EnviroPoint®

be assured

Wireless Environmental Monitoring from NVSI®

EnviroPoint™ powered by accsense®

administration manual

ENVIROPOINT Standard

EnviroPoint®

be assured

revision record.

Revision	Issue date	Nature of Amendment	Section No	Originator
1 Draft 1	31 Jan. 07	Initial Version	All	MR
1-0	14 March 2007	Release	All	RJD
1-0-3	14 June 2007	Revision	All	MHL
1-0-4	20 July 2007	General Review / New Document Numbering	All	MJR
1-0-50	09 Oct 2007	New Software Release	N/A	MJR
Revision 1	28 Sep 2008	General Review / New Document Numbering	All	RJD/SGC/ PAM

EnviroPoint®

be assured

contents

1 ENVIROPOINT THEORY

1.1 The Network

The Accsense Wireless Solution network is based on the IEEE 802.15.4 standard, unlike WiFi routers that are based on IEEE 802.11. The radio, which uses a 2.4 GHz ISM band, has 16 channels but utilizes the quietest channel based on a scan.

Because the gateway communicates with up to sixteen sensor pods via radio frequency transceivers, it is important that the gateway be located within range of at least one pod. The gateway and pod(s) form a mesh network which enables each pod to function as a repeater for others [(Figure 1-1-1)]. Pods can relay messages with a maximum transmit range of 80 meters (260 ft) between two pods or the gateway [assuming 2.2db antennas aboveground in Line of Sight, a range of up to 300m can be achieved with a 9db antenna]. This distance may be shorter indoors or in an area with lots of radio noise, or longer in mines or straight tunnels.

[1]

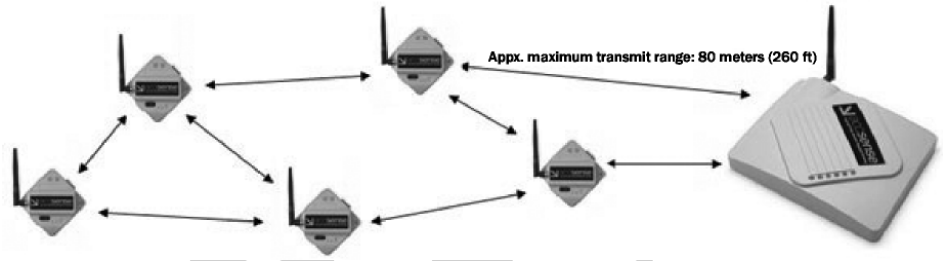


Figure 1-1-1 Maximum operating range using 2.2dBi antennas between the Gateway and/or Sensor Pods is approximately 80 meters (260 ft). [1]

Each pod must be associated to a gateway to relay sensor information back to the network. Since the pods do not necessarily communicate directly with the gateway, each one must establish a permanent identification with the gateway so the gateway can recognise which pod the information originated from. Associations are formed by effectively introducing the pod to the gateway which it will report to, prior to placing the gateway in its physical network location.

1.2 Coexistence

Coexistence of an 802.15.4 Accsense Solution in the presence of other wireless infrastructure, particularly Wi-Fi.

1.2.1 RF Telemetry Product Facts

Wireless Standard: IEEE 802.15.4
Frequency Band: 2.4GHz Industrial, Scientific, and Medical
Frequencies Used: 2405 MHz - 2480 MHz, 16x 3MHz Channels Spaced 5MHz
Transmit Power: 0 dBm (0.79mW)

Accsense understands that customers considering the installation of a wireless monitoring system may have concerns with implementing another wireless technology in their facility. Will the new technology work in an already crowded wireless spectrum? Will the technology interfere with existing wireless infrastructure such as 802.11 Wi-Fi, Building Automation Systems or wireless telephones? The quick answer is "yes". The system will work in the presence of other wireless equipment and Accsense communication protocols were specifically designed with a "good neighbour" policy in mind. No interference is an integral part of an Accsense Fast & Easy system deployment.

1.2.2 General Technical Information

Accsense products utilize the unlicensed the 2.4GHz global Industrial, Scientific, and Medical band employing the IEEE 802.15.4 communications standard, popularized by Zigbee (which Accsense has chosen not to adopt).

1.2.3 Channel Spacing

Channel spacing is the single most effective way to passively mitigate interference between wireless products, including an Accsense system and Wi-Fi. There are sixteen 802.15.4 channels to choose from, each having a bandwidth of 3MHz and a spacing of 5MHz. Figure 1-1-2 illustrates that even in a typical Wi-Fi deployment utilizing channels 1, 6, and 11, there are four remaining clear channels that Accsense products may choose.

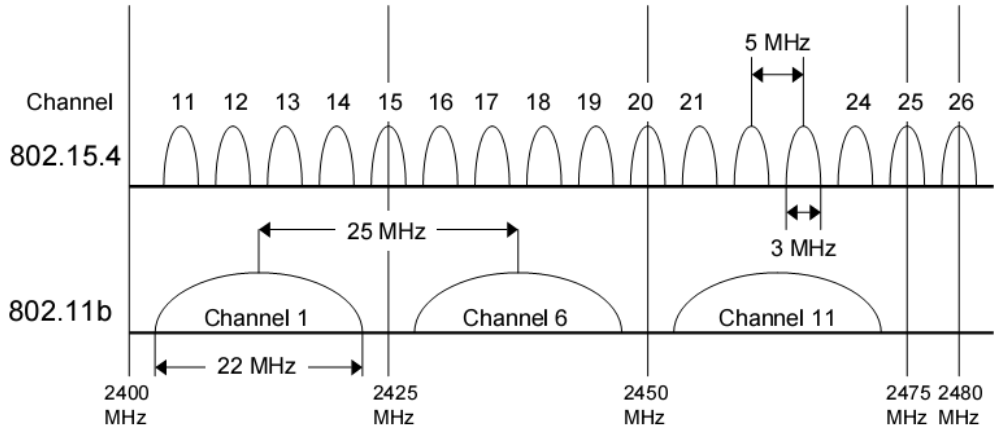


Figure 1-1-2 802.15.4 and 802.11 Frequency Comparisons

The first time an Accsense Gateway is powered on it will scan all available channels and automatically detect and choose to use the one with the quietest radio noise. Customers may verify the channel selected and re-assign the system to another channel using the supplied "Remote Gateway Configuration Utility."
Although the calculations are outside the scope of this document, the 802.15 Task Group 4 (designers of the IEEE 802.15.4 standard) simulated the importance of physical equipment spacing. With a 47+ MHz carrier offset the equipment must only be spaced apart by 0.8 meters to achieve frame error rates less than 10% WITHOUT the use of CCA algorithms (see section 1.2.6).

1.2.4 Duty Cycle

Because Accsense is transmitting a very small amount of data and doing so very infrequently, transmissions have an extremely low duty cycle. In typical installations the duty cycle of Accsense hardware is about 0.0003%, equivalent to a 1ms transmission during each 5 minute interval. The rest of the time the radio is completely powered off and no interference can result. This transmission is synchronized to reduce interference.

1.2.5 Transmit Power

Accsense products have an extremely low transmit power of 0dBm, equivalent to 0.79mW. Emitting less power than a typical Bluetooth headset, and significantly less power than the average Wi-Fi node (usually 100-200mW), Accsense equipment will always lose in a "shouting match" and the amount of electromagnetic radiation is low enough to have an insignificant impact on existing equipment, particularly when coupled with proper frequency spacing. However, as discussed below, the Accsense protocol is very robust and can withstand high noise environments with intelligent built-in retry algorithms.

1.2.6 Clear Channel Assessment

Accsense products incorporate a Clear Channel Assessment (CCA) mechanism which forces the pod to wait to send data until the frequency is determined to be clear. By employing such carrier energy detection, the possibility for interference and collisions is significantly reduced. When coupled with low transmission duty cycles (discussed below), low power and proper frequency spacing, CCA makes a small problem even smaller. If CCA mechanisms fail, and a packet is dropped, retries exist.

1.2.7 Modulation

Accsense products rely on a very robust modulation technique known as Phase-Shift Keying (PSK), instead of Frequency-Shift Keying (FSK) used in Bluetooth and other inexpensive two-way data solutions. Accsense Offset Quadrature-PSK offers extremely good low bit error rate (BER) performance at low Signal-to-Noise Ratios (SNR), especially valuable in noisy radio environments.

Figure 1-1-3 compares the performance of the 802.15.4 (depicted as Zigbee) technique to Wi-Fi, Bluetooth and other proprietary FSK modulation formats.

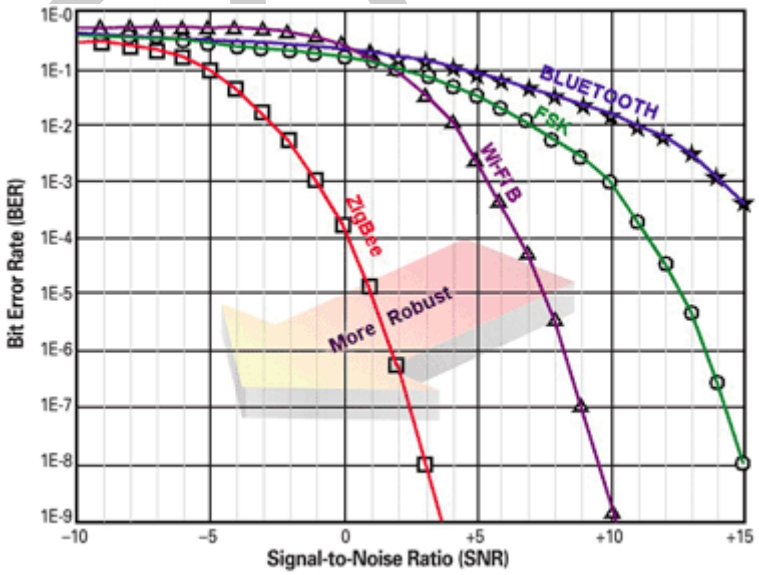


Figure 1-1-3 Comparison of modulation techniques at various SNRs

Proper frequency selection, the extremely low duty cycles and transmit power coupled with the active coexistence CCA mechanisms and modulation make Accsense a "good neighbour" and allow it to thrive in high radio noise environments.

1.2.8 Wireless Communications

When a system is first configured, each sensor pod is "bound" to a single gateway through a simple association procedure. During this process, the gateway and pod store each other's serial numbers to memory and then only communicate with each other. This is a similar concept to MAC address filtering in Wi-Fi networks. In addition to the hardware address-based filtering, a pod also acquires a unique network (PAN) ID and radio frequency channel (from the gateway) during the association process. The gateway will not accept data from another PAN ID or radio channel, resulting in a redundant binding between pod and gateway.

With the methods outlined above, mischievous exploits are nearly impossible. For example, for any faulty or fake data to be sent to the gateway, the attacker would have to ascertain obscure hardware, know the PAN ID, determine the channel and know the serial number of the pod— extremely difficult, if not impossible, to accomplish. In addition, the attacker would have to synchronize transmissions perfectly with wireless communications which is asleep more than 99.9% of the time in order to conserve battery.

1.2.9 Linking between Wireless and Wired Networks

A major point of concern for IT professionals is whether or not an attacker could leverage the Accsense wireless network to gain access to a wired network. The resounding answer is, "No." Within the gateway, the link between the wireless and wired networks is a single low bandwidth RS232 connection that is well controlled and secured. The serial connection links the two main processors of the gateway: One communicates with and controls the wireless network, referred to as the Gateway Radio Control Module (GRCM), and the other receives/transmits data over the internet to the Accsense servers referred to as the Gateway Host Processor (GHP). On the host processor side, this port is not configured to operate as a Unix/Linux console (no pseudo terminal access) and is controlled by a proprietary application written and maintained by Accsense. This proprietary application controls the GRCM using a proprietary console based protocol. This proprietary console based protocol would reject any malicious or unexpected code sent over the wireless and not allow it to pass onto the Ethernet.

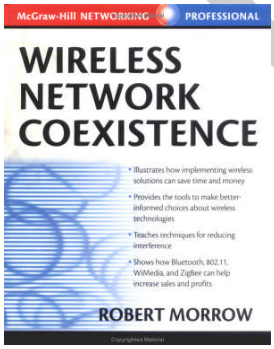
1.2.10 Additional References

There are many valuable internet resources available discussing the coexistence of wireless networks including the following articles:

"Worry Free Wireless Networks" by Terry Hubler
http://www.us.sbt.siemens.com/bau/products/Wireless/HPACEprint.pdf

"IEEE Standard 802.15.4" by Jon Adams
http://www.embedded-computing.com/departments/zigbee/fall_04/

Zigbee Alliance FAQ
http://www.zigbee.org/en/about/faq.asp



Additionally, the book entitled "Wireless network Coexistence" by Robert Morrow and published by McGraw-Hill (ISBN 0-07-139915-1) contains a comprehensive and detailed look at the associated issues.

1.3 Hardware Setup

An Accsense gateway requires an RJ45 Ethernet connection. By default, the gateway is set to acquire its IP address dynamically from a DHCP server and connect to the Accsense web server. The communication between the Accsense gateway and the internet servers is done using the HTTPS protocol over port 443, the same as secure web traffic. The communication is encrypted using SSL, the same technology used for transmitting credit card information over the web. To use the *EnviroPoint* server the gateway has to be reconfigured using the Gateway Configuration Utility.

1.3.1 Accsense Gateway Configuration Utility

The gateways come configured with factory default settings for network connection properties. The *EnviroPoint* Server requires the use of fixed IP addressing. This means you will need to install the Gateway Configuration Utility, as described in section 1.4.5.1 of the Installation Manual, to customize the network settings on each of the gateways to suit your network.

The communication from the gateway is only outbound therefore the gateway does not require an external IP address or an opening in a corporate firewall. However, the gateway has no support for proxy servers and cannot act as a proxy client. In environments where proxy servers are used, the customer must set up a router to act as the proxy client for the gateway.

The wireless communications employed by Accsense are 2.4GHz, but use different frequencies and protocols from Wi-Fi, thus it will not cause interference nor is it an “opening” for attackers to gain access to a corporate network.

1.3.2 Status Indicators.

a) Gateway LED Status indicators

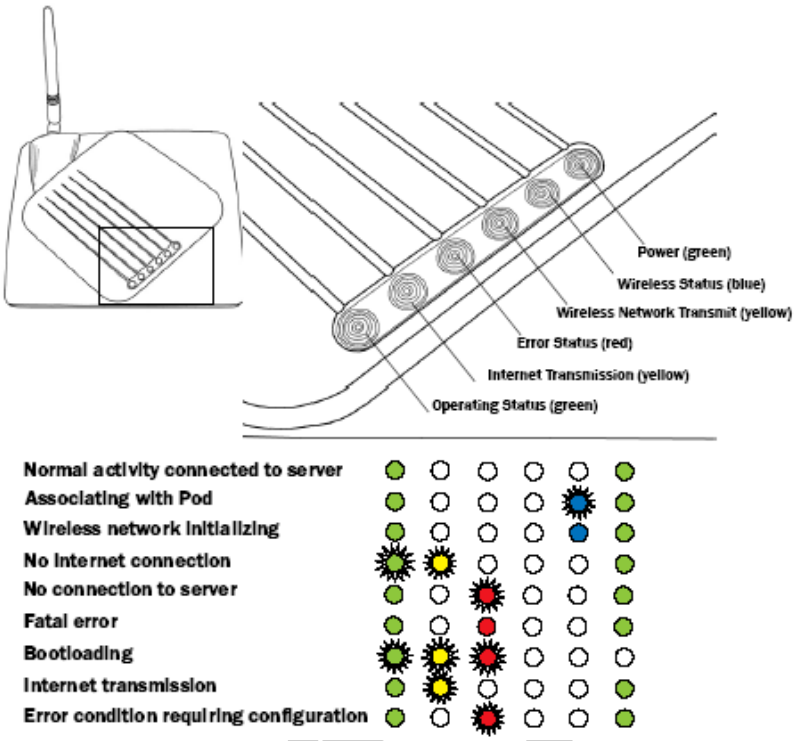


Figure 1-1-4 LED status indicators for Gateway [1]

b) Sensor Pod LED Status Indicators

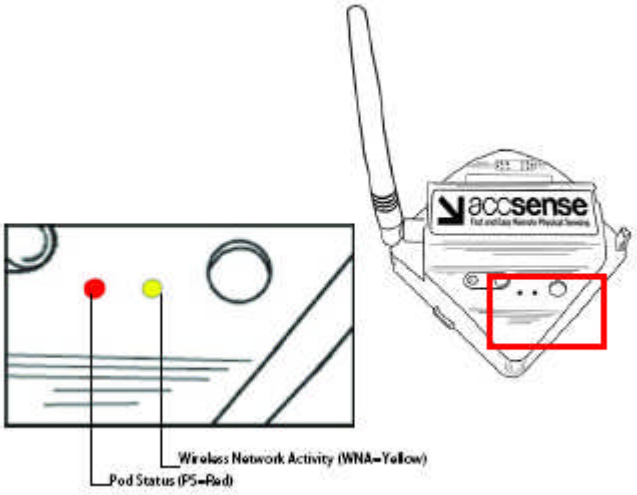


Figure 1-1-5 LED status indicators for Sensor Pod [1]

Pod LED Status	Description
WNA and PS stay constantly lit for 9–30 seconds	Power on
PS stays lit for approx. 1 sec. (WNA may also flash)	Power off
WNA flashes at random rate	Wireless network activity
PS flashes on four times rapidly	Associate button held down for 4+ sec
PS flashes twice, rapidly	Associate button held down for less than 4 sec
PS flashes fast	Attempting to talk to Gateway "association" network
PS flashes medium	Attempting to join Gateway wireless network
PS flashes slow	Attempting to switch to Gateway network
WNA and PS both flash rapidly	Sensor Pod failed to join network
WNA and PS both stay lit constantly for 9–30 sec.	Sensor Pod succeeded in joining network NOTE: See "Power on" (above)
PS flashes twice, rapidly	Sensor pod unable to successfully send a message

Table 1-1 LED messages for Sensor Pod [1]

1.3.3 Location

Gateway location is limited only to places with access to a power outlet and an Ethernet connection. Sensor Pods are limited only by the range and signal quality characteristics of wireless transmission protocols. The physical characteristics of wireless communications across the *EnviroPoint* network will vary greatly between installations. In general terms each pod must be placed within 80 meters (260 feet) of its associated gateway or another pod associated with the same gateway. This distance assumes an outdoor installation with no physical obstructions

between the equipment and using a 2.2dBi (standard supply) antenna. If using 5, 7 or 9dBi antennas, the maximum range may be increased to 300m. Trees, structures, walls within structures, vehicles, people and many other permanent or temporary intrusions between equipment will act to reduce the effective range of wireless communication. Thus the physical location of each Sensor Pod in relation to both the measured variable and other *EnviroPoint* equipment must be carefully planned. It is recommended that you seek the advice of your distributor when planning the physical layout and consistency of your *EnviroPoint* network.

There are documents on the installation CD, under the directory entitled "Go with Product", which can be used as a guide. These documents do not act as an instruction manual but are intended to provide additional information and highlight some of the issues to be considered when planning the layout of a wireless communication network.

The sections below also provide a brief account of the factors that may impact the effective communication range of wireless devices and outline the steps that should be taken when designing a network layout.

1.3.4 Attenuation Basics

Attenuation is simply a reduction of signal strength during transmission. Attenuation is represented in decibels (dB), which is ten times the logarithm of the signal power at a particular input divided by the signal power at an output of a specified medium. For example, an office wall (medium) that changes the propagation of an RF signal from a power level of 10 milliwatts (input) to 5 milliwatts (output) represents 3 dB of attenuation. Consequently, positive attenuation causes signals to become weaker when travelling through the medium.

When signal power decreases to relatively low values, the receiving 802.11.4 radio will likely encounter bit errors when decoding the signal. This problem worsens when significant RF interference is present. The occurrence of bit errors causes the receiving 802.11.4 station to refrain from sending an acknowledgement to the source station. After a short period of time, the sending station will retransmit the frame. At worst case, signal power loss due to attenuation becomes so low that the system will lose connectivity to the network gateway.

The signal strength indicator is the Link Quality Indication (LQI) measurement based on the bit error rate [BER] of the current packet being received from the previous hop of the inbound route, so that it provides information specific to the link-layer connection to the neighbouring device relaying the current packet to the local device.

Causes of attenuation, both signal frequency and range between the end points of the medium, affect the amount of signal reduction. As the range increases, attenuation increases. Attenuation in outdoor applications is based on straightforward and basic free space but indoor applications can be very complex to calculate. In both cases loss formulas can be used (see *Equation 1* and *Equation 2*). The main reason for the indoor difficulty is that indoor signals bounce off obstacles and penetrate a variety of materials that offer varying effects on attenuation (see *Table 1-2 Obstacle attenuation).*

1.3.5 Free Space Loss Formulas

$$\lambda := \frac{c}{f} \qquad \text{Range}(PL) := \frac{\lambda}{4 \cdot \pi} \cdot 10^{\frac{PL}{20}}$$

Equation 1-1 Free space range

$$\mathrm{PathLoss}(r) := 20 \cdot \log\left(\frac{4 \cdot \pi \cdot r}{\lambda}\right)$$

Equation 1-2 Path loss

Items with losses to be added	dB
Human body	3
Cubicles	3 to 5
Marble	5
Window, Brick Wall	2
Glass Window (non tinted)	2
Clear Glass Window	2
Office window	3
Glass wall with metal frame	6
Metal Frame Glass Wall Into Building	6
Metal Frame Clear Glass Wall	6
Metal Screened Clear Glass Window	6
Wired-Glass Window	8
Brick Wall next to a Metal Door	3
Plasterboard wall	3
Cinder block wall	4
Dry Wall	4
Cinder Block Wall	*4*
Sheetrock/Wood Frame Wall	5
Sheetrock/Metal Framed Wall	6
Office Wall	6
Brick Wall	2 to 8
Concrete Wall	10 to 15
Wooden Door	3
Metal door	6
Metal Door in Office Wall	6
Metal door in brick wall	12 to 13

Table 1-2 Obstacle attenuation

As a result, it's often necessary to perform an RF site survey to fully understand the behaviour of radio waves within a facility before installing wireless network gateways.

The ultimate goal of an RF site survey is to supply enough information to determine the number and placement of pods and wireless network gateways to provide adequate coverage throughout the facility. An RF site survey also detects the presence of interference coming from other sources that could degrade the performance of the system.

The need and complexity of an RF site survey will vary depending on the facility, e.g. a small three room office may not require a site survey. The site will probably get by with a single wireless network gateway located anywhere within the office and still maintain adequate coverage. A larger facility, such as an office complex, apartment building, hospital or warehouse, generally requires an extensive RF site survey. Without a survey, the system may end up with inadequate coverage and suffer from low performance in some areas. When conducting an RF site survey, consider these general steps:

1. **Obtain a facility diagram.** Locate a set of building blueprints, if possible. If none are available, prepare a floor plan drawing that depicts the location of walls, walkways, etc.

2. **Visually inspect the facility**. Be sure to walk through the facility before performing any tests to verify the accuracy of the facility diagram. This is a good time to note any potential barriers that may affect the propagation of RF signals, e.g. a visual inspection will discover obstacles such as metal racks and partitions - items that blueprints don't show.

3. **Identify user areas.** On the facility diagram, mark the areas where fixed and mobile pods are to be placed. In addition to illustrating where mobile pods may be moved around, indicate where they will not go. The system may require fewer wireless network gateway points if roaming areas can be limited.

4. **Determine preliminary access point locations**. By considering the location of pods and range estimations between pods and gateways, approximate the locations of gateways to provide adequate coverage throughout the area (preliminary location).
   Consider mounting locations, which could be vertical posts or metal supports above ceiling tiles. Be sure to recognize suitable locations for installing the access point, antenna, data cable and power line. Also think about different antenna types when deciding where to position access points. An access point mounted near an outside wall, for example, could be a good location if a patch antenna with relatively high gain is oriented within the facility.

5. **Verify access point locations.** This is when the real testing begins. It's a two-person job. Install a wireless network gateway at each preliminary location and monitor the signal strength indicator readings by walking with a pod for varying distances away from the access point.
   Take note of data rates and signal readings at different points as the pod is moved to the outer bounds of the gateway's coverage. In a multi-floor facility, perform tests on the floor above and below the access point. Keep in mind that a poor signal quality reading likely indicates that RF interference is affecting the system. Based on the results of the testing, you might need to reconsider the location of some access points and retest the affected areas.

6. **Document findings.** Once satisfied the planned location of access points will provide adequate coverage, identify on the facility diagram the recommended mounting locations. The installers will need this information.

These steps will point you in the right direction but experience really pays off. If you're new to wireless systems, you'll begin to build intuition about the propagation of radio waves after completing several RF site surveys.

NOTE: Underground tunnels act as wave guides giving far greater ranges than above ground. Metal ceilings have been found to behave similarly.

RF interference is still plaguing wireless system deployments. The perils of interfering signals from external RF sources are often the culprit. As a result, it's important that you're fully aware of RF interference impact and avoidance techniques.

1.3.6 Signal Fading

RF signal fading is caused by several factors including: Multipath Reception, Line of Sight Interference, Fresnel Zone Interference, RF Interference and weather conditions.

Multipath Reception – The transmitted signal arrives at the receiver from different directions, with different path lengths, attenuation and delays. An RF reflective surface, like a cement surface or roof surfaces, can yield multiple paths between antennas. The higher the antenna mount position is from such surfaces, the lower the multiple path losses. The radio equipment in the 802.11.4 specification utilizes modulation schemes and reception methods such that multiple path problems are minimized.

Line of Sight Interference – A clear, straight line of sight between system antennas is absolutely required for a proper RF link for long distances outdoors. A clear line of sight exists if an unobstructed view of one antenna from the other antenna exists. A radio wave clear line of sight exists if a defined area around the optical line of sight is also clear of obstacles. Remember that the electric and magnetic fields are perpendicular to the direction of propagation of the RF wave. In setting up wireless networks in buildings, propagation of the RF signal through walls and other items is a fact of life. If you recall the signal attenuation discussion earlier, we can evaluate the related losses. The preceding Table 1-2 presents loss values for typical items through which we want our networks to transmit and receive.

Fresnel Zone Interference – The Fresnel (FRAY-nel) Zone is a circular area perpendicular to and centred on the line of sight. In radio wave theory, if 80% of the first Fresnel Zone is clear of obstacles, the wave propagation loss is equivalent to that of free space.

RF Interference – This was dealt with earlier.

Weather Conditions – At 2.4GHz, most showers of rain can be penetrated with ease.

1.3.7 System Operating Margin (SOM)

SOM (System Operating Margin), also known as ***fade margin***, is the difference of the receiver signal level in dBm minus the receiver sensitivity in dBm. It is a measure of the safety margin in a radio link. A higher SOM means a more reliable over-the-air connection. It is usually recommended to include a minimum of 10 dB to 20 dB SOM and in this system we recommend 18db.

1.3.8 Shadowing

Shadowing is the effect where the received signal power fluctuates due to objects obstructing the propagation path between transmitter and receiver. These fluctuations are experienced on local-mean powers, that is, short-term averages can be used to remove fluctuations due to shadowing.

To put this in contrast, in most papers on mobile propagation, only 'small-area shadowing' is considered: log-normal fluctuations of the local-mean power are measured when the antenna moves over a distance of tens or hundreds of metres. Marsan et al. reported a median of 3.7 dB for small area shadowing. Preller and Koch measured local-mean powers at 10 m intervals and studied shadowing over 500 m intervals. The maximum standard deviation experienced was about 7 dB, but 50% of all experiments showed shadowing of less than 4 dB.

For the *EnviroPoint* system up to 100m, we recommend 3.7dB.

1.3.9 Link Budget

A link budget is the accounting of all of the gains and losses from the transmitter through the medium (free space, walls, etc.) to the receiver in the system. It takes into account the attenuation of the transmitted signal due to propagation, as well as the loss, or gain, due to the antenna. A simple link budget equation looks like this:

Received Power (dB) = Transmitted Power (dBm) + Gains (dB) - Losses (dB)

Equation 1-3 Link budget

NVSI provides an Excel spread sheet to assist with the calculation for each path loss in the RF mesh plus, included here, is an example from the National Artillery Museum at North Head, Sydney, Australia.

Figure 1-1-6 Artillery Museum installation shows the proposed layout with distances, pod type and external antenna placement. The final system had an underground component and required only 3 specialist antennas above ground due to roof skylights in three of the buildings, allowing RF signals to enter and exit.

The following table shows the link budget and margin calculations for the system. Note that distance G of 120m has a link budget that is reasonable but is calculated in the second half of the table to be outside the standard pod range; E and O are marginal.

Tx = transmitter
Rx = receiver

Link	Distance (m)	Tx Pwr	Rx Sensi-tivity	Tx AntG	Tx Coax	Rx AntG	Rx Coax	Fading Margin	Loss	Link Budget
A	***90.9***	-1	-94	9	0	9	0	18	5	88
B	***27.9***	-1	-94	9	0	9	0	18	12	81
C	***25.3***	-1	-94	9	0	9	0	18	11	82
D	***27.7***	-1	-94	9	0	9	0	18	11	82
E	***86.6***	-1	-94	9	3	9	0	18	5	85
F	***69.3***	-1	-94	9	0	9	0	18	6	87
G	***120***	-1	-94	9	0	9	0	18	11	82
H	***65.4***	-1	-94	9	3	9	0	18	5	85
I	***94.1***	-1	-94	9	0	9	0	18	5	88
J	***57.7***	-1	-94	9	0	9	0	18	5	88
K	***72.4***	-1	-94	9	3	9	0	18	5	85
L	***39.6***	-1	-94	9	3	9	0	18	0	90
M	***63***	-1	-94	9	3	9	0	18	5	85
N	***38.5***	-1	-94	9	0	9	0	18	10	83
O	***102.2***	-1	-94	9	3	9	0	18	5	85
P	***30.6***	-1	-94	9	0	9	0	18	10	83
Q	***59***	-1	-94	9	3	9	0	18	5	85

R	***52.1***	-1	-94	9	0	9	0	18	10	83

Link	Range (m)	Margin (m)	Margin (db)	*Shad-owing*	*Link Budget*	*Range (m)*	*Margin (m)*	*Margin (db)*
A	241.6	150.7	**8.5**	*3.7*	*84.3*	*157.8*	*66.9*	***4.8***
B	107.9	80.0	**11.8**	*3.7*	*77.3*	*70.5*	*42.6*	***8.1***
C	121.1	95.8	**13.6**	*3.7*	*78.3*	*79.1*	*53.8*	***9.9***
D	121.1	93.4	**12.8**	*3.7*	*78.3*	*79.1*	*51.4*	***9.1***
E	171.1	84.5	**5.9**	*3.7*	*81.3*	*111.7*	*25.1*	***2.2***
F	215.4	146.1	**9.8**	*3.7*	*83.3*	*140.7*	*71.4*	***6.1***
G	121.1	1.1	**0.1**	*3.7*	*78.3*	*79.1*	*-40.9*	***-3.6***
H	171.1	105.7	**8.4**	*3.7*	*81.3*	*111.7*	*46.3*	***4.7***
I	241.6	147.5	**8.2**	*3.7*	*84.3*	*157.8*	*63.7*	***4.5***
J	241.6	183.9	**12.4**	*3.7*	*84.3*	*157.8*	*100.1*	***8.7***
K	171.1	98.7	**7.5**	*3.7*	*81.3*	*111.7*	*39.3*	***3.8***
L	304.2	264.6	**17.7**	*3.7*	*86.3*	*198.7*	*159.1*	***14.0***
M	171.1	108.1	**8.7**	*3.7*	*81.3*	*111.7*	*48.7*	***5.0***
N	135.9	97.4	**11.0**	*3.7*	*79.3*	*88.7*	*50.2*	***7.3***
O	171.1	68.9	**4.5**	*3.7*	*81.3*	*111.7*	*9.5*	***0.8***
P	135.9	105.3	**12.9**	*3.7*	*79.3*	*88.7*	*58.1*	***9.2***
Q	171.1	112.1	**9.2**	*3.7*	*81.3*	*111.7*	*52.7*	***5.5***
R	135.9	83.8	**8.3**	*3.7*	*79.3*	*88.7*	*36.6*	***4.6***

Brick Wall	5	*Shadowing is the effect that the received signal power fluctuates due to objects*
Sheetrock/Metal Framed Wall	6	*obstructing the propagation path between transmitter and receiver.*
Human body	3	

Table 1-3 Link strength calculations at North Head

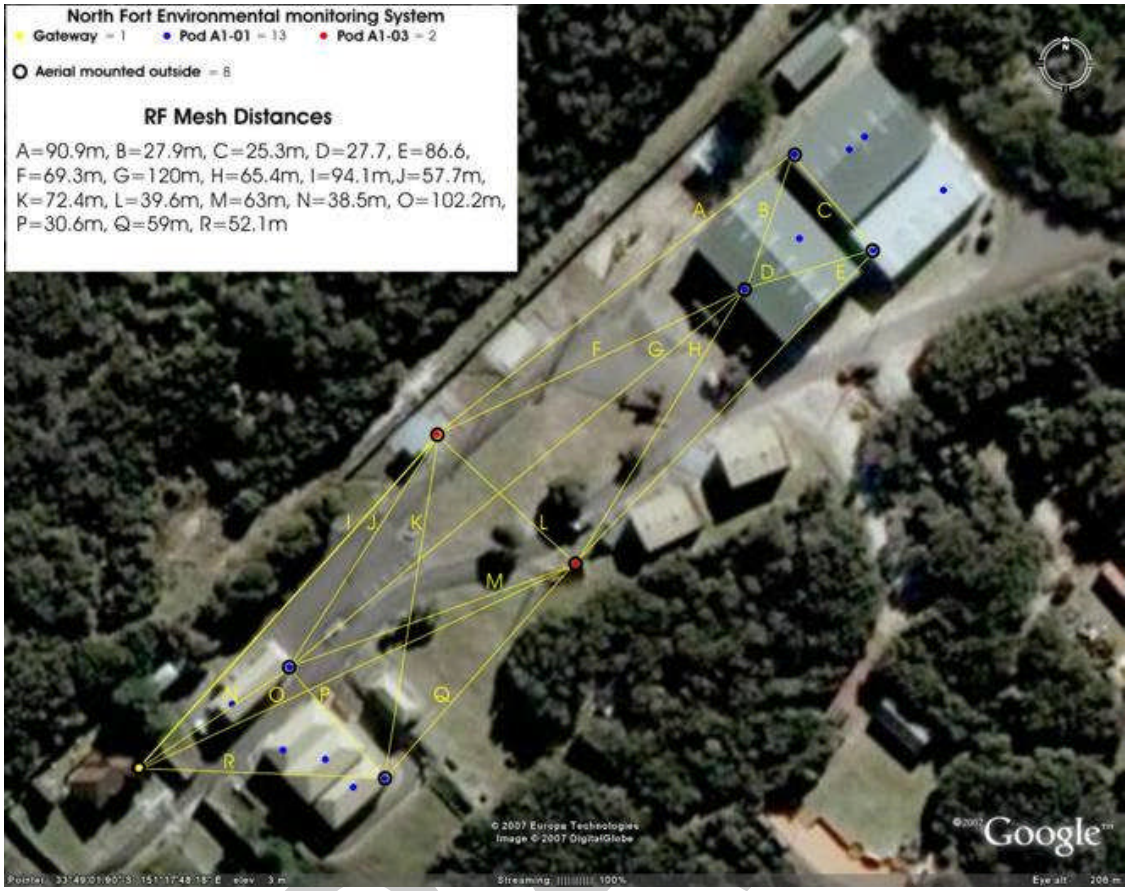


Figure 1-1-6 Artillery Museum installation

2 *ENVIROPOINT* OVERVIEW

Now you've skipped or read the theory, try this: EnviroPoint comprises a fusion of 1 Hardware and 2 Software components.

1. A physical self-contained wireless network of environmental data-monitoring devices developed by Accsense, Inc.

2. A supervisory monitoring and configuration software package developed by Neo Vista System Integrators Pty Ltd.

EnviroPoint is designed for seamless integration with your existing network. By installing the *EnviroPoint* software and using an Ethernet connection to connect to the *EnviroPoint* hardware, *EnviroPoint* becomes a key part of the network.

EnviroPoint is a flexible and powerful environmental monitoring system that is adaptable to monitoring several variables simultaneously from multiple points around the installation site. The power of *EnviroPoint* lies in its scalability. *EnviroPoint* can be configured to measure from one point or, depending on which variation you have purchased, from hundreds of points making it an ideal system for use in both large and small area environments. *EnviroPoint* comes in three variations to provide high quality solutions to meet the needs of a wide range of

customers. The table in Appendix B outlines the features available in the three variations: Lite, Standard and Enterprise.

2.1 Documentation Description

This document is the Administration Manual written to accompany *EnviroPoint* Standard.

This manual should be read by anyone who is responsible for the administration of this system.

Documents included in this package are

1. *EnviroPoint* (Standard) User Guide Manual
2. *EnviroPoint* (Standard) Installation Manual
3. *EnviroPoint* (Standard) Administration Manual

2.2 Components – *EnviroPoint* Standard

- *EnviroPoint* Software
- Accsense Gateway Configuration utility
- *EnviroPoint* Hardware

2.3 On-screen

The main application screen for *EnviroPoint* Configuration is split into two sections. The left hand side displays a tree structure providing intuitive access to the application pages shown on the right hand side of the screen.

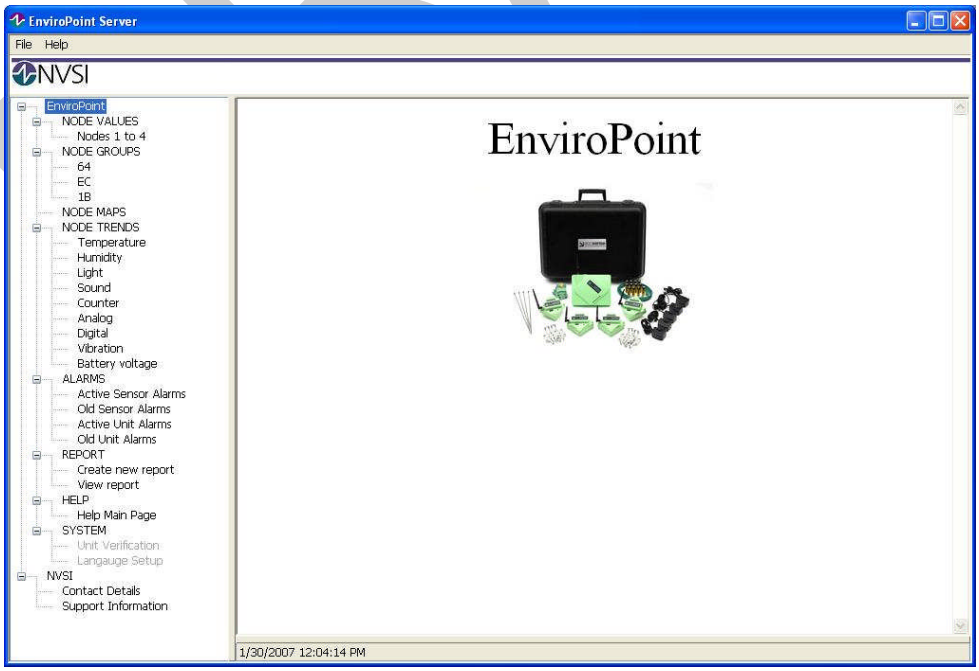


Figure 2-1 The main application screen after configuration

The main screen of Enviropoint is designed to have the look and feel of a web browser.

Each application page is associated with a component of the *EnviroPoint* network. The branches of the tree structure reflect the physical connectivity of the *EnviroPoint* network components, with each level representing a component type.

1. System
2. Node
3. Sensor

2.4 Installation overview

Prior to installing the *EnviroPoint* sensor pods you must install the *EnviroPoint* software and gateways. *EnviroPoint* software has three main components:

1. *EnviroPoint* Database on the server
2. NVSI-Accsense Service on the server
3. *EnviroPoint* Monitor Application on all administrator and user PCs

Each component has a particular role in the system and should be installed on an appropriate machine. Installation instructions and advice for each component can be found in the relevant sections in the Installation Manual.

2.4.1 The *EnviroPoint* Database

The primary role of the database is to maintain the integrity of your *EnviroPoint* system. The database contains both past and present records of measured values, events and system configurations. This data is normally accessed through *EnviroPoint* Monitor. The database is designed to store all historic records in a consistent manner that facilitates traceability.

The database component in *EnviroPoint* Standard should be installed by qualified personnel to ensure the correct configuration.

2.4.2 NVSI-Accsense Service

The NVSI-Accsense Service must be installed on a network server machine that meets the minimum system requirements listed in section 1.2 of the Installation Manual. The service provides the link between the Accsense Gateways and the *EnviroPoint* Database. The service is responsible for relaying incoming measurements and messages to the database, and returning messages and configuration settings to the gateways.

- *EnviroPoint* requires the use of a network-aware service (supplied NVSI-Accsense Service) that must be installed on a central network server. This may be either the same machine as the database server or a separate machine with direct network access to (on the same subnet as) the database server. This machine is referred to as the "*EnviroPoint* Server".
- The *EnviroPoint* network uses SSL encryption for communication which will require the installation of suitable certificates (supplied) in the registry of the *EnviroPoint* Server. This is installed manually to the store. You will need to supply the authentication password to import the certificate.
- *EnviroPoint* requires a certificate of 512bits or greater. The supplied certificate is an unsigned 1024bit.

2.4.3 *EnviroPoint* Monitor

The *EnviroPoint* Monitor application is designed to function as a client application that may be installed on any/all machines in your network. It is responsible for reporting the data recorded by the *EnviroPoint* network. *EnviroPoint* Monitor allows users to receive continuous updates on the system including the current status of the network nodes, the latest data values, historic trends and alarm conditions.

Each instance of the Monitor application requires a connection to the *EnviroPoint* Database to retrieve data and manipulate settings for the *EnviroPoint* Server.
To connect to the database, the Monitor uses a Microsoft Universal Data Link (UDL) file ('Enviropoint.udl') located in the same directory as the executable. Each UDL file stores the information required for the application to locate the appropriate MS SQL 2005 server and connect to the *EnviroPoint* Database.

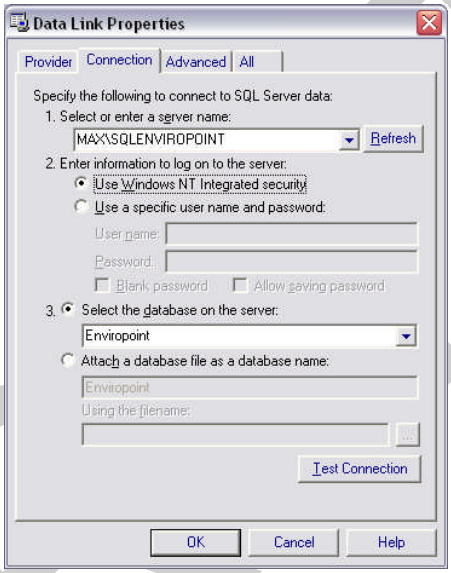


Figure 2-2 UDL screen

It is recommended that users conform to a standard company policy when configuring their UDL file to connect to the server as these files can connect by two different methods: a) Windows authentication and b) SQL authentication (see below).

Section 1.4.9 of the Installation Manual describes the user PC Monitor installation.

2.5 *EnviroPoint* Server User Administration

a) Windows NT Integrated Security utilizes your domain authentication methods to verify the identity of the person connecting to the database. This method connects to the database using the login name of the operating system account which executes the application. Windows authentication is recommended as the most secure way of connecting to your database and is described below.

b) An alternative method is known as SQL authentication and verifies the connection as belonging to a user that has previously been explicitly created in the database server.

2.5.1 Windows Authentication

Integrated security is the simplest and most transparent method (to the user) of controlling the database connection. This method supplies the properties of the currently logged on user to the database. This has the advantage of allowing the creation of operating system security objects such as User Groups for managing permissions given to all users of the *EnviroPoint* System.

To allow users to connect to the *EnviroPoint* Database using integrated security, follow the steps below.

1. Create a User Group on your network domain specifically for *EnviroPoint* users. This will allow administrators to make changes applicable to all users simultaneously.
2. Use MS SQL Management Studio to connect to the SQL 2005 Server which hosts the *EnviroPoint* Database. Your connection must be a member of the 'sysadmin' Server role to make the appropriate changes.
3. Create a new Server Login for the *EnviroPoint* Users Group created in Step 1.
4. Map this Login to the *EnviroPoint* Database and assign the database user to the 'db_datareader' and 'db_datawriter' database roles.

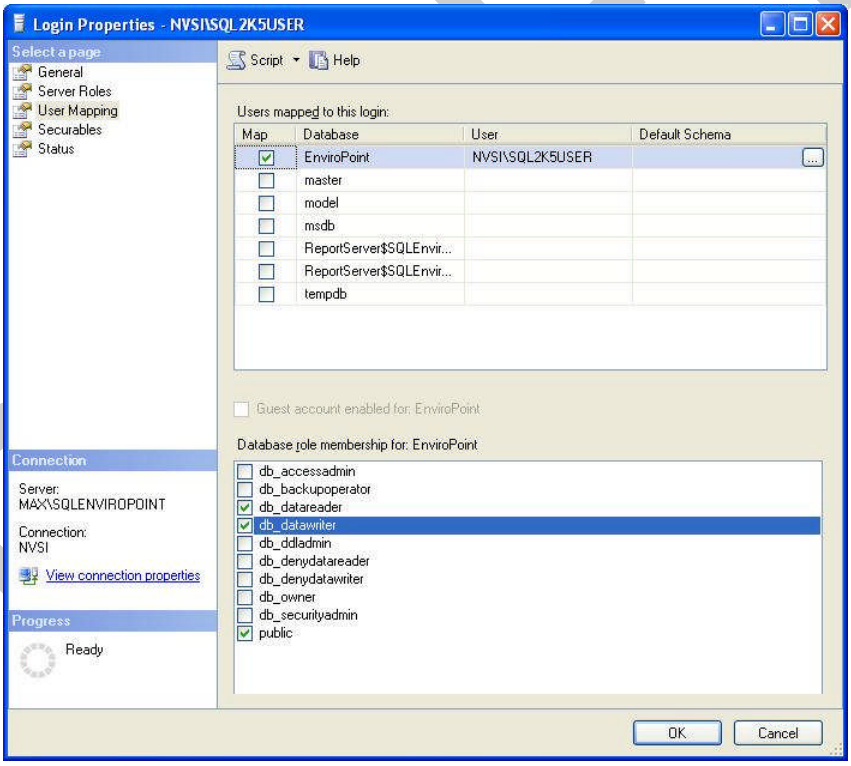


Figure 2-3 Assigning database users

5. After you have created the Login, open the Properties Dialog for the database user created in the *EnviroPoint* Database. In the Securables field you must explicitly grant the 'Execute' permission for this database.

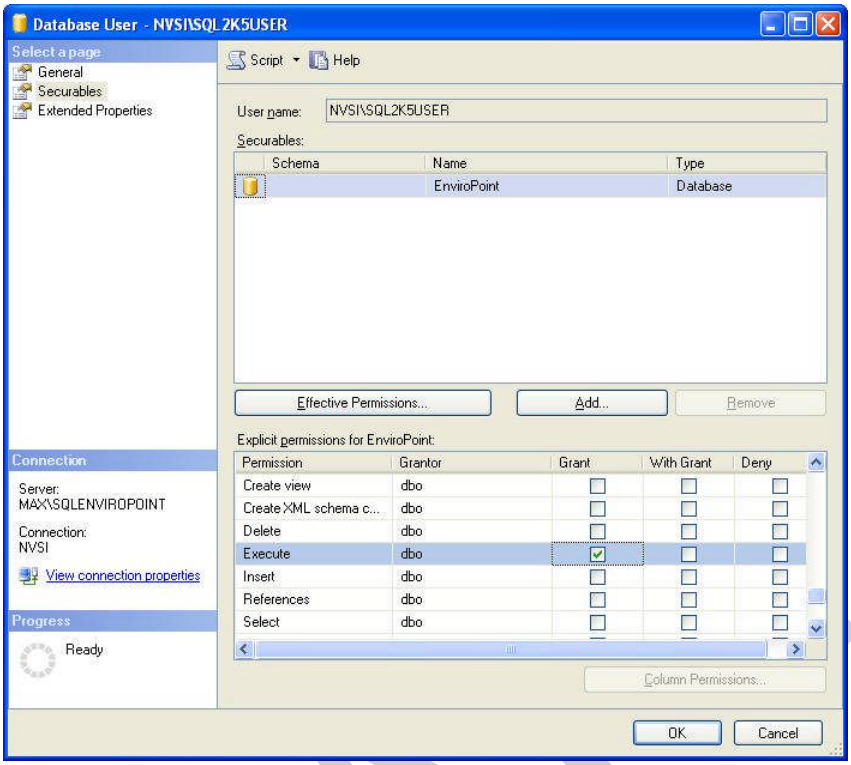


Figure 2-4 Executing Securables

2.5.1.1 User Administration

Access to the *EnviroPoint* Server and Monitor applications is based on user profiles. The Server stores a list of *EnviroPoint* users including user ID, password and access level. As system administrator, you have the highest access level and the ability to manage the profiles of all users on the server. This is done through the Users dialog box. The Users dialog box will appear automatically if there are no user profiles defined. This will occur the first time the *EnviroPoint* Server is run after activation.

At any other time, the Users dialog box can be accessed by selecting “Administrate users” from the file menu.

2.6 Common Maintenance Operations

This section contains instructions for various common procedures.

2.6.1 Data Exporting

You can export data records as an Excel spreadsheet file by selecting Data Export from the tree structure. See the User Guide Manual for more details.

2.6.2 Reports

Reports in EnviroPoint are a very small part of the programme due to there being a full Reporting Services function available in SQL. *EnviroPoint* can produce simple reports, including periodic reports that automatically print, however NVSI recommends SQL Reporting Services should be used if full data manipulation is required.

Here is how to produce a Report Template and Reports in *EnviroPoint*.

2.6.2.1 New Reports

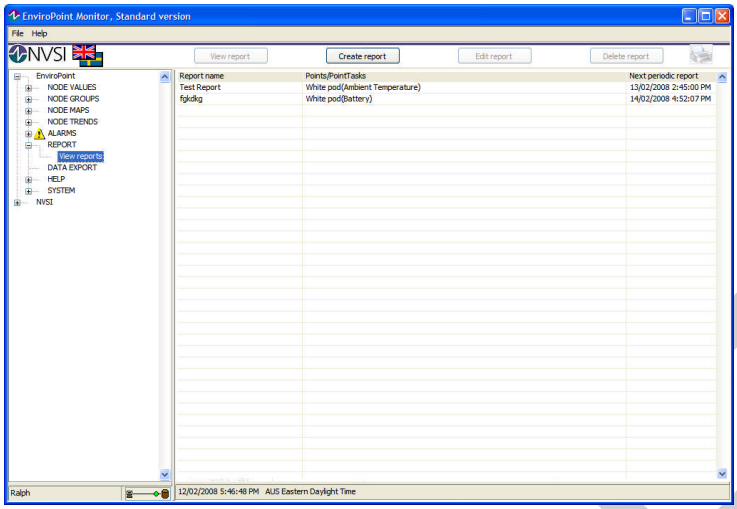


Figure 2-5 Report application page

From the menu tree, open REPORT, then click View reports. Initially the right hand side will be blank. Click the Create report button.

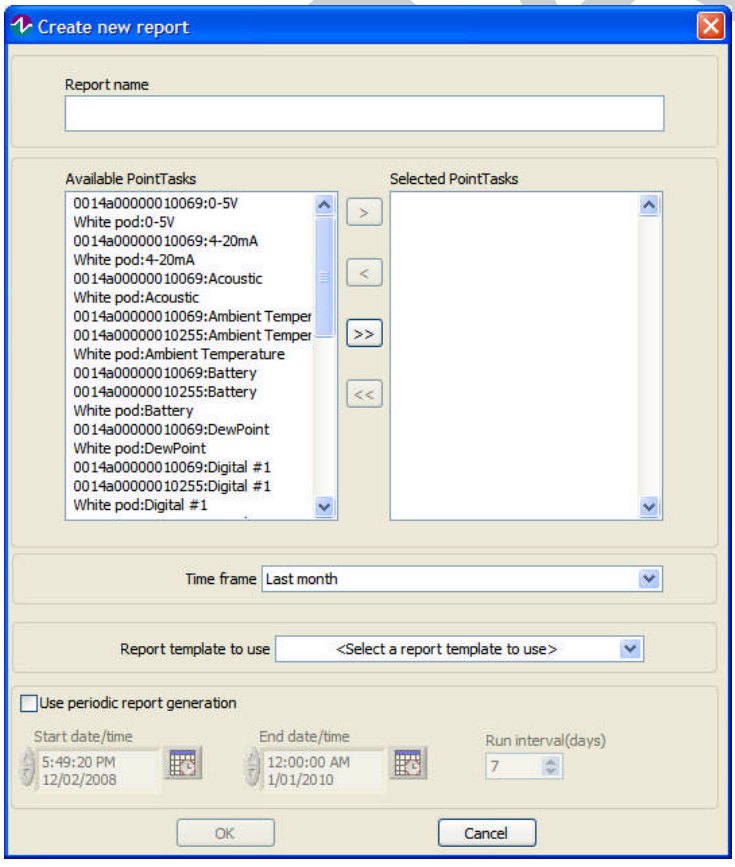


Figure 2-6 Create new report page

Type in the Report name. Then select the trends to be in the report by clicking on the Available Point Tasks, then the single right-pointing arrow (the double arrow selects all data).

Choose a Time frame, then a Report template.

2.6.3 Pod Replacement

If one of the sensor pods is due to be sent away for a calibration check, or if a pod fails, it can be replaced with another pod in the same position. The replacement pod will notify the system that it should be used for readings from that position. This can be done by following these steps:

1. Login to the *EnviroPoint* Server as an administrator
2. Select "Configure Systems" from the file menu
3. In the *EnviroPoint* Configuration window expand the system tree and select the Item Name corresponding to the pod to be replaced.
4. Enter the Unit Serial Number of the replacement pod.
5. Press Change unit.
6. File/Save.
7. Associate the replacement pod with its gateway (Section 1.4.6.2 of the Installation Manual).
8. Physically replace the pod.

2.6.4 Adding new pods and gateways

Short-cut menus attached to each level of the tree structure allow you to create or destroy connected components of the subsequent component type, e.g. accessing the short-cut menu [Right Mouse Button] attached to a system will allow you to add nodes to that system.

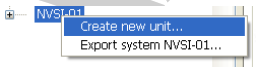


Figure 2-7

To add a gateway to the system, refer to the Installation Manual.

2.6.5 Unit Calibration/Verification

This screen allows you to place units into verification mode. This mode forces the system to ignore alarm settings for this unit and to log data from this unit to an isolated table for the specified verification time period. The time period counts down and, when it has elapsed, the system returns the unit to normal status. Verification mode can be used for testing purposes.

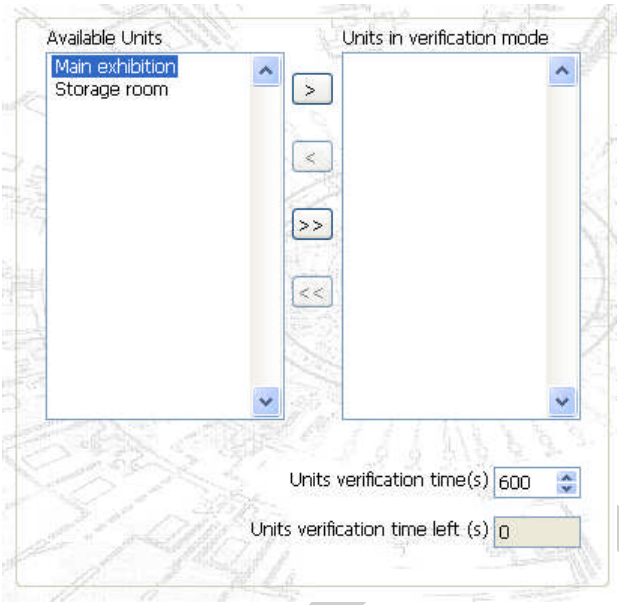


Figure 2-8 Unit verification settings

2.6.6 Setting up alarms

a) Hysteresis

When setting alarm levels, consider the hysteresis necessary to prevent multiple alarms if the parameter hovers around the set limit. For instance, a domestic refrigerator will only begin a cooling cycle when the temperature is slightly above 4°C, and will cool to, perhaps, 3.8°C. The 0.2 degrees is the hysteresis setting for the cooling motor. If too small a hysteresis level is set for an alarm, or none at all, and the parameter moves slightly in and out of the accepted range the result will be ongoing annoying messages that come to be regarded as meaningless (as they are) and future, meaningful alarms may be ignored.

b) Delays

You also need to think about whether alarm delays are required, e.g. when a refrigerator door is opened on a legitimate task. How long should the delay be? Should the same delay be set for an escalation of the alarm?

c) Escalation

Where multiple alarm levels are set for a single parameter, name each one uniquely, otherwise all the alarms will be sent to everyone on the recipient list.

To be written.

2.6.7 Change email addressee/SMS recipient

To be written.

2.6.8 Adding a second system

As administrator, access the short-cut menu [Right Mouse Button] and select Create new system (see Figure 2-9). On the right hand panel there are two tabs to fill in: System information and System configuration. Follow the instructions from section 1.4.4.4 of the Installation Manual to the end of section 1.

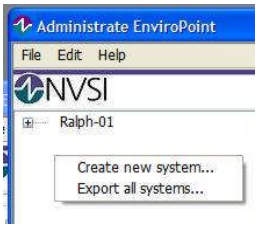


Figure 2-9

2.6.9 Changing between systems

Login to current system using an administrator level user. Select 'Change system…' from the File menu.

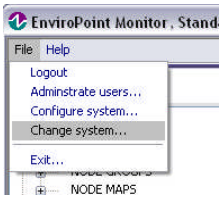


Figure 2-10

Select the System Name from the drop down menu in the 'Configure Database Settings' dialog. Press 'OK'.

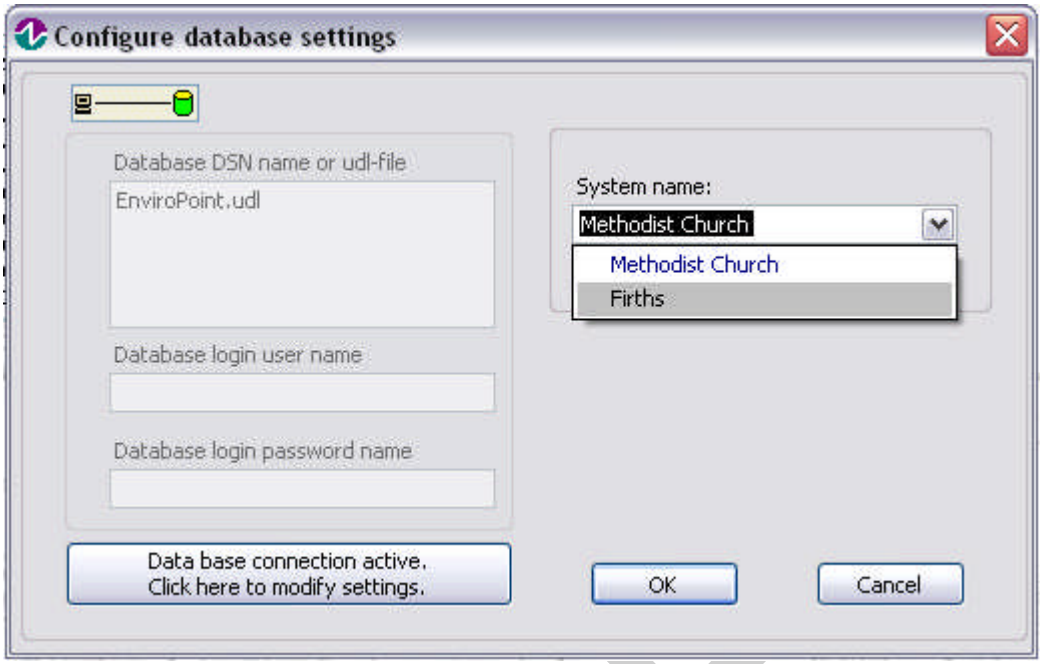


Figure 2-11

When prompted for a Login to the new system press 'Cancel'. Close down and restart EnviroPoint Monitor.

Log in as normal to view the new system.

Repeat these steps to switch back and forth as required.

2.6.10 Custom Database Queries

Individual records of data can be pulled from the SQL Database tables using custom database queries containing the *SELECT* statement. This statement can become quite complex if retrieving data from multiple sources with conditions. As this is the case, only aspects of a statement will be discussed. A new query form can be generated by the user through the 'New Query' option in SQL Server Management Studio. This query can be save as a *.sql file for future use to quickly pull out the latest data in a table.

The fundamental syntax of the *SELECT* statement takes the following form:

SELECT <select_list> FROM <data_source> WHERE <conditions_for_selection>;

The <*select_list*> parameter can take numerous structures. The two most common parameters are '*' option indicating a selection of every piece of data, or a series of column names separated with commas.

i. *SELECT * FROM <data_source> WHERE <conditions_for_selection>;*

ii. *SELECT Column_1,Column_2 FROM <data_source> WHERE <conditions_for_selection>;*

A few other SQL parameters may be used in place of '*' that provide different functionality to the *SELECT* statement. These include the *ALL* and *DISTINCT* parameters. The *ALL* parameter acts in a similar fashion to '*' and selects all entries for a given query, while the *DISTINCT* parameter only selects a single instance of any multiple occurring values within a column.

The <*data_source*> parameter states where the entries used for <*select_list*> come from. This usually consists of a table name. Although multiple tables can be selected, the majority of simple operations can be achieved by referencing only one table.

The *WHERE* statement allows for conditions to be placed on the rows that are returned from the columns specified in the <*select_list*> by introducing a series of expressions into the parameter field. These expressions can refer to a specific value in each of the columns or a range of values.

i.e.

i. *SELECT Column_1 FROM Table_1 WHERE Column_2 = 0;*

ii. *SELECT Column_1 FROM Table_1 WHERE Column_2 > 5 AND Column_2 < 10;*

The other form of these expressions can take the form of a subquery within a *SELECT* such as the following:

i. *SELECT Column_1 FROM Table_1 WHERE (SELECT Column_1 FROM Table_2 WHERE DeviceID = 6) <> NULL;*

In this case the operator '<>' is the standard operator for the phrase 'Not equal to'. It should also be noted that while statements such as these can be constructed, they can prove to be quite cumbersome and a higher level SQL command may be available to accomplish something similar.

In addition to these core SQL concepts there exist two commonly used options that may be added onto a *SELECT* statement that enable any retrieved records to be presented in a useful format. These include the *ORDER BY* clause and the *GROUP BY* clause. These allow data to be sorted with regards to a specific parameter that the user requires. The format of these clauses is presented below:

i. *….WHERE <conditions_for_selection> ORDER BY <user_expression>;*

ii. *….WHERE <conditions_for_selection> GROUP BY <user_expression>;*

After the user expression, the option of *ASC* for ascending order or *DESC* for descending order may be included.

2.7 Trouble shooting

What to do if…

Power cut

Sensor data doesn't update

Pod data reads 0

Several pods aren't updating

Impossible readings

Appendix a – Regulatory Compliance

Australian Communications and Media Authority (ACMA)

EnviroPoint Systems Pty Ltd is an affiliate of Neo Vista System Integrators Pty Ltd, which is the sole Australasian distributor of hardware produced by Accsense, Inc., and is the registered holder of the C-Tick for the hardware. The ACMA awards the C-Tick in recognition of compliance under S.182 of the Radiocommunications Act 1992.

EnviroPoint Systems Supplier Code as listed with ACMA is: **N16909**.

APPENDIX B – *ENVIROPOINT* VARIATION DESCRIPTION

Note: each Node is a Pod or other unit type such as a Web Cam.

***EnviroPoint* Function**	**Lite**	**Standard**	**Enterprise***
EnviroPoint Server Operating System	XP SP2	MS Server 2003 MS Server 2000	MS Server 2003 Enterprise
EnviroPoint Server Database MS SQL Server 2005 Requirement	Express SP1 (Max data 4GByte)	Express SP1 with Advanced Services. Standard Edition. Enterprise Edition.	Enterprise Edition.
Run as a service (PC not required to be logged in)	-	√	√
FDA 21 CFR part 11	-	-	Open System
Server License	Per computer	Per server	Per data centre cluster
Server Installation requirements	Single installer	Requires SQL to be set up & Certificates	Requires SQL to be set up & Certificates
EnviroPoint Monitor Operating System	XP SP2	XP SP2	XP SP2
Monitor Licenses (Concurrent Users)	5	Unlimited Per Site (limited by SQL user CALs)	Unlimited Per Organisation (limited by SQL user CALs)
Monitor Installation requirements	Single installer	Single installer	Single installer
Max Number of Nodes	32	65,536†	1,048,576†
Max Number of Gateways	32	65,536†	65,536†
Software plug-ins for other types of Sensor (i.e. Web Cam)	-	√	√
Web Cam	-	√	√
Node output control (On Pod type A1-08 to A1-10)	-	√	√
Remote Nodes using G3 Mobile connection	-	√	√
Network Security SSL encryption data links	-	√	√
Encrypted Database Tables	-	-	√
Gateway Connection	Direct Stream	Direct Web	Direct Web
Gateway Configuration	Accsense Config Utility	Accsense Config Utility	Inbuilt
Pod history data with a network outage	Nil	Limited by Gateway memory	Limited by Gateway memory
Multiple Systems monitored (each system could be a different division of an organisations)	-	√	√

Location Name is master reference for data (enables pods to be exchanged for each location, i.e. during calibration)	√	√	√
Location of Sensor	√	√	√
Node enable/disable	√	√	√
Node channel selection (Log only selected channel data rates to calibrated data tables)	-	√	√
Validation mode for sensors	-	√	√
Node Channel Calibration	√	√	√
External Sensor Calibration (Calibration factors for both the Pod input plus the sensor)	-	√	√
Pod & Sensor Drift Correction	-	√	√
All raw data stored	√	√	√
All calibrated data stored	√	√	√
Selectable data sample rates per channel	√	√	√
Fast sample rate on alarm	√	√	√
Channel sample data can be started and stopped by time of day at different sample rates	√	√	√
EnviroPoint Monitor: number of display screens	1	2	4
User Logon Control	√	√	√
Digital Signatures	-	-	√
Remote System Configuration	-	√	√
Multi-lingual Support	√	√	√
Node data & info display	√	√	√
Number of nodes able to be displayed on the monitors at one time	32	160 (2x 80)	320 (4x 80)
Node set to a Group	√	√	√
Node Group data & info display	√	√	√
Node Chart Display	√	√	√
Chart Display Printing	√	√	√
Group Node Maps	√	√	√
Group Node Maps type	.jpg .bmp .png	.jpg .bmp .png	.jpg .bmp .png .dfx
Alarms	√	√	√
Alarm Threshold Delay Time	√	√	√
Alarm Hysteresis	√	√	√
Different Alarm limits for selected times of the day	√	√	√
Multi Level Alarms	-	√	√
Group Node Maps Display Alarms	√	√	√

Node Timeout Alarm	√	√	√
Signal Strength Node Alarms	√	√	√
Supply Voltage Node Alarms	√	√	√
Mains Power Node Alarms	√	√	√
Email Alarm Notifications	-	√	√
SMS Alarm Notifications	√	√	√
Active Sensor Alarm Listing	√	√	√
Old Sensor Alarm Listing	√	√	√
Active Unit Alarm Listing (Node functions)	√	√	√
Old Unit Alarm Listing (Node functions)	√	√	√
Alarm Acknowledgement by Operator	√	√	√
System Logs	√	√	√
Audit Logs	-	SQL Triggers	Full
Report Generation	√	√	√
Periodic Report Generation	√	√	√
Digital Signed Reports	-	-	√
Printer Selection	Only default	Selectable	Selectable
Server Web reporting using Reporting Services	-	√	√
Database Data Tables Full Text Search capable	-	√	√
Online Help	√	√	√
Support Information	√	√	√

† Limited by the SQL server system resources and system network.

* Not yet released

GLOSSARY AND BIBLIOGRAPHY

Glossary of Terms

Pod or Unit	Physical sensing unit with internal or external sensors
Gateway	Passes data in an orderly fashion from pods to the computer network
Mesh	A matrix of pods, preferably with multiple data paths to the gateway
Node	A planned pod placement in the mesh. A node may have different consecutive pods due to replacement, e.g. for calibration.
Point	A sensor unit, e.g. a temperature point or voltage point
Association	The initial signal acknowledgement between a pod and a gateway.
USB dongle	Used to relay SMS messages in an alarm event
Router	Connects gateway(s) to an external telephone network for relaying data over long distances
Aircard/datacard	Card containing data sim which fits into the router for telephone network connection

[1] Instruction Manual from Accsense, Inc. – 2006

[2] Accsense Gateway configuration Guide from Accsense, Inc. - 2006