



March 2004
EME102A, EME103A, EME104A
EME108A, EME109A, EME110A
EME111A-xx, EME112A-xx, EME113A-xx

ServSensor

Rev. 1.1



This product carries the CE mark to indicate compliance with the European Directive on Electromagnetic Compatibility (89/336/EEC). It has been tested to EN55024:1998 and EN55022:1998.

Contents

What is ServSensor?	6
1. Installation	8
1.1 Installation steps	8
1.2 Assigning IP address	10
2. Intelligent sensors	14
2.1 Installing and configuring sensors	15
2.1.1 Temperature sensor	19
2.1.2 Dual sensor (Temperature & Humidity)	22
2.1.3 Water detector	26
2.1.4 Airflow sensor	28
2.1.5 AC voltage sensor	31
2.1.6 DC voltage sensor	33
2.1.7 Security sensor	36
2.1.8 Dry contact sensor	38
2.1.9 4-20mA converter	43
2.1.10 Power relay board	46
2.1.11 Smoke detector	48
2.1.12 Motion detector	50
2.2 External sensor integration	52
3. Integration with network management systems	53
3.1 HP OpenView	54
3.1.2 Loading the MIB to NNM	54
3.1.3 NNM menu integration	55
3.1.4 Polling SNMP, thresholds and alarm	57
3.1.5 Traps in NNM	59
3.1.6 Graphing with NNM	60
3.1.7 Using the MIB browser	61
3.1.8 Testing alarms in NNM	62
3.2 WhatsUp Gold	64
3.2.1 Monitoring ServSensor with WhatsUp Gold	64
3.2.2 Browsing SNMP variables	65
3.2.3 Graphing the values of SNMP variables	69

3.2.4 Receiving SNMP traps from the ServSensor	73
3.3 MRTG - free data graphing	80
3.3.1 MRTG installation	80
3.3.2 Sample MRTG graphs.....	84
3.4 Frequently used OID's	86
3.5 ServSensor MIB	90
4. SNMP	91
4.1 MIB on the ServSensor	92
4.2 MIB II on the ServSensor	93
4.3 SNMP traps	95
4.4 Trap thresholds	95
4.5 Trap Var Bind information	96
4.6 Community string	98
5. Web based User Interface.....	99
5.1 Login page	101
5.2 Summary page	102
5.3 Sensors setting	104
5.4 Graphing.....	105
5.5 Traps setting	107
5.6 Mail page.....	108
5.7 Network settings	109
5.8 System page	111
5.9 Help menu	113
6. Utilities.....	114
6.1 Utilities	114
6.1.1 IP set.....	114
6.1.2 Data collection	116
6.2 UCD Utilities	117
6.2.1 SNMP Get.....	117
6.2.2 SNMP Set	121
6.2.3 SNMP Walk.....	125
7. FAQ's	129

What is ServSensor ?

The standalone ServSensor is a new intelligent device for monitoring environmental variations, power, physical threats and security. The ServSensor is a completely embedded host with a proprietary Linux like Operating System, including TCP/IP stack, Web server, email, SMS and full SNMP functionality.

The ServSensor works with every intelligent sensor in the BLACK BOX family. You can connect any of our sensors in any combination to monitor temperature, humidity, water leakage, Airflow including long term graphing, security, detect AC Power Line Voltage, Measure DC Voltage, control relays, and many more. Our sensors include an integrated data collection and graphing package to spot trends in the airflow, temperature, and humidity.

Dry contacts and drivers are available for monitoring UPS status, security systems, and air conditioning status.

Every sensor comes with our unique Autosense feature. Whenever a new type of sensor is plugged in, the Autosense will recognize it and reconfigure the ServSensor to begin monitoring it. In the event of an alarm or temperature / humidity threshold being exceeded, it has ability to send alert notification using Email, SMS and SNMP Traps.

The ServSensor's advanced encrypted micro code updating program can update your firmware over the Internet.

A new web based interface with a user and administrator login feature helps users to prevent unauthorized access to the device and a powerful embedded system logging features is available.

The ServSensor is fully SNMP compliant and configurable. Following initial configuration by the RJ45 port to set basic parameters such as IP address, Subnet Mask, Default gateway, SNMP community strings, trusted IP addresses and trap destinations, the unit is fully configurable from any SNMP terminal or Network Management product. Setup is easy with the embedded web server. There is a simple graphing utility

integrated into the ServSensor that can monitor every temperature, humidity sensor and other such factors and can display you the graphical report.

The ServSensor is supplied with a MIB to allow its interface to SNMP based Network Management systems such as HP Open View, IBM Tivoli, CA Unicenter TNG and others.

1. Installation

1.1 Installation Steps

The ServSensor is a plug and play device you can easily connect to your existing network set up.

Every ServSensor has the factory default IP address of 192.168.0.100, and you can change this address if so needed for your network configuration.

Ensure the following items are available with you before installing the ServSensor :

1. A crossover Category 5 or better network cable with RJ 45 male connector
2. A PC with an Ethernet card installed and configured (you can also plug ServSensor into your LAN)
3. A power socket to plug in the AC to DC adaptor for ServSensor
4. You can also assign the IP address using the web based user interface of ServSensor. Go to any web browser such as Internet Explorer, type the factory default IP address (192.168.0.100) and from the system page enter the IP address and click set button. Use a crossover cable connection to perform this step.

An overview of the installation process consists of:

1. Assign an IP address to the ServSensor .
2. Use the embedded web manager to set sensor thresholds, email and trap information.
3. Use your management station or SNMP script to collect information from the ServSensor .

1.2 Assigning IP address

The ServSensor has a 10 Mb/s Ethernet LAN. It uses one 10BASE-T (RJ-45) connector. To set up the ServSensor you must connect it to the network by plugging in the RJ-45 connector and assigning an IP address.

The ServSensor can have its IP address assigned in several different ways. The first way is to statically assign an IP address. This is the simplest and most commonly used method.

The second method is to use DHCP. This stands for dynamic host configuration protocol. This method requires you to have a DHCP server.

Statically Assigning the IP Address.

Static IP Addresses are often used in equipment such as routers and other network equipment. Once a static assignment of an IP address is made, it never changes. All changes to the IP address are saved to EEPROM and retain their values even if power is lost.

Connecting a host to the ServSensor .

In order to assign the IP address, the ServSensor needs to be on the same LAN as the computer that is assigning the IP address. If the ServSensor is on the other side of a router, the router will change the MAC address and this method will not work. The surest way is to use a crossover cable on the local computer, however you can also use most hubs to connect to the ServSensor . From then on you can change the IP address using IPSet.exe The IPSet.exe method cannot traverse routers.

Assigning the IP Address using IPSet.exe

The CD you have received with ServSensor comes with a program called *IPSet.exe*. The *IPSet.exe* program is designed to run on a Microsoft host. Once the program has started enter the MAC address in the section labeled "Client's Mac Address". The Mac address can be located on the sticker on the ServSensor . Next enter the IP address that you wish to assign to the ServSensor . Then press set.

IPSet.exe first checks the IP address to see if it already assigned. Next it will assign the IP address and then it will check that the address was successfully assigned. If all is well then *IPSet.exe* will report that the assignment is Complete.

You can verify the IP assignment by using ping or by using a browser to access the ServSensor . To use a browser enter the address:

http://<ip_address>

depending on the IP address that you have assigned.

Using a Web browser to assign the IP address.

The ServSensor is shipped with the IP address 192.168.0.100

You can enter this IP address into your web browser and use the browser to change the IP address to the new address. For example enter

http://192.168.0.100

into the URL of the web browser and hit return. Once the page has loaded you can press the Network tab and enter a new IP address for the ServSensor .

However, before you can load the web page you usually have to set up the routing table in the host computer. This is because the IP address 192.168.0.100 is probably on a different subnet than the PC. In the usual case the PC will try to connect to 192.168.0.100 using the default gateway, which is not what you want.

To set up the routing table, open a DOS window and at the command prompt enter

route add 192.168.0.100 10.1.1.20

where *10.1.1.20* is the IP address of the Ethernet interface that the ServSensor is plugged into using the crossover cable (basically your PC). Now ping 192.168.0.100 to see if the connection was successful

Using ARP to Assign the IP Address.

You can assign a new IP address to the ServSensor through the use of ARP. The ARP method may be preferable if you do not have access to a Microsoft host or if you prefer to use another host such as Linux to assign the IP address. You can use this method to assign the initial IP address or if you have forgotten the IP address that was assigned to the ServSensor .

To assign a static IP address to the ServSensor , use ARP. Enter the following from the command prompt:

```
arp -s <ipaddress> <EthernetMACAddress>
```

where *<EthernetMACAddress>* is the Ethernet MAC address located on the sticker on the ServSensor and *<ipaddress>* is the IP address you wish to assign.

For example:

```
arp -s 192.189.207.2 00-40-17-03-b2-04
```

To check that you have entered this command correctly, enter:

```
arp -a
```

Now ping the ServSensor from the DOS prompt. For Example:

```
ping 192.189.207.2
```

It is the ping that actually sets the new IP address.

Testing the new IP Address

You have now assigned your ServSensor a new IP address. You can check that this is the case by using ping or by using a web browser. Whenever a new IP address is assigned to a ServSensor that new IP address is saved in EEPROM. This means that the ServSensor will retain its new IP address even after power is recycled. You can test that is the case by cycling power to the ServSensor .

Assigning the IP Address using DHCP

The ServSensor is shipped with DHCP disabled. So if you want to use DHCP, you must first enable this using either SNMP or the web interface. To use the web interface, press the “Network” tab, select “Use DHCP” and then press set.

With DHCP the ServSensor puts out a request to the DHCP server to be assigned an IP address. This is a broadcast message and is forwarded by routers to the DHCP server. The DHCP server responds by sending the ServSensor a new IP address and a lease period.

When the lease period reaches the renew time, which is normally one half of the lease period the ServSensor will send a message to the DHCP server that loaded it to renew its lease. If the server responds, then the lease is renewed for a period of time chosen by the DHCP server.

If the DHCP server does not respond the ServSensor periodically resends the request until the rebind period, which is normally 7/8 of the lease period. At this time the ServSensor puts out a broadcast message for any DHCP server in the enterprise. If the server responds, then the lease is renewed. If the server does not respond then at the end of the lease the ServSensor will voluntarily take its IP address off of the network while continuing to periodically broadcast a request to any DHCP server.

If the ServSensor has a static IP address assigned, it will no longer send out DHCP requests. If you later wish to turn DHCP back on you can do that using the Web Based Manager.

2. Intelligent Sensors

You can use any of our intelligent sensors with the ServSensor .

The following intelligent sensors are available:

- Temperature sensor
- Dual Sensor (Temperature & Humidity)
- Water Detector
- Airflow Sensor
- AC Voltage Detector
- DC Voltage Sensor
- Security Sensor
- Dry Contact Sensor
- Power Relay Board
- 4-20mA Converter
- Smoke Detector
- Motion Detector
- External Sensor

2.1 Installing and Configuring Sensors

Installing the sensors

Simply open a web browser, plug in the sensor and the device will automatically configure itself. The ServSensor will recognize the sensor and begin monitoring it.

Navigating the interface

Choose the page titled Sensors. On the left hand side of the Sensors page is a list of the different types of sensors. Click on type of sensor and your sensor will appear with its port number. Click on the sensor that you want and you will open the Sensor settings screen.

NOTE

After you plug in the sensor and then refresh the summary screen, your sensor will automatically appear in the list of online sensors. If you click on the link under the type column you will be taken immediately to the Sensor settings screen.

Entering data

To change any of the data fields you must press set after inputting the change. The data will not be entered into the ServSensor until the set button is pressed. After you press set, the web page will be refreshed with the new data. Once you see the new data on the web page, it indicates the ServSensor has accepted the data. The ServSensor will have saved this data to nonvolatile memory and it will be protected in case of power failure.

Sensor status color indicator

The colors red, orange and green indicate at a glance the status, red is critical, orange is warning and green is in the normal field.

Disable Autosense

You can disable the Autosense for any port by click on Advanced Setting link at bottom, left of the Sensors page. Use the list box to pick either Enable or Disable the Autosense for a particular port and then click the Set button.

Configuring the sensors

Description: The description identifies this sensor and appears in several places. The description of the sensor appears in the summary page when this sensor is online. The description field is also included in traps and Email for this sensor so that you can identify the reporting sensor.

Status: The Status field shows the current status of the sensor. When the sensor is offline the status is “noStatus”. When the sensor is online the possible status values are “normal”, “WarningLow”, “CriticalHigh”, “WarningHigh”, “CriticalLow” and “sensorError”.

When the sensor is online, the status is formed by comparing the reading from the sensor to the thresholds. In the case of a switch, the status is formed by comparing the value from the sensor with the Normal State. It is recommended that they not be set too narrow as this may cause unneeded messages to be generated.

Online: This is a read only field that can either be online or offline. When the sensor is offline the status is not updated.

Go Online: You place the sensor online or offline by setting this field. Use the single choice list box to pick either GoOnline or GoOffline. Press the Set button below to implement your choice. When the sensor is offline the status is not updated. It may be convenient to take a sensor offline if it is reporting a large number of errors.

Critical High, Warning High, Warning Low, Critical Low: These thresholds are compared to the sensor value several times a second and the status set accordingly. Some sensors such as the temperature and humidity sensors use these thresholds, whereas other sensors such as dry contact inputs only use the Normal State to formulate the status.

Rearm: The Rearm parameter is useful for sensors whose values can vary such as the temperature and humidity sensor.

The Rearm is used to prevent the sensor from flickering between two states. For example if the Warning High threshold for the temperature sensor is set to 80 degrees and the sensor were to vary between 79 and 80 you could be faced with a very large number of emails, traps, and events logged. The Rearm parameter prevents this by forcing the temperature to drop by the Rearm before changing the state back to normal. In this example if Rearm is set to 2 then the sensor would have to drop from 80 down to 77 before the status would change from Warning High back to normal.

Trap/Email Filter

Send Trap/Email On Normal Disable Feature: If not needed this feature can be disabled by choosing 'disable' in the choice box, some people may not want messages to signify normal conditions. Certain applications and special projects may warrant messages being generated when the sensor returns to a normal condition.

Delay Before Sending Trap/Email On Normal: There is also a delay before sending Trap/Email on normal and is set in the same manner as above. In this case the sensor is in the error state and will ignore momentary fluctuations into the normal state.

Continuous time sensor is normal to report: This is for the elimination of unnecessary messages during minor fluctuations. Enter the time in seconds and press the set button. The amount of time that can be entered is between 0 and 65535 seconds, which equals approximately 18 hours.

Example: an airflow or water flow sensor may have temporary drops in readings that are normal operating characteristics, a logical time limit is set to show abnormal conditions.

Minimum time between each Trap/Email: This is the time in minutes between each Trap/Email. This is to prevent sending of multiple Traps/Email, for a same event over a period of time.

Day of week Filter: With this option you can either enable or disable the time period at which the ServSensor should send emails or Traps. The time limit schedule can be configured so that the ServSensor can send Mails/Traps during a fixed time interval. The settings can be made for every day of the week. The time interval range can be from 00:00 hrs to 24:00 hrs. Mails/Traps will not be sent during the time interval set.

2.1.1 TEMPERATURE SENSOR

Temperature sensors are important where optimum temperature control is paramount. If there is an air conditioning malfunction or abnormal weather conditions, damage to information, delicate electronic equipment or warehouse stock may occur.

Up to 8 temperature sensors can be plugged into RJ-45 jacks on the ServSensor. Optional temperature sensors can be purchased with 15 or 60 feet of cable, allowing the sensors to be positioned in hot spots. The ServSensor auto detects the presence of the sensor. Each sensor has its own SNMP OID so that data can be collected over the network and graphed.

A commonly used SNMP OID for the temperature sensor is the number of degrees. This information can be used for graphing the sensor.

The SNMP OID for temperature sensor degrees on RJ45 #1:
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0

Specifications & Features:

- Never needs Calibration
- Measurement range Celsius: -55°C to +125°C
- Measurement resolution Celsius: 0.5°C increments.
- Measurement accuracy Celsius: $\pm 0.5^{\circ}\text{C}$ accuracy from -10°C to +85°C
- Measurement range Fahrenheit: -67°F to +257°F
- Measurement resolution Fahrenheit: 0.9°F increments.
- Measurement accuracy Fahrenheit: $\pm 0.9^{\circ}\text{F}$ accuracy from +14°F to +185°F

- Communications cable: RJ45 jack to temperature sensor using UTP Cat 5 cable.
- Sensor type: semiconductor microprocessor controlled
- Power source: powered by the ServSensor. No additional power needed.
- ServSensor autodetects the presence of the temperature sensor
- Measurement rate: one reading every second
- Up to 8 temperature sensors per ServSensor
- Full Autosense including disconnect alarm
- The ServSensor Temperature Detail page allows you to set and get the working parameters of a specific temperature sensor in the ServSensor.

Configuring the Temperature Sensor

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the temperature sensor.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Current Reading: The number of Degrees is displayed in this field. This is a read-only field. This is an integer SNMP OID field. This value can be polled via SNMP and the data can be used to graph the temperature. The value displayed can be in Fahrenheit or in Celsius. If communication to the temperature sensor is lost, the sensor value -512 will be returned by an SNMP get.

Status: If at any time communications with the temperature sensor are lost, the status of the temperature sensor is changed to “*sensorError*”. If the communication with the temperature sensor is reestablished, the status will be formed by comparing the Degree to the high and low thresholds.

Degree Type: The Degree Type can be set to Fahrenheit or Celsius. When the Degree Type is changed all the threshold fields will change their values automatically. The ServSensor stores the thresholds for both Celsius and Fahrenheit independently allowing you to switch between the two.

2.1.2 DUAL SENSOR (TEMPERATURE & HUMIDITY)

A new sensor from the BLACK BOX family of sensors, the dual sensor has both temperature and humidity measuring capabilities in a single sensor. Now a single port can have two sensors, saving ports for additional sensors. This extends the capability of the ServSensor to measure up to 2 temperature and 2 humidity sensing parameters, just by connecting 2 dual sensors on ServSensor, and 8 temperature and 8 humidity sensing parameters, just by connecting 8 dual sensors on ServSensor.

Up to 8 dual sensors can be plugged into RJ-45 jacks on the ServSensor. Optional dual sensors can be purchased with 15 or 60 feet of cable, allowing the sensors to be positioned in hot spots. The ServSensor auto detects the presence of the dual sensor. Each sensor in the dual sensor has its own SNMP OID so that data from the temperature and the humidity sensors can be collected over the network and graphed simultaneously.

When the dual sensor is plugged into the RJ45 port, the ServSensor will auto detect the sensor, and it will display Temperature & Humidity for each RJ45 port. The user can click the links for Temperature & Humidity and can enter the settings page to configure the sensors.

Specifications & Features:

Temperature

- Measurement range Celsius: -40°C to +125°C
- Measurement resolution Celsius: 0.04°C
- Measurement accuracy Celsius: $\pm 0.5^\circ\text{C}$ accuracy from -10°C to +85°C
- Measurement range Fahrenheit: -67°F to +257°F
- Measurement resolution Fahrenheit: 0.9°F increments.

- Measurement accuracy Fahrenheit: $\pm 0.9^{\circ}\text{F}$ accuracy from $+14^{\circ}\text{F}$ to $+185^{\circ}\text{F}$

Humidity

- Measurement range: 0 to 100% Relative humidity
- Sensor element wettable without damage
- Resolution: 0.5 %
- Accuracy at 25°C $\pm 3\%$,
- Working Range -20°C $+60^{\circ}\text{C}$
- Communications cable: RJ45 jack to dual sensor using UTP Cat 5 cable.
- Power source: powered by the ServSensor. No additional power needed.
- ServSensor autodetects the presence of the dual sensor
- Up to 8 dual sensors per ServSensor
- Full Autosense including disconnect alarm

Configuring the Dual sensor

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the humidity sensor.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Temperature

A commonly used SNMP OID for the temperature sensor is the number of degrees. This information can be used for graphing the sensor.

The SNMP OID for temperature sensor degrees on RJ45#1:
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0

Current Reading: The number of Degrees is displayed in this field. This is a read-only field. This is an integer SNMP OID field. This value can be polled via SNMP and the data can be used to graph the temperature. The value displayed can be in Fahrenheit or in Celsius. If communication to the temperature sensor is lost, the sensor value -512 will be returned by an SNMP get.

Status: If at any time communications with the temperature sensor are lost, the status of the temperature sensor is changed to “*sensorError*”. If communications with the temperature sensor are reestablished, the status will be formed by comparing the Degree to the high and low thresholds.

Degree Type: The Degree Type can be set to Fahrenheit or Celsius. When the Degree Type is changed all the threshold fields will change their values automatically. The ServSensor stores the thresholds for both Celsius and Fahrenheit independently allowing you to switch between the two.

Humidity

A commonly used OID for the Humidity sensor is the percentage, which can be graphed.

SNMP OID for Humidity sensor on RJ45#1

OID .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.0

Percent: The relative Humidity Percent is displayed in this field. This is a read-only field. This integer OID and can be polled. The data can be used to graph the Humidity.

Status: If at any time communications with the humidity sensor are lost, the status of the Humidity sensor is changed to “*sensorError*”. When communications with the humidity sensor are reestablished, the status will be formed by comparing the percentage to the high and low thresholds.

2.1.3 WATER DETECTOR

Water can enter a building in many different ways and in some cases remain undetected, causing damage and problems to sensitive electronic equipment. Computer and mainframe rooms have a false floor and many instances of undetected water laying in these areas has only been detected after a problem occurred. The Water detector is an important addition to your BLACK BOX Sensor inventory.

The Water detector is an exclusive patent pending design capable of detecting the presence of even distilled water. The water detector contains a microprocessor-controlled capacitance measuring circuitry. This is far more precise than standard commercially available water detectors, which measure the resistance of water. The resistance of water can vary depending upon the impurities in the water. Normal resistance type monitors are unable to detect the presence of distilled water due to its high resistance.

The entire circuit is encased in epoxy allowing the water detector to function while submerged in water.

The water Detector detects water leaks and flooding with a WET/DRY indication in software. The ServSensor will retain any error condition until it is read via an SNMP Get. Therefore if a water detector encounters a critical condition at any time it will report that condition before it returns to a normal state.

The value of the Status for the OID for switch sensors can be *“normal”*, *“noStatus”*, *“critical”* or *“sensorError”*.

For a switch type sensor on RJ45#1 the OID for the status is.

.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.0

Features:

- On/Off alarm signal of Water detected
- Accurate, cost effective Water detecting system

- Electronics are encased in epoxy and submersible
- Electronic circuitry capable of detecting distilled water
- Sensor type - open/closed contact switch
- Power source: powered by the ServSensor . No additional power needed.
- ServSensor autodetects the presence of the Water Detector
- Up to 8 Water Detectors per ServSensor
- Includes disconnect alarm that checks that the sensor is securely plugged into the ServSensor

Configuring the Water Detector

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the water detector.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Status: If the sensor is offline the status is “*noStatus*”. If the sensor is online and there is no water detected the status is normal. If water is detected then the status is critical. If at any time communications with the Water Detector are lost, the status of the Water Detector is changed to “*sensorError*”.

2.1.4 AIRFLOW SENSOR

The airflow sensor is a device that registers airflow in areas where consistent flow is needed, for example in cabinets and racks where the consistent operation of a fan is critical to the operational safety of electronic equipment.

The airflow sensor is placed in the air stream, where the user can monitor the status and the amount of flowing air. In addition to an on/off indication, it also graphs the analog values over a period of time, although not a precision airspeed measurement device. If for example, the fan slows down the user will be given an indication of the change over time. This may happen if the fan is close to failure or the air filter is clogged. The ServSensor shows this information using a graph via the web interface.

The value of the Status for the OID for switch sensors can be *“normal”*, *“noStatus”*, *“critical”* or *“sensorError”*.

The recognized OID for switch Sensors is 1 or 0, for RJ45 #1 it is

OID .1.3.6.1.4.1.3854.1.2.2.1.18.1.3.0

Features:

- On/Off alarm signal of airflow
- Airflow data graphically displayed over time
- Accurate, cost effective flow sensing
- 2 LEDs indicate the status of Airflow and that the sensor is securely plugged into the ServSensor
- Electronics are mounted in a small plastic case
- Sensor type - open / closed contact switch
- Power source: powered by the ServSensor . No additional power needed.

- ServSensor autodetects the presence of the airflow sensor
- Up to 8 Airflow Sensors per ServSensor .
- Includes disconnect alarm that checks that the sensor is securely plugged into the ServSensor

Specifications:

- Data graphically displayed via a web page
- Data collection possible via any SNMP based network management system
- Measurement rate: one reading each second, data logging once per minute
- Communication cable: RJ45 jack to the ServSensor
- Sensor type: Thermistor
- Sensor power: line power from ServSensor
- Trap information: status, sensor number, sensor description, airflow (%)

Configuring the airflow sensor

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the airflow sensor.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Current Reading: The percentage of airflow is displayed in this field. This is a read-only field. This is an integer SNMP OID field. This

value can be polled via SNMP and the data can be used to graph the airflow. The values range is from 0 to 100 %

Status: If the sensor is offline the status is “*noStatus*”. If the sensor is online the status will be formed by comparing the readings to the high and low thresholds. If at any time communications with the Airflow Sensor are lost, the status of the airflow sensor is changed to “*sensorError*”.

2.1.5 AC VOLTAGE DETECTOR

The voltage detector is used to indicate the presence or absence of line voltage. This is useful, for example to tell when the UPS is running on battery power.

The AC Voltage Detector indicates an ALARM/NORMAL condition in software and also via an LED mounted on the sensor. Voltage detectors can detect the presence or the absence of line voltage. It is designed for use worldwide. There is an SNMP interface for getting the alarm/normal status. SNMP traps are sent when critical conditions occur. SNMP polling via 'get' is available to retrieve existing status and configuration parameters. The Web browser interface is also available to display the status and configuration parameters.

When an alarm condition is activated the description and location of the fault can be sent via email, page or traps.

The value of the Status for the OID for switch sensors can be *“normal”*, *“noStatus”*, *“critical”* or *“sensorError”*.

The recognized OID for switch Sensors is 1 or 0, for RJ45 #1 it is

OID .1.3.6.1.4.1.3854.1.2.2.1.18.1.3.0

Specifications & Features:

- Measurement range - Detects voltage at 50V AC to 250V AC
- LED indicator on sensor shows if voltage present
- Measurement Indication - Alarm or Normal
- Communications cable - RJ45 jack to sensor using UTP Cat 5 wire.
- Sensor type - open / closed contact switch
- Power source: powered by the ServSensor . No additional power needed.

- ServSensor autodetects the presence of the voltage sensor
- Measurement rate - multiple readings every second
- Up to 8 AC Voltage sensors on the ServSensor
- Full Autosense including disconnect alarm

Configuring the AC voltage Detector

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the AC voltage sensor.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Status: If the sensor is offline the status is “*noStatus*”. If the sensor is online and there is no AC voltage detected the status is critical. If AC voltage is detected then the status is normal. If at any time communications with the AC voltage detector are lost, the status of the AC voltage detector is changed to “*sensorError*”.

2.1.6 DC VOLTAGE SENSOR

Any company or building with a large battery bank or solar power storage or involvement in the manufacture or storage of batteries needs this sensor.

The DC voltage sensor is a custom sensor that works very much like a digital multimeter. The DC voltage sensor can measure voltages in the range of 0-60 volts.

One popular OID for the DC Voltage Sensors is the percentage of full-scale reading.

For a DC Voltage sensor plugged into RJ45#1 that OID is:

.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.0

Specifications & Features:

- Measurement range - 0-60V
- Overvoltage protection. A relay within the DC Voltage sensor will protect the ServSensor .
- Status range - High Warning, Low Warning, High Critical, Low Critical
- Communications cable - RJ45 jack to sensor using UTP Cat 5 wire, Maximum extension cable length 100 foot with approved low capacitance shielded cable or UTP.
- Resolution - 10 bit A/D converter
- Accuracy - 2LSB
- Power source: powered by the ServSensor . No additional power needed.
- ServSensor autodetects the presence of the DC voltage sensor

- Measurement rate - multiple readings every second
- Up to 8 DC voltage sensors per ServSensor
- Full Autosense including disconnect alarm

Configuring the DC voltage sensor

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the DC voltage sensor.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Current Reading: The percentage of DC voltage is displayed in this field. This is a read-only field. This is an integer SNMP OID field. This value can be polled via SNMP and the data can be used to graph the airflow. The values range is from 0 to 100 %. This value depends on the jumper settings in the DC Voltage sensor box. If 10V is selected, then 0 to 10VDC is mapped to 0 to 100 %, if 20V is selected, then 0 to 20VDC is mapped to 0 to 100%.

A/D base in 1/10-volt increments: This is the minimum voltage that the DC Voltage sensor will output. This value in conjunction with the maximum voltage from the sensor is used to determine the percentage of the sensor.

A/D max, Range 0-40, 40 is 4 volts: This is the maximum voltage that the DC Voltage sensor will output. This value in conjunction with the minimum voltage from the sensor is used to determine the percentage of the sensor. So if the input jumper on the DC Voltage sensor is set to 60, and the input voltage is also 60 volts then the DC Voltage sensor will output 4 volts to the ServSensor and this is 100% of full scale.

Status: The status is formed by comparing the percentage of full scale to the high and low thresholds. So if the A/D base is set to 0(This is 0 volts) and the A/D max is set to 40(this is 4 volts) then if the actual

voltage from the DC Voltage sensor going into the ServSensor is 2 volts, then 2 volts is 50% of full scale. In this case the scale is from 0 to 4 volts and the input is 2 volts, then this is 1/2 of full scale.

The percentage of the input voltage is then compared to the thresholds of Low Warning, High Warning, High and Low Critical that the user has set. From this the status is then computed and emails, traps are sent if necessary.

Jumpers

The DC Voltage sensor has a jumper to set the expected range of input voltages. This can be set to 10, 20, 30, 40 or 60V. You should use the lowest expected settings in order to achieve the maximum resolution.

2.1.7 SECURITY SENSOR

The Security sensor is a magnetic on/off switch that is used as an input to the ServSensor . Security sensors come in pairs. They are active switches that close when one half of the sensor is in close proximity to its mate. When the two sensor pairs are moved apart from each other they open. The ServSensor senses closure and opening and reports the condition.

Security Sensors can be wired in series so that multiple sensors can use a single port on the ServSensor . There are no reasonable limits on the distance of the security sensors from the ServSensor .

The ServSensor will retain any error condition until it is read via an SNMP get. Therefore if a security sensor encounters a critical condition at any time it must report that condition before it can return to a normal state.

A popular OID for switch Sensors is the status. For RJ45 #1 it is

OID .1.3.6.1.4.1.3854.1.2.2.1.18.1.3.0

Features

- On/Off alarm signal when Security Sensors switches open/closed
- Accurate, cost effective Security System
- Electronics are simple and reliable
- Sensor type - open/closed contact switch
- Power source: powered by the ServSensor . No additional power needed.
- ServSensor autodetects the presence of the Security sensor
- Up to 8 Security Sensors per ServSensor
- Includes disconnect alarm that checks that the Security sensor is securely plugged into the ServSensor

Configuring the Security sensor

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the Security sensor.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Status: If the sensor is offline the status is “*noStatus*”. If the sensor is online and there are no open Sensors detected the status is normal. If an open Sensor is detected then the status is critical. If at any time communications with the Sensor are lost, the status of the Security Sensor is changed to “*sensorError*”.

2.1.8 DRY CONTACT SENSOR

The Dry Contact sensor is a simple connection to burglar alarms, fire alarms or any application that requires monitoring by the ServSensor .

These general-purpose switches can be either input or output. When used as an output it can source up to 20mA. You can select the output voltage by setting the Output Level to a Low or a High. When set to Low the pin will output 0 volts. When set as a High the pin will output 5 volts.

When used as an input a switch will retain any error condition until it is read via SNMP. Therefore if a switch encounters a critical condition at any time it must report that condition before it can return to a normal state.

Input pins can be used to detect whether or not an input switch is open or closed. In combination with external sensors, input pins can detect whether a door or window is open or closed, if there is a water incursion and many other conditions.

The input pins work by sensing the presence of a voltage level on an input pin. When the switch is open the voltage is different than when the switch is closed.

To test a dry contact input, wire ground to one side of the switch. Ground is always pin 8 on the connector. Wire the other side of the switch to the switch sensor. Set the “*NormalState*” to High. Set the “*Direction*” to Input. When the switch closes the input pin will be shorted to ground and the switch will change state from normal to critical

Specifications & Features:

- Measurement Indication - Alarm or Normal
- Communications cable - RJ45 jack to sensor using UTP Cat 5 wire.

- Sensor type - open/closed contact switch
- Power source: powered by the ServSensor . No additional power needed.
- ServSensor autodetects the presence of the voltage sensor
- Measurement rate - multiple readings every second
- Up to 8 sensors on the ServSensor
- Full Autosense including disconnect alarm

Configuring the Dry Contact Sensor

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below refer to the fields that are special to the Dry contact sensor.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Direction: The Switch Direction can be either Input or Output. When set as an Input, the sensor will report its status as “normal”, “highCritical”, or “lowCritical”. The status is normal if the “NormalState” matches the current value applied to the sensor. For example if the “NormalState” is high and the Input to the sensor is high then the status is normal. The input voltage should be limited to 0 to 5 volts in order to protect the sensor.

If the Direction of the sensor is Output, the sensor can be used to drive external equipment.

OutputLevel: The Switch “OutputLevel” can be either High/+5 Volts or Low/GND. When set to a High, the output value of 5 volts will be applied to the switch. When set to a Low the “OutputLevel” will depend upon the value of Direction. If Direction is set to Output and the “OutputLevel” is set to low, the Switch will source current in

order to maintain 0 Volts. If Direction is set to Input and the OutputLevel is set to low, the Switch will become tri-state.

The Output level of High will pull-up the switch even if the Direction is set to Input. However when the Switch Direction is set to Input and Output level is set to high the Switch will output a weak pull-up current. This output can be overridden by shorting the pin to ground. In this way an external switch can be determined to be open or closed.

NormalState: The Switch *NormalState* can be either Open/+5 Volts or Closed/GND. When set to a +5 Volts, the input value of 5 volts will cause the status to be reported as “normal”. When set to +5 Volts, the input value of 0 volts will cause the status to be reported as “lowCritical”. When the Switch *NormalState* is set to a Low, the input value of 5 volts will cause the Status to be reported as “highCritical” and the input value of 0 volts will cause the status to be reported as normal.

Information on Dry contact cables

The extension length of the dry contact twisted pairs is limited only by the amount of electromagnetic noise in the area. So the lengths can be quite long, but long cable lengths may create occasional false positives. These false positives can be eliminated with the advanced filtering of the ServSensor . You can define how long a sensor must be in the error condition before changing state from Normal to Critical. You can also define how long the sensor must remain in the Normal state before changing from Critical to Normal.

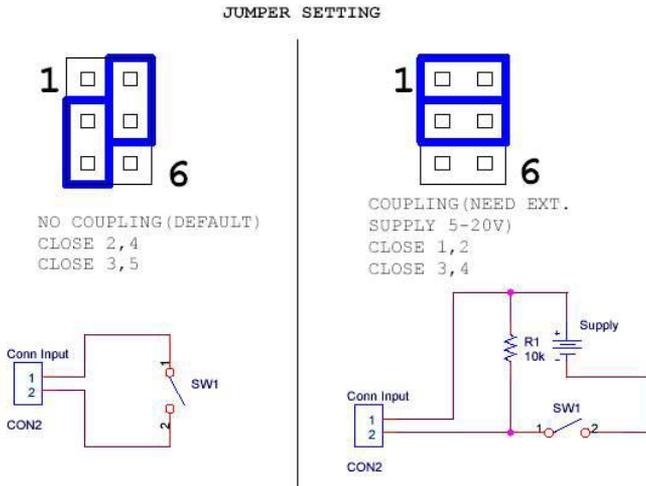
If the dry contact cable is run outdoors where lightning strikes may occur or if the cable length is very long we recommend the use of the ServSensor X20 or the ServSensor X60, which includes integrated opto-isolators. This will protect the ServSensor X20/X60 in case of a lightning strike. This is because there is no connection to the power supply in the ServSensor X20/X60. This is done in order to provide complete isolation and protection to the ServSensor X20/X60.

Special Dry Contact settings for the X20 and X60 models of the ServSensor ports 9-68.

By default, X20 and X60 will have the jumpers set as in Fig 1. for ports 9-68

Fig 1

Fig 2



The simplest setup for Dry Contact inputs is as shipped. In this setup power is provided by the ServSensor to the switches. With the ServSensor providing the power, the switch has +5 Volts applied to pin 1 and GND applied to pin 2. When the switch is open, the input senses +5, when the switch closes, the input senses GND. No additional external power is needed.

Figure 2 shows the jumpers set up to provide opto-isolators support. Opto-isolators provide complete electrical separation between the ServSensor and the dry contact. The ServSensor is therefore protected against possible large voltage spikes caused by lightning for example.

The user can change the settings by opening the top cover of the ServSensor -X20 and changing the jumper settings according to the Fig 2. This will set up the X20 for opto-isolators inputs.

NOTE

Dry contact ports - ports 9-68 on the X20 and X60 models of the ServSensor do not have the Autosense feature. The user has to manually place these ports online.

2.1.9 4-20mA CONVERTER

The 4-20mA signal converter is used to integrate the ServSensor with a 4-20mA transmitter. 4-20mA technology is used to communicate analog signals over long distances where electrical interference is a problem. This solution is often used in the process control industry to collect the analog values from a wide array of remote sensors. Current signals are much less susceptible to noise than voltage signals. A voltage signal can be converted to current and then broadcast over a long distance before it is converted back to voltage and read by the ServSensor .

4-20mA transmitters are common in the industry for use with high quality sensors. With the 4-20mA converter these sensors can now be integrated into the ServSensor enhancing their value with the addition of graphing, web interface, email interface, thresholds, and limits.

One popular OID for the 4-20mA Converters is the percentage of full scale reading.

For a 4-20mA Converter plugged into RJ45#1 that OID is:

.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.0

Specifications & Features:

- Electronics housed in small plastic case
- LED indicators on Converter show connection to ServSensor
- Communications cable - RJ45 jack to sensor using UTP Cat 5 wire.
- Power source: powered by the ServSensor . No additional power needed.
- ServSensor autodetects the presence of the 4-20mA Converter

- Up to 8 4-20mA Converters on the ServSensor
- Full autosense including disconnect alarm

Configuring the 4-20mA Converter

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the 4-20mA Converter.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

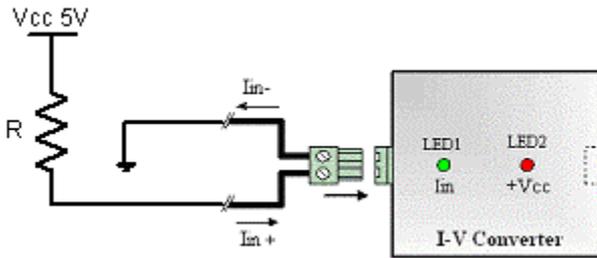
Current Reading: The percentage of current is displayed in this field. This is a read-only field. This is an integer SNMP OID field. This value can be polled via SNMP and the data can be used to graph the airflow. 4-20mA current is mapped to 0 to 100 %.

A/D base in 1/10 volt increments: This is the minimum voltage that the 4-20mA Converter will output. This value in conjunction with the maximum voltage from the sensor is used to determine the percentage of the sensor. For the 4-20mA Converter this value is automatically set to 8. In other words, when the Converter has 4mA as an input, the output to the A/D converter in the ServSensor will be 8 volts

A/D max, Range 0-50, 50 is 5 volts: This is the maximum voltage that the DC Voltage sensor will output. This value in conjunction with the minimum voltage from the sensor is used to determine the percentage of the sensor. For the 4-20mA Converter the A/D max is set to 40. In other words, when the Converter has 20mA as an input, the output to the A/D converter in the ServSensor will be 4 volts.

Status: The status is formed by comparing the percentage of full scale to the high and low thresholds. The percentage of the current to full scale is then compared to the thresholds of Low Warning, High Warning, High and Low Critical that the user has set. From this the status is then computed and emails, traps are sent if necessary.

Below is an illustration of a typical 4-20mA settings:



Input Current

Percent (%)

4.06mA	1
9.9mA	36
15.1mA	69
19.8mA	99

2.1.10 1-PORT POWER SWITCH

The 1-Port Power Switch allows the user Remote actuation of electrical devices over Internet. It provides 1 high-power SPDT 5V relay. It includes Metal Oxide Varistors (MOVs) and Snubber circuits to protect the open contact of the relays from the high voltage spikes or noise transients. It monitors the power & load and accepts a control signal that is sent from the ServSensor .

Applications:

- Power Switching
- On/Off Control
- Activate Alarms
- Process Control
- Energy Management Systems

Specifications & Features:

- Relay contacts rated at 15 A @ 220 VAC with Resistive Load
8 A @ 220 VAC with Inductive Load (P.F=0.4, L/R=7ms)
- Contact Material AgCdO
- Max. Operating Voltage 380 VAC, 125 VDC
- Max. Switching Capacity 4,000 VA, 480W with Resistive Load
2,000 VA, 240W with Inductive Load (P.F=0.4)
- Min. Permissible Load 100mA, 5 VDC
- Power Consumption 5V @ 200mA
- Circuit Breaker 16 A
- 15Amp Fuse 380 VAC, 125 VDC

- Communications cable - RJ45 jack to sensor using UTP Cat 5 wire.
- Sensor type - open/closed contact switch
- Power source: powered by the ServSensor . No additional power needed.
- ServSensor autodetects the presence of the Power Relay Board
- Up to 8 Power Relay Boards on the ServSensor
- Full autosense including disconnect alarm
- Metal Oxide Varistors (MOVs) and snubber circuit protect the open contacts of the relays from high voltage spike.
- 4 LEDs indicate the status of the Relay, Power Supply, AC Line Voltage and AC Load Voltage.
- Dimensions 65(W) x 62(H) x 15(D) mm
- Operating Temperature -40°C to 85°C

Configuring the 1-Port Power Switch

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the Power Relay Board.

For a general description about configuring all sensors including information regarding common configuration parameters please see the [Installing and Configuring Sensors](#) page.

Status: If the sensor is offline the status is “*noStatus*”. If the relay is ON, then the status is “*normal*”, and if the relay is in OFF position, then the status is “*critical*”. If at any time communications with the Power Relay Board is lost, the status is changed to “*sensorError*”.

2.1.11 SMOKE DETECTOR

An important addition to security and safety: These smoke detectors are easy to install and configure. The smoke detector must be mounted on the ceiling for maximum smoke detection.

The value of the Status for the OID for switch sensors can be “*normal*”, “*noStatus*”, “*critical*” or “*sensorError*”.

A popular OID for Smoke Detector Sensors is the status. For RJ45 #1 it is

OID .1.3.6.1.4.1.3854.1.2.2.1.18.1.3.0

Features:

- On/Off alarm signal of Smoke Detected
- Accurate, cost effective Smoke Detector
- LED indicates the status of Smoke Detector
- Sensor type - open/closed contact switch
- Up to 2 Smoke Detector Sensors per ServSensor
- Includes disconnect alarm that checks that the sensor is securely plugged into the ServSensor

Configuring the Smoke Detector

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the Smoke Detector.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Status: If the sensor is offline the status is “noStatus”. If the sensor is online and there is no smoke detected the status is normal. If smoke is detected then the status is critical. If at any time communications with the smoke detector are lost, the status of the smoke detector is changed to sensorError.

When a smoke detector is connected, the ServSensor will sense it as dry-contact sensor. The user can change the description to a smoke detector.

The Web interface settings for the smoke detector are:

Direction: Input

Normal State: Open/+5 Volts

Output Level: Low/GND

2.1.12 MOTION DETECTOR

The motion detector is housed in an attractive wall mountable unit and easily added to your ServSensor network to provide security for any building.

A popular OID for motion detector Sensors is the status. For RJ45#1 it is

OID .1.3.6.1.4.1.3854.1.2.2.1.18.1.3.0

Features:

- On/Off alarm signal of Motion detected
- Accurate, cost effective motion detecting
- LED in housing indicates movement sensed
- Electronics are mounted in attractive, angle adjustable wall mountable unit
- Sensor type - open/closed contact switch
- Power source: powered by the ServSensor . No additional power needed.
- ServSensor autodetects the presence of the Motion Detector
- Up to 2 Motion Detector Sensors per ServSensor
- Includes disconnect alarm that checks that the sensor is securely plugged into the ServSensor

Configuring the motion detector sensor

Since all of BLACK BOX's intelligent sensors are configured similarly not every field is described below. The descriptions below describe the fields that are special to the motion detector.

For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

Status: If the sensor is offline the status is “*noStatus*”. If the sensor is online and there is no motion detected the status is “*normal*”. If motion is detected then the status is “*critical*”. If at any time communications with the motion detector are lost, the status of the motion detector is changed to “*sensorError*”.

2.2 External Sensor Integration

ServSensor external sensor integration allows the user to integrate a custom sensor to the ServSensor while still retaining all of the features of the standard sensors. This interface has the full range of functionality including SNMP integration, email and trap generations with adjustable limits and thresholds.

Customers have added pressure transducers, solar power monitors, battery monitors, and have integrated the ServSensor into laboratory test equipment. For plant nurseries, hospitals and many other applications are possible where monitoring is essential.

This interface can be used by OEMs and engineers to create their own custom data collection systems. The user can configure sensor input voltage range from 0 to 60 volts through the addition of the DC Voltage sensor directly into the ServSensor if the transducers voltage does not exceed 5 volts.

Readings are available in both raw data and as a percentage of full scale. Full scale is user programmable with both the base and top voltage from 0 to 60 volts. SNMP interface shows alarm/normal status. SNMP traps sent when status changes. SNMP polling via 'get' is available. Web browser interface is also available. When an alarm condition is activated the description and location of the fault can be sent via email.

All data values from the sensor are graphed overtime using the internal memory of the ServSensor .

For more information on setting up and configuring an external sensor see the page describing the DC Voltage Sensor.

3. Integration with Network Management System

ServSensor is embedded with full SNMP and can integrate with any SNMP based network management systems, such as HP OpenView NNM, IPSwitch WhatsUp Gold, CA Unicenter TNG, Tivoli, Compaq Insight Manager etc. The ServSensor comes with a MIB file that can be easily loaded to your network management system and can receive SNMP alerts.

By default the traps are for WhatsUp Gold style. The user can change the traps to HP OpenView NNM or to WhatsUp Gold or both by using the command:

```
SNMPset <IP> <community> .1.3.6.1.4.1.3854.1.2.2.1.60.0 i X
```

where *IP* is the IP address of the ServSensor . *community* default is "*public*". and *X* can take 3 values: 1 (WhatsUp Gold style), 2 (HP OpenView Style) or 3 (both Style). By default, the *X* value set is 1.

3.1 HP OpenView

3.1.1 LOADING THE MIB TO NNM

From the NNM menu press Options, then Load / Unload MIBs: SNMP. The dialog box for Loading / Unloading MIBs appears. Press Load. A dialog box entitled: "*SNMP MIB Files Not Found*" appears. Press the Browse button. If you are installing this software from the floppy disk go to A:\bin and find the *sp.mib* file. If you are installing the MIB after running setup the file *sp.mib* can be found in the bin directory under the installation root. For example:

"C:\Program Files\sa\bin\sp.mib"

Press open to load this MIB. Press **OK** to load the Trap definitions.

3.1.1 NNM MENU INTEGRATION

You can easily integrate *hhmsagent* into the NNM menu. You can add graphing, the Web Based Monitor Application, online web based documentation to the NNM Menu. This enhancement is optional but it adds a number of important features.

Because the management and documentation are web based, they can be used on any platform such as an HP-UX box or a Sun or other UNIX system. By adding the Web Based Manager to the NNM menu it becomes easy for the user to interact with the SNMP agent *hhmsagent*, regardless of his location or platform.

The NNM menu is also enhanced to add graphing. The user can graph all of the temperature or humidity values for every ServSensor . Whenever the user wants to observe temperature trends across the enterprise he can do it with a single button.

When the SNMP agent *hhmsagent* was installed on the NT a file was created to allow this menu to be added to NNM. This file is called an Application Registration File or ARF. An ARF file is used by HP to customize and integrate third party applications such as the *hhmsagent* into NNM. The name of this file is called *hhms* and it is located where you installed the agent when you ran *setup.exe*. For example a typical location would be *C:\Program Files\sa\bin\sa*.

In order to integrate this ARF file into NNM you must copy the file to the proper directory so that NNM can find it when it starts. In the simplest case of an NT running NNM that directory might be *C:\OpenView\registration\C*. This path would vary depending upon your choices during installation of NNM. On a UNIX platform the path to copy *hhms* to would be *\$OV_REGISTRATION/\$LANG*. In most cases *\$LANG* would be *C*. The *C* would indicate that the English language is being used. You will find other registration files in that directory such as *ovw*, *ovweb*, and *nmm*.

After you have copied *hhms* to the correct directory you must restart NNM. When NNM restarts you should see *hhms* on the NNM menu. Under *hhms* you should find the menu picks to launch the Web Based

Manager, graph of every temperature sensor, and the status of every sensor.

The *hhms* file can also be customized with a standard text editor. You may wish to include graphs of humidity sensors or switches. In addition any sensor status can be visually graphed.

3.1.4 POLLING SNMP, THRESHOLDS AND ALARM

NNM can read the Status field to determine if any of the sensors has a problem. Polling is the most effective method of monitoring because if network connectivity is lost, polling will reveal this failure. While the ServSensor does send traps there is no guarantee that a trap will be delivered to the monitoring station.

The network traffic generated by polling is very limited. The temperature sensor need only be read once every five minutes or more depending on your needs.

Setting Up Polling

To setup polling go to the NNM toolbar and enter Options/Data Collection & Thresholds: SNMP

The dialog box appears. Enter Edit/MIB Object/New

The dialog to pick the OID to monitor appears. Click on the + to expand the private tree. Then expand enterprises/BLACK BOX/hhmsagent. This exposes the *hhmsagent mib*.

You can monitor the status of an individual sensor by choosing the status OID for that sensor.

A second dialog appears allowing you to further refine the details of what you wish to poll. Enter the IP Address of the ServSensor in the Source field. Press Add to add that data source to the list of nodes to be monitored.

Next you can change the polling interval. For now we will enter 5s. This will cause the node to be polled every 5 seconds. This is often for a working environment. However it will help to test the *hhmsagent* if we poll more often. Once testing is complete we can set the polling to a larger interval.

Set the Threshold Parameters to ≥ 3 . This means that we will cause an alarm to be triggered whenever the status is greater than or equal to

3. When the status is equal to 3 this means that the status of one of the sensors is at warning.

Set the Rearm value to < 3 . When the status is at 2 then the sensors are at or below normal status. When the status is at 1 then the sensors status is *“noStatus”*. The *“noStatus”* status is set when the sensor is set to *“offline”*.

Set the Consecutive Samples to 1 for both the Threshold and The Rearm sections. Set the Rearm Value Type to Absolute. Press OK to add this MIB Object to the collection list and return to the main dialog.

In order for this new collection to become effective you must save it. From the dialog menu enter File/Save. You are now polling the sensor Status

3.1.5 TRAPS IN NNM

The ServSensor sends traps whenever their status changes. These traps are defined in the file `sp.mib`. To act upon these traps open the Event Configuration dialog box under the Options menu of NNM. When the Event Configuration dialog box loads, scroll down the top box until you can select `hhmsagent`. The bottom list box will now list the traps available using *hhmsagent*. Select a trap from the bottom list and then from the Dialog menu press Events/Modify. The Modify Events dialog box appears. Press Event Messages and then press Log and display in category: Choose Application Alert Alarms. Now press Actions.

You may enter a message under the popup window entry. You can include in the message variable binding information if the trap comes from the ServSensor. To include variable binding information, use \$1 \$2 \$3 \$4 \$5 \$6 in your message. These macros are defined here.

You can now close this dialog box and go back to the Event Configuration dialog box. Under the "File" menu choose "Save". Now you will see the traps in the Application Alert Alarm Browser and the All Alarms Browser.

3.1.6 GRAPHING WITH NNM

The easiest way to graph is with utility *xnmgraph*. From a DOS command prompt enter:

You can graph an individual temperature sensor on the ServSensor .

To graph the first temperature sensor on the ServSensor hostname 10.1.1.7 enter:

```
xnmgraph -mib ".1.3.6.1.4.1.3854.1.2.2.1.16.1.3::0:::" 10.1.1.7
```

To graph the second temperature sensor on the ServSensor hostname 10.1.1.7 enter:

```
xnmgraph -mib ".1.3.6.1.4.1.3854.1.2.2.1.16.1.3::1:::" 10.1.1.7
```

The graph utility *xnmgraph* does not save its data. When the program exits, all data is lost. If you wish to keep long-term data you must save it. If you have been collecting data, *xnmgraph* will read it in when it first starts.

To set up data collecting from the NNM menu, enter Options / Data Collection & Thresholds: SNMP. When the Data Collection & Thresholds: SNMP dialog loads enter Edit/MIB Collection / New. When the Collection dialog box loads Set Collection Mode: Store No Thresholds. Enter the Source hostname and add it to the Source List. Press OK to finish with this Dialog and then press File / Save to start collecting.

3.1.7 USING THE MIB BROWSER

Start the browser by pressing Tools from the NNM menu, then SNMP MIB Browser. Enter the Name or Address of the SNMP ServSensor .

Enter the Community name of the ServSensor . The community name is often set to *public*.

Press private to expose the mib tree under the private OID. Then press enterprises, BLACK BOX, hhmsagent.

You will probably not use the MIB browser very much. All of the information available from the MIB browser is also available from the Web Based Manager. The Web Based Manager also contains additional features and is presented in an easier to use format.

What to do if the MIB Browser Doesn't Work

The most common cause of failure to communicate with the ServSensor is the use of the wrong community string or the wrong host IP address. If you believe that those parameters are correct you can trace the communication using a LAN analyzer such as Microsoft's netmon.

3.1.8 TESTING ALARMS IN NNM

The following example tests the first temperature sensor but the idea is the same for the other sensors. The first thing to do is to make sure that the temperature sensor is online. Press the link to the Sensors at the top of the page. Now press the button at the left labeled Temperature. Then choose the first temperature sensor.

If the temperature sensor is plugged into the first sensor RJ-45 the Autosense will have placed this sensor online. Check to see if the sensor is online. The Status should be normal if the temperature is within the thresholds. If the Status is “*sensorError*” make sure that the temperature sensor is plugged into the first sensor RJ-45 jack.

While you cannot set the Status directly, you can test the sensor Status.

Setting the High Warning

In order to cause an alarm to take place you will need to set the High Warning near to the current room temperature but high enough so that it can go back to normal. The status of the temperature sensor will go to “*highWarning*” when the Degree meets or exceeds the high warning threshold. The sensor will not go back to normal however, until the Degree goes below the high warning threshold by the Rearm amount. This is done to prevent the status from flickering.

If the room temperature is 72 and the Rearm is 2, then a good choice to set high warning to is 76. To set the “*highWarning*” use the Web Based Manager. Enter 76 into the “High Warning” field and press Set.

Changing the Temperature

In order to change the temperature, warm the sensor by holding it in you hands. The sensor is the small black plastic package at the end of the cable. Hold the temperature sensor until the Degree starts to rise.

To see the change on the Web Based Manager you must refresh the browser. Press the Temperature0 button. You will see the Degree field begin to change.

Changing the Status

Press the Summary button in the Select a View box of the Web Based Manager. The summary will show the new Degree. When the Degree reaches the High Warning threshold the status of the temperature sensor will change to highWarning.

Verifying Alarms

When the status changed a number of things happened to notify you of this change. A Trap was sent if the ServSensor was configured to send traps. If NNM was polling the Status an Alarm occurred.

If you have set up NNM to receive Traps from the ServSensor you will see a Popup window appear.

If you have set up Polling in NNM verify that an alarm has actually occurred by opening the Threshold Alarms Browser or the All Alarms Browser. There should be an alarm caused by the polled OID Status going to warning that is the integer value of 3.

Resetting the Sensor Status

The temperature sensor will drift back to room temperature. You can see this using the Web Based Manager by pressing the Summary View to refresh the browser. You can also enter a value in the Auto Refresh Browser Interval field. This will cause the browser to automatically refresh itself.

You will see the Degree change. When the Degree plus the Rearm amount is less than the High Warning threshold the status of the sensor and the value of the Status OID will change back to normal. When this Status changes you will again be notified with a Trap. If NNM was polling the Status an Alarm will occur.

Resetting Thresholds

If you changed the NNM polling interval, go back to the NNM Data Collection and Threshold dialog and reset the polling interval to 1 minute.

3.2 Whats UP Gold

3.2.1 MONITORING SERVSSENSOR WITH WHATSUP GOLD

Setting up the MIB identifier

WhatsUp Gold provides a command line program named `mibextra.exe` used to update the MIB and the trap information that WhatsUp Gold references. The program is located in the directory where WhatsUp Gold is installed.

To run the MIB extractor: at the command prompt enter:

```
WhatsUp> mibextra directory_name\sp.mib
```

NOTE

If the mib extractor returns “failed to open file” error, the MIB file `sp.mib` has dependencies. These dependency files are listed in the import section of the MIB file and must be provided in the same directory as the MIB file.

Now see next topic - Browsing SNMP variables

3.2.2 BROWSING SNMP VARIABLES

The SNMP device needed to be monitored must be created and added to a network map, this network map could be the existing one or one newly created.

1. Creating a blank network map

1.1 From the File menu of WhatsUp Gold, select 'New Map Wizard'

1.2 Choose 'Create a blank map'

Press the Finish button. The network map editor window will come up (see Figure 1.)

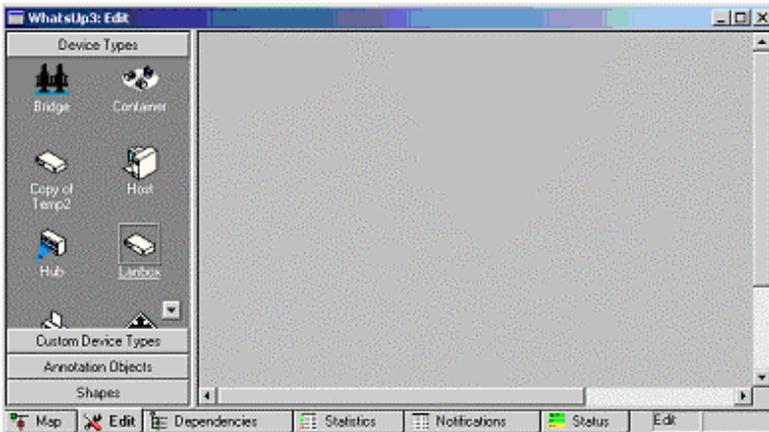


Figure 1 Network Map Editor

2. Creating and adding an SNMP device to the network map

2.1 Right-click the blank area (the right pane).

2.2 Select New Device, and select "Lanbox". A "Lanbox" icon will appear on the map.

3. Configuring the newly created SNMP device

3.1 Double click the icon to open the item properties dialog box.

3.2 On the left pane, select General (see Figure 2).

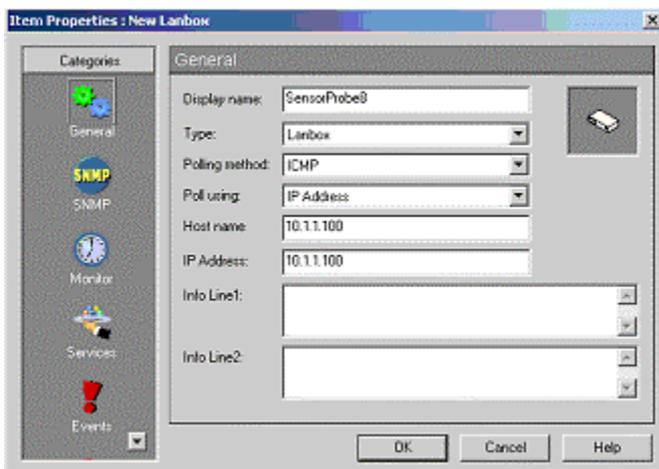


Figure 2 General Property page

3.3 Fill out the form.

All fields are described below:

- Display name: this identifies the SNMP device (i.e. ServSensor).
- Type: this is the device type (i.e. Lanbox).
- Polling Method: this should be ICMP since ServSensor supports only this polling method.

- Poll using: this could be either Hostname or IP Address. If the IP address of the SNMP device was assigned by DHCP server, Hostname would be the suitable choice.
- Host name: this could be the host name that can be resolved to an IP address of the device, or it could be just the IP address of the ServSensor .
- IP Address: this must be the IP address of the ServSensor .
- Info Line1 and Info Line2: information entered in these two fields will be included in notification messages such as SMS and email.

3.4 On the left pane, select SNMP.

3.5 Enable SNMP Manageable Device as show in Figure 3.

3.6 Fill out all fields including Read Community, Write Community, and Device Object ID.

These fields are described below:

- Read Community: this is the password used for SNMP read permission for the ServSensor . The default password is public.
- Write Community: this is the password used for SNMP write permission for the ServSensor . The default password is public.
- Device Object ID: this is the SNMP object identifier for the device. This identifier is used to access a device and read other SNMP data. The device object ID of ServSensor is 1.3.6.1.4.1.3854.1.2.2.1.1.

3.7 Press the OK button to close the window

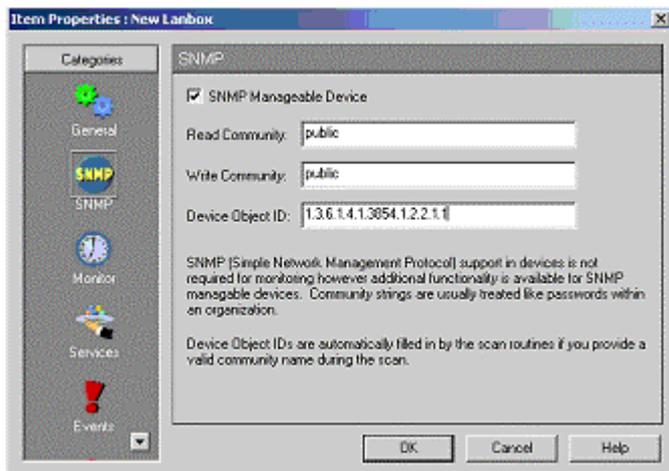


Figure 3 SNMP Property page

3.2.3 GRAPHING THE VALUES OF SNMP VARIABLES

WhatsUp Gold provides a graphing utility named SNMP Graph. Users could select one or more SNMP variables to show a real-time graph of their values, Moreover the utility can graph the change between the last and the current value of a SNMP variable as well as the average change per second in the values of a SNMP variable.

1. Launching SNMP Graph utility

1.1 From SNMP browser, right-click a desired SNMP variable to be monitored on the right pane of the browser as show in Figure 5.

1.2 Select Monitor to open SNMP Graph (see Figure 6).

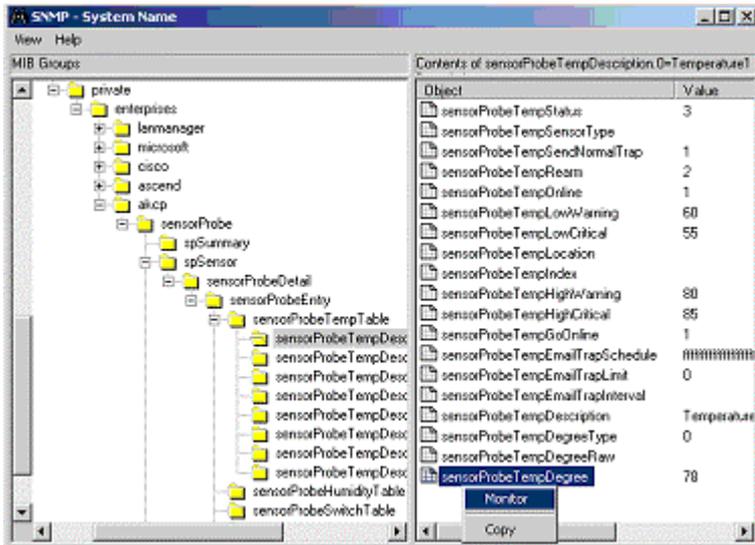


Figure 5 SNMPbrowser

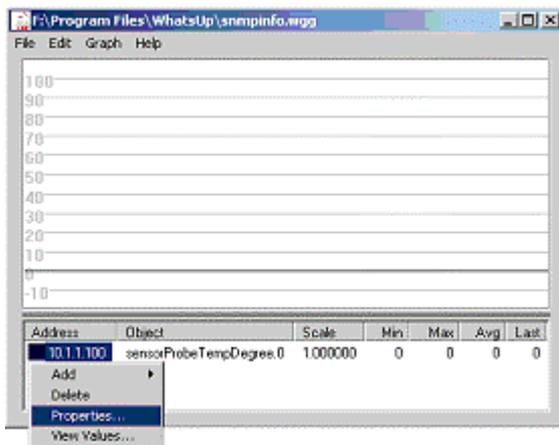


Figure 6 SNMP Graph Utility

2. Setting the item graphing options

By default, the utility graphs the change between the last and the current value of a SNMP variable.

The steps below show how to set the utility to graph the reported values of the SNMP variable.

2.1 Right-click on the IP address column of the desired SNMP variable as show in Figure 6.

Note: There are four menu items including Add (add another SNMP variable), Delete (delete the selected variable), Properties (set graphing options) and View Values (view the raw data used to generate the graph for the selected SNMP variable).

2.2 Select Properties to open Graph Item Properties dialog box (see Figure 7). The description of some interesting properties is described below:

- Host: this is the IP address of the SNMP device.

- Community Name: this is the password used for SNMP read permission.
- Item and Instance: both are used to form the OID of the SNMP variable.
- Absolute values: when it is selected, the utility graphs the reported value of the SNMP variable.
- Auto Scale: when it is selected, the graph scale for the SNMP variable is determined by the utility.
- Allow negative values: when it is selected, the utility allows negative values to be graphed.

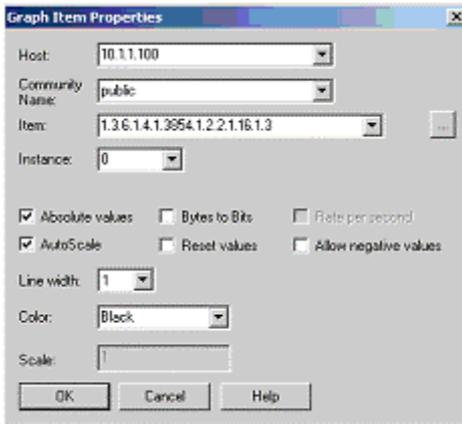


Figure 7 graph Item properties

2.3 Select Absolute values as show in Figure 7.

2.4 Press OK button to apply the setting and close the dialog box.

3. Setting the graph options

3.1 From the Graph menu items of SNMP Graph utility (Figure 6), select Properties to open Graph Option dialog box shown in Figure 8.



Figure 8 Graph options dialog box

3.2 Set up the properties

- Set Interval (seconds) to 3. This is the time interval at which the utility gets the value of the SNMP variable from the SNMP device.
- In Vertical group box, set the Maximum to 180. This determines the highest value on the x-axis scale.
- In Horizontal group box, set Maximum to 100 and Minimum to 50. The Maximum and Minimum determine the highest and lowest value on the y-axis scale respectively.

3.3 Press OK to apply the new setting and close the dialog box.

3.2.4 RECEIVING SNMP TRAPS FROM THE SERVSSENSOR

First, users have to configure the ServSensor to send SNMP traps to the machine running WhatsUp Gold. This can be configured through the web interface of the ServSensor .

1. Setting up the ServSensor to send traps

1.1 Select the Traps Tab to go to the Traps page

1.2 Select Send Traps ON via selection box, enter the Destination IP of the WhatsUp Gold Host and enter the Community. Then press Set

After that do the following steps to set up WhatsUp Gold.

2. Enabling the SNMP Trap Handler

2.1 From the Configure menu of WhatsUp Gold, select Program Options to open Program Option dialog box.

2.2 On the left pane of the dialog box, click Event Servers icon.

2.3 On the right pane of the dialog box, select SNMP Trap.

2.4 Press Configure button to open Configure SNMP Trap Server Properties dialog box shown in Figure 9.

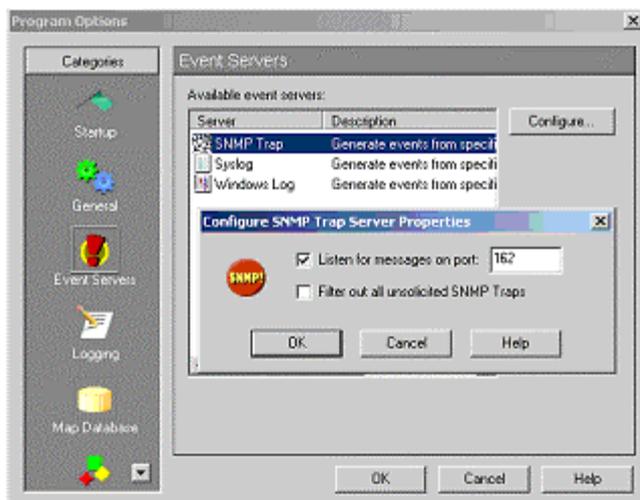


Figure 9 Configure SNMP Trap Server Properties

2.5 Select Listen for messages on port.

2.6 Fill out a listening port number (the default value is the standard SNMP trap Port is 162).

2.7 Press OK button on Configure SNMP Trap Server Properties dialog box

2.8 Press OK button on Program Options dialog box.

3. Assigning SNMP trap events to the ServSensor

3.1 Double click the ServSensor icon on the network map to open the item properties dialog box shown in Figure 2.

3.2 On the left pane, select Events.

3.3 Press Add button located on the right pane. The device event properties dialog box will come up (see Figure 10).

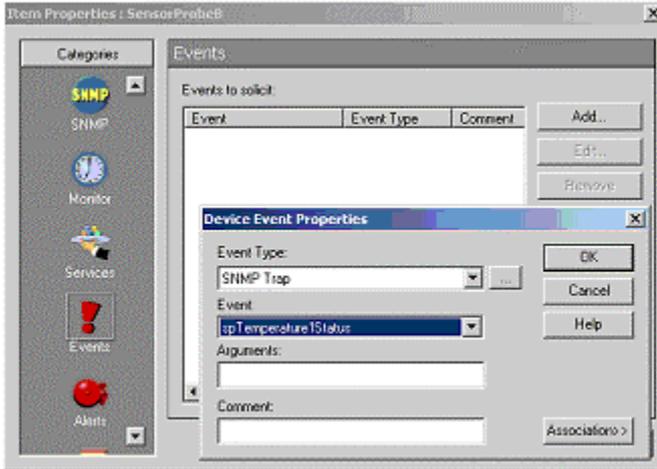


Figure 10 Device Event Properties dialog box

3.4 From Event Type list box, select SNMP trap.

3.5 From Event list box, select spTemperature1Status

3.6 Press OK button to close the dialog box.

3.7 Repeat setup 2.3 to 2.6 to add all spTemperature2Status to spTemperature8Status as show in Figure 11.

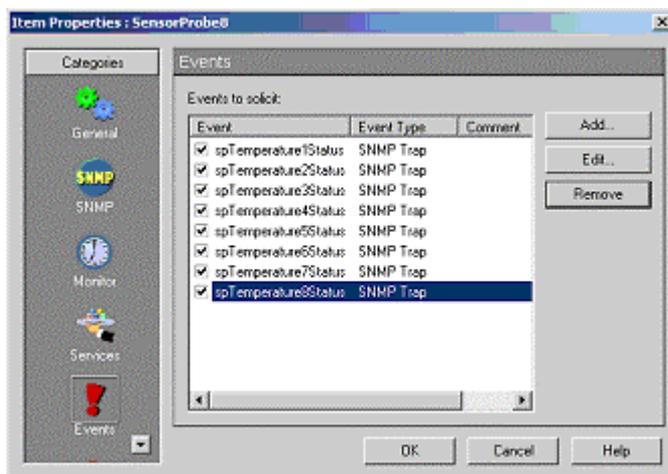


Figure 11 Trap events assigned to the ServSensor

4. Defining Email notifications

There are several notifications supported by WhatsUp Gold including Beeper, Group, Pager, Programs, SMS, SMTP Mail, Sound, and WinPopup. The following steps guide how to configure SMTP Mail.

4.1 From Configure menu of WhatsUp Gold, select Notification Library.

4.2 Select SMTPMail.

4.3 Press New button to open New SMTP Notification dialog box shown in Figure

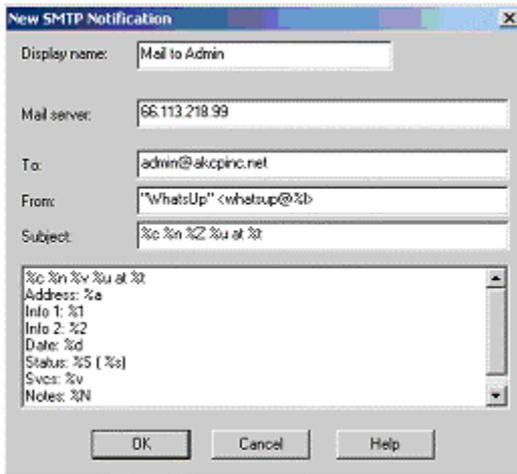


Figure 12 New SMTP Notification dialog box

4.4 Filling out the form

- Display Name: it is a unique name to identify the email notification, for example "Mail to Admin".
- Mail Server: it is the IP address of your SMTP server.
- To: it could be one or more email addresses. Each email address is separated by a comma.
- From: it is an email address that will be the sender of an email notification.
- Subject: it is the subject of an email notification

NOTE

Notification message variables are usually used in the subject and the body field (refer to the WhatsUp Gold documentation for further detail).

4.5 Press OK button to close the dialog box.

5. Setting up notifications for SMTP trap events

5.1 On the left pane of the item properties dialog box, select Alerts.

5.2 Select Enable alerts and Enable logging.

5.3 Press Add button to open Add Alerts dialog box shown in Figure 13.

5.4 In Notification box, select SMTPMail and Mail to Admin.

5.5 In Trigger box, enter 9999.

5.6 Select Send alert even if console response.

5.7 Select On event.

5.8 Press Select Events button to open Active Event dialog box shown in Figure 14.

5.9 Select “Only these specific events listed on this device” and activate desired trap events by clicking the check box corresponding to them. WhatsUp Gold will send a notification when it receives an active trap event. In figure 14, the first three events are active.

NOTE

A notification will also be sent if the ServSensor misses the number of polls specified in the trigger box. To disable this particular notification, set the trigger number to 9999.

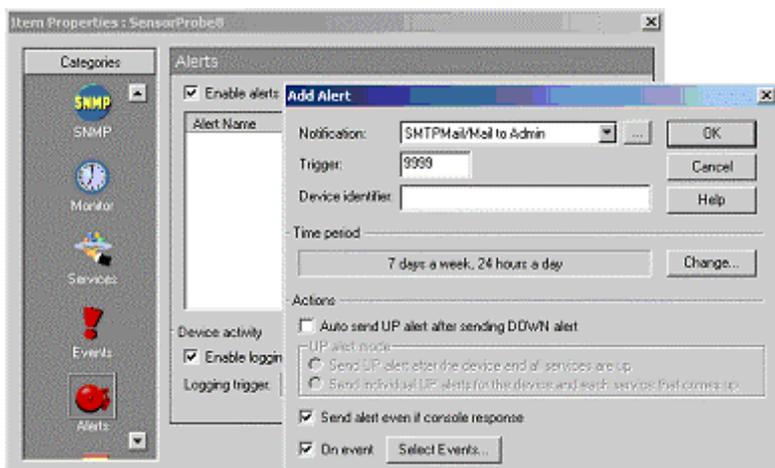


Figure 13 Add Alerts dialog box

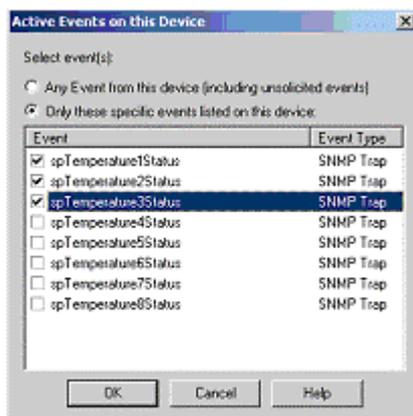


Figure 14 Active Events dialog box

3.3 MRTG - free data graphing

3.3.1 MRTG INSTALLATION

The ServSensor is fully compatible with MRTG. You will need to do to download and install MRTG and then create a configuration script. The configuration script will instruct MRTG how to pull the data from the ServSensor via SNMP. MRTG will then produce an HTML file giving you graphs for daily, weekly, monthly, and yearly statistics.

This HTML file can be recreated at periodic intervals by MRTG providing a live, up to date graph. This HTML file is often published by a web server giving the latest graphs to the all users in the enterprise.

How do I install MRTG?

MRTG can be downloaded from www.mrtg.org. This site has instructions to download MRTG and install it. MRTG will run both on Linux & Windows platforms.

After installation, you need to create a configuration file that will gather information from the ServSensor and plot a graph. Below is a minimal template that can be used to gather data from the ServSensor

Template:

```
/*-----*/
```

```
workdir: /www/MRTG
```

```
NoMib2: Yes
```

```
Target[CONFIG-NAME]:
```

```
1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0&1.3.6.1.4.1.3854.1.2.2.1.17.1.3.1:p  
ublic@192.168.0.205
```

```
MaxBytes[CONFIG-NAME]: 1000
```

```

Options[CONFIG-NAME]: growright, nopercnt, gauge
Title[CONFIG-NAME]: /*Title to display in the html page*/
PageTop[CONFIG-NAME]: /*Page heading */
YLegend[CONFIG-NAME]: Deg C / % Hum
ShortLegend[CONFIG-NAME]: &nbsp;
Legend1[CONFIG-NAME]: Temperature
Legend2[CONFIG-NAME]: Relative Humidity
LegendI[CONFIG-NAME]: Temperature&nbsp;in &deg;C&nbsp;
LegendO[CONFIG-NAME]: Humidity&nbsp;in %&nbsp;

/*****

```

The CONFIG-NAME is the base name for files that will be generated by MRTG, when the above script is run. More details on the configuration file syntax can be found in the link below:

<http://people.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg-reference.html>

You can add more configurations to the above template to customize it for your needs.

The above sample gives the graphs for the Temperature Sensor connected to port1 and humidity sensor on port2 of the ServSensor with IP 192.168.0.205 and community as public.

Below is a list of OID's for temperature & humidity sensors. To find out an OID connected to a particular port, the user has to read the last digits of the OID. In the web-interface, the ports are numbered from 1 to 8 and the corresponding OID last digits are from 0 to 7.

Temperature OID's:

- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0 #this is the temperature 1
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.1 #this is the temperature 2
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.2 #this is the temperature 3
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.3 #this is the temperature 4
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.4 #this is the temperature 5
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.5 #this is the temperature 6
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.6 #this is the temperature 7
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.7 #this is the temperature 8

Humidity OID's:

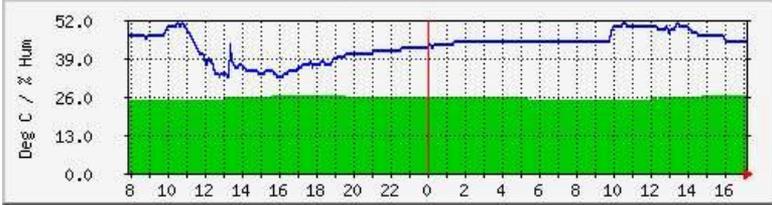
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.0 #this is the humidity 1
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.1 #this is the humidity 2
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.2 #this is the humidity 3
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.3 #this is the humidity 4
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.4 #this is the humidity 5
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.5 #this is the humidity 6
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.6 #this is the humidity 7
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.7 #this is the humidity 8

This link also gives you the sample configuration files similar to the above template, which is used to gather data from the ServSensor .

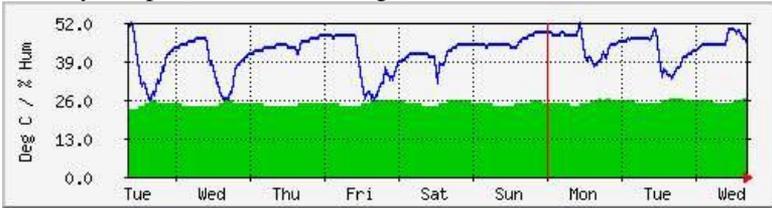
Any sensor producing a graphical data in the ServSensor can be configured in MRTG.

3.3.2 SAMPLE MRTG GRAPHS

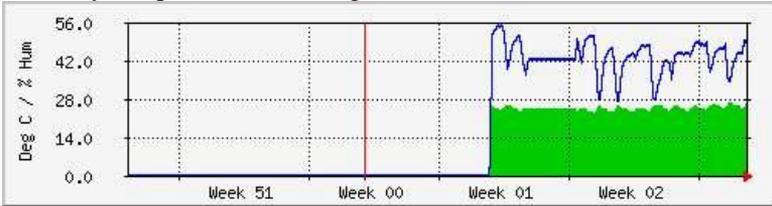
`Daily' Graph (5 Minute Average)



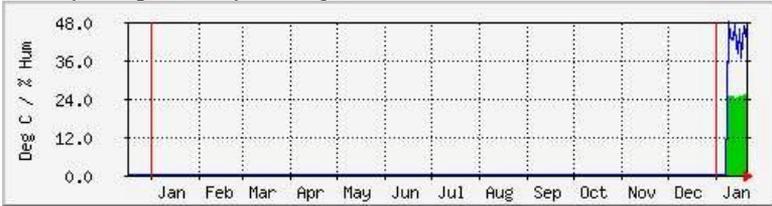
`Weekly' Graph (30 Minute Average)



`Monthly' Graph (2 Hour Average)



`Yearly' Graph (1 Day Average)



Max Temperature in °C	27.0	Average Temperature in °C	25.0	Current Temperature in °C	27.0
Max Humidity in %	59.0	Average Humidity in %	44.0	Current Humidity in %	31.0

GREEN ### Temperature

BLUE ### Relative Humidity

3.4 Frequently used OID's

Here you can find the frequently used OID's for the temperature, humidity & switch type sensors. To find out an OID connected to a particular port, the user has to read the last digits of the OID. In the web-interface, the ports are numbered from 1 to 8 and the corresponding OID last digits are from 0 to 7.

Temperature OID's:

- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0 #this is the temperature 1
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.1 #this is the temperature 2
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.2 #this is the temperature 3
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.3 #this is the temperature 4
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.4 #this is the temperature 5
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.5 #this is the temperature 6
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.6 #this is the temperature 7
- .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.7 #this is the temperature 8

Humidity OID's:

- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.0 #this is the humidity 1
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.1 #this is the humidity 2
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.2 #this is the humidity 3
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.3 #this is the humidity 4
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.4 #this is the humidity 5
- .1.3.6.1.4.1.3854.1.2.2.1.17.1.3.5 #this is the humidity 6

.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.6 #this is the humidity 7

.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.7 #this is the humidity 8

Switch Type sensors:

The type of switch can be found using the following OID's:

.1.3.6.1.4.1.3854.1.2.2.1.18.1.9.0

.1.3.6.1.4.1.3854.1.2.2.1.18.1.9.1

.1.3.6.1.4.1.3854.1.2.2.1.18.1.9.2

.1.3.6.1.4.1.3854.1.2.2.1.18.1.9.3

.1.3.6.1.4.1.3854.1.2.2.1.18.1.9.4

.1.3.6.1.4.1.3854.1.2.2.1.18.1.9.5

.1.3.6.1.4.1.3854.1.2.2.1.18.1.9.6

.1.3.6.1.4.1.3854.1.2.2.1.18.1.9.7

The values of this OID and corresponding sensors are:

Value	Sensor Type
4	Water
6	Security
8	Airflow
10	Dry Contact
12	Relay
13	Voltage

14	Motion Detector
----	-----------------

The switch status can be found out using the following OID's:

.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.0 #this is the switch 1
.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.1 #this is the switch 2
.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.2 #this is the switch 3
.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.3 #this is the switch 4
.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.4 #this is the switch 5
.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.5 #this is the switch 6
.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.6 #this is the switch 7
.1.3.6.1.4.1.3854.1.2.2.1.18.1.3.7 #this is the switch 8

To set a switch output to high:

The OID's are:

.1.3.6.1.4.1.3854.1.2.2.1.18.1.8.0
.1.3.6.1.4.1.3854.1.2.2.1.18.1.8.1
.1.3.6.1.4.1.3854.1.2.2.1.18.1.8.2
.1.3.6.1.4.1.3854.1.2.2.1.18.1.8.3
.1.3.6.1.4.1.3854.1.2.2.1.18.1.8.4
.1.3.6.1.4.1.3854.1.2.2.1.18.1.8.5
.1.3.6.1.4.1.3854.1.2.2.1.18.1.8.6
.1.3.6.1.4.1.3854.1.2.2.1.18.1.8.7

This is helpful for remote actuation of a device, when a certain parameter is set.

Example: if a temperature sensor is connected on port 1 and a dry contact cable is connected on port 2, and the temperature exceeds threshold, then the management software can send an SNMP Set to the dry contact on port 2 with the following command:

```
SNMPset 192.168.0.100 public .1.3.6.1.4.1.3854.1.2.2.1.18.1.8.1 i 1
```

The *i* denotes an integer value

i can take 2 values: 1 = output high, 2 = output low

This will make the dry contact pins output a +5V which can turn on a relay.

For other examples, please see the file **spinit.bat** located at \utilities\mib in the help CD.

For full definitions of all OIDs and their possible values please see the file sp.mib

3.5 ServSensor MIB

SP.MIB

This MIB file is given along with this software to load all the MIB files compatible with HP OpenView, CA Unicenter TNG, UC Davis SNMP package, Veritas etc.

This file is located in the folder `\utilities\mib\` in the help CD provided along with the product.

4. SNMP

The ServSensor is fully compliant with SNMP V1 and has been tested on a number of different platforms including **Hewlett Packard** and their **OpenView** platform, **Computer Associates** and their **TNG** platform, **Cabletron** and their **Spectrum** platform, **IBM Tivoli**, **Veritas**, **WhatsUp Gold**, **Microsoft SNMP**, as well as various **UNIX** systems including **Linux**, **BSD**, and **Sun**.

The MIB for the ServSensor is available and is called sp.mib This MIB can be loaded into a MIB browser and used to access the agent.

4.1 MIB on the ServSensor

For a formal definition of a specific OID consult the file `sp.mib`

You can use standard SNMP tools to access the MIB on the ServSensor . For example the utility `SNMPutil` can be used from the command line of a NT to get information from the ServSensor .

There are also utilities from UCD that we can send upon request. With these standard SNMP utilities you can set and get SNMP parameters from a script file.

For example the following line gets the first temperature sensor:

```
SNMPget 10.1.1.7 public .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0
```

The following line gets the second temperature sensor:

```
SNMPget 10.1.1.7 public .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.1
```

The programs `SNMPget.exe` and `SNMPset.exe` are located in the folder `\utilities\mib\` in the help CD provided along with the product.

4.2 MIB II on the ServSensor

MIB-II is a standard MIB that is supported by many manufacturers. This is useful because the same OID can be used on different boxes to get standard information. For example this information includes how long the box has been running, the name of the manufacturer, the system contact, and other information.

The settable parameters such as the system contact, the system name, and the system location can be set using standard SNMP tools. Once these parameters are set, they are saved to EEPROM and are restored whenever the ServSensor reboots. These settable parameters are limited to 35 characters.

Listed below are the MIB-II variables that are supported by the ServSensor .

sysDescr

DESCRIPTION: "A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating system, and networking software. It is mandatory that this only contains printable ASCII characters." ::= { System 1 } .1.3.6.1.2.1.1.1.0

sysObjectID

DESCRIPTION: "The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router'." ::= { System 2 } .1.3.6.1.2.1.1.2.0

sysUpTime

DESCRIPTION: "The time (in hundredths of a second) since the network management portion of the system was last reinitialized." ::= { System 3 } .1.3.6.1.2.1.1.3.0

sysContact

DESCRIPTION: "The textual identification of the contact person for this managed node, together with information on how to contact this person." ::= { System 4 } .1.3.6.1.2.1.1.4.0

sysName

DESCRIPTION: "An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name." ::= { System 5 } .1.3.6.1.2.1.1.5.0

sysLocation

DESCRIPTION: "The physical location of this node (e.g., 'telephone closet, 3rd floor')." ::= { system 6 } .1.3.6.1.2.1.1.6.0

sysIfNumber

DESCRIPTION: "The Number of Interfaces this device supports" ::= { interfaces 1 } .1.3.6.1.2.1.2.1.0

sysIfIndex

DESCRIPTION: "Unique Index for this entry" ::= { interfaces 2.1.1 } .1.3.6.1.2.1.2.2.1.1.0 1,3,6,1,2,1,2,2,1,1,0

4.3 SNMP Traps

The implementation of Traps on the ServSensor is complete and fully featured. Features include a 35-byte description field for every sensor within the ServSensor. This includes a different description field for every possible sensor plugged into every possible port.

Every sensor has programmable limits and thresholds. A different trap message is sent for each sensor type such as temperature, humidity, switch, etc. The trap messages include 6 var bind fields that include the current sensor status (**normal**, **highWarning**, **highCritical**, **lowWarning**, **lowCritical**, **sensorError**), the current sensor value, the level exceeded, the sensor index, the sensor name, the sensor description.

All of the trap information can be included in messages that you format. The description of the sensor and its current value are useful in creating meaningful messages.

The trap system supports the two trap destinations.

4.4 Trap thresholds

The ServSensor checks the thresholds of each of its alarms once per Trap Poll Interval (twice per second). The ServSensor only checks the status of those sensors that are online.

4.5 Trap Var Bind Information

When the ServSensor sends traps it uses a different trap for every sensor. For example when a temperature sensor trap is sent, an enterprise trap of 6 and a specific type of 100 plus the port number of that sensor is used. When the humidity trap is sent an enterprise trap of 6 and a specific type of 200 plus the port number is used. When the switch trap is sent an enterprise trap of 6 and a specific type of 300 plus the port number is used. All of the switch sensors such as the water detector, voltage monitor, and security sensor share the switch trap.

In addition to the trap type information, Variable Bind Information is also included. Six Var bind fields are attached to the trap. These fields are described in order:

1. The status of the sensor. This can be:

noStatus(1),

normal(2),

highWarning(3),

highCritical(4),

lowWarning(5),

lowCritical(6),

sensorError(7)

2. The sensor value. For a temperature sensor this would be the degree. For a humidity sensor this would be the relative humidity. For a switch it would be a 1 or a 0.

3. Sensor Level Exceeded. The threshold value that was exceeded.

4. Sensor Index. The RJ-45 jack that the sensor is plugged into. This will be 0 or 1 for RJ-45 1 or 2.

5. **Sensor Name.** For example temperature0, humidity1, water1.
6. **Sensor Description.** The description that was previously entered into the ServSensor for that sensor.

4.6 Community String

By Default the community string is "**public**". This is also the password for the **User** and **Administrator**. When the Administrator password is changed, that will become the new community string for SNMP read/write operations. If the User password is changed, that password becomes the new community string for SNMP read operations. That is the password for Administrator or User can be used as the community string for SNMP read/write operations, and only the Administrator password can be used for the SNMP write operations.

5. Web based User Interface

The best way to get to know the ServSensor is through the Web Based Manager.

NOTE

Javascript needs to be enabled in the Web Browser for the ServSensor Web Interface to work.

The Web Based Manager has a list of functions reachable by pressing the links at the top of the web page. The links are described below:

Summary

Look at the Summary View by pressing that link at the top of the page. This section shows the summary status of all the sensors that are online. This gives a single page overview of the sensors in the ServSensor that you have placed online.

You can leave your browser on the summary page and set the Auto Refresh Browser Interval so that the page continually refreshes itself with the latest values.

Sensors

The Sensors View is used to show and change information for every sensor in the ServSensor. This section allows you to drill down into the sensor. From there you can set the Description, Thresholds, and many other values.

Traps

The ServSensor can send traps to two different trap collectors. You can set up the traps using this page.

Mail

You can send mail and pages when thresholds for alarms are reached.

System

The System page displays information for the ServSensor . From here you can view the MIBII variable such as System Description, System Contact, System Name. You can change the set and get passwords and more.

Help

This is a link to the web based help that is available using the Internet

5.1 Login Page

ServSensor comes with an advanced login feature with two levels of password protection. There is a read only user password and a read/write administrator password to protect the device configuration. The password settings are encrypted and saved into the device to prevent unauthorized access.

Open your browser window, type the IP address of ServSensor and enter, the Login Page is then loaded.

The login page will be skipped if you have chosen to not use passwords. To use passwords or to enter a new password, go to the "System" menu, and password settings. This will force later logins to go through the Login Page.

Login as User

The User login allows you to access the system, but does not allow changing any settings. You can navigate all the pages.

The default "**User**" password is "**public**"

Login as Administrator

Administrator login gives you all privileges to change the system configurations.

The default "**Administrator**" password is "**public**"

To change the password, login as "**Administrator**" with default password, go to "**System**" menu on the web page and type your new "**User**" password and "**Administrator**", click on the "Set" button.

You can see the current login status from the top right corner of the web page and you can log off the system by clicking "**Log off**" link.

5.2 Summary Page

The summary page gives you a convenient single page overview of all the sensors that are online. Info on each sensor includes the Port, Type, Description, Reading, Status, and Graph link, and Auto Refresh.

These features are explained in detail below.

Auto Refresh Web (sec.): The Summary page can be automatically refreshed by entering the desired period in seconds in the Auto Refresh Web (sec.) field. Enter the number of seconds and then click the "Start" button next to the field.

If the page is rapidly updating it may be difficult to enter a new value. In that case you should stop the browser from refreshing by pressing Stop in the web browser. You can now enter a new refresh value. To disable refresh enter 0 for the refresh period and press the Summary link at the top of the page.

Port: This is the Autosense RJ45 sensor port that the sensor may be plugged into. It is numbered from 1 to 2 in ServSensor and 1 to 8 in ServSensor 8.

Type: This field shows the type of sensor, for example temperature, humidity, security. The ServSensor can autodetect any intelligent sensors from BLACK BOX and this field will be updated accordingly.

Description: The description of the field is the value entered in the "Sensor settings" page.

NOTE

For a shortcut to configure the sensor, click on the link to go to the settings page of each sensor

Reading: Reading gives the current sensor reading.

Status: The Status field shows the status of each sensor plugged into the ServSensor . The value may be "Normal" " Warning" or "Critical or Not Plugged in".

View Graph: Every temperature sensor, humidity sensor, DC Voltage and Airflow sensor can be graphed simultaneously. To view their graph press the link "View Graph" next to the sensor.

Sys Log: System log gives the status of each and every event that occurred at a particular date and time. System log will help you to view the events generated by the device. You can navigate using the First, Previous, Next and Last button to review the events. The Sys Log can also be linked to a remote Sys Log receiver.

5.3 Sensors setting

This page use for setting the any sensor properties. For a general description about configuring all sensors including information regarding common configuration parameters please see the Installing and Configuring Sensors page.

5.4 Graphing

The graphing capabilities of the ServSensor are designed for functionality: they are simple and easy to use. However if greater flexibility is desired you should consider the use of third party graphing tools. BLACK BOX has written a data capture utility that it includes for no charge on the CD ROM included with the system. This utility records the value of a sensor on a host system. It is then possible to use a large number of third party tools to graph this data.

How much data can be graphed?

The ServSensor has enough memory to save 8640 data points for each sensor. If data is recorded every 15 minutes, there is enough data to display measurements for 90 days. If the recording is made every minute, there is enough memory to hold data for 6 days.

Note: Whenever power is recycled the data logging is reinitialized and all previous data is lost.

Whenever a sensor is taken off-line and then placed back online the data logging is reinitialized and all previous data is lost.

High and low values

The High value and the low values for every period are displayed. If the sensor is removed and a **sensorError** is observed, then no value will be recorded at that time.

Time Accuracy

The time is determined by a battery-backed clock in the ServSensor .

Data averaging

The data recorded is the average for the high and low value during that period. The data is clipped at 0 and 100. Any value over 100 will display as 100. Any value less than 0 will display as 0.

Click on a time to zoom in

There is too much data to display all of it on a single page. Therefore the data is averaged before being shown. When you click on a time to zoom in on, all data for that period of time is displayed.

5.5 Traps Setting

The ServSensor can send trap message to two different hosts. Whenever the status changes for a sensor that is online a trap message can be sent.

A different trap message is sent for each sensor type such as temperature, humidity, and switch. The trap messages include 6 variable fields that include the current sensor status (normal, highWarning, highCritical, lowWarning, lowCritical, sensorError), the current sensor value, the level exceeded, the sensor index, the sensor name, the sensor description.

If trap is not needed it should be turned off. This will reduce network traffic and allow the ServSensor to operate faster. If you do not need it we suggest that you disable the traps resend feature.

To configure Traps click the link at the top of the web page labeled "**Traps**".

Send Trap: Turn Traps on or off with this choice. Use the list box to pick either On or Off. Press the Set button to implement your choice.

Destination IP: This is the IP address of the destination host that will collect this trap.

Community: This is the Community of the host that will receive this trap. This is often set to "public".

Resend Warning and Error Traps: You can choose to have traps resent on a periodic interval. This may be a good idea because trap messages are not guaranteed to be delivered. Traps are based on the UDP communications protocol. Each packet is transmitted, but there is no check to see if they were lost or garbled.

Resend Interval (seconds): You can set the period between which a warning or error trap messages will be re-transmitted. The minimum period is 10 seconds. This time period is also used when resending email messages.

5.6 Mail Page

The ServSensor can send mail to any SMTP host. Whenever the status changes for a sensor that is online an email message can be sent.

If mail is not needed it should be turned off. This will reduce network traffic and allow the ServSensor to operate faster. If you do not need it we suggest that you disable the email resend feature.

To configure Email click the link at the top of the web page labeled "**Mail**".

Send Mail: Turn Mail on or off with this choice. Use the list box to pick either On or Off. Press the Set button to implement your choice.

SMTP Server IP Address: This is the IP address of the SMTP server in dotted decimal notation, not the DNS name.

Timeout (in seconds from 10 to 30): You can increase the timeout for SMTP hosts that have poor connectivity. It is best to leave this number as low as possible while still allowing for communication to the SMTP host to continue.

Resend Interval (seconds): You can set the period between which a warning or error mail message will be re-transmitted. The minimum period is 10 seconds. This time period is also used when resending trap messages.

Maximum Times to Resend: You can resend the email message a number of times by choosing this option. Only warning and error messages are resent.

Attach Picture: This is used to turn ON/OFF the option to attach a picture with the email.

Mail From: This is the email address of the sender of the email. Due to anti spam features of many SMTP servers, the Mail From 'address' must be listed as authorized by the SMTP host otherwise you will receive a failure message that the host will not Relay this message.

Mail Recipient: The email address of the person that will receive the email. This is in the form name@domain.com

Mail Cc1 - Cc5: You can add up to 5 additional recipients for email

Test Mail: You can choose to send a test mail message when first setting up the system, or any time thereafter. Before a test message can be generated all of the necessary information such as the SMTP server, recipient, from address must be entered.

Status of the Most Recent Mail: The possible values are "noStatus", "success", and „fail".

Last Error Message: This is a debugging aid. If the mail is not successful you may find an indication of the reason for the problem here.

5.7 Network Settings

IP Address: You can change the IP address of your ServSensor using this option. Enter the new IP address and click "Set".

Subnet Mask: Set the subnet mask of the device using this option.

Default Gateway: Set the default gateway of the device using this option.

Use DHCP: The ServSensor can use DHCP to assign its IP address, or can use a statically assigned IP address. To use DHCP choose Use DHCP from the list box and press set. To stop using DHCP choose Do Not Use DHCP from the list box and press set. Statically assigning an IP address also turns off DHCP. You can force the ServSensor to voluntarily give up its IP lease and request a new IP lease by choosing Use DHCP from the list box and press set.

Ethernet MAC ID: This is the MAC ID of your ServSensor . This is a read only field.

Ethernet Duplex Mode: This is the Duplex Mode and speed of your ServSensor . This is a read only field.

5.8 System Page

System Description: This is a Mib II value set when the microcode for the ServSensor was installed. It includes the build time and version of the microcode. This is a read only field.

Example: ServSensor 8 VSP8224 Jan 20, 2004

System Name, System Location, and System Contact: These are MIB II values that can be accessed via standard SNMP utilities and often used in management platforms to gain information about the ServSensor .

Use Password: This option enables you to turn on/off the password security, disabling this option could allow any user to login to the system and tamper with the settings.

Send Debug Messages: Debug messages can be an aid in determining the operation of the ServSensor . Debug messages are sent to the host that the browser is running on, or the host where the SNMP set originated from. To view the debug messages use the samon utility with the -no command line input.

NOTE

Debug messages should normally be turned off to reduce network traffic.

Data Collect Period (1 to 60 mins): This controls how often data is collected for use in the graphing.

Display Logo: Turn off displaying the logo by using this option. This option should normally be turned off to allow the web pages to be loaded faster.

Date and Time Settings: Using this option you can change the system time and date as you wish. The time is saved to the battery-backed clock and is reloaded by the system at reboot time.

Password Settings: Use this option to set the new password for "Administrator" and "User"

Clear Syslog: Here you can clear the syslog messages for this ServSensor .

Remote Syslog: You can set up the ServSensor to send its syslog message in a standard format acceptable to a remote syslog server (for example the Logalot system from Somix).

Remote Syslog IP Address, Remote Syslog Port: You can set the IP address and port of the remote syslog server to which the ServSensor will send the log messages.

5.9 Help Menu

The ServSensor has online help available. Press the link at the top of the page and you will load the help file using the Internet.

This is the same help manual as the manual that you are currently reviewing.

6. Utilities

6.1 Utilities

6.1.1 IP SET

The IPSet.exe program is used to assign the initial IP address of the system. It is designed to run on a Microsoft host. Once the program has started enter the MAC address in the section labeled "Client's Mac Address". The Mac address can be found on the ServSensor. Next enter the IP address that you wish to assign to the ServSensor . Then press set.

IPSet.exe first checks the IP address to see if it already assigned. Next it will assign the IP address and then it will check that the address was successfully assigned. If all is well then IPSet.exe will report that the assignment is Complete.

You can verify the IP assignment by using ping or by using a browser to access the ServSensor. To use a browser enter the address *http://10.1.1.7* depending on the IP address that you have assigned.

This utility is located in the help CD provided along with the device.

6.1.2 DATA COLLECTION

This utility can be used to collect SNMP data from the ServSensor or other SNMP hosts. The program is configured through the use of command line options and a text file `OID.txt`. The output of the data collection is stored in a text file. The data output text file name includes the IP address of the host being collected. For example `data10.1.1.7.txt` is the file name for the data collection output when monitoring the ServSensor with IP address 10.1.1.7. In this way you can collect data from many different hosts in the same directory simultaneously. Once the data has been collected it can be read into a spreadsheet such as excel.

This utility is located in the folder `\BLACK BOX_utilities\datacollect` in the help CD.

Usage

```
DataCollect -IP -Pass [-Oid] [-Out] [-v] [-Poll]
```

where:

-IP x.x.x.x: The IP address of the host to collect data from

-Pass Community: The Read Community String

-Out FileName: Optional output filename

-v: Print the version of this software

-Poll: How often to collect data

How to collect data

Create a file called `OID.txt` in the same directory as the program `dataCollect`. The file `OID.txt` contains a list of the OIDs that you wish to collect data for. If you wish to run multiple data collections from the same directory you can give each input file a different name such as `OID10.1.1.7.txt`. In this case you will inform `dataCollect.exe` of the new name by using the option `-Oid nameOfTextFile`. Each line contains one OID. You may have comments following the OID.

A typical line in the OID.txt file could be:
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0 #this is the temperature 1

Start the program dataCollect. A typical command line could be:

```
dataCollect -IP 10.1.1.7 -Pass public -Poll 5
```

The program dataCollect will print to the screen after every pass of the data collection. When you have collected enough data press CTRL-C to stop the program from running.

The data output file called for example data10.1.1.7.txt should be copied to a new directory for analysis. This is suggested because the next time dataCollect is run it will overwrite the output file.

Read the data output file into excel. Excel will load the text input wizard. You should choose “Delimited” and press “Next”. You should then choose comma and press Finish.

Example

```
datacollect -IP 192.168.0.30 -Pass public -Poll 5
```

6.2 UCD Utilities

6.2.1 SNMP GET

This utility is used to collect data from ServSensor . The SNMP GET operation is used by the SNMP manager applications to retrieve one or more values from the managed objects maintained by the SNMP agent. The applications will typically do an SNMP GET request by providing the host name of the agent, one or more OID's along with the specific instance of the OID. The value of OID is printed on the screen. To run this utility we need a supporting DLL file libSNMP.dll which is located in the same directory as the executable file.

Usage:

```
SNMPget [options...] <hostname> {<community>} [<objectID> ...]
```

Options

UCD-SNMP version: 4.1.1

- h this help message.
- H display configuration file directives understood.
- V display version number.
- v 1/2c/3 specifies SNMP version to use. Version 1 or 2c specific.
- c <c> set the community name (v1 or v2c) Version 3 specific.
- Z <T> set the destination engine boots/time for v3 requests.
- e <E> security engine ID (e.g., 800000020109840301).
- E <E> context engine ID (e.g., 800000020109840301).
- n <N> context name (e.g., bridge1).
- u <U> security name (e.g., bert).
- l <L> security level (noAuthNoPriv|authNoPriv|authPriv).

-a <A> authentication protocol (MD5|SHA).

-A <P> authentication protocol pass phrase.

-x <X> privacy protocol (DES).

-X <P> privacy protocol pass phrase

General communication options:

-p <P> use port P instead of the default port.

-T <LAYER> use LAYER for the network layer.(UDP or TCP).

-t <T> set the request timeout to T.

-r <R> set the number of retries to R.

Debugging:

-d dump input/output packets.

-D all | <TOKEN[,TOKEN,...]> turn on debugging output for the specified TOK s.

General options:

-m all | <MIBS> use MIBS list instead of the default MIB list.

-M <MIBDIRS> use MIBDIRS as the location to look for MIBs.

-P <MIBOPTS> toggles various defaults controlling MIB parsing.

MIBOPTS values:

u: allow the usage of underlines in mib symbols.

c: disallow the usage of "--" to terminate.

Comments:

d: save the descriptions of the mib objects.

e: Disable mib errors of MIB symbols conflicts.

w: Enable mib warnings of MIB symbols conflicts.

W: Enable detailed warnings of MIB symbols.

Conflicts:

R: Replace MIB symbols from latest module

-O <OUTOPTS> Toggle various defaults controlling output display

OUTOPTS values:

n: Print OIDs numerically.

e: Print enums numerically.

b: Don't break OID indexes down.

q: Quick print for easier parsing.

f: Print full OIDs on output.

s: Print only last symbolic element of OID.

S: Print MIB module-id plus last element.

-I <INOPTS> Toggle various defaults controlling input parsing:
INOPTS values:

R: Do random access to OID labels.

b: Do best/regex matching to find a MIB node.

Example:

```
SNMPget -M c:\temp 10.1.1.7  
public.1.3.6.1.4.1.3854.1.2.2.1.16.1.10.0
```

Where:

c:\temp is the folder where the MIB files (*ifmib.txt*, *ipmib.txt*...etc.) are located

10.1.1.7 is the IP address of the ServSensor

public is the community name

.1.3.6.1.4.1.3854.1.2.2.1.16.1.10.0 is the OID

Example output:

z enterprises.3854.1.2.2.1.16.1.10.0 = 20

6.2.2 SNMP SET

This utility is used to set the SNMP Objects using the OID's for ServSensor . The SNMP SET operation is used by the management applications and applets to modify the value of the managed object. Most of the managed objects will have a default value maintained by the agent. But sometimes applications will be modifying the data for one or more MIB variables, in which case it will use the SNMP SET operation. The new value set is printed on the screen. To run this utility we need a supporting DLL file libSNMP.dll that is located in the same directory as the executable file.

Usage:

```
SNMPset [options...] <hostname> {<community>} [<objectID>
<type> <value>...] ]
```

Options

UCD-SNMP version: 4.1.1 -h this help message.

-H display configuration file directives understood.

-V display version number.

-v 1/2c/3 specifies SNMP version to use. Version 1 or 2c specific.

-c <c> set the community name (v1 or v2c) Version 3 specific.

-Z <T> set the destination engine boots/time for v3 requests.

-e <E> security engine ID (e.g., 800000020109840301).

-E <E> context engine ID (e.g., 800000020109840301).

-n <N> context name (e.g., bridge1).

-u <U> security name (e.g., bert).

-l <L> security level (noAuthNoPriv|authNoPriv|authPriv).

-a <A> authentication protocol (MD5|SHA).

-A <P> authentication protocol pass phrase.

-x <X> privacy protocol (DES).

-X <P> privacy protocol pass phrase

General communication options:

-p <P> use port P instead of the default port.

-T <LAYER> use LAYER for the network layer.(UDP or TCP).

-t <T> set the request timeout to T.

-r <R> set the number of retries to R.

Debugging:

-d dump input/output packets.

-D all | <TOKEN[,TOKEN,...]> turn on debugging output for the specified TOK s.

General options:

-m all | <MIBS> use MIBS list instead of the default MIB list.

-M <MIBDIRS> use MIBDIRS as the location to look for MIBs.

-P <MIBOPTS> toggle various defaults controlling MIB parsing.

MIBOPTS values:

u: allow the usage of underlines in MIB symbols.

c: disallow the usage of "--" to terminate.

Comments:

d: save the descriptions of the MIB objects.

e: Disable MIB errors of MIB symbols conflicts.

w: Enable MIB warnings of MIB symbols conflicts.

W: Enable detailed warnings of MIB symbols.

Conflicts:

R: Replace MIB symbols from latest module

-O <OUTOPTS> Toggle various defaults controlling output display

OUTOPTS values:

n: Print OIDs numerically.

e: Print enums numerically.

b: Don't break OID indexes down.

q: Quick print for easier parsing.

f: Print full OIDs on output.

s: Print only last symbolic element of OID.

S: Print MIB module-id plus last element.

-I <INOPTS> Toggle various defaults controlling input parsing:

INOPTS values:

R: Do random access to OID labels.

b: Do best/regex matching to find a MIB node.

type - one of i, u, t, a, o, s, x, d, n

i: INTEGER, u: unsigned INTEGER, t: TIMETICKS, a: IPADDRESS

o: OBJID, s: STRING, x: HEX STRING, d: DECIMAL STRING

U: unsigned int64, I: signed int64, F: float, D: double

Example:

```
SNMPset -M c:/temp 10.1.1.7 public
1.3.6.1.4.1.3854.1.2.2.1.16.1.10.0 i 30
```

Where:

c:\temp is the folder where the MIB files (ifmib.txt, ipmib.txt...etc.) are located

10.1.1.7 is the IP address of the ServSensor

public is the community name

.1.3.6.1.4.1.3854.1.2.2.1.16.1.10.0 is the OID

i is the data type to be set 30 is the data to be set

Output

```
enterprises.3854.1.2.2.1.16.1.10.0 = 30
```

6.2.3 SNMP WALK

This utility fetches the SNMP objects using SNMP GET NEXT from an agent specified by the hostname. The value of the next OID is printed on the screen. To run this utility we need a supporting DLL file libSNMP.dll.

Usage:

```
SNMPget [options...] <hostname> {<community>} [<objectID> ...]
```

Options:

UCD-SNMP version: 4.1.1 -h this help message.

-H display configuration file directives understood.

-V display version number.

-v 1|2c|3 specifies SNMP version to use. Version 1 or 2c specific.

-c <c> set the community name (v1 or v2c) Version 3 specific.

-Z <T> set the destination engine boots/time for v3 requests.

-e <E> security engine ID (e.g., 800000020109840301).

-E <E> context engine ID (e.g., 800000020109840301).

-n <N> context name (e.g., bridge1).

-u <U> security name (e.g., bert).

-l <L> security level (noAuthNoPriv|authNoPriv|authPriv).

-a <A> authentication protocol (MD5|SHA).

-A <P> authentication protocol pass phrase.

-x <X> privacy protocol (DES).

-X <P> privacy protocol pass phrase

General communication options

-p <P> use port P instead of the default port.

-T <LAYER> use LAYER for the network layer.(UDP or TCP).

-t <T> set the request timeout to T.

-r <R> set the number of retries to R.

Debugging:

-d dump input/output packets.

-D all | <TOKEN[,TOKEN,...]> turn on debugging output for the specified TOK s.

General options:

-m all | <MIBS> use MIBS list instead of the default mib list.

-M <MIBDIRS> use MIBDIRS as the location to look for MIBs.

-P <MIBOPTS> toggles various defaults controlling MIB parsing.

MIBOPTS values:

u: allow the usage of underlines in MIB symbols.

c: disallow the usage of "--" to terminate.

Comments:

- d: save the descriptions of the MIB objects.
- e: Disable MIB errors of MIB symbols conflicts.
- w: Enable MIB warnings of MIB symbols conflicts.
- W: Enable detailed warnings of MIB symbols.

Conflicts:

- R: Replace MIB symbols from latest module
- O <OUTOPTS> Toggle various defaults controlling output display

OUTOPTS values:

- n: Print OIDs numerically.
- e: Print enums numerically.
- b: Don't break OID indexes down.
- q: Quick print for easier parsing.
- f: Print full OIDs on output.
- s: Print only last symbolic element of OID.
- S: Print MIB module-id plus last element.

- I <INOPTS> Toggle various defaults controlling input parsing:

INOPTS values:

- R: Do random access to OID labels.

b: Do best/regex matching to find a MIB node.

-C <APPOPTS> Toggle various application specific behaviour:

APPOPTS values:

p: Print the number of variables found.

i: Include the requested OID in the search range.

Example:

```
SNMPwalk -M c:\temp 10.1.1.7 public  
1.3.6.1.4.1.3854.1.2.2.1.16.1.10.1
```

Where:

c:\temp is the folder where the MIB files (ifmib.txt, ipmib.txt...etc.) are located

10.1.1.7 is the IP address of the ServSensor

public is the community name

.1.3.6.1.4.1.3854.1.2.2.1.16.1.10.0 is the OID

Output:

```
enterprises.3854.1.2.2.1.16.1.11.0 = 1
```

7. FAQ's

Q: Why am I unable to set the IP to the device using IPSet utility provided in the help CD?

A: Possibly:

a) The device is not hooked up properly with the LAN/network/Patch cable. The best method is to use a crossover cable from a computer directly to the ServSensor .

b) The PC used to configure is on a different subnet than the device. IPSet.exe will not work across routers.

Q: What is the default IP of the device?

A: The default IP assigned at the factory is: 192.168.0.100

Q: If the IPSet fails, is there any other method of assigning the IP?

A: Please do the following

a) find out the IP address of your network adapter by entering the command

ipconfig

b) Add the IP address of the ServSensor to the routing table by entering "route add 192.168.0.100 x.x.x.x" where x.x.x.x is the IP address of the network adapter

c) ping 192.168.0.100. If the ping works then open up your browser and access the web interface of the device by typing the IP 192.168.0.100.

Q: Can I use the default IP of the device to access the web interface and later assign the desired IP?

A: Yes, you can access the web interface by entering the IP 192.168.0.100 in your browser.

Q: I'm able to ping the device IP, but I'm not getting the web interface when I enter the IP in the browser?

A: Possible causes:

a) The proxy settings of the browser may be preventing the access to the device. Please disable the proxy settings to access the web interface.

b) You have updated the firmware, but you have not updated the html code update. Html code updates has to be done, after the firmware update is done.

Q: Where can I find the MAC address of the device?

A: The MAC address of the device can be found on the bottom cover of the device, and also on the web interface under System page.

Q: After some days of use, I have changed the IP of the device. But it changes to the old IP after a few hours. How can I prevent this?

A:

a) What is happening is that after the IP address has been changed by the user, it is being changed back by a network management program. One way that you can change the IP address is to statically set the ARP cache to associate the MAC address with the IP address and then ping it. Therefore someone or some automated network management

program can later come by and ping the old IP address and thereby reset the IP address back to the previous value.

b) The way to prevent this from happening is to go to the send an SNMP command to the device to disallow IP changes to be made. We do not have this command on the user interface because once set the IPSet program can no longer be used to change the IP address until an SNMP command is sent to the box to undo this setting and allow the IP address to once again be changed.

The command to disable the IP change is:

```
SNMPset <IP> <community> .1.3.6.1.4.1.3854.1.2.2.1.62.0 i X
```

Where:

IP is the IP address of the device

community default is "public"

X can take 2 values: 1 (enable IP change), 2 (disable IP change).

NOTE

If the user forgets the IP address while this setting is in effect the device will be unusable.

Q: Where can I find the MIB file for the device?

A: The MIB file for the device can be found in the help CD, under the directory: *\utilities\mib*

Q: I cannot set the device to send mails?

A: Possible causes may be:

a) The SMTP server is entered is wrong.

- b) Send mail option is not enabled in the Mail settings page.
- c) The timeout period entered is too low.
- d) The gateway IP is not entered in the network page
- e) The mail from address is not set
- f) The mail server is not responding
- g) The mail from address is not validated in the mail server
- h) The mail server settings prohibit it from accepting connections from the device IP
- i) The firewall in the network is preventing the SMTP traffic.

Q: I cannot log in to the device.

A: Possible causes may be:

- a) The password entered is wrong.
- b) The password has been changed by another user.

Q: I'm not able to change the settings in the device.

A: You have logged into the device as a user. Only an administrator can make changes to the settings.

Q: How can I recover a lost password?

A: You need to contact BLACK BOX support.

Q: The device is not able to send Traps

A: Possible causes may be:

- a) The destination TRAP IP is not set in the TRAP settings page.
- b) The community entered is wrong.
- c) The firewall is blocking the TRAP traffic.
- d) The send Trap option is Off.

Q: I have HP OpenView, but I'm not able to receive the Traps.

A: Possible causes may be:

- a) For changing the Traps to HP OpenView style, you need to send an SNMP command to the device given below:

```
SNMPset <IP> <community> .1.3.6.1.4.1.3854.1.2.2.1.60.0 i X
```

Where:

IP is the IP address of the ServSensor

community default is "public"

X can take 3 values: 1 (WhatsUP gold style), 2 (HP OpenView Style), 3 (both Style). By default, the *X* value set is 1.

Q: I have assigned the gateway IP, and when I say set, it reverts back to the default IP?

A: This happens when the device is not able to find the IP entered. When the IP is entered, the device searches for the IP, if it's found, it will accept the IP entered, else it will revert back to the default IP.

Q: Is the temperature sensor built inside the ServSensor ?

A: No. We tried to do that when we first designed the ServSensor . It is much cheaper to have an integrated temperature sensor. That is the purpose of the grill on the top of the box. What we found is that there is no way to stop the heat from the ServSensor from affecting the temperature sensor; this ranges between 2 to 4 degrees Celsius. What would have been necessary had we proceeded with that design would have been to "tune" out the offset by applying a fudge factor. The problem is that this fudge factor would have had to change depending on the temperature and the operating conditions. So if we add in fudge factor for normal room temperatures it would have to change when there was a problem with the air conditioning and the ambient temperature was higher. Because of all these reasons, we came up with the external sensors, so that the measurements done by that sensor are accurate and there is no need for calibration.



© Copyright 2004. Black Box Corporation. All rights reserved.

BLACK BOX Network Services