80 Virtual Sensors User Manual

Table of contents

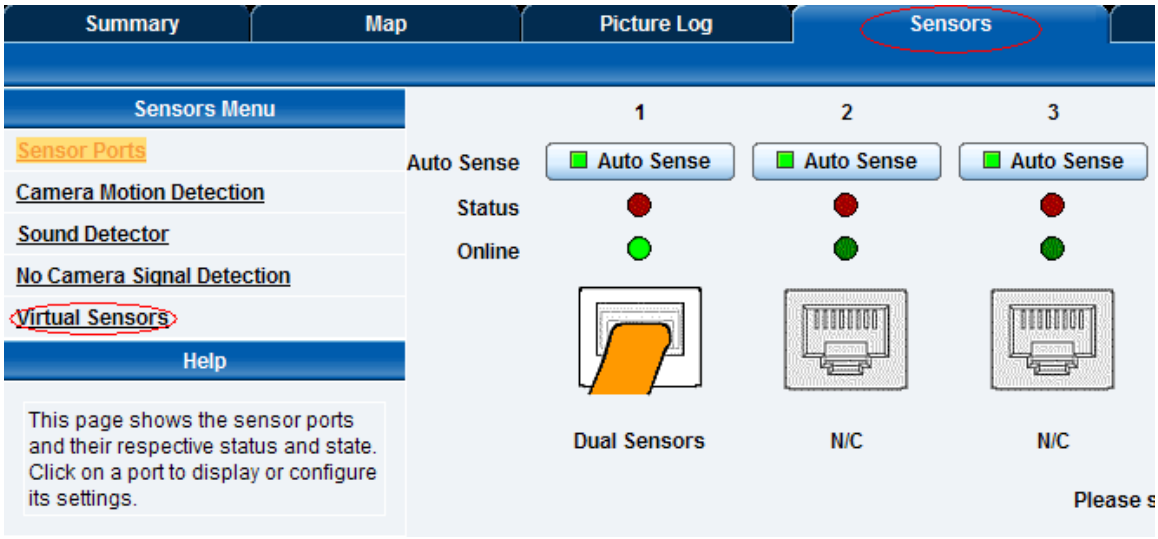
1. Introduction:

Virtual sensors can be a very powerful tool in your monitoring system. On the securityProbe, you can have up to 80 of these virtual sensors and they allow for a multitude of applications.

Integration with MODBUS networks with the securityProbe as a MODBUS master/slave, SNMPget and ping commands and others are all possible from the virtual sensors. An example use of this could be to use the securityProbe as a probe manager. If you had a securityProbe and multiple sensorProbe devices they could all be monitored, mapped and alerted via the securityProbe. You can perform SNMPget commands on a server to monitor memory or CPU load, or you can ping network enabled devices and be alerted if they go offline.

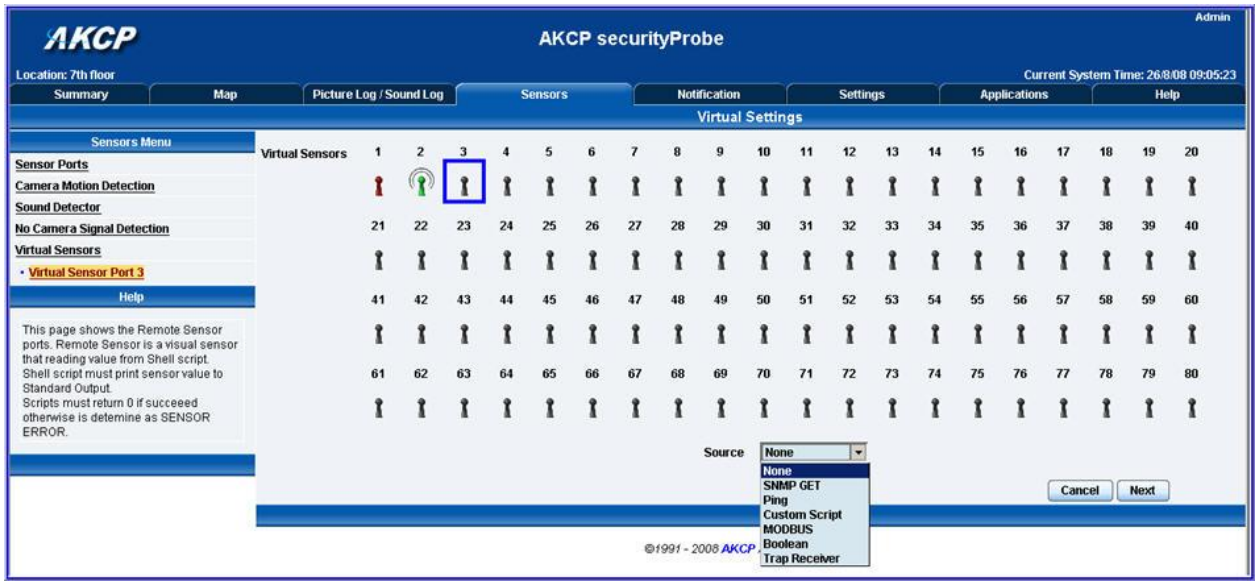
2. Configuring Virtual Sensors

The virtual sensors are found in the **Sensors tab** and **"virtual sensors"** from the left hand menu.



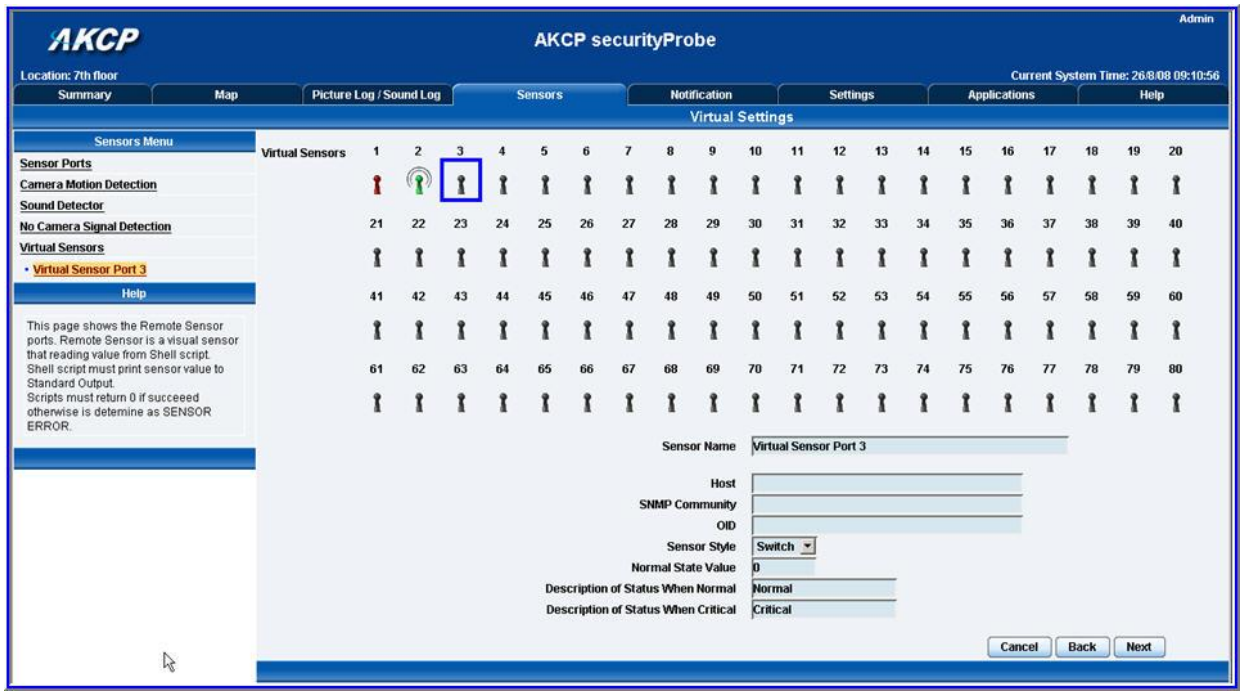
You will then be presented with the following screen, showing your 80 virtual sensors:-

Click on the first available virtual sensor (in this case 3) you can then choose what type of sensor to setup from the next screen. First click on the **"Configuration"** button, then you will have a choice of SNMP Get, Ping, Custom Script, MODBUS, Boolean, or Trap Receiver.



3. SNMP GET:

If you select SNMP get from the menu and click next, you will get the following page:



Sensor Name: - Input the name you wish to use to identify your virtual sensor.

Host: - The IP address of the unit on which you wish to perform an SNMPget command. For example, this could be the IP address of a sensorProbe2 device.

SNMP community: - The SNMP write access password, default is usually “public”.

OID:- The OID for what you wish to monitor. If for example you want to poll temperature data from a sensorProbe 2 device with a temp sensor on port 1, then you would use the following OID:

1.3.6.1.4.1.3854.1.2.2.1.16.1.3.0

where the last digit (0) is port 1. For port 2 the last digit would be 1. If you are monitoring some other device, you will need the relevant OID for what you wish to measure. You may use the **"Get SNMP OID"** button to get OIDs for AKCP devices/sensors.

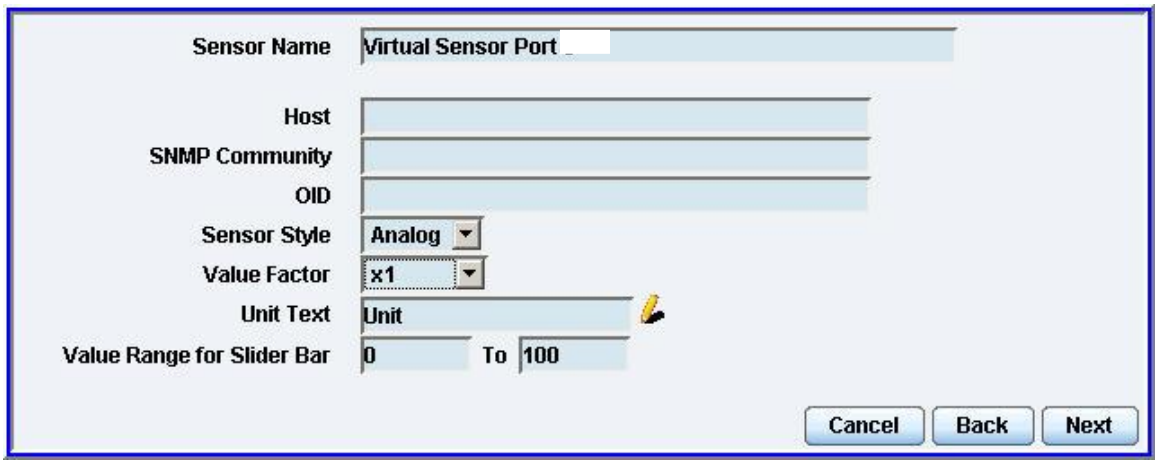
Sensor Style: - Choose either switch or analog. A switch sensor would be for example a water sensor, on or off, an analog sensor would be a temperature sensor or humidity sensor, or some other sensor that gives a data value.

Description when Normal: - ex., Normal, Critical, Online etc.

Description when Critical: - ex., Critical, Offline, Low etc.

Normal State value: - 0 or 1 (for switch type sensor only).

If you choose an **analog** style sensor, you will get a slightly different menu:



Value Factor gives you the chooses from the drop down menu as x1, x 0.1, x 0.01 or x0.001

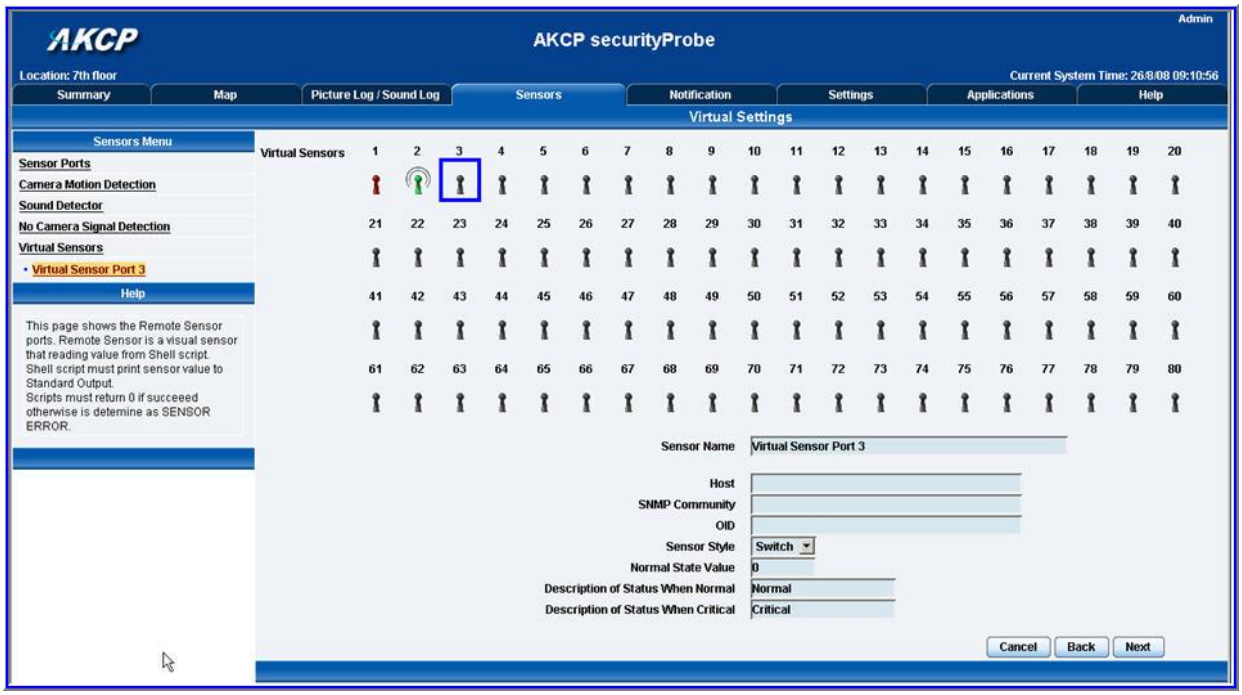
Unit text: - example, if measuring temperature "degrees centigrade" or if measuring humidity "percentage humidity" etc.

Value range for slider bar: - The range that you wish to measure. For temperature you could put the max at 100 for 100 degrees, or humidity, 100 for 100%.

When finished, click on **next**, you can then configure the time interval between data polling.

4. PING

If you select a Ping virtual sensor and click next, you will get the following screen:-



Sensor Name: - The name you wish to use to identify the sensor, for example “Ping of server”

Host: - The IP address of the network device you wish to ping

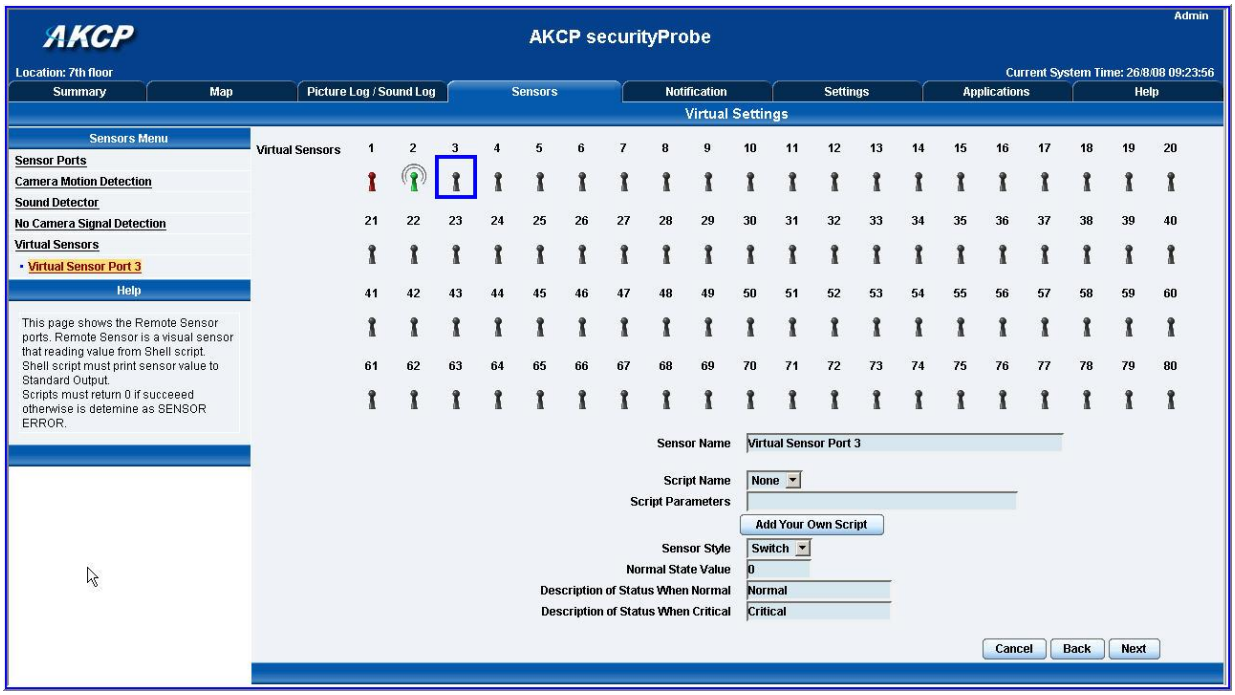
Description when Normal: - ex., online

Description when critical: - ex., offline

Normal state value: - 0 = ping successful, 1 = ping times out.

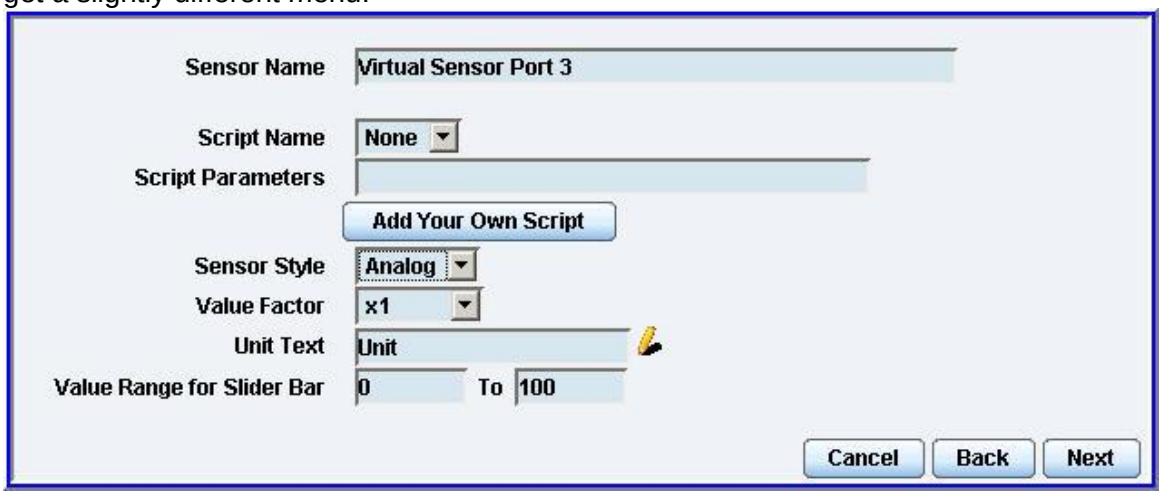
5. CUSTOM SCRIPT

If you select a Custom Script and click next, you will get the following screen:-



Sensor Name: - The name you wish to use to identify the sensor, for example “Custom Script of sensor”

You can add **Script Parameters**. **Add Your Own Script** button allows you to attach your own script file. If you have chosen **Analog** from the **Sensor Style** option you will get a slightly different menu:



The securityProbe supports Perl and Bash scripts. When uploading these types of script files, you have to conform to the Linux script file format specifications. Most importantly, these files need headers like this:
#!/

for Perl script:	#!/usr/bin/perl
for Bash (shell) script:	#!/bin/sh
for PHP script:	#!/usr/bin/php -q

The SEC is using a hash-bang tag (#!) to validate the script. It checks if there is the hash-bang tag (#!) at the beginning of the script. This tag is used to give the interpreter path to run the script, for example the PHP interpreter.

The file must be in UNIX format, if it's created in the Windows format it will not work as the SEC is running Linux (the line break characters are different).
You need to convert the file format to UNIX (you can use Notepad++ program: Format Menu> Convert to UNIX Format) before using it.

How to generate an SNMP Set on a remote device as an action

First you need to create a "Custom Script" action in the Notifications page, and then add the script below.

Note: check the script format requirements in the previous section.

This is a Bash script so it needs a file header like this: #!/bin/sh

```
#!/bin/sh

COMMUNITY=$1
DESTINATION=$2
SET_VALUE=$3
snmpset -v1 -c$COMMUNITY $DESTINATION .1.3.6.1.4.1.3854.1.2.2.1.18.1.3.0 i
$SET_VALUE
```

The script requires 3 arguments.
Specify them by entering them in the **Arguments** box of the Custom Script action.

Example of the arguments value:
public "192.168.0.100" 2

Where

public	means the SNMP community
"192.168.0.100"	means the destination IP address
2	means the value needed to be set (must be an integer)

Setting Up a Timed Virtual Sensor Custom Script

This Custom Script (request the file from support) can be run on the virtual sensor to trigger a sensor at a certain time:

Use the attached (please request from support) script with these settings below:

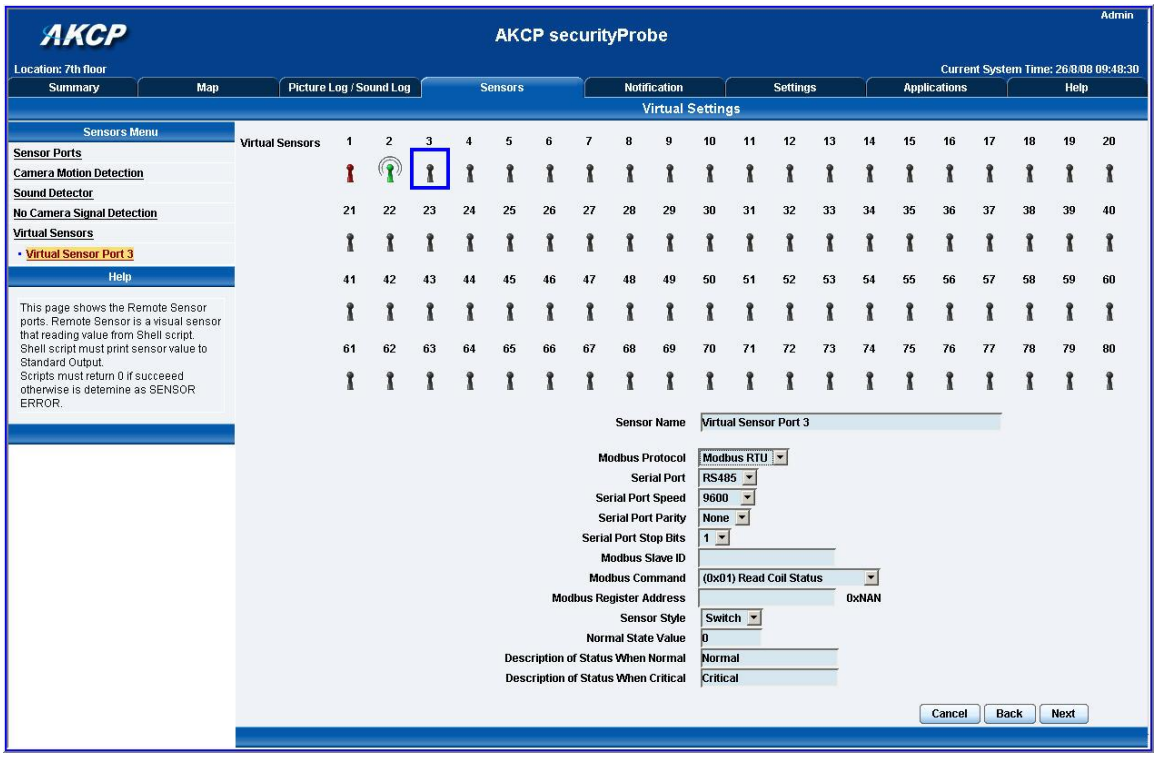
Script Parameters: TIME_HOUR TIME_MIN example:20 0 (means 20:00)
Sensor Style: Switch
Normal State Value: 0

The custom script virtual sensor status will change to critical when the time is matched. So, for example, if you wanted the camera to take a picture at a certain time, you would need to first create the picture log action, and link the virtual sensor with that picture log action.

For example, you can also then link this custom script to trigger a switch type sensor.

6. MODBUS

If you select MODBUS and click next, you will get the following screen:-



Sensor Name: - The name you wish to use to identify the sensor, for example “MODBUS”

You can select the Modbus Protocol to either **Modbus RTU (serial)** or **Modbus TCP (Ethernet Network)**.

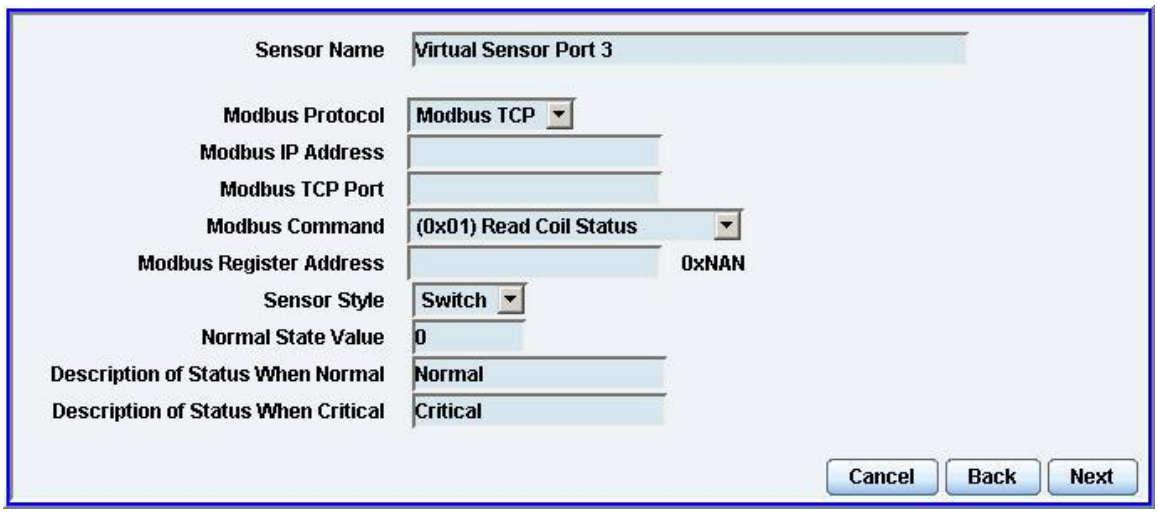
7. MODBUS RTU

If selecting the Modbus RTU protocol, you will use the RS485 port to connect the Modbus device. See the following picture of the securityProbe with the RS485 port highlighted.

Still following the screen shot above, you will then select your **Serial Port Speed**, your **Serial Port Parity** as *None*, *Odd* or *Even*. Select the **Serial Port Stop Bits** as *1* or *2*, enter the **Modbus Slave ID** (each slave in a network is assigned a unique unit address from *1* to *247*), the **Modbus Command**, which includes 4 options for the virtual sensor: *(0x01) Read Coil Status*, *(0x02) Read Input Status*, *(0x03) Read Holding Registers* and *(0x04) Read Input Registers*. You will then enter the **Modbus Register Address** and the **Style** of the sensor, the **Normal State Value** and **Descriptions** of the sensor status.

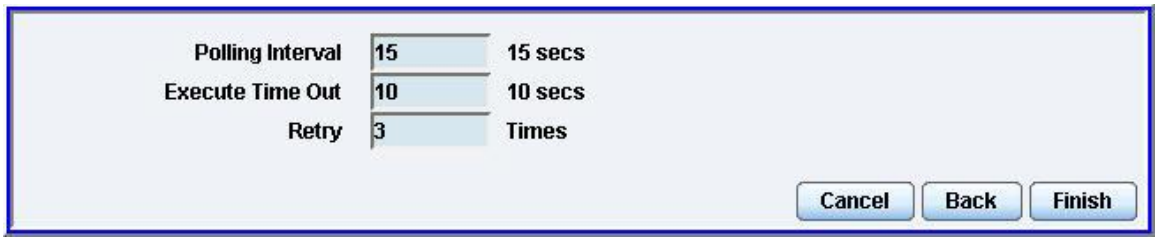
8. MODBUS TCP

If selecting the Modbus TCP protocol, you will get the following screen:



You will then enter your **Modbus IP Address**, your **Modbus TCP Port**, and again your **Modbus Command**, your **Modbus Register Address**, your **Sensor Style**, **Normal State Value** and the **Descriptions** of the sensor status.

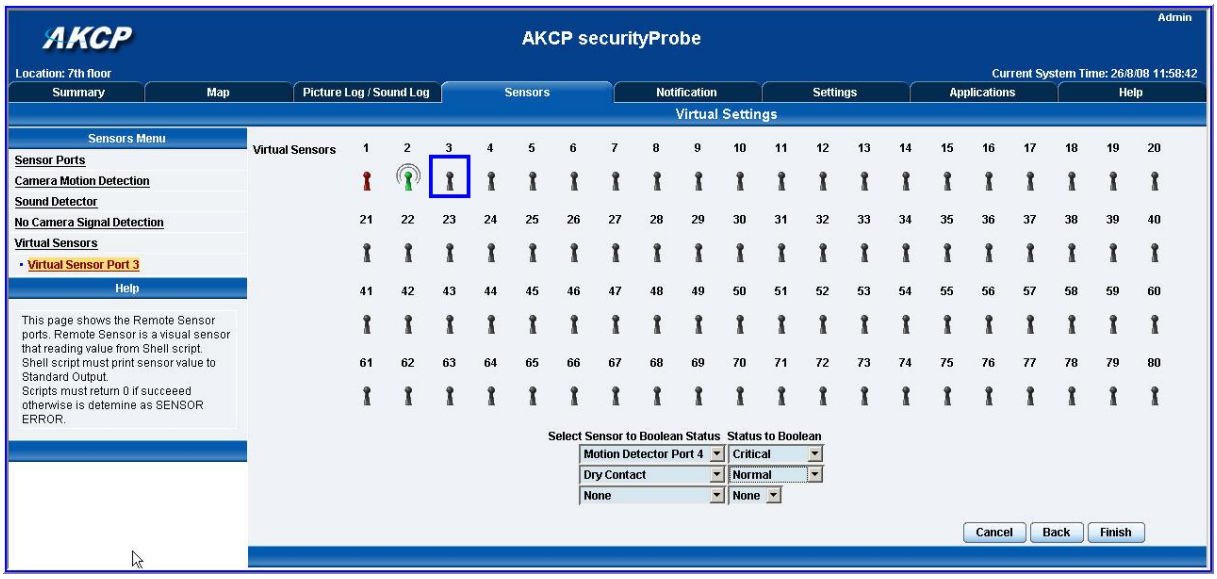
You will get the follow screen when choosing either Modbus RTU, or Modbus TCP:



This screen is where you will enter your **Polling Interval**, your **Time Out periods** for the sensor and also your **Retry amount**. You will click on the **Finish** button to complete the Modbus setup wizard and return to the Virtual Sensor main screen.

9. Boolean

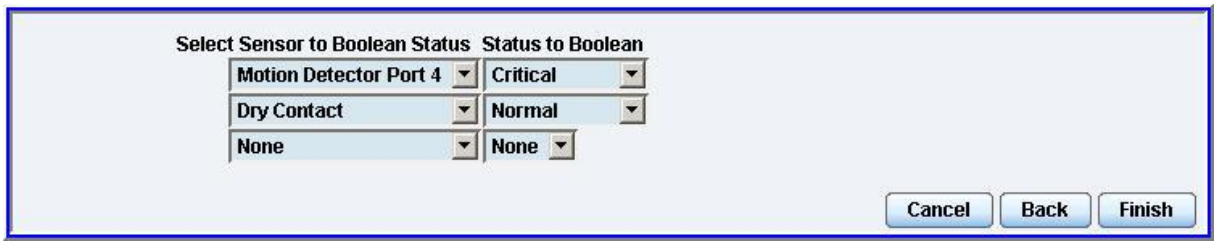
If selecting Boolean, you will get the following screen:



Boolean works on the virtual sensor by checking the status of, for example 2 to 3 sensors and if the sensors status matches that of the setting, they will return a value of 1 (TRUE). The normal value is 0 (FALSE).

The Boolean virtual sensor is an AND type Boolean: all configured statuses have to be TRUE to have the virtual sensor's final status return TRUE (or 1).

For example, you can set your motion sensor to *critical* and the dry contact to *normal* like the image example below, and then set your notification page to make the notification:

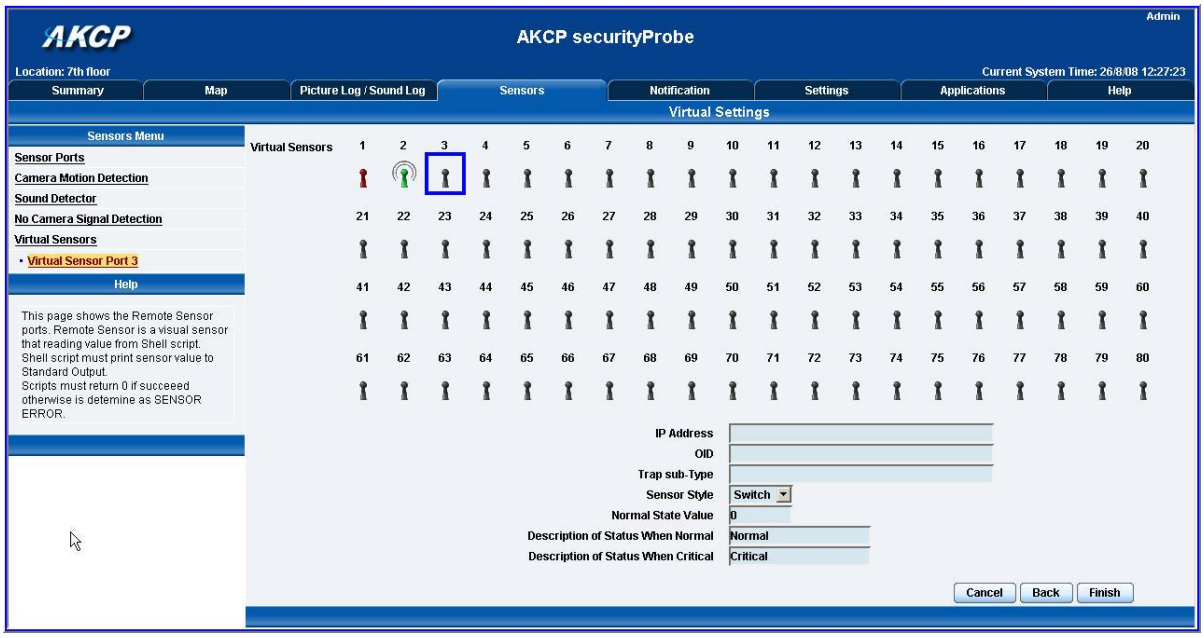


The virtual sensor will return TRUE (1) status when the Motion Detector is in *critical* status AND the Dry Contact is in *normal* status.

Otherwise, in all other cases, the virtual sensor will return FALSE (0) status.

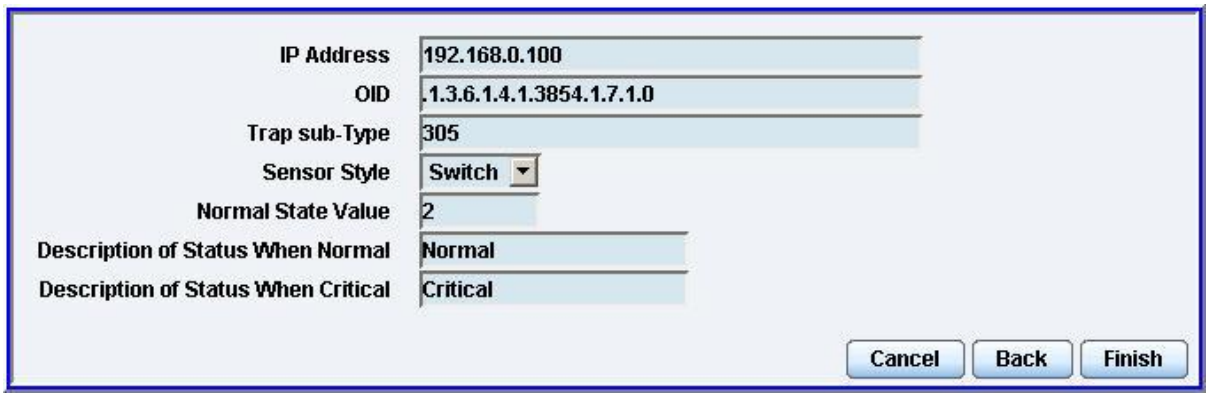
10. Trap Receiver

If selecting the Trap Receiver, you will get the following screen:



The Trap Receiver feature on the Virtual Sensor will check 3 parameters before setting a value. These three parameters are the **IP Address**, the **sensors OID** and the **Trap sub-type**.

In our example below the Trap is sent by the motion sensor on port 5 of our sensorProbe unit. Our *device IP* is 192.168.0.100. Our sensorProbe *Trap Type* is set to the specific sub type and will check status of our motion sensor in the following screen.



The Trap Receiver feature on the Virtual Sensor will check 3 parameters before setting a value.

Normally the Trap will have 6 OIDs:

1. spSensorStatus (.1.3.6.1.4.1.3854.1.7.1.0). The current integer status of the sensor causing this trap to be sent.

(noStatus(1), normal(2), highWarning(3), highCritical(4), lowWarning(5), lowCritical(6), sensorError(7), turnOn(8), turnOff(9)).

2. spSensorValue (.1.3.6.1.4.1.3854.1.7.2.0).The current integer value of the sensor causing this trap to be sent.

3. spSensorLevelExceeded (.1.3.6.1.4.1.3854.1.7.3.0).The integer level that was exceeded causing this trap to be sent.

4. spSensorIndex (.1.3.6.1.4.1.3854.1.7.4.0).The integer index of the sensor causing this trap to be sent.

5. spSensorName (.1.3.6.1.4.1.3854.1.7.5.0).The name of the sensor causing this trap to be sent.

6. spSensorDescription (.1.3.6.1.4.1.3854.1.7.6.0).The description of the sensor causing this trap to be sent.

The specific value depends on the sensorProbeTrap type (.1.3.6.1.4.1.3854.1.2.2.1.60.0)

If it is set to specificTypeTrap(1) specific value is to show the sensor type and port (Specific value of Motion Sensor port 5 is 305)

If it is set to generalTypeTrap(2) specific value is to show the sensor type (Specific value of Motion Sensor port 5 is 30)

If it is set to bothTypeTraps(3) device will send the trap two times specific value will show sensor type and show sensor type and port (Specific value of Motion Sensor port 5 is 305 and 30)

If it is set to statusTypeTraps(4) specific value is up to status of sensor (spSenUnknownStatus(51), spSenNoemalStatus(52), spSenWarningStatus(53), spSenCriticalStatus(54))

Example: Trap send by Motion Sensor port 5 on our device, IP is 192.168.0.100 sensorProbeTrapType is set to pecificTypeTrap and need to check the status of the Motion Sensor:

IP Address is 192.168.0.100

OID is .1.3.6.1.4.1.3854.1.7.1.0

Trap sub-Type(Specific) is 305

Sensor Style is Switch

Normal State Value is 2 (2 means sensor status is normal so far)

Please contact support@akcp.com if you have any further technical questions or problems.

Thanks for Choosing AKCess Pro!