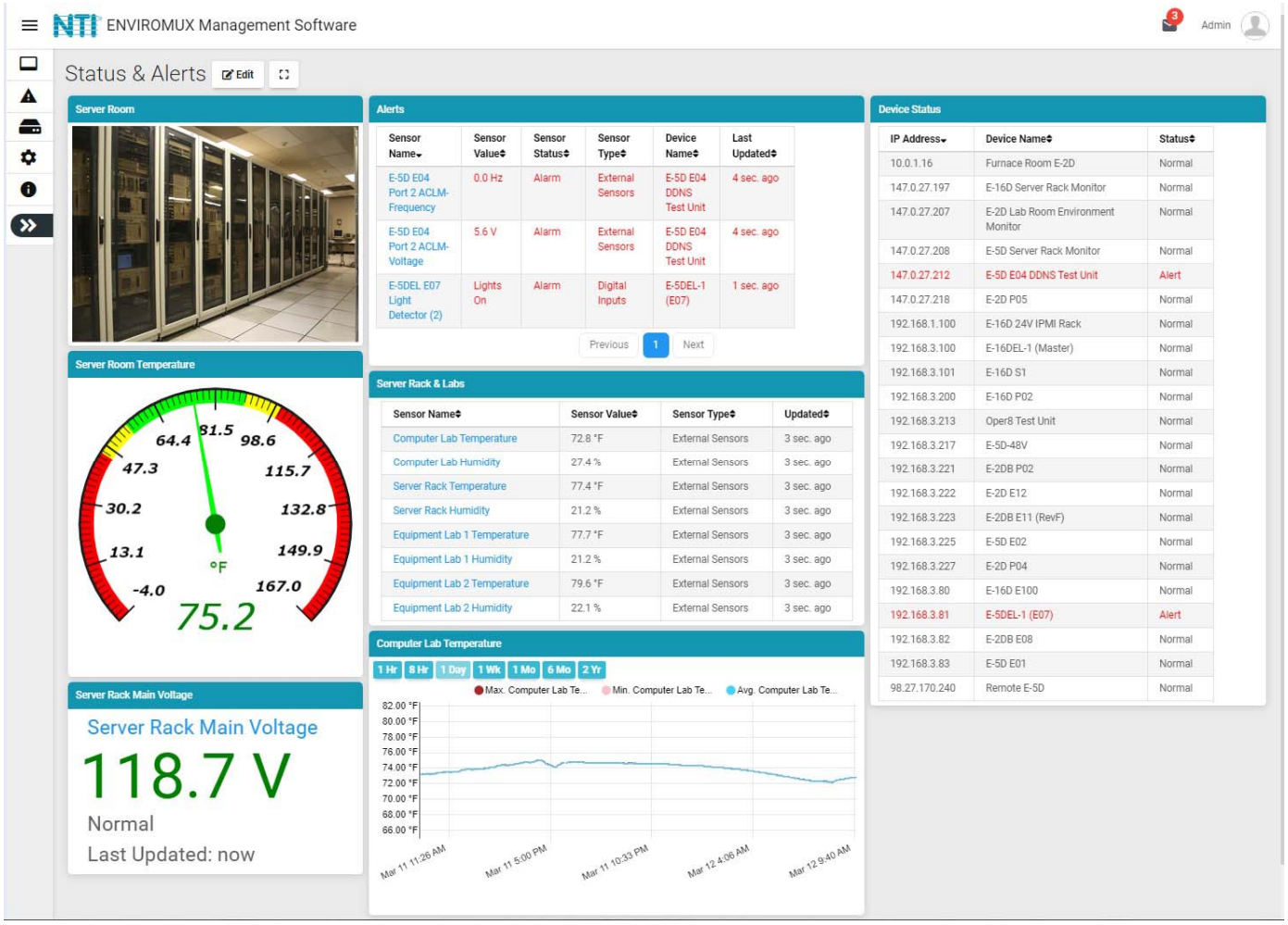
NETWORK TECHNOLOGIES INCORPORATED
1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.networktechinc.com

ENVIROMUX® Series

E-MNG-SH

Enterprise Environment Monitoring System
Self-Hosted Management Software



TRADEMARK

ENVIROMUX and the NTI logo are registered trademarks of Network Technologies Inc in the U.S. and other countries. All other brand names and trademarks or registered trademarks are the property of their respective owners.

COPYRIGHT

Copyright © 2020-2022 by Network Technologies Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of Network Technologies Inc, 1275 Danner Drive, Aurora, Ohio 44202.

CHANGES

The material in this guide is for information only and is subject to change without notice. Network Technologies Inc reserves the right to make changes in the product design without reservation and without notification to its users.

VERSION

Release Version 1.0.1.3.

Table of Contents

Table of Figures

INTRODUCTION

E-MNG-SH is a self-hosted Software program that provides an easy-to-use, unified interface for monitoring and configuring up to 3,000 E-16D, E-5D, and E-2D monitoring systems (Devices) and all connected sensors (internal, external, digital input and IP sensors and output relays via Ethernet. Supported IP sensors (when connected to Devices) include E-MICRO-TRH(P) and E-1W(P). The Software is installed on a Windows-based server or computer (the Server) to actively poll all Devices for status information and alerts. Any computer, smartphone, or tablet with a web browser can be used to access the Software. All enabled users can be kept up to date on sensor statuses and be alerted instantly when a sensor goes out of range of a configurable threshold.

Features:

- Devices may be monitored individually or in a group
- Display values and status for individual sensors or list of sensors.
- Unlimited number of users can access the Software program at the same time.
  - Users can configure their own Dashboards to display the data relevant to them and the window arrangement.
- Customize Dashboards to display Device status, sensor data, gauges, graphs, maps and IP camera snapshots.
- Any computer, smartphone, tablet with a web browser installed can be used to access the Software.
  - Access is operating system independent through the HTML5 user interface on the computer/smartphone/tablet's web browser.
  - No clients or special apps to install.
- Self-hosted Software – ideal for users in industries that require local Software management solutions for security or data privacy purposes.
- Plot the placement of E-LLDC-xx Liquid Location Detection Sensor Cables on floor plan maps to visually see the specific location of liquid presence when detected.

Software Requirements:

- Windows 7/8/10/11 32 or 64-bit, Windows Server 2008/2012/2016/2019/2022 32 or 64-bit.
- Requires firmware version 4.15 or later in E-xD Devices.

Note: We recommend the server/computer is protected by a firewall and anti-virus software if the server /computer is going to be accessed from the internet..

Server Roles and User Access:

One user is assigned as Super Admin to register the license and complete Software setup, plus has access to all Admin privileges.

Users with Admin access have privileges to add/delete E-xD Devices, edit sensors, set up Dashboards, acknowledge/dismiss alerts, simulate alerts, view logs, view sensor data, and monitor Dashboards. Admins can also add/edit/delete users (Administrators and Operators). Any number of users can be assigned as Admin.

Users with Operator access can acknowledge/dismiss alerts, view logs and sensor data, and monitor Dashboards. An unlimited number of users can be assigned as Operator.

Users with Read Only access can view alerts, logs, sensor data and monitor Dashboards. An unlimited number of users can be assigned as Read Only.

Virtual Machines

The E-MNG-SH self-hosted Software program now supports a floating Virtual Machine-friendly license.

MATERIALS

Materials supplied with this package:
NTI E-MNG-SH ENVIROMUX Self-Hosted Management Software including:

- NTI ENVIROMUX-Management-Software-Installer_Vx.x.x.x _x64.exe or
  NTI ENVIROMUX-Management-Software-Installer_ Vx.x.x.x _x86.exe (vx.x.x.x = the version number)
  The current version number is 1.0.1.3.
- Adobe pdf file of this manual

Note:

x86 is for 32 bit servers or computers which can only run 32 bit Windows OS and limits the maximum RAM size to 4GB.

x64 is for 64 bit servers or computers which run 64 bit Windows OS and has a much larger RAM size limit.

LIMITATIONS

- The Management Software:
  - Only Devices (E-xD) can be added with current version.
    - E-MICRO-TRH(P) and E-1W(P) can be added when attached to an E-xD as an IP Sensor.
  - Managing Device sensors on cascaded Devices are not supported currently.
  - Any changes to Device configuration done locally will require a re-load on the E-MNG-SH Software
  - Cannot change, save or restore individual E-xD configurations from the E-MNG-SH Software
  - Internet Explorer does not work with the E-MNG-SH Software

DOWNLOAD

To get the installer, go to our website .

- If you wish to evaluate the software, click on "**Request Server Software Evaluation**" and fill out the registration form. We will send the files and you can install it as described under "Installation".
- To purchase the software, you can go to our website or contact an authorized representative or NTI sales associate directly at 330-562-7070. NTI will email you links to the software and a link to request a license activation key.

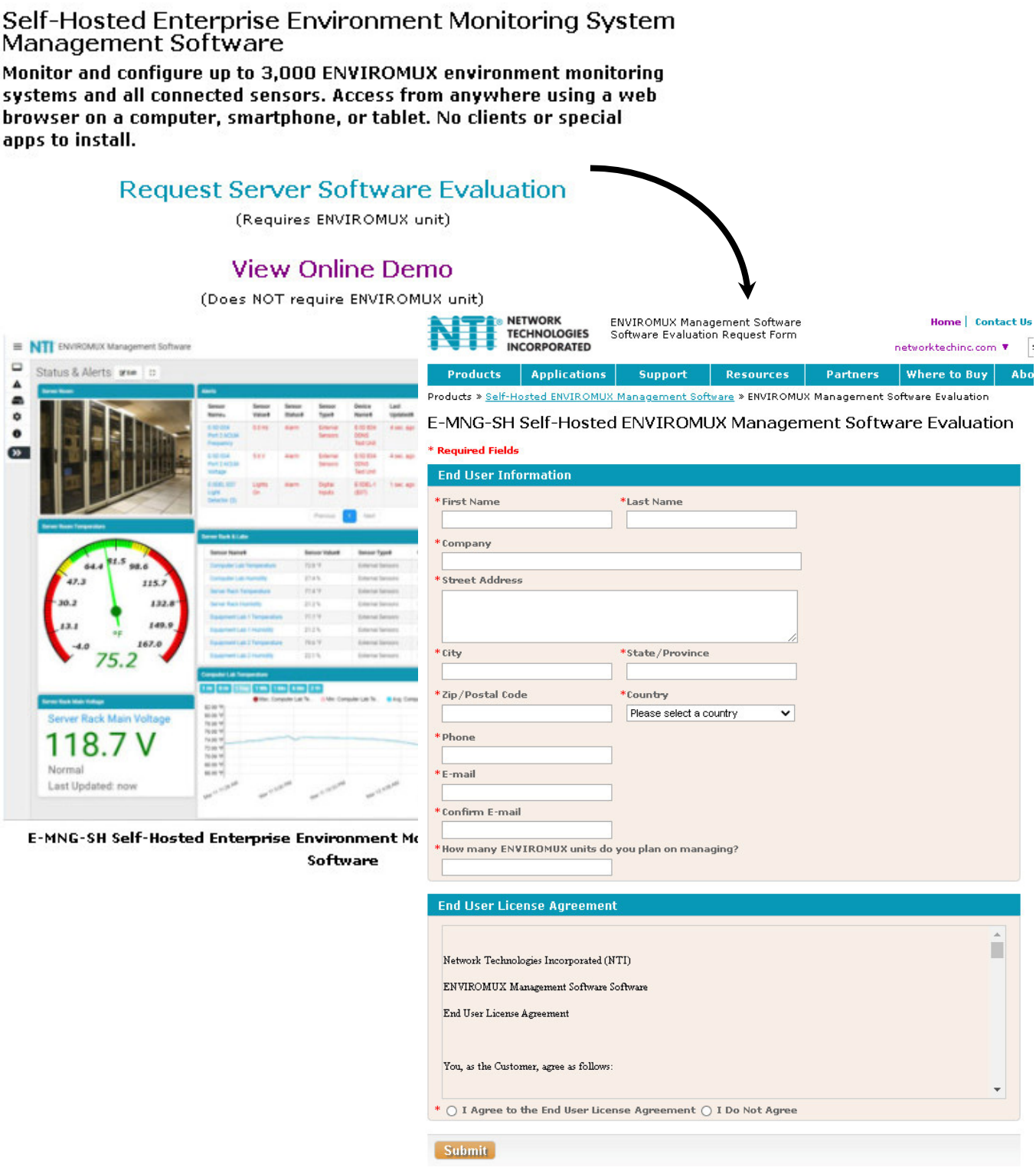


Figure 1- Registration Form

Whether you are evaluating the software, or purchasing it, you will receive an email with links for a download of the software. **NOTE: The download exe files can only be accessed and downloaded once**. Please be sure that you will be able to save the files to a local computer prior to using the links.

The email will also include the serial number for your copy of the software. Be sure to make note of it as you will need to refer to it when you request the license key or if you call for assistance with the software.

INSTALLATION

To install the Software on a Windows-based server or computer, double-click the appropriate version of ENVIROMUX-Management Software-Installer. (No need for Administrator privileges).

- For a 32 bit computer/server install ENVIROMUX-Management-Software-Installer_ Vx.x.x.x **_x86**.exe.
- For a 64 bit computer/server install ENVIROMUX-Management-Software-Installer_Vx.x.x.x **_x64**.exe

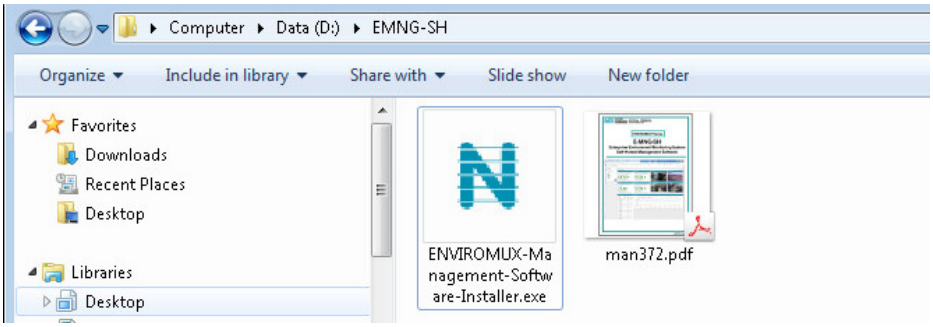


Figure 2- Locate the installation file on your local hard drive

Click to "Agree".

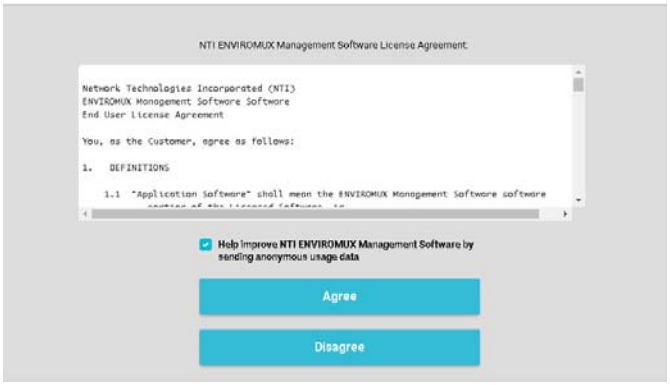


Figure 3- Agree to terms

The email address needs to be a valid email address. The password will be whatever you want to use to access the E-MNG-SH Software. After entering that information, click "Set Admin".

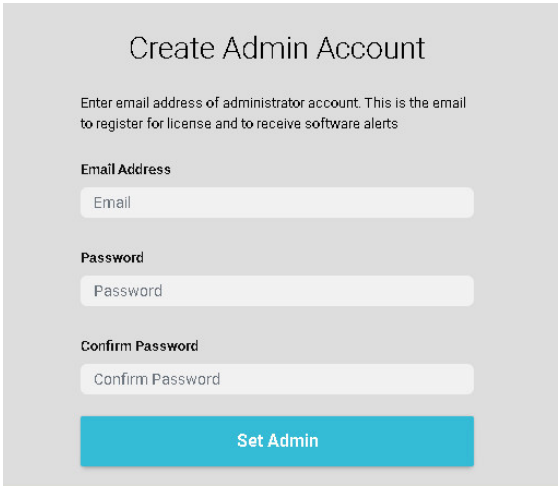


Figure 4- Create Admin login account

You will be prompted for a license key. To request a license key, contact NTI. This key will be unique to this Windows user and installation of the management program. You will need the serial number for the software provided on the email that provided the software download. If you already have a license key enter the license key here and click “Activate License".

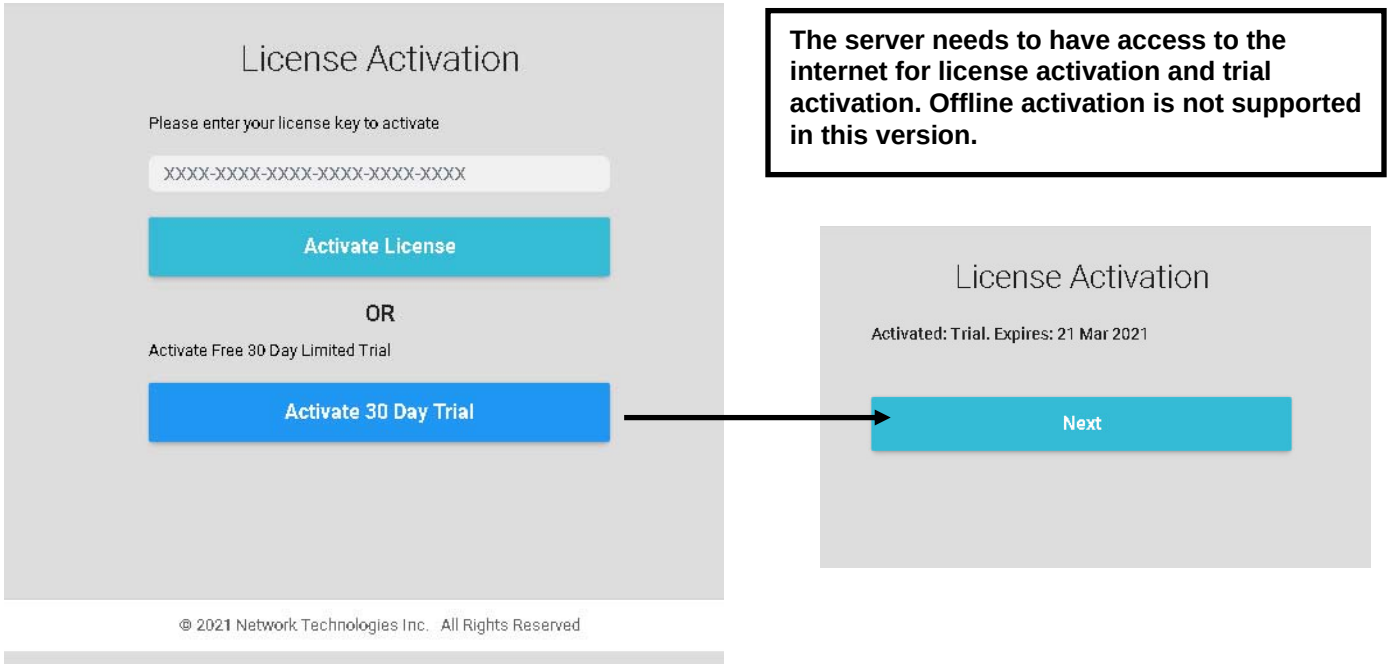


Figure 5- Activation screen

If you choose to just demo the Software at this time, click "Activate 30 Day Trial". You can activate the license later by going to the Settings -> Application Settings page. With a trial activation, the software will be fully functional for 30 days, after which you will need to activate the license to resume operation. None of your settings will be lost.

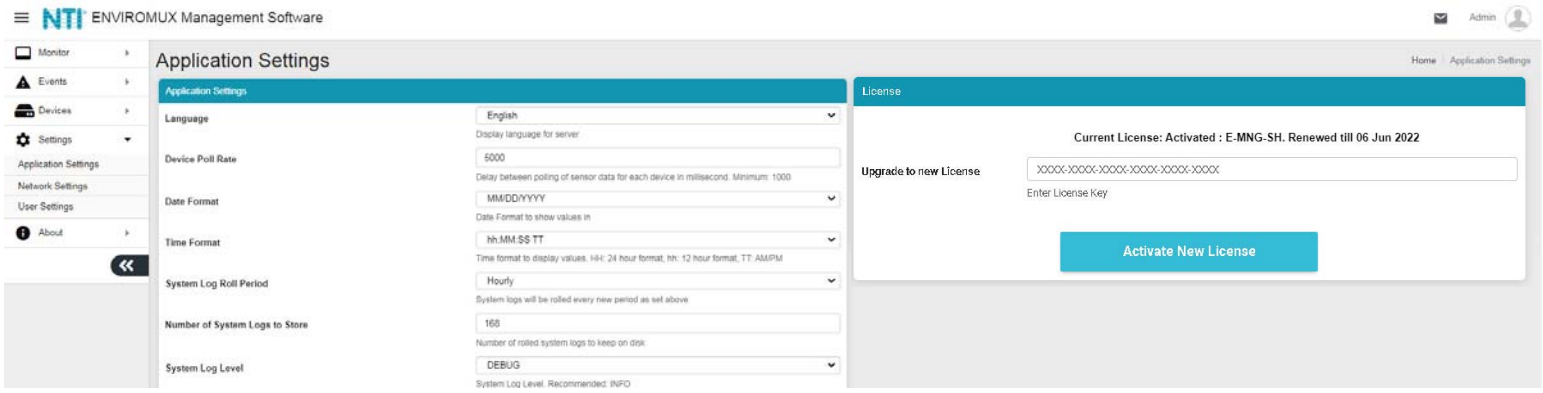


Figure 6- Activate later

Once the software license is activated, the software will auto-renew every 30 days. If the Server is not connected to the internet, the software will continue to function for 30 days after the first attempt to renew it. After 5 days of unsuccessful attempts (once each hour), the following screen will replace the standard License Activation screen. Within the next 25 days you will need to connect the Server to the internet and have it auto-renew or manually click the "**Try License Renewal**" button.

Notifications will be sent to registered users via email when there is only 14 days, 7 days and 2 days left before expiration.

Failure to successfully renew the license will result in the software becoming unusable.

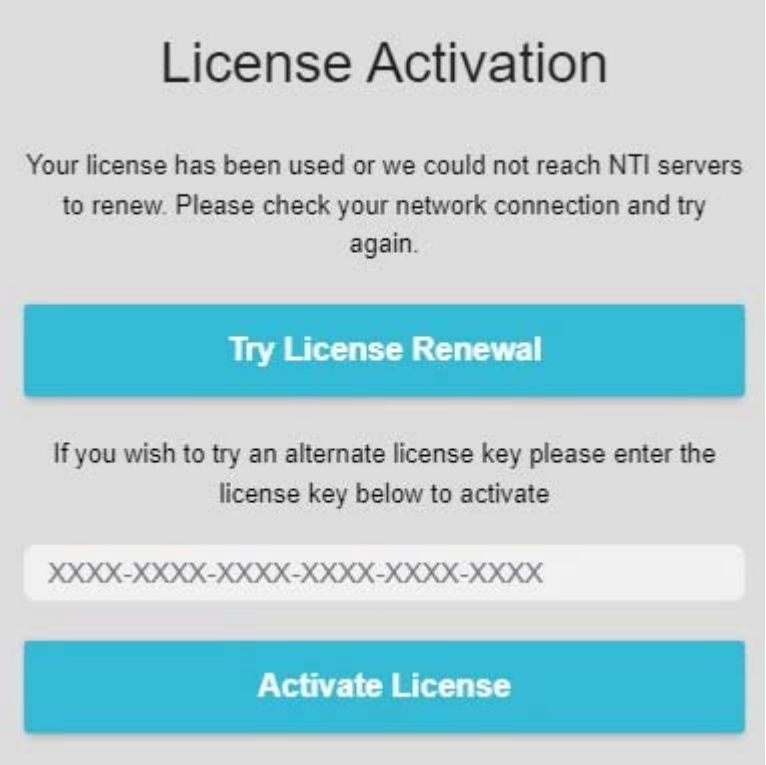


Figure 7-Manually Renew License

Cloning Software

If the Software is installed on a virtual machine (VM) and this VM needs to be cloned to another computer, this can be done and the Software will continue to work with the same activation license, however only one instance of the activated software will function at a time. When you clone a VM like this, Please be sure to shutdown the old software or uninstall it, before the next license renewal. If you continue to run both old and cloned softwares, with the same license, they will interfere with each other and one of them will get locked out.

Once the program is installed, a teal "N" will appear on your desktop and a shortcut on the taskbar. A shortcut will also be added to the “Start Menu”-> All Programs list.

Note: This is a web-based software. The icon is used only for starting the software on a server. Management and monitoring of the software is done through the browser.

Note: Ensure that the server firewall allows TCP port access as set in the application settings (see page 8).

Any computer, smartphone, or tablet with a web browser installed can be used to access the E-MNG-SH software. Access is operating system independent through the HTML5 user interface on the computer/smartphone/tablet’s web browser.

To access the E-MNG-SH, simply enter in the IP address or Server host name of the ENVIROMUX Management System into the URL bar on your browsing computer/smartphone/tablet. If your computer/smartphone/tablet has network access to the E-MNG-SH, you will be presented with the login screen. The server can be configured by anyone with access to it that has administrative privileges.

Users with only "Operator" privileges can assess the E-MNG-SH and view the monitored Devices, but they cannot change any settings. For more on privileges, see page 11.

The Software will open to two empty lists under the Home page. The Home page will display the IP addresses of the Devices being monitored and a list of any alerts associated with sensors being monitored on those Devices.

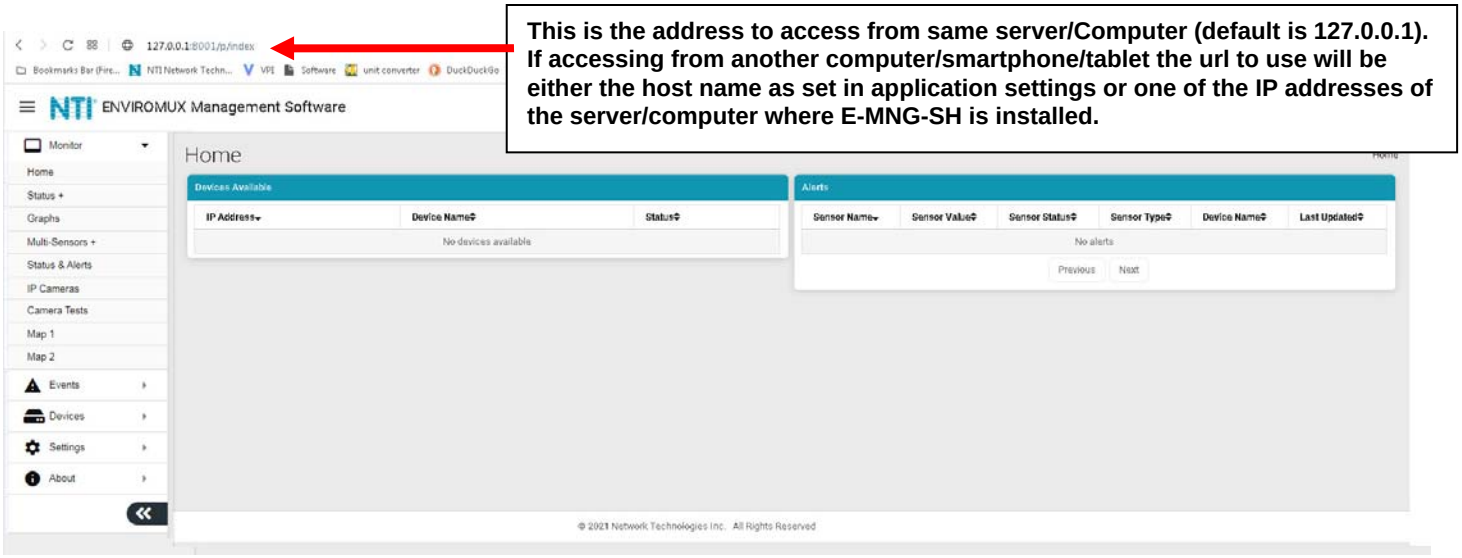


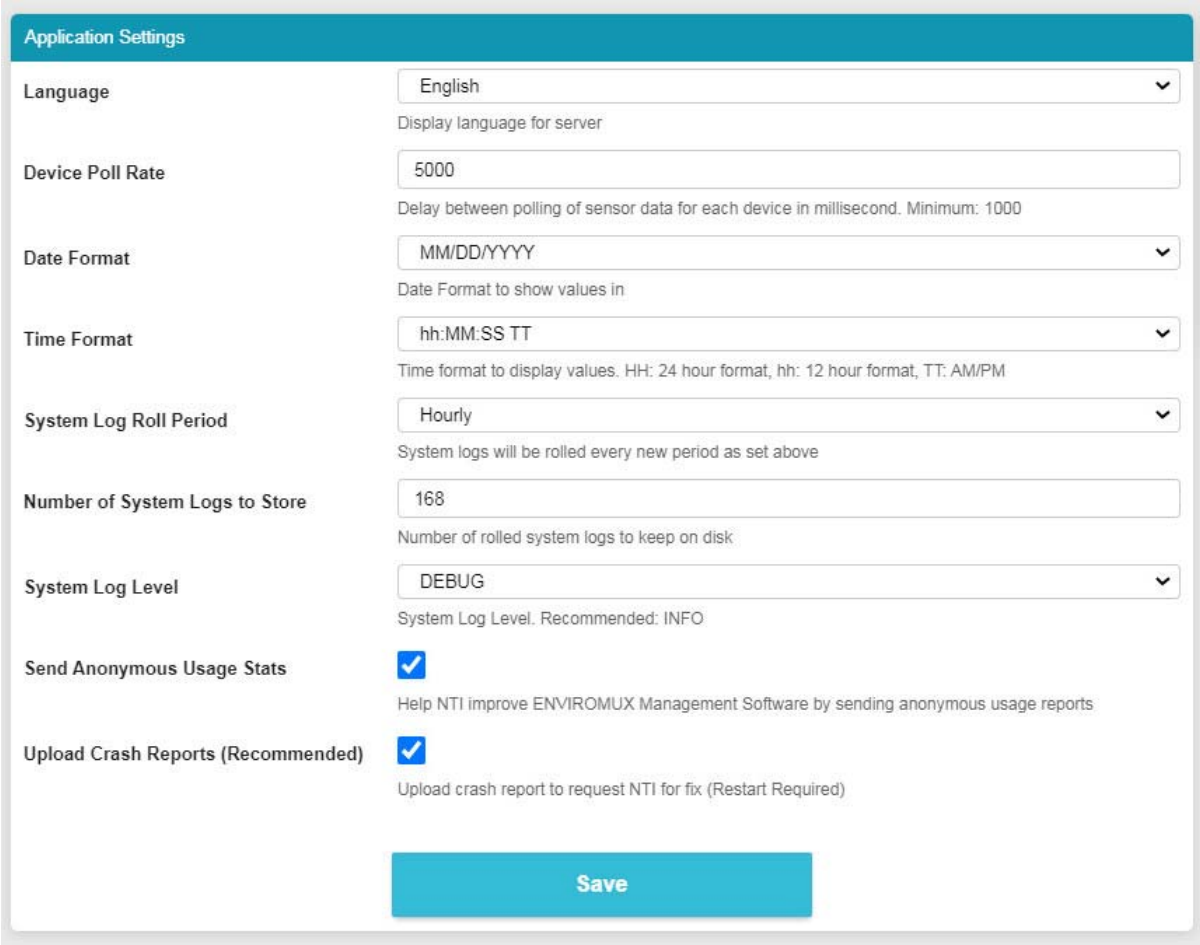
Figure 8- View of the Home screen

To configure the E-MNG-SH to manage your devices and sensors, go to the Settings pages. Under Settings you will find three submenus,

- Applications Settings
- Network Settings
- User Settings

Make sure all of the details for operating the E-MNG-SH are as desired.

Application Settings



Application Setting	Description
Language	Only English is available at this time
Device Poll Rate	Delay time between polling data for each sensor attached to each Device, measured in milliseconds (Min. is 1000)
Date Format	Format of how the date will be displayed in the Software- six to choose from
Time Format	Format of how the time will be displayed in the Software- four to choose from
System Log Roll Period	System Logs will be rolled as often as set here- Hourly, Daily, Weekly, Monthly, Quarterly or Yearly
Number of System Logs to Store	Number of system logs to store on disk- There is no limit.
System Log Level	Select the types of messages that will be logged in the system.log file on Software (see below)
Send Anonymous Usage Stats	Place a checkmark if you approve of sending anonymous usage reports to NTI to help improve this Software
Upload Crash Reports	Place a checkmark in the box to have your Software upload crash reports to NTI and to request a fix. We strongly recommend enabling upload of crash reports. If disabled, NTI will not be able to help with any fixes because of a possible Software crash

System Log Level

- CRITICAL only logs messages that cause Software to exit
- ERROR logs messages with Device, server communication, sensor or user errors including CRITICAL messages
- WARNING will log messages including possible issues with setup or communication including ERROR & CRITICAL
- INFO logs informative messages including WARNING, ERROR & CRITICAL
- FINE logs extra informative messages that logs Device communication including INFO,WARNING, ERROR & CRITICAL
- DEBUG logs all messages which may be too verbose for normal usage but helps with debugging any software issues, including FINE, INFO, WARNING, ERROR & CRITICAL

Don't forget to click "Save" once this is complete.

Network Settings

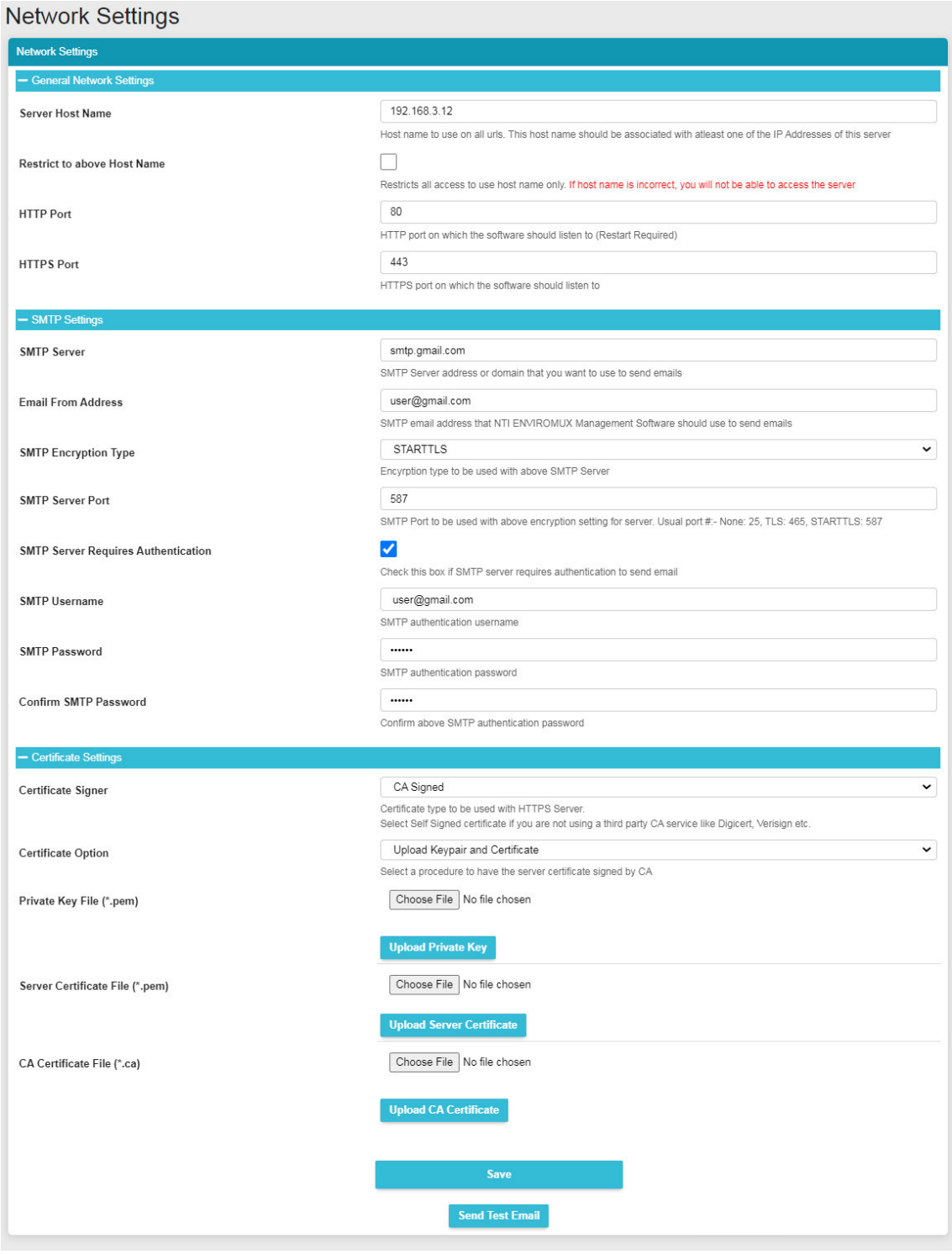


Figure 10- Network Settings

Network Setting	Description
Server Host Name	If you want to access the server with a specific domain name, please set that domain name here **The DB browser can be used to recover from an incorrect host name. (See next page)**
Enable Above Host Name	Enable the Host Name assigned to the Server- restricting access to the Server by using the Host Name only.
HTTP Port	Port on which the Server will be connected with . This is the default HTTP port. If you change this, you will need to add ":<port#>" to the end of the IP address. i.e. If you change it to 85, you will need to enter <IP ADDRESS>:85 in the URL bar to access the Server.
HTTPS Port	HTTPS port on which the Server will be connected with.

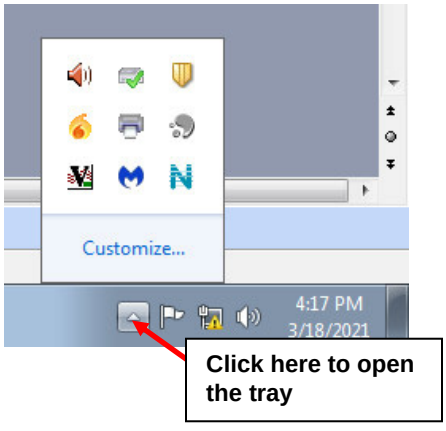
Network Setting	Description
SMTP Server	Enter a valid SMTP server address
Email From Address	Enter email "From" address to be used by E-MNG-SH to send messages from
SMTP Encryption Type	Choose encryption type from dropdown menu: STARTTLS, TLS or None
SMTP Server Port	Enter port used by SMTP Server (default is 587)
SMTP Server Requires Authentication	Place a checkmark in here if the SMTP Server requires authentication to send messages
SMTP Username	Enter the SMTP Username for the E-MNG-SH-if encryption is checked
SMTP Password	Enter the SMTP Password for the E-MNG-SH- if encryption is checked
Confirm SMTP Password	Re-enter the SMTP Password for the E-MNG-SH
Certificate signer	Certificate type to be used with HTTPS Server. Select self-signed certificate if you are not using a third party CA service like Digicert, Verisign, etc.
Certificate Option	Select a procedure to have the server certificate signed by CA
Private Key File	Choose and upload a private key file in *.pem format.
Server Certificate File	Choose a server certificate and upload in *.pem format
CA Certificate File	Choose and upload a CA Certificate file in *.ca / *.crt format.

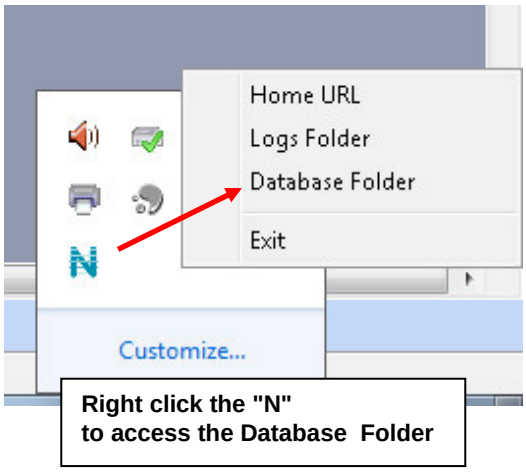
Don't forget to click "Save" once this is complete. You can test your settings by clicking "Send Test Email". An email will be sent to any configured users.

Server Host Name

If you want to access E-MNG-SH with a specific domain name, please set that host + domain name (also referred to as FQDN (Fully Qualified Domain Name)) here (for example "monitor.enviromux.com"). This FQDN should be associated with at least one of the IP Addresses of this server or computer. In the event the FQDN set is incorrect and access is restricted to this FQDN (as set in "Enable Above Host Name"), you would not be able to login to E-MNG-SH. In this case you can correct the FQDN by following the below procedure.

1. Access the server or computer where E-MNG-SH is installed. Open the database folder and locate the "settings.db" file. (You can right click on the E-MNG-SH icon (teal colored "N") in the system tray to access the database folder.)





2. Exit E-MNG-SH software now
3. Open "settings.db" with any SQLite editor like DB Browser or DBeaver
4. Set the desired FQDN in "HOST_NAME" column of "EMANAGER_SETTINGS" table
5. Save these changes and close the file. Restart E-MNG-SH now and you should be able to login with a correct host name.

User Settings

There is a limit of 1000 users that can be configured to access the E-MNG-SH. To add users, go to Settings -> User Settings . Enter the first and last name, email address and password for that user to use to access the E-MNG-SH.

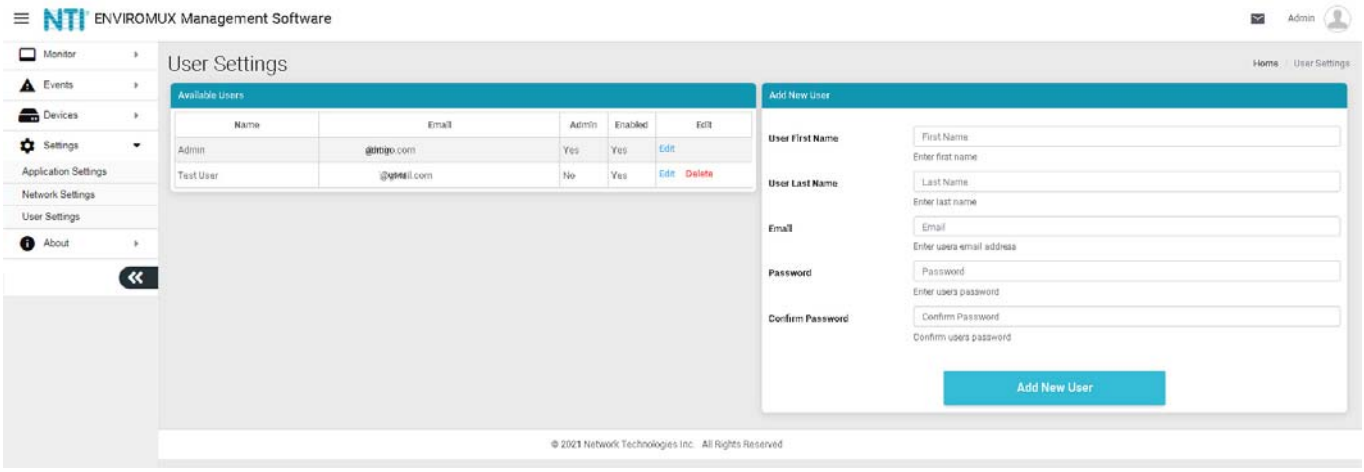


Figure 11- User Settings for Adding Users

Once a user has been established, click on "Edit" in the "Available Users" window to bring up the Edit User page and add additional information. You can also, instead, click on "Delete' to remove the user altogether.

First decide what access level this user will have:

Super Admin- This user cannot be deleted and is the same user used in license registration and managing the E-MNG-SH.
Admin - User has administrative privileges to make changes to the configuration of the E-MNG-SH
Operator- User only has access to the information provided on the E-MNG-SH. No changes can be made.
Read Only- User can see everything the E-MNG-SH has to offer, but cannot change any settings or add anything.

Note: Only Admin users can edit other user's passwords, the Operator users can edit their own password only

Be sure to check the "User Enable" block to give the listed user access to the E-MNG-SH.

Place a checkmark in "Sound Alerts" to enable the user to hear audible warnings about an alert being sensed while the user is monitoring a Dashboard.

Place a checkmark in "Enable Alerts" so the user can receive emails about sensor alerts or reports generated (page 30).

The Title, Department and Company are optional information that can be provided for reference.

On this page the user's password can also be changed. After entering, click "Set New Password".

When finished, be sure to click "Save User".

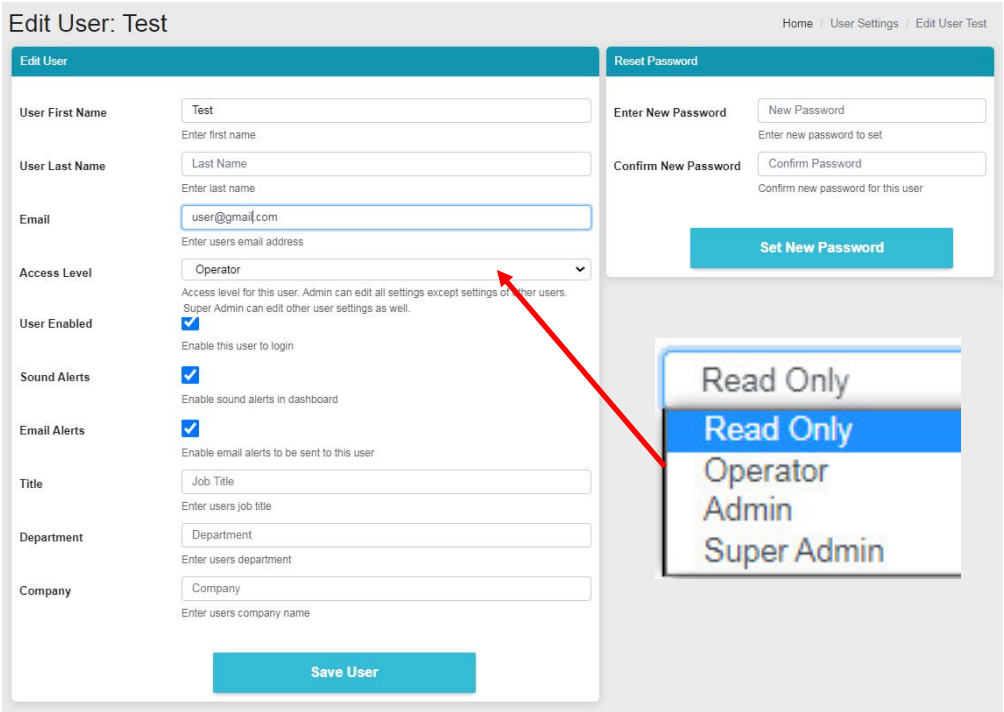


Figure 12- Edit user settings

DEVICES

Under Devices, in the menu, there are four options to select.

- Device Settings
- Sensor Settings
- Add or Remove Device
- Maps

The Device Settings page displays all the Devices you have configured to be monitored and the groups you have established for the management of those Devices. You can click on the IP Address of each to view status and adjust settings of each sensor in each device.

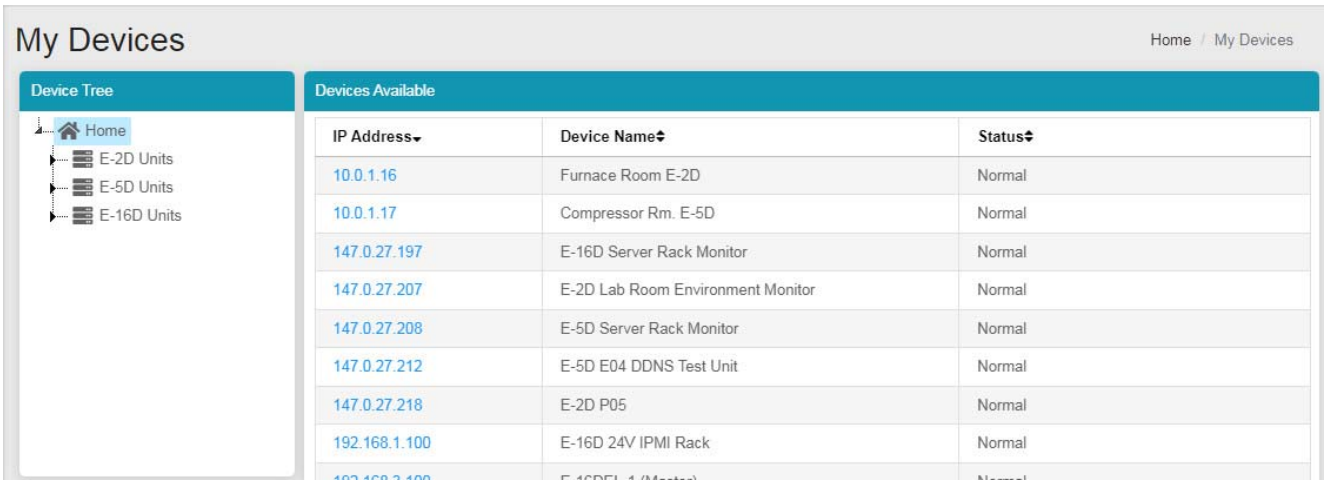


Figure 13- My Devices List

Next, under Sensor Settings, you have a "My Sensors" list of all sensors, IP addresses and cameras connected to the Devices being monitored.

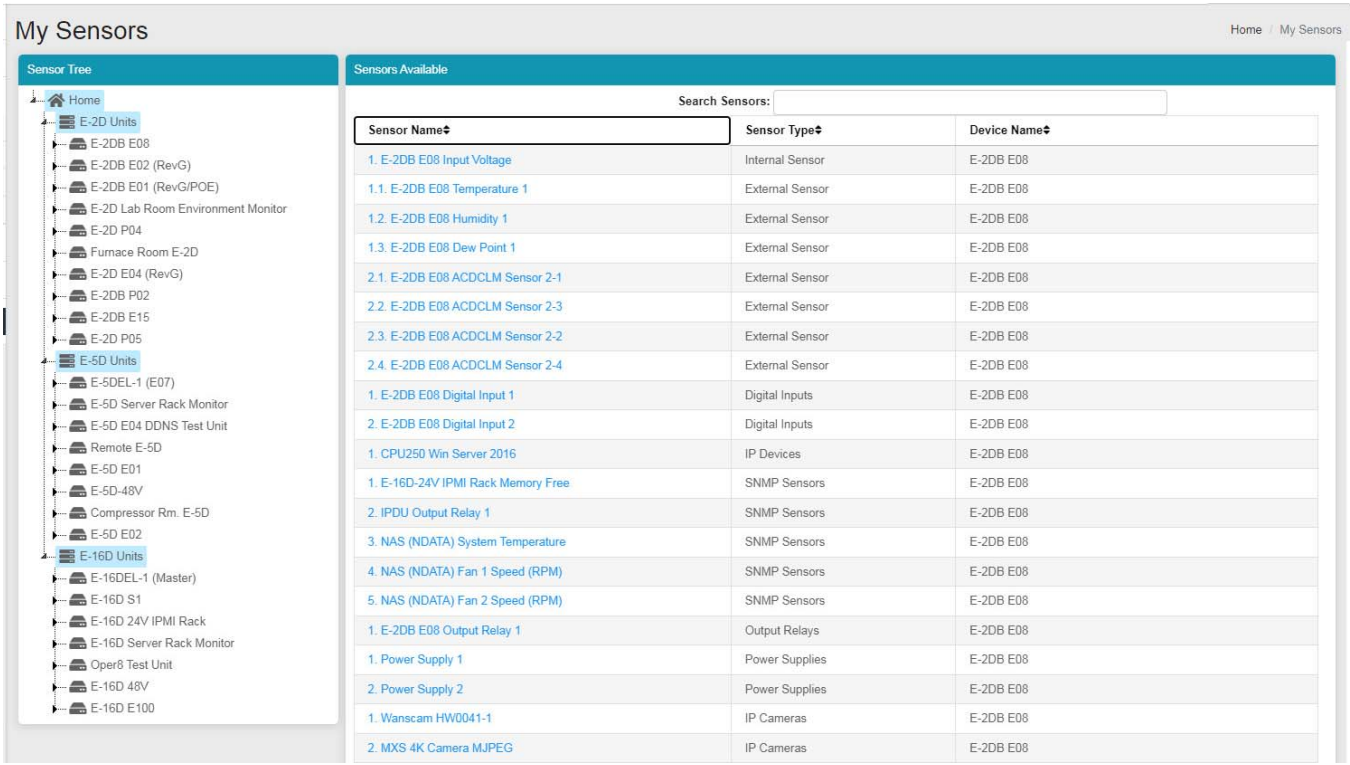


Figure 14- My Sensors List

Next is the “Add Or Remove Devices” page for adding more Devices to be monitored and adding groups to put the Devices into. Groups makes it easier to manage how the sensors and Devices will be monitored. From this page they can also quickly be removed from the list.

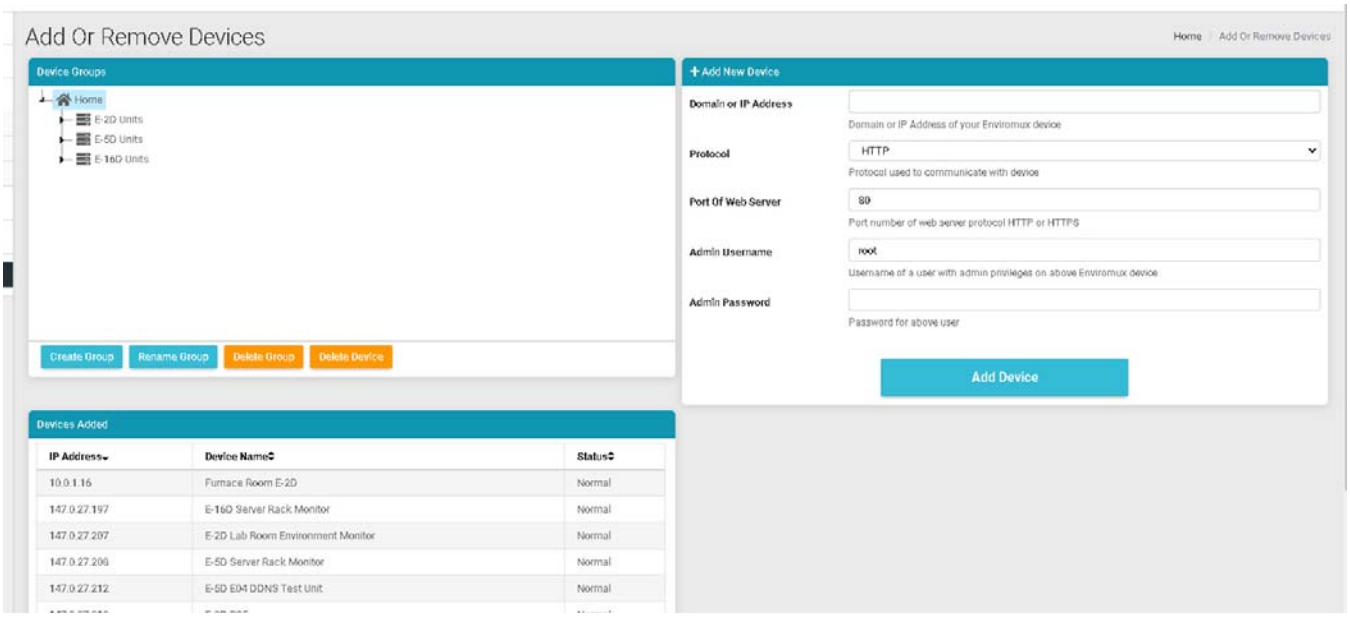


Figure 15- Add or Remove Devices

Lastly, use the “Maps” page to upload an unlimited number of images of a map, building, or server room (examples). Images must be .jpg or .png format, with a maximum size of 20MB (any resolution). On these images you can place markers for Places, Devices, or individual Sensors that you want to easily monitor the status of. Many map images are pre-loaded for you to choose from.

1. To setup a map, first select either “Floorplan” from the Map Type dropdown, or select a specific location from the pre-loaded maps. If you select “Floorplan”, you will have the option to load a custom image. Locate the image file to be uploaded (must be .jpg or .png format). Then click "Upload".

2. Once uploaded, you can click on the map to have it enlarge in the viewing window.

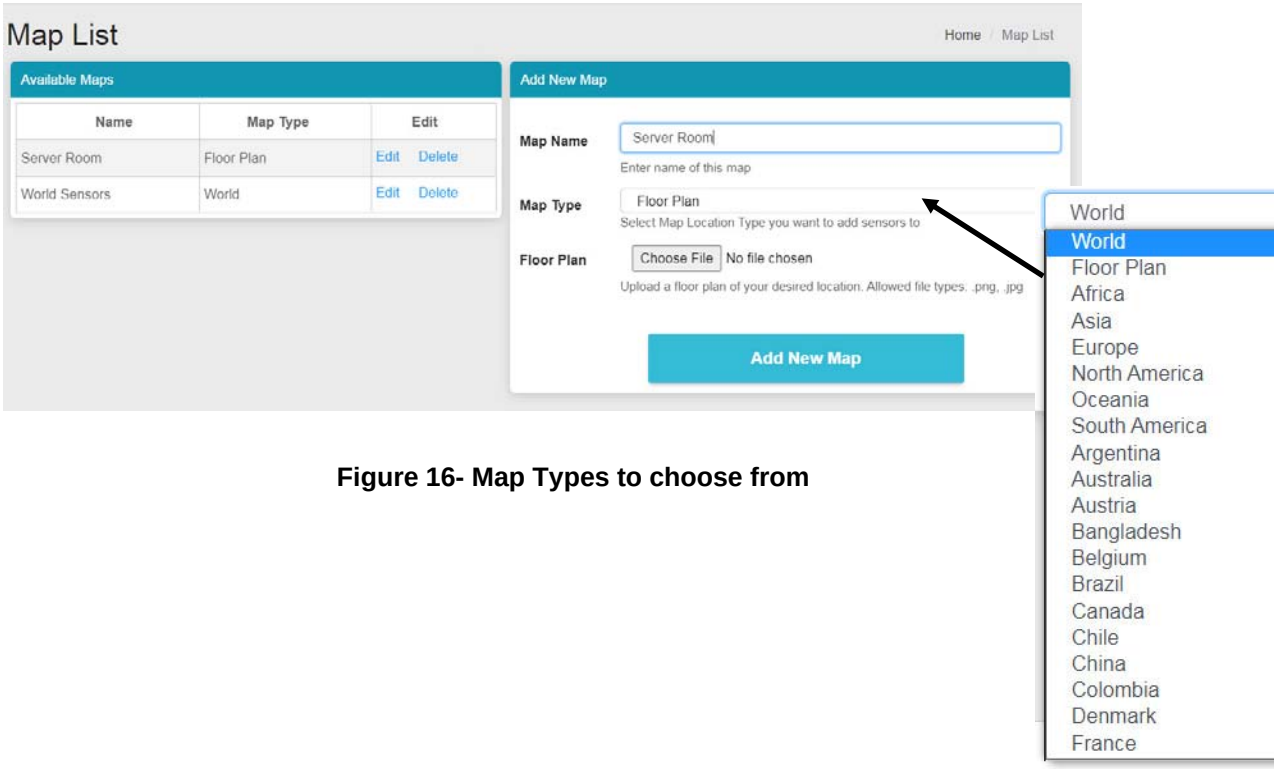
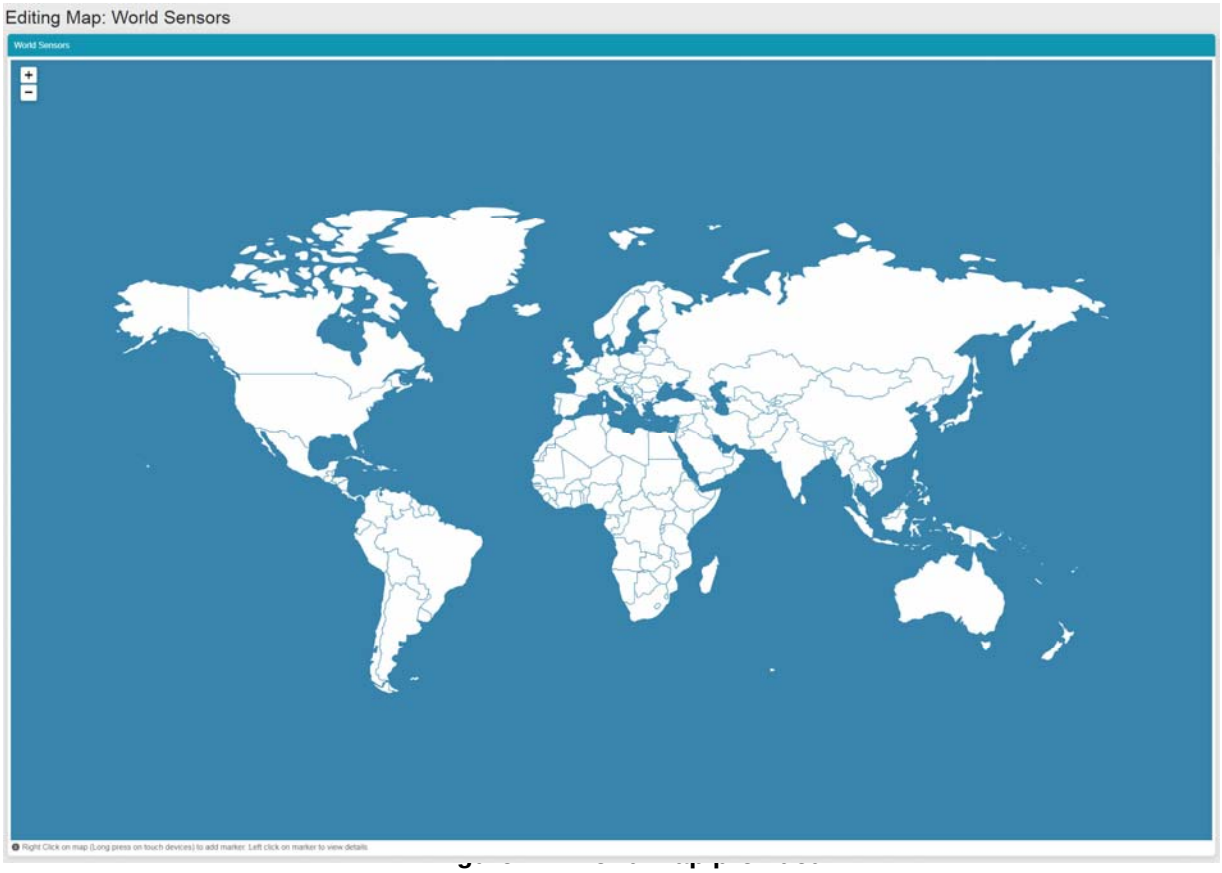


Figure 16- Map Types to choose from



3. Right click anywhere in the image to add a marker. A prompt for “Add Marker” will display. Click on that to bring up a list of sensors to be monitored in a Place, from a Device, or individual sensors.

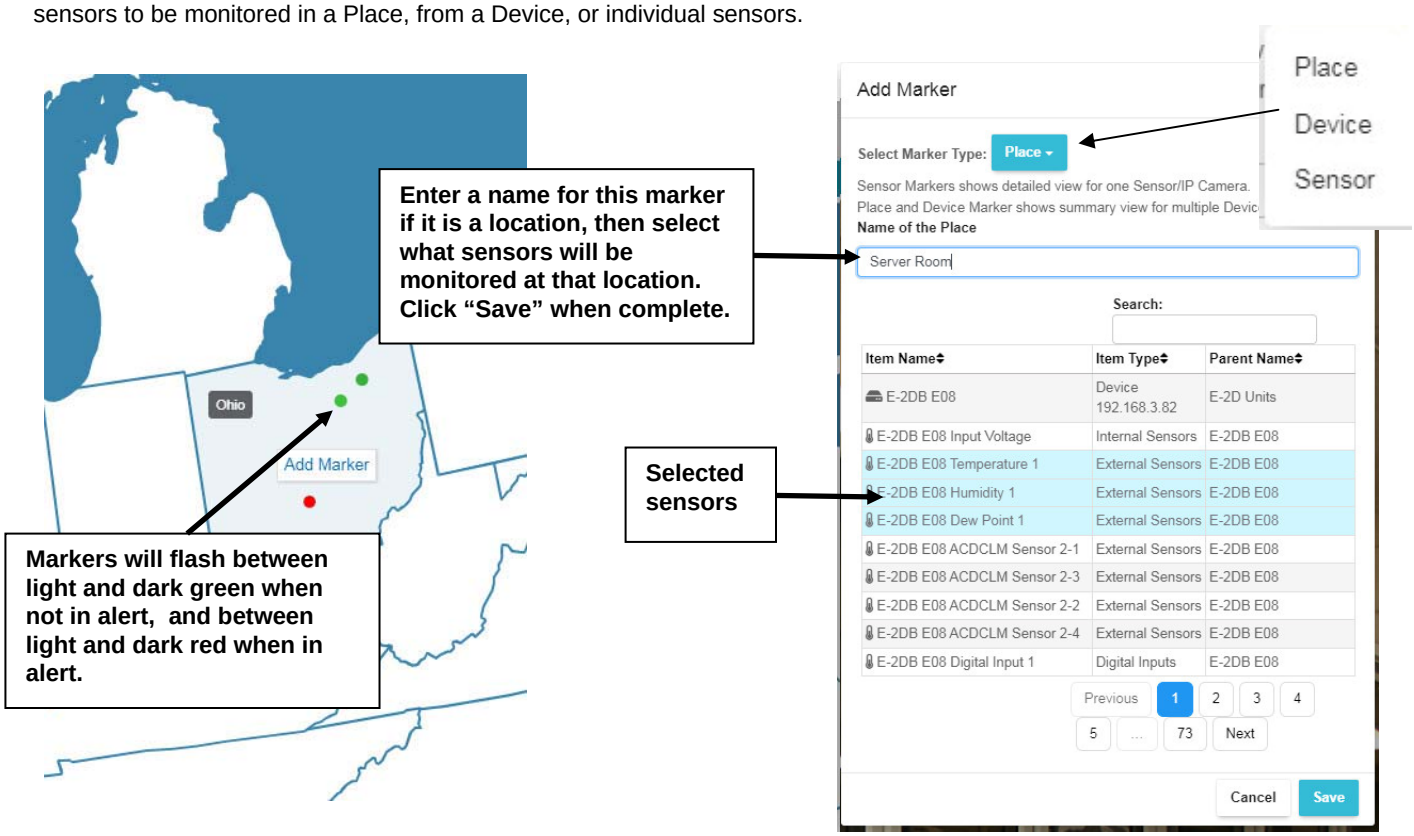


Figure 18- Loading maps and placing markers

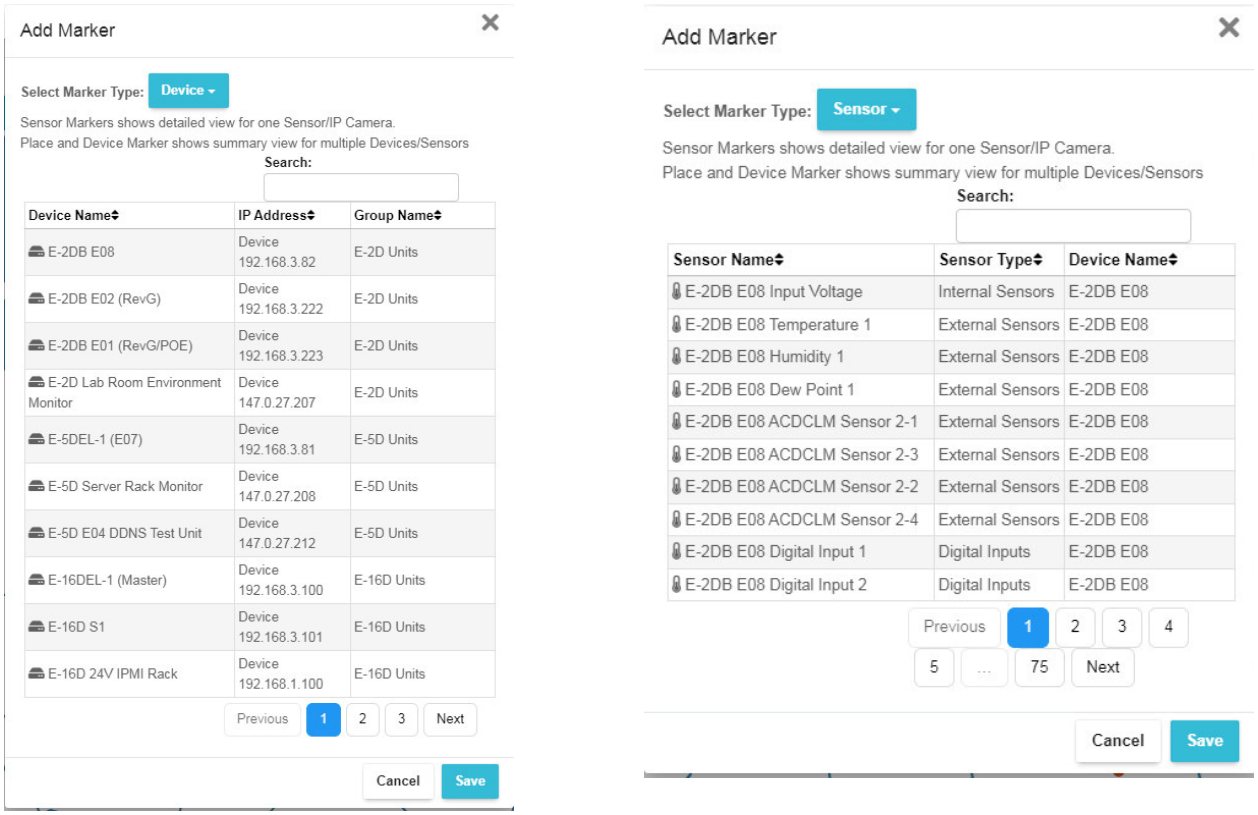


Figure 19- Markers for Device or Sensor

With your maps and markers defined, you can create a Dashboard and add your map to it (see page 24) .

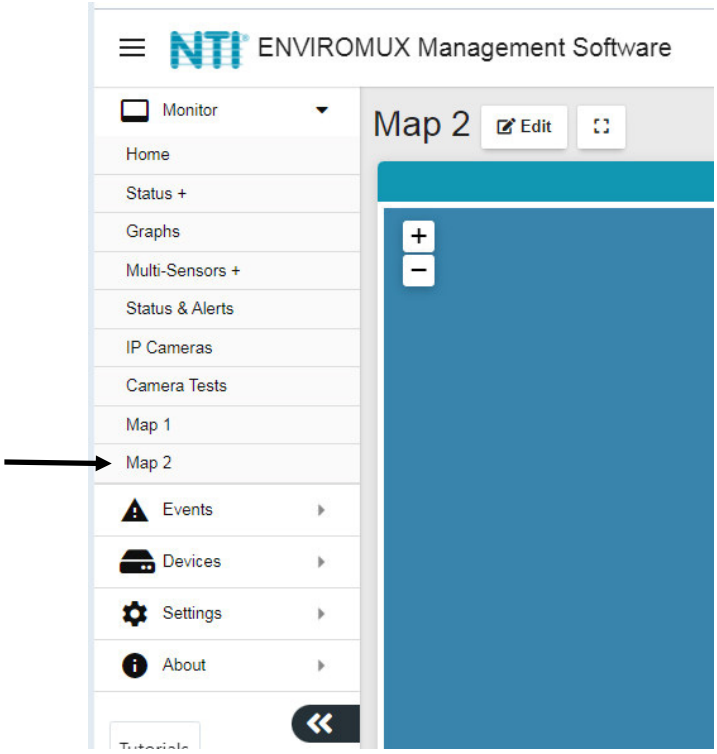


Figure 20- Use a configured map to monitor select sensors

With the map on the screen, click on any marker and the sensor or sensors associated with the Location/Device will be displayed and the status of those sensors will be indicated.

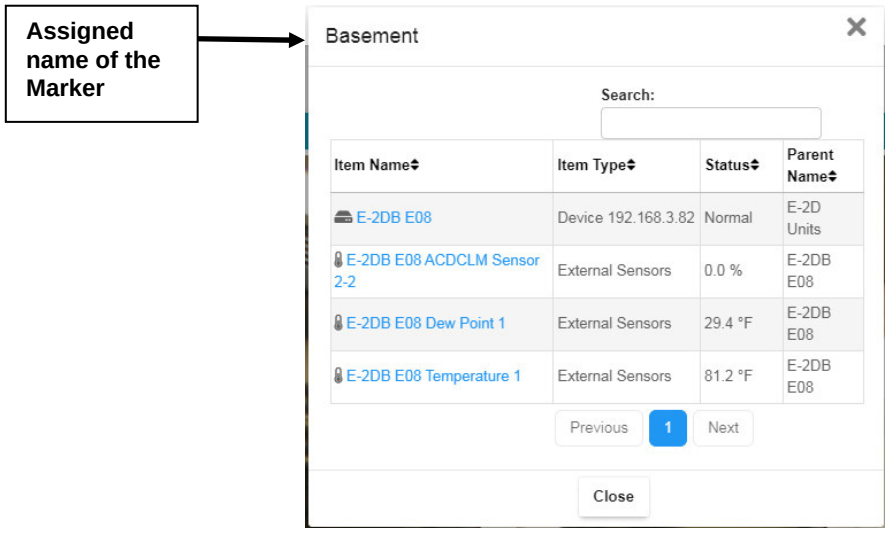


Figure 21- Sensor status at location "Basement"

Devices to Monitor

Before adding a Device, select the group under which the Device needs to be added. If no selection is made the Device will be added to the “Home” group.

To add a Device, click on "Devices"-> "Add or Remove Device" in the side menu. A window will open as shown on the next page.

Enter 1) the Domain or IP address for the Device,

2) the connection protocol (HTTP or HTTPS),

3) the server port number (usually 80 for HTTP and 443 for HTTPS)

4) any user with admin privileges on the E-xD can be used

5) the user with admin privileges password

6) press “Add Device”.

If the IP address is valid, the message "Connecting to Device" will be followed by "Device added successfully" and the Device will appear in the Devices Added list. The sensors attached to that Device will be sensed and added to the "My Sensors" page.

If the IP address or Domain is not valid or accessible, the message “**Error 913: Connection Timeout**” will be displayed.

TIP: If you don’t know the IP addresses of the Devices to be monitored, you can use the included NTI Discovery Tool (page 20) to identify them (provided they are all connected to the same LAN).

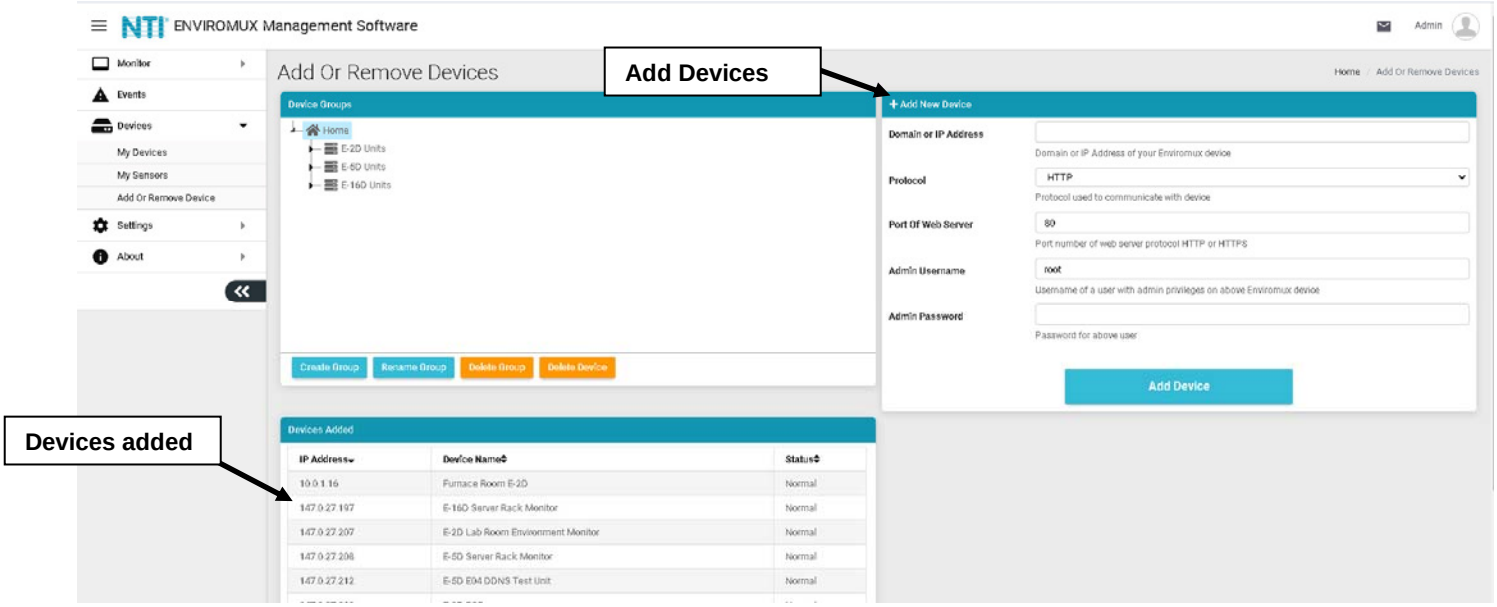


Figure 22- Add Devices to monitor

Continue adding until all Devices to be monitored are listed.

Groups

Groups can be used to organize your Devices as viewed on the Dashboard.

The name of the default group "Home" can be changed. Below it has been changed to "Server Room". Click the name, click on "Rename Group", and enter the new name. Press Enter key to save.

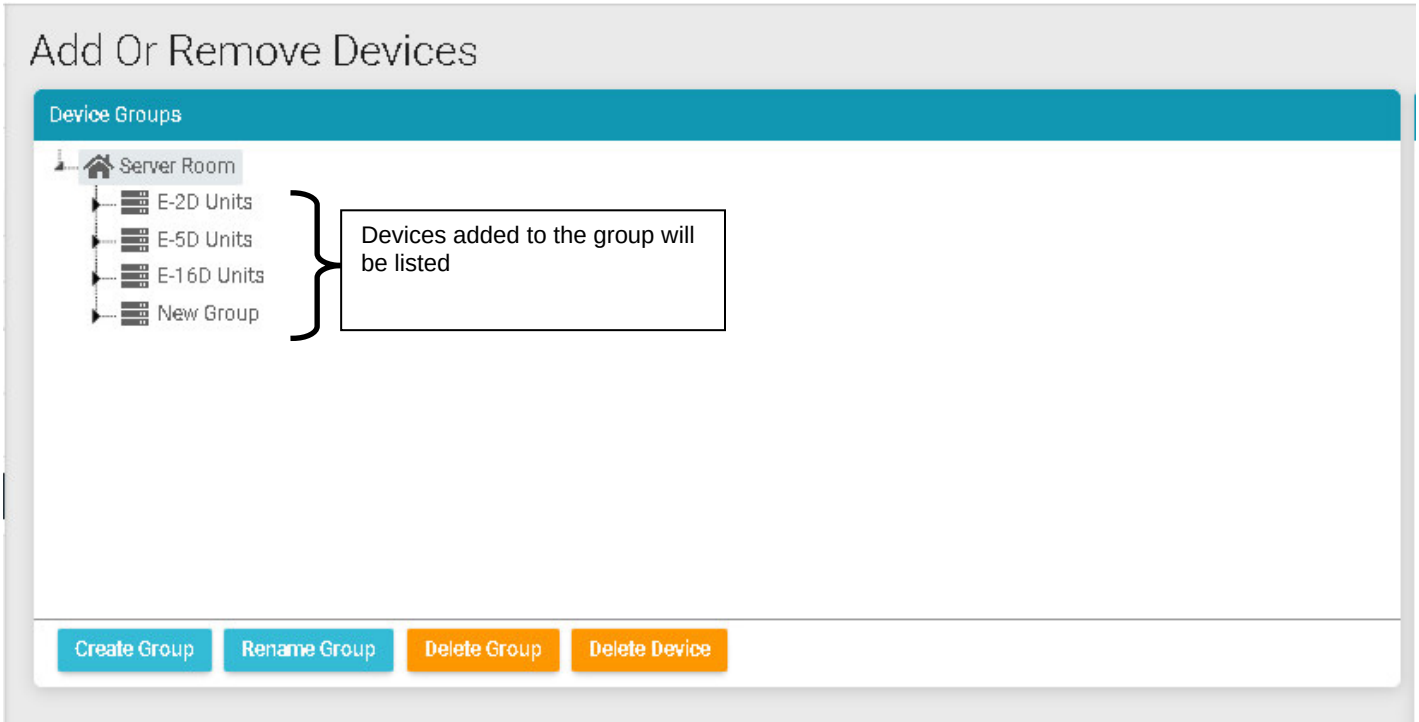


Figure 23- Primary group, and New Group added

Click "Create Group" to add an additional group. While the “New Group” name is selected (highlighted) , any Device that is entered will fall under that group.

To remove a group, while the group to be removed is selected (highlighted), click "Delete Group".

To move a Device from one group to another group, first select the Device in the group to remove it from, then click "Delete Device".

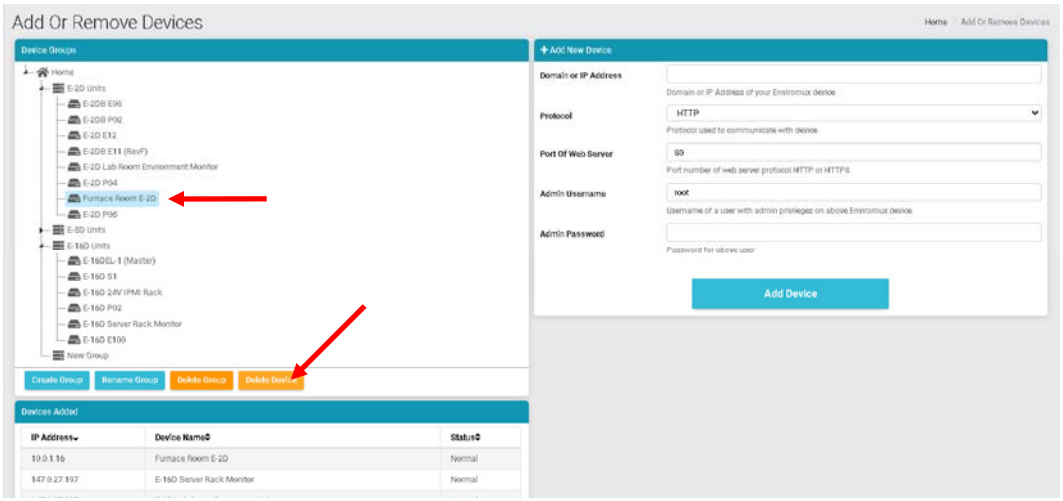


Figure 24- Select Device to delete

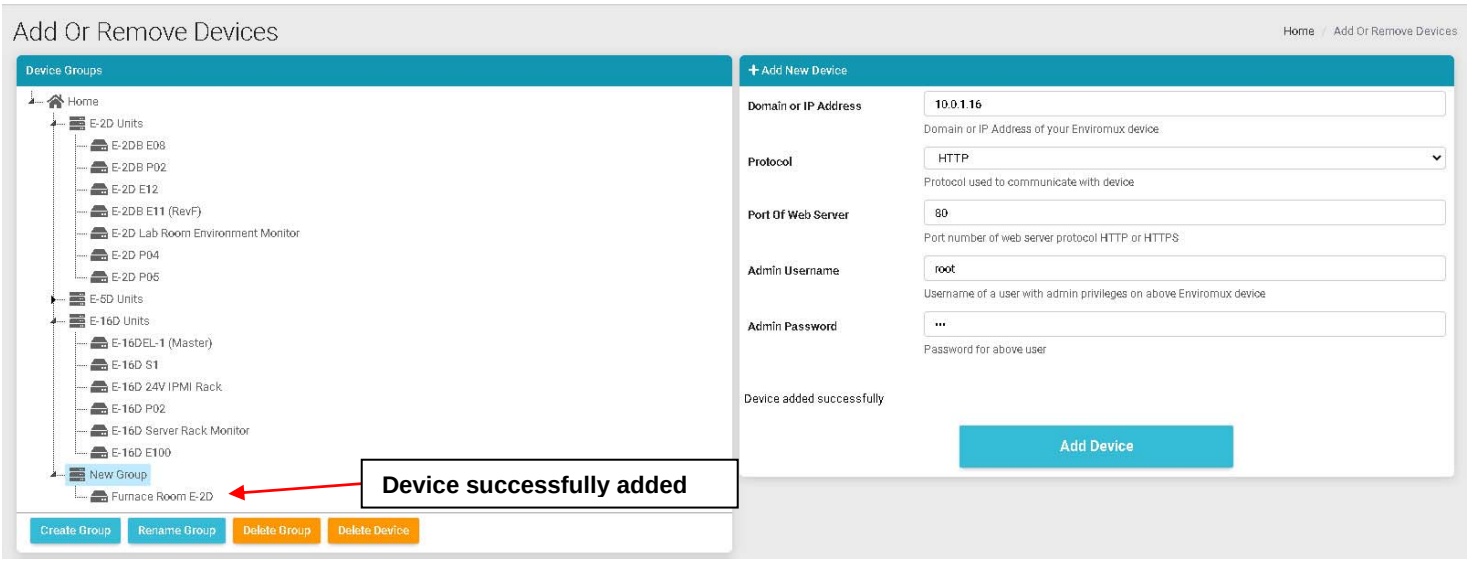


Figure 25- Device moved/added to New Group

Now select the new group name to add it to (above it is "New Group"), and re-enter the IP address and additional information. Click "Add Device". If successful, the message "Device added successfully" will appear and the Device will be listed under the new group name.

If you do not know the IP address of the Device you want to add, you can use the included NTI Discovery Tool (page 20) to identify them (provided they are all connected to the same LAN).

To reload the configuration for a Device, rename the Device or delete the Device, you can right-click the Device in the list from the Add Or Remove Devices menu.

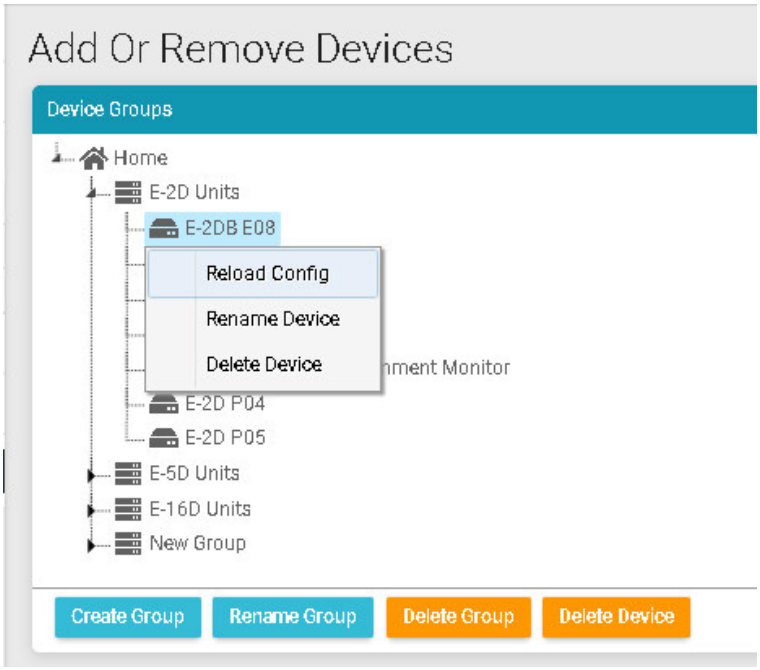


Figure 26- Additional features from Add Devices menu

The user can access and change configuration settings for a Device by going to the My Devices menu, double-clicking the Group, and then the Device. Accessing the Device this way will open up the list of configuration options for the Device.

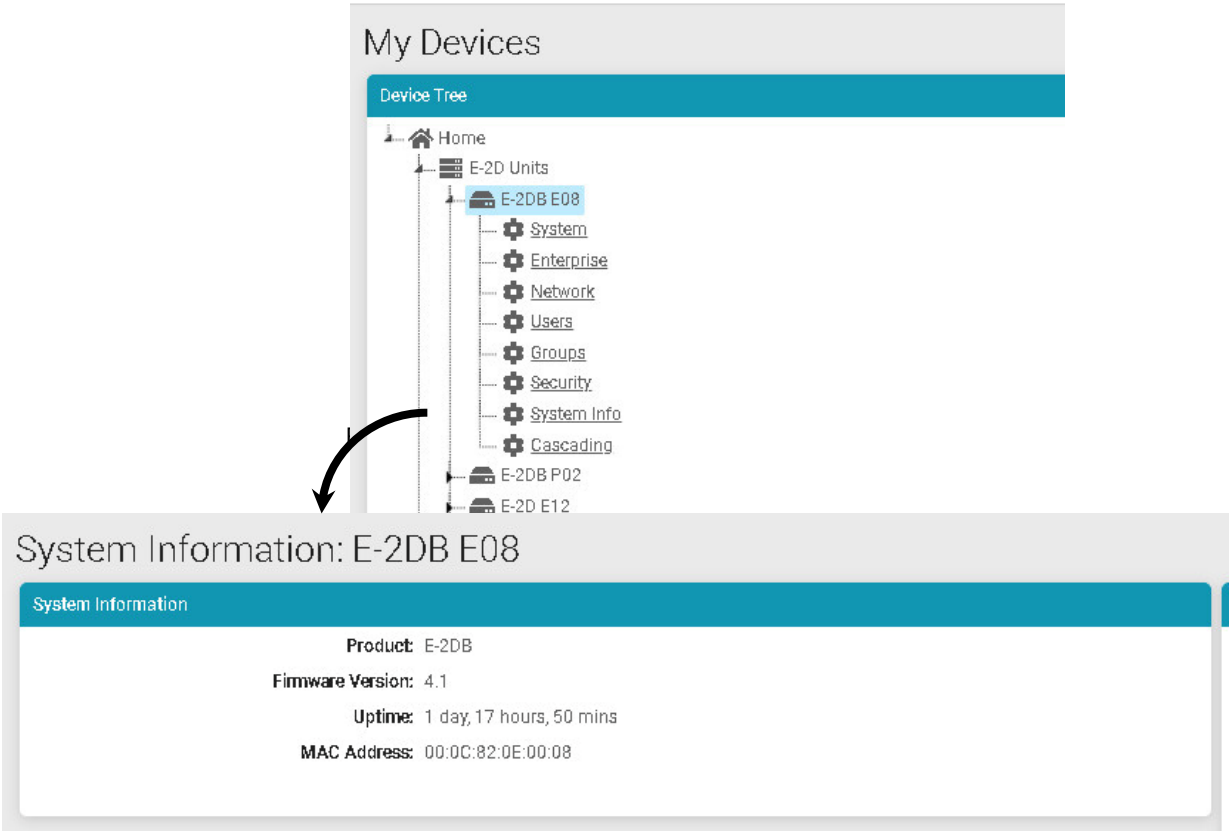


Figure 28- System Info page for the Device

Device Discovery Tool

In order to easily locate the Device on a network, the NTI Device Discovery Tool may be used. The Discovery Tool is available on many of our webpages, including http://www.networktechinc.com/download/d-environment-monitor-16.html. Download the discovery.zip, extract the contents to your PC and click on the file *NTIdiscover.jar* . This will open your browser and display the Device Discovery Tool page.

Note: The Device Discovery Tool requires the Java Runtime Environment to operate.

Note: The computer using the Device Discovery Tool and the ENVIROMUX must be connected to the same physical network in order for the Device Discovery Tool to work.

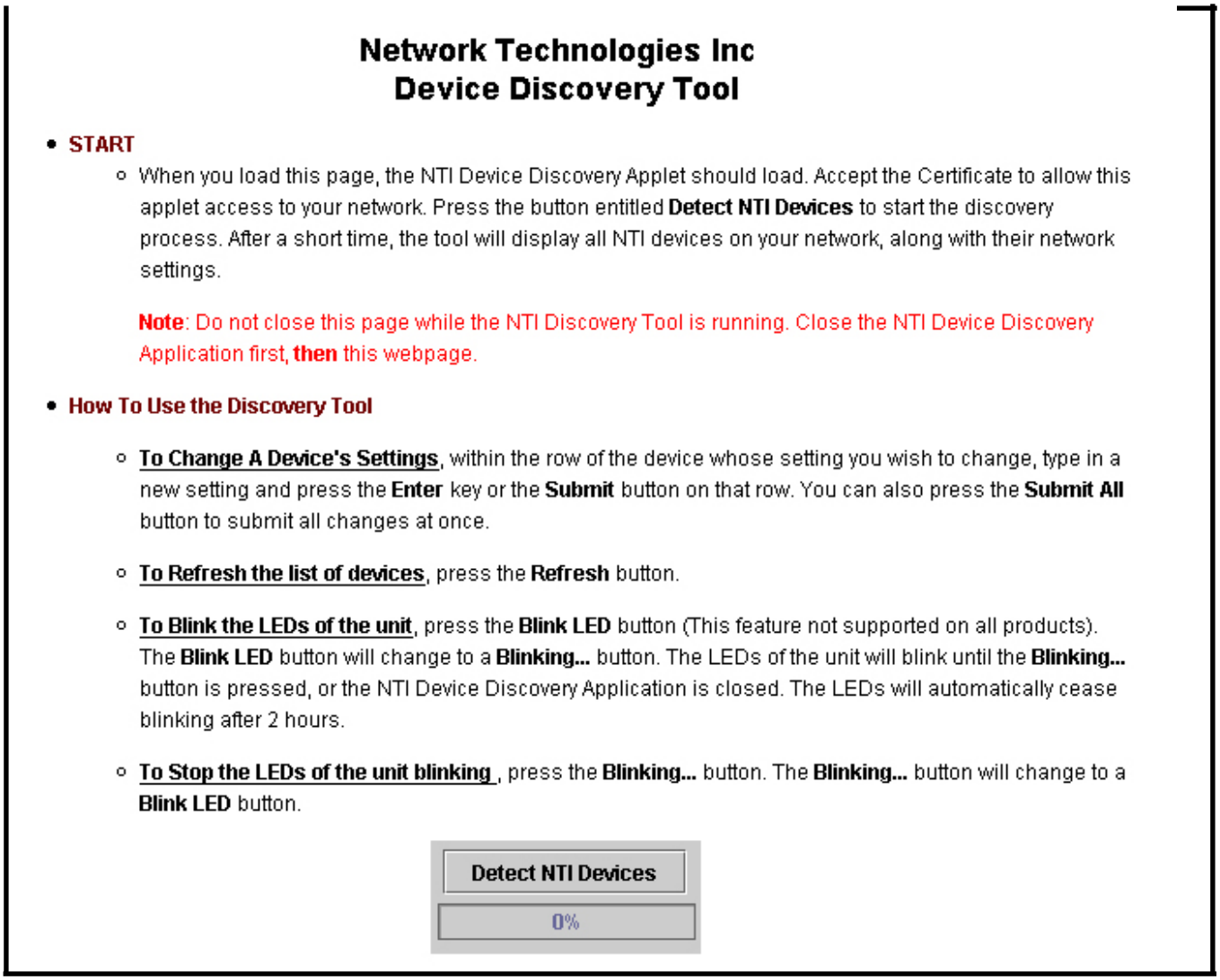
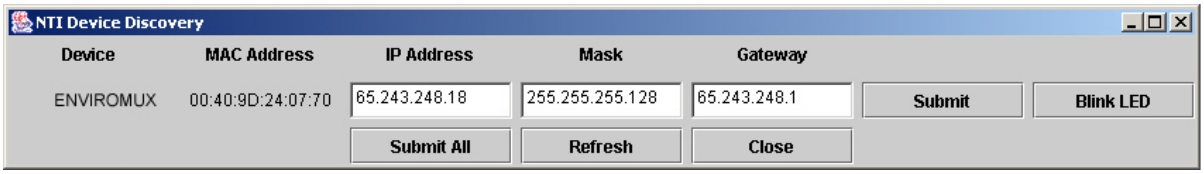


Figure 29- Device Discovery Tool page

Use the Device Discovery Tool to display all NTI ENVIROMUX Devices on the network, along with their network settings. Follow the instructions on the Device Discovery Tool page to use the tool and to change the Device settings if so desired.



VIEW SENSORS INDIVIDUALLY

With Devices added, you can now view the sensors connected to those Devices. Select My Sensors from the side menu.

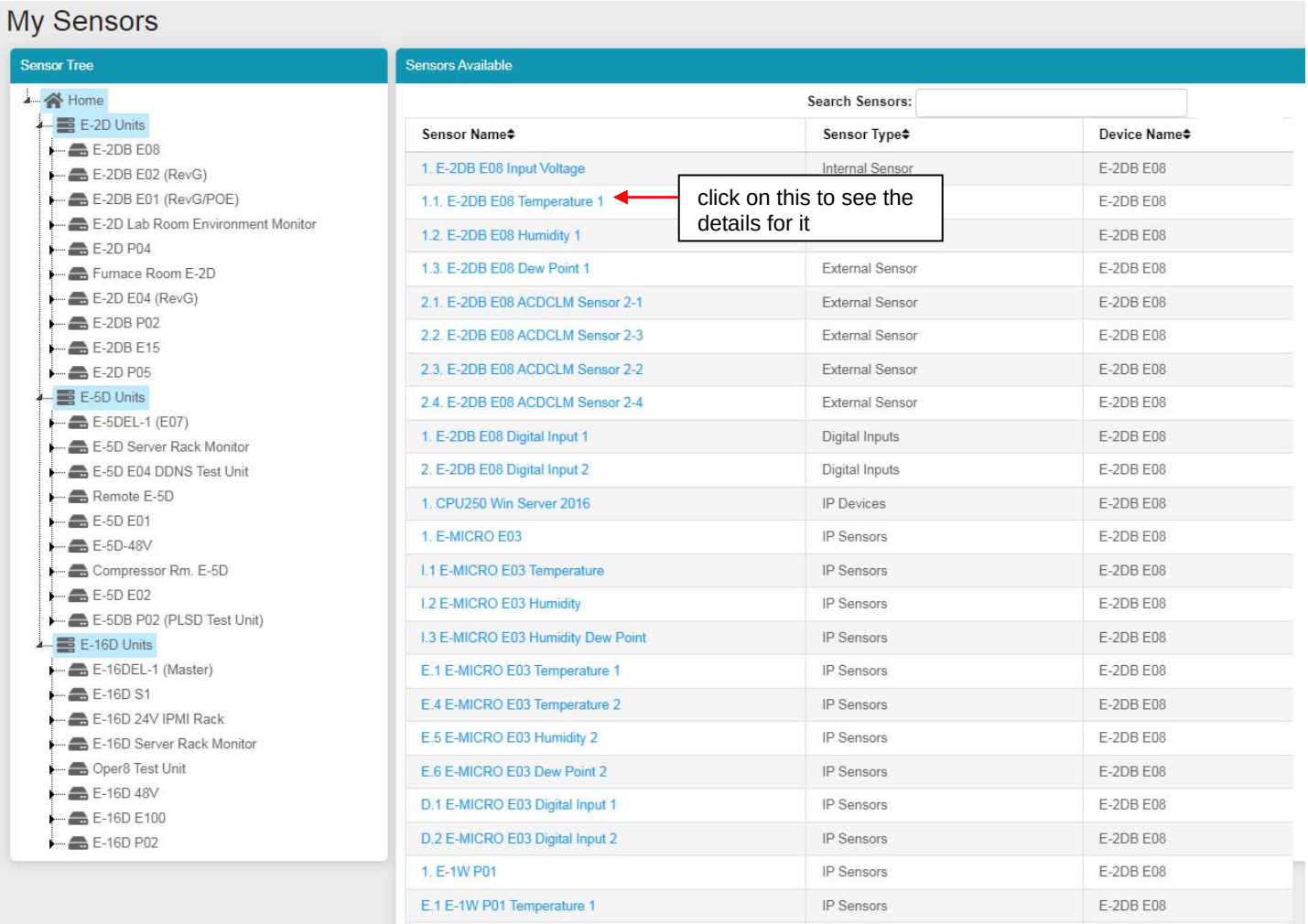


Figure 30- Sensors being monitored

The initial list will be all of the sensors, cameras, remote IP Devices and IP Sensors (E-MICRO-TRH(P) and E-1W(P)) that are attached to the Devices and are now being monitored by the E-MNG-SH. To see the details for a specific sensor in that list, click on the blue text for the Sensor Name.

Sensor values, a historical graph, and all settings for that sensor can be viewed. Settings can also be changed if desired.

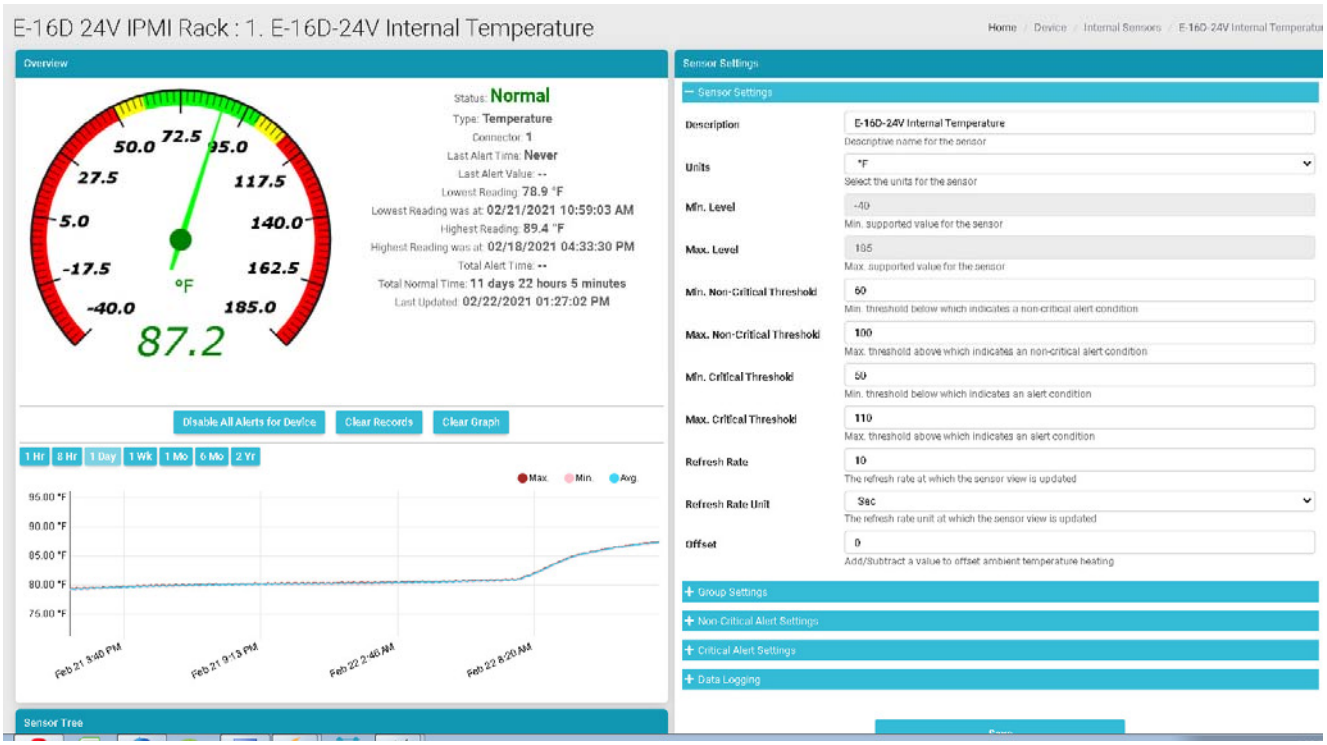
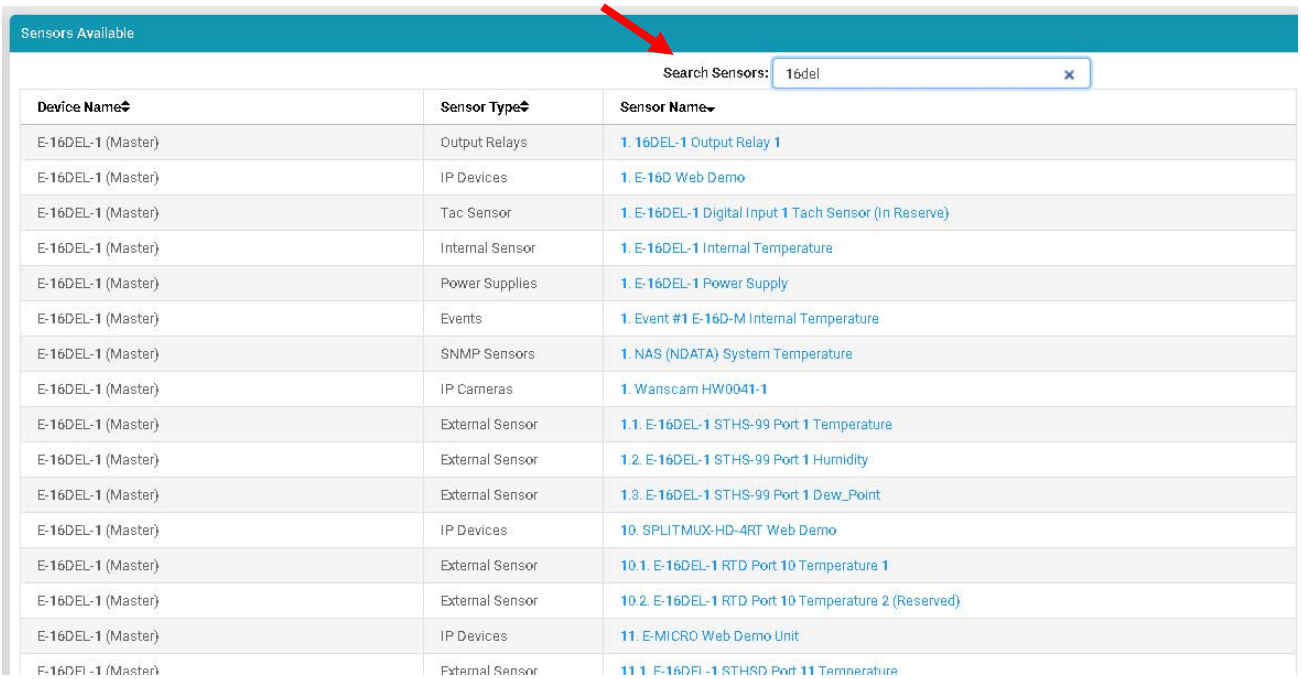


Figure 31- Details for Internal Temperature Sensor

To quickly find a sensor, type all or part of a sensor name or Device name in the “Search Sensors” box.



Device Name	Sensor Type	Sensor Name
E-16DEL-1 (Master)	Output Relays	1. 16DEL-1 Output Relay 1
E-16DEL-1 (Master)	IP Devices	1. E-16D Web Demo
E-16DEL-1 (Master)	Tac Sensor	1. E-16DEL-1 Digital Input 1 Tach Sensor (In Reserve)
E-16DEL-1 (Master)	Internal Sensor	1. E-16DEL-1 Internal Temperature
E-16DEL-1 (Master)	Power Supplies	1. E-16DEL-1 Power Supply
E-16DEL-1 (Master)	Events	1. Event #1 E-16D-M Internal Temperature
E-16DEL-1 (Master)	SNMP Sensors	1. NAS (NDATA) System Temperature
E-16DEL-1 (Master)	IP Cameras	1. Wanscam HW0041-1
E-16DEL-1 (Master)	External Sensor	1.1. E-16DEL-1 STHS-99 Port 1 Temperature
E-16DEL-1 (Master)	External Sensor	1.2. E-16DEL-1 STHS-99 Port 1 Humidity
E-16DEL-1 (Master)	External Sensor	1.3. E-16DEL-1 STHS-99 Port 1 Dew_Point
E-16DEL-1 (Master)	IP Devices	10. SPLITMUX-HD-4RT Web Demo
E-16DEL-1 (Master)	External Sensor	10.1. E-16DEL-1 RTD Port 10 Temperature 1
E-16DEL-1 (Master)	External Sensor	10.2. E-16DEL-1 RTD Port 10 Temperature 2 (Reserved)
E-16DEL-1 (Master)	IP Devices	11. E-MICRO Web Demo Unit
E-16DEL-1 (Master)	External Sensor	11.1. E-16DEL-1 STHSD Port 11 Temperature

Figure 32- Use Search Sensors box

To see sensors connected to a specific Device, double-click or expand the Device in the group.

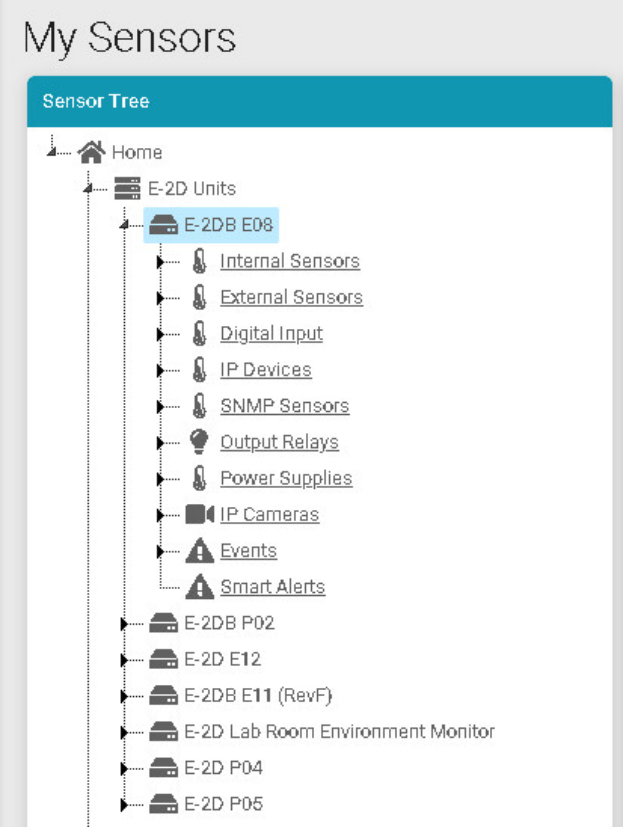


Figure 33- Sensors, relays, IP Cameras etc attached to a specific Device

If you click once on a specific sensor category, the screen format will change and show the status of all sensors in that category.

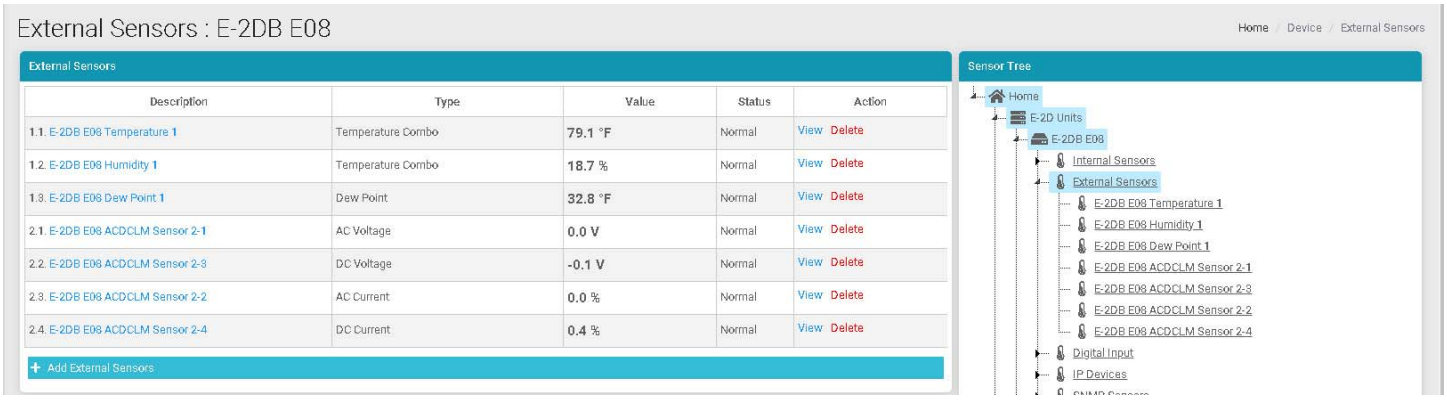


Figure 34- External Sensors connected to specific Device

From that screen you can view each sensor, or delete it from the list.

SETUP A DASHBOARD

Groups of sensors can be monitored in Dashboards containing rows and columns displaying the status of individual sensors. Each of the sensors monitored on each of the Devices can be added to various Dashboards and organized in rows and columns as necessary for easy viewing.

To get started, click the "Edit" button next to "Dashboard1".

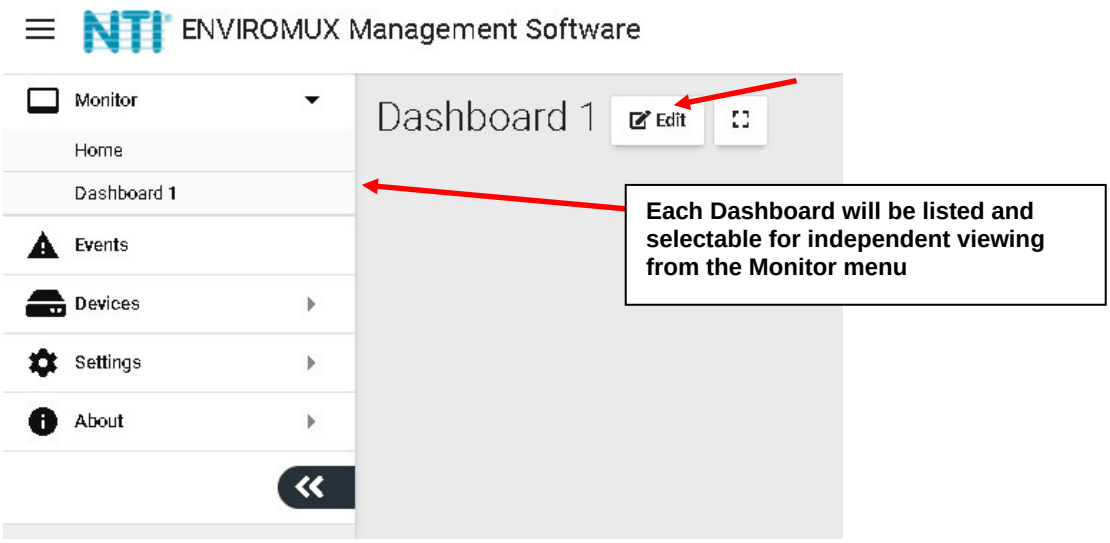


Figure 35- Initial Monitoring Dashboard menu

This will open the window into the options available for creating new Dashboards. With the editing window open, you can change the name of the Dashboard, add a new Dashboard, or add a new row of monitored sensors to the layout. If you click the Finish Edit button, the editing window will close and the configured Dashboard will remain.

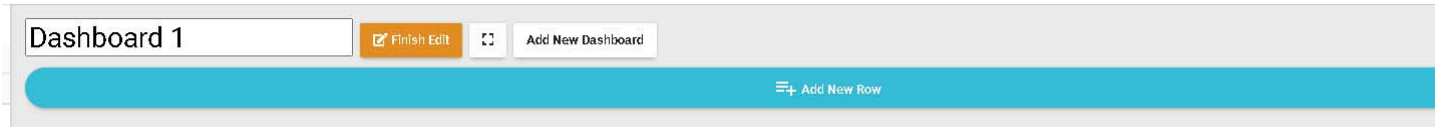


Figure 36- Dashboard options

Click "Add New Row" to establish your first row of sensors. Clock the "X" to delete the row and all columns in it.

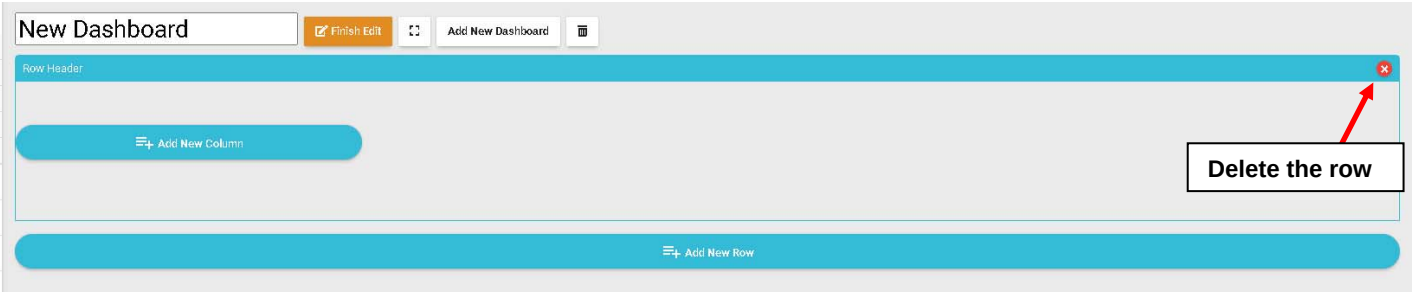


Figure 37- How to add Columns or delete Rows

Then click the "Add New Column" to create a column in that row. Click it multiple times for multiple columns.
We recommend all columns fit in the same row side by side. To resize the columns click on the Decrease or Increase icon, as many times as needed, and that column will resize accordingly after a short delay (see also page 27) .

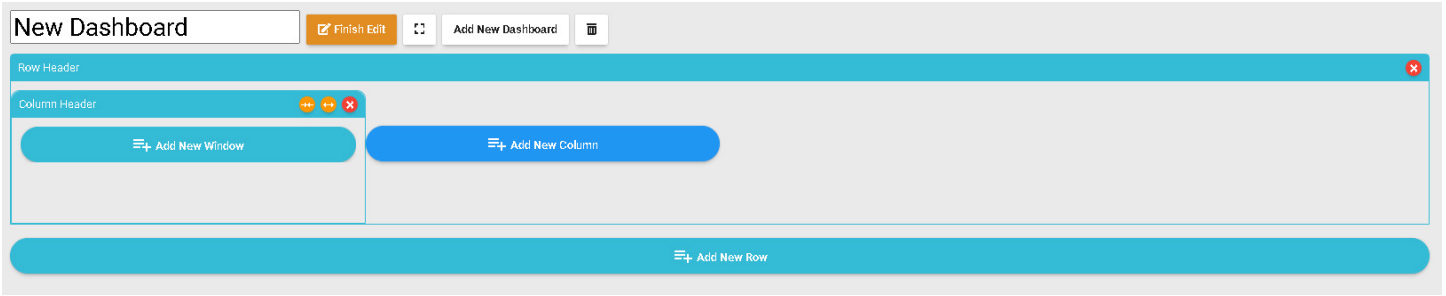


Figure 38- Ready to add a sensor window

To add a sensor, in the Column Header, click the "Add New Window". A list of all sensors connected to all of the Devices will appear, 10 at a time. Select which sensor is to be monitored in the column. You can also enter a name to associate with that sensor. Navigate through the many sensors available.

Sensors can be viewed as individual sensors, graphs for single sensors, gauges for single sensors and much more. IP Camera snapshots, an alerts list, or Device status can also be viewed.

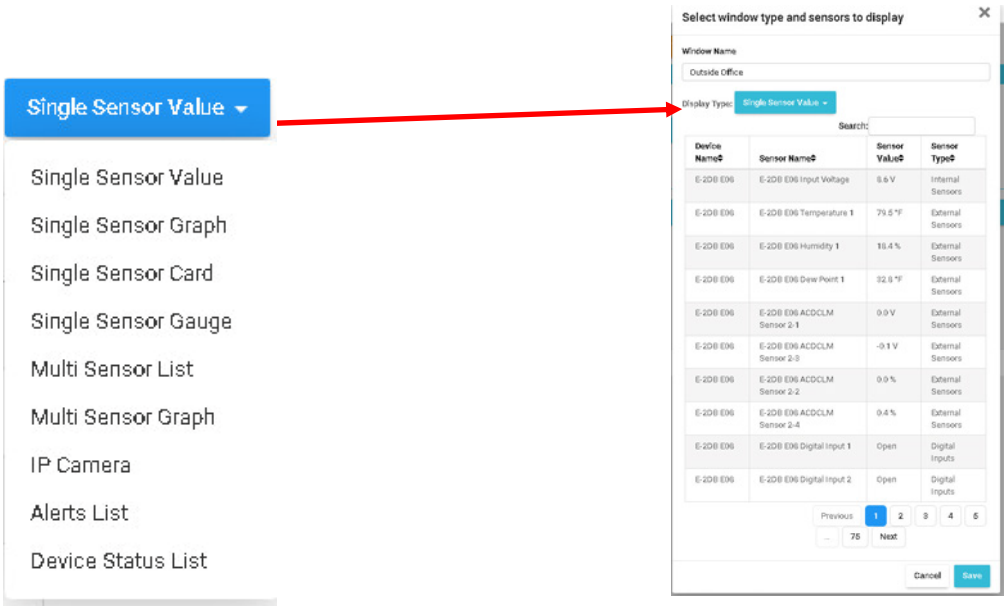


Figure 39- Select sensors to view

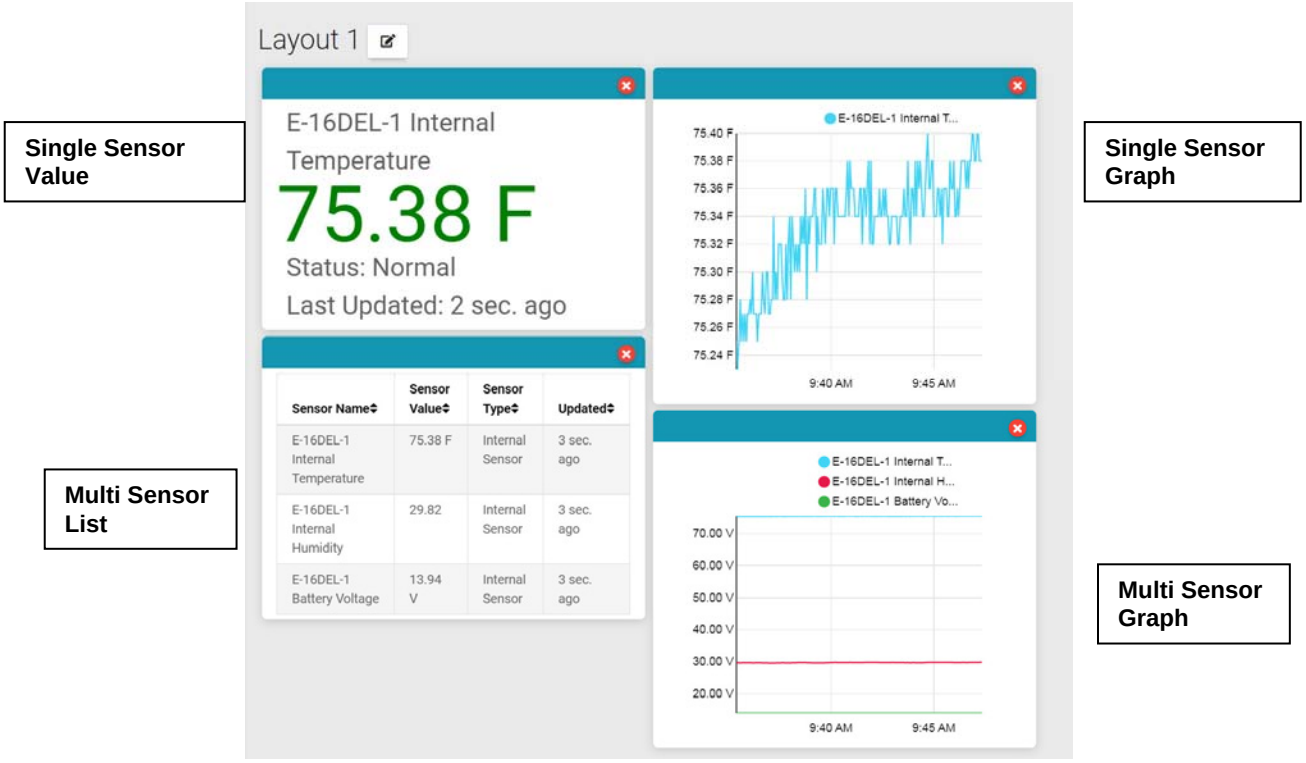


Figure 40- Multiple types of views available

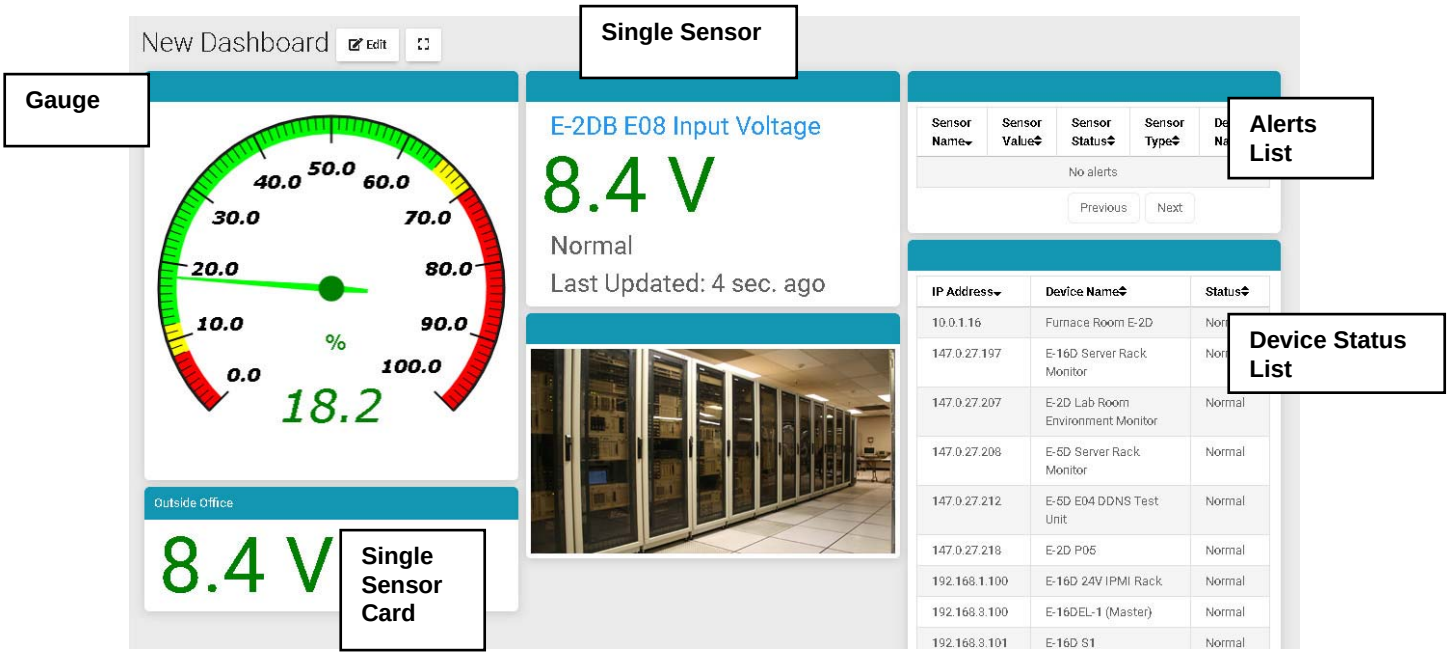


Figure 41- More types of views

To select one sensor, click one listed item and it will turn blue. Click "Save" to enter that in the column.

To select multiple sensors, there is no need to hold the shift key. Clicking one after the other keeps the sensor selected.

To deselect a sensor, click the sensor again.

Once done click "Save" to enter them in the same window.

To quickly locate the sensor you want to display, use the Search box to enter characters in the description to sort the available sensors and display only the ones that include your search parameters.

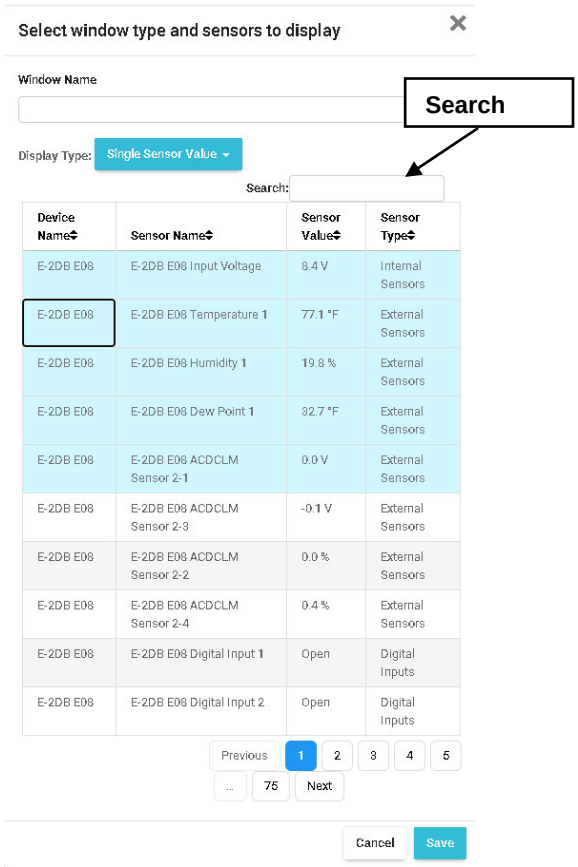


Figure 42- Select one or more sensors

To delete a window in a column, click the red "X" in the upper right corner of the window.

If you wish to change the order in which your sensors are viewed, you can move a window from one column to another. First add the column if it doesn't already exist, "then simply drag the window by holding the window header bar to the target column. While dropping to the target column, that column will show a white placeholder indicating that the window can be dropped there.

Use the Increase button to increase the width of a selected column.

Use the Decrease button to decrease the width of a selected column.

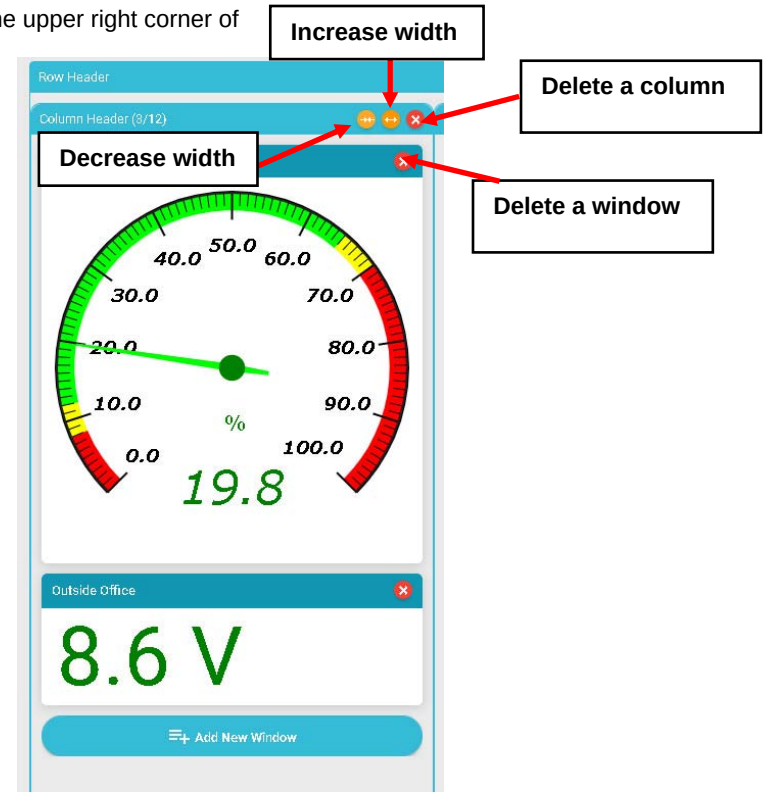


Figure 43- Change the width of a column

To add a new group of sensors to a separate row, Click "Add New Row" and configure the new row in the same fashion.

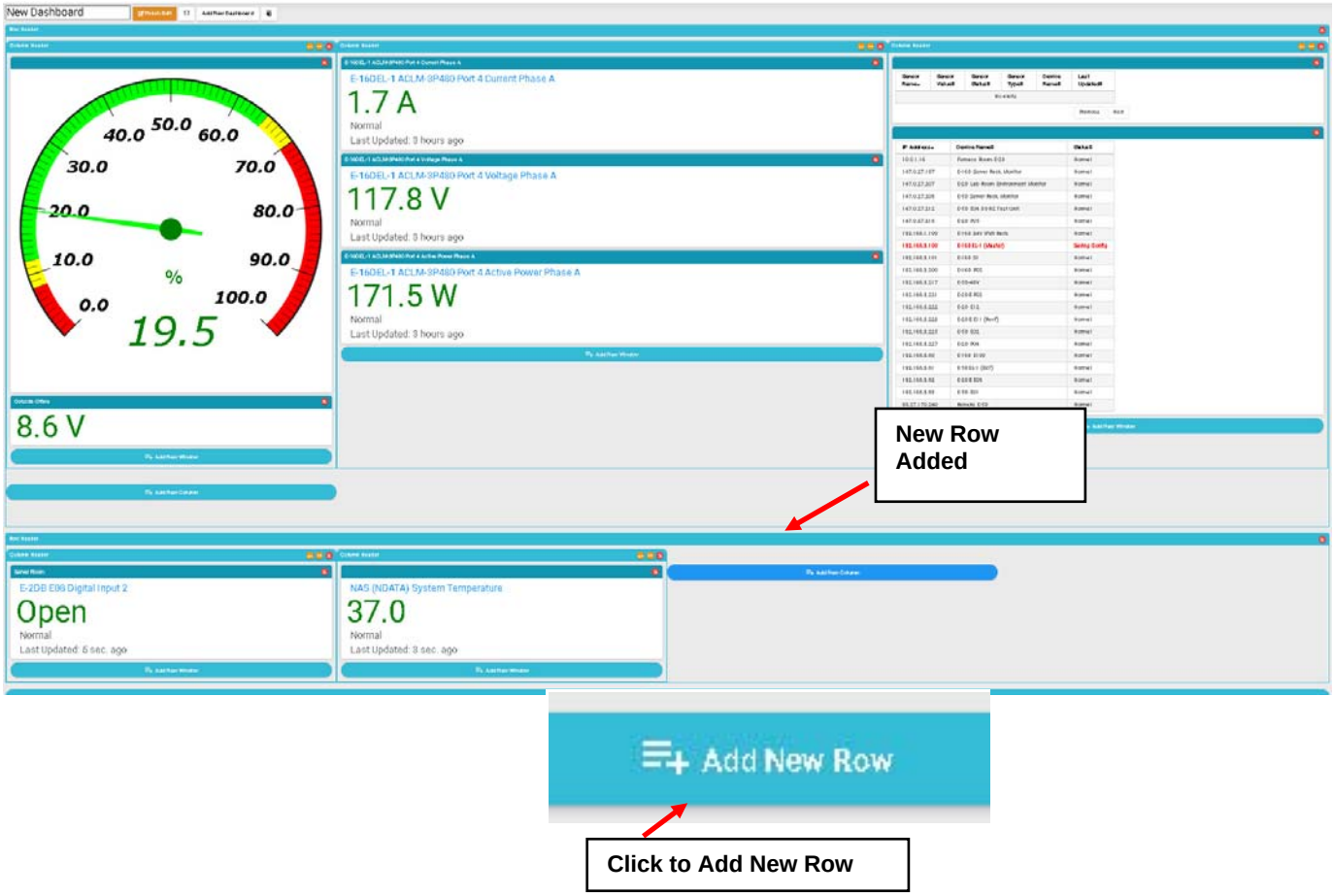


Figure 44- Add a new row of sensors

To logout of the server without shutting the Server down,
click on the Root icon in the upper right corner of the screen, and
click on "Log Out".

Message number (image right) indicates the number of alerts triggered since the last alert was viewed or acknowledged by this user

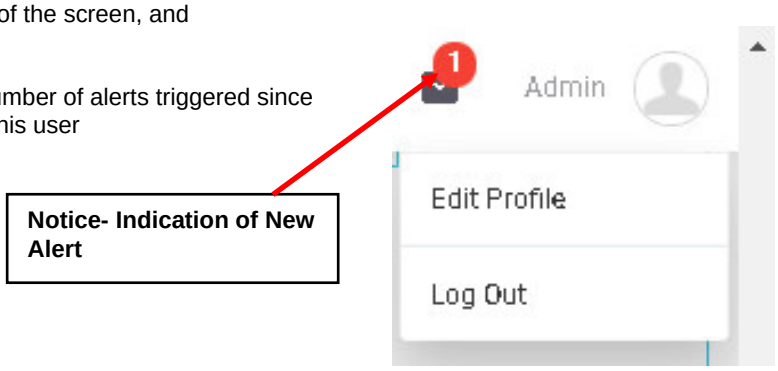


Figure 45- Log out

There is no limit to the number of Dashboards that can be setup to organize the type of sensor data you want to see. For example, a "Graphs" Dashboard was setup to view only the graphs from specific sensors.

When in full screen mode (see bottom of this page), scrolling the screen is not possible. Please make sure all windows fit inside the screen to be visible on the monitor.

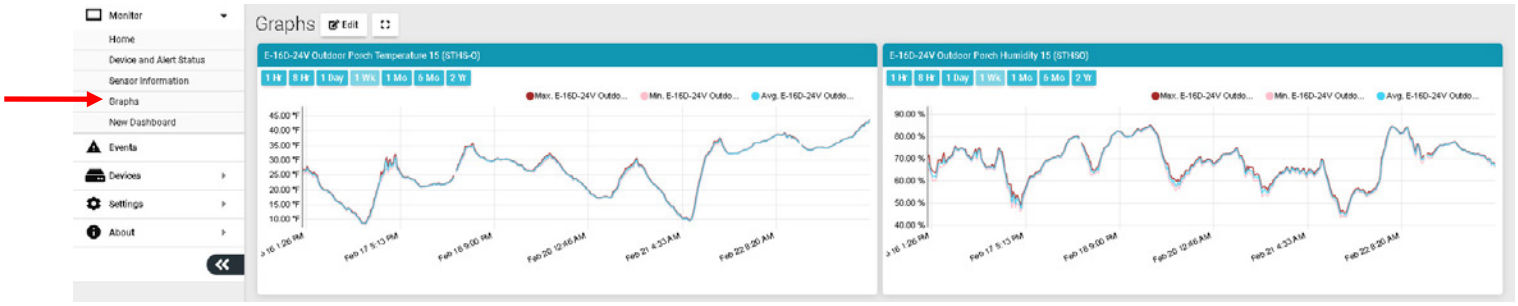
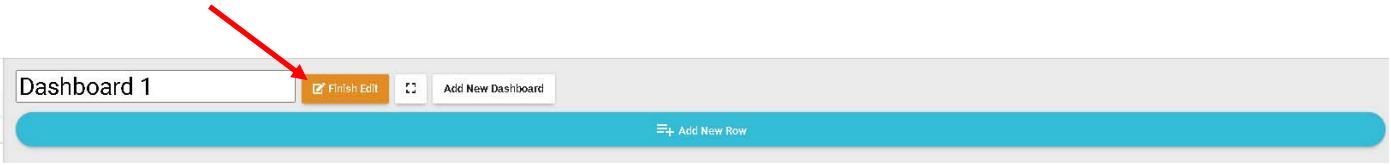


Figure 46- Dashboard setup to display specific content

Once you are finished editing a Dashboard, click "Finish Editing"



While viewing your Dashboard, to make it fill your screen, click on the small box to the right of the Edit button. Press the "Esc" key to return to normal viewing.

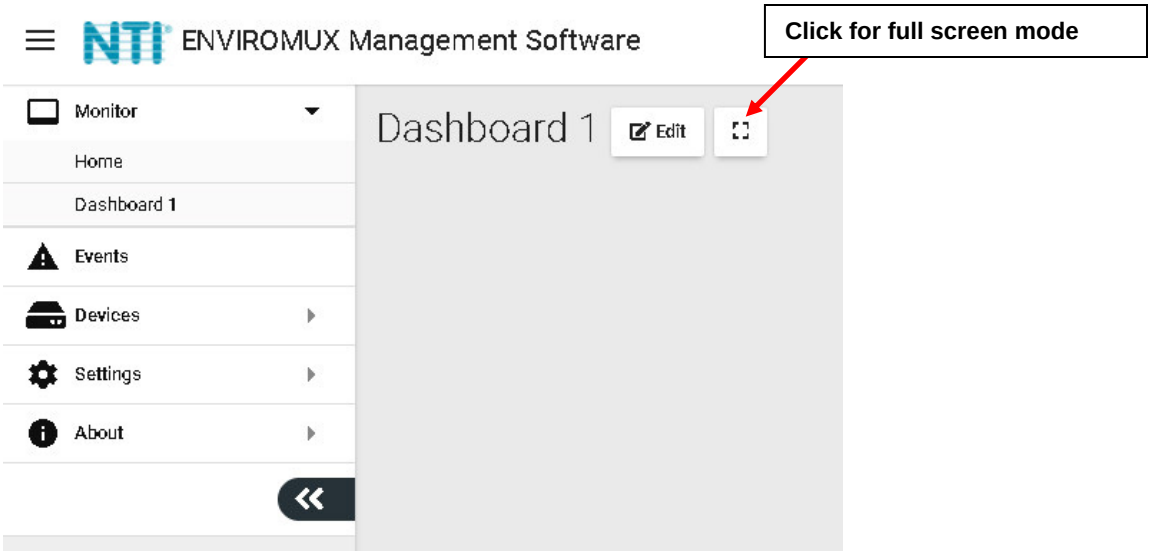


Figure 47- Enable full screen view

EVENTS MENU

The E-MNG-SH can provide information on alerts generated by the devices it is monitoring, and will provide that information in three different forms.

Events Log will provide a list of events that have occurred for each device/sensor the E-MNG-SH is monitoring.

Reports, once configured, will contain event information on selected sensors, devices (and all sensors connected to those devices), or markers assigned to configured maps. The information the reports will provide includes 1) the combined number of alerts that have been generated by each selected sensors/device's sensors/markers in the maps and 2) the combined length of time each of those devices/sensors/ markers were in alert. The frequency of reports and the data present in reports can be configured by "Triggers" and "Actions" respectively.

Recordings are a collection of IPCAM snapshot recordings that have been saved as configured in each sensor alert that is set to provide a snapshot recording from a connected IPCAM.

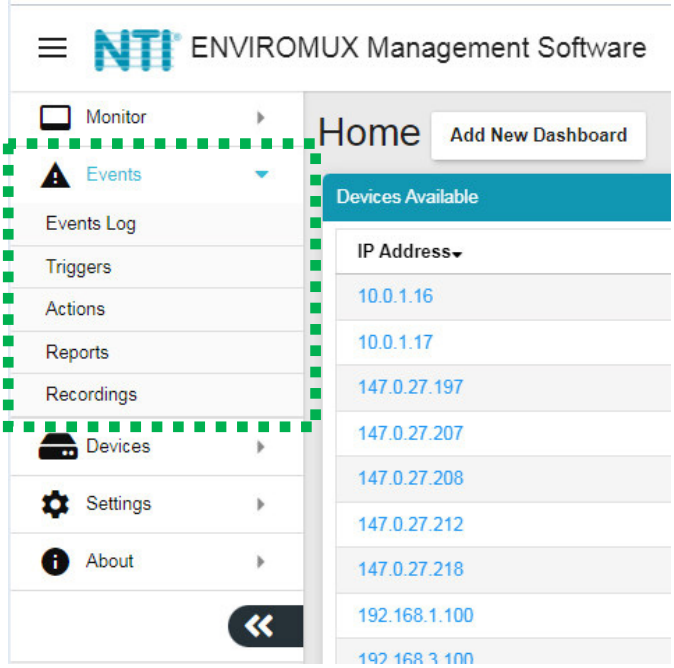


Figure 48- Events Menu

Events Log

The Events Logs is where Sensor Events, Smart Alerts and Alert messages are individually recorded. The time of each event, the type of event and the source of each event are recorded.

Alert logs are recorded in red font.

When the alert is Acknowledged or Dismissed, the alert will show up in the Events Log along with the name of the user.

From the link in the message, you can click and go directly to the sensor to see its current state.

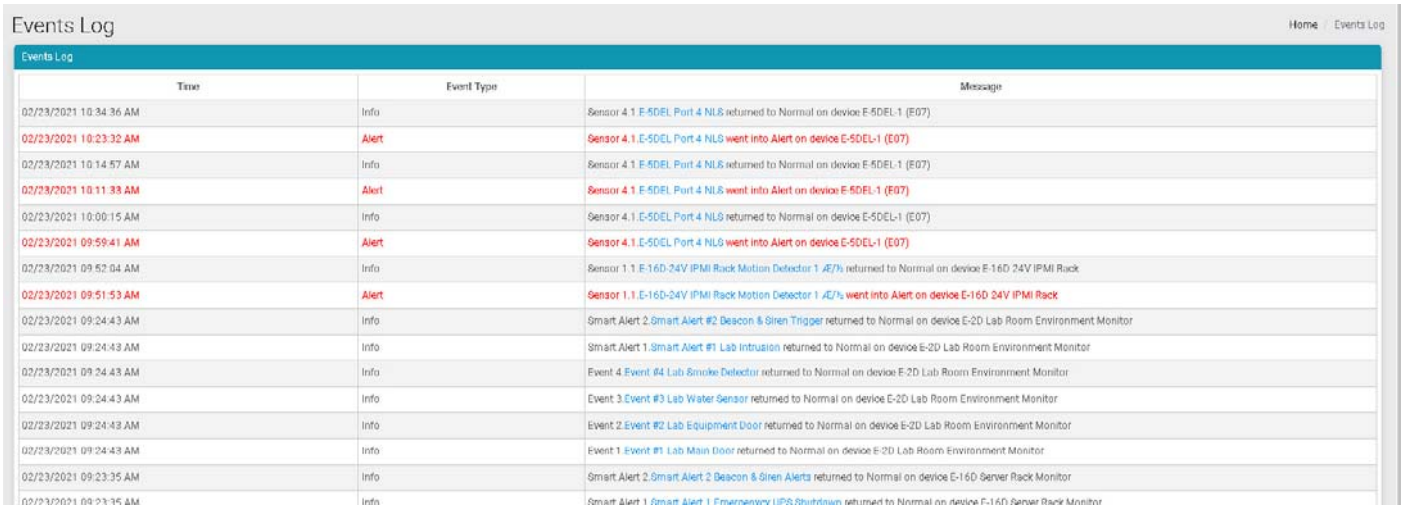


Figure 49- Events Log

If a sensor is in alert, you can directly connect to it and Acknowledge or Dismiss the alert.

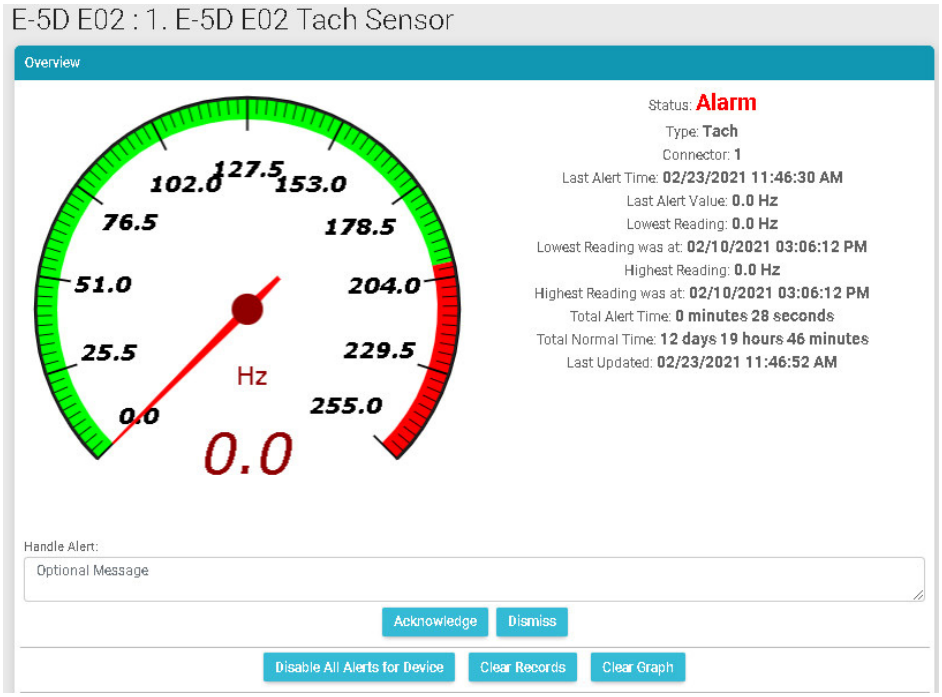


Figure 50- Connect directly to acknowledge or dismiss alert

Whether the Event is viewed on the Events Log page, or from a Dashboard displaying the event, you can click on the sensor in the image and address the event directly.

You can click on the alert to Acknowledge/Dismiss the alert directly from Dashboard.

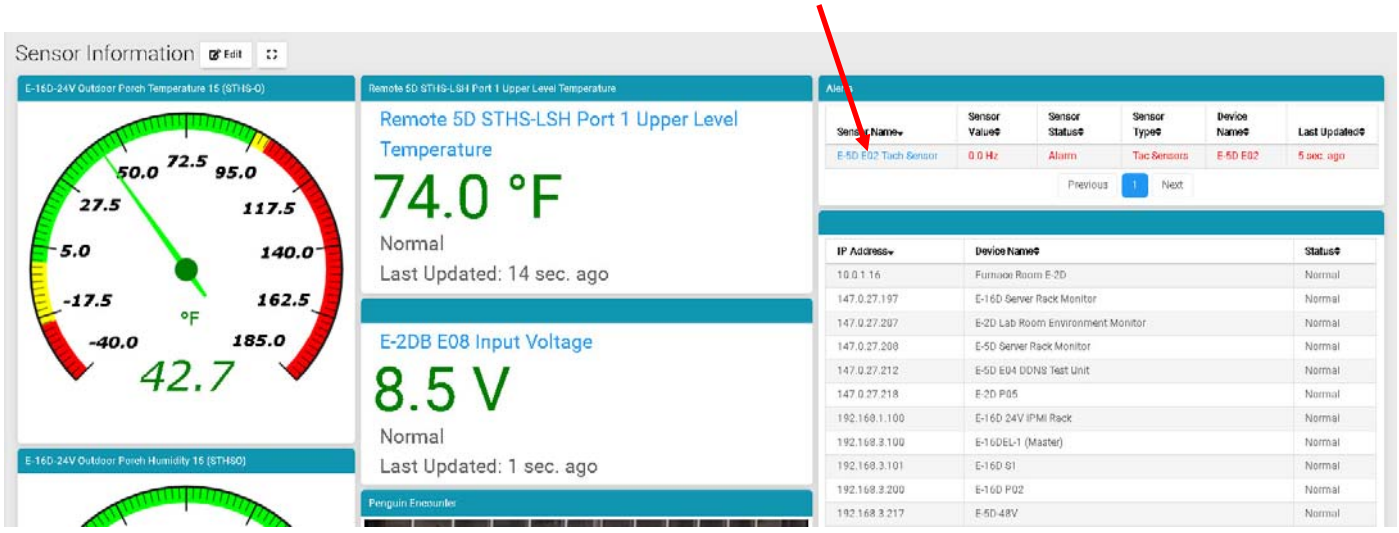


Figure 51- View and connect directly with sensor through the Dashboard

When you click on the alert from the Dashboard, a pop-up will display providing the option to acknowledge or dismiss it.

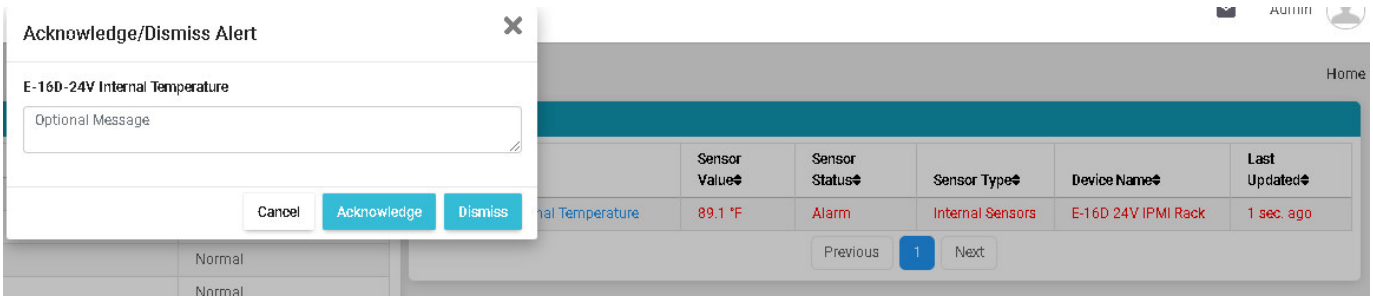


Figure 52- Acknowledge or Dismiss alert pop-up

Reports

Reports will contain event information on selected sensors and devices individually or in groups as they are assigned to Devices, or markers assigned to configured maps. Before you must configure Actions to be reported on and Triggers for how often to have Reports generated.

First click on “Actions” in the Events menu. Apply a name to the Action you will create. Then click on “Add New Action” and your new Action will appear in the list to the left.

Once the Action is listed, click on “Edit” to configure it.

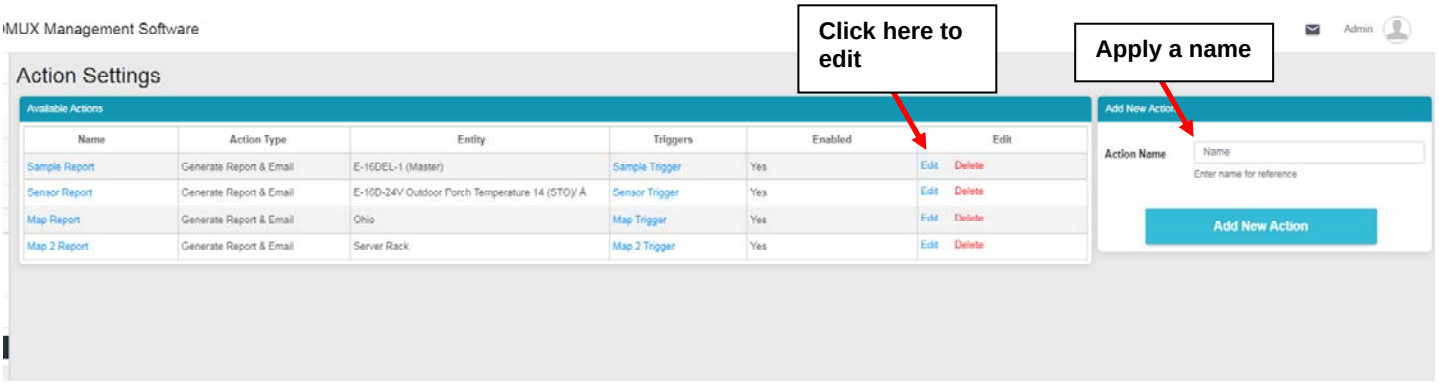


Figure 53- Action List

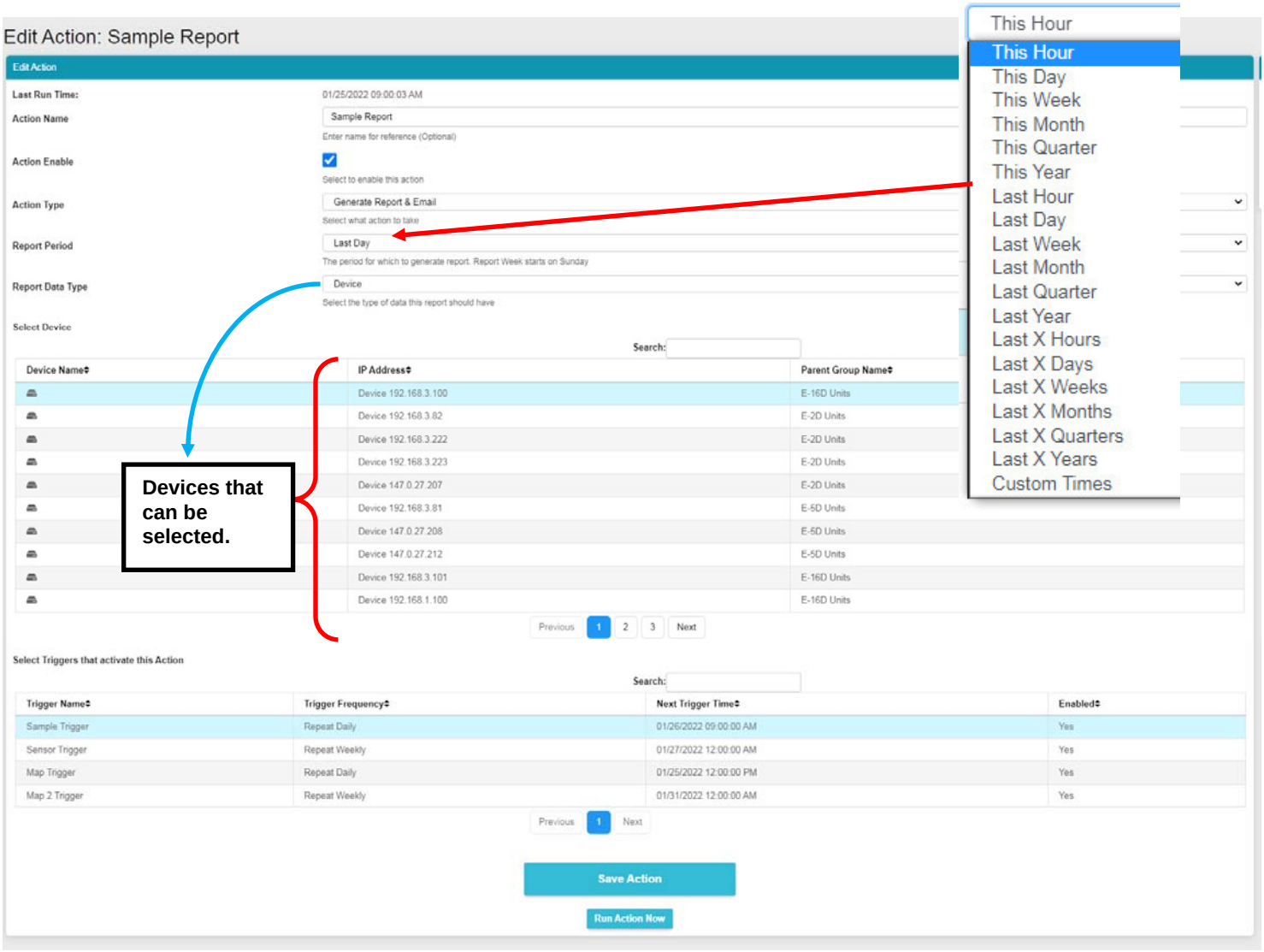


Figure 54- Action Options

Be sure to enable the “Action Enable” block. Otherwise reports will not be generated.

For Action Type, select between “Generate Report” and “Generate Report & Email”. If you select “Generate Report & Email” then all users with “Email Alerts” selected (Figure 12) will received reports via email.

The Report Period is the data in the time period that reports should include. A long list of time periods is available to select from.

The Report can include alerts from specific sensors, sensors that are connected to specific devices (E-xD units) or sensors identified with markers place in configured maps. Available selections will adjust depending upon what Report Data Type you select.

Once Triggers have been set up, they will appear in the list. Triggers determine how often the Action will be initiated and when. Either select a Trigger to cause the action to occur and generate a report, or configure a new Trigger first (on the next page).

Be sure to click “Save Action” to retain your changes. To test the result of the action, click “Run Action Now”. The Report generated by that action should appear under Reports, and if you have selected it, each user with Email Alerts enabled will also receive a pdf copy of the report.

Triggers

Triggers determine how often an Action will be taken and a Report generated from that Action.

Click “Triggers” in the Events menu. Apply a name to the Trigger you will create. Then click on “Add New Trigger” and your new Trigger will appear in the list to the left.

Once the Trigger is listed, click on “Edit” to configure it.

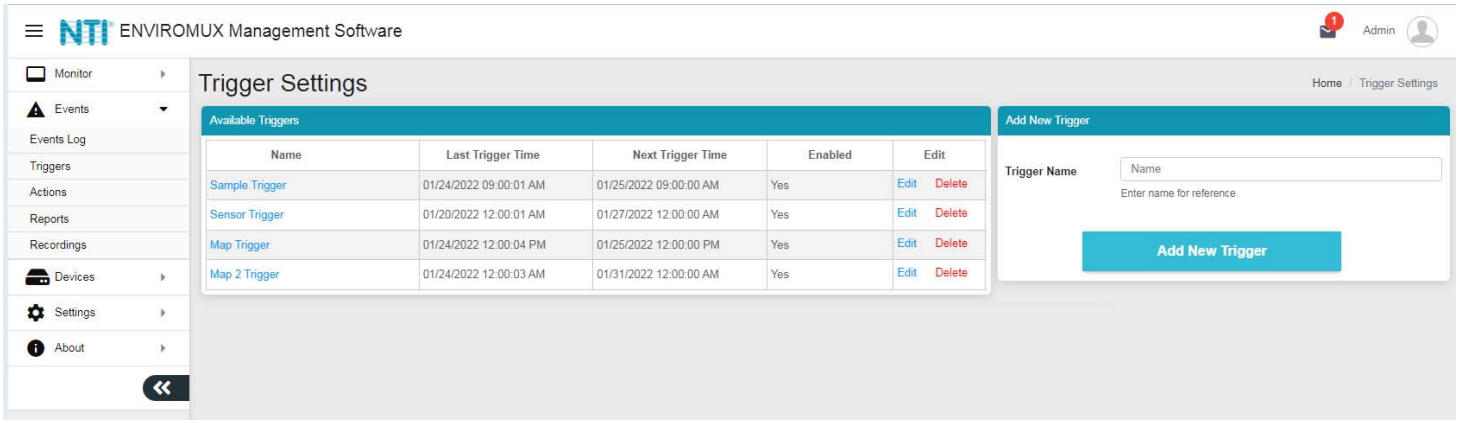


Figure 55- Trigger List

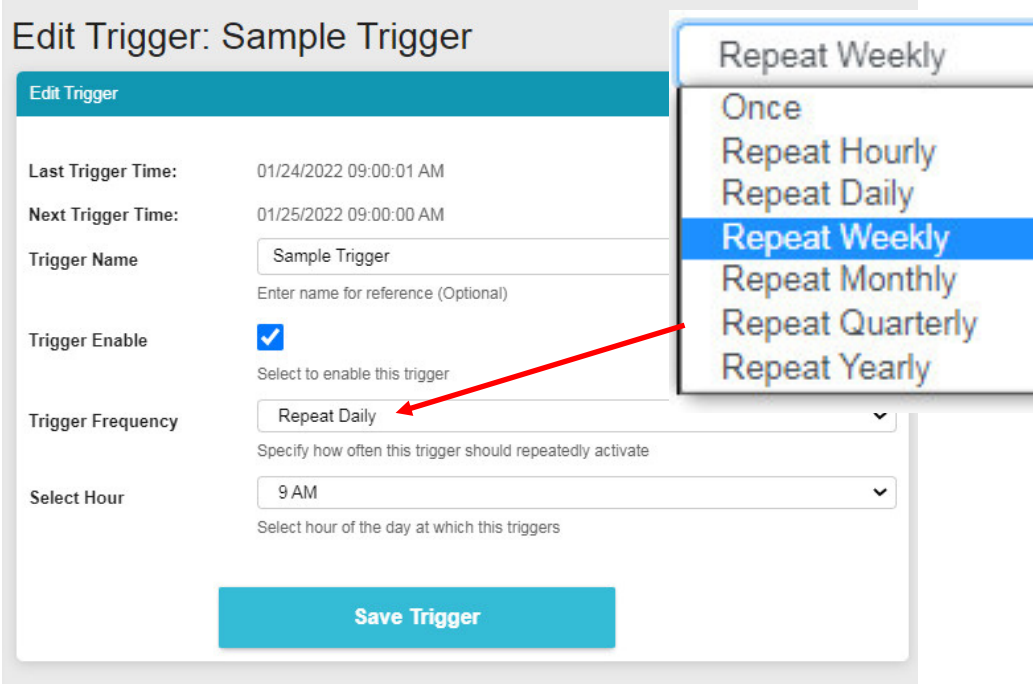


Figure 56- Trigger Options

If the Trigger had been previously setup, the last trigger time and next trigger time will be indicated.

The name given to the Trigger will be displayed and can be changed.

A checkbox to enable the Trigger is provided so that it can be used.

Select the Trigger Frequency from a list of options. Depending upon what Trigger Frequency is selected, the option for fine tuning the frequency will change. (See next page)

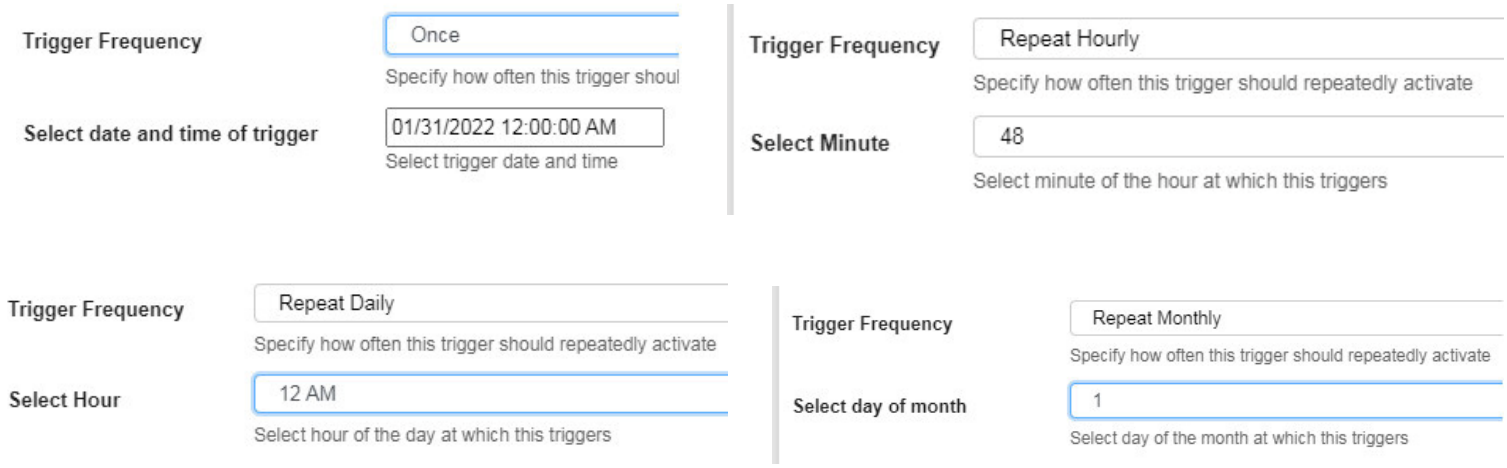


Figure 57- Option detail for Trigger Frequency

Be sure to click “Save Trigger” to retain your changes.

With Triggers and Actions setup, Reports will be generated and added to the Report List.

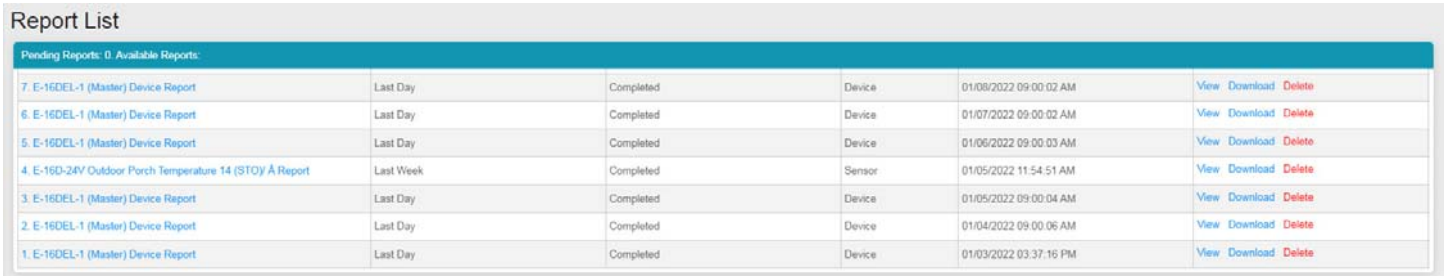


Figure 58- Reports list

With a report in the list, you can click “View” to see the content immediately, click “Download” to save it for viewing later, or click “Delete” if you don’t want it in the list any longer.

The sensor report will provide a graph indicating the total number of alerts generated by each sensor and the total length of time that sensor was in alert.

Maps and device reports provide an alert details summary and its trends (see image on next page). A maximum of 800 reports wil be stored before the software automatically deletes the oldest reports.

Figure 59- Report showing sensor alert trends

Recordings

Recordings are snapshot recordings from selected IPCAMs when a sensor goes into alert. The IPCAM and the length of time it will record will be selected under critical alert settings for that sensor (below). Recordings are collections of snapshots from the camera, taken as frequently as the refresh rate for the camera is set for.

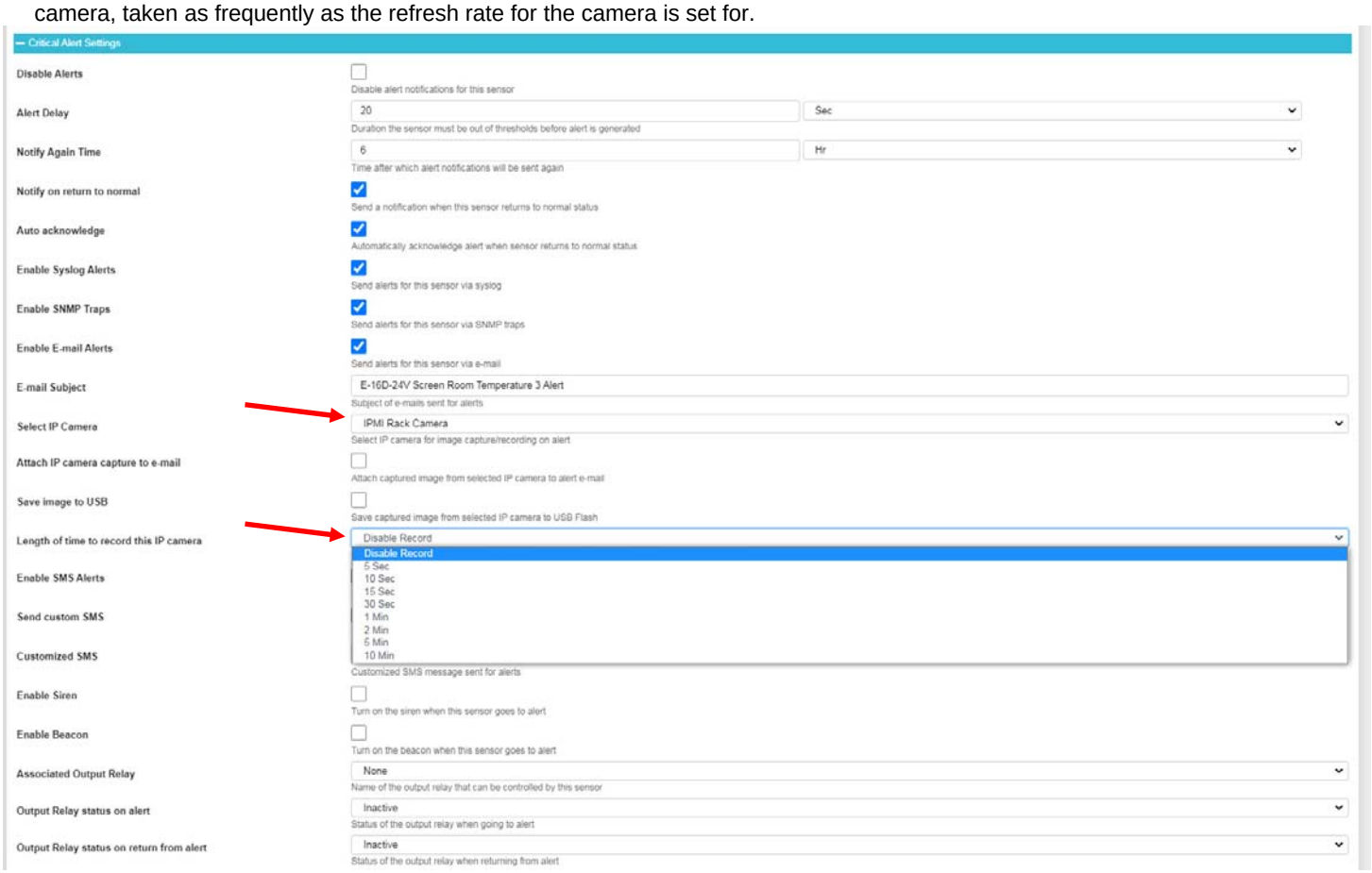
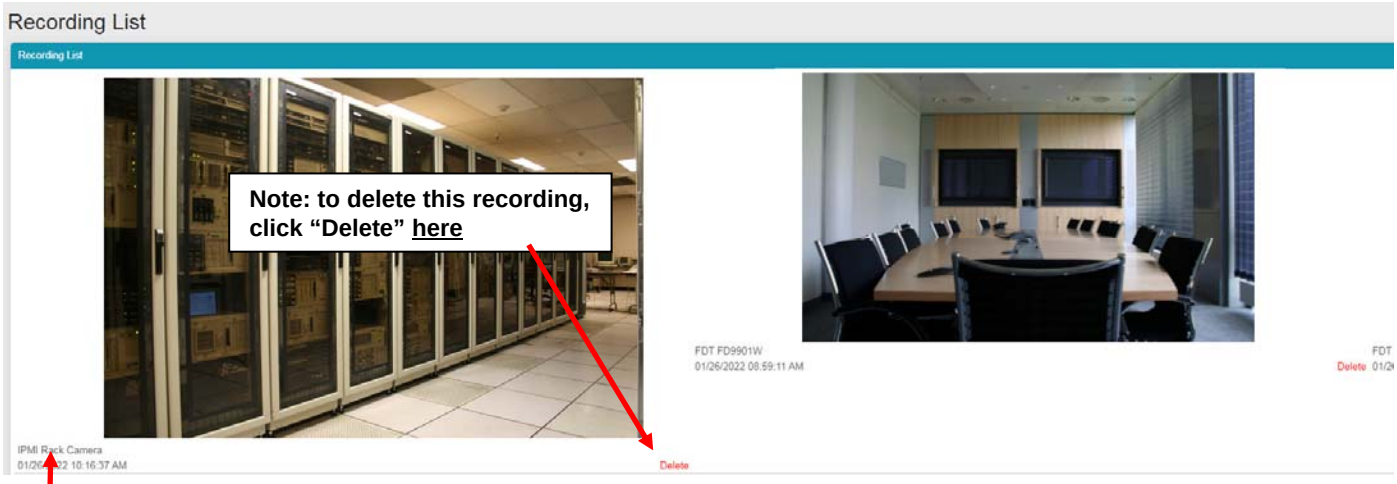


Figure 60- User settings to enable Recording

To see your recordings, click on “Recordings” in the Events menu. The camera the recording came from and time it was recorded will be in the bottom left corner of the recording. To delete a recording, click “Delete” in the bottom **right** corner of the recording image. Up to 1000 recordings will be stored before the software automatically deletes the oldest recording.



Label shows where the video was captured from and when

Figure 61- Recording list

THE ABOUT MENU

The About menu includes tools for viewing the firmware version you are using and any details about it, as well as providing a link the this manual and a link to a contacts page should you need to contact NTI. Lastly it provides a link to the firmware downloads page where you can get access to the most current version of the E-MNG-SH program.

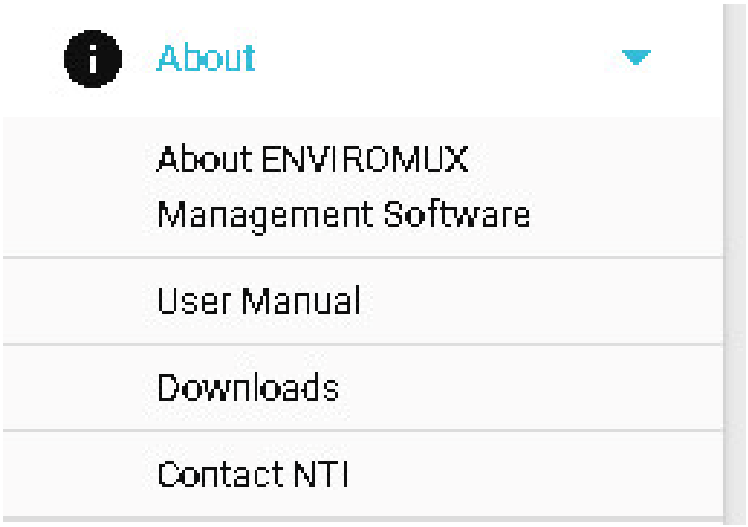
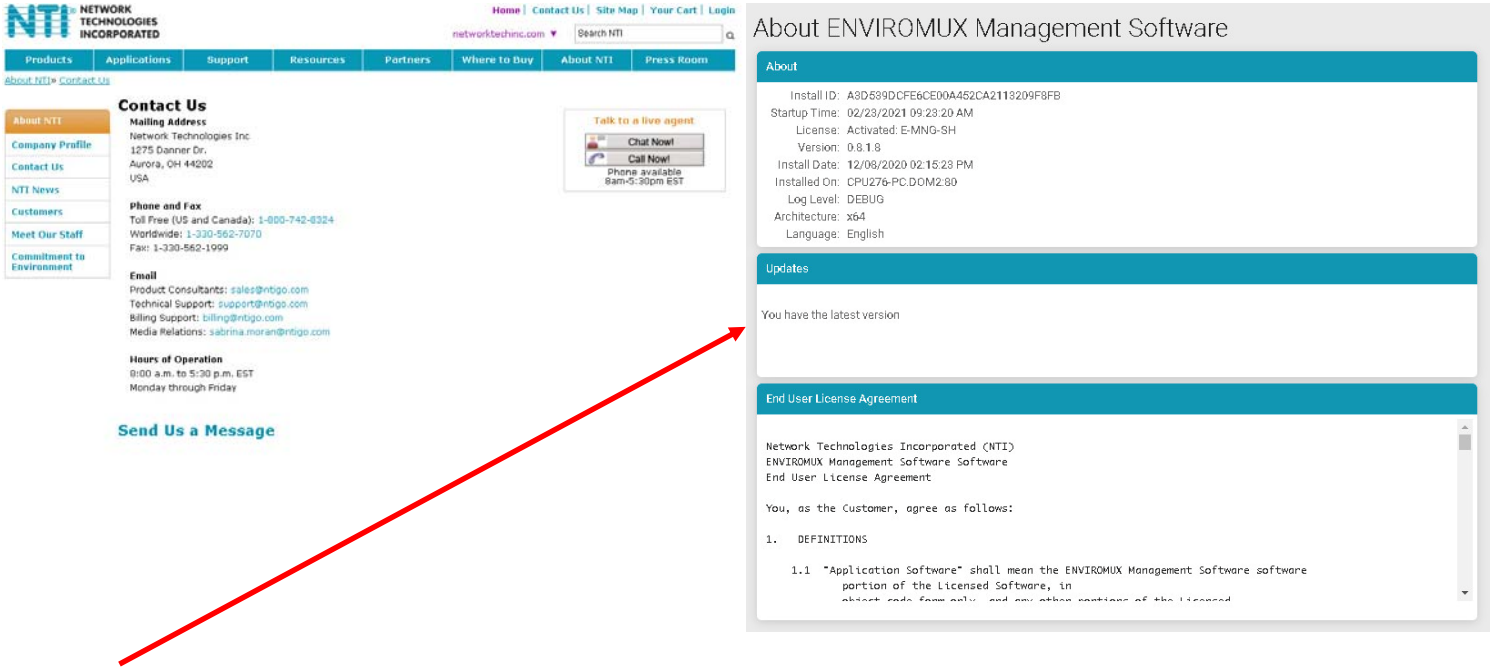


Figure 62- About menu



From the "About ENVIROMUX Management Software" page you can also, at a glance, see if another more current version of the software is available, without having to actually leave the program and go to the Downloads page.

SHUT DOWN E-MNG-SH SERVER

To shut down the E-MNG-SH completely, left click the tray icon in the bottom right corner of your desktop.

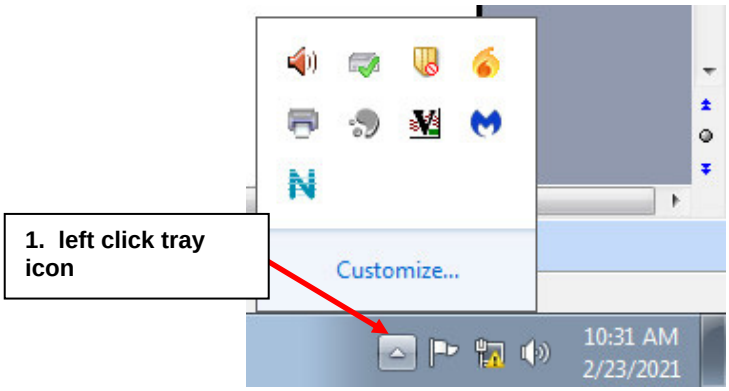


Figure 63- Click on Tray icon

Then right click the E-MNG-SH icon, and select Exit.

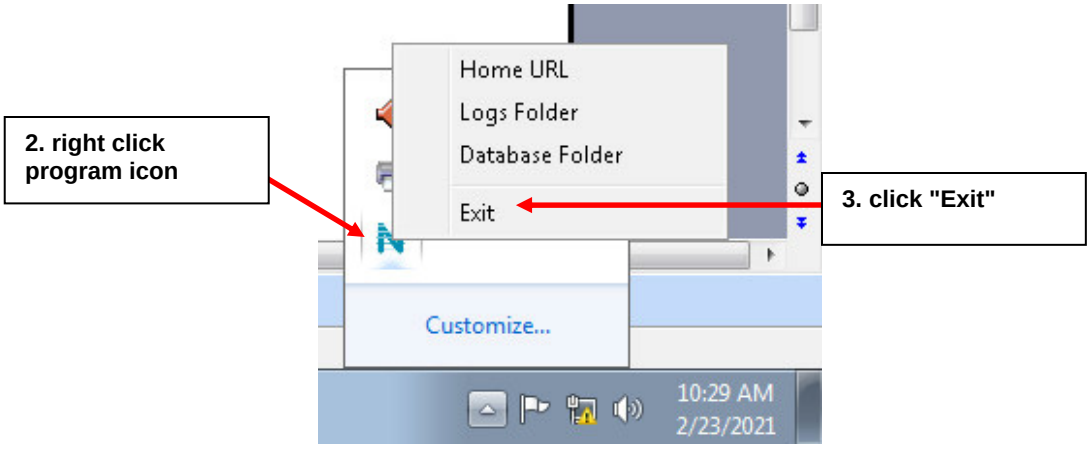


Figure 64- Exit the program

OTHER TYPE DEVICES

The E-MNG-SH can be accessed from any network-connected computers/smartphone/tablet (provided the computer/smartphone/tablet has access to the Server the E-MNG-SH is on).

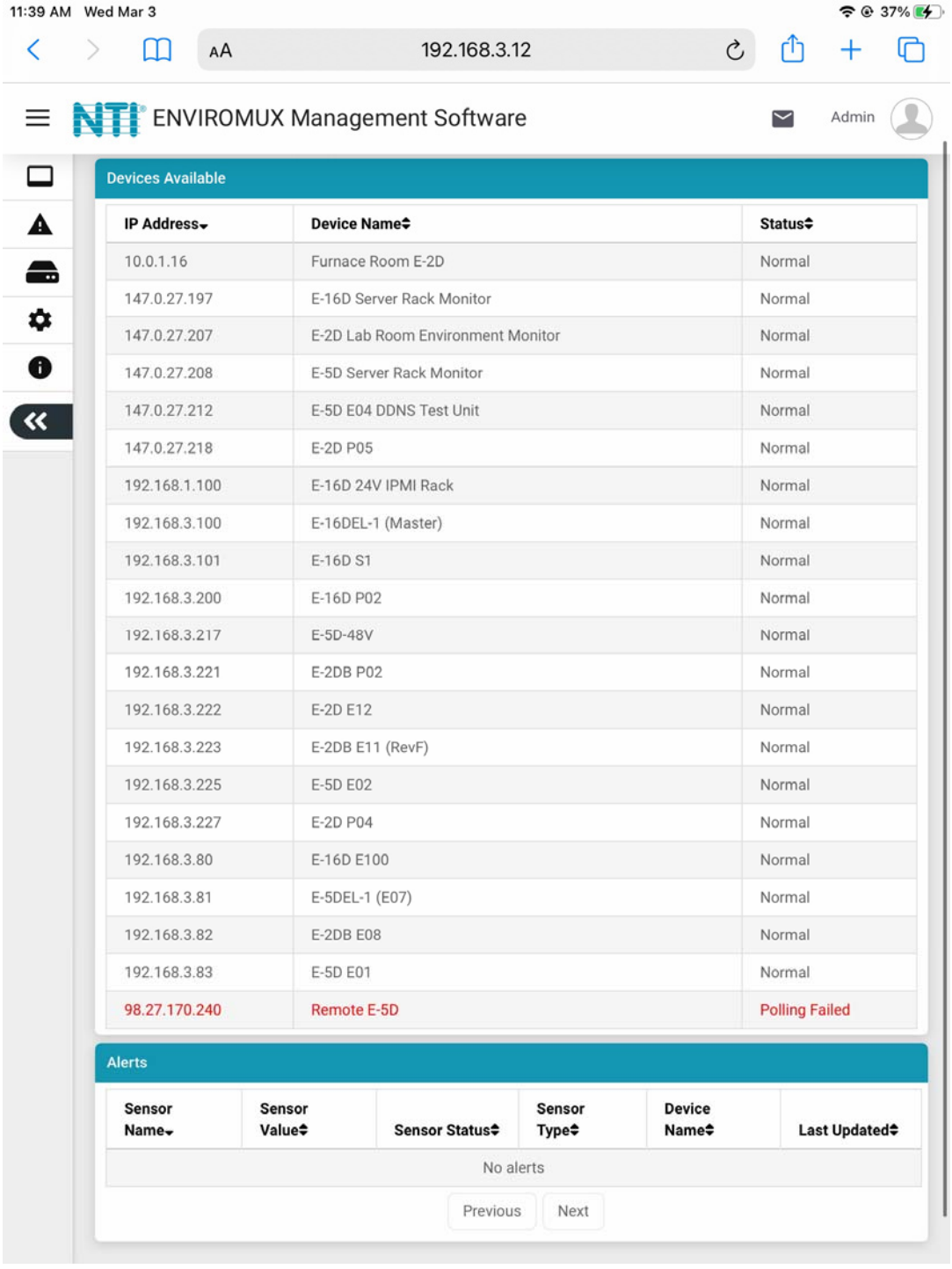


Figure 65- Screenshot from an iPad

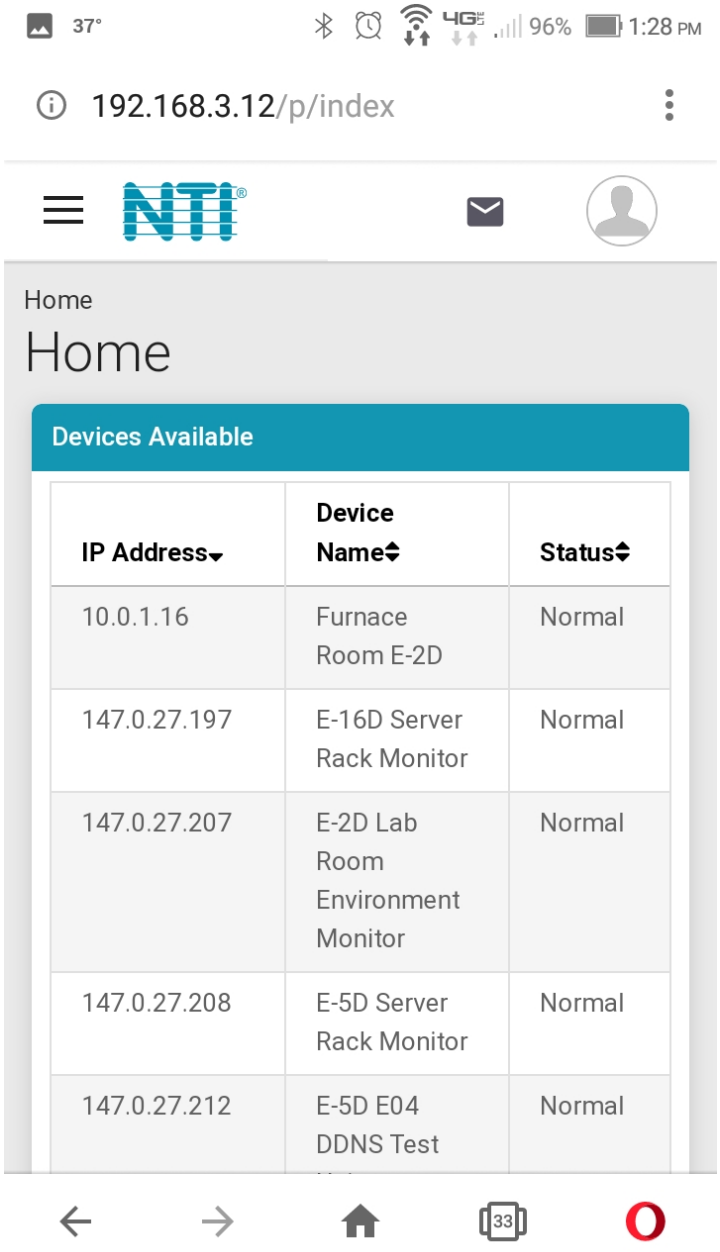


Figure 66- Screenshot from a smartphone

UNINSTALL THE PROGRAM

To uninstall the program: Go to the appropriate programs settings page (i.e. Control Panel -> Programs and Features) and select the “ENVIROMUX Management Software” to uninstall.

Note: Uninstalling the program will also remove any settings and saved sensor values. The license will remain (the license is not transferable)

SOFTWARE UPDATE

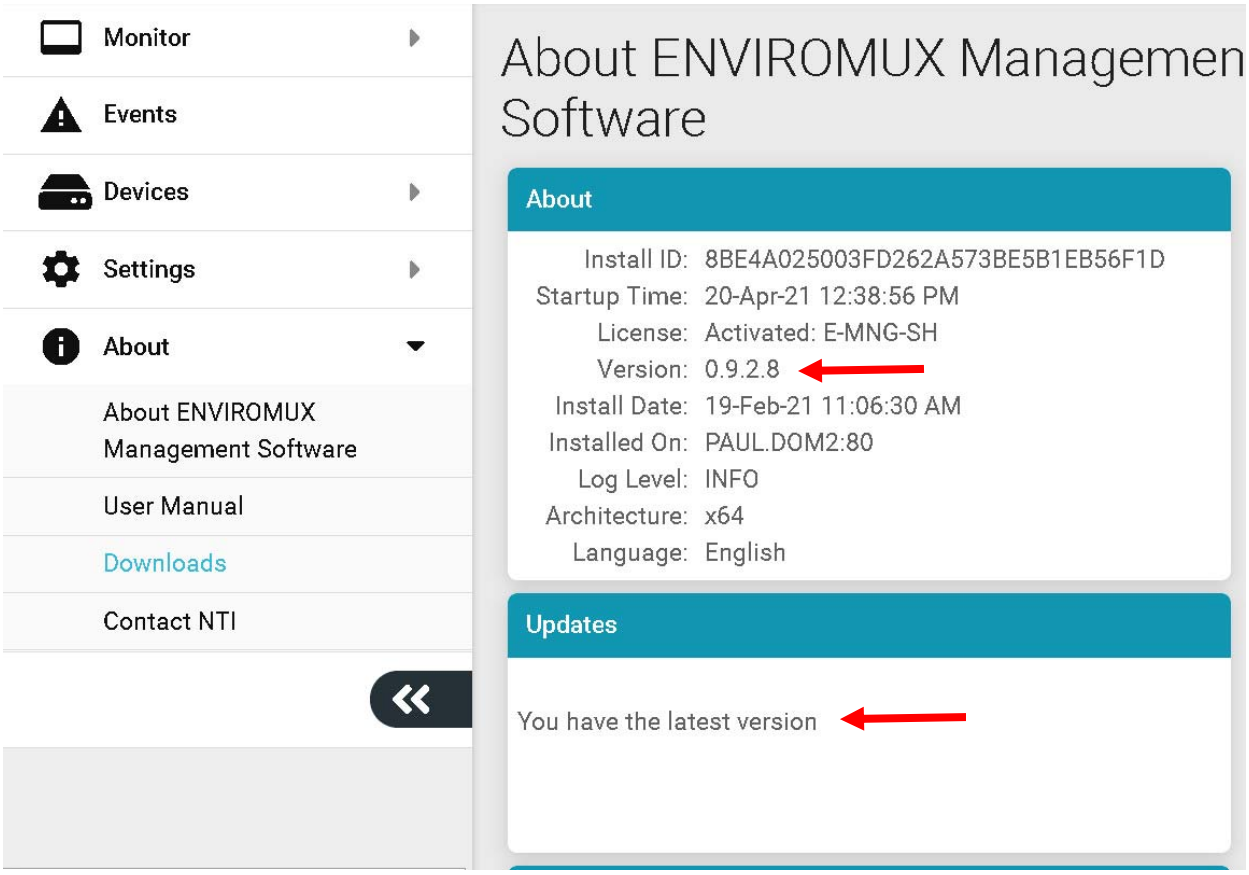
From time to time a new version of this program will be available. If you decide to update, follow these steps.

1. Download the new software version to the computer/server the E-MNG-SH is installed on.

2. Shut down the E-MNG software if running on this computer/server.

3. Double-click on the new installation file to install. Once the update has completed, it will prompt for login from the default browser.

Login to the E-MNG-SH and verify that the update has worked. Cick on "About" in the side menu, then click "About ENVIROMUX Management Software". The version number shown there will indicate what version you are running. The Updates section will get refreshed after the next update check.



INDEX

Man372 Rev 4/16/22