

Integration with Network Management Systems

Network Management System (NMS) Integration

The securityProbe 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 securityProbe comes with a MIB file, which can be easily loaded to your network management system and can receive SNMP alerts.

By default, the traps are set to the style of WhatsUp Gold. The user can change this to HP OpenView NNM or to WhatsUp Gold or both by using the following 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 securityProbe.
- <community> is a community string of securityProbe. The 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.

HP OpenView

Loading the MIB to NNM

From the NNM menu, press `Options > Load / Unload MIBs: SNMP`. The dialog box for Loading/Unloading MIBs appears. Press `Load`. Browse to the MIB file of the securityProbe. The file name is `sp.mib`, and it is included in a companion CD at `\akcp_utilities\mib`. Press `open` to load this MIB. Press `OK` to load the Trap definitions.

NNM Menu Integration

Adding securityProbe to the NNM Menu

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

Because the Web based user interface 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 user interface to the NNM menu, it becomes easy for the user to interact with the SNMP agent, regardless of his location or platform.

The NNM menu is also enhanced to add graphing. The user can graph the temperature or humidity values for every system. For example, whenever the user wants to observe temperature trends across the enterprise, he can do so with a single button.

.An Application Registration File or ARF file is used by HP OpenView to customize and integrate third party applications such as the **securityProbe** into NNM. The name of this file is called **cp8.arf**. The sample ARF file is located in the companion CD that you received when purchasing the securityProbe. It is in a `\akcp_utilities\Openview\` directory. The file in this directory is only an example; hence, you will need to modify it to the way you would like it to work. For example, adding menu for graphing temperature sensor, and adding menu to access the web based user interface. Please consult the HP OpenView Documentation on how to create and use registration files.

In order to integrate this ARF file into NNM, you must copy the file to the correct directory so that NNM can find it when it starts. In the simplest case of a Windows PC running NNM, that directory could be in `C:\HP OpenView\registration\C`. This path would vary depending upon your choices during installation of NNM. On a UNIX platform, the path to copy ARF 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 `nnm`.

After you have copied ARF to the correct directory you must restart NNM. When NNM restarts you should see securityProbe on the NNM menu. Under securityProbe menu you should be able to launch the web user interface, graph temperature sensor, and the status depending on what you customized in the ARF file.

The ARF 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.

Polling SNMP, Thresholds, and Alarm

NNM can read the Status field to determine if any of the sensors have a problem. Polling is the most effective method of monitoring network connectivity failures. While the securityProbe 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 only needs to be read once every five minutes or more. This will depend on your current requirements.

Setting Up Polling

To setup polling go to the NNM toolbar and click **Options > Data Collection & Thresholds: SNMP**

The dialog box appears. Click **Edit > MIB Object > New**

The dialog to pick the OID to monitor appears. Click on the **+** to expand the **private** tree. Then expand **enterprises > AKCP > securityProbe**. This exposes the securityProbe MIB.

You can monitor the status of an individual sensor by choosing the status OID for that sensor. For example, **sensorProbeTempStatus** is for the status of temperature sensor.

A second dialog appears allowing you to further refine the details of what you wish to poll. On the "**Set Collection Mode**", select "**Store, Check Thresholds**". Enter the IP Address of the securityProbe 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 5 seconds. This will cause the node to be polled every 5 seconds. This is too often for a working environment. However, it will help to test the securityProbe 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, the sensors are at or below normal status. When the status is at 1, 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, click **File > Save**. You are now polling the sensor Status

Polling using RO (read only) and RW (read-write) communities. Follow the example below.

```
snmpset <IP> <community> .1.3.6.1.4.1.3854.1.2.2.1.60.0 i { ro | rw }
```

where

- <IP> is the IP address of the securityProbe.
- <community> is a community string of securityProbe. The default is "public", and
- <ro> or <rw> values or either ro or rw.

Traps in NNM

The securityProbe sends traps whenever the status of their sensors 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 (**Options > Event Configuration**). When the Event Configuration dialog box loads, scroll down to the top box and select securityProbe. The bottom listbox will now list the traps available. Select a trap from the bottom list, and then from the Dialog menu click **Edit > 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 (varbinds) if the trap comes from the securityProbe. To include variable binding information, use **\$1**, **\$2**, **\$3**, **\$4**, **\$5**, and **\$6** in your message. These macros are defined here. The variable binding information is described in the **Description** tab. For example, entering "**\$6 is \$2, status is now \$1**" will display "**Temperature1 Description is 77, status is now normal**" if the temperature sensor is 77 degree with its status being normal, and the description is Temperature1 Description.

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.

Graphing with NNM

The easiest way to graph is with utility `xnmgraph`.

You can graph an individual temperature sensor on the securityProbe.

To graph the first temperature sensor on the securityProbe 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 securityProbe 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 click **Options > Data Collection & Thresholds: SNMP**. When the Data Collection & Thresholds: SNMP dialog loads click **Edit > MIB Collection > New**. When the Collection dialog box loads, Set Collection Mode: Store No Thresholds. Enter the Source of the IP address for the securityProbe, and add it to the Source List. Press OK to finish with this Dialog and then press File > Save to start collecting.

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 securityProbe.

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

Press **private** to expose the MIB tree under the private OID. Then press **enterprises > AKCP > securityProbe**.

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 user interface. The web user interface 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 securityProbe 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.

If all else fails send an email to support@akcpinc.com

Testing Alarms in NNM

The following example tests the first temperature sensor. 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 temperature button on the left menu. Then choose the temperature sensor you want to test.

If the temperature sensor is plugged into the first RJ-45 sensor port, the Autosense will activate this sensor. Once activated the sensor should display 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 RJ-45 sensor port.

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 rearm prevents false notifications being sent, as the temperature can flicker between the warning value and the current temperature. The rearm will give a margin for this difference.

For example, if the room temperature is 72 and the Rearm is 2, then a good choice is to set Warning High is to 76. To set the **HighWarning** use the web user interface. Enter 76 into the Warning High field and press Save to save your current settings.

Changing the Temperature

Change the temperature by warming the sensor in you hands. The sensor is the small black plastic package connected at the end of the cable. Hold the temperature sensor until the temperature starts to rise.

To see the change in temperature you must refresh the web page.

Changing the Status

Press the Summary tab on the top of the web user interface. The summary will show the new temperature. When the Degree reaches the High Warning threshold the status of the temperature sensor will change to **Warning**.

Verifying Alarms

When the status changes you will be notified of this change. A trap would be sent if they have been configured to send. If NNM was polling the status, then an alarm would have occurred. If you have set up NNM to receive Traps from the system, a Popup window would display.

If you have set up Polling in NNM you can 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 that has gone to warning (integer value 3).

Resetting the Sensor Status

The temperature sensor will eventually drift back to room temperature. You can see this using the web interface by pressing the Summary tab to refresh the browser. By entering a value in the auto refresh browser interval field will automatically cause the browser to refresh itself.

When the temperature plus the rearm value 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 the status changes a trap will be sent and an alarm will occur from the NNM polling the status.

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 1m.

Monitoring with WhatsUp Gold

Adding MIB to WhatsUp Professional

In some cases, you may want to add MIB files to the WhatsUp Professional system to make it easier to find specific OIDs within the MIB file. If you are reporting and alerting on non-enterprise OIDs, you may be able to use the MIB files already installed with the application.

To add the MIB file to the application, copy the file to the Ipswitch\WhatsUp Professional\Data\Mibs folder in your installation directory. Once the MIB is in that directory, you must restart the WhatsUp Professional application to see the MIB in the MIB Browser.

Where to get MIBs

If you do not have the MIB files you need for your devices that you can try.

<http://www.akcp.com/downloads/sp.zip>

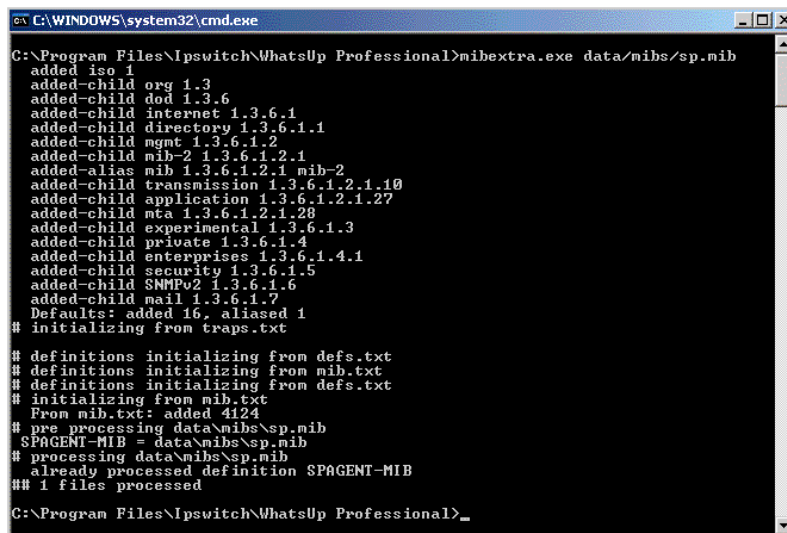
Setting up the MIB identifier

WhatsUp Gold provides a commandline 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



```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Ipswitch\WhatsUp Professional>mibextra.exe data\mibs\sp.mib
added iso 1
added-child org 1.3
added-child dod 1.3.6
added-child internet 1.3.6.1
added-child directory 1.3.6.1.1
added-child mgmt 1.3.6.1.2
added-child mib-2 1.3.6.1.2.1
added-alias mib 1.3.6.1.2.1 mib-2
added-child transmission 1.3.6.1.2.1.10
added-child application 1.3.6.1.2.1.27
added-child mta 1.3.6.1.2.1.28
added-child experimental 1.3.6.1.3
added-child private 1.3.6.1.4
added-child enterprises 1.3.6.1.4.1
added-child security 1.3.6.1.5
added-child SNMPo2 1.3.6.1.6
added-child mail 1.3.6.1.7
Defaults: added 16, aliased 1
# initializing from traps.txt
# definitions initializing from defs.txt
# definitions initializing from mib.txt
# definitions initializing from defs.txt
# initializing from mib.txt
From mib.txt: added 4124
# pre processing data\mibs\sp.mib
SPAGENT-MIB = data\mibs\sp.mib
# processing data\mibs\sp.mib
already processed definition SPAGENT-MIB
## 1 files processed
C:\Program Files\Ipswitch\WhatsUp Professional>_
```

Note: if the mib extractor returns “failed to open file” error, the MIB files 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.

An SNMP Performance Monitor

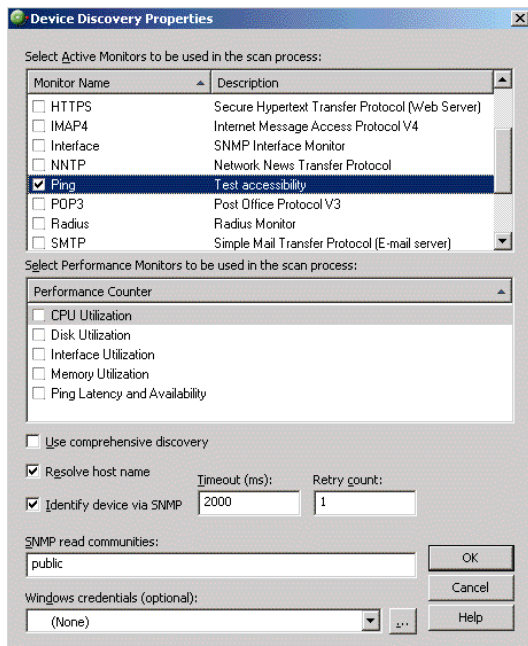
You install a SNMP enabled temperature sensor in the server room, and want to configure WhatsUp Professional to monitor and chart the temperature readings on the sensor. Here are the steps to configure this type of monitor:

1. Right-click on the map you want to add the temperature sensor to.
2. From the right-mouse menu, select New > New Device.
3. On the Add New Device dialog, enter the IP address of the sensor.



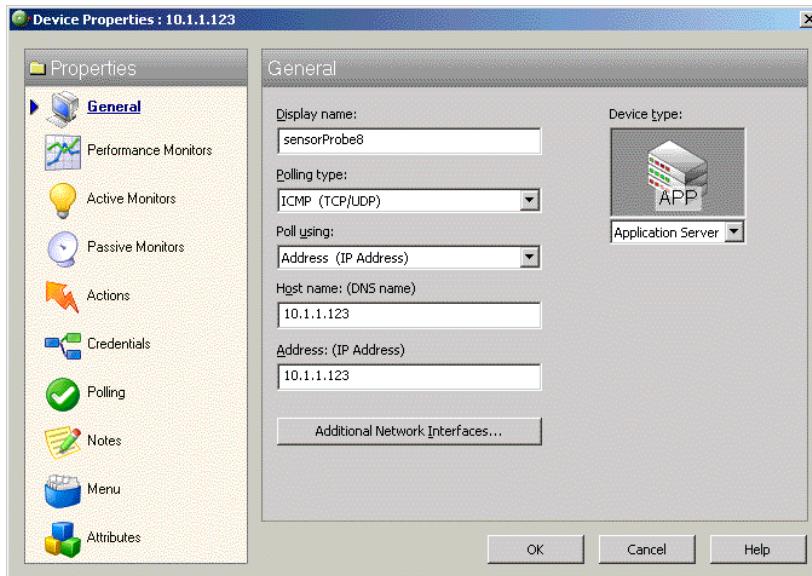
4. Click Advanced.

5. On the Device Discovery Properties dialog, clear the active and performance monitor selections (leaving only the Ping active monitor) and enter the read community sting in the SNMP read box. In this case, the string is 'public.'



6. Click OK.

7. On the Add New Device dialog, click OK. WhatsUp Professional then scans the IP address using the SNMP community string to identify the device.



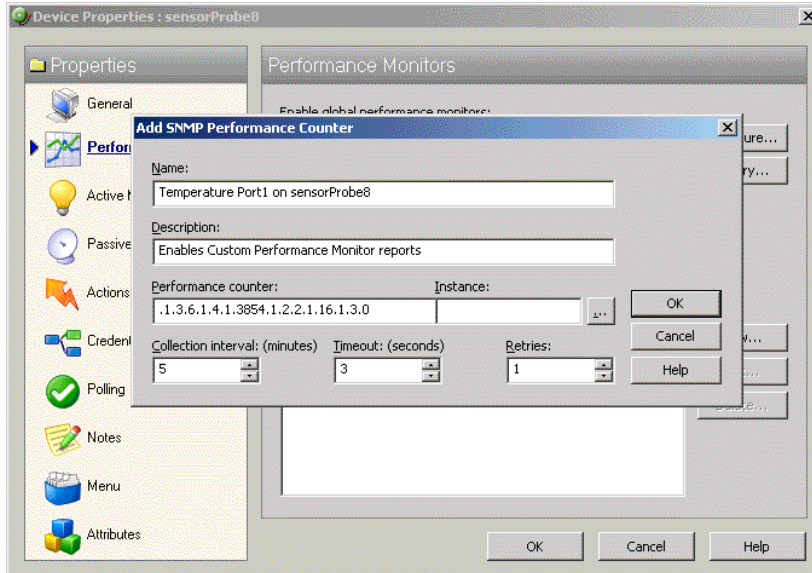
8. When the scan is complete, Device Properties for that device appears. Select the Performance Monitors section.

9. In the Performance Monitors section, click New.

10. Select SNMP Performance Monitor as the type and click OK.

11. On the Add Performance Counter dialog, enter 'Temperature Port1 on sensorProbe8' in the Name box.

12. After reading through the User Manual for the sensor, we know that the performance counter OID for the temperature on the device is .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0 Enter that number in the Performance counter box.



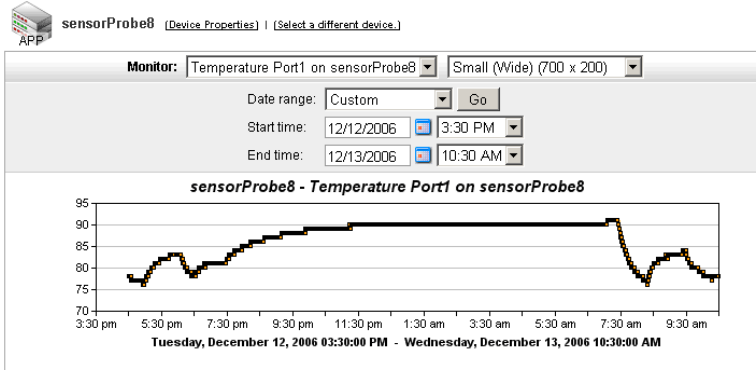
If you only have the full MIB file, and do not have the specific OID for the performance counter, you must import that MIB file and browse to the specific performance counter in the MIB. To access the MIB Browser, click the Browse (...) button. Once you select the proper counter, the Performance counter box is filled in with the OID.

13. In the Collection Interval box, enter 5 to have WhatsUp Professional collect the data on the device every 5 minutes.

14. Click OK to add the monitor and begin collecting data.

It may take several polls to produce enough data to see anything interesting on your graph. Once you have enough data, you can view the performance reports by:

1. Right-click on the device icon and select Device Reports from the right-mouse menu. The Report View opens to the Device Reports list.
2. Select the Custom Performance Monitor report. This report shows the data collected on the device since the monitor was activated.



The report graphs all of the temperature readings gathered at the specified interval. You can change the date and time of the displayed data to show more detail on the graph.

Below the graph, the summary bar shows the maximum, minimum, and average value for the time period selected.

An SNMP Active Monitor

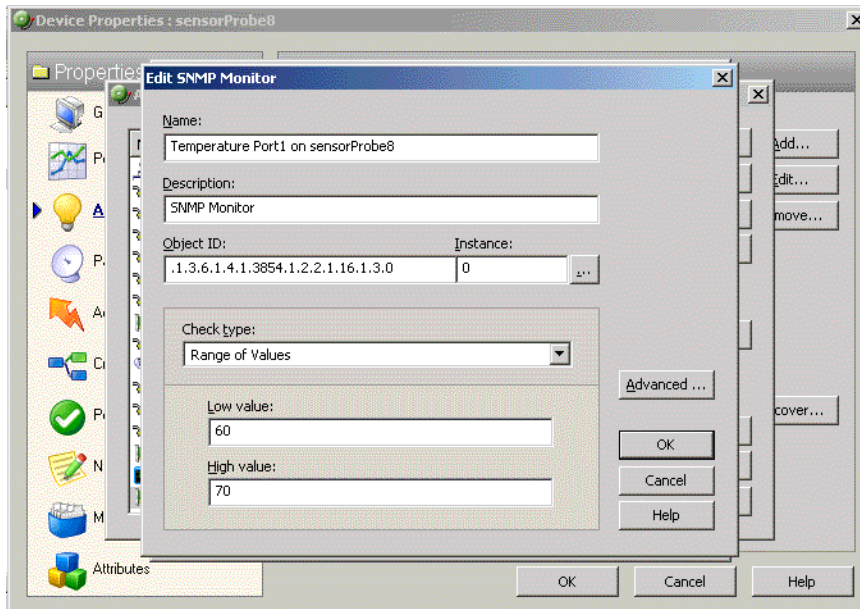
Now that you have several days of performance data for your device, you notice that you had occasional spikes in the data that you can't account for. You can't tell if a door was left open, a device was turned on, or anything else that would explain this type of spike. You decide that you want to be notified when one of these spikes occurs, but only if the spike is, in your opinion, too high.

To do this, you can create an active monitor that watches the returned value and makes sure that the value falls in an acceptable range. To create this monitor:

1. On the Device Properties for the temperature device, select Active Monitors.
2. On the Active Monitors section, click Add. The Select Active Monitor Type dialog appears.
3. Since you do not have an active monitor of this type configured in the Active Monitor Library, click Browse (...) to access the Active Monitor Library.
4. In the Active Monitor Library, click New.
5. Select SNMP Monitor as the type of monitor you want to create.
6. In the New SNMP Monitor dialog, enter 'Temperature Range' in the Name box.
7. Since we already created the performance monitor with this data, we know that the performance counter OID for the temperature on the device is .1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0. Enter that number in the Performance counter box.
8. In the Check type pull-down menu, select 'Range of Values.'

9. We know from the performance monitor that the temperature sensor reports the temperature 60°F. Therefore, enter 60 in the Low value box as the lowest temperature that should be in the server room.

10. Enter 70 as the High value box, since anything over 70°F is considered too high for the room.

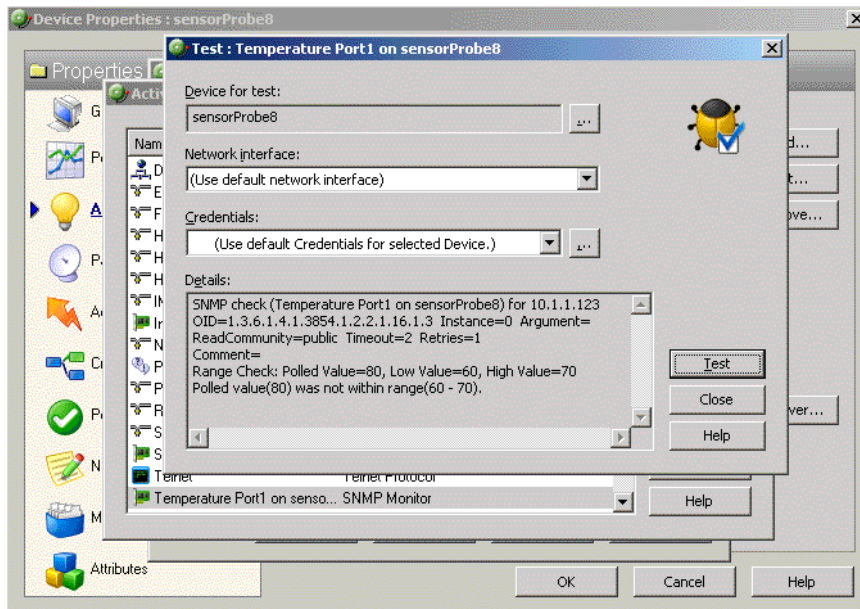


11. Click OK to add the monitor to the Active Monitor Library, and then click OK to record the selection of the new monitor type.

12. On the Select Active Monitor Type dialog, click Next.

13. Select Enable Polling for this Active Monitor and click Next.

14. Select the type of action scenario you want to use for your monitor. An action profile that you have configured through the Action Profile Library, or select Apply individual actions to build a list of actions that you select from the Action Library.



15. Click Finish to begin using this active monitor on the device.

Now that the monitor is configured, you are alerted when the temperature reported by the sensor falls outside of the acceptable temperature range.

An SNMP Passive Monitor

You decide to create an SNMP Passive Monitor that listens for critical error message.

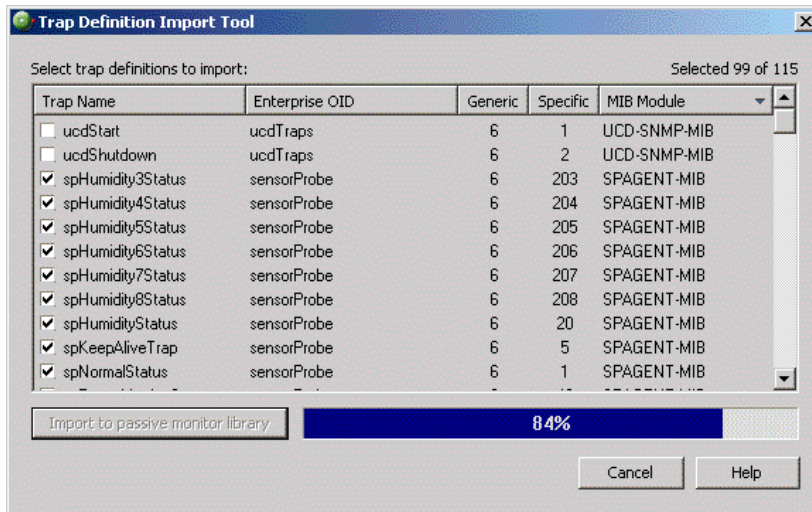
1. Configure your device to send SNMP Traps to your WhatsUp Professional computer.

Send Trap	On
Destination IP	192.168.0.1
Community	public
	Save Reset

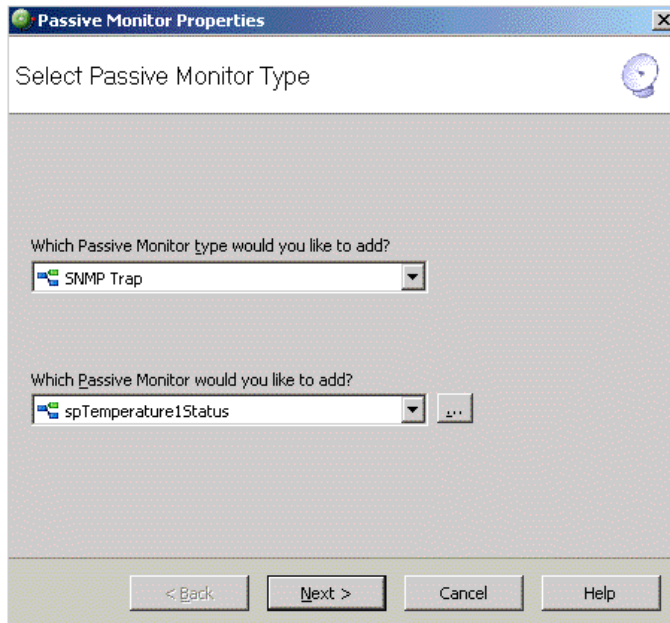
2. Turn on the SNMP Trap Listener by accessing Configure > Program Options > Passive Monitor Listeners in the WhatsUp Professional console. SNMP Trap and click Configure. On the configuration dialog, select Listen for messages on port 162. Click OK to turn the listener on, and click OK to close the dialog.

If you have Windows Trap Listener enabled on the WhatsUp Professional computer, the SNMP Trap Listener will not work. You must turn the Windows Trap Listener off first.

3. Import Trap to passive monitor library by accessing Tools > Import Trap definitions.
Select trap definitions to import.



4. On the Device Properties for the sensorProbe device, select Passive Monitors.
5. On the Passive Monitors section, click Add. The Select Passive Monitor Type dialog appears.



6. If you do not have an active monitor of this type configured in the Passive Monitor Library, click Browse (...). to access the Passive Monitor Library.
7. In the Passive Monitor Library, click New.
8. Select SNMP Trap as the type of monitor you want to create.

9. In the SNMP Passive Monitor instance dialog, enter 'Temperature Port1 Critical Alerts' in the Name box.

10. In the Generic type (Major) box, select 6 Enterprise Specific.

The screenshot shows the 'SNMP Passive Monitor Instance' dialog box. It has the following fields and controls:

- Name:** Text box containing 'Temperture Port1 Critical Alert'.
- Description:** Text box containing 'SNMP Monitor'.
- Enterprise/OID:** Text box containing '1.3.6.1.4.1.3854.1' with a browse button (...).
- Generic type (Major):** Dropdown menu set to '6 Enterprise Specific'.
- Specific type (Minor):** Dropdown menu set to '101'.
- Payload:** A list box with one entry: '1\,3\,6\,1\,4\,1\,3854\,1\,7\,1\,0=4'. To the right of the list are buttons: 'Add...', 'Edit...', 'Remove...', 'OK', 'Cancel', and 'Help'.

11. Click the Browse (...) button to access the SNMP MIB Browser.

12. In the SNMP MIB Browser, find private > enterprises > akcp > sensorProbe > sensorProbe# > spTemperature1Status. This is the SNMP Trap ID for the Temperature MIB.

13. Click OK.

14. In the Enterprise/OID box, delete the last two digits behind the 2 in the OID. This should leave 1.3.6.1.4.1.3854.1 in the box.

15. In the Payload box, click Add to build the expressions that you want to match on for the passive monitor.

16. Click OK to add the monitor to the Passive Monitor Library, and then click OK to record the selection of the new monitor type.

17. On the Select Passive Monitor Type dialog, click Next.

18. In the Setup Actions for Passive Monitors dialog build a list of actions that you have created in the Action Library. When a trap is received that match the payload, these actions are fired.

The SNMP Trap Listener is currently **ON**

Time	Trap	Payload
Wednesday, December 13, 2006 02:12:20 PM	spTemperature1Status	TrapName=sensorProbe-101 TrapMajor=6 TrapMinor=101 spSensorStatus.0=4 CommunityName=public 1.3.6.1.4.1.3854.1.7.1.0=4 spSensorDescription.0=Temperature1 Description 1.3.6.1.4.1.3854.1.7.2.0=81 spSensorLevelExceeded.0=70 1.3.6.1.4.1.3854.1.7.3.0=70 Packet Type=Trap spSensorName.0=Temperature1 1.3.6.1.4.1.3854.1.7.4.0=0 1.3.6.1.4.1.3854.1.7.5.0=Temperature1 Protocol Version=SNMPv1 1.3.6.1.4.1.3854.1.7.6.0=Temperature1 Description spSensorValue.0=81 Timetick=1 days 02:26:27.50 spSensorIndex.0=0 Object=1.3.6.1.4.1.3854.1 (sensorProbe)
Wednesday, December 13, 2006 02:12:10 PM	spTemperature1Status	TrapName=sensorProbe-101 TrapMajor=6

<http://www.ipswitch.com/Support/whatsup/guide/v800/12snmpa4.html>

<http://www.ipswitch.com/products/whatsup/professional/docs/snmp.pdf>

MRTG

MRTG

MRTG will monitor SNMP network devices and draw graphs showing how much traffic has passed through each interface. The securityProbe is fully compatible with MRTG. You will need to download and install MRTG, and then create a configuration script. The configuration script will instruct MRTG how to pull the data from the system via SNMP. MRTG will then produce an HTML file giving you graphs for daily, weekly, monthly, and yearly statistics.

The HTML file can be recreated at periodic intervals by using MRTG to provide a live up to date graph. A web server will give the latest graphs to all users in the enterprise will publish this HTML file.

How do I install MRTG?

MRTG can be downloaded from <http://www.mrtg.org>. This site has instructions on how to download MRTG and install it. MRTG will run on both Linux and Windows platforms.

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

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:public@192.168.0.205  
MaxBytes[CONFIG-NAME]: 1000  
Options[CONFIG-NAME]: growright, nopercent, gauge  
Title[CONFIG-NAME]: /*Title to display in the html page*/  
PageTop[CONFIG-NAME]: /*Page heading */  
YLegend[CONFIG-NAME]: Deg C / % Humid  
ShortLegend[CONFIG-NAME]: &nbsp;nbsp;  
Legend1[CONFIG-NAME]: Temperature  
Legend2[CONFIG-NAME]: Relative Humidity  
LegendI[CONFIG-NAME]: Temperature&nbsp; in &deg;C&nbsp;nbsp;  
LegendO[CONFIG-NAME]: Humidity&nbsp; in %&nbsp;nbsp;  
*****
```

The CONFIG-NAME is the base name for files, which will be generated by the 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 to your needs.

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

Below is a list of OID's for temperature and 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 #temperature on port 1
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.1 #temperature on port 2
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.2 #temperature on port 3
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.3 #temperature on port 4
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.4 #temperature on port 5
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.5 #temperature on port 6
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.6 #temperature on port 7
.1.3.6.1.4.1.3854.1.2.2.1.16.1.3.7 #temperature on port 8

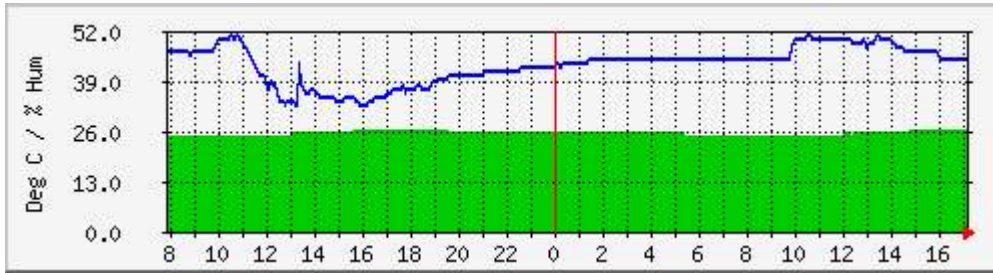
Humidity OID's:

.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.0 #humidity on port 1
.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.1 #humidity on port 2
.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.2 #humidity on port 3
.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.3 #humidity on port 4
.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.4 #humidity on port 5
.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.5 #humidity on port 6
.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.6 #humidity on port 7
.1.3.6.1.4.1.3854.1.2.2.1.17.1.3.7 #humidity on port 8

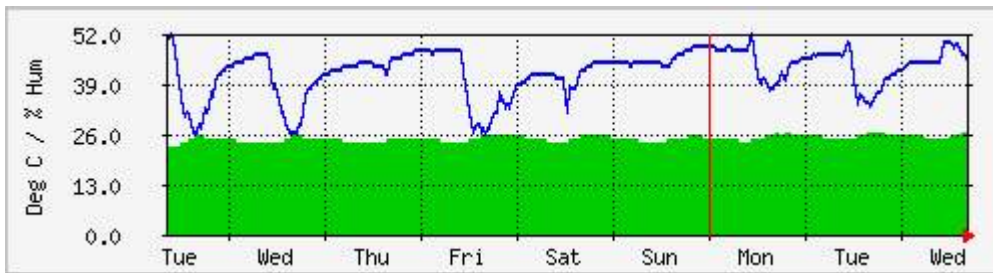
Any sensor producing a graphical data in the system can be configured using MRTG. For more information on configuring the system with MRTG, please mail us at support@akcpinc.com.

Sample MRTG Graphs

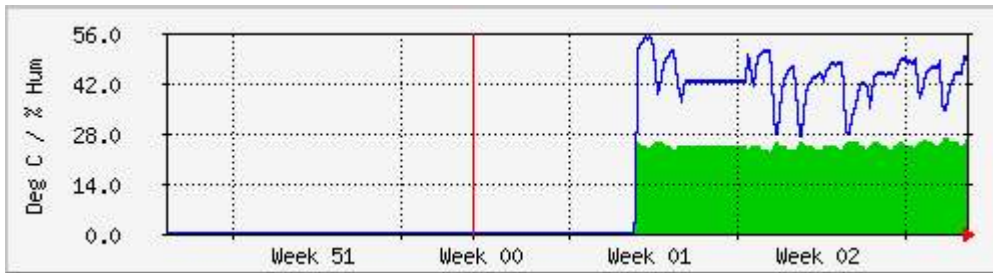
`Daily' Graph (5 Minute Average)



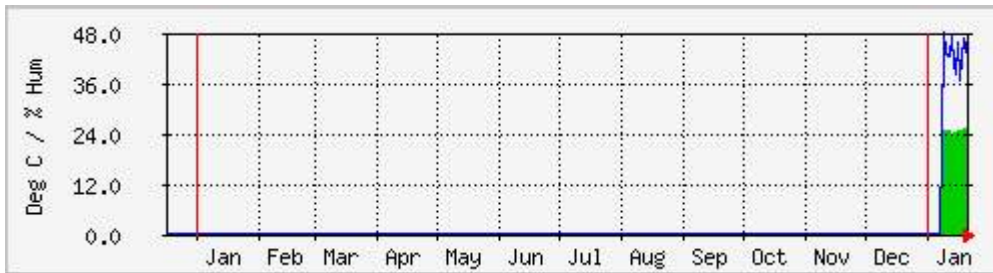
`Weekly' Graph (30 Minute Average)



`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

Other NMS

Other NMS

The securityProbe can be integrated with any Network Management System that is SNMP compliant.

If you need any information on integrating with any NMS, you can contact the technical support team at support@akcpinc.com