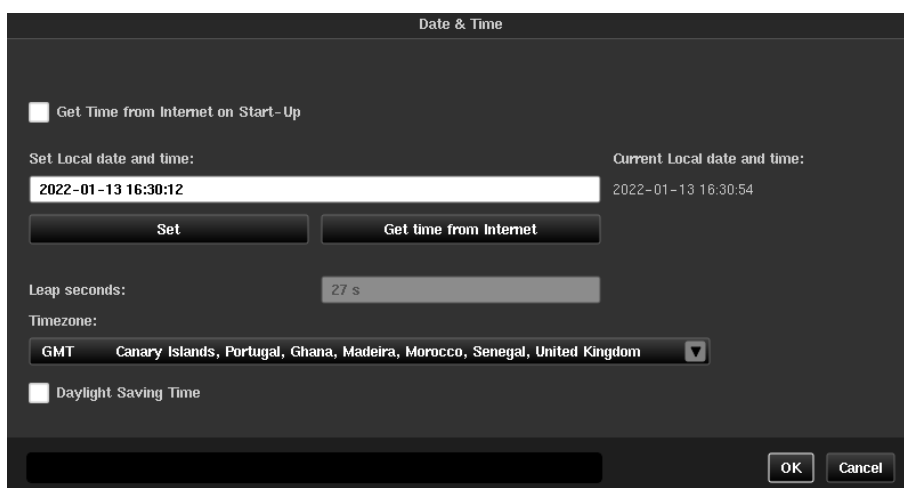
The date and the time can be entered manually using the **Set** button or can be synchronized with universal time by pressing the **Get time from Internet** button if an external network connection is available. If GNSS is connected to Sentinel the date and time will automatically be synchronized to this, overriding date and time set by other methods.

If checked, **Get Time from Internet on Start-up** option allows to automatically synchronize date and time from the internet before the GNSS receiver starts up.

Checking the **Daylight Saving Time** box adjusts system time for daylight saving.

Display
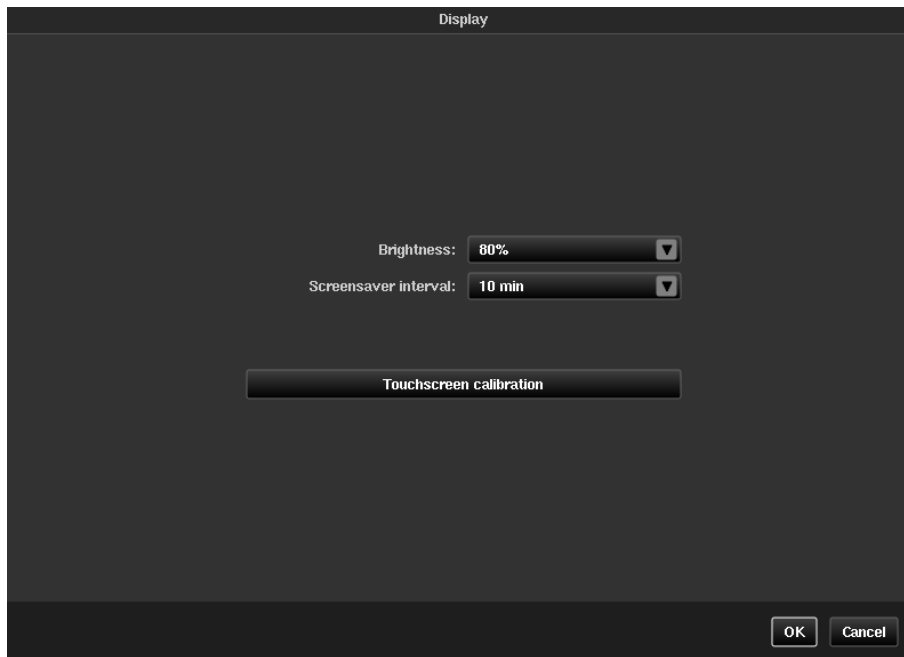
There are the following options on the Display page:

Brightness   Allows to choose LCD backlight intensity with 20% step

Screensaver interval   Defines time interval after which LCD backlight is switched off

Touchscreen calibration is an automated operation performed by a special utility that asks the user to touch several highlighted points in the screen. Instrument reboot is required to finalise the calibration procedure, so pressing the **Touchscreen calibration** button displays the following warning:
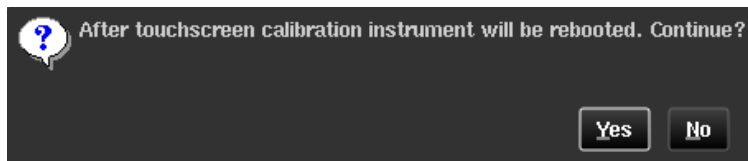
Network and Sharing

Ethernet

The displayed screen is used to define parameters of the Ethernet management connection. IP address, subnet mask and default gateway can be entered manually or set automatically using DHCP. If DHCP is used the IP address allocated will be displayed in the IP address field. MAC address field is read only and just for information.

It is possible to configure an IPv4 connection and IPv6 connection at the same time if required. The configuration for both options can be either Disabled, DHCP or Manual and do not need to be set to the same mode.
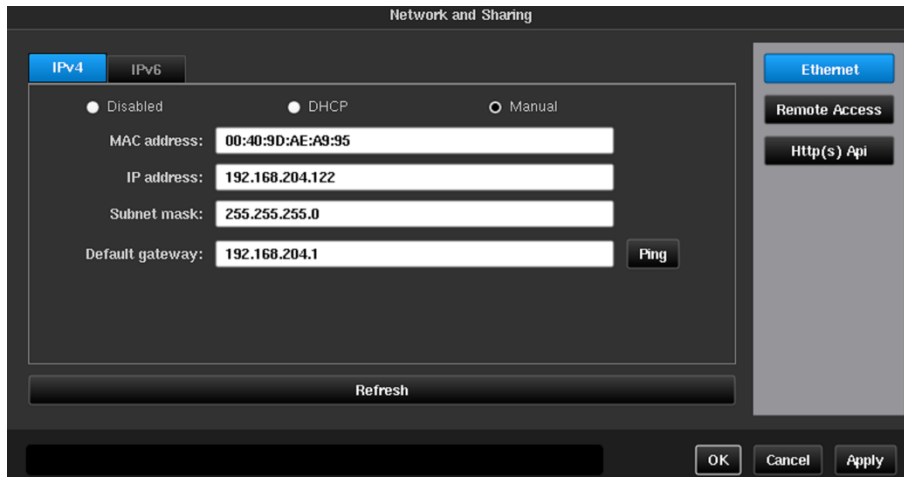
Remote Access
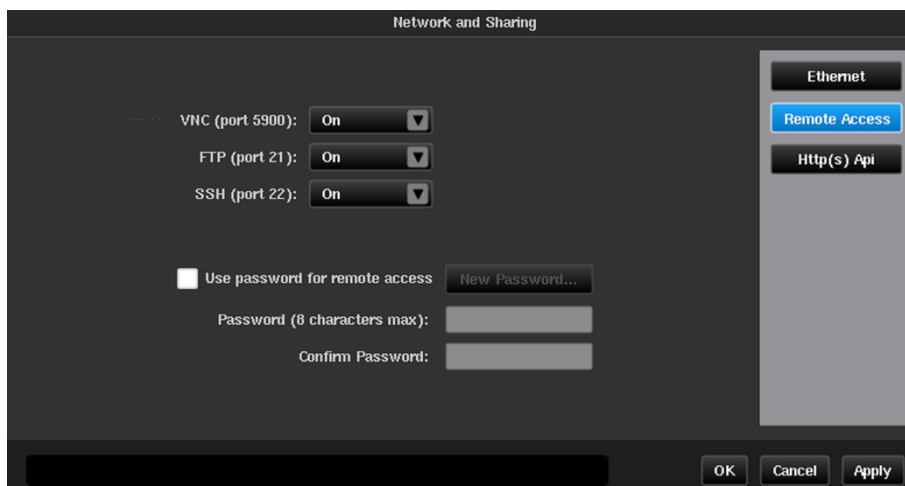
Sentinel provides several ways of remote access via Ethernet:

VNC Virtual Network Computing, allows user to see screen of Sentinel on remote computer using client software

FTP File Transfer Protocol, allows access to Sentinel internal and external memory from FTP client software

Service access Used by Calnex customer support to access instruments if required

By default, no password is required for **VNC** and **FTP** connections. To enable password protection set **Use password for remote access** flag and type a password in corresponding fields. To change password, press **New Password...** button. The user name for FTP connection is fixed – *remote*.

Note: Remote access settings changes are applied only after instrument reboot.

HTTP(S) API

Sentinel has an HTTP based API that can be used to perform remote control of the Sentinel unit. This interface is configured via the options available on this page.

|	
Enable HTTP API Interface	This allows access to the API interface via the HTTP protocol. Where security is a conce[rn] for having open access to the Sentinel API it is recommended to disable this access me[thod] and turn on authentication for the API. To disable access to the Sentinel API fully then [both] HTTP and HTTPS should be disabled.
Enable HTTPS API Interface	Where security is a concern for access to the Sentinel API then it is recommended to us[e] HTTPS and disable the HTTP interface. To disable access to the Sentinel API fully then [both] HTTP and HTTPS should be disabled.
Key Seed	This is the seed value that is used as part of the authentication handshake when authentication is enabled.
Authentication Enabled	This enables authentication on the API interface.
Clear logins when seed changes	When set, changing the value of the Key Seed will cause all sessions currently logged i[n to] the API interface to be logged out.
Cached login timeout	This is the time that a login to the API interface will last before a new login would be required. All logins are cleared when the Sentinel is rebooted.

File Management

The File Management screen is used to manage the measurement files. A drop-down list provides information on available space on the internal memory of the instrument, or on the external USB memory stick if connected. The files can also be moved via the Ethernet network when they have been saved internally.
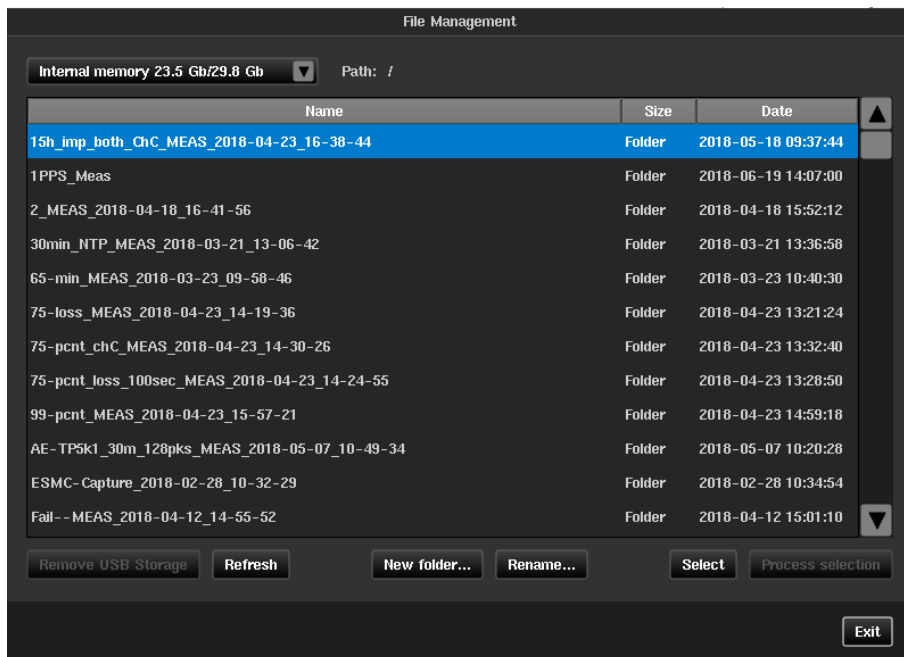
If you want to remove an external USB memory storage device, press **Remove USB Storage** button before unplugging to ensure that data has been saved properly. If the display is not updated after plugging / unplugging USB memory press the **Refresh** button to force display update.

Note: To aid remote control of the Sentinel the **Remove USB Storage** button changes to **Remount USB Storage** button when the external USB memory storage device has been dismounted. The device can be remounted by pressing this button which then returns to **Remove USB Storage**.

Various buttons are available at the bottom of the File dialog. The **New folder...** button is used to create a new folder. The folder name is entered using the virtual keyboard. The **Rename...** button is used to rename a file or folder, in the same way. The **Select**/**Unselect** button is a toggle used to select/unselect files and folders in the list for further processing using **Process selection** button; the selected items are identified by highlighting and switching to italic characters.

Note: Files and/or folders remain selected even when user chooses a folder different from which selected items belong to. This allows processing of files and/or folders from several different locations in memory.

The **Process selection** button is enabled when at least one file or folder is selected and will indicate the number of files currently selected. A window is opened with the available operations, applicable to the internal memory and to any external memory: **Move here**, **Copy here**, **Remove**, **Unselect all**, **Cancel**.
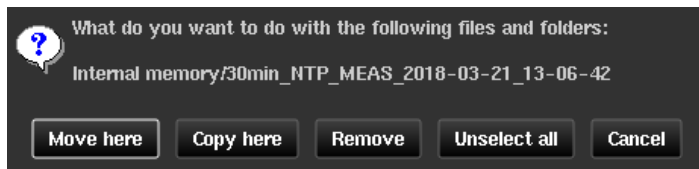
Installed Options

This screen shows the list of licensed options that are installed on Sentinel. If one or more Packet Modules are installed, then the **PDV** option will display. If a 10GbE Packet module is installed, then an entry will appear for each licensed port and the relevant interface speeds available for that port.

Packet module options can be upgraded in the field through a file supplied by Calnex. This file should be copied to either Sentinel internal or external memory and selected through the **Load Options File** button. Once the file has been loaded, Sentinel will reboot, and the new options will be enabled.

Log

Sentinel keeps a log of different events (start up, power down, timebase warming, measurement start, loss of signal etc.) that can be seen in the **Log** page. The Log can be exported to a CSV spreadsheet that can be read by many spreadsheet editors and text viewers. An explanation of the events in the log can be found in **Appendix D**.

About

The **About** screen identifies the firmware installed in the instrument and enabled Sentinel options.
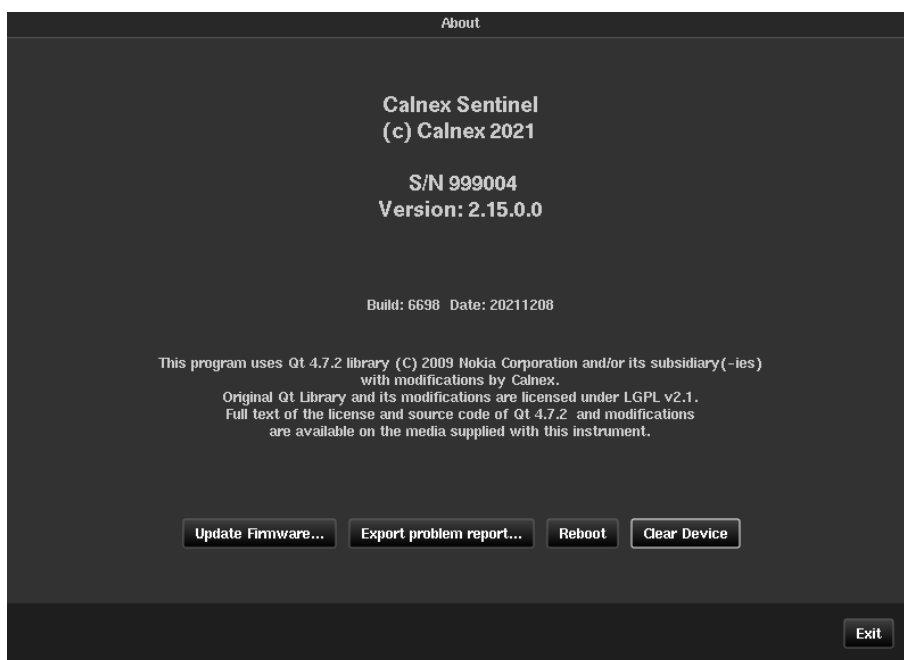
Update firmware...	Used for updating Sentinel unit from a firmware image located in internal or external memory (USB flash). The instrument is rebooted to finalise the firmware update
Export problem report...	Allows the user to save internal system logs to a specified place in internal or external memory of Sentinel. In the instance of a problem this information can be sent to Calnex customer support to help in investigation
Reboot	Allows the Sentinel to be rebooted without removing power
Clear Device	Deletes all measurement and configuration data from the device. When selected, a warning message will appear to confirm this action will be taken

Operation

5.1 Measurements

The measurements are made by pressing the **Start/Stop** (toggle) button.

By default, the measurement starts immediately, but a warm-up time may elapse first. Measurement start can be programmed to a timer set up by the user via **Settings**.

Note: If an OTA module is fitted and is enabled in the Mode page, the measurement will not start until the OTA card has locked to the selected frequency. If the OTA card is not being used it should be disabled in the Mode page.

While a measurement is in progress, pressing the **Stop** key stops the measurement immediately. The measurement will still be saved for the completed duration before **Stop** was pressed.

A measurement with a defined measuring time stops automatically after the set time has elapsed.

The default characteristics are:

- Sample time: *33ms*
- Duration: *10min*
- Reference: *Auto* selection between internal oscillator and external reference

These characteristics can be modified and saved in the **Settings** screen as previously described.

By default, the user will be prompted to select where to save the measurement.

Throughout the duration of the measurement, the TIE and/or Raw PDV are displayed, with plot scale adjustment as the time elapses. The calculated functions (MTIE and TDEV together with PDV Distributions, Selected PDV metrics: FPP, MAFE, and 2Way TE) and PTP Statistics can also be displayed during measurement acquisition.

The remaining measurement time is displayed on the status line at the bottom of the screen.
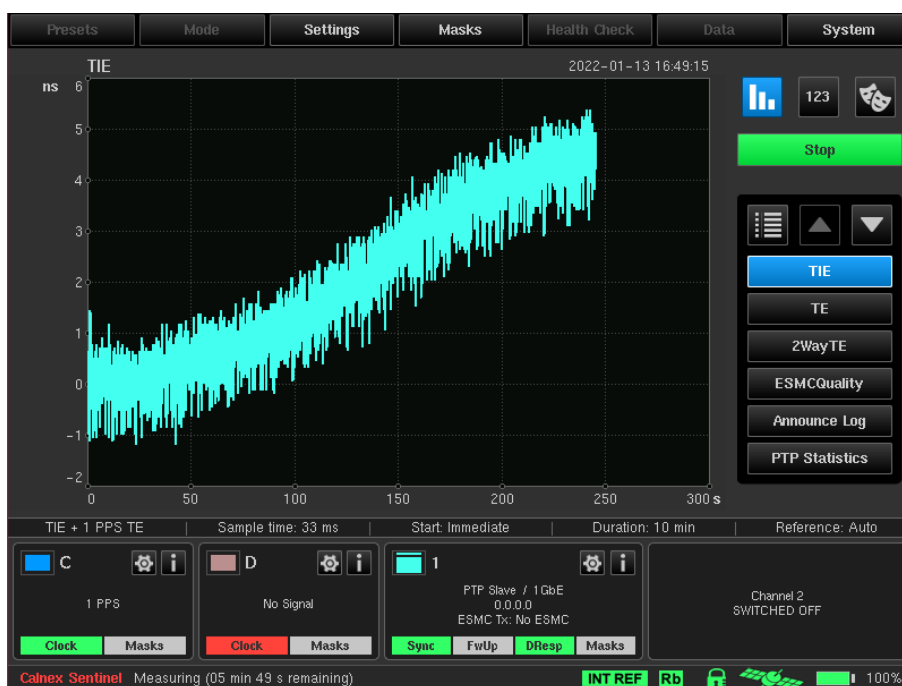
5.2 Saving Measurement Data

Measured TIE data, Raw PDV data (measured Fwd, Rev and Path Delay) and 2Way TE calculated data can be saved in the instrument or on an externally connected USB memory stick. All calculated metrics will not be saved. Measurement data will be stored in binary format. For each measurement, a separate folder will be created with the default name in a form **MEAS_date_time** where **date_time** corresponds to the time at the start of measurement. The folder will contain a file named **measurement.sta** which is used to record measurement settings. A set of measurement files will also be present with at least one for each input channel available. The measurement files will be named in the form **channelX** for Raw TIE data, **channelX_[FWD_PDV | REV_PDV | PATH_DELAY]** for Raw PDV data, **channelX_2Way_TE** for 2Way TE data and **channelX_ESMC_QUALITY** for SyncE SSM message transitions. Channel files in binary format will have **.dset** as their extension. A text file (**measurement.summary.txt**) is also saved in the folder, detailing a Pass/Fail summary for each channel along with the value of any user defined masks. Additionally PTP announce message arrival time and header fields are logged and stored in a CSV format file (**announce_message_updates.sentinel**).

Saved measurement data that has been exported via a USB memory stick or over the Ethernet connection can be loaded into the Calnex CAT analysis software package on a workstation or laptop for further analysis.
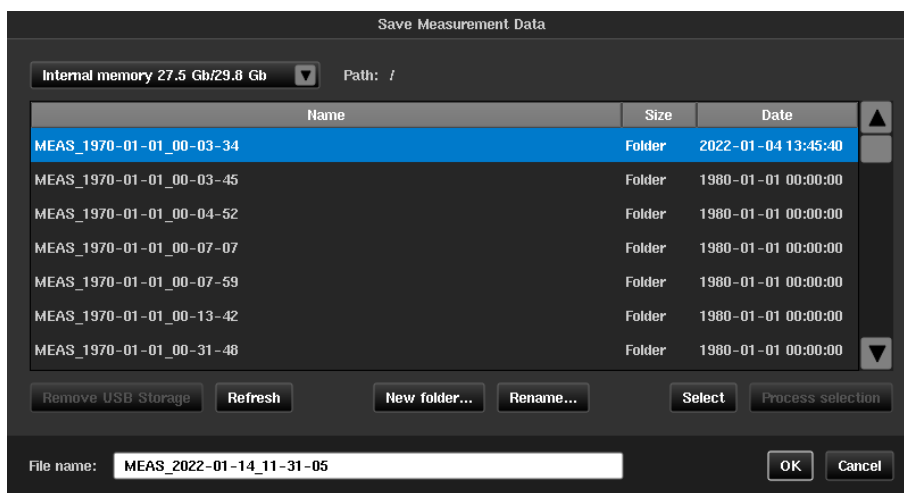
When a new measurement is started the user will be prompted to save the measurement. The window above will appear to select the saving location. The user can select internal instrument memory or connected USB memory stick. The default folder name can be changed.

This folder can be renamed, copied, moved, or deleted using the **Settings** menu. It can also be copied or moved using the USB interface or the Ethernet network, via an **FTP** connection.

After a measurement has stopped the instrument needs some time to do a post-processing of measurement data (calculate metrics). During this stage a dialog box is shown on the screen. Post-processing of measurement results can be cancelled with no loss of data by pressing the **Abort** button of the displayed dialog.

When the measurement has completed, if there are masks enabled, the overall Pass/Fail status is displayed in a dialog box along with the location of the measurement results. Test Passed will be displayed if no measured values fall out with the applied masks. If required, the summary of the test results can be displayed by selecting the **View Report** button.
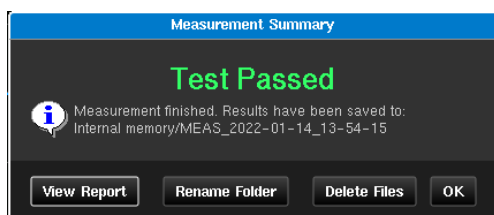
Measurement Result Graph

Sentinel creates a graph for every measurement and its associated metrics. The graphs that are displayed and the order that they appear in the navigation panel can be configured by pressing the graph selection button highlighted below.

A Hide / Show checkbox and associated measurement description is available for each graph. Graph ordering can be changed by highlighting the graph name and pressing the **Order** arrow buttons.
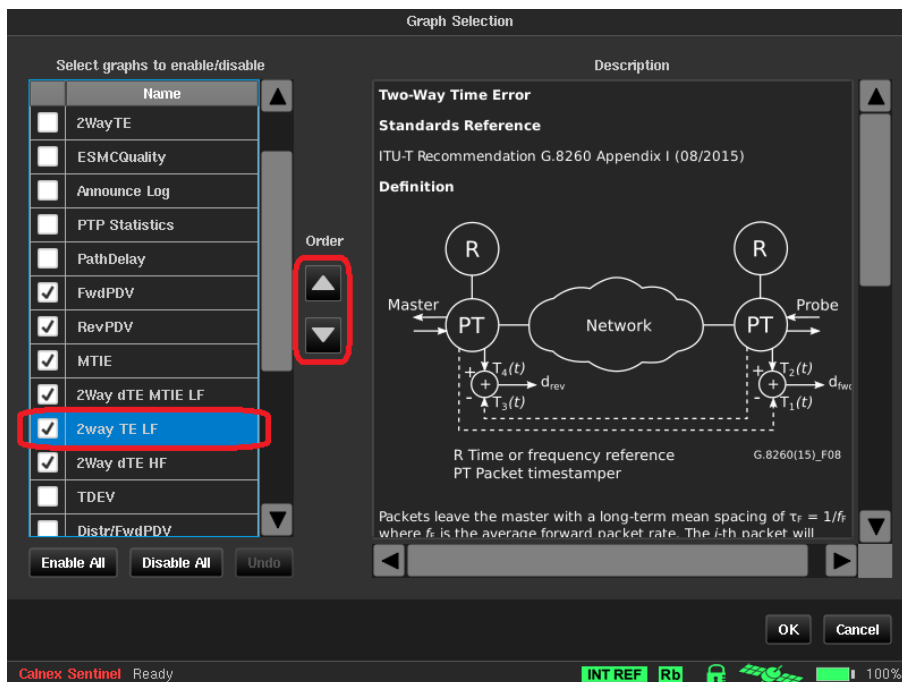
The measurements made remain displayed on the screen until a new measurement sequence is started by pressing the **Start/Stop** button.

The following metrics are calculated from the measurement results.

Metrics for TIE data

TIE	Time Interval Error
MTIE	Maximum Time Interval Error
TDEV	Time Deviation

Metrics for Raw PDV data (Fwd PDV, Rev PDV, Path Delay)

Fwd/Rev/Path Delay distribution	FD/RD/PD Distribution

Metrics for Selected PDV data

FPP	Floor Packets Percentage
MAFE	Maximum Average Frequency Error
SelPDV	Packet Delay Variation Selection

Metrics for Time Error data

TE	Time Error
2Way TE	2Way Time Error
2Way dTE MTIE LF	2Way Dynamic Time Error MTIE Low-Pass Filtered
2Way TE LF	2Way Time Error Low-Pass Filtered
2Way dTE HF	2Way Dynamic Time Error High-Pass Filtered
pktSelected2WayTE	Packet-Selected 2Way Time Error for PTS/APTS networks

Standard masks are available to be overlaid on the applicable MTIE, TDEV, FPP, MAFE and 2Way TE displays. The masks are selected in the **Settings** menu and are displayed by default once selected as described in Masks section above.

Three special kinds of masks are available – TIE mask, Time Error (TE) mask and FPP mask. It is possible to setup parameters of these masks and turn them on/off from **Settings** window. TIE mask marks acceptable range for TIE values. TE mask marks acceptable range for 2Way TE values. FPP mask marks minimum acceptable floor packets percentage.

The various measurements made, and the masks applied are clearly identified. A solid line is used to indicate each of the measurements being made on each graph. Each channel uses a specific colour. The colour used is the same as that shown in the **Channel Widget**. A dashed line is used to represent a mask.
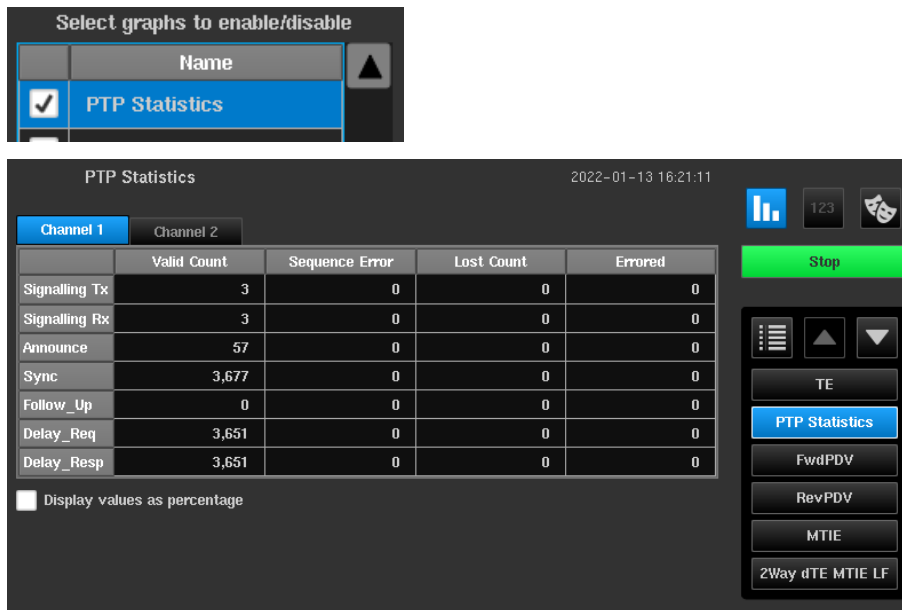
This means that the quality of the measured signal can be interpreted immediately. For FPP measurement to be compliant, its representative curve must be above the mask. For all other measurements to be compliant, the representative curve must be below the mask.

All active channels are automatically checked versus all relevant active masks in real-time. Mask pass / fail status is displayed inside each active channel widget, in relation with the selected masks (for MTIE and TDEV metrics). Detailed information about check results are displayed in the masks table.
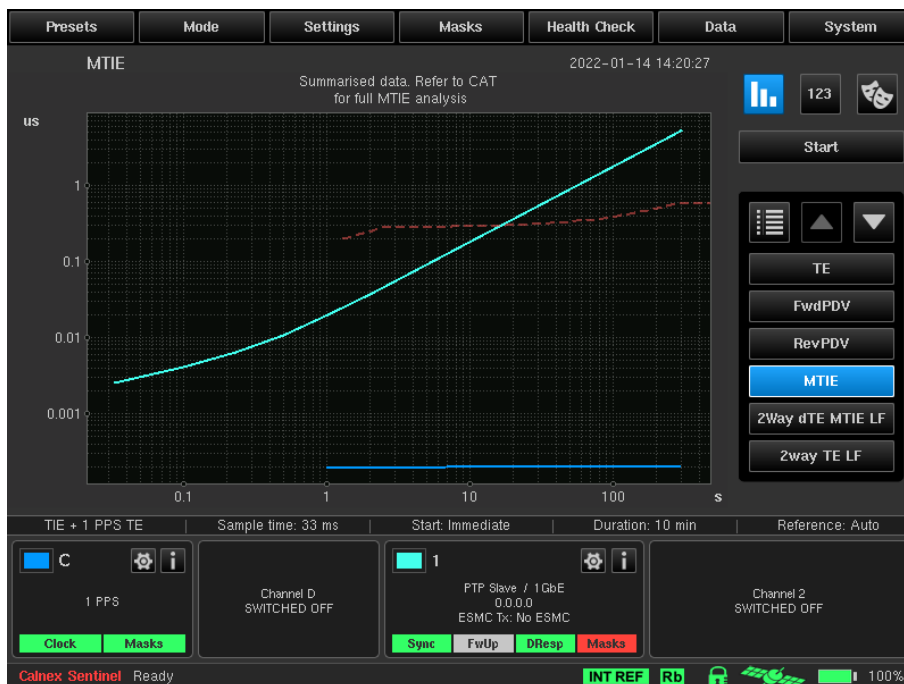
Metric for PTP Statistics

If a PDV measurement has taken place then statistics of the PTP packets used in the measurement can be displayed by selecting to show the PTP Statistics metric on the Graph Selection page.

Statistics are held separately for each PTP card and are selected by the **Channel _x_** tabs at the top of the table.

Columns indicate the number of PTP packets received that had a PTP sequence error, lost PTP packets or errored PTP packets.

Statistics can also be displayed as a percentage rather than an absolute count.

The rows indicate the different types of PTP packets. Results are stored in .csv format to a file named **_ptp_measurement_statistics.sentinel_** in the folder specified when the measurement was started.

Note: In pseudo slave mode Signalling Tx and Delay_Req messages originate from Sentinel and all others from the GM.

Note: In monitor mode all packets are received from the TAP or splitter and so the messages from the GM will show up on one channel and the messages from the T-TSC on the other. All signalling will appear in the Signalling Rx row. Signalling from the GM will be on the channel that has Sync messages and signalling from the T-TSC will be on the other channel.

Viewing Mode

The buttons indicated by (4) allow the user to switch between views. The default view shows only the measurement graphs selected.

7.1 Masks Table

A list of all currently selected masks and the status of each of these masks for relevant channels can be displayed by selecting the **Mask** 🎭 button at the top right of the Sentinel main display as highlighted below.
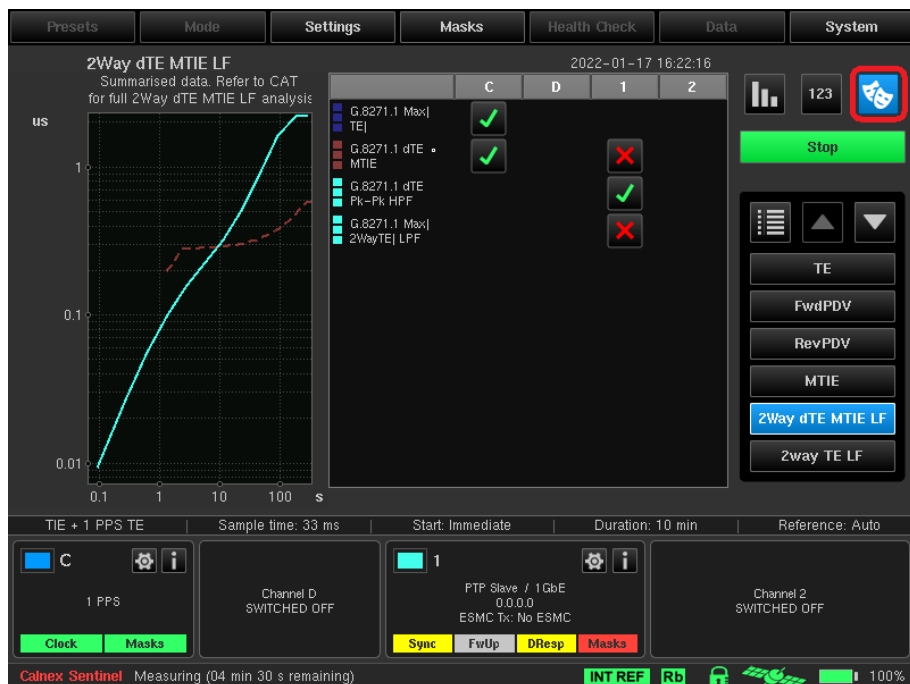
This table shows all enabled masks in rows and channels in columns. The button displays ✔ if all metrics are OK versus each mask. If at least one metric has failed, then ✗ is displayed. It is possible to press these buttons and a popup menu will appear demonstrating the list of all metrics for the selected channel together with the status of mask check. Selecting an item from this popup menu will switch the screen to display corresponding metric. Also, it is possible to touch the mask name in the list of masks to enable/disable it.

7.2 Measurement Analysis

The measurement analysis can be toggled on / off by pressing the Analysis button highlighted below. This displays the mean, standard deviation, initial phase offset and final value for the currently displayed graph.
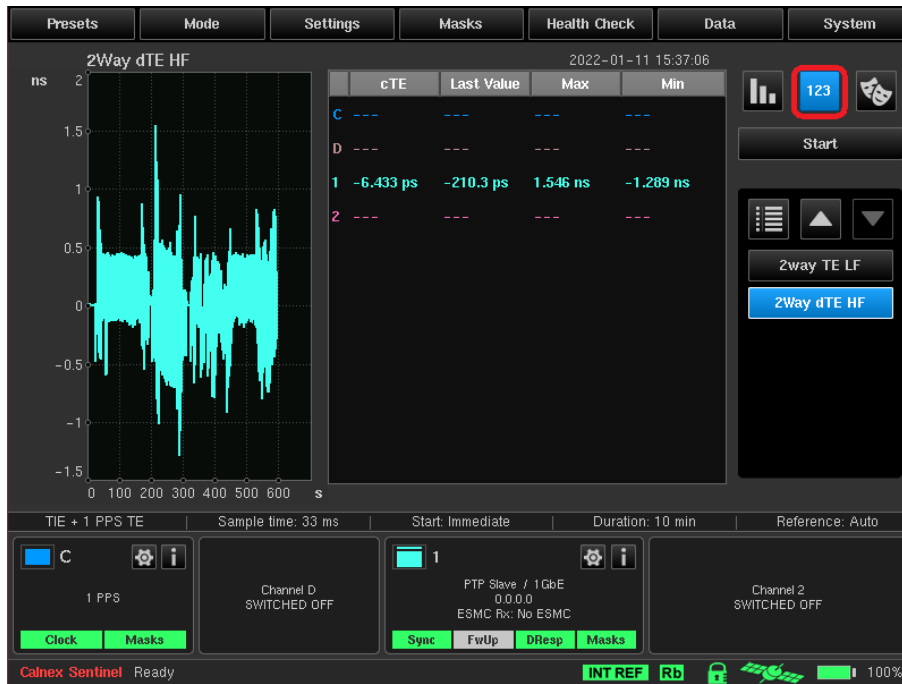
Widgets & Icons

A Widget is displayed at the bottom of the screen for each of the input modules and corresponding channels. Each input module will feature one or more channel. Each Widget is named based on the corresponding symbol on the Side panel of the Sentinel. For the display below one Clock module is installed with channels C & D, two Packet modules are installed represented by channels 1 & 2.

A series of status icons are available on the bottom status bar of Sentinel indicating the state of various modules/features of the Sentinel unit.

8.1 Measurement channels

Each populated measurement channel has an associated widget to indicate the status and configuration of the channel and to allow quick access to the channel settings. Each channel has a specific colour in the top left which corresponds to the graph for that channel
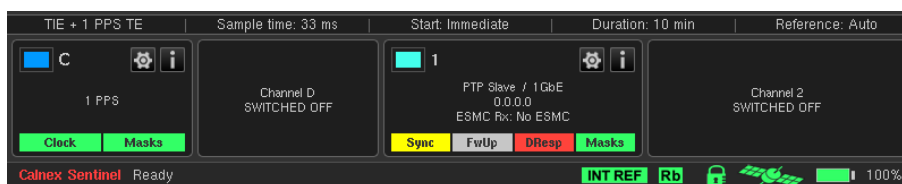
The coloured button in the top left of each Widget for a channel can be used to bring the channel to the foreground of the displayed measurements (**Bring to top**) or to hide it from the measurement screen and mask test (**Hide**). When hidden the background of the input signal data will be greyed out and the coloured button can be used to re-enable display of the channel (**Show**).

Loss of signal LEDs and Mask pass / fail results are displayed at the bottom of the widget.

A green LED indicates that the associated clock signal, OTA lock or PTP/NTP message is present or that the mask has passed.

A red LED indicates that the associated clock signal, OTA lock or PTP/NTP message is absent or that the mask has failed.

A yellow LED indicates that the associated clock signal, OTA lock or PTP/NTP message has been absent but is now present again.

A grey LED indicates that the associated PTP message is not relevant (e.g. Follow Up when running in 1-step mode) or the test has not run long enough to validate the mask.

The settings button on a widget will navigate directly to the settings page for that channel.
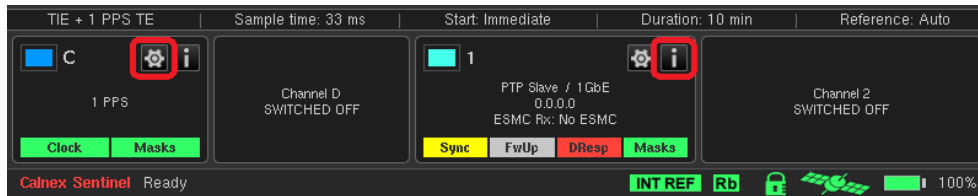
The Info button will display more detailed information on the selected channel.

PTP
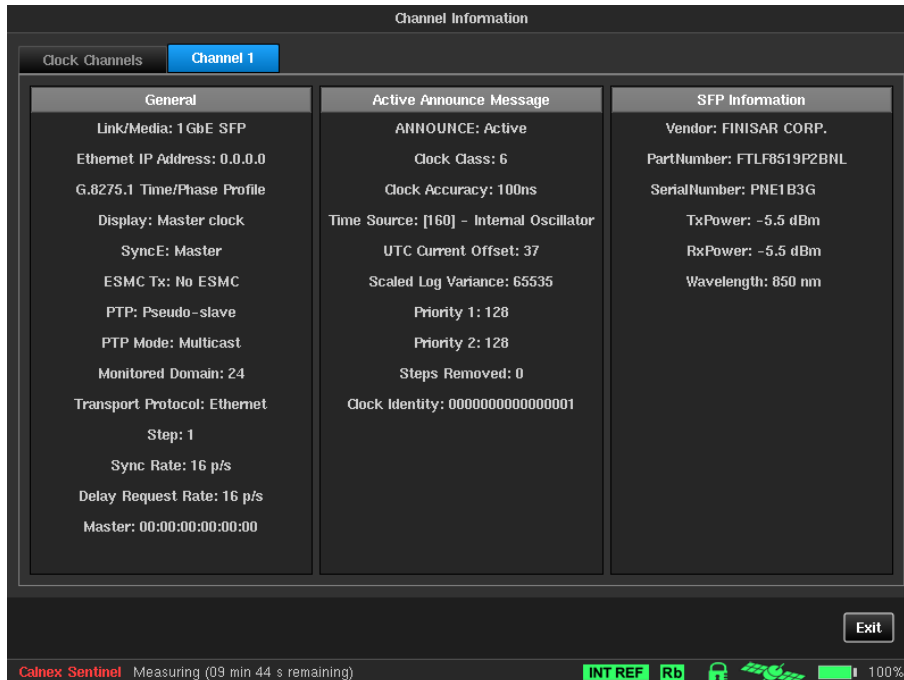
NTP

OTA-LTE

OTA-NR

8.2 Status icons

A summary screen of the status icons can be displayed by pressing the status icon display area.
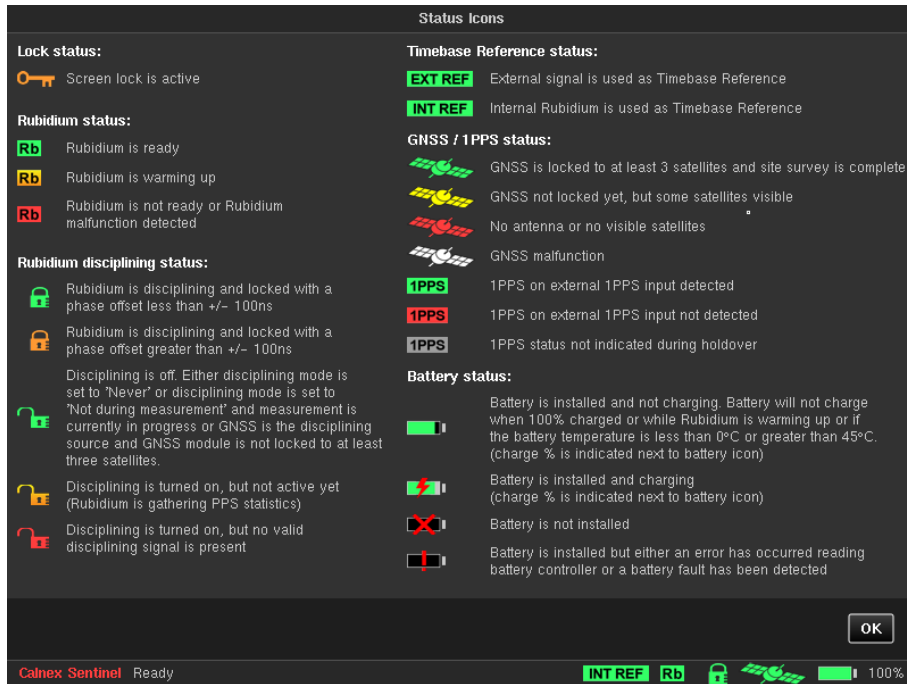
8.3 Real Time Marker

A real time marker can be placed on any of the measurement graphs by touching the desired point on the screen. The marker can be removed by touching the marker a second time.
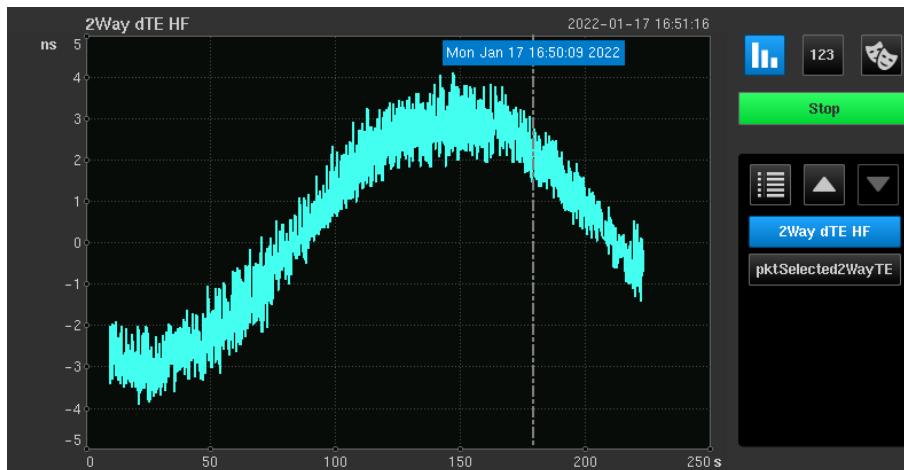
Remote Access

9.1 VNC Access

Sentinel firmware includes a **VNC** server enabling the instrument to be remote-controlled by a PC connected to the network. This PC must have **VNC** client software installed.

For access to the instrument, its IP address must be known to the remote PC. This setting is available for configuration in the **System** menu as detailed previously.

It is possible to define the IP address manually (depending on the characteristics of the network to which the instrument is connected) or to obtain a **DHCP** IP address through the network router. This address is then displayed in the **IP address** field.
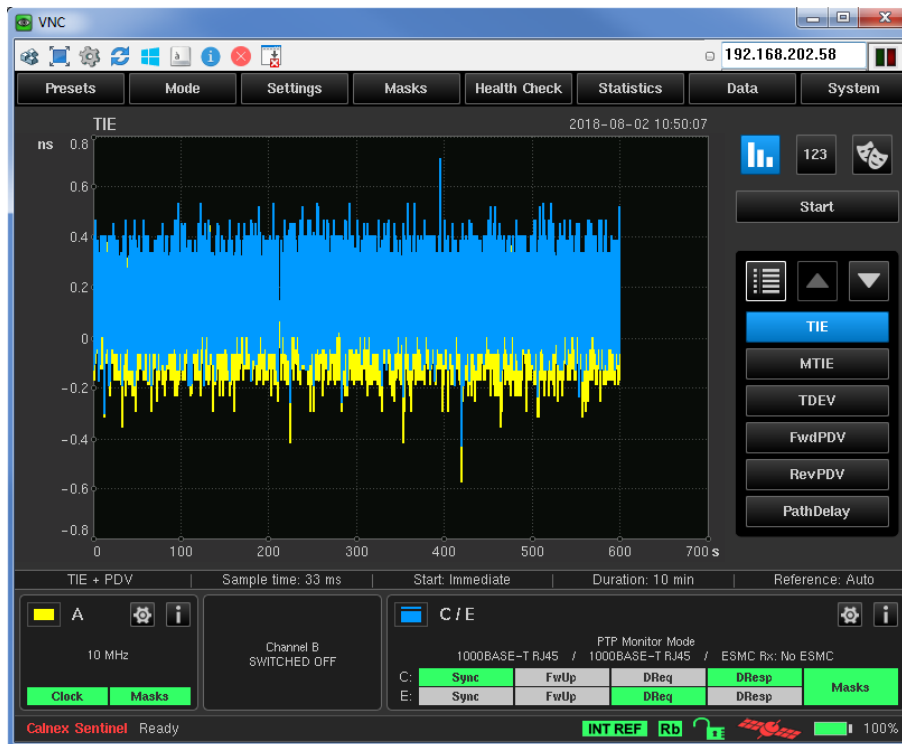
A **VNC** client can then be used to display the instrument graphic interface on the remote PC. The instrument can be controlled in the same way as on the instrument itself.

Remote Control

Sentinel can be controlled via an HTTP based API. A selection of features that are available via this service are as follows: measurements can be started and stopped; raw measurement data can be downloaded; device configuration can be viewed and modified. The interface also allows new firmware to be downloaded to the device without needing local access.

The device can be accessed via HTTP and HTTPS and where HTTPS is being used it is also possible to enable authentication to prevent un-authorised access to the device.

10.1 Authentication

The Sentinel remote control interface can be protected via an API interface. The authentication is implemented as a seed, key exchange. Authentication is enabled via the Network Sharing screen as shown below.

Information on the above options is available in section 4.7.

Authentication where required is enabled via the Authentication Enabled flag. A Key Seed should also be set at that point. The key seed is required each time a user wishes to start an authentication session with the Sentinel remote control API.

To start an authenticated session the *getkey* API call should be made passing the currently set key that has been configured within the Sentinel settings. On receiving the valid seed, Sentinel will return an access key that can be used for all services requiring authentication.

Example

An example handshake with sentinel using authentication would be as follows.

```
curl -k https://10.0.0.100/api/getkey?seed=1234
```

This will result in a response being received like the following

```
34954a1a5ac07c8ed130d4444badb1e524f812d10e2180ced8cbb52f4344e17e
```

For the following commands, the key has been shortened for clarity, but the full key would need to be passed to the API call to pass authentication.

```
curl -k https://10.0.0.100/api/version?key=34954a1a5ac07c8ed130…
curl -k
https://10.0.0.100/api/lockscreen?"key=34954a1a5ac07c8ed130…&password=12345"
curl -k https://10.0.0.100/api/login?key=34954a1a5ac07c8ed130d444…
```

After the login API call has been made it is no longer required to pass the key for each command as we have logged into the API using the required key and the *login* API call.

```
curl -k https://10.0.0.100/api/startmeasurement
curl -k https://10.0.0.100/api/logout
```

For the API calls *getkey* and *logout*, the key is not required. Following the logout call the key is required on each subsequent call.

```
curl -k https://10.0.0.100/api/stopmeasurement?key=34954a1a5ac07c8ed130…
```

The key obtained via *getkey* is valid until the next power cycle of the Sentinel or until the Key Seed is changed within settings.

Login

Sentinel considers authentication against a particular IP address. Once you have logged in to the interface, any access from the same source IP address will be accepted without the need for the key to be provided on each request. Where this is an issue, you should avoid using the login function and instead should provide the key on each API request.

A login will remain valid until *logout* has been called or the timeout period as set via the HTTP(S) API option screen has passed.

10.2 API Interface Service List

List

API Call

/api/list

Summary

Display a list of available API calls

Description

This call displays a list of all available API calls available for the interface. The access modes allowed for the current configuration is also displayed. Examples of where the access modes allowed can change are as follows.

- When authentication is enabled only HTTPS access is allowed.
- *getkey* and *login* are only ever available via HTTPS as these services deal with accessing the API via authentication.
- The access mode will not be available if that access mode has been disabled in the configuration of the API

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

Returns

Basic HTML table of all services available via the remote-control API

Example

Browser
http://192.168.123.123/api/list

Curl
curl http://192.168.123.123/api/list

GetKey

API Call

/api/getkey

Summary

Obtain API key for authentication

Description

This call is used to obtain the current API key required for authentication. The key is based on the seed set within the configuration and another random seed internal to the Sentinel. The current security seed must be provided to this call as a parameter. If the correct seed is provided as e.g., *seed=1234,* the required API key will be returned as plain text. The returned key should be used for all subsequent API calls requiring authentication. The API key changes each time Sentinel is restarted, or the API seed is changed.

Parameters

Name	Description	Required
seed	The value of the currently configured seed key for the API stored within settings	✓

Returns

The returns the required API key for the current session, an example would be as follows.

```
34954a1a5ac07c8ed130d4444badb1e524f812d10e2180ced8cbb52f4344e17e
```

This call returns a `403 Forbidden error` if it is accessed via HTTP.

Example

Browser
https://192.168.123.123/api/getkey?seed=1234

Curl
curl -k https://192.168.123.123/api/getkey?seed=1234

The parameter -k for curl is used in this case as we have no valid SSL certificate configured and we are telling curl to allow insecure connections.

Both examples assume that the seed is configured to 1234 in the Sentinel settings.

Logout

API Call

/api/logout

Summary

Logout of an authenticated session for the current source IP address

Description

This call logs the current IP address out of an authenticated session resulting in all further API calls now needing authentication. If other users were sharing the same source IP for communication with Sentinel, they would also be logged out. No error will be triggered if the current IP address is not logged into the Sentinel via authentication.

Parameters

Name	Description	Required
	No parameters required	

Returns

JSON status code indicating success status:

```
{
"result" : true
}
```

Example

Browser
https://192.168.123.123/api/logout

Curl
curl -k https://192.168.123.123/api/logout

Login

API Call

/api/login

Summary

Log into the Sentinel using authentication

Description

This logs into the API service and removes the need for authentication on future API calls. This API allows you to authenticate against Sentinel for the IP address used to access Sentinel. Supplying authentication would not be required for future API calls if this login remains valid. The login would be stopped if Sentinel is rebooted, the login timeout expires, or the logout service is called. If multiple devices or users may access the Sentinel from the same IP address then security should be considered before this option is used, and it may be better to authenticate each API call.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and login has not been used	✓

Returns

On success this call will return a JSON string indicating success. The JSON result will also indicate the period when authentication will expire:

```
{
"result" : true,
"message" : "Session will expire in 3600 seconds"
}
```

On failure Sentinel will respond with a *401 Authorization Required* error

Example

Browser

https://192.168.123.123/api/login?key=823de38663e1…

Curl

curl -k https://192.168.123.123/api/login?key=823de38663e1…

The keys have been shortened in the above examples for clarity, but calling this API requires the full key obtained from *getkey* API call.

StartMeasurement

API Call

/api/startmeasurement

Summary

Start a measurement for the current Sentinel configuration

Description

This starts a measurement for the current configuration and enabled channels. A measurement will be started for the currently set duration or continuous if continuous mode is configured. If continuous mode is set the files will be stored on internal memory within the continuous folder as normal. If continuous mode is not set the measurement data will be stored a folder based on the start date and time as normal. No option is available to change the save path for measurements or to save to external memory locations.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

Returns

JSON status code indicating success status:

```
{
"result" : true,
}
```

On failure, Sentinel will give an indication of why a measurement could not be started.

```
{
"result" : false,
"message" : "Measurement already running"
}
```

Example

Browser
https://192.168.123.123/api/startmeasurement

Curl
curl -k https://192.168.123.123/api/startmeasurement

StopMeasurement

API Call

/api/stopmeasurement

Summary

Stop the currently running measurement

Description

This command will stop both regular and continuous mode measurements.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

Returns

JSON status code indicating success status:

```
{
"result" : true,
}
```

On failure, Sentinel will give an indication of why the measurement could not be stopped.

```
{
"result" : false,
"message" : "No measurement running"
}
```

Example

Browser
https://192.168.123.123/api/stopmeasurement

Curl
curl -k https://192.168.123.123/api/stopmeasurement

GetStatus

API Call

/api/getstatus

Summary

Get the device status and readiness for making a measurement

Description

This returns a JSON formatted string indicating the readiness to begin a measurement on the Sentinel. This indicates if installed modules would be ready to start a measurement and whether the configured timebase reference is ready for a measurement to be started.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

Returns

JSON status indicating device readiness to perform a measurement:

```
{
"referenceReady": true,
"modulesReady": true,
"measurementActive": false
}
```

If any status indicates a ready as false, then it will not be possible to start a measurement on Sentinel at that time.

Example

Browser
https://192.168.123.123/api/getstatus

Curl
curl -k https://192.168.123.123/api/getstatus

GetMeasurementStatus

API Call

/api/getmeasurementstatus

Summary

Get the status of any running measurement

Description

This call provides a JSON formatted result giving an indication of whether a measurement is currently active.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

Returns

JSON status of any current measurement:

```
{
"measurementActive": true
}
```

Example

Browser
https://192.168.123.123/api/getmeasurementstatus

Curl
curl -k https://192.168.123.123/api/getmeasurementstatus

GetChannelList

API Call

/api/getchannellist

Summary

Get a list of all currently installed or enabled channels

Description

This service provides a JSON formatted list of measurement channels installed in the Sentinel. This shows a list of the channels installed in the unit. Passing the parameter active shows those channels that are enabled for measurement.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

active   Limit the returned channel list to those channels that are enabled via the
                mode page

Returns

JSON formatted list of installed channels:

```
{"channels": ["C", "D", "2"] }
```

Example

Browser
https://192.168.123.123/api/getchannellist

Curl
curl -k https://192.168.123.123/api/getchannellist?active

GetChannelDataTypes

API Call

/api/getchanneldatatypes

Summary

Get a list of all valid data types for all installed or enabled channels

Description

This service provides a JSON formatted list of data types for each of the installed channels. This list shows what data types can be used with the *getdata* API call.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	
active	Limit the returned channel list to those channels that are enabled via the mode page	

Returns

JSON formatted list of installed channels:

```
{"channels":
    [
        {"C": {"dataTypes": [ "tie" ]}},
        {"D": {"dataTypes": [ "tie" ]}},
        {"2": {"dataTypes": [ "tie", "2wayte", "pd", "fwdpdv", "revpdv", "esmc" ]}}
    ]
}
```

Example

Browser
https://192.168.123.123/api/getchanneldatatypes?"active&key=3823de38663…"

Curl
curl http://192.168.123.123/api/getchanneldatatypes

GetData

API Call

/api/getdata

Summary

Get measurement data for the specified data type and channel

Description

This service returns a CSV list of measurement points for the specified channel and datatype. The list returned are those values for the specified parameters that have been measured since the last request.

Specify *reset=true* on the request to begin data collection from the beginning of available data.

The data returned is ordered as **[timestamp (UTC)], [measurement value (s)]**.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	
channel	The channel indicator for the data this is to be obtained. The valid channel numbers are indicated by a call to *getchannellist*.	✓
datatype	The data type that should be obtained for this call. The valid data types are available via the *getchanneldatatypes* call.	
	If no datatype is specified tie data will be returned by default.	
reset	Restart the data stream from the beginning of the available data. This will normally be from the start of the measurement or from the start of the day whilst running in continuous mode.	
	This parameter should be set to *true* for it to be actioned.	

Returns

This call returns a CSV formatted list of measurement data for the specified channel. This data is ordered as **[timestamp (UTC)], [measurement value (s)]**. Nothing will be returned if no data is available for the specified channel and data type.

```
…
1614874626.033000,-330000.033000000345
1614874626.066000,-660000.066000000108
1614874626.099000,-990000.099000000162
1614874626.132000,-1320000.131999999983
1614874626.165000,-1650000.165000000037
1614874626.198000,-1980000.198000000324
1614874626.231000,-2310000.231000000145
1614874626.264000,-2640000.263999999966
1614874626.297000,-2970000.297000000253
1614874626.330000,-3300000.330000000075
1614874626.363000,-3630000.362999999896
1614874626.396000,-3960000.396000000183
1614874626.429000,-4290000.429000000469
1614874626.462000,-4620000.462000000291
1614874626.495000,-4950000.495000000112
1614874626.528000,-5280000.527999999933
1614874626.561000,-5610000.561000000685
1614874626.594000,-5940000.594000000507
…
```

Example

Browser

https://192.168.123.123/api/getdata?channel=1&datatype=2wayte

Curl

curl http://192.168.123.123/api/getdata?"channel=C&datatype=tie&reset=true"

GetSettings

API Call

/api/getsettings

Summary

Get the current Sentinel configuration in the preset file format

Description

This service provides a list of all settings in the current Sentinel configuration. The format used is the same as that used for a saved preset using the Sentinel GUI. The file obtained with this command can be loaded into a Sentinel using either the *setsettings* API call or the Recall Settings option on the Sentinel GUI.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

Returns

A preset format list of the current Sentinel settings:

```
[api]
cached_login_timeout=1 hours
clear_cahce_seed_change=Yes
http_enabled=Yes
https_enabled=Yes
key_seed1=12345
key_seed1_enabled=No

[e1t1_outputs]
e1_encoding=HDB3
e1_framing=HDB3 without CRC-4
mode=Disabled
t1_encoding=B8ZS
t1_framing=D4/Superframe
…
```

Example

Browser
https://192.168.123.123/api/getsettings

Curl
curl http://192.168.123.123/api/getsettings

SetSettings

API Call

/api/setsettings

Summary

Upload a new configuration to the Sentinel in preset file format

Description

Upload a new complete settings configuration to the Sentinel. The file uploaded should be in the same format as obtained via getsettings. It would also be possible to change the Sentinel configuration using this file and the Recall Settings menu option on the Sentinel GUI.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	
action	If this parameter is set to *default* whilst calling the service, all settings will be restored to their default values.	

Returns

JSON status code indicating success status:

```
{
"result" : true,
}
```
On failure, Sentinel will give an indication of why the measurement could not be stopped.

```
{
"result" : false,
"message" : "Could not load settings"
}
```

Example

Browser
Not Applicable

Curl
curl -k https://192.168.123.123/api/setsettings –data-binary @settings.preset

In this case the file called *settings.preset* will be uploaded to the Sentinel and applied as a new configuration if it passes validation. The current settings can be downloaded using *getsettings* and used as a template for required new configuration. Alternatively, preset files can be saved within Sentinel using the Save Preset option.

Get

API Call

/api/get/[required setting(s)]

Summary

Get a parameter or group of parameters from the current Sentinel configuration

Description

This service call returns one or more parameters from the Sentinel configuration based on the specified parameter name or group. The following shows an example of what can be specified.

/api/get	When specified without any additional information this API call will return a list of all groups that are available within the Sentinel configuration. These groups correspond to those included in the preset file obtained via the *getsettings* API call.
/api/get/measure	This would return a list all settings in the measure group.
/api/get/measure/meas_time	This would return only the value for the *meas_time* parameter.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

Returns

A list of one or more parameters is returned with their current values. A section of what would be returned for */api/get/measure* is as follows:

```
…
measure/transparent_mode/monitored_ip1=10.32.1.163
measure/transparent_mode/monitored_ip1_ipv4=10.32.1.163
measure/transparent_mode/monitored_ip1_ipv6=2000::000a
measure/transparent_mode/monitored_ip2=10.32.1.168
measure/transparent_mode/monitored_ip2_ipv4=10.32.1.168
measure/transparent_mode/monitored_ip2_ipv6=2000::000b
measure/transparent_mode/monitored_mac1=E00000000001
measure/transparent_mode/monitored_mac2=F00000000001
measure/transparent_mode/monitored_slave_clkid=0000000000000000
measure/transparent_mode/monitored_master_clkid=0000000000000000
measure/transparent_mode/monitored_mode=0
measure/transparent_mode/include_correction_field=1
measure/context/meas_started=
measure/context/meas_stopped=
measure/context/reference_used=2
measure/ch0/installed=0
measure/ch0/used=false
measure/ch0/signal_type=
measure/ch0/freq=1
measure/ch0/pulse_width=1
measure/ch0/trig_level=0
measure/ch0/vmin=0
measure/ch0/vmax=0
…
```

The actual returned parameter list will vary depending on the current configuration of Sentinel and the installed modules and options available.

Example

Browser
https://192.168.123.123/api/get/measure

Curl
curl http://192.168.123.123/api/get/api/http_enabled

Set

API Call

/api/set/[required setting]

Summary

Set a parameter within the Sentinel configuration

Description

This API call sets one individual setting within the Sentinel configuration. The required value is passed to the API. In general, it is recommended to determine the required options via the Sentinel screen and identify which setting requires to be changed to switch between various modes of operation. These parameters can then be sent to the Sentinel using the *set* call.

There is no additional information available as to the range of values that are appropriate for each parameter beyond that displayed on the Sentinel settings screens.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	
value	Specify the new value required for the parameter being set.	✓

Returns

A JSON formatted status will be returned if the group name or parameter name is not valid:

```
{
"result" : false,
"message" : "No parameter match found - measure/unknown"
}
```

Or

```
{
"result" : false,
"message" : "Not a valid group name - measure1"
}
```

If the parameter and group name is valid the new setting for the parameter will be returned in the same format as the get API call would return. If the parameter could not be set due to it falling outside its allowed range, the current value will be returned.

Example

Browser
http://192.168.123.123/api/set/measure/meas_time?value=1800

Curl
curl -k https://192.168.123.123/api/set/api/http_enabled?value=0

LockScreen

API Call

/api/lockscreen

Summary

Lock the local Sentinel GUI preventing accidental changes whilst under remote control

Description

This service can be used to lock the GUI and prevent accidental modifications taking place at the device whilst remote control is in operation. It is also possible to specify a password using the *password* parameter option. When set this password would be required to unlock the Sentinel via the GUI. The password is not required when unlocking via the *unlockscreen* service.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	
password	Specify a password that must be used when attempting to unlock the Sentinel GUI locally.	

Returns

JSON status code indicating success status:

```
{
"result" : true,
}
```

Example

Browser
http://192.168.123.123/api/lockscreen?password=1234

Curl
curl -k https://192.168.123.123/api/lockscreen

UnlockScreen

API Call

/api/unlockscreen

Summary

Unlock the local Sentinel GUI

Description

This service unlocks the Sentinel GUI to allow local operation at the device. A password is not required for this service even if a password was set via the *lockscreen* API call.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	

Returns

JSON status code indicating success status:

```
{
"result" : true,
}
```

Example

Browser
https://192.168.123.123/api/unlockscreen

Curl
curl -k https://192.168.123.123/api/unlockscreen

GetProblemReport

API Call

/api/getproblemreport

Summary

Download a problem report from Sentinel

Description

This API call prepares a new problem report and downloads the file when available. The file once downloaded, can be provided to Calnex support where required. This will aid investigation of any current Sentinel device issues.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	

Returns

A problem report file as would be obtained via the Export Problem Report option on the **About** page.

Example

Browser
https://192.168.123.123/api/getproblemreport

Curl
curl -k https://192.168.123.123/api/getproblemreport -JO

GetScreenShot

API Call

/api/getscreenshot

Summary

Download a screen shot of the current GUI display on Sentinel

Description

This service performs a screen captures of the currently displayed Sentinel GUI. The capture will be downloaded as a PNG file.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	

Returns

A screen shot in PNG format.

Example

Browser
https://192.168.123.123/api/getscreenshot

Curl
curl -k https://192.168.123.123/api/getscreenshot -JO

Instrument

API Call

/api/get/[selection]

Summary

This API call obtains information about the Sentinel device

Description

This service obtains a series of JSON formatted information about the Sentinel. The information selections available are as follows:

/api/instrument/information   This will return the device type and serial number.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used	

Returns

JSON information for the requested selection, an example for the instrument/information is as follows:

```
{
    "HwType": "Sentinel",
    "SerialNumber": "300285",
    "HwCapabilities": []
}
```

An error in JSON format will be returned if the selection is not valid:

```
{
"result" : false,
"message" : "Not a valid subservice - information1"
}
```

In the above error, *instrument/information1* was requested rather than *instrument/information*.

Example

Browser
https://192.168.123.123/api/instrument/information

Curl
curl http://192.168.123.123/api/instrument/information

Version

API Call

/api/version

Summary

Get the version of the Sentinel firmware installed on the unit.

Description

Obtain the version of the firmware installed on Sentinel.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	

Returns

JSON formatted information on the firmware installed on the Sentinel unit:

```
{ "firmware": "2.13.0.1.5569-20210302" }
```

Example

Browser
https://192.168.123.123/api/version

Curl

curl -k https://192.168.123.123/api/version

Reboot

API Call

/api/reboot

Summary

Reboot the Sentinel device.

Description

This service reboots the Sentinel device, no prompt or interlock will be provided. *action* must be included in the request or the reboot will not take place, this is a mechanism to prevent accidental reboot by calling this API. No mechanism is available to stop this service once it has been called.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	
action	This parameter must be included and must be set equal to reboot for the reboot to be actioned.	✓

Returns

JSON formatted status for the request:

```
{
"result" : true,
"message" : "Sentinel will now reboot"
}
```

Example

Browser
https://192.168.123.123/api/reboot?action=reboot

Curl
curl -k https://192.168.123.123/api/reboot?action=reboot

InstallCertificate

API Call

/api/installcertificate

Summary

Install a PEM format certificate and key file for SSL.

Description

Install a new certificate file for the API Interface in PEM format. This must be a combined certificate and key file. The API interface will be restarted after installing the certificate. After the *pem* certificate file has been installed the API service will be restarted and the new certificate should be in use. If the certificate cannot be installed the Sentinel will default to a built-in certificate file.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	

Returns

JSON formatted status for the request:

```
{
"result" : true,
"message" : "The API Interface will now be restarted"
}
```

Example

Browser
Not Applicable

Curl
curl -k https://192.168.123.123/api/installcertificate –data-binary @certificate.pem

ClearDevice

API Call

/api/cleardevice

Summary

Clear all user data from the Sentinel device.

Description

This service clears all user information from the device. All user measurements, settings and log files will be deleted. This will also clear installed certificate files where present. *action* must be included in the request to prevent accidental device erasure by calling this API. No mechanism is available to stop this service once it has been called. Data is not recoverable, and any required data should be removed from the Sentinel before calling this API. The API call will give an indication if any of the user files could not be delete from Sentinel.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	
action	This parameter must be included and must be set equal to cleardevice for the *cleardevice* to be actioned.	✓

Returns

JSON formatted status for the request:

```
{
"result" : true,
"message" : "Device data cleared. The device will now reboot."
}
```

If action is not included on the API call as a parameter the following response will be received:

```
{
"result" : false,
"message" : "Confirmation not provided"
}
```

If all user data cannot be deleted the following response will be received:

```
{
"result" : false,
"message" : "Device data could not all be removed. Please retry or reboot and then
retry."
}
```

Example

Browser
https://192.168.123.123/api/cleardevice?action=cleardevice

Curl
curl -k https://192.168.123.123/api/cleardevice?action=cleardevice

UpdateFirmware

API Call

/api/updatefirmware

Summary

Load a new firmware version onto the Sentinel device.

Description

This service loads a new firmware version onto the Sentinel device as provided by Calnex. This firmware would normally be uploaded via the About page of the System menu but can also be uploaded and applied via this remote API service.

Parameters

Name	Description	Required
key	Authentication key obtained from *getkey* where enabled and *login* has not been used.	
action	This parameter must be included and must be set equal to cleardevice for the *cleardevice* to be actioned.	✓

Returns

JSON formatted status for the request:

```
{
"result" : true,
"message" : "Installing firmware Version: 2.14.0.0.1234-20210924"
}
```

If the provided file cannot be installed then the following will be returned:

```
{
"result" : false,
"message" : "Update failed, check firmware file"
}
```

Example

Browser
Not Applicable

Curl

curl -k https://192.168.123.123/api/updatefirmware --data-binary @/home/user/sentinel_fw_R14.0.0.tar

10.3 Recovery API Interface Service List

The API service calls should not be used in normal operation and their equivalents in the API service list should be utilised. These services are intended for recovering the Sentinel to a working state if it is being unresponsive to API calls and there is no local access available to the unit to perform corrective actions.

These services are not limited to https, may not make use of any https certificate installed and also do not require authentication for use. These limitations are all intended to aid recovery as some of these mechanisms may be the cause of limited API access normally.

Clear

API Call

/api/clear

Summary

Clear all user data from the Sentinel device.

Description

This service clears all user information from the device. All user measurements, settings and log files will be deleted. This will also clear installed certificate files where present. *action* must be included in the request to prevent accidental device erasure by calling this API. No mechanism is available to stop this service once it has been called. Data is not recoverable after calling this service. The API call will give an indication if any of the user files could not be delete from Sentinel.

Parameters

Name	Description	Required

action	This parameter must be included and must be set equal to clear for the *clear* to be actioned.	✓

Returns

JSON formatted status for the request:

```
{
"result" : true,
"message" : "Device data cleared. The device will now reboot."
}
```

If action is not included on the API call as a parameter the following response will be received:

```
{
"result" : false,
"message" : "Confirmation not provided"
}
```

If all user data cannot be deleted the following response will be received:

```
{
"result" : false,
"message" : "Device data could not all be removed. Please retry or reboot and then
retry."
}
```

Example

Browser
http://192.168.123.123/api/clear?action=clear

Curl
curl http://192.168.123.123/api/clear?action=clear

Reset

API Call

/api/reset

Summary

Reboot the Sentinel device.

Description

This service reboots the Sentinel device, no prompt or interlock will be provided. *action* must be included in the request or the reboot will not take place, this is a mechanism to prevent accidental reboot by calling this API. No mechanism is available to stop this service once it has been called.

Parameters

Name	Description	Required
action	This parameter must be included and must be set equal to reboot for the reboot to be actioned.	✓

Returns

JSON formatted status for the request:

```
{
"result" : true,
"message" : "Sentinel will now reboot"
}
```

Example

Browser
http://192.168.123.123/api/reset?action=reset

Curl
curl http://192.168.123.123/api/reset?action=reset

© Calnex Solutions

Calnex CAT PC Software Guide

Calnex Analysis Tool (CAT) is a standalone PC Software package that can be used for comprehensive analysis of TIE, PDV and TE measurements made by Sentinel. It also has a comprehensive report generation capability.

Files can be loaded in to CAT as follows: Open File then navigate to file(s) location.
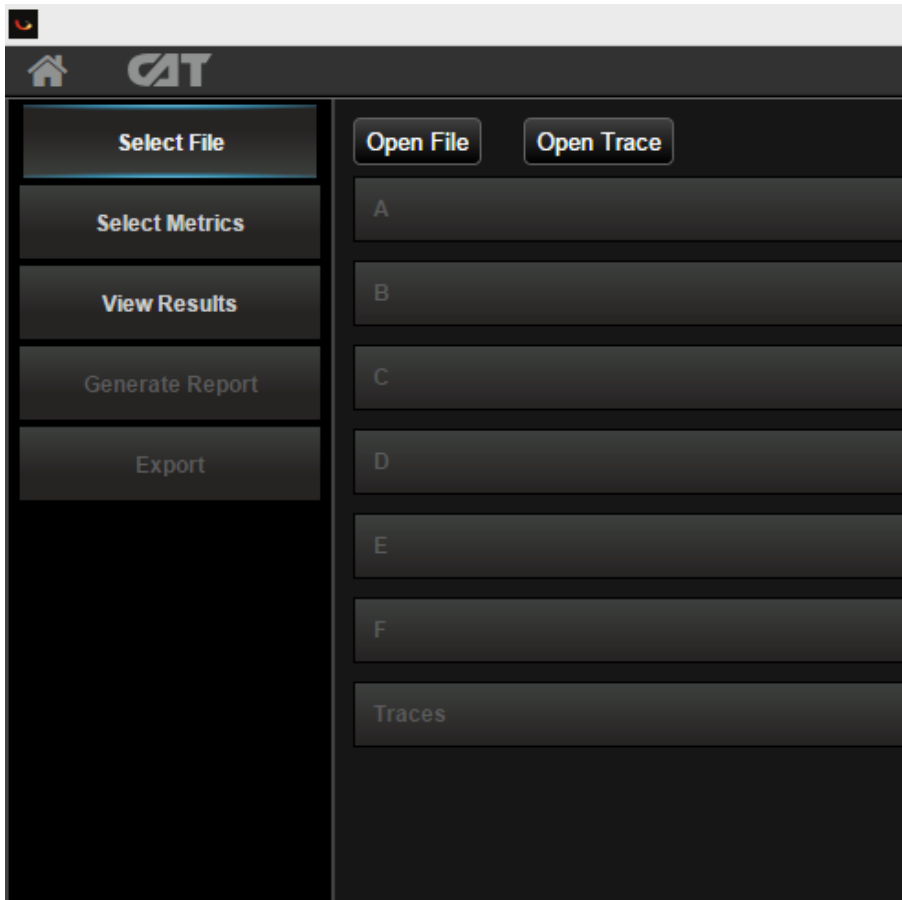
Binary files from Sentinel can be used. Multiple files can be added at the same time.

Once these files have been imported the required metrics can be selected from the Select Metrics menu by selecting the appropriate tick box

Then the Calculate button should be pressed. The metrics will be calculated and the graphs will appear in the relevant tab.
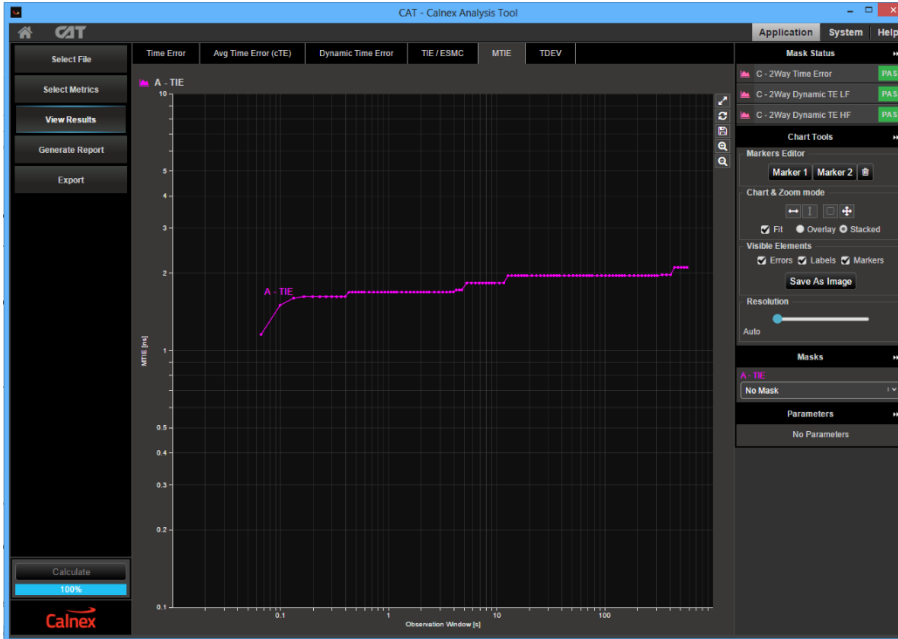
Once analysis has been completed a pdf report can be created. Go to Generate Report and Save Report. You can enter further details to the report on this screen also.

Metrics Available

Clock Metrics

- MTIE/TDEV Analysis for Frequency
- ClkFFO

Packet metric Analysis for PTP and NTP

- PDV (PTP and NTP)
- FPP/FPC/FPR
- Packet TIE/MTIE/TDEV/FFO
- MAFE
- Packet Distribution (PDD)

Time Error Metrics

- PTP TE, cTE, dTE, Max |TE|
- PTP pktSelected2WayTE (ITU-T G.8271.2 APTS and PTS networks)

Clock Metrics

- MTIE/TDEV Analysis for Frequency
- ClkFFO

Preventative Maintenance

12.1 Update Firmware

Firmware update files can be obtained from the Calnex Customer Support.

They are installed via the instrument USB interface using the **About** page of the **System** menu.
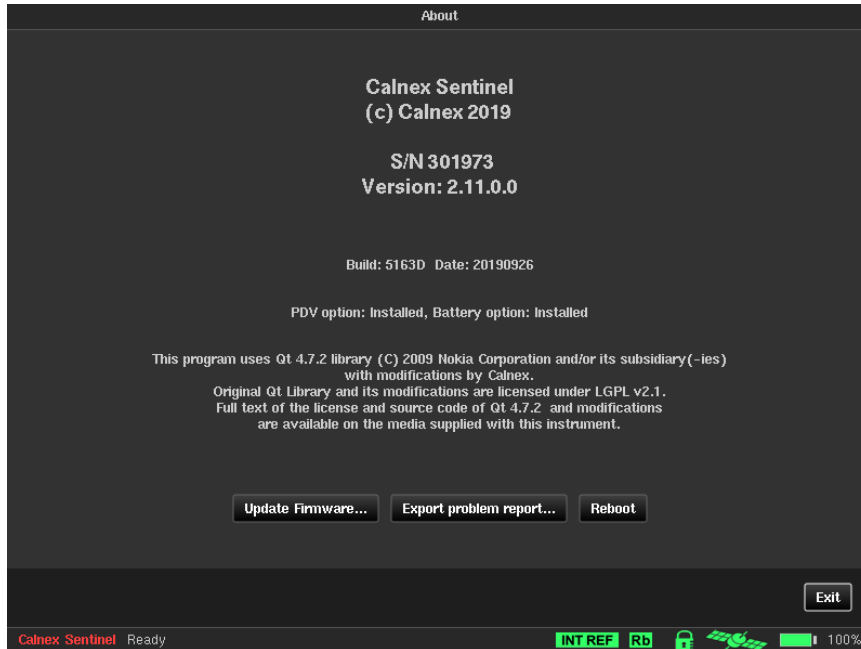
This screen identifies the firmware installed in the instrument, and displays the **Update firmware**… button. Press this button, then follow the instructions given on screen to locate the update source file and run the update. The update source file name should be in the following format **sentinel_fw_Rx.y.z.tar**.

Note: The update file is an archive file but the contents should not be extracted as Sentinel will not be able to install the firmware from the extracted files.

Note: The instrument is rebooted after firmware update has completed.

> **WARNING**:
>
> Never interrupt a firmware update operation.

Appendix A: Signal Types

The following signal types are available, subject to firmware update:

1 PPS	25MHz (Ethernet)	1.544MHz (T1, Clock)	155.52MHz (STM-1)
125MHz (Ethernet)	5MHz	64kbit/s (E0)	44.736Mbit/s (T3)
155MHz (STM-1)	64kHz (E0, Clock)	2.048Mbit/s (E1)	10MHz
156.25MHz	8kHz (E0, Clock)	34.368Mbit/s (E3)	51.840Mbit/s (STM-0)
162.25MHz	2.048MHz (E1, Clock)	1.544Mbit/s (T1)	155.52Mbit/s (STM-1)

Appendix B: Built-in Masks

The following masks are available, subject to Firmware update:

ANSI DS1 Interface	G.824 T1 PRC Interface
ANSI DS1 Transient	G.824 T1 Traffic Interface 1544
ANSI OC-N Interface	G.8261.1 Case 3
ANSI OC-N Transient	G.8261 E1 CES Case1
ANSI PRS Interface	G.8261 E1 CES Case2
ANSI SMC Holdover	G.8261 Enhanced SyncE Wander Limit (ePRTC)
ETSI PDH Interface	G.8261 T1 CES Case1
ETSI PRC Interface	G.8261 Wander Limit EEC Opt1
ETSI SEC Interface	G.8261 Wander Limit EEC Opt2
ETSI SSU Interface	G.8261 Amd.2 Short Chain Network Limits (Fig 19)
ETSI Wander Gen PRC	G.8261.1 FPP Network Limit
ETSI Wander Gen SEC	G.8262 Wander Gen EEC Opt1
ETSI Wander Gen SSU	G.8262 Wander Gen EEC Opt2
G.812 Type II-III Wander Gen	G.8262 Wander Transfer EEC Opt2
G.812 Type I Wander Gen	G.8262 Wander Switch EEC-2
G.813 Holdover SEC opt2	G.8271.1 Max|2wayTE| LPF
G.813 Switch SEC opt2	G.8271.1 Max|TE|
G.813 Transfer SEC Opt2	G.8271.1 dTE MTIE
G.813 Wander Gen SEC Opt1	G.8271.1 dTE Pk-Pk HPF
G.813 Wander Gen SEC Opt2	G.8271.2 APTS Pk-Pk Network Limit
G.823 E1 PDH Sync Interface	G.8271.2 PTS Network Limit
G.823 E1 PRC Interface	G.8272 Wander Gen PRTC
G.823 E1 SEC Interface	MAFE 16ppb
G.823 E1 SSU Interface	MAFE NSN HRM 1
G.823 E1 Traffic Interface 2048	MAFE NSN HRM 2
G.824 T1 PDH Ref Interface	PDV Distribution
G.824 T1 PDH Ref Interface SEC Opt2	

Appendix C: Reference Material

For additional information (test procedures) for Sentinel refer to the following:

- Field Test Plan for Frequency Synchronisation using PTP[2]
- Field Test Plan for Frequency Synchronisation using NTP[3]
- Synchronization Test Plan for TDD-LTE[4]
- Making OTA Sync Measurements with Calnex Sentinel[5]

---

[2] Calnex Document CX5018
[3] Calnex Document CX5017
[4] Calnex Document CX5019
[5] Calnex Document CX5027

Appendix D: List of Sentinel Log Messages

The following table details messages that will appear on the **Log** page of the **System** menu, their meaning and whether any troubleshooting actions are required.

System Events		
Log Text	**Explanation**	**Action Required**
Started up	System start up	None
Powering system down	System power down	None
Configuration data was restored from backup as errors were detected	Configuration integrity check failed, data restored from last good settings	Ensure that Sentinel power down procedure is followed.
Last power down was unexpected	System shutdown procedure was not followed	Ensure that Sentinel power down procedure is followed.
Rubidium Events		
Log Text	**Explanation**	**Action Required**
Entering transport mode	Battery backed up transport mode was selected during shutdown	None
Warming Up	Initial Rubidium state when Sentinel is powered on from cold. Takes ~10mins to warm up	Error condition only if Rubidium remains in this state constantly. In this case export a problem report and power cycle Sentinel.
Hold-Over	Rubidium will enter Hold-Over when the **Internal Reference Disciplining Source** is set to *Ext 1 PPS* in the **Measurement->Timebase** page and there is no External 1 PPS input present	None
Manual Hold-Over	Rubidium is placed in Manual Hold-Over by the software, when starting a measurement and *Not during measurement* is selected as the **Internal Reference Disciplining Mode** or *Never* is selected as the disciplining mode in the **Measurement->Timebase** page or when the **Internal Reference Disciplining source** is *GNSS* and GNSS is in the unlocked state	None
Disciplining	Rubidium is disciplining to a valid 1 PPS source (External 1 PPS or GNSS)	None
Initialising Rubidium	Rubidium phase information was not maintained during last power down.	None
No initialisation required	Rubidium phase information was maintained during last power down.	None. Either AC cord was left connected or transport mode was successful.

Measurement Events

Log Text	Explanation	Action Required
Signal absent on channel *x*	Clock module loss of Signal. Indicated on channel widget by the status LEDs	Clock signal is not within expected range or not driven. Ensure a **Signal Check** was executed prior to starting measurement. Verify signal integrity on an oscilloscope or by connecting to a different measurement channel on Sentinel.
Signal momentarily disappeared on channel X	Clock module has briefly had a loss of signal. Indicated by the status of the channel LED on widget	None
Link lost on channel Y	Ethernet link lost on channel	Check network connection and **Channel X->Ethernet** settings on Sentinel
Link restored on channel Y	Ethernet link restored on channel	None
Sync message flow on channel Y: absent	PTP Sync messages are absent. Messages for follow-up, delay request and delay response can also be generated. Indicated on channel widget by change of state for LED	Check PTP master is generating messages and verify **Channel X->PTP** settings on Sentinel match the PTP master settings
FwUp message flow on channel Y: not tracked	No follow-up message in channel flow i.e. 1-step. Can also apply to sync, delay request and delay response messages in monitor mode as only one direction is monitored on each channel	None
Sync message flow on channel Y: momentarily disappeared	Sync message has momentarily disappeared. Messages for follow-up, delay request and delay response can also be generated. Indicated on channel widget by change of state for LED	Check network and PTP master integrity

In the above messages,

X refers to a clock channel i.e. A or B if module is fitted in slot A-B, C or D if fitted in slot C-D or E or F if fitted in slot E-F.

Y refers to a packet based channel i.e. C if fitted in slot C-D or E if fitted in slot E-F

Attempting measurement restart	Measurement start after power failure; only applicable if Auto-restart is ON	None
Measurement started	Measurement started	None
Measurement finished	Measurement finished	None
Measurement failed	Failed to start PDV measurement	Export problem report and power cycle Sentinel.
External Reference lost	External reference is selected as measurement time-base but no clock is detected	Verify reference is connected to the **Freq in** connector on Sentinel and is generating 1, 5

		or 10MHz. Check signal integrity on oscilloscope.
Internal Reference failure	*Internal* or *Auto* is selected as **Timebase Reference** in **Measurement->Timebase** page and Rubidium is not locked or is Warming Up	Wait until Rubidium has warmed up and has stabilised. Setting **Measurement Start Behaviour** to *Wait till Timebase Reference is ready* in the **Measurement->Timebase** settings page will delay the measurement start until this occurs. If Rubidium status icon is red or does not leave the warming up state, export a problem report and power cycle Sentinel.

GNSS Events

Log Text	Explanation	Action Required
GNSS locked	Sentinel is locked to at least 3 satellites, the survey status is 100% and the antenna status is not shorted	None
GNSS unlocked	Indicates that Sentinel was previously locked to GNSS and has now lost lock. This usually means that Sentinel is no longer locked to 3 satellites	If a GNSS antenna is connected, the number of visible satellites and their strength can be checked on the **Settings->GNSS** page

Hardware Events

Log Text	Explanation	Action Required
Communication with battery lost	Unable to read statistics from battery module	Indicated by 🔲 battery status icon. If problem does not clear, export a problem report and power cycle Sentinel.
Communication with battery restored	Successful read from battery module after previous failure	None. Battery communication error has cleared.
Failed to set up Battery for Standby	Cannot set battery to correct settings for entering transport mode.	Export a problem report and power cycle Sentinel.
High battery temperature detected, charging paused	Battery charging is limited to a battery temperature 0°C ≤ T ≤ 45°C. This message shows that the battery temperature is outside this range.	None. If Sentinel is operating within its specified ambient range of 0°C ≤ T ≤ 40°C the battery temperature will return to within the charging range.
High battery temperature cleared	Battery temperature has returned to within the charging range (0°C ≤ T ≤ 45°C).	None.
Battery voltage low after charging, Battery Fault	Battery has failed to maintain its charge, indicating a battery fault.	Indicated by 🔲 battery status icon. Export a problem report and power cycle Sentinel. If problem does not clear contact Calnex support.
Battery current low when charging, Battery Fault	Battery has failed to accept a charging current, indicating a battery fault.	Indicated by 🔲 battery status icon. Export a problem report and power cycle Sentinel. If

		problem does not clear contact Calnex support.
Battery charge time excessive, Battery Fault	Battery has failed to charge within the specified time limit, indicating a battery fault.	Indicated by ▯❗▯ battery status icon. Export a problem report and shutdown Sentinel. Contact Calnex support.
Battery charging enabled	Charging has commenced	None.
Battery fully charged	Battery has reached full capacity, charging is disabled.	None.
Temperature sensors reading failed	Unable to read from processor board temperature sensors	Check cooling fan on side of Sentinel is spinning. If fan is not spinning or the problem does not clear, export a problem report and power cycle Sentinel.
Temperature sensor readings restored	Successful read from processor board temperature sensors after previous failure	None. Sensor communication error has cleared.
Other Events		
Log Text	**Explanation**	**Action Required**
Enable calibration options	Calibration page enabled	None

A problem report can be generated by pressing the **Export problem report...** button on the **About** page of the **System** menu and saving to internal memory or an external USB drive. If after power cycling Sentinel, the problem does not clear then the problem report should be forwarded to Calnex along with a description of the fault and a block diagram of the test setup.