User Manual

BTH UPS SNMP MONITOR v 11.06

Table of Contents

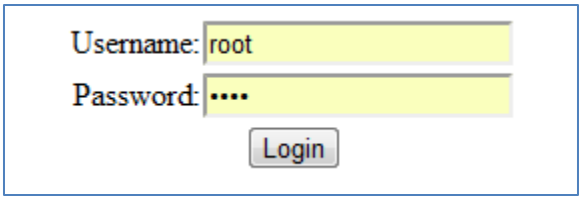
1 Install

Please see “README.TXT”.

2 Users

There are three kinds of users, *viewer*, *admin* and *root*. Only one build-in *root* is allowed, they could control everything. *Root* is the special one from *admin* group as *root* has all the power of *admin* and other important authority. *Anyone* will be mentioned and it means any kind, any one of the users.

3 Login



Anyone should login to manage or view system.

The default password for *root* is *root*. Three more uses: *admin1*, *admin2* and *user1*. Their default passwords are the same as the usernames.

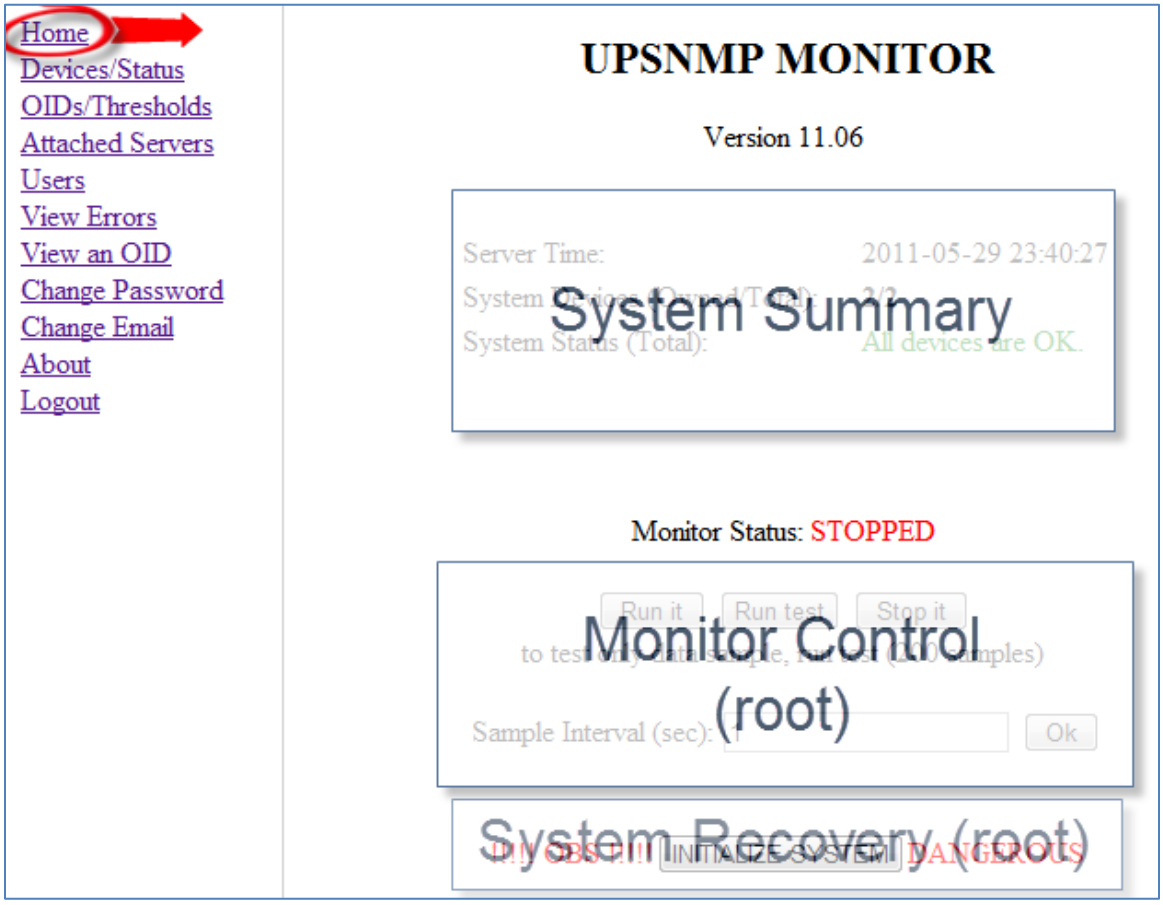
Please change it after logged in.

4 Display Overview

There are three areas: LOGO, MENU and Main Display.

5 Menu

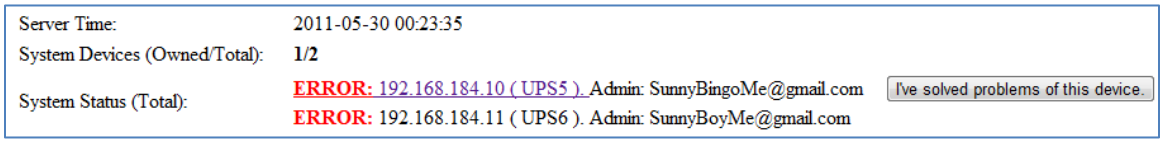
5.1 Home (restricted authority)



5.1.1 System Summary (restricted authority)

At *home*, *anyone* could see *System Summary*. *System Devices* now showing: 2/2 which means there are 2 devices in the system, and this logged-in user could control all of them as this user is *root*. Normally, it would be 1/2 or 3/5 etc. For *viewer*, it should be 0/2 or 0/5.

The *System Status* usually is "*All devices are OK.*" If there are some problems, it would be:



where *anyone* could see the *ERROR: device ip (Device Name) Admin's email.* of all devices, but only *admin* who own this device or *root* could click the url to see what happened in *Details of Device* window. The *admin* or *root* also could reset this flag after they solved problems. To make sure the problems will be noticed, the flag should be reset manually.

5.1.2 Monitor Control (root only)

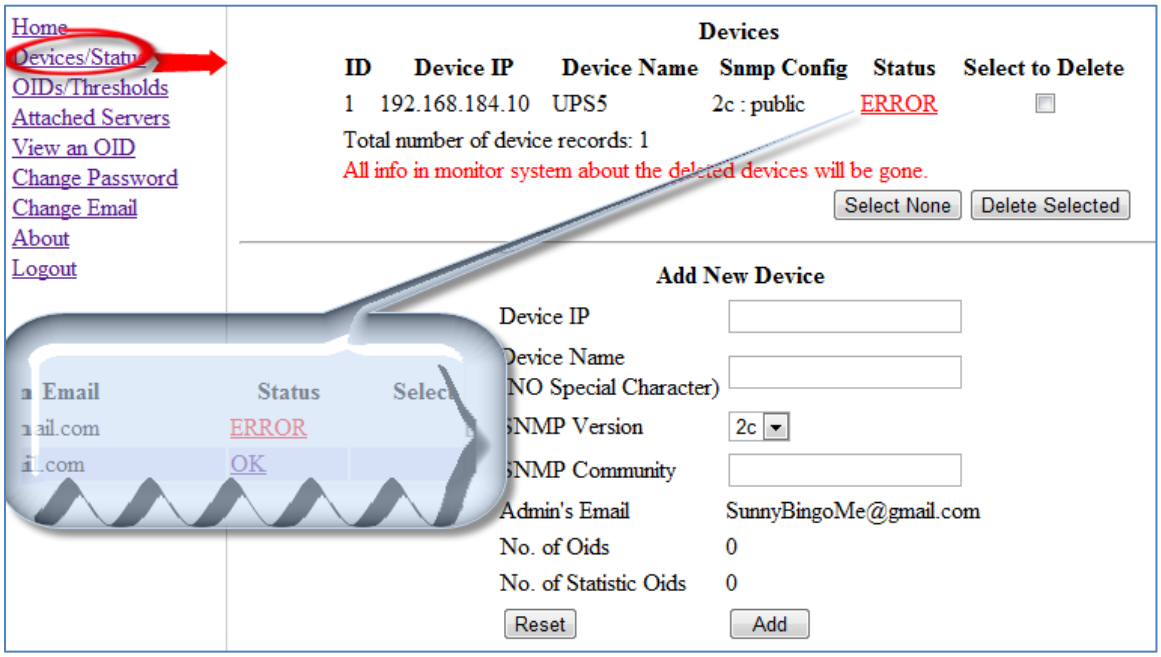
Though *anyone* could see the status of monitor, only *root* could stop or start the background perl monitor. The probe/sample interval will be configured by *root* here, too.

5.1.3 System Recovery (root only)

You could initialize the whole system via this button. Take care to use it because all history and the operations/actions will be gone, while only the demo users, devices, OIDs and attached servers will stay.

5.2 Devices and Status (admin only)

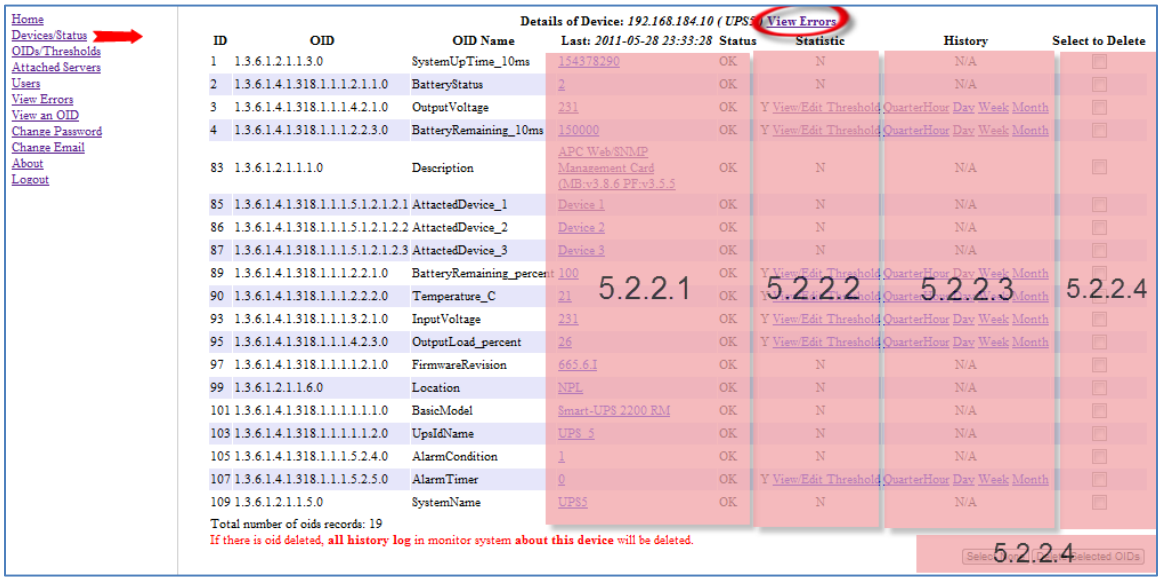
5.2.1 Devices Table



The *admins* and *root* could add or delete devices whose OIDs would be monitored by SNMP here. One device could be seen only by the *admin* who added it or the *root*.

The *Status* could be *ERROR* or *OK*, a user could click to see the details in *Details of Device* window.

5.2.2 Details of Device window

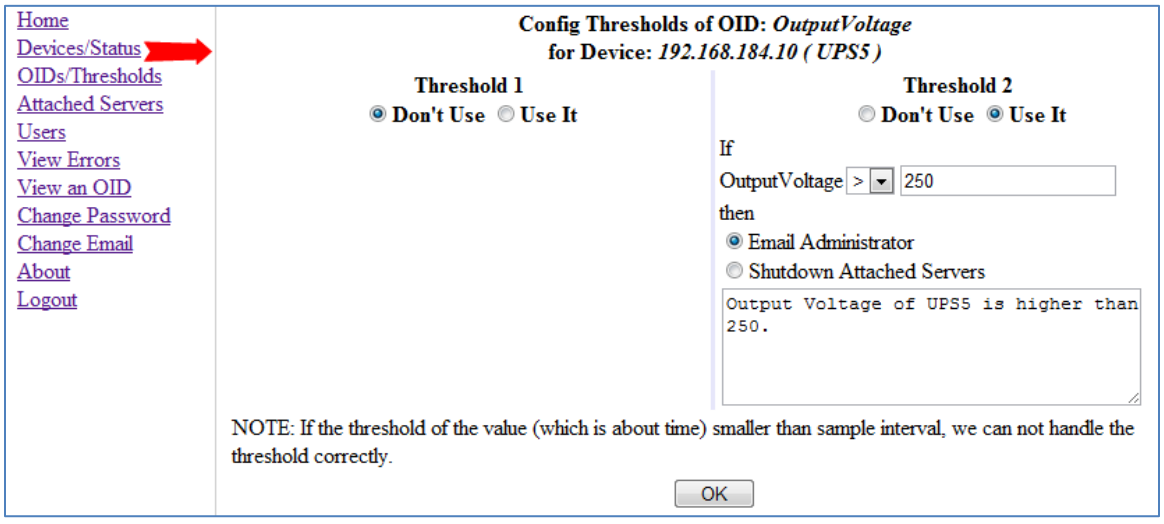


Here, a user could know the details of one device.

5.2.2.1 Current Values and Status

NOTE: If the *Status* of one device is *ERROR*, but the *statuses* of all OIDs of the same device are *OK*, it usually means *No response from remote host* when the monitor query this device. A user could click *View Errors* on the top to view the latest 1000 errors of this device.

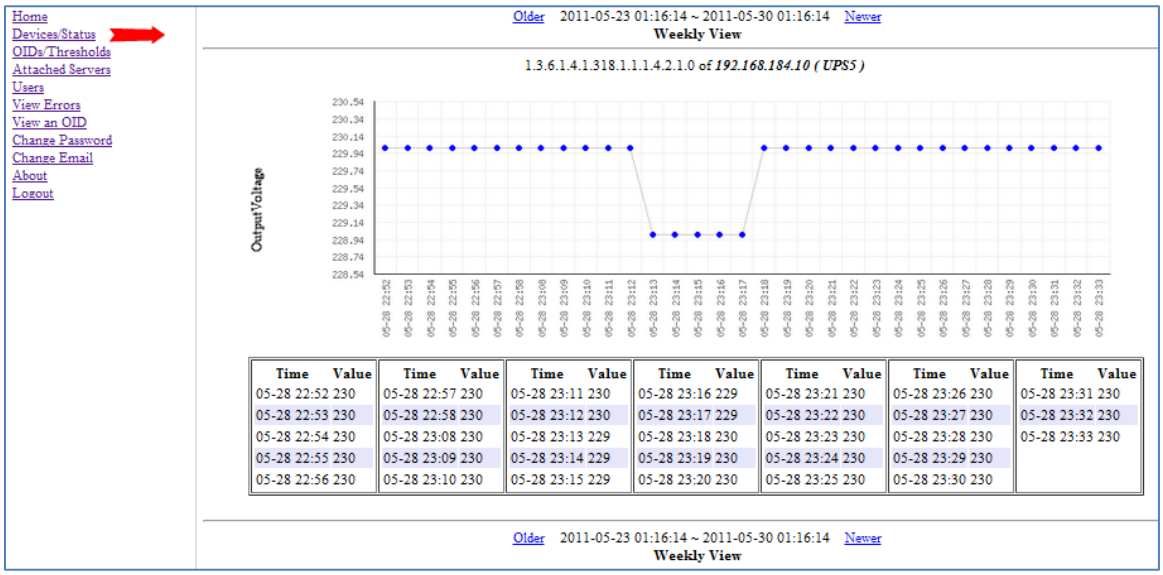
5.2.2.2 Thresholds



For a *Statistic OID* (see 5.3), a user could configure the thresholds for it. There are two thresholds for each OID at most. The alarm email could be sent or the *Attached Servers* (see 5.4) will be shut down when the battery is low or the voltage is too high etc. The *ERROR FLAG* will be set which the user could see in *Home* window or *Device and Status* window.

NOTE: Only one email will be sent for each device if the user does not reset the *ERROR FLAG* for the specific device.

5.2.2.3 History

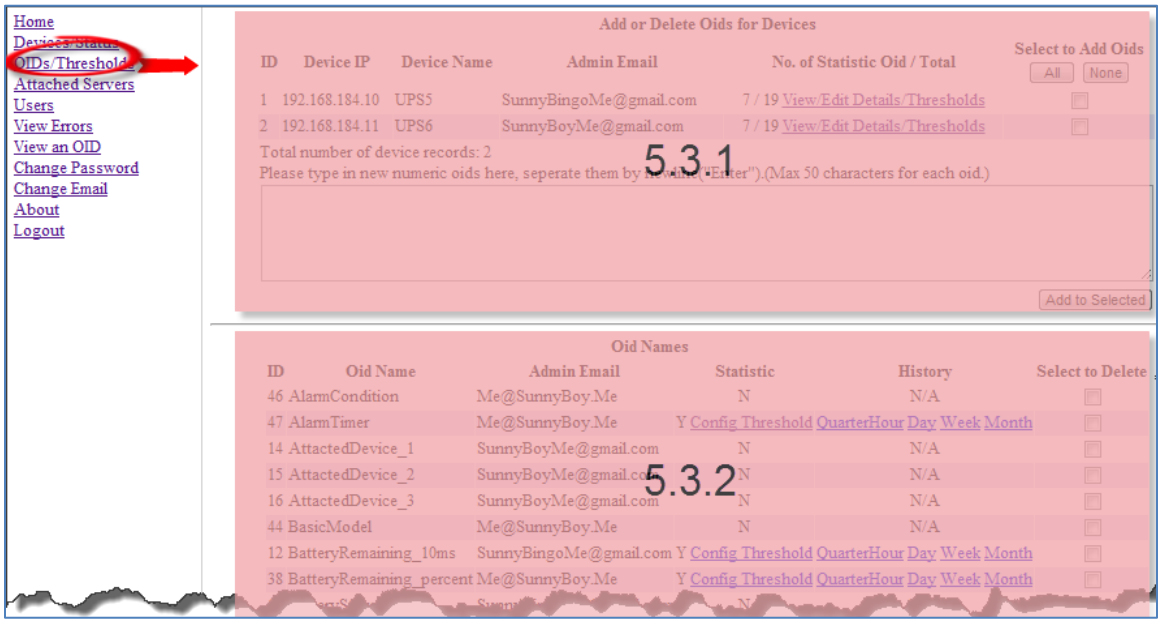


A user could view the history of each OID by one of four *View Types*: Quarter-hourly, Daily, Weekly or Monthly. The resolution of Quarter-hourly view is 15 seconds (but not higher than the sample resolution) at most and only the last 1 hour is available. The resolutions of the other three are 1 hour at most. In the last three *View Types*, the user could click the specific time slot on the graph to see details and the data will be stored for 5 months.

5.2.2.4 Delete OIDs

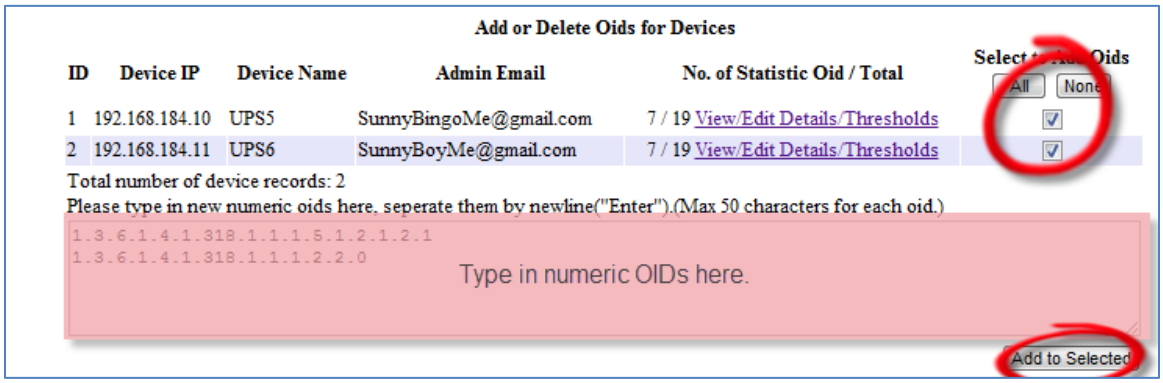
A user could select some OIDs and *Delete Selected OIDs* (To add OIDs, see 5.3.1).

5.3 OIDs and Thresholds (admin only)

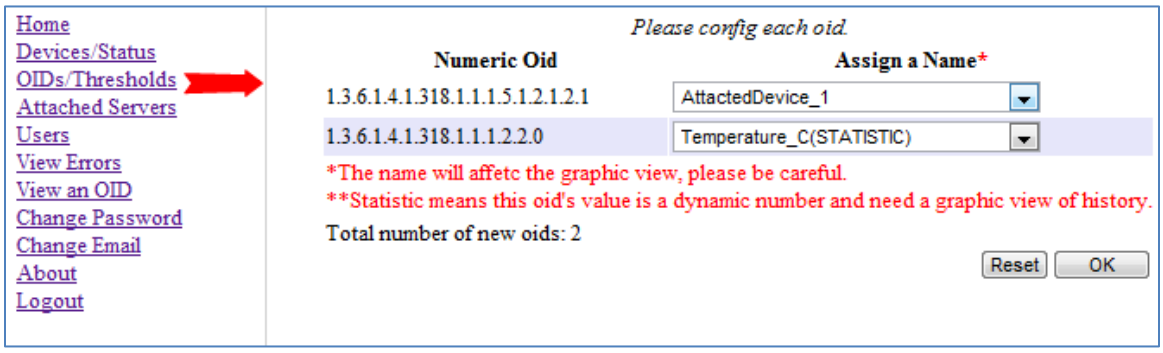


An *admin* could add OIDs here and *root* could configure the *OID Names*.

5.3.1 Add OID(s)



Type in the numeric OIDs which would be monitored and *Add to Selected* devices above.



When ask to assign a name to each numeric OID, choose the suitable name.

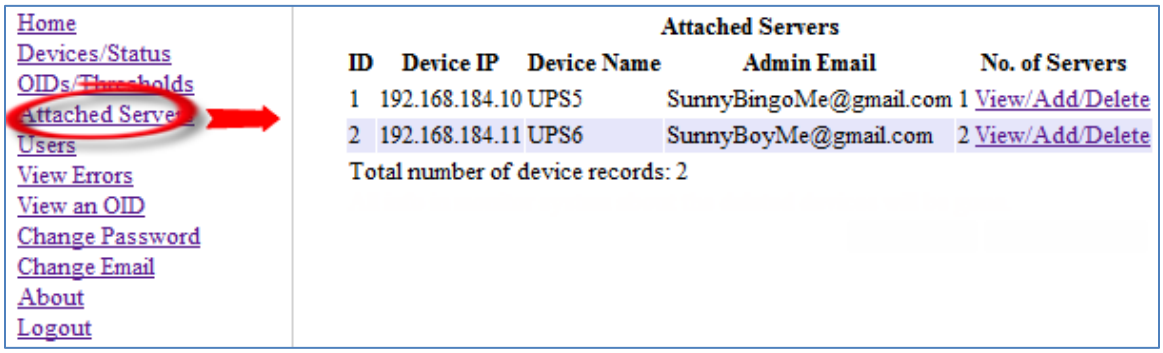
NOTE: Only the one with a *Statistic OID Name* will have the history graphs and values to view.

5.3.2 OID Names

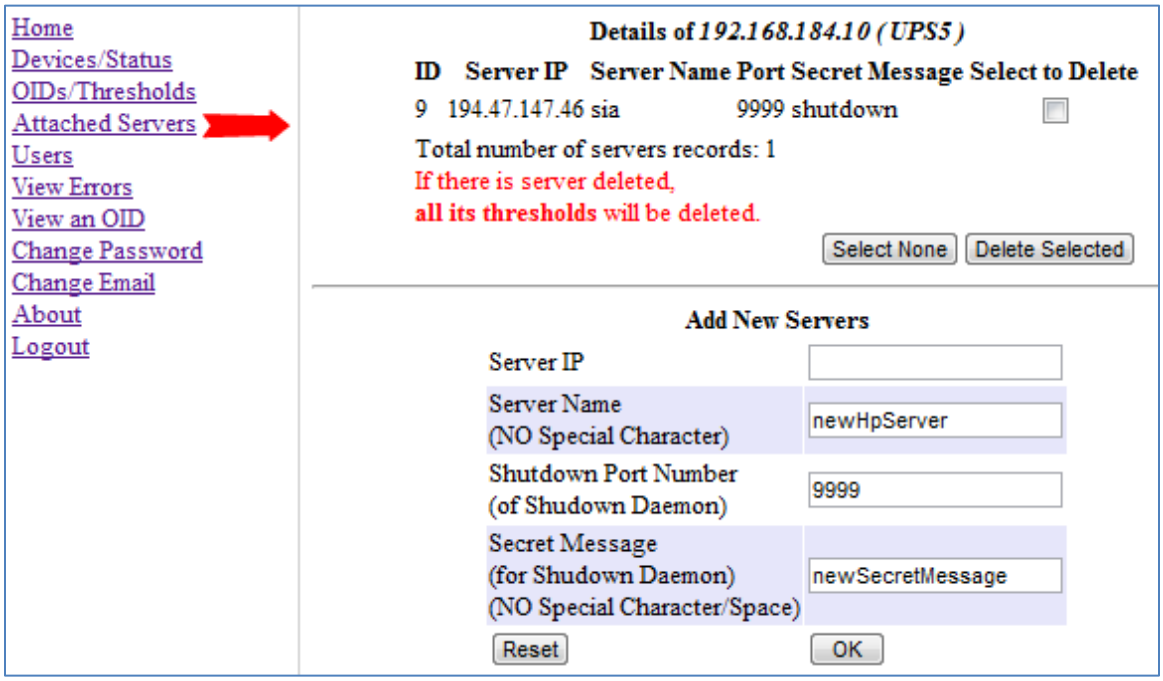
Root could add/delete/change OID names here, just like what could be done in the *Details of Device* window. As the *OID Names* will affect the whole system, *admin* shall apply to *root* to add/delete/change OID names if needed.

NOTE: 1. When deleting an *OID Name*, all OIDs with the name will be deleted. 2. Every device could not have the same numeric OID or *OID Name* more than once.

5.4 Attached Servers (admin only)



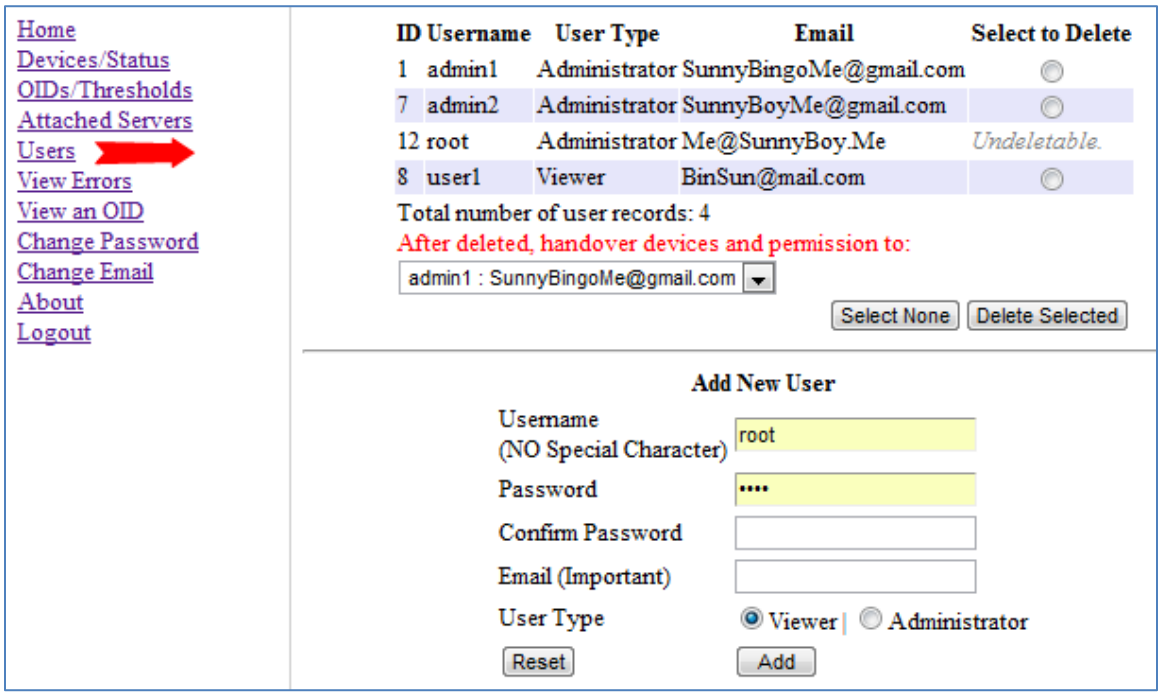
An *admin* could only choose one of the devices owned by the *admin*-self to configure the attached servers to shutdown (should be configured in thresholds, see 5.2.2.2).



An *admin* could delete/add new servers.

NOTE: To shut down the attached servers when an UPS going down, a daemon perl script (*shut.pl* in the folder *monitor*) should running on the *Shutdown Port Number* of the servers and the main monitor should have the permission to create a socket to send *Secret Message* to the specific *Shutdown Port Number* of the attached servers.

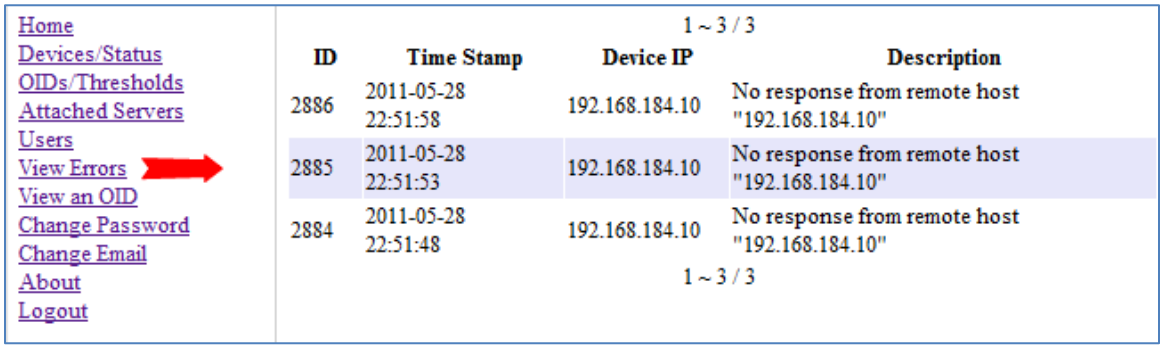
5.5 Users (root only)



Root could add/delete users here (except the *root*-self).

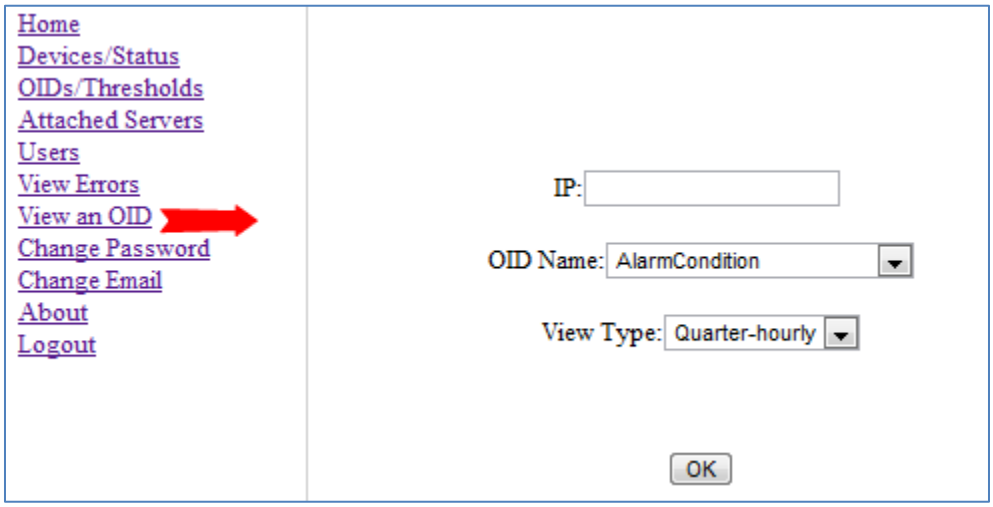
NOTE: When deleting a user, the authority and devices of the user should be handover to an already-exit *admin*.

5.6 View Errors (root only)



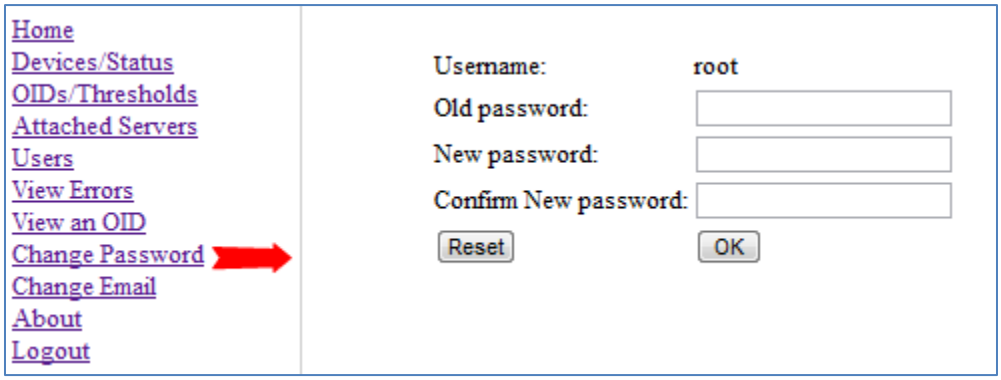
Root could see all errors of the whole system here without any restrict to specific devices owned (all devices are owned by *root*).

5.7 View an OID (anyone)



Anyone could view the history graph and values if they know the IP of the device.

5.8 Change Password (anyone)



Anyone could change the password for themselves. All passwords will be encrypted by MD5.

5.9 Change Email (anyone)

Anyone could change the email for themselves.

5.10 About (anyone)

Anyone could find the information about the system here.

5.11 Logout (anyone)

Please logout on time to keep system and data in safe (Though the web session may expire after 24 minutes if there is not any operation).