

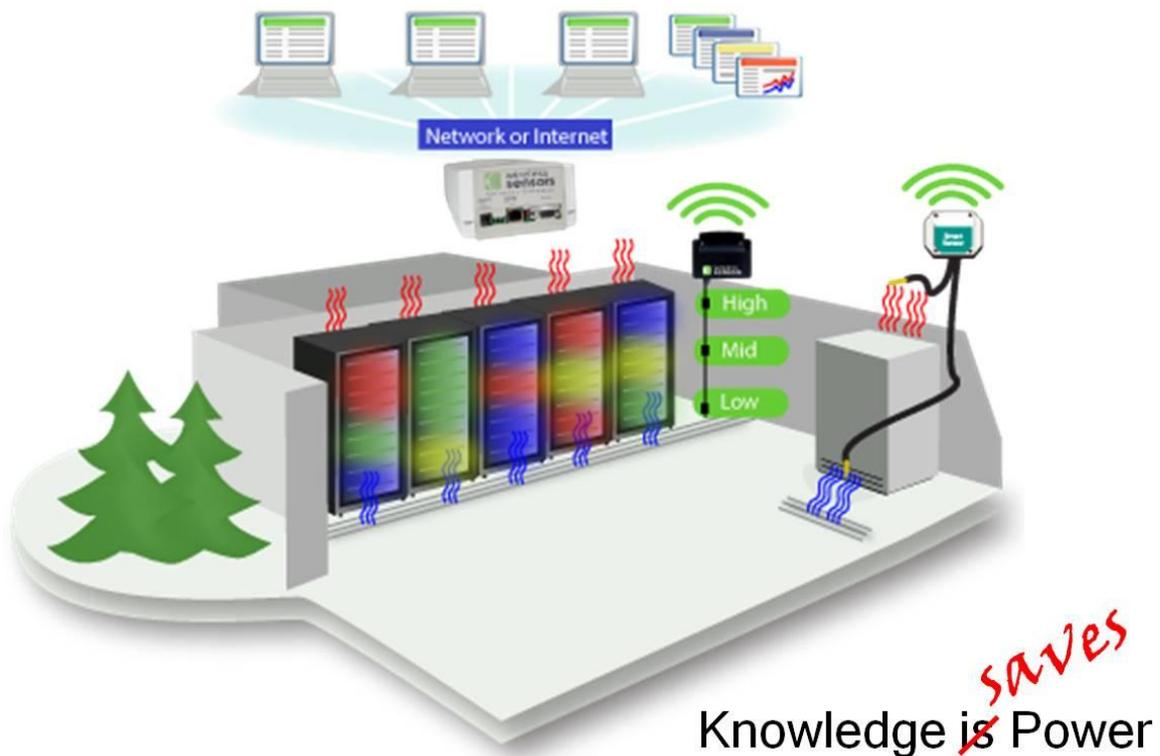


SensiNet

Rack Sentry

Data Center

Handbook



Knowledge ~~is~~ Power

Table of Contents

1. SENSINET® RACK SENTRY PRODUCT LINE.....	3
1.1 OVERVIEW.....	3
1.2 SERVICES GATEWAY.....	3
1.3 MESH ROUTERS.....	3
1.4 SMART SENSORS.....	4
1.4.1 Rack Sentry Multipoint Temperature Smart Sensor.....	4
1.4.2 Rack Sentry Temperature and Humidity Smart Sensor	4
1.4.3 RTD Smart Sensor.....	4
1.4.4 4-20mA Current Smart Sensor	4
1.4.5 0-10V Voltage Smart Sensor	4
1.4.6 Contact Closure Smart Sensor	4
2. SENSINET DEPLOYMENT OVERVIEW.....	5
2.1 STEP 1: GATHER INSTALLATION INFORMATION	5
2.2 STEP 2: DETERMINE ENVIRONMENT TYPE	5
2.3 STEP 3: SELECT SENSINET COMPONENTS	5
2.4 STEP 4: DEPLOY AND COMMISSION SENSINET	5
3. VALUABLE SITE INFORMATION.....	6
3.1 DATA CENTER AND IT ENVIRONMENTS.....	6
3.2 NETWORK INFORMATION	6
4. DETERMINING ENVIRONMENT TYPE.....	7
4.1 DATA CENTER	7
4.2 COMPUTER ROOM.....	8
4.3 NETWORK CLOSET.....	8
5.1 DATA CENTER	9
5.1.1 Breaking Installations into Multiple, Smaller Networks	12
5.1.2 Determine Mesh Router Requirements.....	13
5.2 COMPUTER ROOM	15
5.3 NETWORK CLOSETS.....	16
6.1 DATA CENTER	16
6.1.1 Services Gateway Placement.....	16
6.1.2 Mesh Router Placement.....	17
6.1.3 Sensor Placement	17

6.2 COMPUTER ROOMS AND NETWORK CLOSETS 18

6.2.1 Services Gateway Placement..... 18

6.2.2 Mesh Router Placement..... 18

6.2.3 Smart Sensor Placement..... 18

7. SENSINET SERVICES GATEWAY19

7.1 OVERVIEW 19

SENSINET SERVICES SITE20

7.2 SENSINET SERVICES GATEWAY GUIDELINES FOR INSTALLATION ON IT NETWORKS..... 20

7.3 SENSINET SERVICES GATEWAY INTEGRATION – WEB SERVICES..... 21

7.4 WIRELESS SENSORS SERVICES GATEWAY INTEGRATION – OPC 21

7.5 WIRELESS SENSORS SERVICES GATEWAY INTEGRATION – ODBC..... 22

7.6 SENSINET SERVICES GATEWAY INTEGRATION – MODBUS 23

7.7 SENSINET SERVICES GATEWAY INTEGRATION – HTTP..... 24

7.8 SENSINET SERVICES GATEWAY INTEGRATION – SNMP..... 25

1. SensiNet[®] Rack Sentry Product Line

1.1 Overview

SensiNet[®] is a complete wireless sensor network built for Data Center and other IT environments where high reliability is required. The SensiNet Rack Sentry system includes everything you need to monitor important process and environmental data in a Data Center, Computer Room or Network Closet.

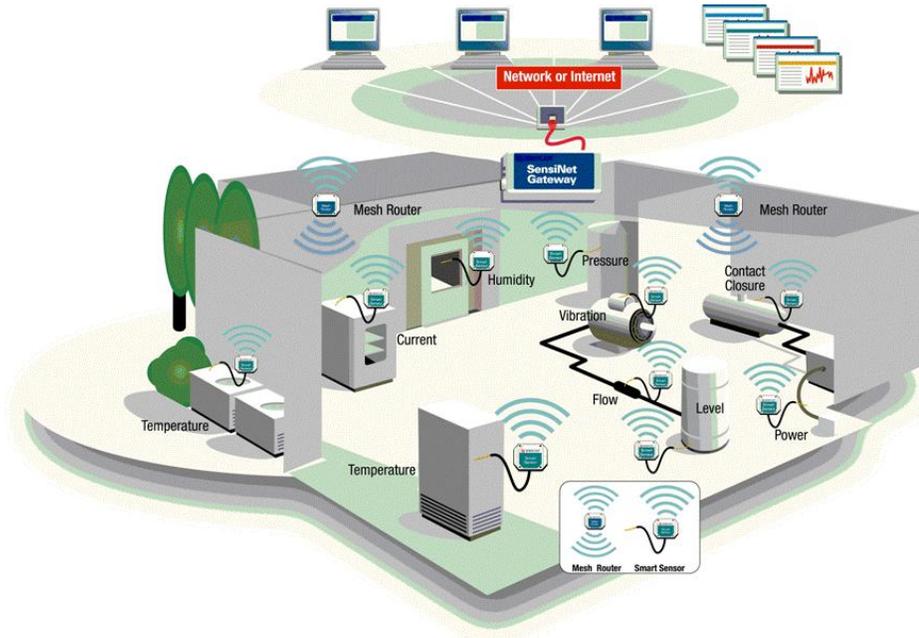


Figure 1: SensiNet graphical deployment.

1.2 Services Gateway

The SensiNet Services Gateway for the SensiNet Rack Sentry system provides data access and external communication for SensiNet. SensiNet Services Gateway is a self-contained network management and access appliance that lets you securely access and analyze data collected by Smart Sensors using a convenient browser interface. For larger installations with existing monitoring and legacy control software already in place, the SensiNet Services Gateway communicates sensor data directly to most BMC's and DCIM solutions and any other software compatible with ModBus, ODBC, SNMP, OPC and SOAP.



1.3 Mesh Routers

The SensiNet Mesh Router is an intelligent repeater that optimizes and extends the operating range of a SensiNet wireless sensor network. Every mesh router establishes direct communication links with at least two other Mesh Routers or Gateways in the network. This redundancy ensures that a wireless message coming from or going to a wireless sensor or another Mesh Router will be received.



1.4 Smart Sensors

Smart Sensors provide customers with the real-time environmental, equipment status and process information required for analysis and key decision making. Every Wireless Sensors Smart Sensor connects industry standard sensors to SensiNet, the most reliable wireless sensor networking technology available. Furthermore, every SensiNet Smart Sensor includes RF power amplification to deliver the maximum connection range possible—even in the harshest RF environments. Wireless Smart Sensors are available for use in the 2.4 GHz unlicensed band.

1.4.1 Rack Sentry Multi-Point Temperature Sensor

The Rack Sentry Multi-Point features the ability to “daisy chain” temperature sensors using standard CAT5 patch cables. Up to three sensors are supported as standard and this number can be increased under special circumstances. These sensors can be added and or reconfigured in the field and are deployed without costly wiring.



1.4.2 Rack Sentry Temperature and Humidity Smart Sensor

The SensiNet Rack Sentry integral sensor series are real-time temperature and humidity monitoring devices with embedded sensors and are available as temperature only or with temperature and RH.



1.4.3 RTD Smart Sensor

The SensiNet TEMP Smart Sensors are wireless temperature measuring devices. All of the devices operate at 2.4GHz and are FCC and CE approved. They report highly accurate and repeatable real-time temperature measurements to a central management application.



1.4.4 4-20mA Current Smart Sensor

The SensiNet CURR Smart Sensors are input current monitoring devices. The CURR-1022 operates on 2.4 GHz and is an FCC and CE approved device that wirelessly transmits 4-20mA sensor data.



1.4.5 0-10V Voltage Smart Sensor

The SensiNet VOLT Smart Sensors are analog input voltage monitoring devices. The devices are real-time wireless transmitters of 0-10v sensor data. The VOLT-1022 operates at 2.4 GHz and is FCC and CE approved.

1.4.6 Contact Closure Smart Sensor

The CONT-1022 transmits all state changes of an attached circuit, as well as continuously transmits the current state of the circuit at a user-defined interval. When used with the SensiNet Gateway, the status is accessible via a variety of formats, including OPC, ModBus and SOAP/XML. The CONT-1022 can be used with a variety of switches including mechanical, IR and magnetic. Two contacts are supported for each CONT-1022.



2. SensiNet Deployment Overview

This section provides a brief overview of the steps required to successfully install a SensiNet system and the details of this process are more fully described later in this document.

2.1 Step 1: Gather Installation Information

Certain customer information is useful to specify and deploy a SensiNet wireless sensor network. This includes area floor plans or schematics with locations of sensors, power and Ethernet drops.

2.2 Step 2: Determine Environment Type

Use the descriptions to determine if the environment is Data Center, Computer Room or Network Closet.

2.3 Step 3: Select SensiNet Components

Specifying a SensiNet system involves determining how many SensiNet Services Gateways, Mesh Routers and Smart Sensors you will need. Smart Sensor number and location are determined by the requirements of the application, while determining the necessary Services Gateway and Smart Sensor numbers is a two-step process. If the overall installation is very large, break the installation down into multiple, smaller networks. Then determine Mesh Router requirements for each network.

2.4 Step 4: Deploy and Commission SensiNet

SensiNet deployment involves installing the Smart Sensors, Mesh Routers and Services Gateways according to the demands of the installation and each environment type has its own unique characteristics and is described in its own section. Network commissioning is generally most effective when the Gateway is commissioned first, then the Mesh Routers and finally the Smart Sensors. This procedure allows for the network to form rapidly and in optimal fashion.

3. Valuable Site Information

This section describes valuable information which allows for a smooth and effective installation.

3.1 Data Center and IT Environments

SensiNet Rack Sentry systems are most often deployed in three area categories based on the number of rooms/floors to be instrumented, area of the room and number of server racks. These three areas are considered to be Data Centers, Computer Rooms or Network Closets, and are described in Section 4. The SensiNet Rack Sentry system is appropriate for all three areas and understanding the individual characteristics of each allows for the selection of the appropriate components to address the unique needs of each application and ensure robust network performance.

3.2 Network Information

SensiNet has a very low IT footprint requiring only an Ethernet connection and a web browser to access all functions. The system is shipped configured to receive its IP address from a DHCP server upon connection and power up. A small “discovery” application is supplied which locates the IP address it has been assigned so a browser can be “pointed” to it. It is useful to know the network it is connected to so you can assure the discovery application and Gateway are located on the same network, otherwise the application cannot “see” the Services Gateway. Once you have connected to the Gateway you can assign a fixed IP address if you intend to connect directly to a workstation instead of through a network. You may need a “crossover” cable (depending on your computer’s Ethernet port) and will need to make sure you know the IP address, network ID and subnet mask for the workstation. If not familiar with these network concepts your IT department should be able to help. No other network services are required.

3.3 System Interface Requirements

The SensiNet Services Gateway serves as the “head end” of the wireless network and can operate in either a stand-alone mode or as a protocol server to DCIM and Building Automation Systems (BMS). The embedded appliance nature of the Services Gateway allows it to provide monitoring, data collection, data visualization and alarming without the need for higher level systems and no additional software. All system setup and monitoring functions are accessed through standard web browser. The standard protocol options include SNMP, Modbus TCP, OPC, ODBC and SOAP.

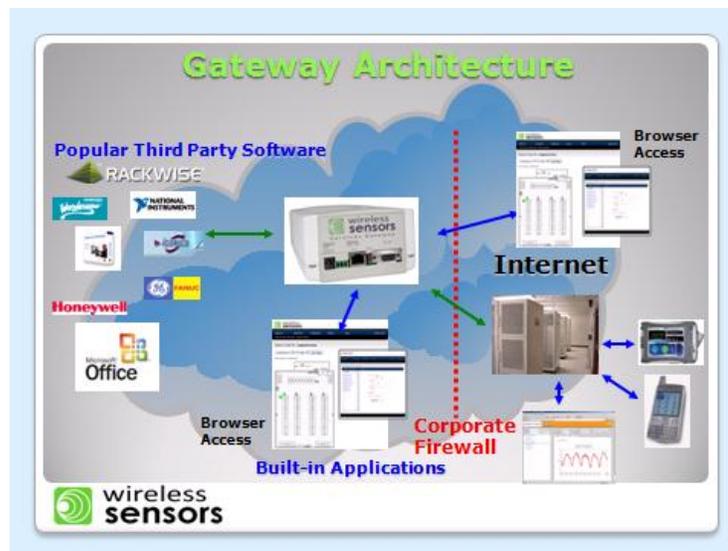


Figure 2: SensiNet Services Gateway Architecture.

4. Determining Environment Type

Wireless Sensors defines IT Environments into three broad categories: Data Center, Computer Room and Network Closet, where SensiNet systems are typically deployed. Each environment has unique properties that affect how SensiNet is specified and deployed.

4.1 Data Center

Data Center environments are typically a large open room, with precision cooling, UPS and high voltage power systems, with few obstacles to wireless performance. Supporting posts and small lightly constructed offices are not uncommon as part of a Data Center and do not degrade wireless performance.



Figure 3: Typical Data Center

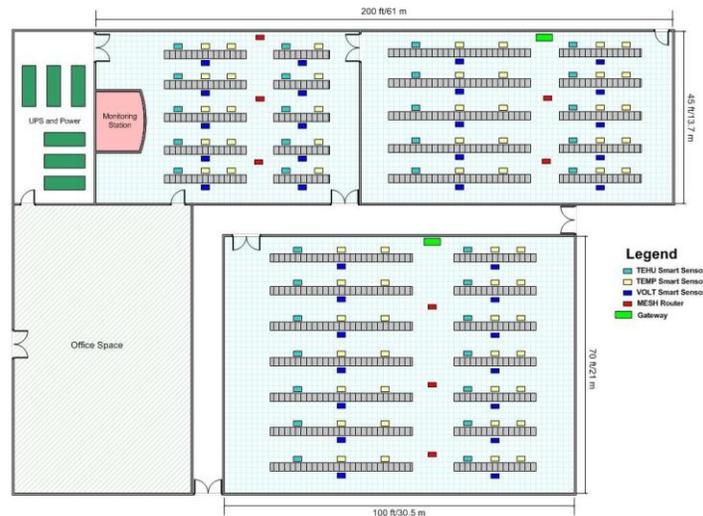


Figure 4: Typical Data Center Layout

These spaces are commonly configured with a raised floor containing cabling and providing distribution of cooling air. They are increasingly being configured in a hot aisle and cold aisle configuration in an effort to increase efficiency by delivering cooling air to the server inlets.

4.2 Computer Room

Computer room environments typically have a smaller foot print than a purpose built Data Center and often lack Data Center specific cooling systems (rather they use building air called comfort cooling). Usually a Computer Room contains a UPS and higher voltage power than an office space. Computer rooms are sometimes repurposed rooms in an office space environment. None the less, these rooms serve the same function as a Data Center, just on a different scale of sophistication and complexity. Just like a Data Center, Computer Room environments need to be managed to provide an optimal environment for server performance. The building construction might be drywall and stud or it could be metal and concrete. Most often the IT staff is responsible for this both the space and the equipment contained in it.



Figure 5: Computer Room

4.3 Network Closet

A network closet typically contains network switch gear, one or more servers and are in close proximity to end users. Because of their small size and lack of proper cooling, Network Closets may be cooled by the standard building HVAC system or may be equipped with in room air conditioners which are rarely monitored by any other system.



Figure 6: Network Closet

5. Specifying a Rack Sentry Wireless Sensor Network Solution

While the application dictates the number and type of Smart Sensors to be installed, the environment determines the number of SensiNet Services Gateways, and Mesh Routers required in the particular environment whether Data Center, Computer Room, or Network Closet. Each environment has unique properties that result in various specification procedures.

5.1 Data Center

Data Centers today rely on a wide range of equipment to deliver the mission critical processing to their constituents and this includes servers, network switches and storage. These components have very diverse power consumption characteristics and resultant cooling requirements. These components tend to be grouped together in the data center resulting in a plan view heat load profile depicted in figure 7.

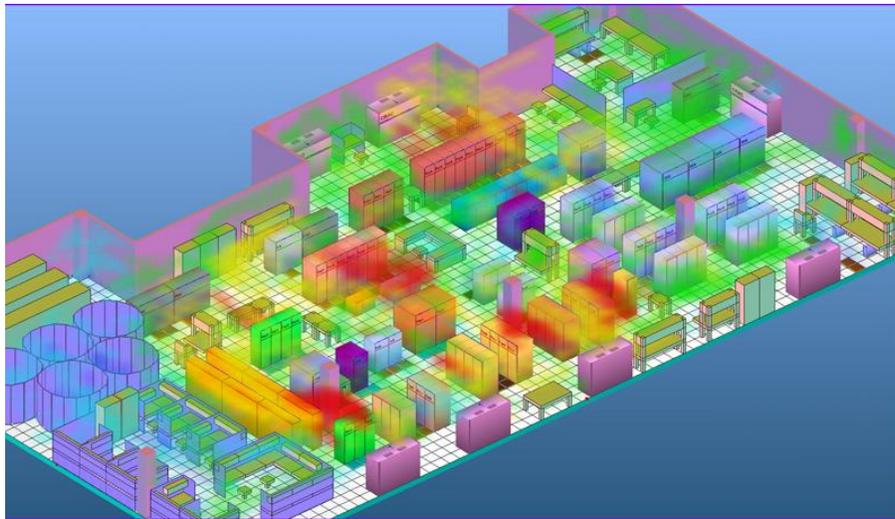


Figure 7: Data Center Thermal Profile

This profile presents an interesting control challenge due to the widely varying temperatures and requires that air distribution systems be adjusted to deliver cooling in proportion to the equipment heat load in two dimensions while many cooling systems are configured to control based on a single sensor input (often supply air temperature). This two dimensional problem requires that cooling air delivery systems be balanced to provide the appropriate volume of air to the required area. This task is often accomplished by the use of adjustable perforated floor tiles allowing air to flow where it's needed. This balancing usually takes place under the presumption that steady state conditions exist. Modern data centers are commonly arranged into hot and cold aisle configurations to promote efficient delivery of conditioned air and return of hot air back to the CRAC (Computer Room Air Conditioner) or CRAH (Computer Room Air Handler). In a properly balanced system all the cooling air is ingested at the server inlets and exhausted to the hot aisle where it is directed back to the CRAC's or CRAH's without stratification or recirculation. A system operated in this condition is operating at peak efficiency with all conditioned air being used to maintain the desired server temperature.

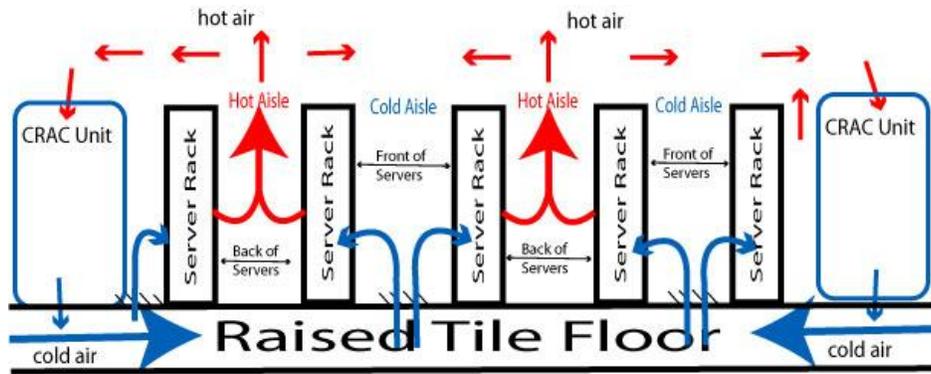


Figure 8: Hot Aisle Cold Aisle Design Concept

Most often the cooling system does not perform according to the original design due to increased server power density, under floor air blockages, unbalanced CRAC / CRAH performance, improperly located perforated tiles, removed blanking panels and a multitude of other factors. This imbalance transforms the design model shown in figure 7 to more closely resemble the temperature pattern depicted in Figure 8.

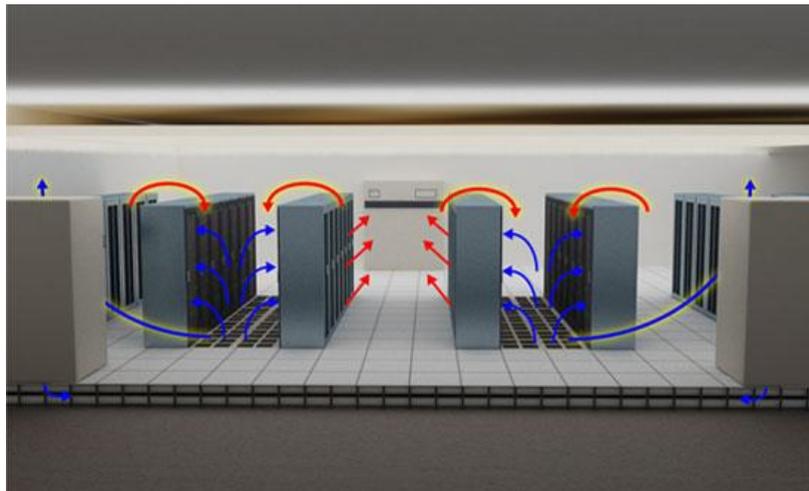


Figure 9: Hot Aisle Cold Aisle Recirculation

These factors make the cooling system operation in a modern data center a three dimensional problem which demands a sensor system with three dimensional granularity. As a result the recommendation from many industry experts is for temperature sensors to be located at the low, mid and high point server inlets in quantities sufficient to represent this three dimensional variability. The SensiNet Services Gateway provides three dimensional visualization of sensor data to assist with this problem and the screen capture in figure 10 shows an example of this user configured capability.

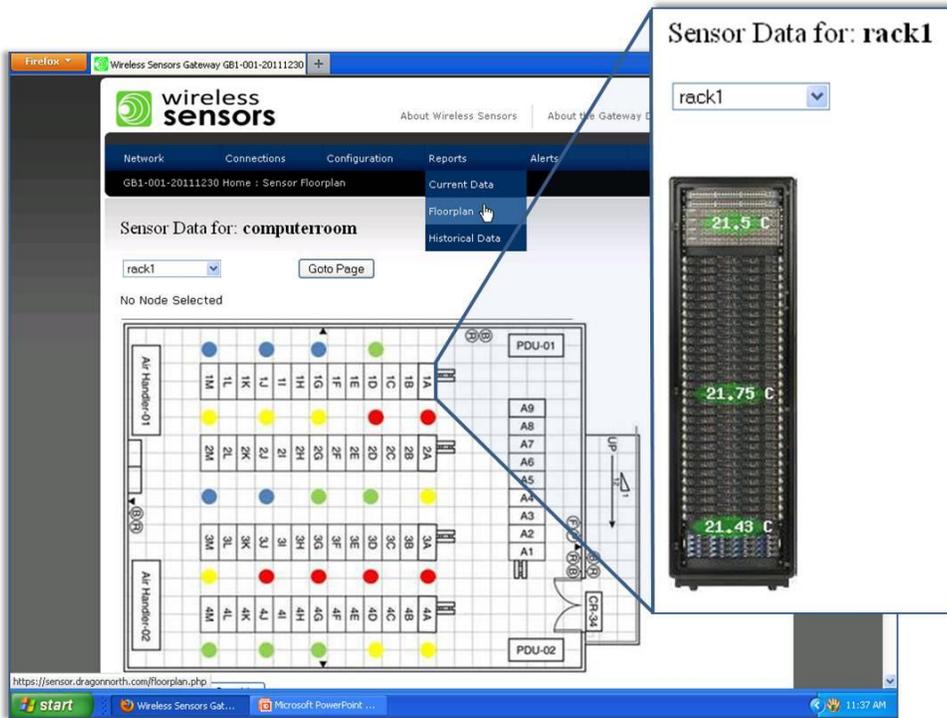


Figure 10: Sample Floor Plan View

Our experience suggests a distribution similar to that in figure 10 provides the proper level of granularity.

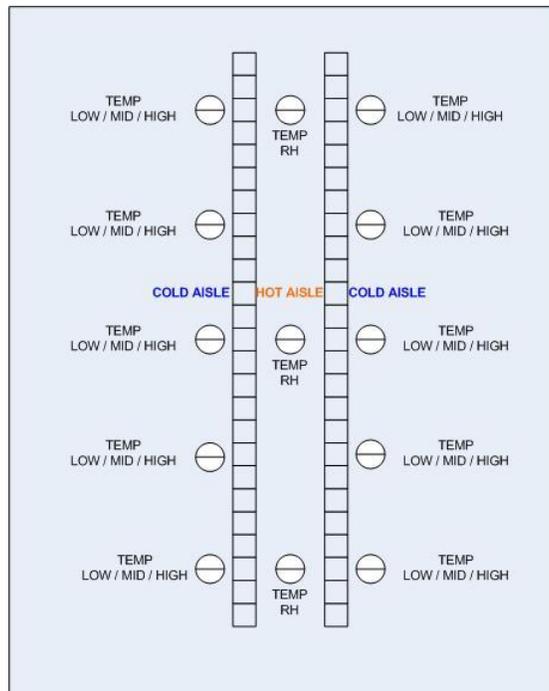


Figure 11: Suggested 50 Rack Layout

Using this recommendation the appropriate number of sensors per room can be determined and from here the layout for Gateway and Mesh Routers can be determined.

Data Center environments are typically a large open room, with precision cooling, UPS and high voltage power systems, with few obstacles to wireless performance. Supporting posts and small lightly constructed offices are not uncommon as part of a Data Center and do not degrade wireless performance.

Specifying a SensiNet wireless sensor network is a two-step process. First, break down the installation into the appropriate number of networks. Second, for each network, determine the number and placement of Mesh Routers required on site.

5.1.1 Breaking Installations into Multiple, Smaller Networks

Large installations are typically broken down into multiple, smaller networks. Often this is unavoidable because there may be a remote building or multiple floors, however, there are a variety of situations where this is a good practice and will result in more stable networks. Each new network will have its own Gateway. By determining the optimal number of networks for stable operation; you will determine the number of Gateways required for the installation. The Gateway requires Ethernet and line-power, so location of these should be a consideration for optimal Gateway placement.

This section gives examples to each of the rules for breaking down networks that are listed below.

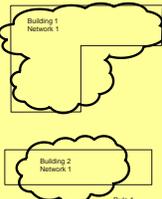
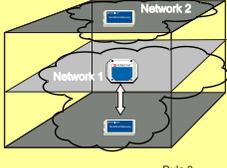
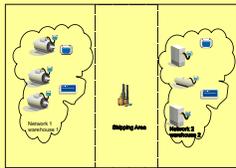
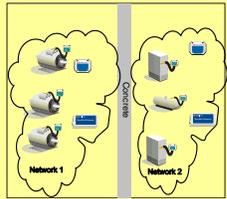
<p>Rule 1: Each separate building will require a separate network.</p> 	<p>Rule 2: No more than two floors should be combined in a network and only one if floors contain metal pans.</p> 
<p>Rule 3: Create two or more networks when transmitting across dynamic, high-movement environments such as roads, warehouses or shipping yards.</p> 	<p>Rule 4: Enclosed concrete areas will require their own network.</p> 
<p>Rule 5: Remote clusters of nodes require their own network.</p>	

Figure 12: Rules for breaking installations into multiple, smaller networks.

Once the installation is broken down into smaller, manageable networks, you must now determine the required number of Mesh Routers and location.

5.1.2 Determine Mesh Router Requirements

Mesh Router specification guidelines and the Mesh RangeFinder table are described below. Use these two tools to determine the optimal number and placement of Mesh Routers.

Mesh Router Placement Guidelines

Follow these guidelines when deciding Mesh Router placement.

1. Place Mesh Router roughly halfway between a Smart Sensor or a cluster of Smart Sensors.
2. Maximize use of open space such as hallways.
3. Minimize number of walls and other obstacles transmitting through.
4. When using multiple Mesh Routers to connect to a Smart Sensor, place Mesh Routers equal distance apart from the Smart Sensors.

Mesh RangeFinder

The Mesh RangeFinder allows you to calculate the maximum range to expect in each point to point connection. While it is optimal to place a Mesh Router halfway between a Smart Sensor or a cluster of Smart Sensors, if the halfway distance is greater than what is calculated by the RangeFinder, then extra Mesh Routers may be required. The Mesh RangeFinder table is shown below.

Commercial Areas = 200' Base			
Wall Type	0-10'	50'	100'
Drywall	25'	50'	50'
Concrete	50'	100'	n/a

Figure 13: Mesh RangeFinder

For every wall the signal passes through, subtract the corresponding distance from the baseline distance to determine the maximum recommended range for the Mesh Router.

Example #1: Open air (no obstacles)

When there are no obstacles to be transmitted through, there is no need to reduce the base range, thus the maximum recommended range between routers is 200'. Figure 8 below shows this graphically.

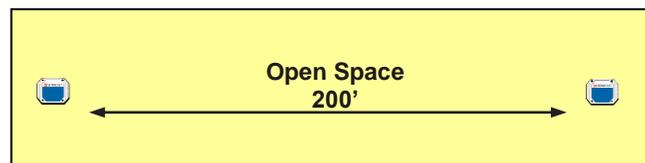


Figure 14: Maximum recommended range for open air transmission.

Example #2: One wall 10' away

Subtract 25' from the base range to get a maximum recommended range of 175' ($200' - 25' = 175'$). See Figure 9 below.

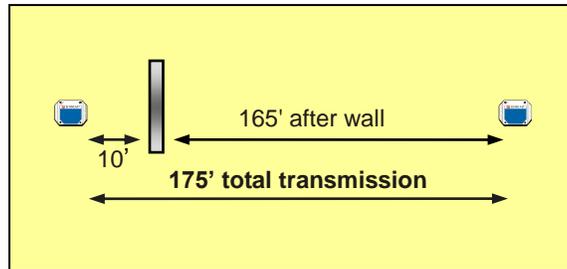


Figure 15: Recommended transmission range for obstacle 10' from transmitter.

Example #3: One wall 50' away

Subtract 50' from the base range for a maximum recommended range of 150' ($200' - 50' = 150'$). See Figure 10 below.

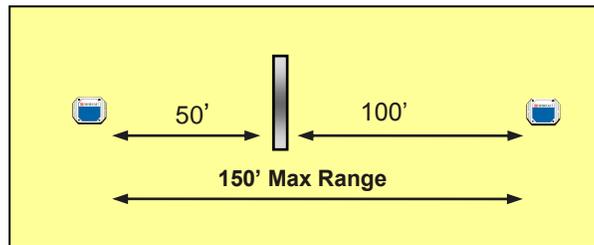


Figure 16: Recommended transmission range for obstacle 50' from transmitter.

Example #4: Two walls: one wall 10' away and a second wall 50' away.

Subtract 25' because of the wall 10' away then subtract an additional 50' because of the wall 50' away ($200' - 25' - 50' = 125'$). See Figure 11 below.

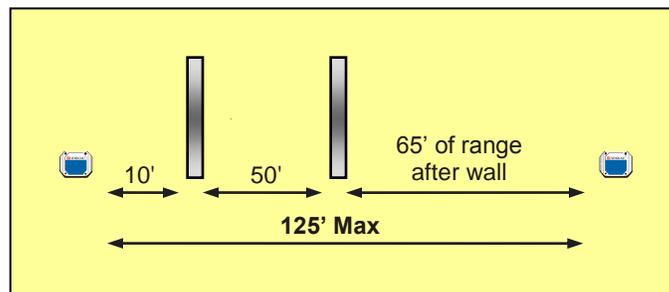


Figure 17: Transmitting through two walls.

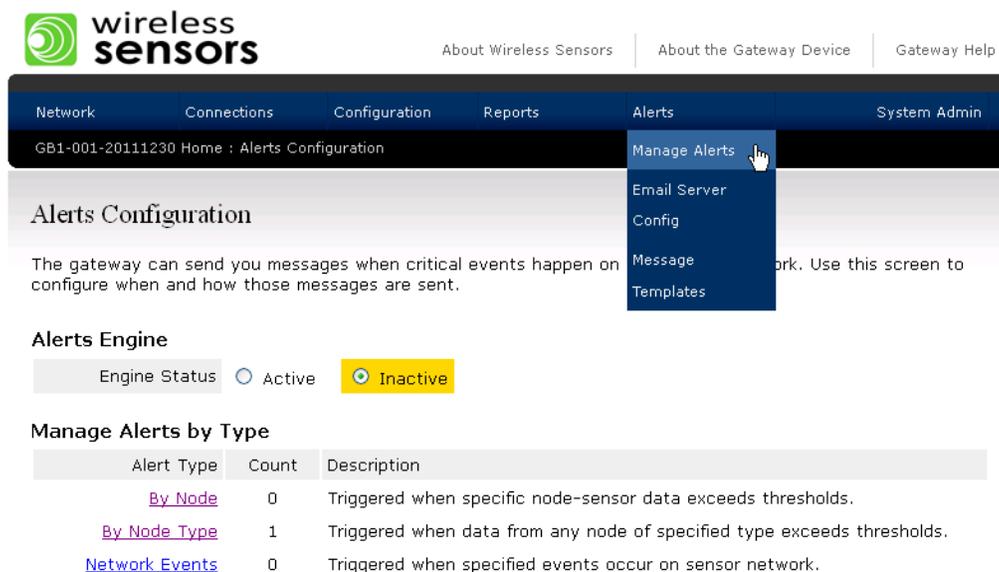
5.2 Computer Room

Computer room environments typically have a smaller foot print than a purpose built Data Center, lack Data Center specific cooling systems (rather they use building air called comfort cooling), and are re-purposed rooms in an office space environment. That being the case, it is unusual to find obstructions that will impede wireless performance in a computer room. Just like a Data Center, Computer Room environments need to be managed to provide an optimal environment for server performance.



Figure 18: Computer Room Environment

The design and layouts vary as greatly as the enterprises they serve but a common attribute is that the entire operation is often the responsibility of one person or group. These systems have no less challenging environmental concerns but they are combined with a requirement that the monitoring system be uncomplicated. Components required for these systems require a single Services Gateway and the appropriate number of sensor nodes. The ability of the Gateway to operate in a standalone mode and delivery alert data via email notification enhances the value for these application environments.



The screenshot shows the 'Alerts Configuration' page in the Wireless Sensors gateway interface. The page title is 'Alerts Configuration' and the breadcrumb is 'GB1-001-20111230 Home : Alerts Configuration'. The 'Alerts' menu is open, showing options: 'Manage Alerts', 'Email Server Config', 'Message Templates', and 'Work'. The 'Alerts Engine' is currently 'Inactive'. Below is a table titled 'Manage Alerts by Type'.

Alert Type	Count	Description
By Node	0	Triggered when specific node-sensor data exceeds thresholds.
By Node Type	1	Triggered when data from any node of specified type exceeds thresholds.
Network Events	0	Triggered when specified events occur on sensor network.

Figure 19: Services Gateway Alert Setup Screen

5.3 Network Closets

A network closet typically contains network switch gear, a server or two and is often in close proximity to end users. Because of their small size and lack of proper cooling, Network Closets can be difficult to maintain at optimal temperature and humidity for best performance. This is further complicated by the fact they are usually unmanned so any cooling system anomalies can easily go undetected.

The footprint for these environments is usually very small so wireless range is rarely a problem unless there are multiple closets located throughout a facility which need to be combined onto one sensor network. In this case the design considerations described under the Data Center section could apply.

The fact that the Gateway is an embedded appliance is of great value in these environments since it requires virtually no network resources



Figure 20: Network Closet Environments.

6. Deploying a SensiNet Wireless Sensor Network Solution

This section describes the various deployment best practices for Data Center, Computer Room, Network Closet environments.

6.1 Data Center

SensiNet wireless sensor networks are best brought on line in the following order: Services Gateway, Mesh Routers, then Smart Sensors.

6.1.1 Services Gateway Placement

Use the following guidelines to determine Services Gateway placement.

1. Place near Ethernet drop and line power or run these to the Gateway.
2. Place high, near the ceiling similar to the sensor placement described above.
3. For large Data Centers, place at the center of the room then use Mesh Routers to communicate to either side of obstacles.

6.1.2 Mesh Router Placement

Use the following guidelines to determine Mesh Router placement.

1. Lengthen transmission distances from transmitters in open space and shorten when transmitting around obstacles or walls.
2. Make use of open space by placing high above equipment and transmitting down rows and above server cabinet tops.
3. Place in line of sight to Gateway, other Mesh Routers and Smart Sensors whenever possible.
4. Minimize the number of obstacles the signal transmits through.
5. Place near line power or run it to the Mesh Router.

6.1.3 Sensor Placement

Below are best practices guidelines for deploying a stable SensiNet Wireless Sensor Network. SensiNet is typically deployed in the following order: Gateway, Mesh Routers then Smart Sensors.

Customers determine general area for sensor placement. Use the following guidelines for final placement.

1. Place at rack inlet and hot aisle, at each stratification layer. For best coverage install sensors at every 3rd rack. You may desire to add sensors to heavily populated racks or in racks that house critical systems. Each CRAC should be outfitted with a CRAC pack to monitor outflow and return temperature. Monitoring the Delta T (a measurement of the delta between the outflow and return temperature) with third party sensors, can offer a better measurement than on board sensors because sensor placement can be optimized for each particular installation.
2. Place sensors high in the hot aisle to monitor the return air temperature and along the top of a Row to detect “mixing” of cold and hot air.

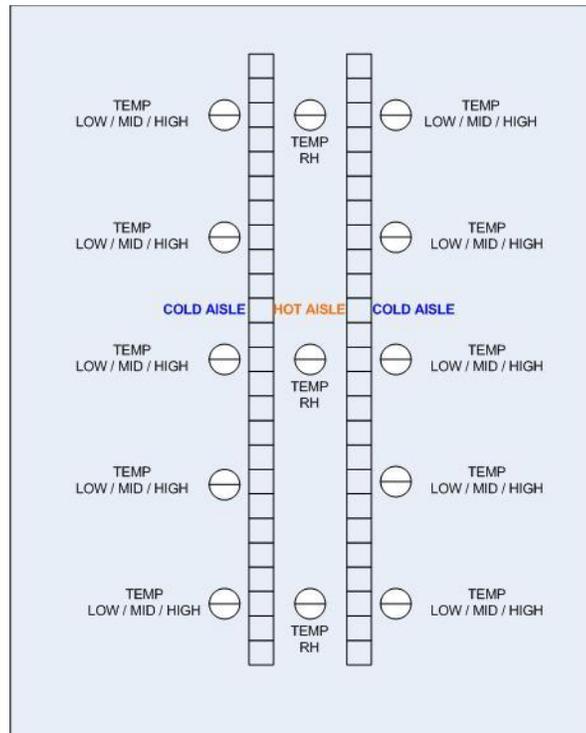


Figure 21: Example of Recommended Sensor Placement.

6.2 Computer Rooms and Network Closets

SensiNet wireless sensor networks are best brought on line in the following order: Services Gateway, Mesh Routers then Smart Sensors. Since the characteristics of a Computer Room and Network Closet are similar they are combined in this section.

6.2.1 Services Gateway Placement

Use the following guidelines to determine Services Gateway placement.

1. Place near Ethernet drop and line power or run these to the Gateway inside the Computer Room.
2. Place high near the ceiling similar to the sensor placement described above.

6.2.2 Mesh Router Placement

Use the following guidelines to determine Mesh Router placement.

1. If the Computer Room is small (less than 5000 Sq ft) and is open with no walls to attenuate the signals, a mesh router may not be needed.
2. If a mesh router is needed, make use of open space by placing high above equipment and transmitting down hallways, corridors and above obstructions.
3. Place in line of sight to Gateway, other Mesh Routers and Smart Sensors whenever possible.
4. Place near line power or run it to the Mesh Router.
5. Avoid mounting on steel columns or beams.

6.2.3 Smart Sensor Placement

1. Place at rack inlet, at each stratification layer. For best coverage install sensors at every 3rd rack. You may desire to add sensors to heavily populated racks or in racks that house critical systems. Place in line of sight of the Gateway and Mesh Routers whenever possible
2. If the Computer Room is being cooled by the buildings comfort cooling system, place sensors at each delivery vent and return vent.
3. In the room is small and has no obstructions or corners for sensors to “see around” then a mesh router may not be necessary

7. SensiNet Services Gateway

This section contains information about the SensiNet Services Gateway.

7.1 Overview

The SensiNet Services Gateway provides data access and external communications for the SensiNet wireless sensor network. A self-contained network management and access appliance, SensiNet's Services Gateway lets you securely access and analyze the data collected by Smart Sensors using a convenient browser interface. The Gateway provides SensiNet Network configuration tools and allows three methods for viewing data:

1. Third Party Software Integration
2. Standalone HMI
3. SensiNet Services Site

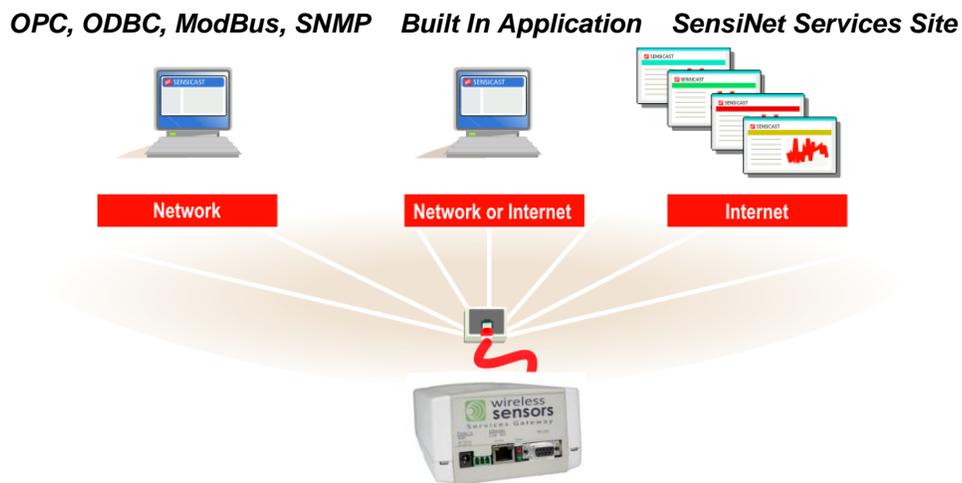


Figure 22: Wireless Sensors Services Gateway capabilities and protocols

Third Party Software Integration

For larger installations with existing monitoring and legacy control software already in place, the SensiNet Gateway communicates sensor data directly to dozens of software applications including:

- Wonderware
- ICONICS
- Intellution
- Citect
- LabView
- Other ModBus, ODBC, and OPC-compatible software

Standalone HMI

The SensiNet Gateway provides standalone HMI capability including the following functions:

- Graphical and tabular real-time and historical data
- Alarms

SensiNet Services Site

The Services Gateway can integrate with the SensiNet Services Site.

1. View sensor data from any web browser in any location
2. Graphical and tabular real-time and historical data
3. Alarms

7.2 SensiNet Services Gateway Guidelines for Installation on IT Networks

The SensiNet Services Gateway provides data access and external communications for the SensiNet wireless sensor network. Gateway usage guidelines are provided below.

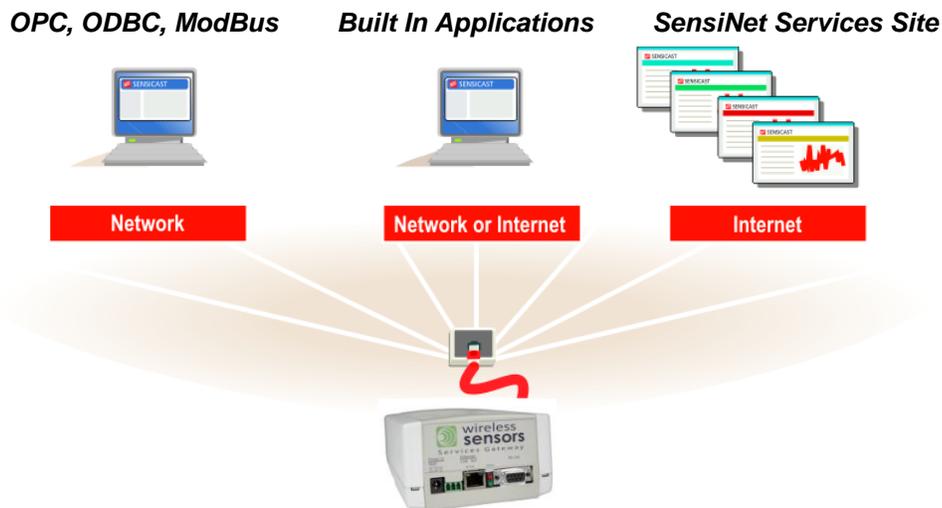


Figure 23: Wireless Sensors Services Gateway capabilities and protocols

Best Practices

Wireless Sensors recommends the steps outlined below in order to make the best use of your Gateway:

1. Configure access control to the Gateway by navigating to Configuration->User Access. It is recommended that administrative privileges are only given to the appropriate users.
2. Power your Gateway through an uninterruptible power supply.

7.3 SensiNet Services Gateway Integration – Web Services

The SensiNet Services Gateway is easily configurable to use web services to transmit data. This allows for designing web applications to make use of the sensor data aggregated by the Gateway.

To manage the SOAP data access on the Gateway, navigate to **Configuration -> Data Connections -> Web Services**. This will produce the screen in Figure 33.



Figure 24: Gateway web services configuration screen

The basic steps for configuring Web Services are:

1. Activate the service by selecting “Active” in the pull-down menu

7.4 Wireless Sensors Services Gateway Integration – OPC

The SensiNet Services Gateway is easily configurable to communicate via OPC. The SensiNet OPC server software can aggregate data from any or all Gateways on the subnet and provides OPC data services to third-party software.

The basic steps for configuring OPC are

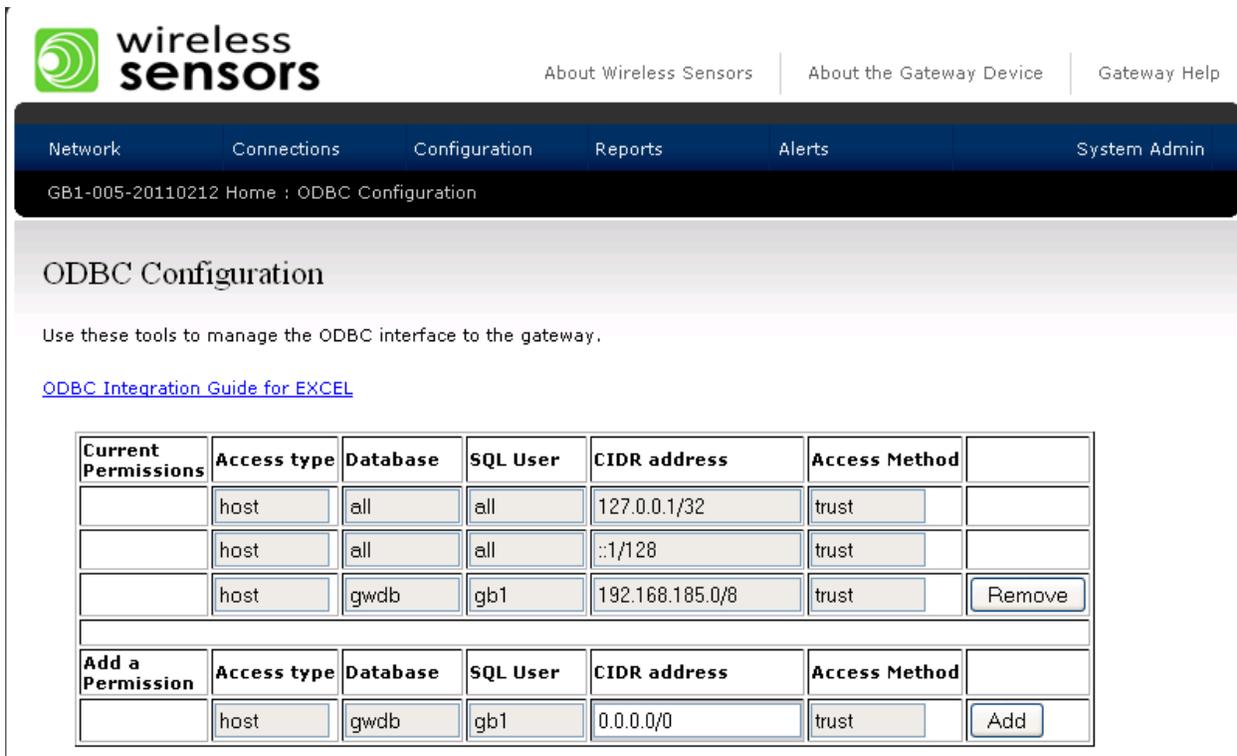
1. Install and configure SensiNet OPC server SW on host PC
2. Configure Gateway to add an ODBC host connection for server PC
3. Configure SensiNet OPC server SW
4. Map OPC tags to variables in third-party software

When finished changing information, click Save Changes to save the information.

7.5 Wireless Sensors Services Gateway Integration – ODBC

The Wireless Sensors Gateway is easily configurable to communicate via ODBC. This allows multiple third-party applications access to the data on the Gateway.

To manage the OPC data access on the Gateway, navigate to Configuration -> Data Connections -> ODBC. This will produce the screen in Figure 34.



Wireless Sensors Gateway Interface: ODBC Configuration

Use these tools to manage the ODBC interface to the gateway.

[ODBC Integration Guide for EXCEL](#)

Current Permissions	Access type	Database	SQL User	CIDR address	Access Method	
	host	all	all	127.0.0.1/32	trust	
	host	all	all	::1/128	trust	
	host	gwddb	gb1	192.168.185.0/8	trust	Remove
Add a Permission	Access type	Database	SQL User	CIDR address	Access Method	
	host	gwddb	gb1	0.0.0.0/0	trust	Add

Figure 25: Gateway ODBC configuration screen

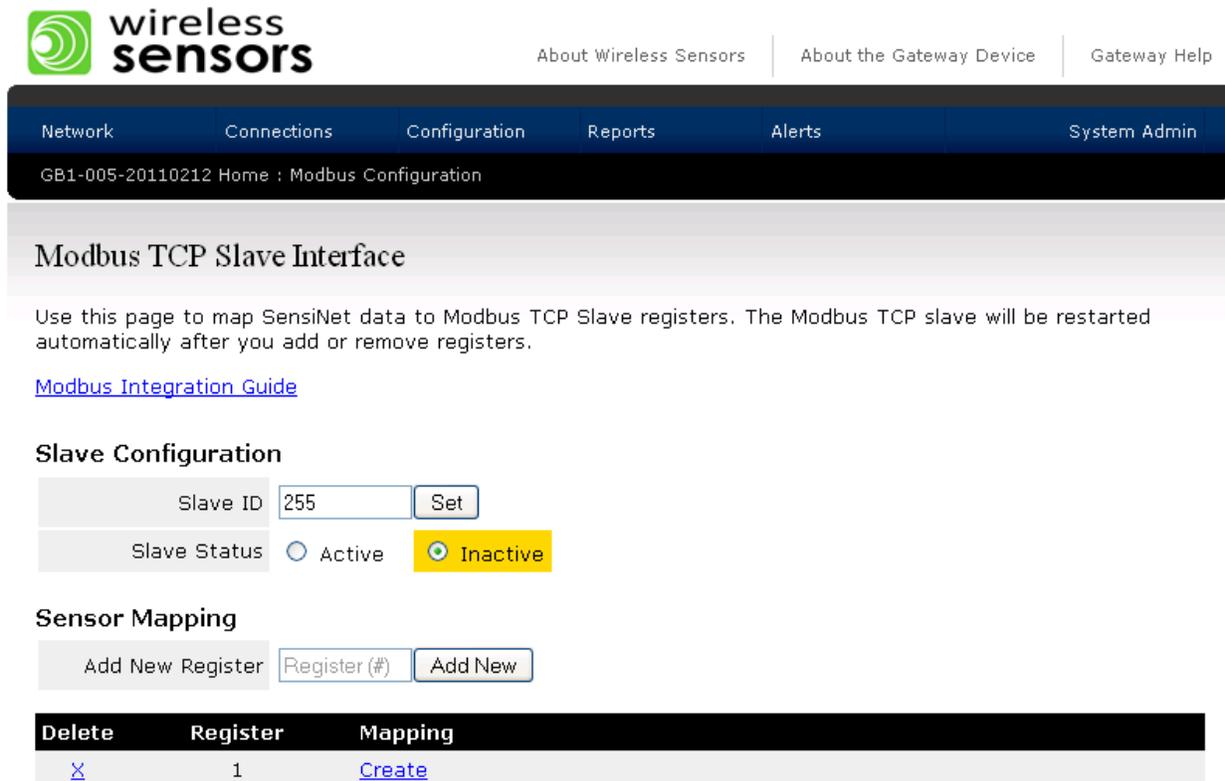
The basic steps for configuring ODBC are:

1. Enter the Classless Inter-Domain Routing (CIDR) Address of the client machine or network. For example, the CIDR address for a single host might be 192.168.185.76/32 and for a network 192.168.185.0/24.
2. Leave the other fields with the default values and click "Add"

7.6 SensiNet Services Gateway Integration – ModBus

The SensiNet Services Gateway is easily configurable to communicate via ModBus TCP/IP to external devices. The Gateway acts as a ModBus slave to make data available to ModBus master devices. In the Gateway Interface, SensiNet Smart Sensor devices ports can be mapped to ModBus registers.

To manage the ModBus slave feature on the Gateway, navigate to **Configuration -> Data Connections -> ModBus**. This will produce the screen in Figure 35.



The screenshot shows the 'Modbus TCP Slave Interface' configuration page. At the top, there is a navigation bar with 'Network', 'Connections', 'Configuration', 'Reports', 'Alerts', and 'System Admin'. Below this is a breadcrumb trail: 'GB1-005-20110212 Home : Modbus Configuration'. The main heading is 'Modbus TCP Slave Interface'. A descriptive text states: 'Use this page to map SensiNet data to Modbus TCP Slave registers. The Modbus TCP slave will be restarted automatically after you add or remove registers.' A link for 'Modbus Integration Guide' is provided. The 'Slave Configuration' section includes a 'Slave ID' field with the value '255' and a 'Set' button, and a 'Slave Status' section with radio buttons for 'Active' and 'Inactive' (which is selected). The 'Sensor Mapping' section has an 'Add New Register' button, a 'Register (#)' input field, and an 'Add New' button. Below this is a table with columns 'Delete', 'Register', and 'Mapping'.

Delete	Register	Mapping
X	1	Create

Figure 26: Gateway ModBus configuration screen

Within the ModBus Configuration page you can set several options:

1. Set ModBus slave option as Active or Inactive by clicking the appropriate radio button.
2. Set Gateway ModBus slave ID by typing the ID into the appropriate field.
3. Change ModBus register mapping by entering new information into the appropriate fields.

When finished changing information, click Save Changes to save the information.

7.7 SensiNet Services Gateway Integration – HTTP

The SensiNet Services Gateway is easily configurable to transmit via HTTP. This allows you to transmit sensor data to an Application Service Provider site.

To manage the OPC data access on the Gateway, navigate to **Configuration -> Data Connections -> HTTP**. This will produce the screen in Figure 36.

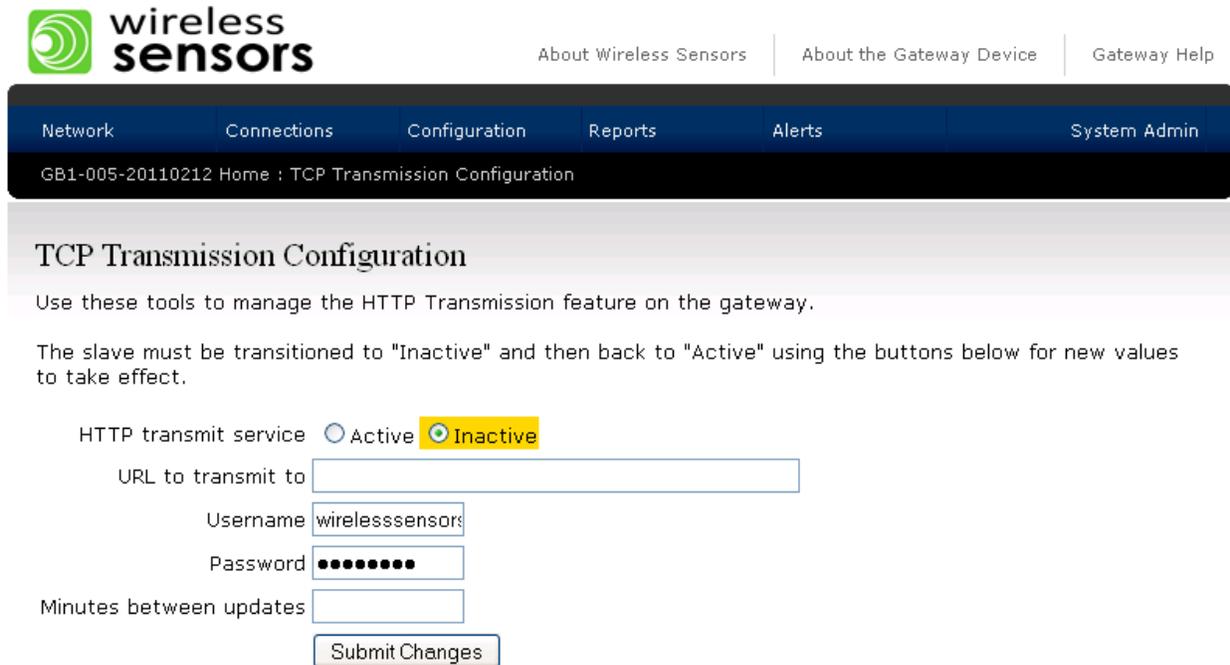


Figure 27: Gateway HTTP Transmission configuration screen

The basic steps for configuring HTTP are:

1. Activate the service by selecting the “Active” Radio Button.
2. Enter the destination URL to transmit data to.
3. Enter the password required for the site data is being transmitted to.
4. Specify the time between updates in minutes.

7.8 SensiNet Services Gateway Integration – SNMP

The SensiNet Services Gateway supports communication with any SNMP enabled system and the MIB is available from Wireless Sensors for this purpose. The system is read only and uses the Public SNMP Read Community parameter setting of: sensicast. An example of the SNMP setup using an open source SNMP tool called GETIF version 2.2 available at <http://www.wtcs.org/snmp4tpc/getif.htm> is shown in figure

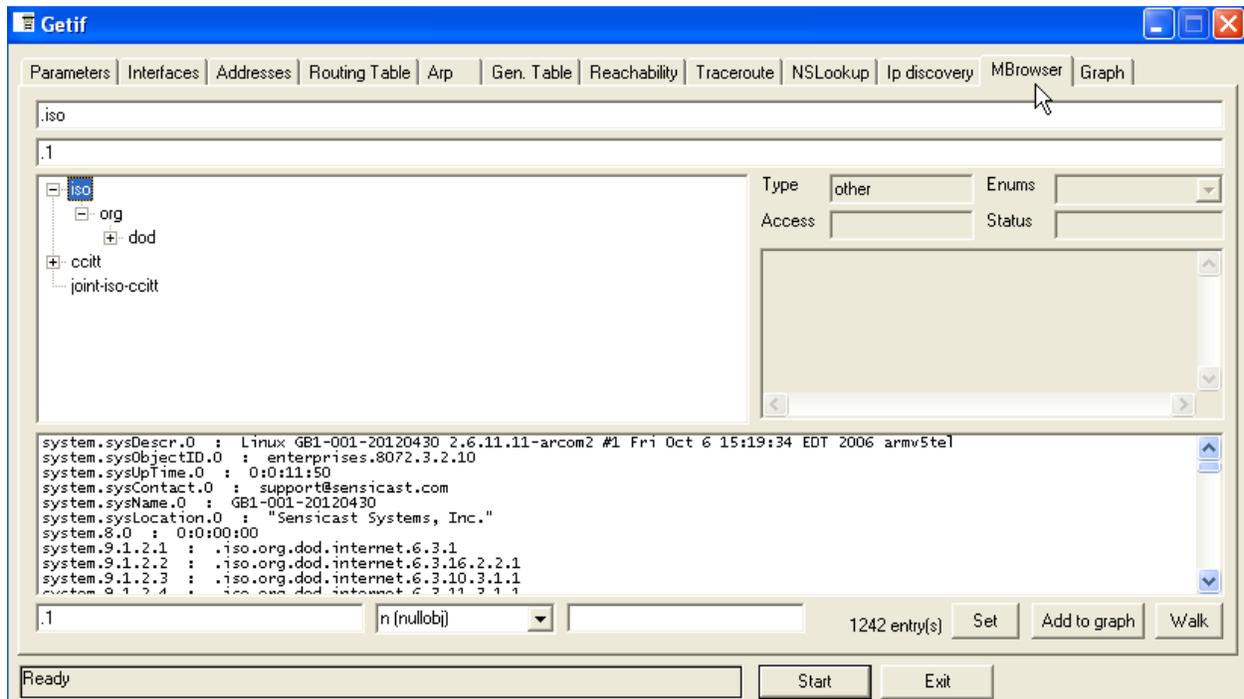


Figure 28: Gateway SNMP GETIF Setup Example

This results in a return of sensor data from the Services Gateway as shown in Figure 29 from the GETIF application where H002B9705446 represents the MAC address of the sensor node being polled.

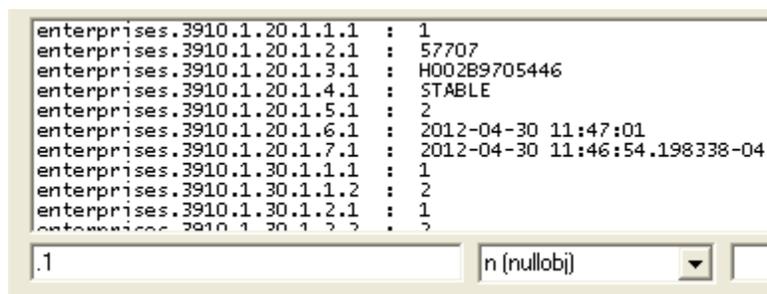


Figure 29: Gateway SNMP GETIF Data Example