



ERT USER MANUAL for VIPER – SMART GATEWAY



TABLE OF CONTENTS

OVERVIEW	3
SMART GATEWAY BENEFITS	3
OTHER DIFFERENCES	3
SMART GATEWAY HARDWARE INFORMATION	4
EXTERNAL PORTS.....	4
ANTENNAE AND SIM CARDS	5
Interpreting LEDs on the Gateway:	5
GATEWAY NAME AND POWER SWITCH.....	6
INTERNAL EQUIPMENT.....	7
USING THE SMART GATEWAY	8
Logging in to the Internal Laptop	8
Windows Remote Desktop Connection from within the EPAERT1 WiFi Network	8
Windows Remote Desktop Connection via the Internet	8
External Monitor, Keyboard and Mouse	9
Internal Touch Screen Display – Last Resort	9
Troubleshooting the Internal Laptop (Motherboard)	10
Troubleshooting Remote Desktop Connection to the Smart Gateway	11
Logging in to the Cradlepoint Router.....	13
Quick Reference Sheet for Accessing the Smart Gateway Laptop & Cradlepoint	13
Section 1 – Using the External Ports on the Smart Gateway.....	14
Using COMx (Traditional LINC Cable Port).....	14
Troubleshooting Serial (COM Port) Connections	18
Using the USB Ports to Connect Instruments – Serial to USB (i.e., DustTraks).....	19
Using the Ethernet (RJ45) Port (SPM Flex)	20
Section 2 – Smart Gateway MeterApp.....	21
Smart Gateway Sensors	21
Additional Signal and SINR Information	22
Troubleshooting the Smart Gateway MeterApp	22
Adding the Smart Gateway MeterApp to a Survey Controller Run	24
Section 3 – Smart Gateway WiFi and Security	27
Disabling/Enabling WiFi	27
Changing WiFi Network Name (SSID) in the Gateway.....	29
Disabling WiFi Security	31
Enabling WiFi Security	32
Section 4 – Cradlepoint GPS Settings.....	33
Overview	33
Troubleshooting the Cradlepoint GPS Settings	33
Section 5 – Internet Sources	36
Internal SIM Card	36
External WiFi Source.....	37
Ethernet Connection – Hard Wired	37
Troubleshooting WiFi and Ethernet internet sources	38
Section 6 – Directly connecting a RAE Host to the Smart Gateway.....	40
Overview	40
Install ProRAE Guardian Software	40
Attaching ProRAE Host to the Smart Gateway	40
Configuring ProRAE Guardian	41
Configuring Viper Survey Controller	44
Configuring PRG2CAP.....	44
Creating a Survey Controller Run with ProRAE Guardian Instruments	45
Tips, Tricks and Troubleshooting	45



OVERVIEW

The Smart Gateway can be used as a traditional gateway following the normal Viper user guide procedures or you can choose to transition tasks where you previously used a laptop or a Virtual Machine to now directly run on the gateway. There is also an opportunity to connect instruments directly, eliminating the need for LINC's.

SMART GATEWAY BENEFITS

- Longer Battery Life (15 hours)
- Internal Laptop – Run Survey Controller Locally, eliminating need for VM & potential to run other data acquisition software in parallel (ProRAE Guardian)
- MeterApp To Monitor Battery Life, Gateway Temperature, Disk Space & RAM
- External serial Port can be used to directly connect an instrument without a LINC
- Connect additional instruments via USB/Serial connections and virtual com ports
- Auto-Detects SIM Card Provider and Selects Appropriate Firmware
- Built-In GPS – Coordinates Distributed to All Attached Instruments

OTHER DIFFERENCES

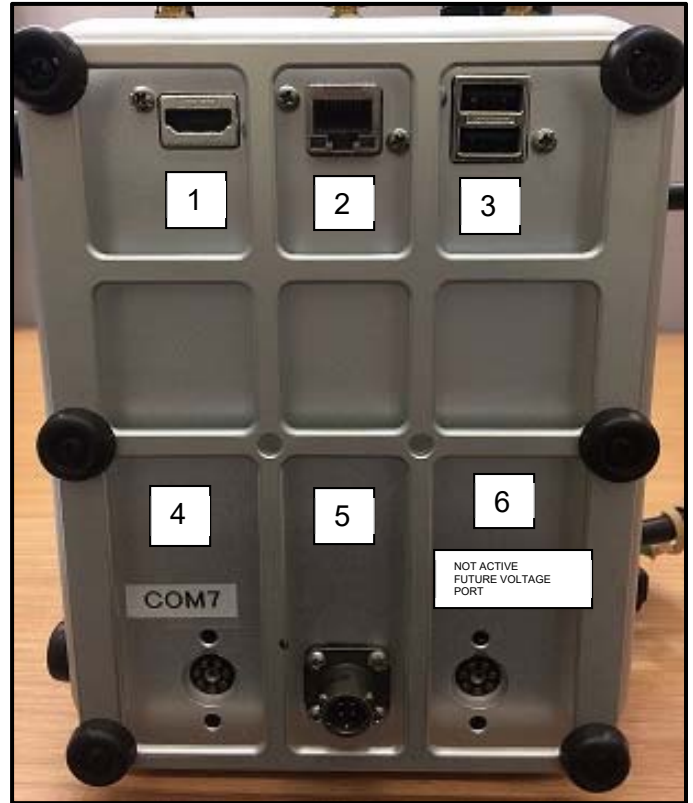
- No Mesh Radio – (external add-on module under development by Safe Environmental Engineering)
- Ability To Use Multiple Internet Sources with Private IP Addresses and Still Push Data to Deployment Manager (Technically Advanced Feature).
- Potential for Bluetooth Instrument Connections



SMART GATEWAY HARDWARE INFORMATION

EXTERNAL PORTS

1. **HDMI Monitor Port**
Connect an external monitor to the internal laptop.
2. **RJ45 (Ethernet) Port**
Can be configured as LAN or WAN
 - a. LAN – Connect instruments with Ethernet Outputs (i.e., SPM Flex)
 - b. WAN – Obtain internet access from an external network via hardwired Ethernet (home/work internet connection).
3. **USB Ports**
Can connect external keyboard and mouse to to the internal laptop or can be used to connect Serial (RS-232) instruments.
4. **Traditional LINC Cable port (Gen 3 and Above)**
Connect an instrument using a traditional LINC cable. The MeterApp will be configured for a Serial connection. The port label will indicate the Com Port number assigned to that connection.
5. **Smart Gateway External Power Connection**
Connect the power cord to run the gateway with power or to charge the internal battery. The internal battery lasts 15 hours with the internal monitor off. Battery strength can be monitored via the Smart Gateway MeterApp.
6. **Port is currently not active**
It is expected that in the future, this port will be used for connecting instruments that output data via voltage.





ANTENNAE AND SIM CARDS



To insert the SIM card, remove the two screws on the SIM door, install the SIM in either slot, put the **screws back in**. (Gateway **will not** boot up if the SIM port screws are out)

FIRST TIME INSTALLATION: When installing your SIM card for the first time, leave the gateway powered on for several hours in order to allow the SIM card to obtain its IP Address and register itself on the internet.

Interpreting LEDs on the Gateway:

LEDS	
INDICATOR	BEHAVIOR
	POWER The Cradlepoint IBR900/IBR950 must be powered using an approved 9-33 V DC power source. <ul style="list-style-type: none">Green = Powered ON.No Light = Not receiving power. Check the power switch and the power source connection.
	WIFI BROADCAST Indicates WiFi activity (IBR900 only). <ul style="list-style-type: none">Green = On and operating normally.Yellow = Attention.
	GPS Indicates the status of GPS connection. <ul style="list-style-type: none">Blue = GPS locked.Blinking Blue = Obtaining lock.No Light = Off/no lock.
	INTEGRATED MODEM Indicates information about the integrated modem. <ul style="list-style-type: none">Green = Modem has established an active connection.Blinking Green = Modem is connecting.Amber = Modem is not active.Blinking Amber = Data connection error. No modem connection possible.Blinking Red = Modem is in the process of resetting.No Light = Modem not connected.
	SIGNAL STRENGTH Blue LED bars indicate the active modem's signal strength. <ul style="list-style-type: none">4 Solid Bars = Strongest signal.1 Blinking Bar = Weakest signal. (A blinking bar indicates half of a bar.)
Other	ADDITIONAL LED INDICATIONS <ul style="list-style-type: none">Several different LEDs blink when the factory reset button is detected.Two of the modem LEDs blink red in unison for 10 seconds when there is an error during NCOS upgrade.Dock Ethernet LEDs: only right LED will light up and/or blink with data.When an external USB modem is plugged in, only the Signal Strength LEDs will light up.



GATEWAY NAME AND POWER SWITCH

Gateway Name:

The Gateway Name is labeled on the side of the gateway with the handle. The gateway name is EPAERTXXX where X represents a unique number.

Power Button:

Depending on the build of your Smart Gateway, the power switch can be either a toggle switch or a push button. The toggle switch is convenient in that it allows the gateway to remain on when switching between shore power and battery. However, it is easy to accidentally turn the switch on/off when picking up the gateway or when packing the gateway in a case. If it is necessary to ship the Gateway, it is recommended that a piece of tape be applied over the switch to keep it in the off position during shipping.

Motherboard Reset Port:

There is a port covered by a screw that allows for a hard-reset of the gateway motherboard. See the troubleshooting section later in this manual for additional details.





INTERNAL EQUIPMENT

**The photo here is for illustration
Purposes only. There is typically NO
NEED to open a Smart Gateway**

1. Cradlepoint IBR900LP6 Router

<https://cradlepoint.com/products/cor-ibr900-series>

- Auto-detects SIM provider and selects appropriate Firmware
- Can obtain internet access via Ethernet and WiFi in addition to Cellular signals
- Obtains and provides GPS for instruments that are directly connected to the gateway
- Broadcasts WiFi (EPAERT1)

2. Touch-Screen Monitor & Gateway Battery

- Access to the internal laptop if Remote Desktop Connection and External Monitor/Keyboard/Mouse are not working. Behind the touch-screen is the gateway's battery (black).



1

2

3. Internal Computer Info

- Windows 10 – 64 Bit 4 GB RAM
- **64 GB Hard Drive (40 GB Free)**

View basic information about your computer

Windows edition

Windows 10 Enterprise 2016 LTSC

© 2016 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Atom(TM) x5-Z8350 CPU @ 1.44GHz 1.44 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: Pen and Touch Support with 10 Touch Points



USING THE SMART GATEWAY

The Smart Gateway contains both a Cradlepoint Router and a laptop. Login to the laptop to run Viper Survey Controller locally. Login to the Cradlepoint Router to determine internet connection status and to change internet configuration.

Logging in to the Internal Laptop

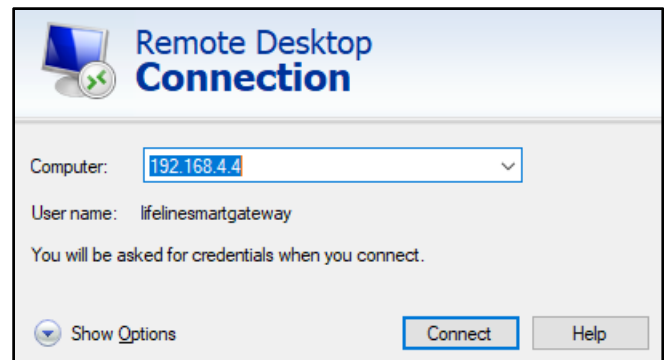
The internal laptop in the Smart Gateway serves a few purposes. First, the laptop acts as its own 'virtual machine'. Viper Survey Controller can be configured and managed on the Smart Gateway, and as long as a SIM card is installed, Survey Controller can be managed remotely – similar to an ERT-provided Virtual Machine. There is also a 'Smart Gateway MeterApp' that runs on the internal laptop. This 'MeterApp' monitors the performance of the Smart Gateway, including metrics such as temperature, battery life, disk space, etc.

The recommended option for logging in to the Smart Gateway's internal laptop is through Windows Remote Desktop Connection from another laptop or tablet.

Windows Remote Desktop Connection from within the EPAERT1 WiFi Network

The steps below illustrate how to access the Smart Gateway laptop from the EPAERT1 WiFi Network

- Power on the Smart Gateway. Wait at least 5 minutes before trying to login
- Connect a laptop (or mobile device capable of running Remote Desktop Connection) to the EPAERT1 WiFi network
- Run Windows Remote Desktop Connection
- Computer Name = 192.168.4.4
- Username = \LifelineSmartGateway
- Click the Connect button
- Contact ertsupport@epa.gov to obtain the password
- Enter the password obtained. Click OK.
- Click Yes past the security warning screen
- The Smart Gateway Windows 10 screen will be displayed in the Remote Desktop window. Operate the Smart Gateway laptop as you would any other laptop.



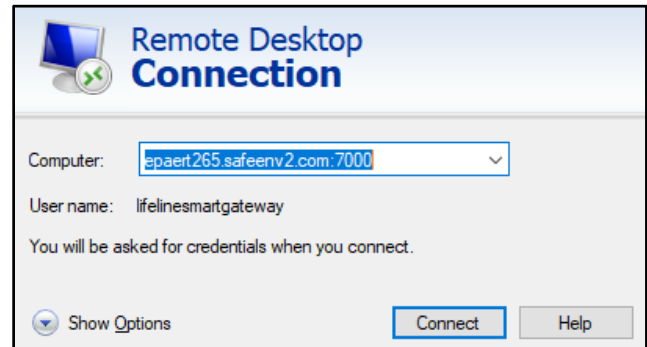
Windows Remote Desktop Connection via the Internet

The steps below illustrate how to access the Smart Gateway laptop using Windows Remote Desktop Connection from a laptop that is not on the EPAERT1 WiFi network. This method requires that the Smart Gateway has a SIM card installed and the SIM card is using a Public IP Address. If you are unfamiliar with determining the IP Address of the SIM card installed, refer to Section 10/Step 5 of the ERT Viper User Guide or contact ERT Support for assistance.

- Power on the Smart Gateway. Wait at least 5 minutes before trying to login
- Gateway SIM must have a public IP Address



- Using an internet-connected laptop or mobile device (not on the EPAERT1 WiFi network), run Windows Remote Desktop Connection
- Computer Name = the EXTERNAL gateway address followed by :7000 (i.e., EPAERT265.SAFEENV2.COM:7000)
- Username = \Lifeline SmartGateway
- Contact ertsupport@epa.gov to obtain the password
- Enter the password obtained. Click OK
- Click Yes past the security warning screen
- The Smart Gateway Windows 10 screen will be displayed in the Remote Desktop window. Operate the Smart Gateway laptop as you would any other laptop.



External Monitor, Keyboard and Mouse

- Connect an external HDMI monitor to the HDMI port on the back of the Smart Gateway
- Connect a keyboard and mouse to the USB ports on the back of the Smart Gateway
- Power on the Smart Gateway
- The Smart Gateway Windows 10 screen will be displayed on the external HDMI monitor

Internal Touch Screen Display – Last Resort

- Remove the 7 torx screws holding the Gateway closed
- Open the Gateway
- The monitor is a touch screen with a virtual keyboard
- If the monitor doesn't wake-up when you touch the screen, use the 'PC Wakeup' button located inside the Gateway below the Cradlepoint



router.





Troubleshooting the Internal Laptop (Motherboard)

In some instances, the internal laptop doesn't boot up at all. There are two (2) options for resetting the laptop.

Option 1:

- Remove the 7 torx screws holding the Gateway closed
- Open the Gateway and power it up
- Depress the 'PC Wakeup' button for 30 seconds
- Release the 'PC Wakeup' button and power the gateway off and on



Location of Torx Screws

Option 2:

- With the Smart Gateway powered up, back out the torx set screw (circled below in red). After removing the screw, insert a device that is long enough to depress the internal reset button for 30 seconds. The reset button is small and will only depress a tiny bit. After 30 seconds, stop depressing the reset button and remove the device being used. **NOTE:** The torx wrench from option 1 above can be used to reset the laptop.
- Power the Smart Gateway off and on.



NOTE: The port may not directly line-up with the motherboard reset switch. Contact ERT Support if you are not successful with Option 1 and/or 2.



Troubleshooting Remote Desktop Connection to the Smart Gateway

1. Can't connect via Remote Desktop Connection from within the EPAERT1 WiFi network:

If you can't use Remote Desktop Connection locally to access the Smart Gateway Laptop from a computer or mobile device connected to the EPAERT1 WiFi network, you have two options:

- Connect an external (HDMI) monitor, USB keyboard and USB mouse to the ports on the back of the Smart Gateway
- Open the Gateway and use the touch screen monitor.

If you are able to connect to the Internal laptop using one of the two options above, follow the steps below to verify that the internal Smart Gateway Laptop has the correct IP Address (192.168.4.4). If you cannot access the Smart Gateway at all, please contact ERTSupport.

Check the IP Address of the Smart Gateway Laptop:

There is an IP Address Reservation in the Cradlepoint which is supposed to maintain the IP Address of the laptop. By default, the laptop IP Address should be 192.168.4.4. The steps below illustrate how to check the IP Address of the internal Smart Gateway Laptop.

On the Smart Gateway Laptop:

To see the Smart Gateway Laptop's IP Address

- Click the search icon and type CMD and press enter to **open a command prompt**
- Type '**IPCONFIG /all**' and press enter
- Look under the Ethernet Adapter section for the **Ipv4 Address** and make note of what that says
- Also, under the Ethernet Adapter section, make note of the **Physical Address**

```
Ethernet adapter Ethernet 5:  
Connection-specific DNS Suffix . : local.tld  
Description . . . . . : Realtek USB FE Family Controller #5  
Physical Address. . . . . : 00-E0-4C-36-3D-28  
Pnp Device ID . . . . . : Net  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::18a7:75da:af50:beb7%3(Preferred)  
IPv4 Address. . . . . : 192.168.4.70 (Preferred)  
Subnet Mask . . . . . : 255.255.0.0  
Lease Obtained. . . . . : Wednesday, August 29, 2018 8:05:20 AM  
Lease Expires . . . . . : Wednesday, August 29, 2018 8:05:20 PM  
Default Gateway . . . . . : 192.168.4.1  
DHCP Server . . . . . : 192.168.4.1  
DHCPv6 IAID . . . . . : 50389068  
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-1B-4A-3F-00-E0-4C-36-00-01  
DNS Servers . . . . . : 192.168.4.1  
NetBIOS over Tcpip. . . . . : Enabled
```

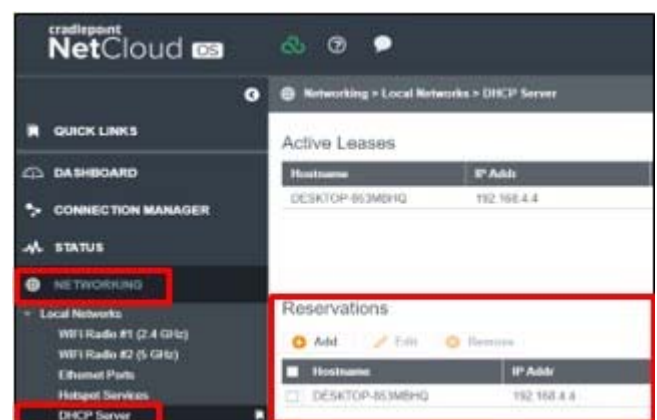
Follow the steps in this guide to correct the IP Address if it is NOT 192.168.4.4:

https://response.epa.gov/sites/5033/files/Correcting_A_Smart_Gateway_Laptop_IP_Address.pdf

Check the IP Address Reservation on the Smart Gateway Cradlepoint:

To see the IP Reservation:

- On the Smart Gateway Laptop, open a browser and type 192.168.4.1 to **access the Cradlepoint Router**
- Contact ertsupport@epa.gov to obtain the password
- Navigate to '**Networking**' – '**Local Networks**' – '**DHCP Server**'
- There should be a Reservation for the Smart Gateway Laptop. The reservation's **hardware address** should **match** the Smart Gateway Laptop's physical address and **the IP Address should match** the Smart Gateway's IP Address





2. Can't connect via Remote Desktop Connection over the internet:

and you can't use Remote Desktop Connection to access the internal laptop on the Smart Gateway, check that the "Remote Desktop Connection Port Forwarding Rule" is properly configured on the CRADLEPOINT router.

The steps below illustrate how to check the Port Forward Rule in the Cradlepoint.

Option 1 Login to the Smart Gateway Cradlepoint from within the EPAERT1 Wifi network:

- Connect a laptop or mobile device to the EPAERT1 network
- Open a browser and type 192.168.4.1 to access the Cradlepoint Router
- Contact ertsupport@epa.gov to obtain the password
- Follow steps for checking the Cradlepoint port forward rule below

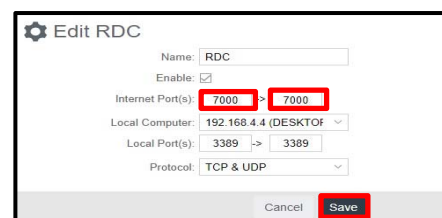
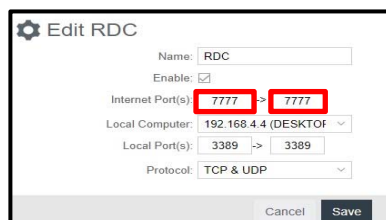
OR

Option 2 Login to the Smart Gateway Cradlepoint over the internet:

- To access the Cradlepoint Gateway over the internet, the Smart Gateway must have internet access (working SIM Card, etc)
- From a laptop or mobile device, open a browser and type EPAERTxxx.safeenv2.com:8080 to access the Cradlepoint Router
- Contact ertsupport@epa.gov to obtain the password
- Follow steps for checking the Cradlepoint port forward rule below

Check the Cradlepoint Port Forward Rule

- Navigate to 'Security – Port Forward & Proxy'
- The Internet Port should be '7000'. If it is not, edit the Internet Port and change it. Click Save.





Logging in to the Cradlepoint Router

The steps to login to the Cradlepoint Router on a Smart Gateway are the same as a traditional gateway. See Section 10/Step 4 of the ERT Viper User guide for additional details.

Quick Reference Sheet for Accessing the Smart Gateway Laptop & Cradlepoint

Accessing the Smart Gateway's Internal Laptop	Accessing the Cradlepoint Router
<p>Option 1a: Windows Remote Desktop Connection via EPAERT1 WiFi Network</p> <ul style="list-style-type: none">Connect a laptop or mobile device capable of running Remote Desktop Connection to EPAERT1Run Windows Remote Desktop ConnectionComputer Name = 192.168.4.4Username = \LifelineSmartGatewayContact ertsupport@epa.gov to obtain the password. Enter password and Click OKClick Yes past the security warning screen <p>Option 1b: Windows Remote Desktop Connection via the Internet</p> <ul style="list-style-type: none">Must be using an internet source with a public IP Address in the Gateway (Cradlepoint)Using an internet-connected laptop or mobile device capable of running Remote Desktop Connection software, run Windows Remote Desktop ConnectionComputer Name = The EXTERNAL gateway address followed by :7000. i.e., EPAERT231.SAFEENV2.COM:7000Username = \LifelineSmartGatewayContact ertsupport@epa.gov to obtain the password. Enter password and Click OK.Click Yes past the security warning screen	<p>Option 1: Via the EPAERT1 WiFi Network</p> <ul style="list-style-type: none">Connect a laptop or mobile device to the EPAERT1 WiFi networkOpen a browser and type 192.168.4.1Contact ertsupport@epa.gov to obtain the password
<p>Option 2: External Monitor, Keyboard and Mouse</p> <ul style="list-style-type: none">Connect an external HDMI monitor to the HDMI port on the back of the Smart GatewayConnect a keyboard and mouse to the USB ports on the back of the Smart Gateway	<p>Option 2: From the Internal Smart Gateway Laptop</p> <ul style="list-style-type: none">Open a browser and type 192.168.4.1Contact ertsupport@epa.gov to obtain the password
<p>Option 3: Open the Gateway</p> <ul style="list-style-type: none">Remove the screws holding the Gateway closedThe monitor is a touch screen with a virtual keyboard	<p>Option 3: From an outside Internet connection</p> <ul style="list-style-type: none">Must be using an internet source with a Public IP address in the Gateway (Cradlepoint)Open a browser and type the Smart Gateway's external DNS Name labeled on the outside of the Gateway (EPAERT231.SAFEENV2.COM:8080)Contact ertsupport@epa.gov to obtain the password



Section 1 – Using the External Ports on the Smart Gateway

The Smart Gateway has four (4) external ports for connecting instruments. There is one (1) port to which a traditional gateway LINC cable can be attached (COMx), an Ethernet Port and two (2) USB ports which can be configured to communicate with RS232 Serial connections. There is an additional port for future expansion which could potentially be used for instruments that output voltage, but the port is currently not functional. Refer to the 'Smart Gateway Hardware Information' section of this document for additional details.

The external LINC port on the Gateway will be assigned a COM port number that matches the setting in Windows on the Laptop inside the Gateway. The LINC numbers that are added to Survey Controller will represent the COM port to which the instrument is connected. It is recommended that a standard naming convention be used for these custom LINC numbers. For consistency, keep the name convention with the 1000 series and include the COM Port number for the connection. For example, when connecting a cable to a port assigned COM5, a LINC will be added to the equipment inventory in Survey Controller with a number of 1005. If connecting an instrument to a port assigned COM6, the LINC number in Survey Controller would be 1006, and so on. The COM port should be identified using Windows Device Manager for each instrument attached via USB prior to adding to Survey Controller. NOTE – An SPM Flex will NOT be assigned a COM port number since it connects to the Ethernet port on the Smart Gateway. See the SPM Flex section for additional details.

Using COMx (Traditional LINC Cable Port)

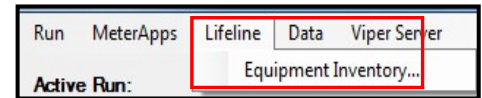
When using the traditional LINC cable port on the Gateway (Gen 3 and above), note the COM port number labeled on the outside of the Gateway. Substitute that number for the COMx reference in the steps below.



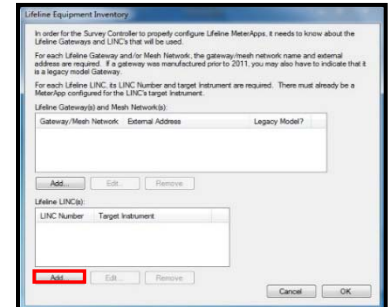
1. **Login to the Gateway's internal laptop.** Refer to the 'Accessing the Smart Gateway' table above for login options.
2. Add a custom LINC number for COMs to Survey Controller. For illustrative purposes, COM5 will be used.



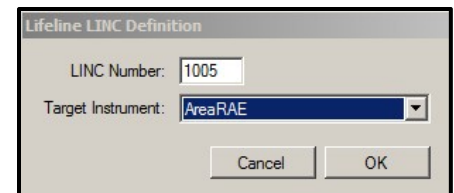
- Select 'Lifeline Equipment Inventory' from the Survey Controller Menu



- Click the **Add** button immediately under the **Lifeline LINC(s)** section



- Enter a LINC number of 100x (the COM port number labeled on the outside of the Gateway). This LINC number will be used for any instrument connected to the COMx traditional LINC cable port on the Gateway. See the overview above for additional information on assigning custom LINC numbers.



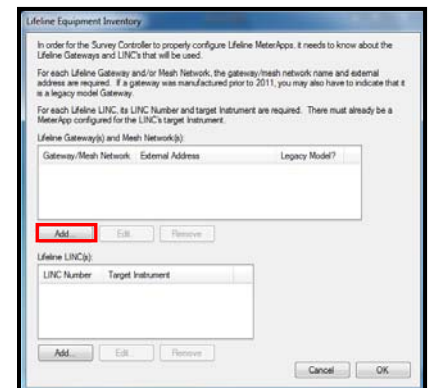
- Select which instrument is connected to the port. If a different instrument will be connected to that port at a later date, simply modify the 1005 'LINC' number and select the appropriate instrument. Stated otherwise, LINC 1005 will always represent the COM5 port on the Smart Gateway.

- Click OK.

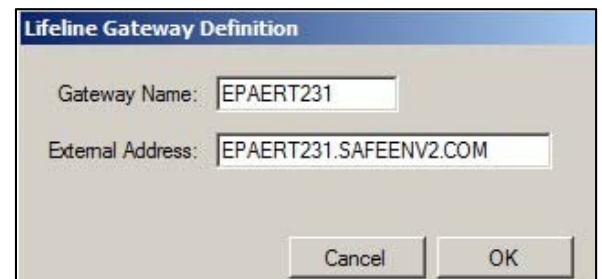
3. Add the Smart Gateway to Survey Controller

The process of adding a Smart Gateway is the same as adding a traditional Gateway.

- Open VIPER Survey Controller. From the menu, select **Lifeline>Equipment Inventory**
- Under the Lifeline Gateway(s) and Mesh Network(s) dialog box, click **Add**.



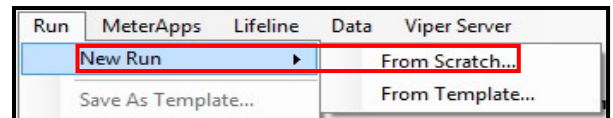
- Enter the Gateway name. The Gateway name will be affixed to the outside of the Gateway case.
- Enter the External address of the Gateway.
NOTE: The external address is always the Gateway Name followed by .safeenv2.com.
- Click OK when finished.





4. Creating a Run on the Internal Smart Gateway Laptop
The instructions below illustrate an instrument connected to the traditional LINC cable port on the Smart Gateway that is assigned a COM5 port number.

- Run Survey Controller on the internal Gateway laptop
- From the menu, select **Run>New Run>From Scratch**
- Click **Next** on the Viper Run Configuration Wizard
- Complete the Run Description information
- Run Name/ID – Include the **Region** and **name** of the site/response exercise
- The run description is required and could include the instruments involved in the run, as well as the scope of work
- The Location Description is optional, but helpful for further identification of the run
- Click **Next**



Run Configuration Wizard

In the space below, please provide a unique name for the Run, and a brief description of the run.

The Run Description might include the purpose of the survey, and/or any details that may help interpret the recorded data.

The Location Description is optional, but might include information that would help identify incorrectly recorded coordinates. As with the Run Description, this information might help interpret the recorded data.

Run Name/ID: R02 Westville Warehouse 10-20-2014

Run Description: Conducted PM10 Air Monitoring Using DataRams at 3 fixed perimeter location

Location Description (optional): Actions level was established at 150 ug/m3

Back Cancel **Next**

- Click **Add** on the LINC Configuration screen

Using the "Add...", "Edit...", and "Remove" buttons below, specify the configuration of each LINC to be used in this Run.

Along with each LINC's name (i.e. ".34"), you'll also need to know which Gateway it is connecting to, and whether to use the local WiFi or global Cellular network to communicate with the LINC.

LINC Configuration:

LINC Name	Instrument	Gateway	Comm Mode
-----------	------------	---------	-----------

Add... Edit... Remove

Back Cancel Next

- From the Gateway dropdown menu, **select the Smart Gateway** to which the instrument is connected. If the gateway does not appear in the list, it must first be added to the Lifeline Equipment Inventory
- **Select the custom LINC** that represents the COM port to which the instrument is attached. LINC 1005 is selected for illustrative purposes. If the LINC does not appear in the list, it must first be added to the Lifeline Equipment Inventory
- Select a **Comm Mode of WiFi** since the run is being configured on the version on Survey Controller running on the Smart Gateway

LINC Configuration

LINC Type:

☒ Lifeline ☐ Generic CAP Stream

Gateway: EPAERT231

LINC: .1005 - AreaRAE

Comm Mode: WiFi

Cancel OK

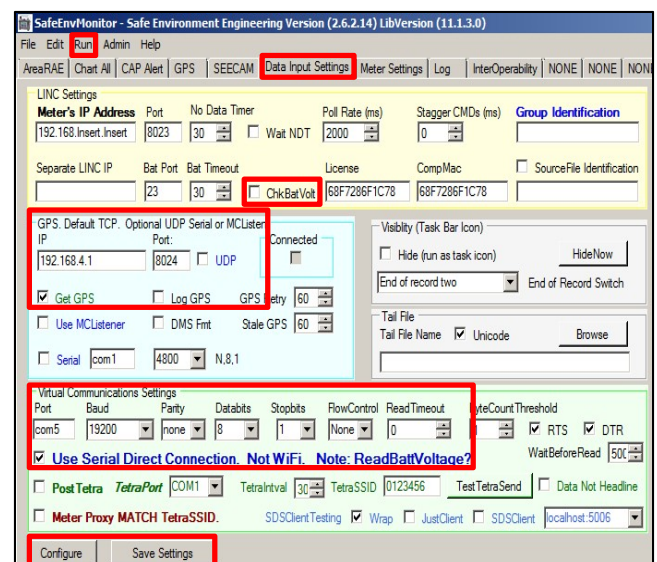
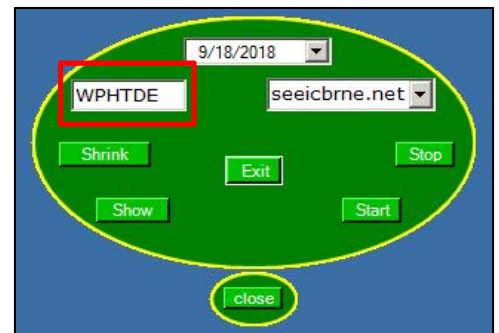


- Continue through the run configuration screens. Reading intervals can be configured and fixed coordinates can be entered; however, the Smart Gateway will provide coordinates if none are entered. Click **Finish** on the Run Configuration Complete window.
- Click **Yes** when prompted to Start Recording Data



5. Configure the MeterApp for a Serial connection to the instrument

- **Unlock the MeterApp**
- To obtain the unlocked password, use the SEEPasswordGeneratorPlus.exe (in the 'Meters' folder on the desktop). Click on **Admin – Unlock** in the MeterApp and enter the code from the password generator.
- **Stop the MeterApp** by clicking the Run option in the Menu and select Stop
- Open the '**Data Input Settings**' tab
- Under '**Virtual Communications Settings**' section, enter '**Com5**' for the port (use the Port number labeled on the outside of the Smart Gateway)
- **Select the appropriate baud rate for your instrument** (refer to the Instrument section of the Viper Guide)
- **Remove the checkmark from 'Chk-Bat Sig'** (may also say Chk-Bat Volt)
- Put a checkmark in '**Use Serial Direct Connection. NotWiFi**'
- Under the '**GPS.Default TCP Optional UPD Serial or MC Listen**' section
 - In the IP box, enter **192.168.4.1** (this will obtain the GPS from the Cradlepoint)
 - In the Port box enter **8024**
 - Put a checkmark in **Get GPS**
- Click the **Save Settings** button
- Click the **Configure** button
- Start the MeterApp Run by click on **Run – Start**
- Sensors should turn green and samples should increment
- Survey Controller should turn green



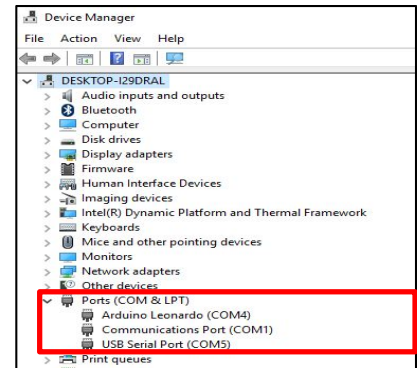
If the sensors in the MeterApp do not turn green and receive readings, close the MeterApp using the 'x' in the upper right corner and let the MeterApp open again on its own.



Troubleshooting Serial (COM Port) Connections

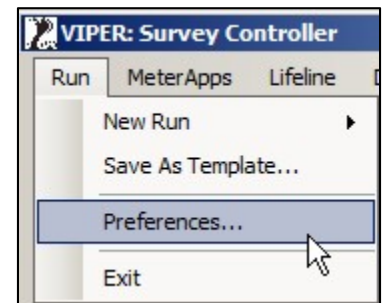
If the MeterApp does not turn green:

- Verify the COM Port and Baud Rate are correct on the Data Input Settings tab of the MeterApp
- Close the MeterApp by clicking on the 'x' in the upper right corner and let the MeterApp launch on its own
- Verify that the COM Port assigned in Device Manager is the same as labelled on the outside of the SmartGateway.
 - Click the Windows Search Icon in the lower left corner of the screen
 - Type 'Device Manager' in the search bar and press enter
 - Expand the 'Ports (COM & LPT) section'. The COM Ports that are assigned will show in the list.
 - When the connection is made on the Smart Gateway, Device Manager should display the COM Port assigned for that instrument connection

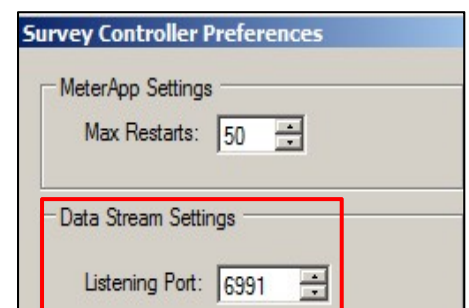


If the MeterApp turns green and Survey Controller shows 'No Data' in the latest reading column:

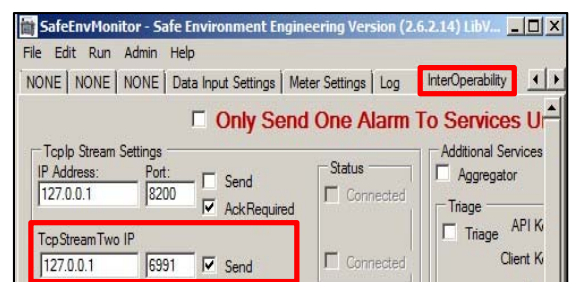
- Verify that the MeterApp is configured to send to the correct Survey Controller Listening Port
 - In Survey Controller, verify the Listening Port
 - Click on Run and select Preferences



- Under the Data Stream Settings, make note of the listening port. This port will be 6991 by default



- Unlock the MeterApp
- Switch to the 'Interoperability' Tab
- Verify that the TCPStreamTwo IP is set to 127.0.0.1, the port is 6991 and there is a checkmark in the 'Send' box
- Click the 'Save and Configure' button





Using the USB Ports to Connect Instruments – Serial to USB (i.e., DustTraks)

Section 5 of this guide outlines how to directly connect a RAE Host to the Smart Gateway USB port and configure a run in Survey Controller.

When connecting an instrument using a Serial (RS-232) to USB connection, the Laptop inside the Smart Gateway will assign a COM port number for that connection. If using both USB ports on the Gateway or if using a USB splitter to add instruments, it is important to only **connect one instrument at a time** in order to identify which COM port is assigned to which connection.

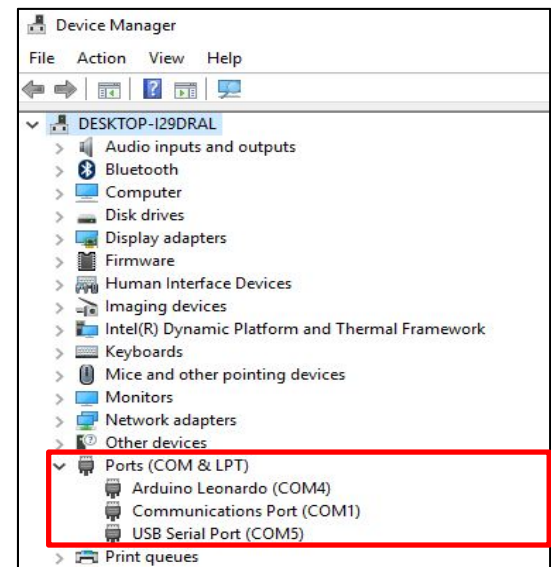


Hardware Note: Only certain Serial (RS-232) to USB connectors will work. If the connector is not automatically assigning a COM port number, try another connector. The connector should be FTDI compliance and use a Virtual Com Port Driver. The driver that is already loaded on the laptop in the Gateway should be sufficient when used with the proper connector.

1. Open Device Manager – BEFORE CONNECTING the Serial to USB cable to the Gateway

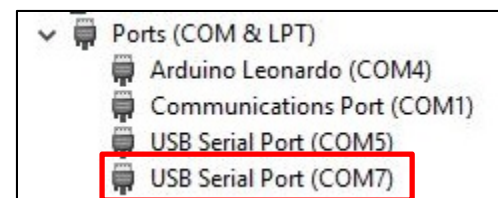
- Click the Windows Search Icon in the lower left corner of the screen
- Type 'Device Manager' in the search bar and press enter
- Expand the 'Ports (COM & LPT)' section. The COM Ports that are already assigned will show in the list. Make note of which COM ports are already assigned.

KEEP THIS WINDOW OPEN



2. Connect the instrument to the 'Serial to USB Cable' and connect the USB end to one of the USB ports on the Smart Gateway.

- DustTrak Note: Since the DustTrak connection is USB and the Smart Gateway connection is USB, a Female to Female DB9 Null Modem cable must be used between two Serial to USB connectors.
- When the connection is made on the Smart Gateway (USB cable is plugged in), Device Manager should display the new COM port assigned for that instrument connection. Make note of the new COM Port.



3. From this point forward, the steps are the same as outlined in Section 1.

- **Add a custom LINC number for COM7 (LINC 1007)** to Survey Controller
- **Start a Run** in Survey Controller
- **Unlock the MeterApp, Stop the MeterApp Run and configure it for COM7 and the instrument-specific baud rate**
- **Start the MeterApp Run.** Sensors should turn green and samples should increment...



Using the Ethernet (RJ45) Port (SPM Flex)

1. Verify that the Ethernet Port is configured as LAN
 - Login to the Cradlepoint and navigate to Networking – VLAN Interfaces (Refer to the table above for login information for the Cradlepoint modem)

VLAN Interfaces			
<div>+ Add ✎ Edit ✖ Remove</div>			
UID	VID	Mode	Ports
<input type="checkbox"/> wan	1	WAN	
<input checked="" type="checkbox"/> lan	2	LAN	0U U 2U

- Look where port 0U is configured. If it is in the LAN section, the Ethernet Connector is set to work for an instrument connected to the external Ethernet port (i.e., SPM Flex). If the 0U port is missing or is in the WAN section, see the Internet Sources section below for details on configuring the Ethernet port to have 0U in the LAN section.
2. From this point forward, the steps are the same as outlined in Section 1 EXCEPT, the instrument will be using an IP Address instead of a COM port in the 'Data Input Settings' tab of the MeterApp and the custom LINC number will be the last three digits of the Flex's IP Address.
 - **Add a custom LINC** number for the Ethernet Port to the Equipment Inventory in Survey Controller. **Use the last three digits of the SPM Flex IP address** as the LINC number. For Example, an SPM Flex with an IP address of 192.168.3.150 would have a LINC of 150 added to Survey Controller. An SPM Flex with an IP address of 192.168.3.142 would have a LINC of 142 added to Survey Controller, etc.
 - **Start a Run** in Survey Controller
 - **Unlock the MeterApp**, Stop the MeterApp Run, and configure the 'Data Input Settings' tab as shown
 - **Configure the MeterApp** to use the IP Address
 - In the **LINC Setting** section, verify the SPM Flex's **IP Address** in the 'Meter's IP Address' box
 - Enter **port 502** for an SPM Flex
 - **Remove** the checkmark from **ChkBat-Sig**
 - Configure GPS as shown
 - Click **Save and Configure**
 - Start the **MeterApp Run**
 - Click **Run – Start**

SPM Flex LINC 150 EPAERT231 Wifi - Safe Environment Engi

File Edit Run Admin Help

SEECAM Training Hydrogen Cyanide (HCN) Data Input Settings

LINC Settings

Meter's IP Address Port No Data Timer

192.168.3.150 502 30 ☐ Wait NDT

Linc IP or ComPort Bat Port Bat Timeout ☐ ChkBat-Sig

192.168.3.150 23 30 LINC

GPS. Default TCP. Optional UDP Serial or MCListen

IP Port

192.168.4.1 8024 ☐ UDP ☐ Connected

☒ Get GPS ☐ Log GPS GPS Retry 60

Sensors should turn green and samples should increment.
Close the MeterApp and let it re-launch if the sensors don't turn green.



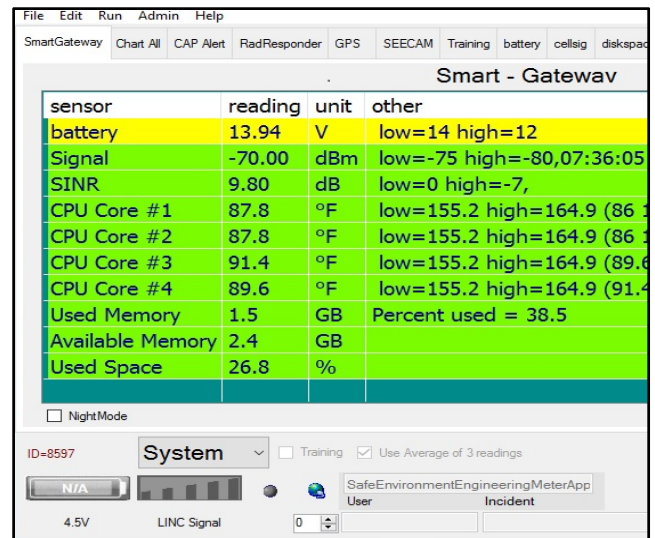
Section 2 – Smart Gateway MeterApp

Safe Environment Engineering has developed a Smart Gateway MeterApp to monitor the performance of the Smart Gateway. This MeterApp can be added to Survey Controller and allows for viewing Smart Gateway performance metrics such as battery life, cellular signal strength and noise interference, CPU, temperature, available disk space and memory use (RAM). Deployment Manager alarms and notifications can also be configured on these metrics, and alert you when potential Smart Gateway performance issues exist.

The Smart Gateway MeterApp also contains some default alarm values for the battery, CPU temperature, cell signal strength and noise interference. Other than the battery values, the other default values were developed on deployments at large venues during high-attendance popular events. As such, those default alarm values might not be representative of a typical EPA removal deployment. ERT and Safe Environment Engineering welcome feedback on any observations about these performance metrics/alarms and how they may differ during EPA responses, and what values were more appropriate for the response.

Smart Gateway Sensors

- **Battery:** Monitors the Smart Gateway battery life. A full battery is indicated by a reading above 16 volts. The MeterApp will turn Yellow to indicate a warning when the battery reading falls below 14 and red when the battery reading falls below 12.
- **Signal:** Monitors the cell signal strength from the SIM card. *See the graphic and discussion below for additional information signal strength.* The default values will turn the MeterApp sensor yellow when signal strength falls below -75 and red when signal strength is below -80. Rule of thumb is a lower negative number is better. Information is also provided on time of the last acquisition and which cellular carrier is being utilized.
- **SINR:** Signal to noise ratio. Sometimes you can have a great signal strength but still have bad bandwidth. This can happen when there is a lot of cellular noise. Usually a range of +7 to +20 is good. Zero or negative is bad. *See the graphic and discussion below for additional information on SINR.*
- **CPU:** Monitors the temperature of the laptop CPU. There are 4 values – one for each of the quad-processors installed. The MeterApp CPU sensor will turn yellow when temperature exceed 155.2 °F and red when it exceeds 164.9 °F. These values are based on the highest operating temperature for the processor of 194 °F. The default alarm values are yellow at 80 percent of 194 °F and red at 85 percent of 194 °F.
- **Used Memory:** Displays the amount of RAM being used. This is informational and MeterApp alarms cannot be configured on this value. The motherboard has a total of 4GB RAM.
- **Available Memory:** Displays the amount of RAM available. The motherboard has a total of 4GB RAM. MeterApp alarms can be configured on Available Memory.





- **Used Space:** Displays the amount of hard drive space used. The Smart Gateways have a 60GB hard drive. Alarms can be configured on the percentage of disk space used. Viper Survey Controller stores 'raw and compiled' data locally on the hard drive. Assuming that Survey Controller was pushing data to Deployment Manager, it is recommended that when a deployment is completed, the files stored locally on the Smart Gateway be deleted from the hard drive. If data was not transmitted to Deployment Manager, copy these files off of the Smart Gateway and store them as needed. The files are located in C:\Program Files (x86)\Viper\Viper Field Survey Controller\Data.

Additional Signal and SINR Information

The graphic here can be used as a reference for understanding the Signal and SINR values. Use these values together when deciding where to deployment instruments. The SINR values can vary significantly depending on the venue of the deployment. For instance, the SINR may bounce from +10 to =10 in stadium environments with large crowds recording opening ceremonies, etc. Be patient and see if fluctuation settles down before choosing to relocate equipment.

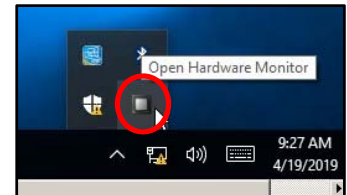
RSSI	Signal Strength
> -70 dBm	Excellent
-70 dBm to -85 dBm	Good
-86 dBm to -100 dBm	Fair
< -100 dBm	Poor
-110 dBm	No signal

SINR Value	Throughput
> 10	Excellent
6 to 10	Good
0 to 5	Fair
< 0	Poor

Troubleshooting the Smart Gateway MeterApp

The Smart Gateway MeterApp will automatically launch each time the gateway is powered up.

Open Hardware Monitor: The Smart Gateway MeterApp obtains its information from another program called 'Open Hardware Monitor'. This program runs automatically on the Smart Gateway. If this program is accidentally stopped, the MeterApp will not be able to obtain metrics. To restart the program, a shortcut can be found on the desktop of the Smart Gateway laptop in a folder called 'Meters'. An icon will be minimized in the tray when the program is running.



If the Smart Gateway MeterApp is not reporting all of its sensors (see Smart Gateway Sensors section above), there are some settings that might not be set in the **Open Hardware Monitor**.

sensor	reading	unit	other
battery	15.8	V	low=14 high=12
Signal	-73.00	dBm	low=-75 high=-80,11:45:33 Verizon mdm-fccf08b
SINR	1.60	dB	low=0 high=-7
CPU Core 0	0	F	
CPU Core 1	0	F	
CPU Core 2	0	F	
CPU Core 3	0	F	
CPU Core 4	0	F	

HighMode ☐

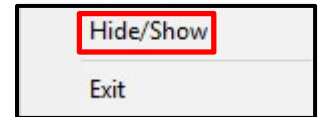
Activity ID: System Training ☐ Use Average of 3 readings

4.5V LINC Signal 0 User Incident

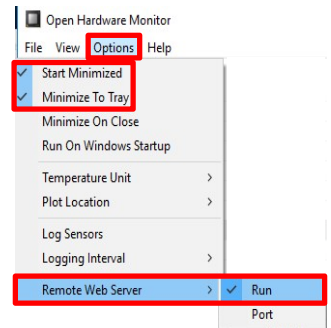
GPS OFF DataIn:18 # Samples: 18 Run(dd hh:mm:ss) 00:00:00:23



To open the **Open Hardware Monitor**, click the ^ in the taskbar to expand the list of icons. Right-click on the **Open Hardware Monitor** icon and select **Hide/Show**.



Under **Options**, make sure there is a checkmark in the **Start Minimized** and **Minimize To Tray**, and Remote Web Server is set to **Run**.



Arduino Board: The battery strength is obtained from an Arduino board in the Smart Gateway. If the programming for this board is changed or corrupted, the battery signal strength will not be available.



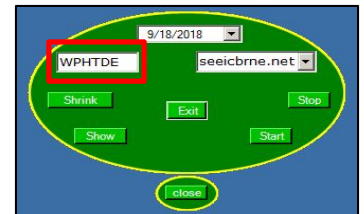
Adding the Smart Gateway MeterApp to a Survey Controller Run

The metrics in the Smart Gateway MeterApp can be added to a Survey Controller Run. This enables you to request Deployment Manager alarms and notifications to be configured on those metrics so you can be alerted when things such as the Smart Gateway battery level are decreasing or internal temperature is increasing.

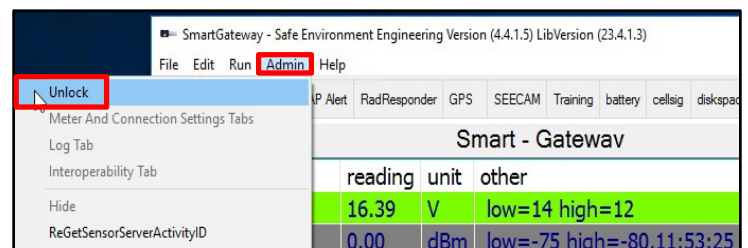
NOTE: It is HIGHLY RECOMMENDED to use Survey Controller's 'Reading Interval' feature when adding the Smart Gateway MeterApp to a run. Each 'sensor' in the MeterApp collects readings every second. By specifying a reading interval in Survey Controller of perhaps 5 minutes for the Smart Gateway MeterApp, you will greatly reduce the number of readings recorded. Refer to the Viper User Guide – Section 3, Part E for additional information on configuring readings intervals in Survey Controller.

1. Modify the MeterApp to work in Survey Controller

- **Open the Password Generator** program located in the 'Meters' folder on the desktop. The program name is SEEPassword Generator Plus.EXE.

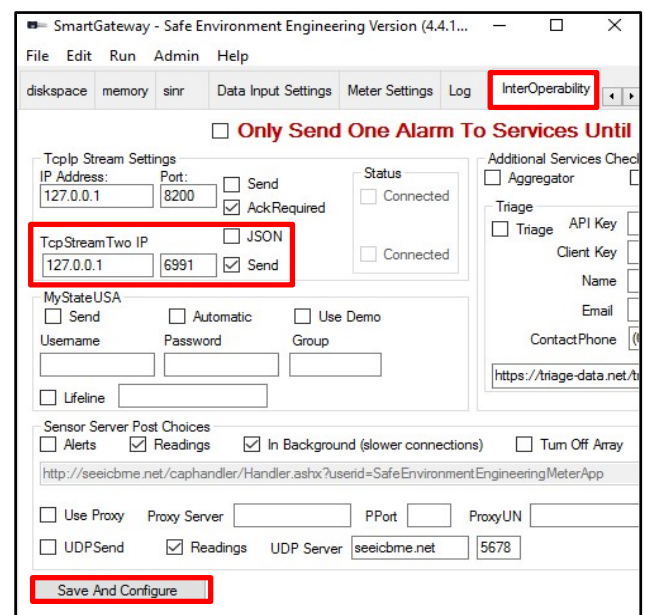


- In the Smart Gateway MeterApp, click on **Admin** and select **Unlock**. Enter the code displayed in the password generator.



INTEROPERABILITY SETTINGS

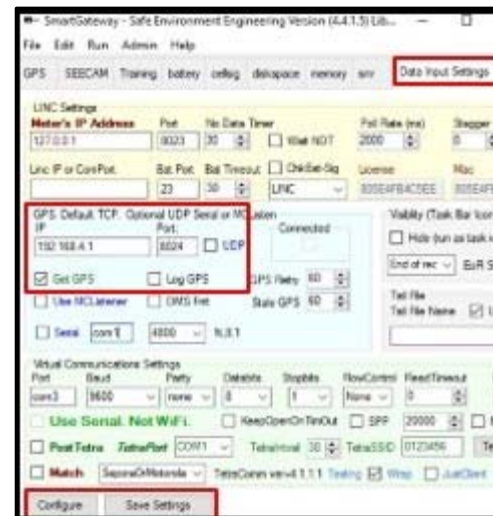
- Switch to the **InterOperability** tab
- Enter a **TcpStreamTwo** IP of **127.0.0.1**
- Enter a **Port** of **6991** for TcpStreamTwo IP
- Put a checkmark in the **Send** box for TcpStreamTwo
- Click **Save and Configure**





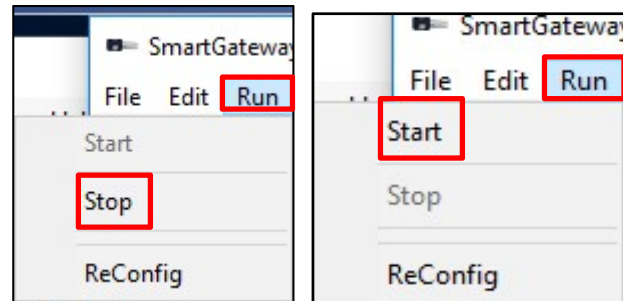
DATA INPUT SETTINGS

- Switch to the **Data Input Settings** tab
- Enter **192.168.4.1** in the GPS Default TCP IP
- Enter **8024** for the GPS Port
- Put a checkmark in **Get GPS**
- Click **Save Settings**
- Click **Configure**



STOP AND RESTART THE MeterApp

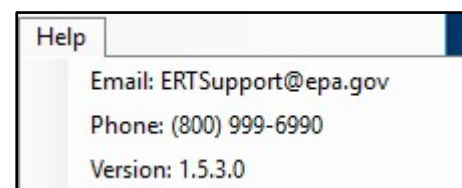
- Click **Run** in the MeterApp Menu
- Select **Stop**
- Click **Run** in the MeterApp Menu
- Select **Start**



2. Verify the version of Viper Survey Controller

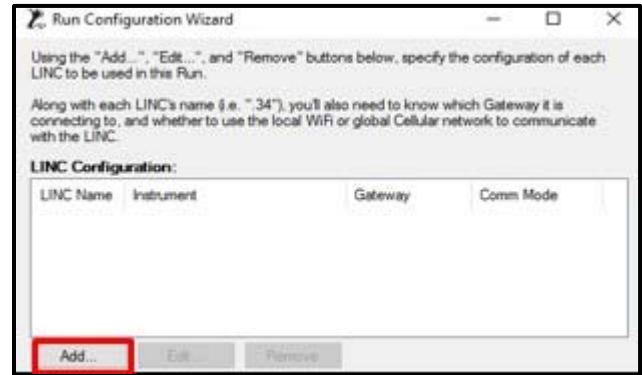
The Smart Gateway MeterApp is compatible with Viper Survey Controller **v1.5.3**. It will not function correctly with earlier versions of Survey Controller.

- Click the **'Help'** menu in Survey Controller
- If the version displayed is earlier than 1.5.3, the latest version of Survey Controller must be installed
- First Un-Install the existing version of Survey Controller
- Refer to 'Section One – Part B' of the Viper User Guide for instructions on installing Viper Survey Controller

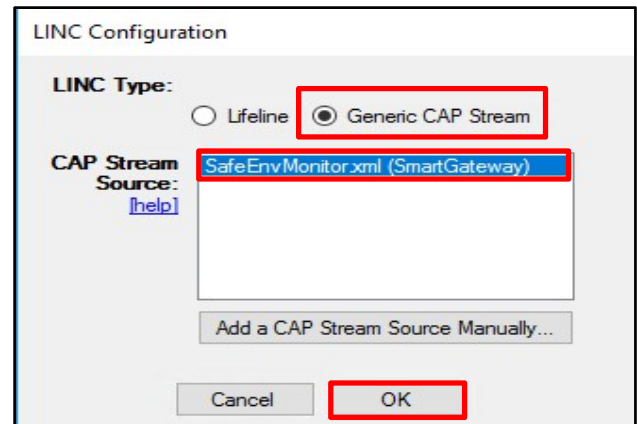




3. Add the Smart Gateway MeterApp to a Survey Controller Run
 - Start a run and click **'Add'** on the LINC Configuration window

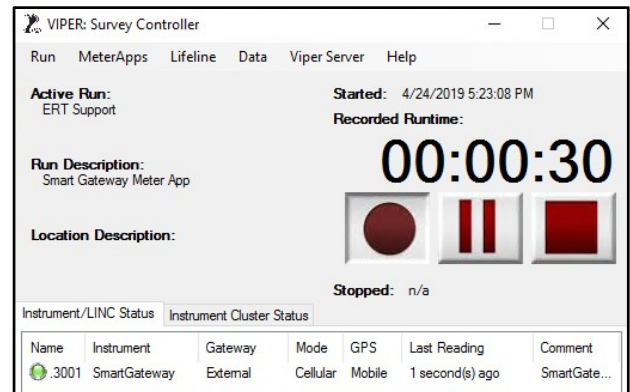


- Select the **'Generic Cap Stream'** radio button
- Click on **'SafeEnvMonitor.xml (SmartGateway)'** in the CAP Stream Source box
- Click **OK**

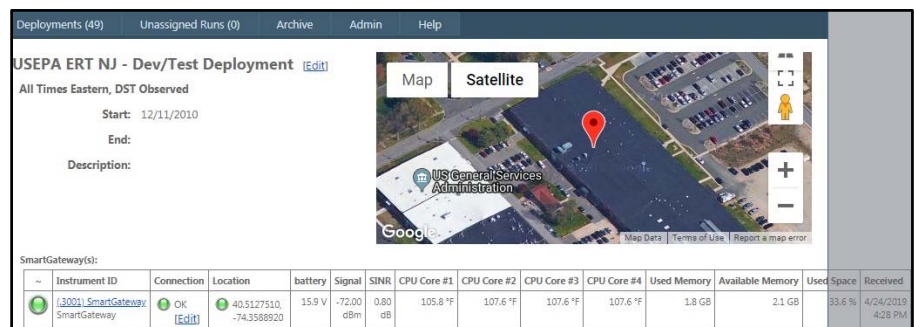


Note: If the SafeEnvMonitor.xml file does not show in the CAP Stream Source box, make sure the Smart Gateway MeterApp is running.

- Add any additional LINC/Instruments for the run and start the run



The Smart Gateway Sensors will be displayed in Deployment Manager. Alarms and notifications can be set on the Smart Gateway sensors.





Section 3 – Smart Gateway WiFi and Security

Unlike traditional gateways, the WiFi signal on the Smart Gateway is configured on the Cradlepoint Router. There are also two (2) WiFi radio frequencies – 2.4 GHz and 5 GHz. The primary differences between the 2.4 GHz and 5 GHz wireless frequencies are range and bandwidth. 5 GHz provides faster data rates at a shorter distance. 2.4 GHz offers coverage for farther distances, but may perform at slower speeds. Both frequencies are configured by default to broadcast EPAERT1.

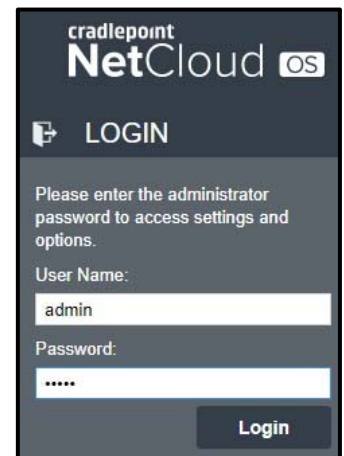
Disabling/Enabling WiFi

Follow the steps below to enable or disable WiFi on the Smart Gateway.

NOTE/Caution: *If the Smart Gateway has no SIM card and you disable the WiFi, you will have to hardwire a keyboard, mouse and monitor (or use the touch screen) to use the internal laptop to login and access the Cradlepoint.*

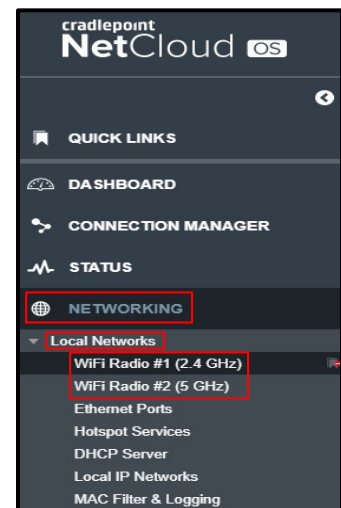
1. Connect a laptop to the EPAERT1 network and open a browser (Chrome is preferred).
2. Navigate to <https://192.168.4.1>
3. Enter the User Name and contact ertsupport@epa.gov to obtain the password

Username: admin



The image shows the login interface for Cradlepoint NetCloud OS. It features a dark header with the 'cradlepoint NetCloud OS' logo. Below the header is a 'LOGIN' section with a prompt: 'Please enter the administrator password to access settings and options.' There are two input fields: 'User Name:' with the text 'admin' and 'Password:' with masked characters '*****'. A 'Login' button is located at the bottom right of the login section.

4. Navigate to **Networking**.
5. Select Local **Networks**.
6. Select the WiFi Radio (#1 or #2)



If you want to enable/disable ALL radios, select the main Enable/Disable buttons. However, if you want to enable or disable individual radios, follow the steps below (recommended).

Wireless Radio: **Enable** **Disable**



7. Select the EPAERT1 WiFi Name (SSID).
8. Click Edit.

Wireless Radio: **Enable** **Disable**

Wireless Access Points / SSIDs

Edit **Duplicate Settings**

WiFi Name (SSID)	Security Mode
<input checked="" type="checkbox"/> EPAERT1	WPA2 Personal (AES)

9. Toggle Enables on or off by removing/replacing the checkmark. Click the 'Save' button.

EPAERT1

Configuration

WiFi Name (SSID): EPAERT1

Hidden: ☐

Isolate: ☐

WMM: ☒

Enabled ☒

Security Mode: WPA2 Personal

WPA Settings

WPA Cipher: AES

WPA Password: Unmask Password

Re-key Interval: 3600

Protected Management Frames: Disabled

Minimum Bitrates: ☒ 1Mbps ☒ 6Mbps ☒ 24Mbps

Cancel **Save**

EPAERT1

Configuration

WiFi Name (SSID): EPAERT1

Hidden: ☐

Isolate: ☐

WMM: ☒

Enabled ☐

Security Mode: WPA2 Personal

WPA Settings

WPA Cipher: AES

WPA Password: Unmask Password

Re-key Interval: 3600

Protected Management Frames: Disabled

Minimum Bitrates: ☒ 1Mbps ☒ 6Mbps ☒ 24Mbps

Cancel **Save**



Changing WiFi Network Name (SSID) in the Gateway

Caution – this is an advanced task and could render a Smart Gateway unable to communicate with standard EPA LINC's.

LINC's connect to the WiFi network, so changing the WiFi network of a Smart Gateway will require the LINC's to be changed to match the new WiFi network name. It is recommended that the LINC SSID's be changed **before** the Smart Gateway SSID.

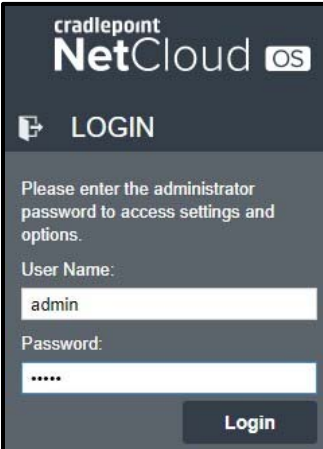
It is important to label the Gateway with the new SSID to avoid confusion and assist with reconfiguring the Gateway back to EPAERT1 as necessary.

1. Verify your computer is connected to the Smart Gateways WiFi network (EPAERT1 by default).
CAUTION: Remember to change the SSID on the LINC's before changing the SSID of the Gateway. Refer to the Viper User Guide, Section Seven – Part C: Changing the WiFi Name (SSID) on a LINC.

2. Open a browser (Chrome is preferred), navigate to <https://192.168.4.1>.

3. Enter User Name and Contact ertsupport@epa.gov to obtain the password

User Name: admin

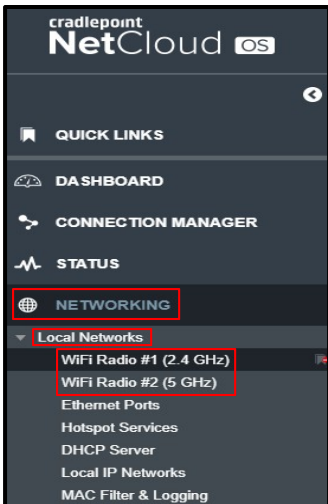


The image shows the login page of the Cradlepoint NetCloud OS. At the top, it says "cradlepoint NetCloud OS". Below that is a "LOGIN" header. The main text says "Please enter the administrator password to access settings and options." There are two input fields: "User Name:" with the value "admin" and "Password:" with masked characters "*****". A "Login" button is at the bottom right.

4. Navigate to **Networking**.

5. Select **Local Networks**.

6. Select the **WiFi Radio** (#1 or #2).
Note: LINC's can connect to either 2.4 GHz or 5 GHz, but they typically connect to the 2.4 GHz network which has a longer range.



The image shows the "NETWORKING" section of the Cradlepoint NetCloud OS. The "NETWORKING" menu item is highlighted with a red box. Under "Local Networks", "WiFi Radio #1 (2.4 GHz)" and "WiFi Radio #2 (5 GHz)" are listed, both highlighted with red boxes. Other options include "Ethernet Ports", "Hotspot Services", "DHCP Server", "Local IP Networks", and "MAC Filter & Logging".



7. Select the EPAERT1 WiFi Name (SSID).
8. Click Edison.

Wireless Radio: **Enable** **Disable**

Wireless Access Points / SSIDs

Edit **Duplicate Settings**

WiFi Name (SSID)	Security Mode
<input checked="" type="checkbox"/> EPAERT1	WPA2 Personal (AES)

9. Enter a New SSID Name.
10. Click Save.

NEW SSID

Configuration

WIFI Name (SSID): **NEW SSID**

Hidden: ☐

Isolate: ☐

WMM: ☒

Enabled: ☒

Security Mode: WPA2 Personal

WPA Settings

WPA Cipher: AES

WPA Password: **Unmask Password**

Re-key Interval: 3600

Protected Management Frames: Disabled

Minimum Bitrates: ☒ 1Mbps ☒ 6Mbps ☒ 24Mbps

Save



Disabling WiFi Security

By default, the Viper Smart Gateways are configured with an SSID of EPAERT1 and require a security password. There may be some instances when having an 'open' WiFi connection is desirable (e.g., a LINC is not security enabled and cannot connect to the EPAERT1 network). In this instance, Wireless Security Settings can be modified in the EPAERT1 Smart Gateway Cradlepoint to unsecure the WiFi network.

1. Connect to the EPAERT1 network.
2. Open a browser (Chrome is preferred), navigate to <https://192.168.4.1>.
3. Enter User Name and contact ertsupport@epa.gov to obtain the password.

User Name: admin

The screenshot shows the login interface of the Cradlepoint NetCloud OS. It has a dark theme with the title 'cradlepoint NetCloud OS' at the top. Below the title is a 'LOGIN' section with a prompt: 'Please enter the administrator password to access settings and options.' There are two input fields: 'User Name:' with the text 'admin' and 'Password:' with masked characters '*****'. A 'Login' button is at the bottom right.

4. Navigate to **Networking**.
5. Select **Local Networks**.
6. Select the **WiFi Radio** (#1 or #2)

The screenshot shows the 'NETWORKING' menu in the Cradlepoint NetCloud OS. The 'NETWORKING' option is highlighted with a red box. Below it, the 'Local Networks' section is expanded, showing 'WiFi Radio #1 (2.4 GHz)' and 'WiFi Radio #2 (5 GHz)', both of which are also highlighted with red boxes. Other options like 'Ethernet Ports', 'Hotspot Services', 'DHCP Server', 'Local IP Networks', and 'MAC Filter & Logging' are listed below.

7. Select the **EPAERT1** WiFi Name (SSID).
8. Click **Edit**.

The screenshot shows the 'Wireless Access Points / SSIDs' configuration screen. At the top, there is a 'Wireless Radio:' section with 'Enable' and 'Disable' buttons. Below this is a table of access points. The first row is highlighted with a red box, showing 'EPAERT1' as the WiFi Name (SSID) and 'WPA2 Personal (AES)' as the Security Mode. There are 'Edit' and 'Duplicate Settings' buttons above the table.

WiFi Name (SSID)	Security Mode
EPAERT1	WPA2 Personal (AES)



9. Under **Security Mode**, select '**Open**'.
10. Click **Save**.

The screenshot shows the EPAERT1 Configuration page. The 'WPA Settings' section is expanded, showing a dropdown menu for 'Security Mode' with 'Open' selected. Other settings include 'WPA Name (SSID): EPAERT1', 'Hidden: ☐', 'Isolate: ☐', 'WMM: ☒', 'Enabled: ☒', 'WPA Cipher: WPA / WPA2 Personal', 'WPA Password: [masked]', 'Re-key Interval: WEP Auto', and 'Protected Management Frames: ☒'. The 'Save' button is highlighted in red.

Enabling WiFi Security

- Follow steps 1 through 8 above to navigate to the **Security Mode** option
- Select WPA2 Personal for Security Mode
- Assign a WPA Password of. Contact ertsupport@epa.gov to obtain the password

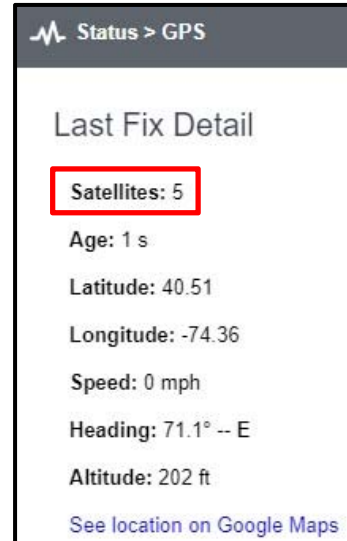
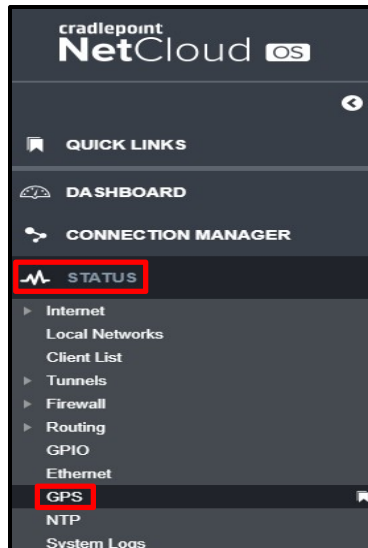


Section 4 – Cradlepoint GPS Settings

Overview

The GPS on the Cradlepoint acts like an independent 'client' and delivers GPS to all of the Meters that are connected. If the Cradlepoint can't see the satellites, GPS will not be provided.

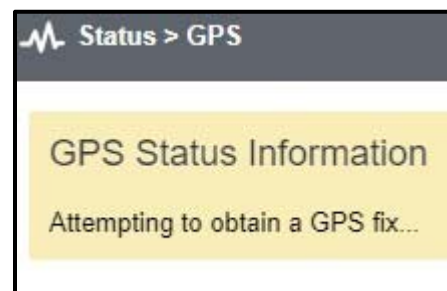
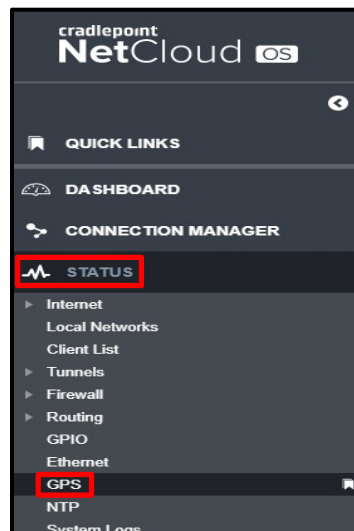
To verify that you are getting GPS and to see the number of satellites, login to the Cradlepoint and navigate to **STATUS | GPS**. The screenshot below indicates that the Cradlepoint successfully acquired GPS Signal.



NOTE: The GPS Antennae must be fully attached to the Cradlepoint to receive GPS. If you are not receiving GPS, unscrew the GPS antennae and then reattach it.

Troubleshooting the Cradlepoint GPS Settings

This screenshot indicates that the Cradlepoint has not successfully acquired GPS. The following steps should be followed to make sure that GPS is correctly enabled on the Cradlepoint.





- To make sure GPS is enabled on the Cradlepoint, navigate to **SYSTEM | ADMINISTRATION | GPS** and make sure that **Enable GPS** is checked.

System > Administration > GPS

Global Positioning System

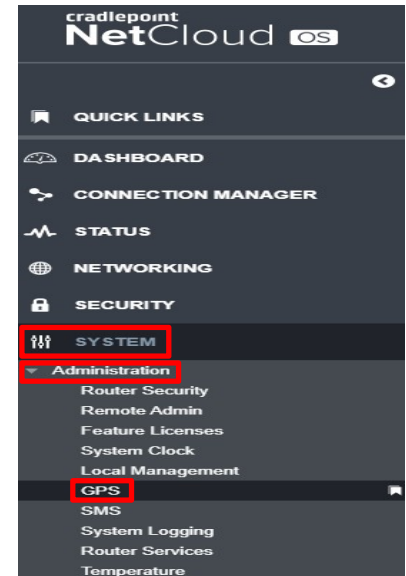
Enable GPS: ☒

Note: Some carriers disable GPS support in otherwise supported r

Enable GPS Lock LED: ☒

Enable GPS Keepalive: ☐

TAIP Vehicle ID #: 0000



- There should be one entry under the **'Send to Clients'** section of that screen.

Send to Client(s)			
<div>+ Add ✎ Edit ✕ Remove</div>			
Name	State	Port	Language
<input checked="" type="checkbox"/> GPS	Enabled	8024	NMEA

- Put a **checkmark** in the entry and click **'Edit'**. Add or Edit GPS page 1 of 3 settings should be set to:

- Check** in Enable this Server
- Server Name – **GPS**
- Check** in Enable GPS server on LAN
- Check** in Enable GPS server on WAN
- Port: **8024**

⚙ Add or Edit GPS

Server Details

Enable this Server: ☒

Server Name:

Enable GPS server on LAN: ☒

Enable GPS server on WAN: ☒

Port:

1 of 3 Next



- Add or Edit GPS page 2 of 3 settings should be set to:

- Choose Language = **NMEA**
- **Check** in Report NMEA GGA sentences

2 of 3

- Add or Edit GPS page 3 of 3 settings should be set to:

- Default Time Interval (seconds) = **2**
- Stationary Distance Threshold (meters) = **20**
- Everything else = **0**
- Click **Finish**

3 of 3

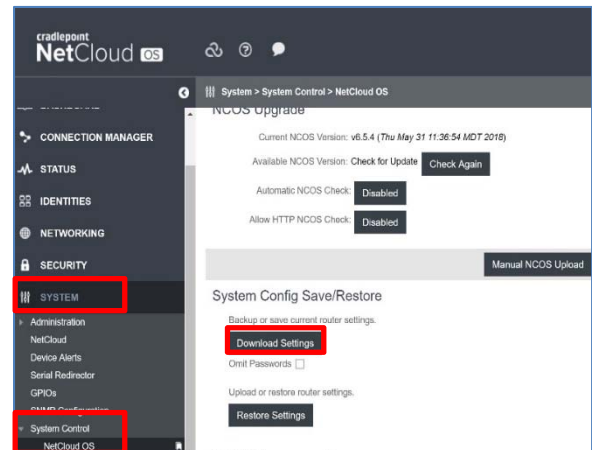


Section 5 – Internet Sources

The Smart Gateway supports acquiring internet access via a SIM card, WiFi Source or Ethernet Source. If the source of the internet access is behind a router and/or uses a private IP Address (vs. a Public/Static IP Address), Survey Controller running on the internal laptop will still be able to push data to Deployment Manager. However, remote administration of the Gateway will not be possible and remote administration of the internal laptop will not be possible without using 3rd party software such as 'Go To Assist', Adobe Connect, etc. As such, it is recommended that the primary internet source for the Smart Gateway should be a SIM card with a Public IP Address. Purchasing this type of SIM card can be done by contacting your Regional Working Capital Fund Coordinator and requesting a SIM Card with a Public/Static IP Address.

The steps below are considered Technically Advanced and should be performed with caution. It is recommended that the Cradlepoint Router Configuration be saved before making these changes.

- Login the Cradlepoint Gateway to backup the current configuration
- Open the System Menu
- Open the System Control Menu
- Select NetCloud OS
- Click Download Settings under the 'System Config Save/Restore' section



Internal SIM Card

This Gateway carries Firmware for AT&T, Verizon, and Sprint. It auto-detects which carrier's SIM is inserted and switches to that version Firmware automatically. There is no need to 'flash' the Gateway if/when switching between carriers. You can see which firmware is selected by logging into the Cradlepoint and navigating to SYSTEM | SYSTEM CONTROL | FIRMWARE.



For additional information on **Interpreting LEDs on the Gateway**, see the **Antennae & SIM Cards** section of this guide.



External WiFi Source

If cell service isn't available but a WiFi connection is available, the Cradlepoint in the Gateway can be configured to use the WiFi as its source of internet and data will be pushed to Deployment Manager. However, if the WiFi network assigns a private IP Address to the Cradlepoints, runs must be configured on the internal laptop or on another laptop connected to the EPAERT1 network. Also, if the Cradlepoint receives a private IP address, remote administration of the Cradlepoint is not possible.

The following is a list of private (and reserved) IP Address Ranges:

- 10.0.0.1 to 10.255.255.254
- 172.16.0.1 to 172.31.255.254
- 192.168.0.1 to 192.168.255.254
- 100.64.0.1 to 100.127.254.254

Follow the steps below to configure the Cradlepoint to use a WiFi as its internet source:

- Login to the Cradlepoint and navigate to NETWORKING – WiFi as WAN, or Client
- Under Radio Settings, in the WiFi Client Mode select WiFi as WAN and click Save
- Scroll down to Site Survey and click Refresh
- Highlight the SSID you want to use as your internet source and click IMPORT
- Enter the security password (if applicable) and his SAVE
- Scroll up and that Network should now be in the Saved Profiles
- Navigate to Connection Manager and select Devices
- The WiFi profile should be listed – you might have to scroll down to see it
- Highlight the WiFi profile and drag it to the top of the list so it is the first priority
- The WiFi profile should now show 'Connected' in the CONDITIONS column

If the WiFi profile does not show 'Connected' in the CONDITIONS column, see the section below on **Troubleshooting Internet Sources**

Ethernet Connection – Hard Wired

The Ethernet's connection can be configured for WAN (Hard Wired Internet) or LAN (for SPM Flex or other Ethernet instruments) and specifically the 0U (zero U) VLAN Port must be moved to either WAN or LAN depending on what you need the Ethernet connection to do.

Internally in the Gateway, we are modifying the behavior of the RJ45 plug in the Cradlepoint that is right next to the brass antennae fitting. The other RJ45 cable that is closest to the power cord on the Cradlepoint goes to the internal laptop's Ethernet port.

Follow the steps below to configure the Cradlepoint to use an Ethernet connection as its internet source

VLAN Interfaces			
<div>+ Add ✎ Edit ✕ Remove</div>			
<input type="checkbox"/> UID	VID	Mode	Ports
<input type="checkbox"/> wan	1	WAN	
<input checked="" type="checkbox"/> lan	2	LAN	0U U 2U



Login to the Cradlepoint and navigate to NETWORKING | VLAN INTERFACES

- Look where port 0U is. If it is in LAN, the Ethernet Connector is set to work for an SPM Flex or other Ethernet-connected instrument. The 0U port needs to be configured as WAN for the Gateway to obtain internet via Ethernet.
- To move the port to WAN, put a checkmark in the LAN box and select EDIT.
- Check Port 0 and remove it. Say Yes to confirm and click Save
- Back at the VLAN INTERFACES window, put a checkmark in WAN and select EDIT.
- Add Port 0 with a mode of Untagged and click SAVE
- Click Save again.

Port	Mode
Port 0 (Ethernet WAN)	Untagged

- Navigate to Connection Manager and selected DEVICES
- Scroll the list until you see the Ethernet profile and drag Ethernet to the top of the list
 - The Ethernet profile should now show 'Connected' in the CONDITIONS column

If the Ethernet profile does not show 'Connected' in the CONDITIONS column, see the section below on Troubleshooting Internet Sources

Troubleshooting WiFi and Ethernet internet sources

After modifying the Cradlepoint to use either a WiFi or Ethernet source and the profile doesn't show as 'Connected', try the steps below until the profile displays as 'connected'.

- Remove the checkmark in the Availability column from all other profiles – except for the one you want to use

WAN Device Interface Profiles & Priority			
<div>Add Edit Delete Control</div>			
	Profile Name	Conditions	Availability
			<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Modem-8619763b	type is Modem + tech is LTE/3G + uid is 8619763b	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Internal LP6 (SIM2 - Verizon)	(Connected)	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Ethernet-wan	type is Ethernet + uid is wan	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	(VID: 1)	(Unplugged)	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Ethernet	type is Ethernet	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	WWAN-54:b8:0a:de:04:26	type is WWAN + uid is 54:b8:0a:de:04:26	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	WiFi as WAN	type is WWAN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

- Wait a minute or two to see if the profile changes to connected. If not, continue to the next steps.



- Modify the Gateway Subnet Mask temporarily.
 - Navigate to NETWORKING – LOCAL NETWORKS – LOCAL IP NETWORKS
 - EDIT THE PRIMARY LAN
 - SELECT Ipv4 Settings
 - Change the subnet mask from 255.255.0.0 to **255.255.255.0** and click Save
 - Navigate back to Connection Manager and select Devices
 - The profile should now show 'Connected' in the CONDITIONS column
 - Set the Subnet Mask back to 255.255.0.0
 - Navigate to NETWORKING – LOCAL IP NETWORKS
 - EDIT THE PRIMARY LAN
 - SELECT Ipv4 Settings
 - Change the subnet mask back to 255.255.0.0



Section 6 – Directly connecting a RAE Host to the Smart Gateway

Overview

Since the Smart Gateway has a built in laptop, ProRAE Guardian (PRG) can be installed on the laptop and the RAE Host can be directly connected to the USB Port(s) on the Smart Gateway using a compatible Serial (RS-232) to USB connector. **NOTE: See the hardware note on page 18 about the type of Serial to USB connectors that are compatible.**

There are several advantages to running PRG locally on the Smart Gateway laptop:

- The ability to remote into the Smart Gateway laptop and see the status of ProRAE Guardian and Survey Controller via Remote Desktop Connection (RDC) from any computer.
- By running Survey Controller on the Smart Gateway laptop, Survey Controller provides local data storage in the event the Smart Gateway's internet connection goes down.

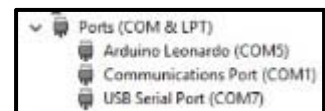
Install ProRAE Guardian Software

Install ProRAE Guardian software on the Smart Gateway. When running the install, at the 'Installation Options' window, select '**Custom Installation**'. When you are prompted to install the '**Guardian Web Application**' select '**Cancel**'.

Always verify that the Smart Gateway laptop time is correct for the time zone set

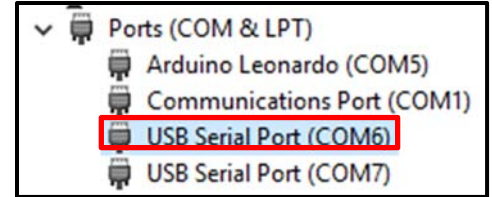
Attaching ProRAE Host to the Smart Gateway

1. Login to the Smart Gateway laptop (refer to Logging in to the Internal Laptop discussed earlier).
2. **Open Device Manager BEFORE CONNECTING the RAE Host Serial to USB cable to the Gateway.** Click the Windows search icon in the lower left corner of the screen and type 'Device Manager' in the search bar and press enter.
3. Scroll down to and expand the 'Ports (COM & LPT)' section. The COM Ports that are already assigned will show in the list. Make note of which COM ports are already assigned.
4. Connect the ProRAE Host directly to one of the USB ports on the Smart Gateway.





- When the connection is made on the Smart Gateway, Device Manager should display the new COM port assigned for that instrument. Make a note of the new COM port.



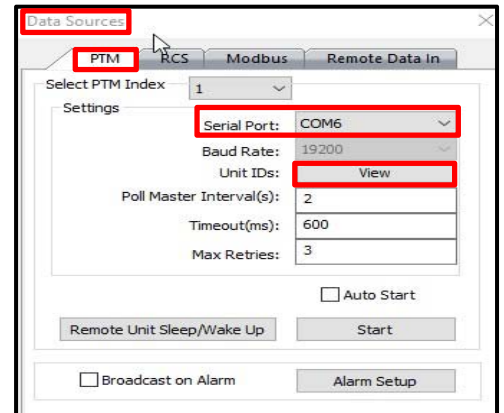
NOTE: When attaching new devices, do them one (1) at a time to make sure you know which Port is assigned to which device.

Configuring ProRAE Guardian

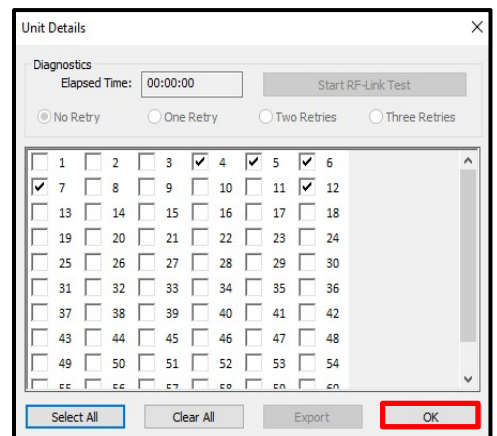
Prior to starting a run in Survey Controller, there are several configuration changes that need to be made in the Smart Gateways instance of the ProRAE Guardian software. The steps below outline the changes that need to be made.

- Open ProRAE Guardian.
- Under **Data Sources | PTM Tab**, verify that the correct Serial Port is selected. The Serial Port should match the COM port identified in Device Manager when the RAE Host was connected (step 5 above).

Note: if ProRAE Guardian started automatically, you will have to hit 'Stop' to be able to select the unit in the step below.



- Click on View (depicted above) and select the instrument IDs being deployed. Click OK.





4. Under **Data Sources | Remote Data In** tab, make sure there is **NO** checkmark in '**Cascade In Mode**'.

Data Sources

PTM RCS Modbus **Remote Data In**

☐ Viewer Mode - View data from a remote PRG PC

Parameters (Remote PRG PC)

Remote PRG PC Address:

Remote PRG PC Port:

☐ **Cascade In Mode** - Receive data from remote PCs

Parameters (This PC)

Listen Port:

☐ Enable Backup Port:

Max # of remote PCs:

☒ Enable User Authentication

☐ Auto Start

Start

5. Under **Options | Data Options | Data Forwarding** tab, place a checkmark in **Cascade Out Mode** and enter **Remote PC IP Address 127.0.0.1** and **Remote PC Port 9727**. Put a checkmark in **Auto Start** and click **Set**.

- Make sure there is **NO** checkmark in '**Enable Remote Viewers**'
- If you cannot change the Remote PC Port, uncheck and then recheck the '**Cascade Out Mode**'.

Data Options

Formats Alarm **Data Forwarding** Web Viewer Care Center Platform

☐ Enable Remote Viewers - Allow remote Viewers to view data from this PC

Parameters (This PC)

Listen Port: ☐ Enable Backup Port:

Max Viewers:

☒ **Cascade Out Mode** - Send data to a remote PC

Parameters (Remote PC)

Remote PC IP Address:

Remote PC Port:

☐ Enable User Authentication

Username:

Password:

☒ Auto Start

Set Cancel

6. A logon screen appears after you have Set the Data Forwarding Parameters. Enter the following logon information:

Username: administrator

Password: XXXXXXXXXXXX

Logon

Some features require user logon. Please enter your username and password below to access these features. Always make sure you remember your password. The only way to gain access to these features after losing user-defined passwords is to re-install PRG and use the default administrator account.

User Name:

Password:

OK Cancel



7. Click on **Data Sources | PTM** tab and click

The screenshot shows the 'Data Sources' dialog box with the 'PTM' tab selected. The 'Start' button is highlighted with a red box. The settings are as follows:

Setting	Value
Select PTM Index	1
Serial Port	COM6
Baud Rate	19200
Unit IDs	View
Poll Master Interval(s)	2
Timeout(ms)	600
Max Retries	3
Auto Start	<input type="checkbox"/>
Remote Unit Sleep/Wake Up	<input type="checkbox"/>
Broadcast on Alarm	<input type="checkbox"/>
Alarm Setup	<input type="button" value="Alarm Setup"/>

Start.

8. The instruments will now be displayed in the ProRAE Guardian software and will appear online in the System Information window.

Status	Fault	Image	Update Time	Unit ID	SN	UserLabel1
			10:46:21	5	W01A00002186	
			10:46:25	4	W01A00000564	

The screenshot shows the 'System Information' window with the following log messages:

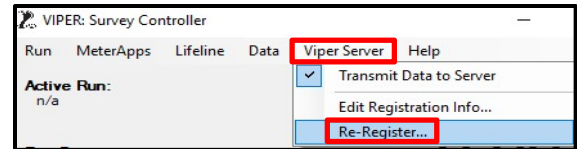
- 09/20/2019 10:44:43: Connected with Location Engine.
- 09/20/2019 10:42:10: SafetyNex started ...
- 09/20/2019 10:45:50: PTM: Open serial port 6
- 09/20/2019 10:45:53: AreaRAE Pro(W01A00000564) goes online.
- 09/20/2019 10:45:54: AreaRAE Pro(W01A00002186) goes online.

NOTE: For ProRAE Guardian to recognize instruments, those instruments must be set to the same Network ID as the RAE Host. ERT/EPA uses a Network ID of 438.



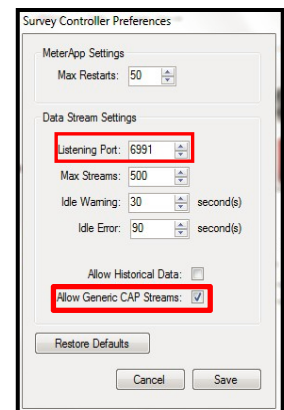
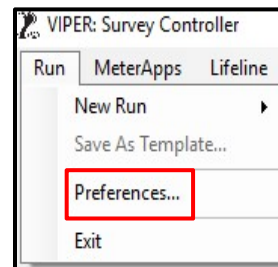
Configuring Viper Survey Controller

1. Open Survey Controller.
2. **Re-register** Survey Controller if this is the first run for a new deployment.



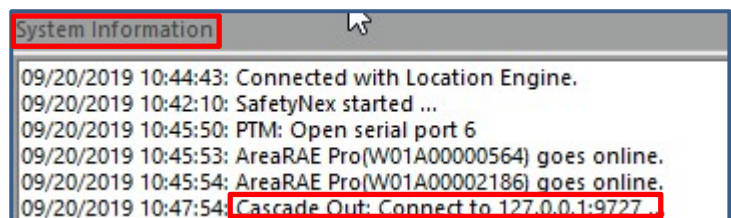
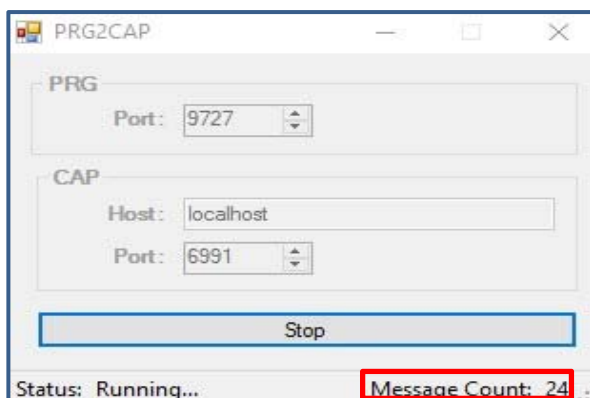
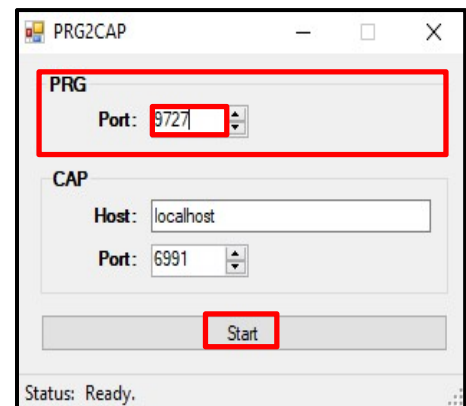
3. Click on **Run | Preferences**.
 - a. Verify the **Listening Port** is **6991**
 - b. Verify there is a checkmark in **Allow Generic CAP Streams**.

Note: PRG instruments are added to Survey Controller as 'Generic CAP' since a traditional LINC isn't being used.



Configuring PRG2CAP

1. Make sure Survey Controller is open.
2. Open **PRG2CAP**.
 - a. Verify the **PRG Port** is set to **9727**
 - b. Verify the **CAP Host** is set to **localhost** and the **Port** is set to **6991**
 - c. Click **Start**.



The Message Count displayed at the bottom of the PRG2CAP window should start incrementing. If the Message Count does not start incrementing, return to ProRAE Guardian and make sure Cascade Out... is in the System Information window and that the instrument data is updating (currently being collected) in ProRAE Guardian.



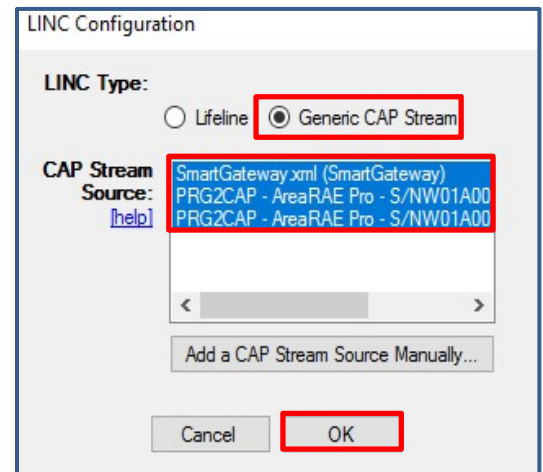
Creating a Survey Controller Run with ProRAE Guardian Instruments

Generic CAP Streams are added when a run is being created in VIPER Survey Controller's 'Run Configuration Wizard'. It is very similar to the way LINC/instruments are added.

1. Start a new run in Survey Controller.
2. After entering the Run Name and Description, in the Add LINC/Instrument dialog box, select '**Generic CAP Stream**' as the LINC Type. The instruments from ProRAE Guardian should appear, as well as any other Generic CAP streams, such as the Smart Gateway MeterApp or the NOAA MeterApp (if running).

This list is updated in real-time as Survey Controller receives data. If an instrument is missing, it may take a few moments for PRG2CAP to receive that instrument's data from the ProRAE Guardian software. Wait until all desired instruments are listed.

3. Select the desired instrument(s) using the 'Control Click' and/or 'Shift Click' allowing multiple instruments to be selected.
4. Click **OK** when the desired instruments are selected.
5. Click **Next** through the Survey Controller wizard and make any other necessary changes, such as identifying the AreaRAE locations, selecting reading intervals, etc. (see Viper User Guide, Section Three – Part E for additional information). When all changes have been made, click Finish. Answer **Yes** to 'Start Recording Data Now'.



Tips, Tricks and Troubleshooting

- RAE Systems has a service called 'Care Center SVC' that also listens in on Port 9727. If there is a conflict, change the Port in ProRAE Guardian and PRG2CAP to 9728.
- If no instruments appear when adding a LINC/Instrument, PRG2CAP is not sending CAP to Survey Controller. The issue is either between the ProRAE Guardian software and PRG2CAP, or between PRG2CAP and Survey Controller. Verify in ProRAE Guard | Systems Options that the data is 'Cascading Out'.
- PRG2CAP also writes an error log next to its executable (.exe) for troubleshooting purposes.