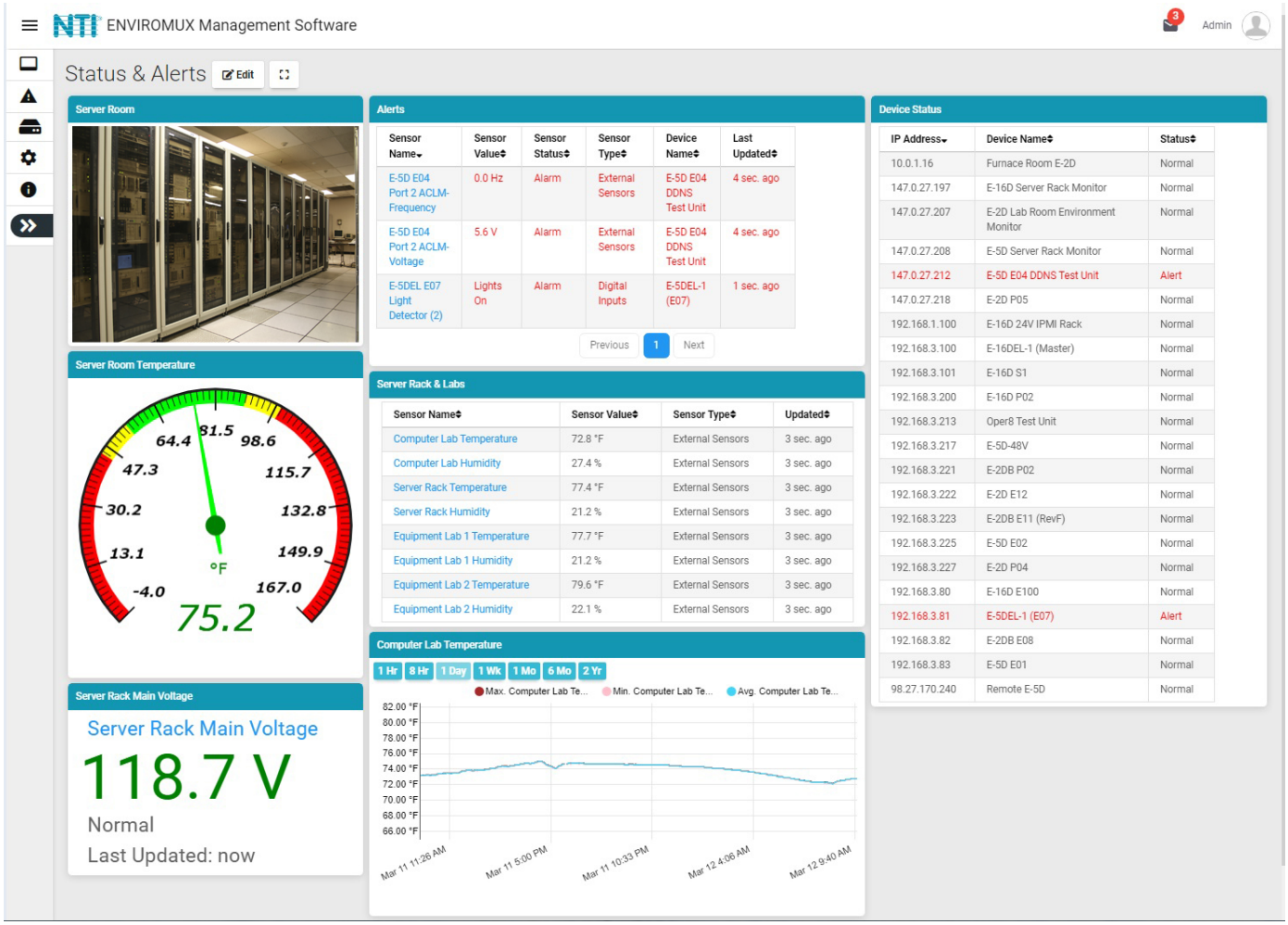
NETWORK TECHNOLOGIES INC
1275 Danner Dr
Aurora, OH 44202
Tel:330-562-7070
Fax:330-562-1999
www.networktechinc.com

ENVIROMUX® Series

E-MNG-SH

Enterprise Environment Monitoring System
Self-Hosted Management Software



TRADEMARK

COPYRIGHT

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 1.6.7.0

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, E-2D, E-MICRO-TRH(P) and E-1W(P) 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.
- Supports HTTP REST API to poll and download sensor data with response in JSON format.
- Unlimited number of users can access the Software program at the same time.
  - o 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.
  - o Access is operating system independent through the HTML5 user interface on the computer/smartphone/tablet's web browser.
  - o No clients or special apps to install.
- Sends email and/or SMS alert messages.
  - o Supports all email servers, including Gmail.
  - o SMS providers supported: Twilio, Sinch
  - o Customize messages for each sensor by creating message templates.
- 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 64-bit, Windows Server 2008/2012/2016/2019/2022 64-bit.
- Requires minimum firmware version 4.15 or later in E-xD Devices. We recommend version 4.19.
- Requires minimum firmware version 3.28 and maximum version 3.32 in E-MICRO-TRH(P) Devices.
- Requires minimum firmware version 3.10 and maximum version 3.15 in E-1W(P) 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.

Version with Non-Renewing License

To use a version of the self-hosted Software program that does not require monthly license renewal, order E-MNG-SH**NR**. The server still needs to have access to the internet for trial activation but offline activation for this version is explained on page 8.

Hardware Requirements

Below table contains details on recommendation for Minimum Server Hardware requirements for running E-MNG-SH. Storage space required depends on your Log Level, number of ENVIROMUX devices added, IP Camera Recording rate, number of logs retained and Log Rolling Period. For software installation we recommend minimum of 3GB free space. We recommend to start with minimum 250GB total storage space and expand as needed.

Number of ENVIROMUX Devices	Server CPU Core Count Required	RAM size Recommended
10	4	6GB
30	6	8GB
600	8	12GB
1100	8	16GB
1600	12	20GB
2100	12	24GB
2600	14	28GB
3000	14	32GB

NOTE: We strongly recommend SSD for storage instead of HDD

Network Port/Firewall Requirements:

To communicate with devices E-MNG-SH uses HTTP/HTTPS port as set on ENVIROMUX devices added.

To communicate with users E-MNG-SH uses HTTP/HTTPS port as set in Settings -> Network Settings of Server's IP

For License lock renewal and Gmail/Microsoft 365 authorization E-MNG-SH should be able to access https://www.networktechinc.com on port 443

For Gmail and Microsoft 365 emails E-MNG-SH should be able to access respective email server domains

For SMS through Twilio/Sinch E-MNG-SH should be able to access respective SMS server domains

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 (vx.x.x.x = the version number)
  The current version number is 1.6.7.0.
- Adobe pdf file of this manual

LIMITATIONS

- The Management Software:
  - Managing Device sensors on cascaded Devices are not supported currently.
  - 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.

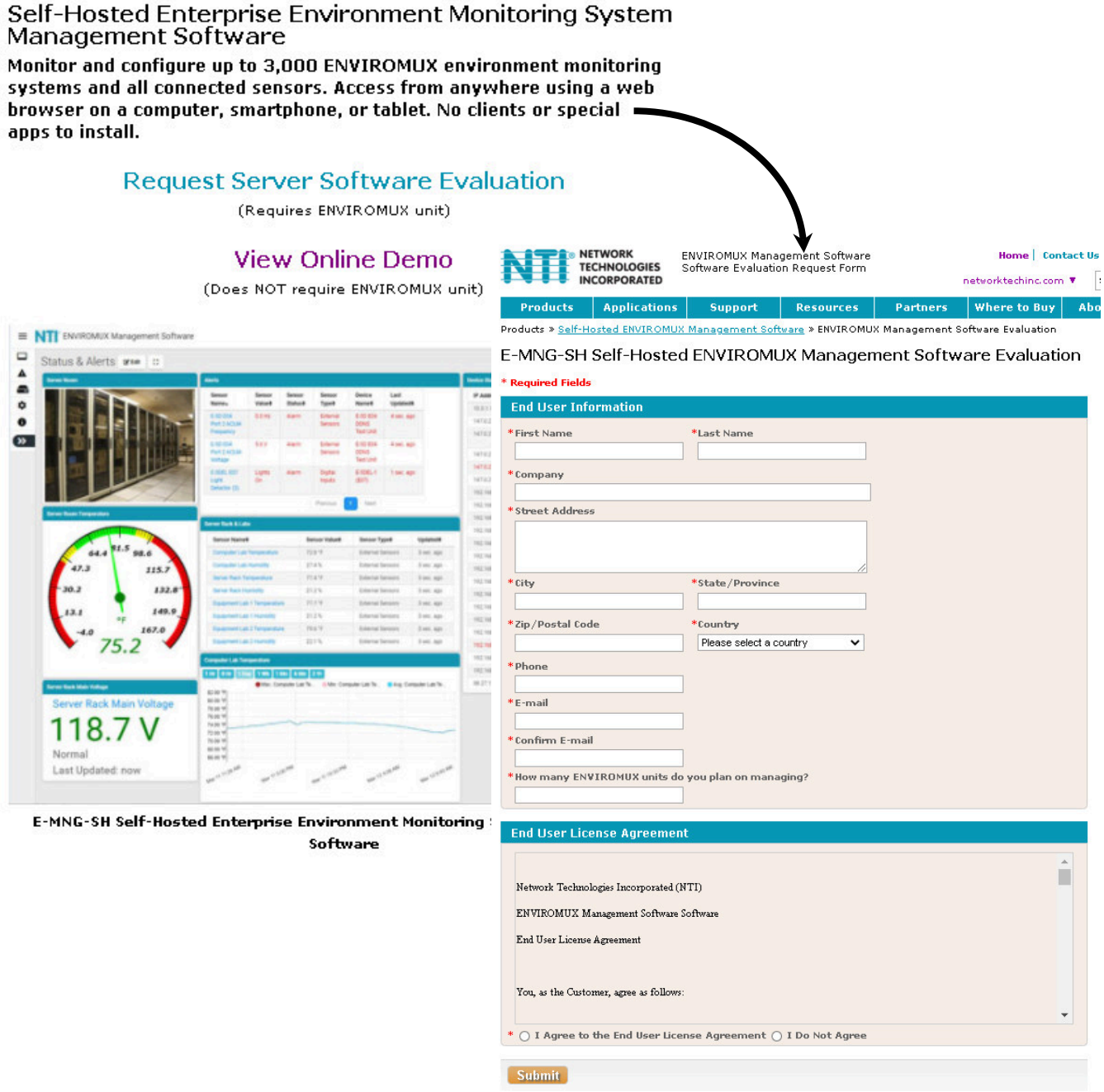


Figure 1- Registration Form

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 ENVIROMUX-Management Software-Installer. (No need for Administrator privileges).

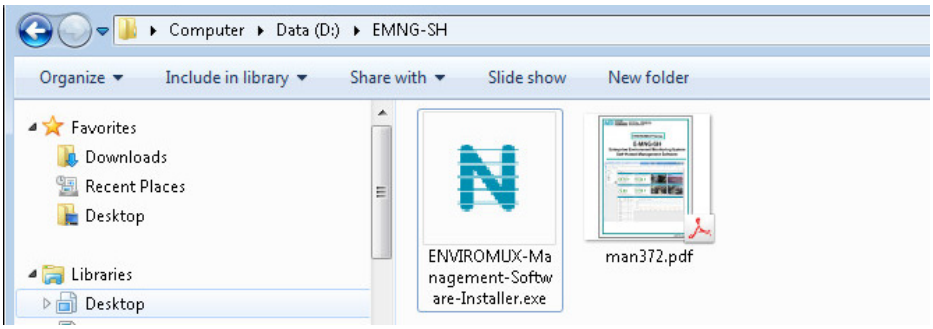


Figure 2- Locate the installation file on your local hard drive

Click to "Agree".

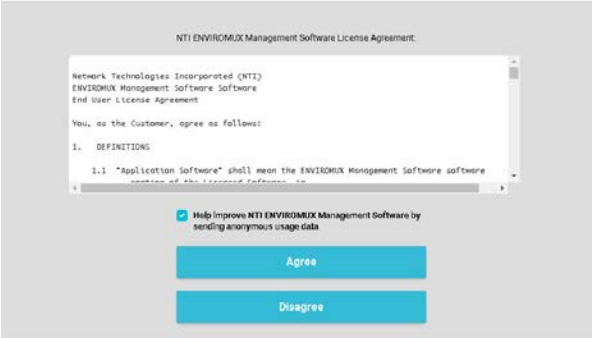


Figure 3- Agree to terms

Choose whether to install the software as an application or as a service. Installing as a service is **strongly recommended**. As an application, you will need to open the application each time the server it is installed on is powered ON, and only then will you be able to access it from other devices. As a service, the software will open and be ready to access any time your power the server ON. If you click "Cancel", the software will not be installed.

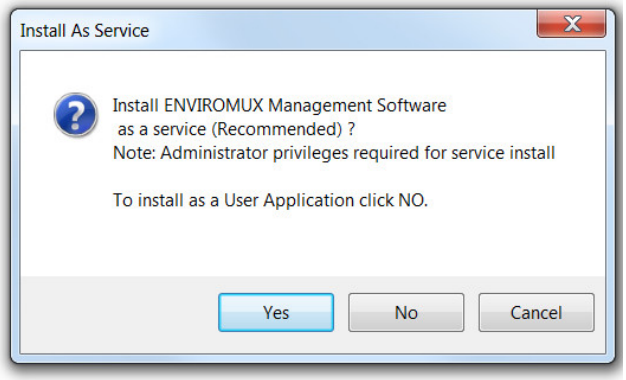


Figure 4- Install software as a service, or an application

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".

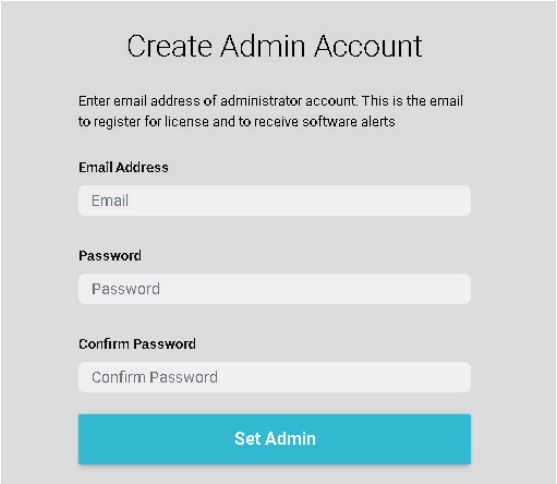
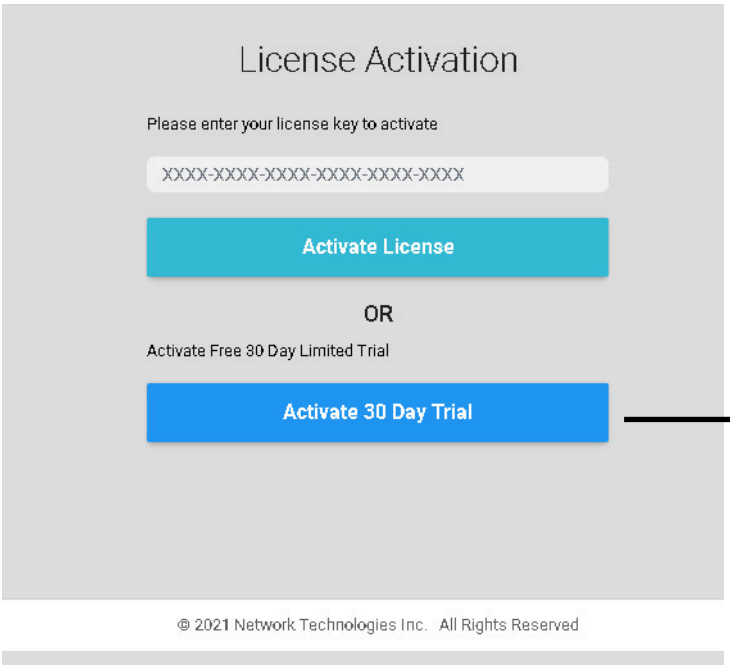


Figure 5- Create Admin login account

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".



The E-MNG-SH server needs to have access to the internet for license activation and trial activation. Offline activation for E-MNG-SHNR is described on page 8.

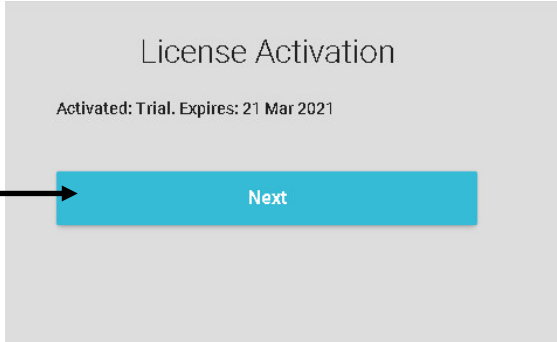


Figure 6- Activation screen

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.

Note: The 30 Day Trial activation will only work if the computer the ENVIROMUX Management Server is on is connected to the internet during the trial activation.

If the license key you received is for the E-MNG-SHNR and you have installed the ENVIROMUX Management Server to a computer that is offline, when you enter the key you will be prompted for "Offline Activation" and a "License File" (see page 8).

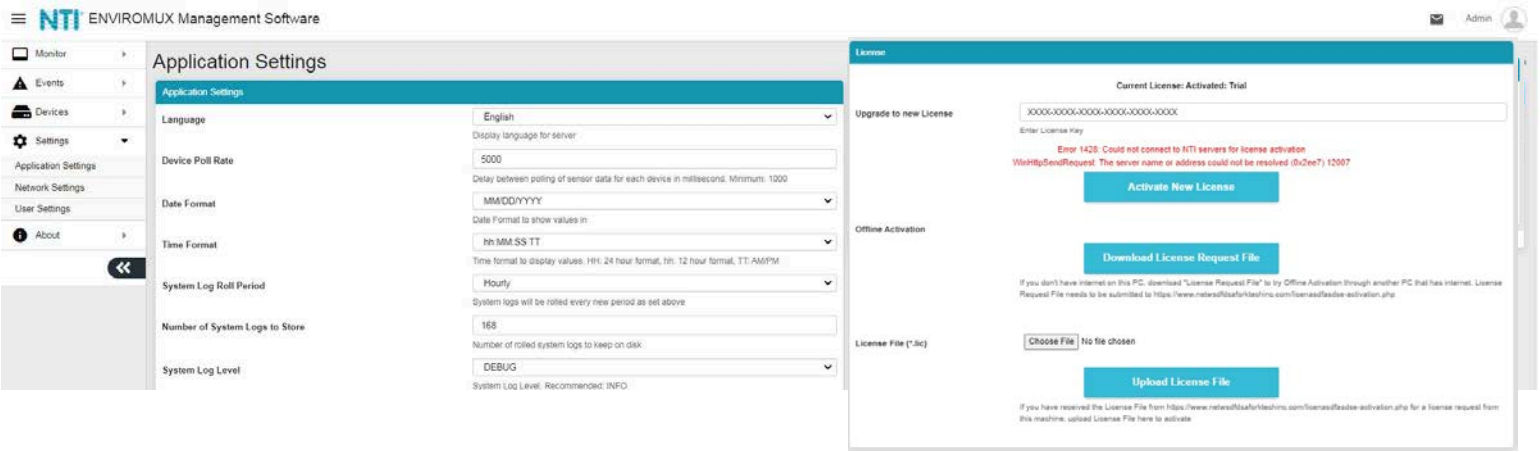


Figure 7- Activate later

If using an E-MNG-SH license, once the software license is activated, the software will renew the license lock 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 the lock. After 5 days of unsuccessful attempts (once each hour), the following screen (right) 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.

Note: To access the activation server an exception may be needed in your firewall by domain name with domain www.networktechinc.com port 443

If exception cannot be added by domain name and the IP address is really necessary then allow 65.243.248.0/25 subnet port 443 (this format automatically includes 65.243.248.0 thru 65.243.248.127 in the exception)

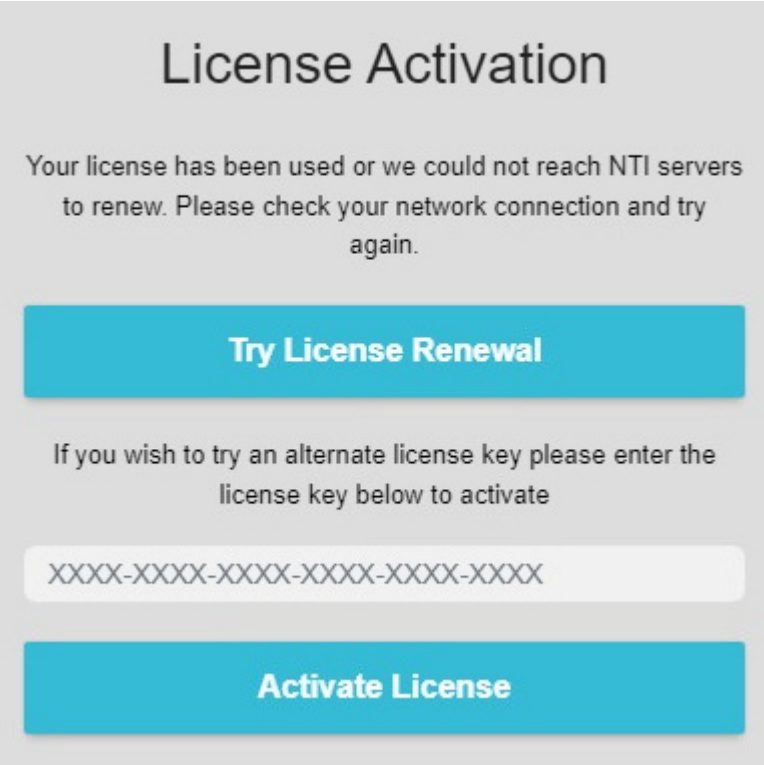


Figure 8- Manually Renew License

Alternatively, you can purchase **E-MNG-SHNR** which is a version of the software that can be activated using internet connection or offline and does not require a license lock renewal in order to continue functioning. (Offline activation for E-MNG-SHNR is described on page 8.) Call **NTI at 330-562-7070** or contact your NTI sales representative for more details.

When installed as a service, if the software crashes for any unforeseen reason, it is set to auto restart up to 3 times within a three hour window. If it crashes more than three times, it will not auto restart. Contact NTI for assistance with any crash.

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 software, with the same license, they will interfere with each other and one of them will get locked out.

Offline Activation

If the license key you received is for the E-MNG-SH**NR**, and you are trying to activate the software offline, when you enter the key the activation will fail and you will be prompted for "Offline Activation" and a "License File" .

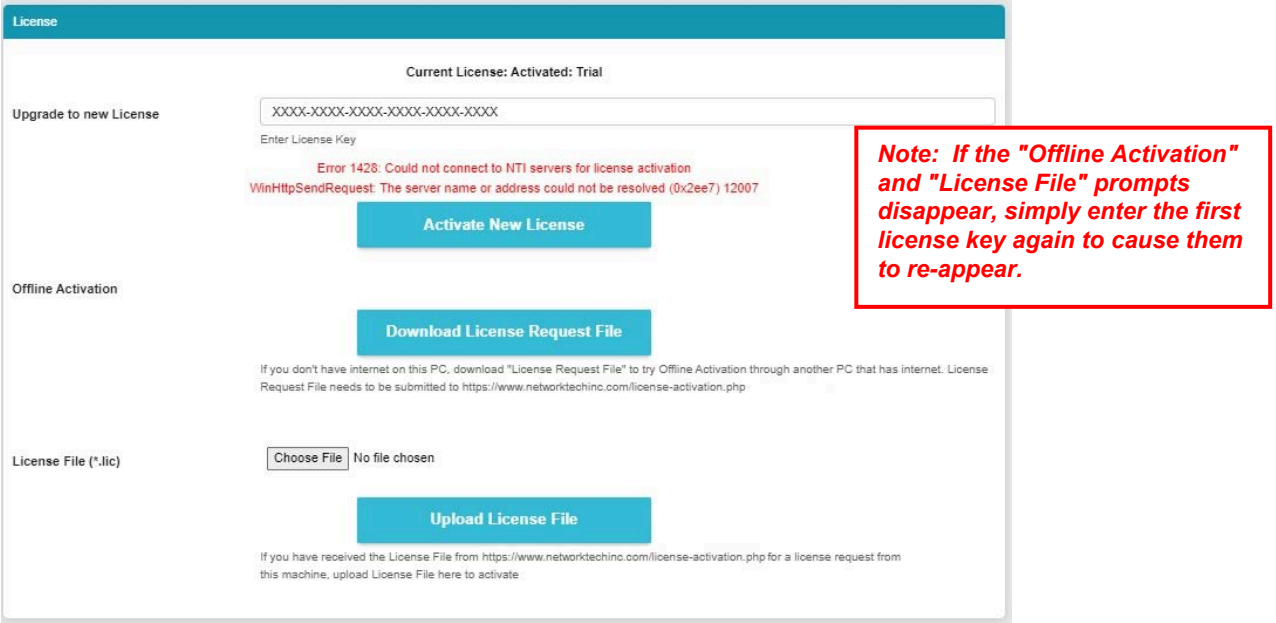


Figure 9- Offline Activation prompts

Click once on "**Download License Request File**". The ENVIROMUX Management Software will automatically save a ***xxxx.req*** (License Request File) to the browser's configured download directory. Transfer that ***xxxx.req*** file to a computer that has internet access that can connect to the NTI website.

From a browser on the internet-connected computer, go to the Offline Activation URL https//www.networktechinc.com/license-activation.php and upload the ***xxxx.req*** file (License Request File). Make sure the computer does not have any internet filters in place that would block a download. You will receive a ***xxxx.lic*** (License File) in return.

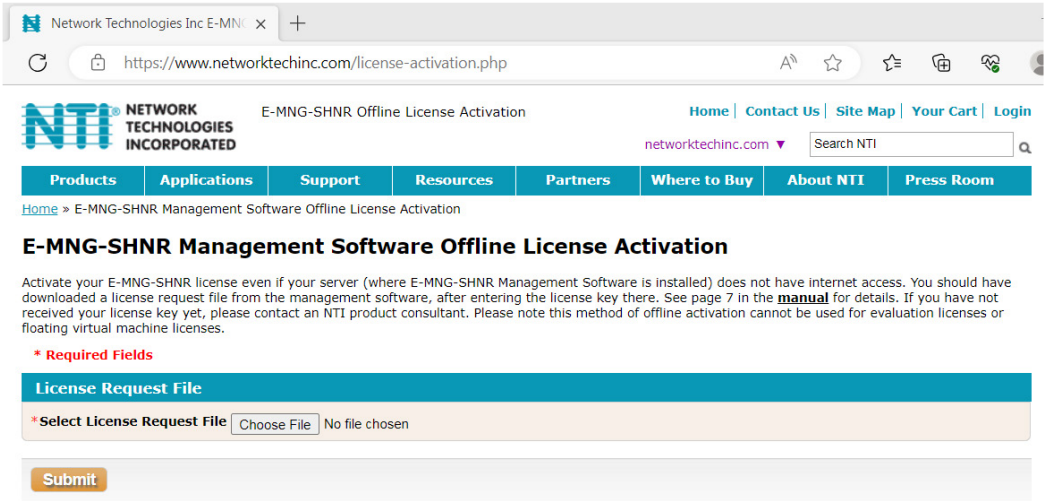


Figure 10- Offline License Activation website

Transfer this License File back to the ENVIROMUX Management Software server, click "Choose File" and select the License File downloaded. Now click once on "**Upload License File**" to upload and activate the ENVIROMUX Management Software license file.

Note: If the "Offline Activation" and "License File" prompts disappear, simply enter the first license key again to cause them to re-appear.

Using Proxy

If your server needs to use a proxy to reach NTI license server or any ENVIROMUX devices, you can setup WinHTTP proxy and software will use this proxy server to reach the NTI license server..

The *Netsh.exe* tool is used to configure a system-wide static proxy. You can use commands in the netsh winhttp context to configure proxy and tracing settings for Windows HTTP. The Netsh commands for winhttp can be run manually at the netsh prompt or in scripts and batch files.

To configure a proxy server by using the Netsh.exe tool

To use the Netsh.exe tool to configure a proxy server, follow these steps:

1. Select **Start** > **Run**, type cmd, and then select **OK**.
2. At the command prompt, run the following command and then press <Enter>.

```
netsh winhttp set proxy <proxyservername>:<portnumber>
```

In this command, replace <proxyservername> with the fully qualified domain name of the proxy server.
Replace <portnumber> with the port number for which you want to configure the proxy server.

For example, replace <proxyservername>:<portnumber> with proxy.domain.example.com:80.

For more on setting up the winhttp proxy, please refer to the below link:

Microsoft Netsh winhttp proxy

Don’t forget to restart E-MNG-SH service after setting the proxy

Installation Continued

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 11). This is the protocol used for communication (along with HTTPS).

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 (provided the server is ON and the E-MNG-SH is running).

Users with only "Operator" privileges can access the E-MNG-SH and view the monitored Devices, but they cannot change any settings. For more on privileges, see page 23.

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.

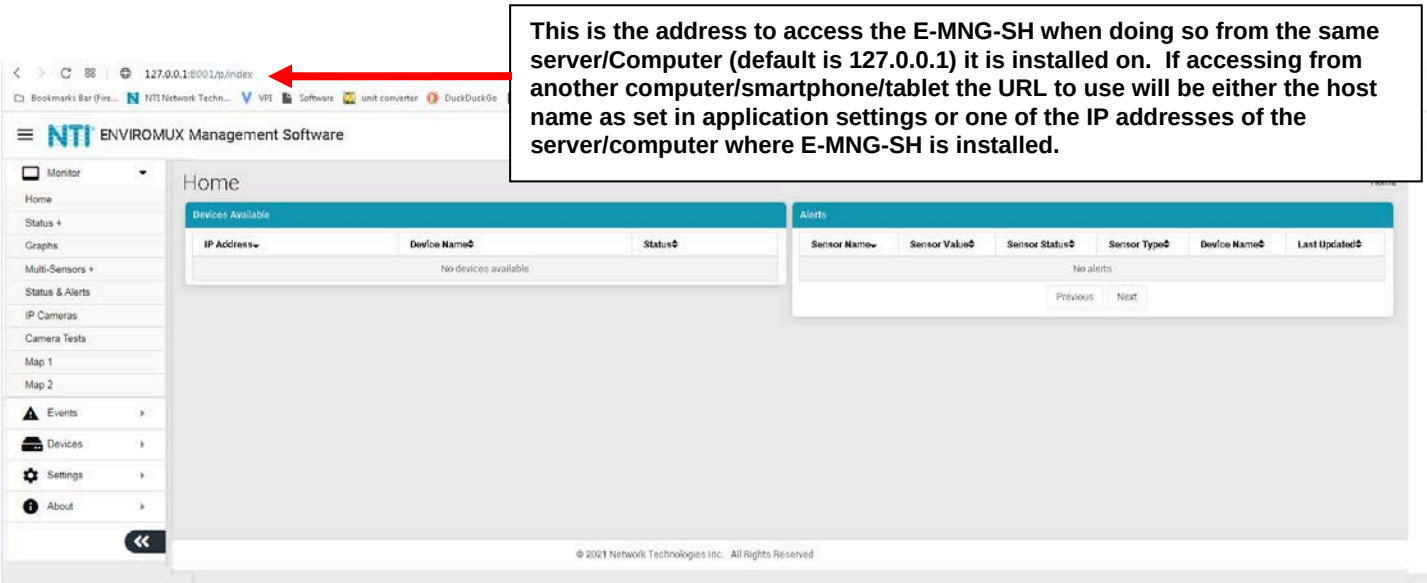


Figure 11- View of the Home screen

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

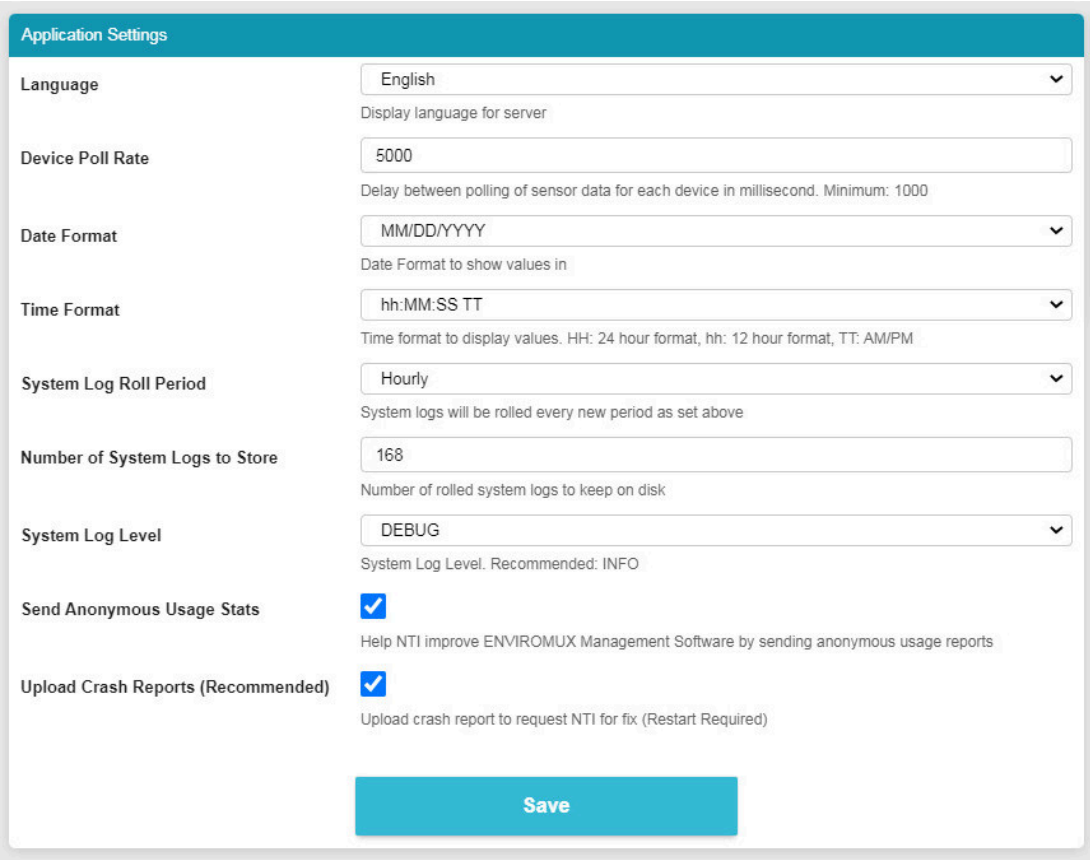


Figure 12- Application Settings

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

The Network Settings page provides settings for all of your connectivity options, including General Network Settings, Email/SMTP Settings, LDAP Authentication Settings, SMS Settings and Certificate Settings.

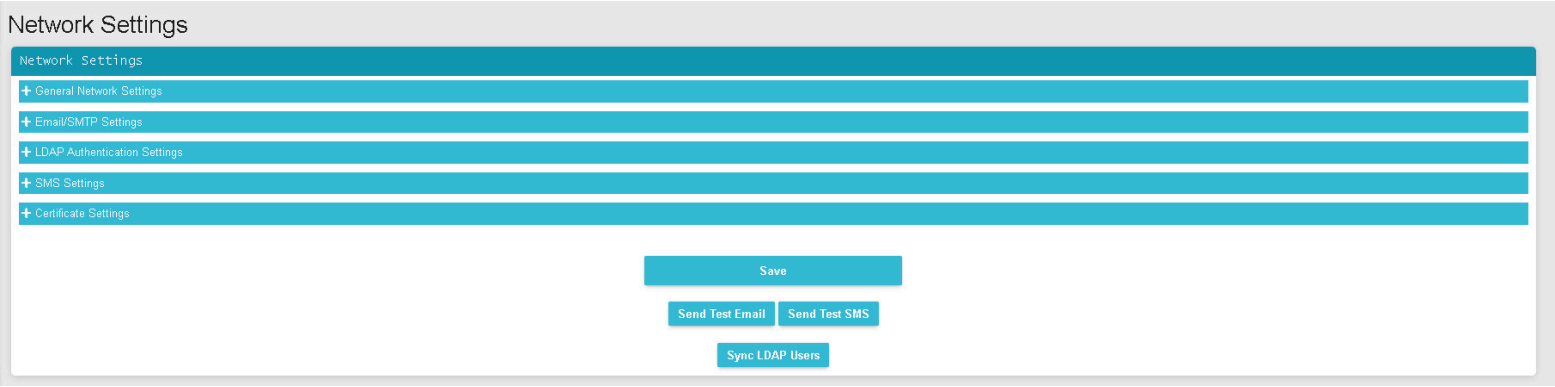


Figure 13- Network Settings Page

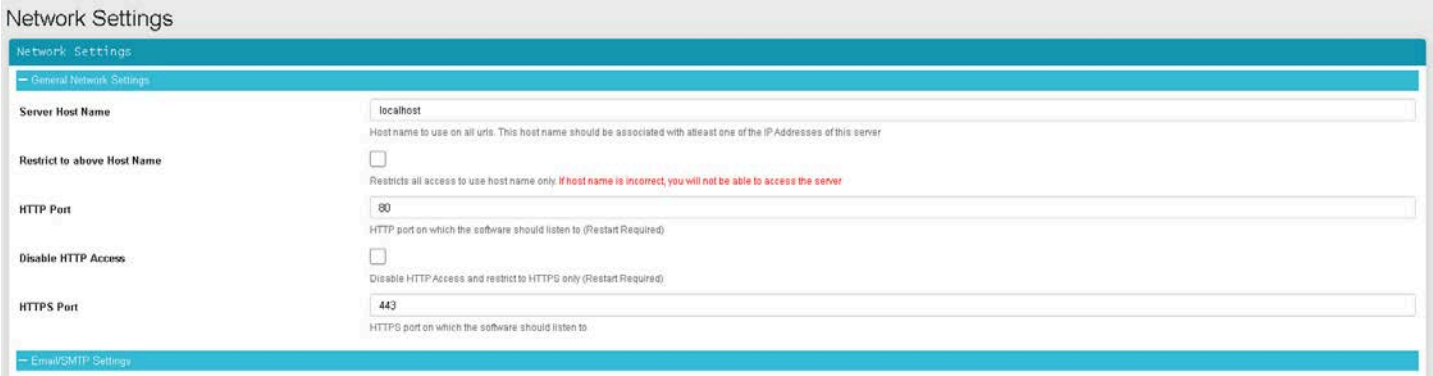


Figure 14- General Network Settings

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 page 22)**
Restrict to 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.
Disable HTTP Access	Place a checkmark in this box (default is empty) if you want to restrict access to HTTPS only. If a checkmark is placed in this box, a restart will be required for it to take effect.
HTTPS Port	HTTPS port on which the Server will be connected with.

Note: If HTTP Access is disabled, only then HSTS (HTTP Strict Transport Security) will be enabled. Some other web security headers like Frame Options, CORP and CSP will **also be enabled by default.**

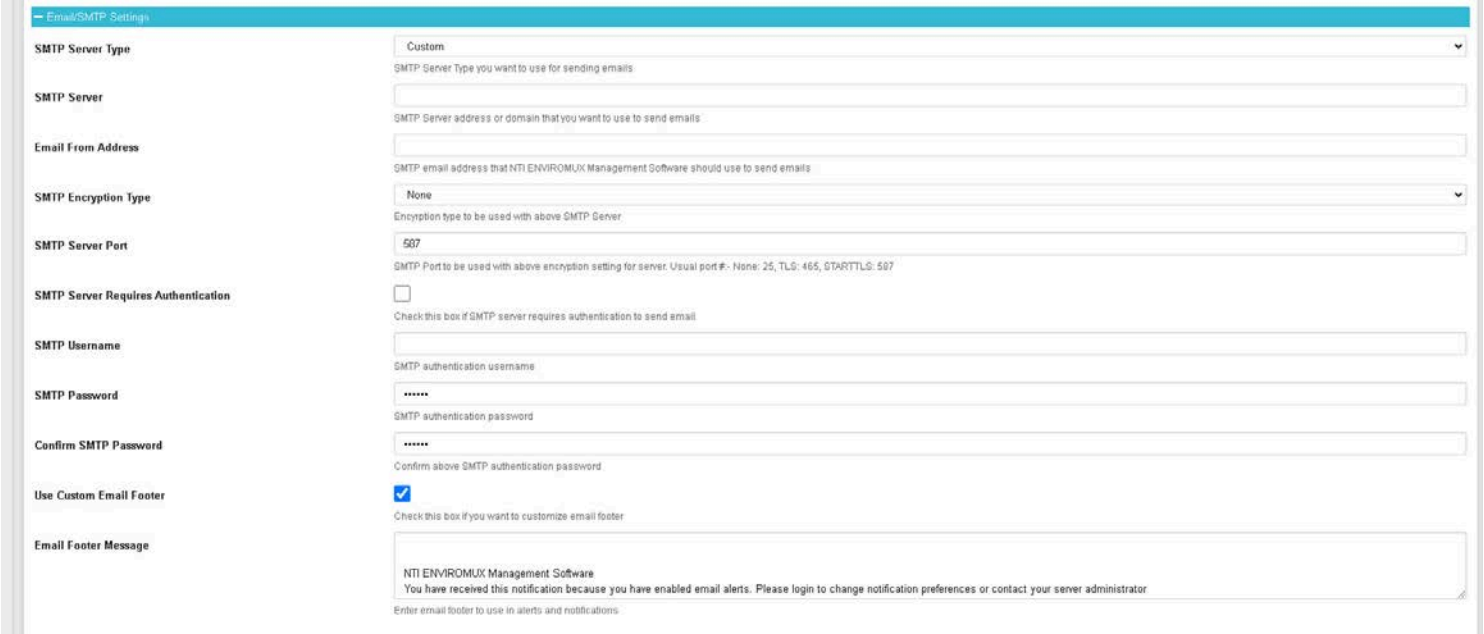


Figure 15- Email/SMTP Settings

Network Setting	Description
SMTP Server Type	Select "Custom" or "Gmail" (Most of the settings that follow are only for a "Custom" SMTP server)
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 with STARTLS encryption)
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
Use Custom Email Footer	Place a checkmark in the box if you want to customize the Email footer
Email Footer Message	When a checkmark is in the “Use Custom Email Footer” option, a box appears where you can enter a message that will appear in the footer of all alerts and notifications sent out by the management software.

Gmail SMTP Server

When "SMTP Server Type" is set to Gmail, a valid Gmail address must be entered into the "Email From Address" field. With that field filled, click the "Authorize with Google" button. Then follow the prompts to get Gmail authorized.

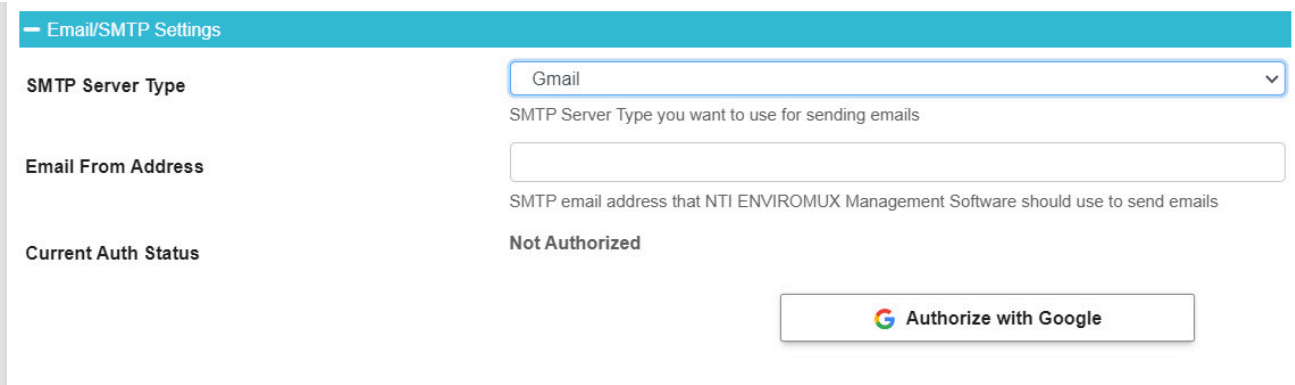


Figure 16- SMTP Server Type- Gmail

"Current Auth Status" will indicate the Authorization status for Gmail. If Authorization is expired, it will automatically renew unless authorization has been revoked by the user. If not authorized or auto renew of authorization is failing, you have to Reauthorize again by using the below procedure (shown in screenshots). Any email failures and associated reasons will be logged in the *system.log* file

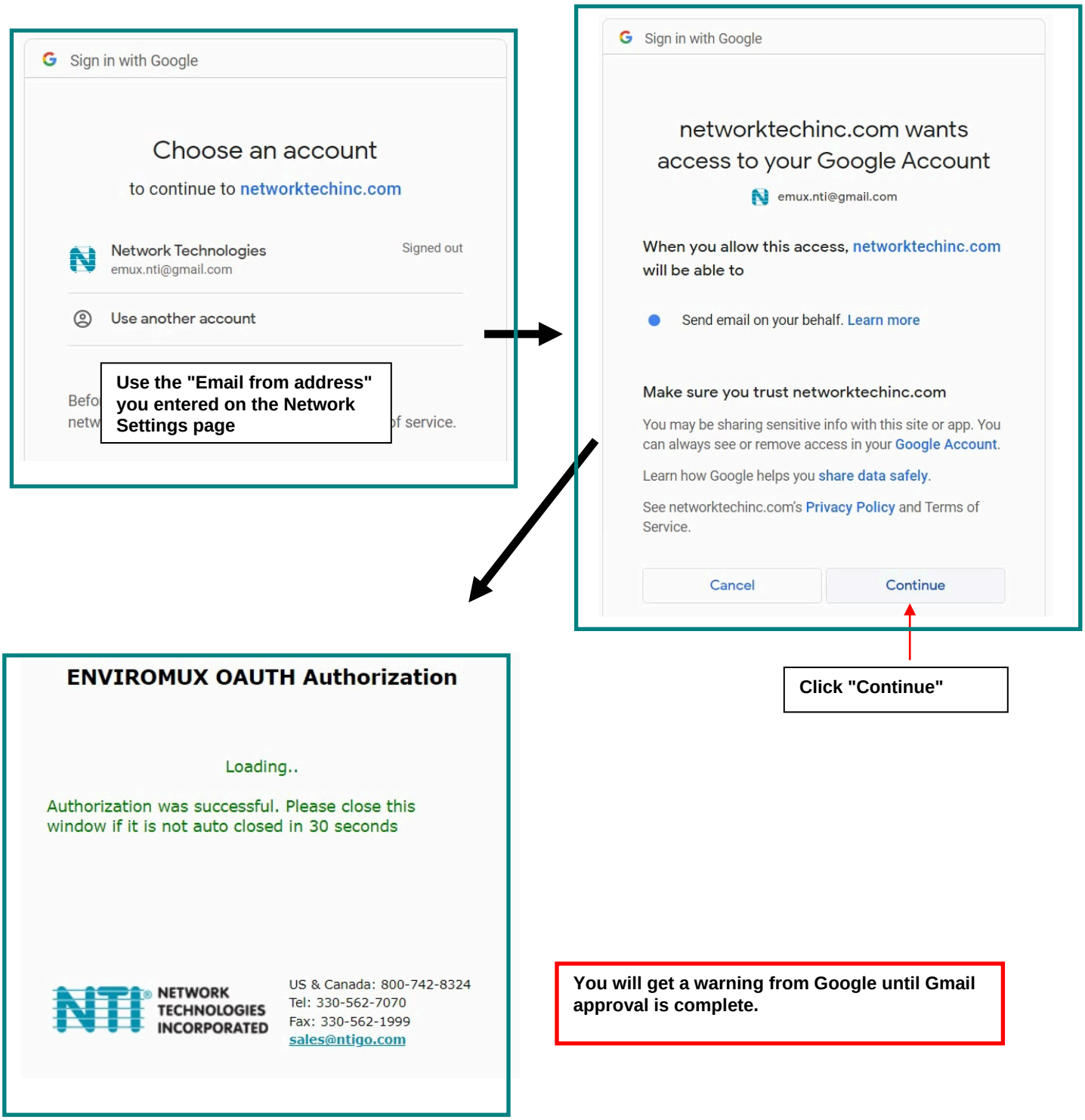


Figure 17- Steps in getting Gmail Authorization

LDAP Settings

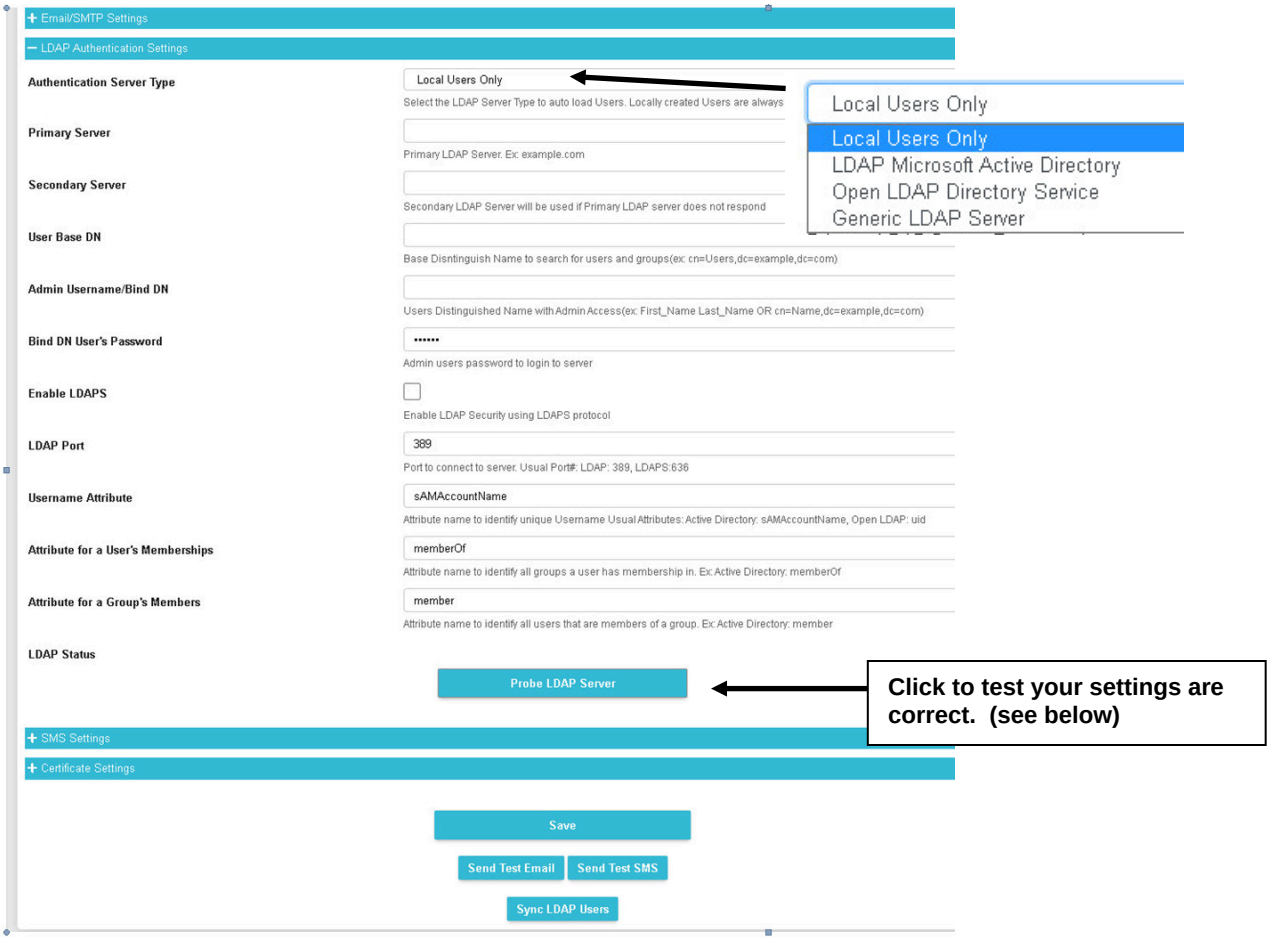


Figure 18- LDAP Authentication Settings

LDAP Authentication Settings	Description
Authentication Server Type	Select Local Users Only, LDAP Microsoft Active Directory, Open LDAP Directory Service or Generic LDAP Server
Primary Server	Enter a valid primary LDAP server address (ex. Example.com)
Secondary Server	Enter a valid secondary LDAP server address in case the primary LDAP server does not respond
User Base DN	Enter the Base Distinguished Name to search for users and groups (ex. Cn=users, dc= example, dc=com
Admin Username/Bind DN	User's Distinguished Name with admin access (ex. First_Name Last_Name, OR cn=name, dc=example, dc=com
Bind DN User's Password	Admin user's password to log into LDAP server
Enable LDAPS	Place a checkmark inside to enable the LDAP Security using LDAPS protocol
LDAP Port	Enter the port number to connect to the server. Usual Port for LDAP: 389, LDAPS: 636
Username Attribute	Attribute name to identify unique Username Usual Attributes: Active Directory: sAMAccount Name, Open LDAP: uid
Attribute for a User's Memberships	Attribute name to identify all groups a user has membership in. (ex: Active Directory: memberOf)
Attribute for a Group's Members	Attribute name to identify all users that are members of a group. (ex: Active Directory: member)
LDAP Status	Click on "Probe LDAP Server" to test your settings are correct. Probe will do connection test and provides available Users and Groups. This will not store the available users.

At the bottom of the page is a button for "Sync LDAP Users". Use this to load Users and Groups from LDAP server to E-MNG-SH software to allow authentication. Any LDAP User properties can be set in E-MNG-SH software (Ex mobile number) but it may get overridden by values received from LDAP Server (if set in LDAP server). When changing user properties, we recommend doing so in the LDAP server.

The E-MNG-SH has been tested to work with Microsoft LDAP and Open LDAP. The E-MNG-SH will automatically sync with the configured LDAP server twice each day, starting 10 hours after the last settings were saved.

Note: When LDAP Authentication has over 30 LDAP errors within 8 hours, the management server will block LDAP requests for 3 days.

The E-MNG-SH software does not support two users or groups with the same Name (CN), even if they differ in DN.

All users, Local or LDAP users, should have unique email addresses.

Support for LDAP Groups

When an LDAP user belongs to multiple LDAP groups, the group with highest privilege will be assigned to this user.

When any properties (Ex: Enable Email) change for any LDAP Group, such properties saved on a Group member will be overwritten.

By default, all LDAP users get "Read Only Auth". Admins can edit Auth Level of any LDAP group in the E-MNG-SH software which gets applied to Group members.

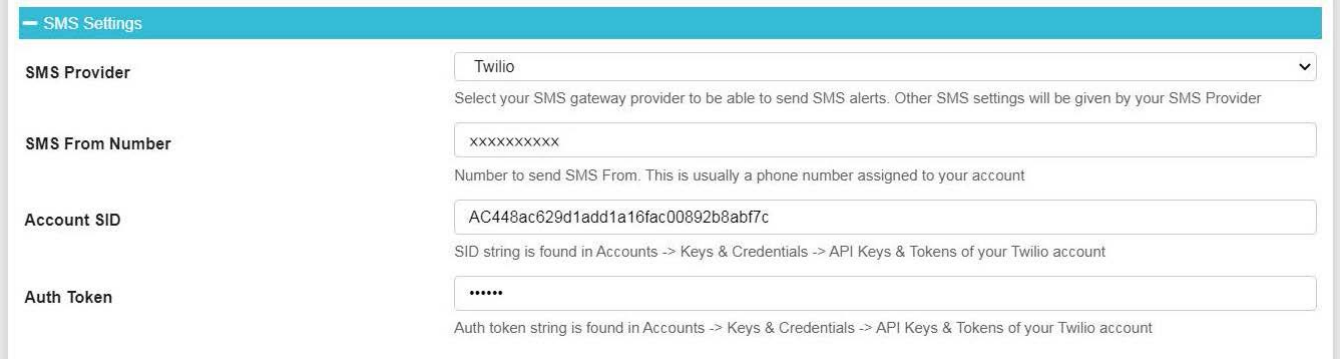


Figure 19- SMS Settings for Twilio

SMS Settings

Network Setting	Description
SMS Provider	Click the down arrow to select your SMS Provider. Choose between Sinch, Twilio and None.
SMS From Number	Enter the phone number provided by your SMS Provider.
Account SID/Service Plan ID	Enter the ID number provided by your SMS Provider.
Auth Token/Bearer API Token	Enter the API Token provided by your SMS Provider.

Tips for Twilio SMS Signup:

If asked for Programming Language use "Other", for integration use Own Code and No hosting options is required.
You will be assigned a phone number for your account or you have to sign up for a phone number with relevant authorizations for your country of Choice. For example in USA you have to sign up for A2P 10DLS to send SMS to unverified numbers. If you want to use a short code you have to sign up for relevant short code within Twilio

Get your Account SID and Auth Token and enter in E-MNG-SH software
You can find these details in your Twilio Console page -> Account Info

By default Twilio allows sending SMS to numbers only in the home country you selected during signup.
To send internationally you have to select the desired countries in Geo Permissions by going to
Console -> Develop -> Messaging -> Settings -> Geo Permissions

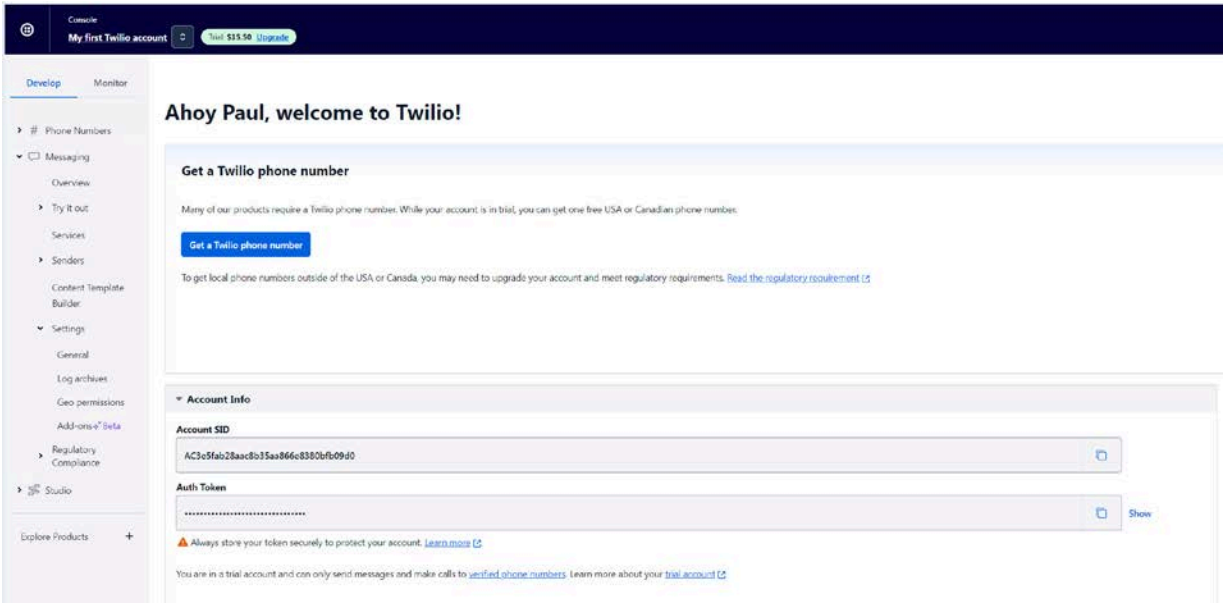


Figure 20- Twilio Console Page

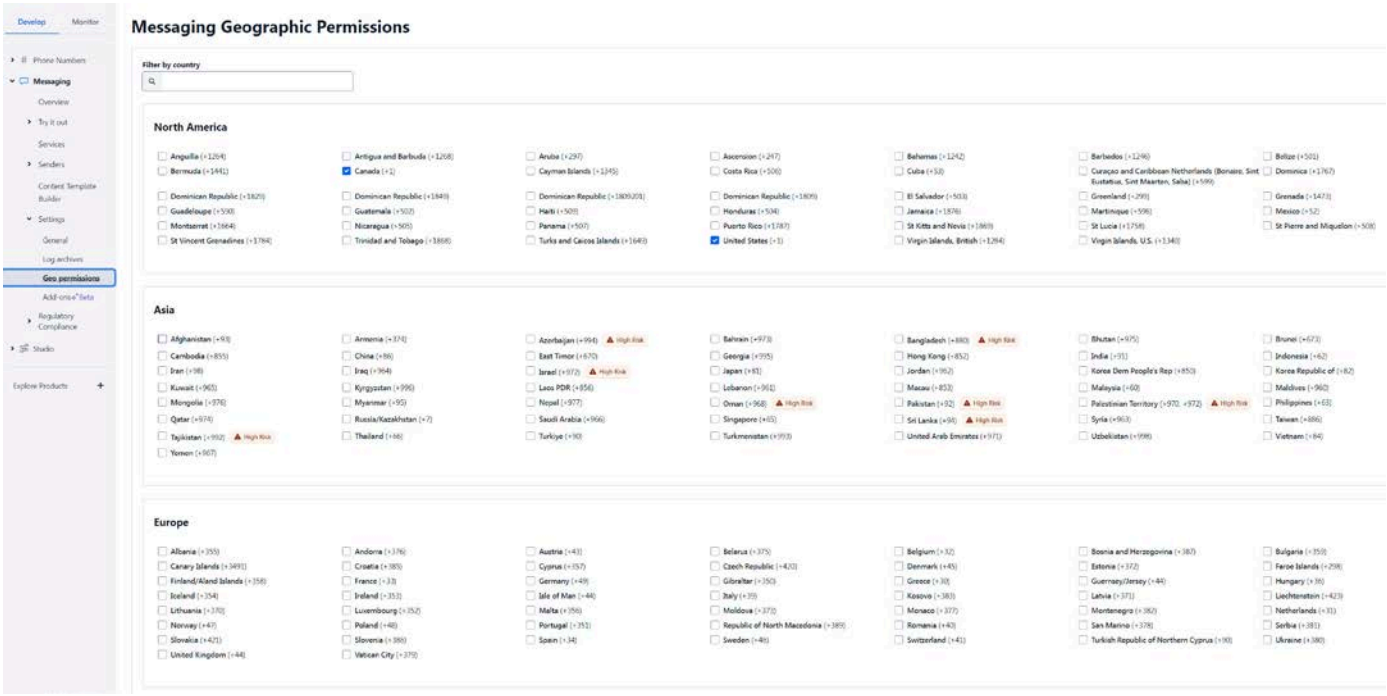


Figure 21- Twilio- Setting Geo Permissions

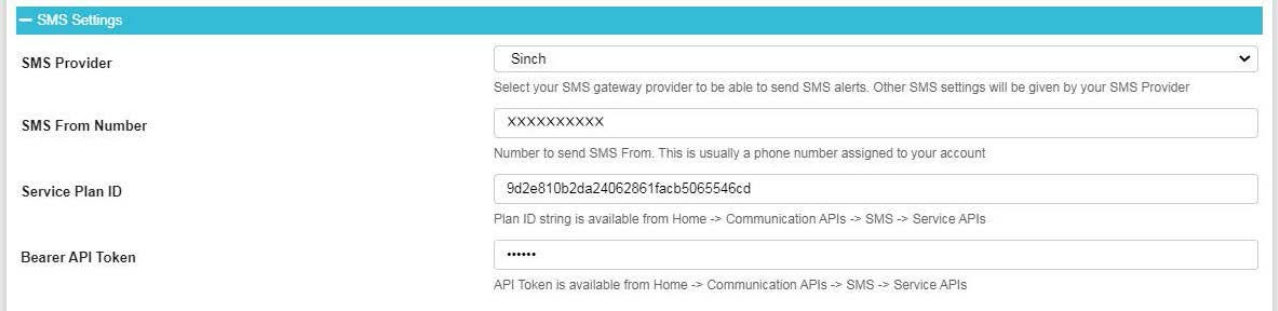


Figure 22- SMS Settings for Sinch

Click "Send Test SMS" after saving your SMS Settings. If there is an SMS delivery failure, reasons for it will be logged in *system.log*. If the SMS delivery failed and it shows successful delivery in *system.log*, please check your SMS Provider account, as it may be held up due to a billing/authorization issue.

Certificate Settings

Menu changes based on the option selected. E-MNG-SH provides several ways to install an x509 certificate to work with HTTPS secure browsing.

a. Self-Signed with Signer Option as E-MNG-SH Signed:

This is the most simple option to setup and is the default. E-MNG-SH will generate the key, CA certificate and Server certificate as needed. Users only have to Download and install the CA certificate provided by E-MNG-SH

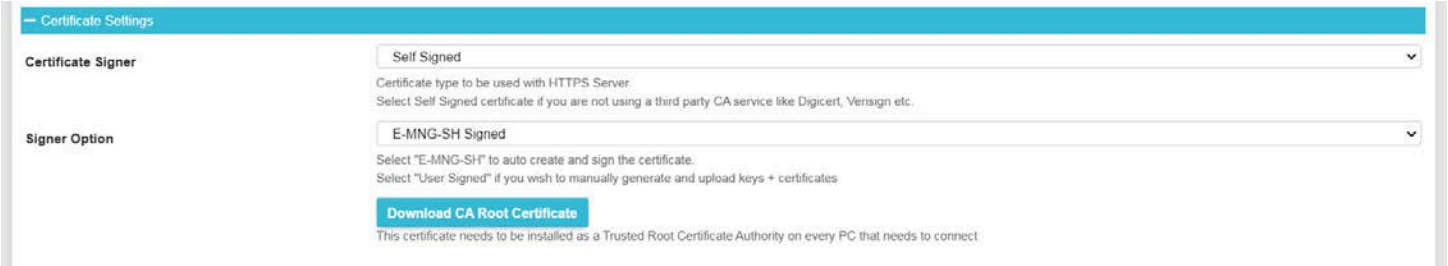


Figure 23- Self-signed Certificate Setting Options

b. Self Signed with User Signed Certificate:

E-MNG-SH understands you want to generate your own key, server certificate and CA certificate. You can use a procedure similar to How to Create x509 Certificate (Section I) to generate all 3 files and upload them to E-MNG-SH. Here we assume the CA certificate you upload is already set as Root Certificate for the users connecting to server.

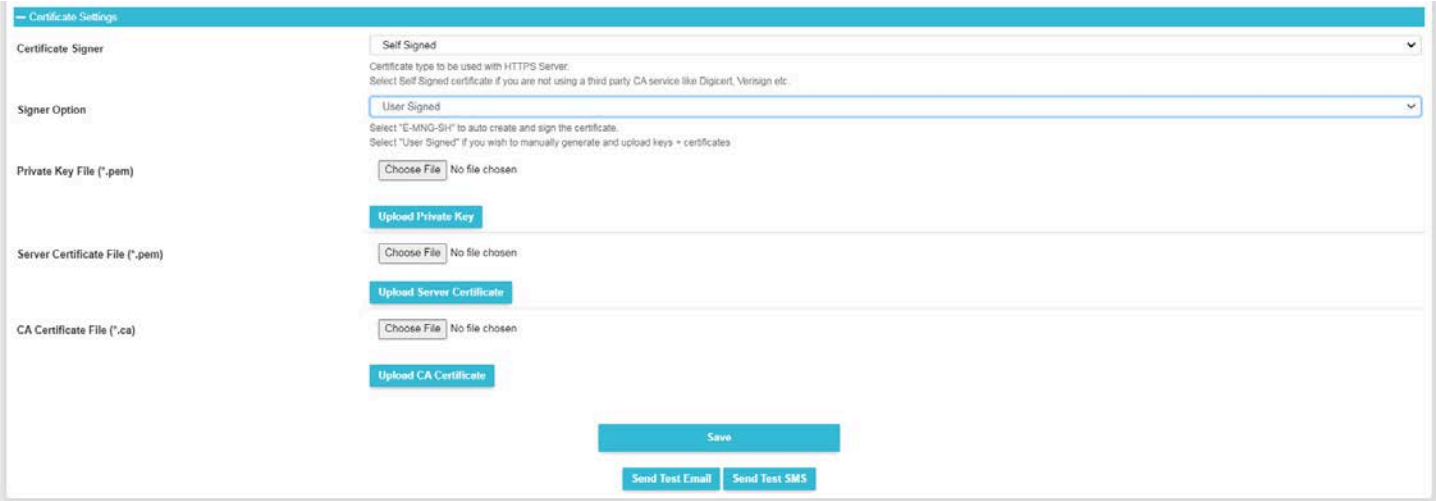


Figure 24- Self-signed and User Signed Setting Options

c. CA Signed with Generate CSR option:

Here you will be using a third party CA whose certificate will already be uploaded to your user's PC's/Devices like Digicert, Verisign etc. In this case the key file will be generated by E-MNG-SH. These external CA expect only a CSR file, containing server details, to generate the server certificate for you. You can get this CSR file by filling out the required details. You have to upload this CSR file to your CA and get your server certificate as well as their CA certificate. Upload both certificates to E-MNG-SH and you are set.

Please note: You have to upload the server certificate for the same CSR you previously generated meaning you cannot regenerate a CSR after a server certificate has been created. Otherwise the key will mismatch the server certificate.

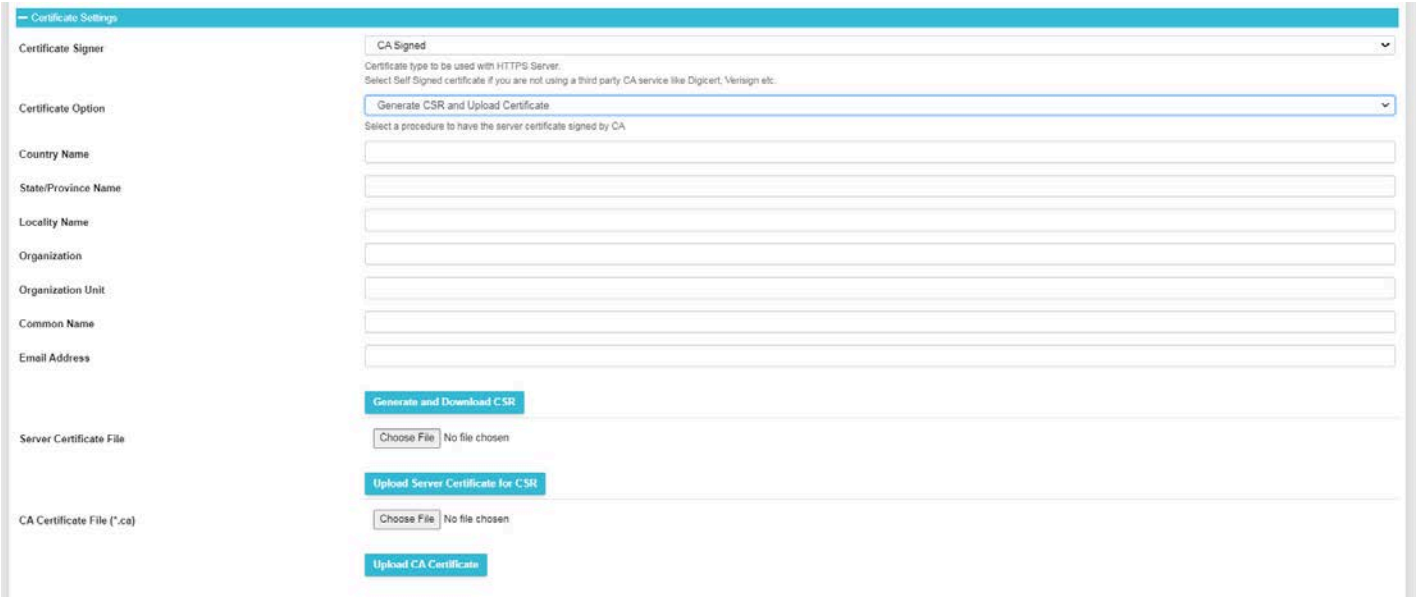


Figure 25- CA Signed and Generate CSR Setting Options

d. **CA Signed with Uploading keypair & Certificate:**

This case is same as step C, except you will have to generate the key yourself and also generate the CSR for it using a step similar to How to Create x509 Certificate (Section II) . You will have to upload Keypair, server certificate and CA certificate in this case.

Figure 26- CA Signed with Upload Keypair and Certificate Setting Options

Please note if any certificate options are changed, it requires the E-MNG-SH server to be restarted to load new certificate details. Please refer to the Shutting Down/Restarting section in this manual

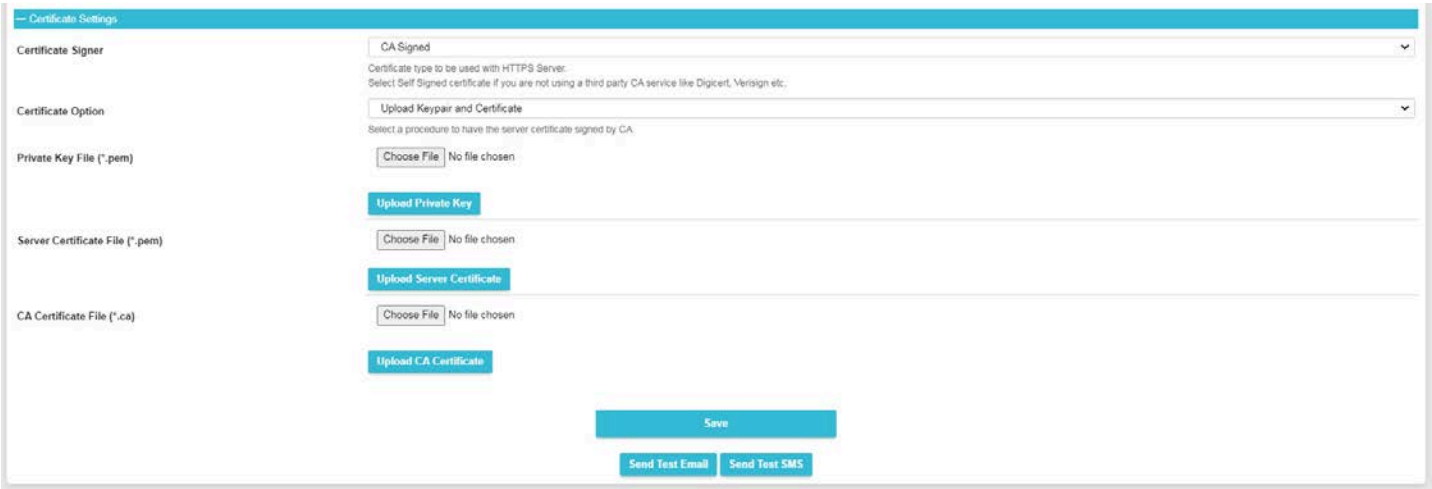


Figure 27- CA Signed Certificate Setting Options

Network Setting	Description
Certificate signer	Certificate type to be used with HTTPS Server. Select self-signed certificate (x509) if you are not using a third party CA service like Digicert, Verisign, etc. CA signed certificate will provide more options.
Signer Option	Select between E-MNG-SH Signed and User Signed (If "User Signed" is selected- the fields above will appear)
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.

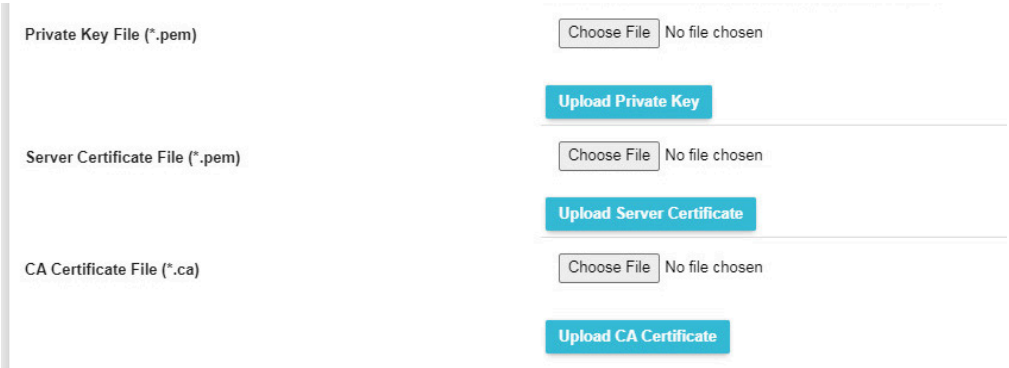
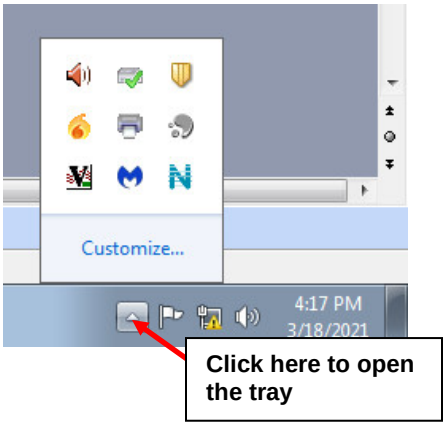


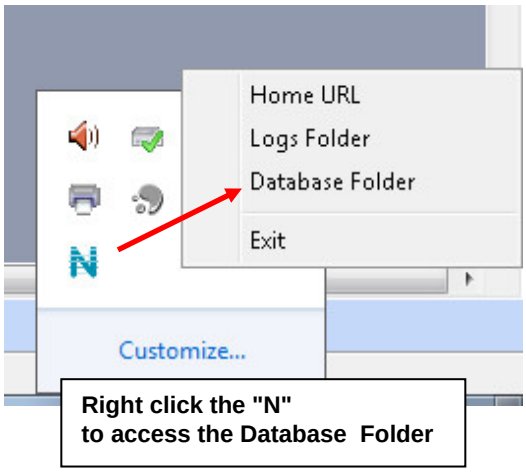
Figure 28- Security Configuration-X509 Certificate

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 "Server Host Name" on page 12), 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.

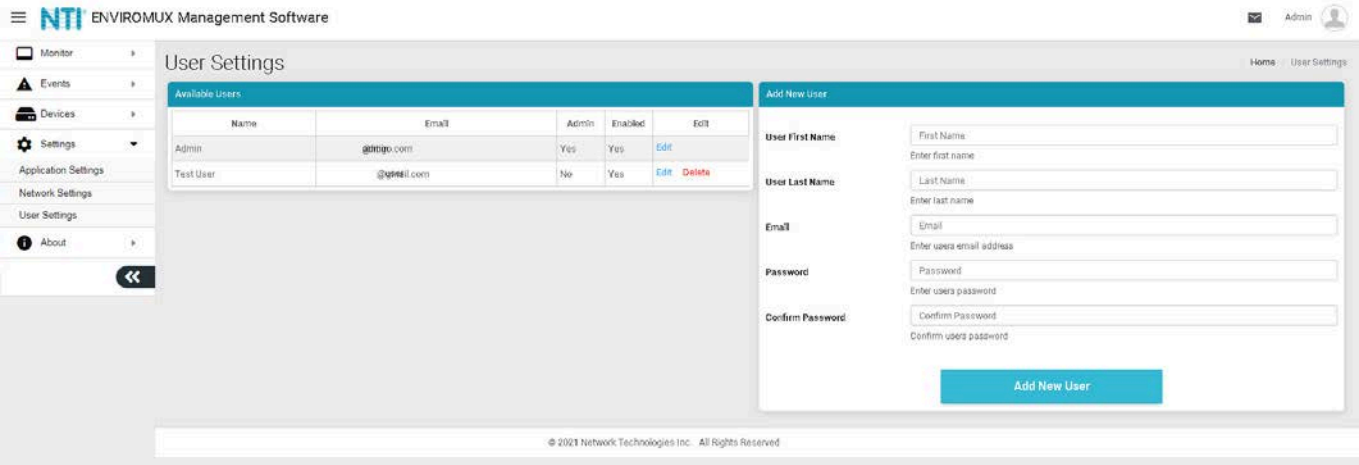


Figure 29- User Settings for Adding Users

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. The operator can also change relay settings on the E-xD units being monitored, and acknowledge alerts from the sensors connected to them.
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

Enter a phone number (or two) if you want messages sent to this user's telephone via SMS (see page 16).

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 43).

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".

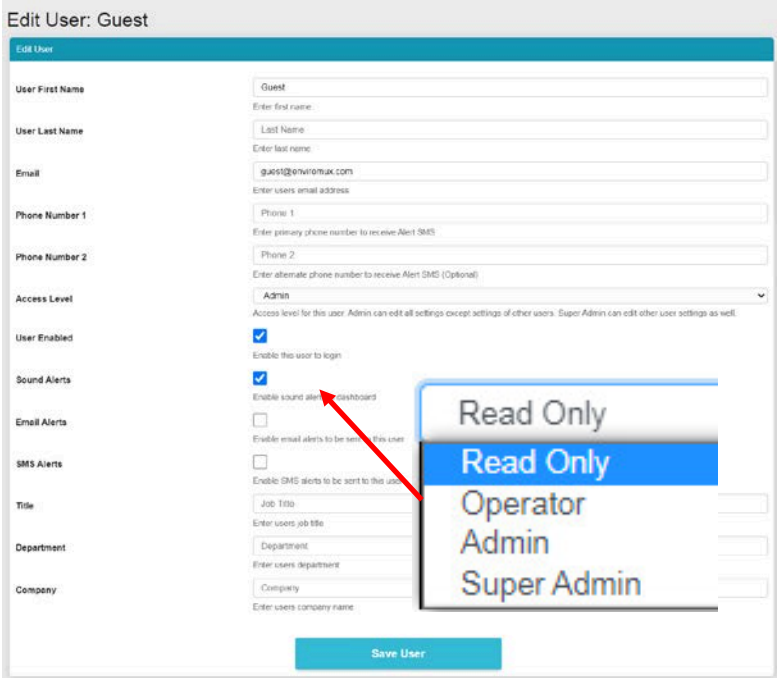


Figure 30- Edit user settings

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.

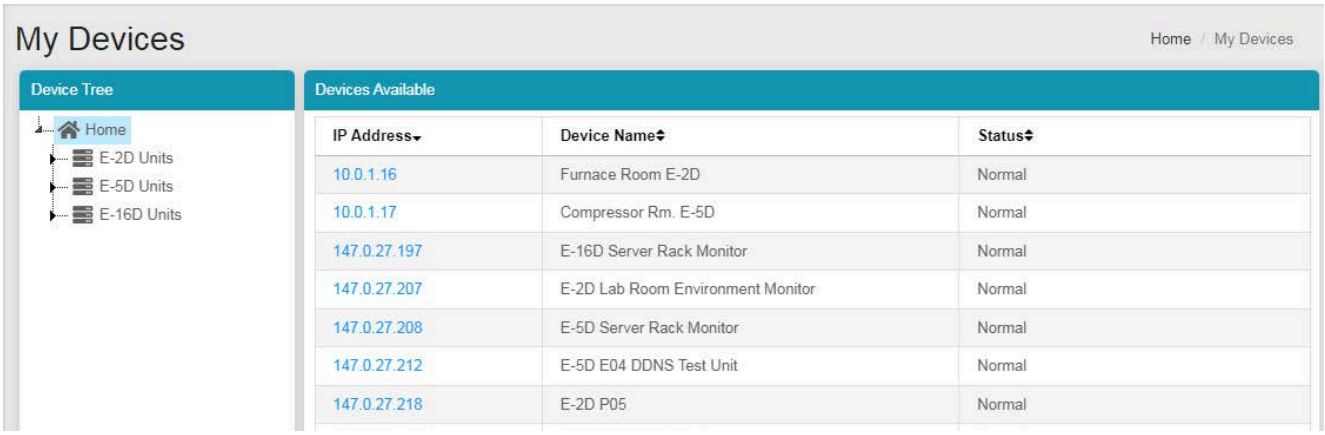


Figure 31- My Devices List

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

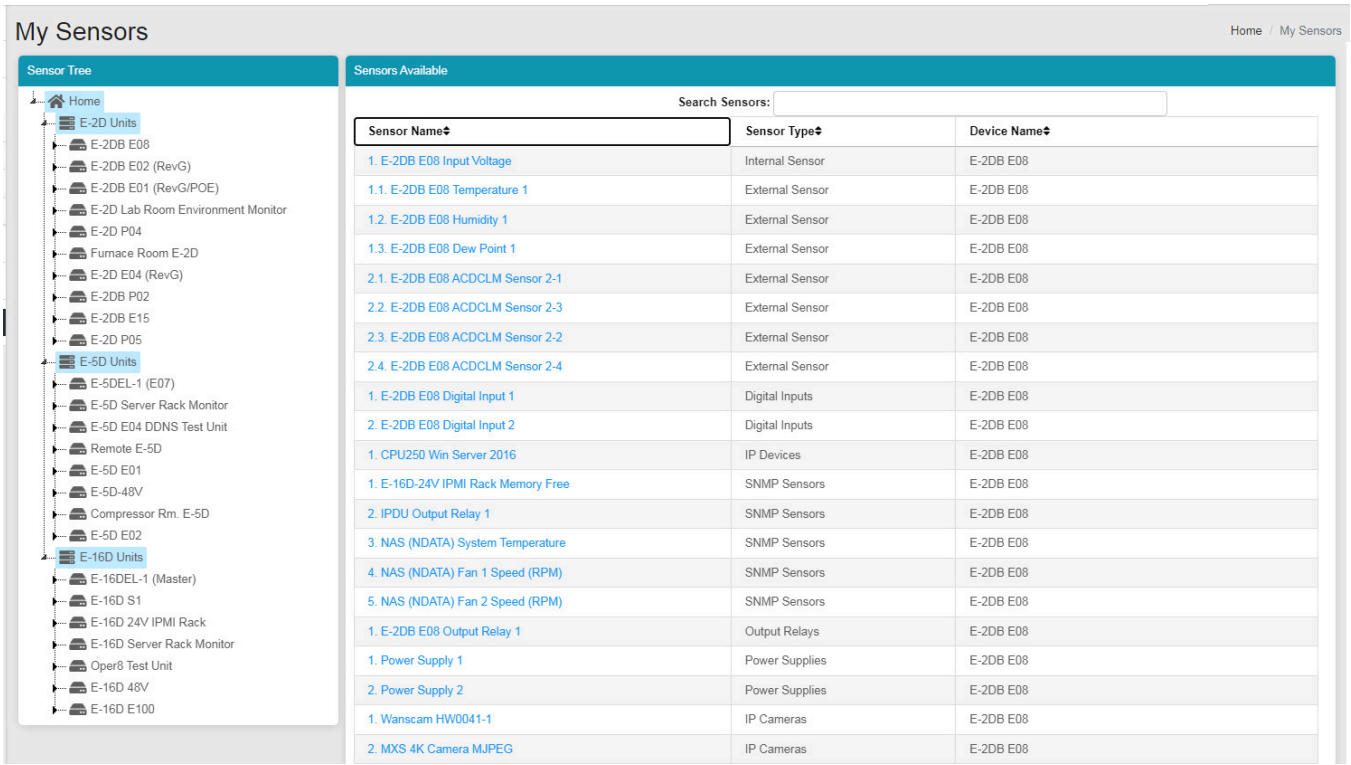


Figure 32- My Sensors List

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.

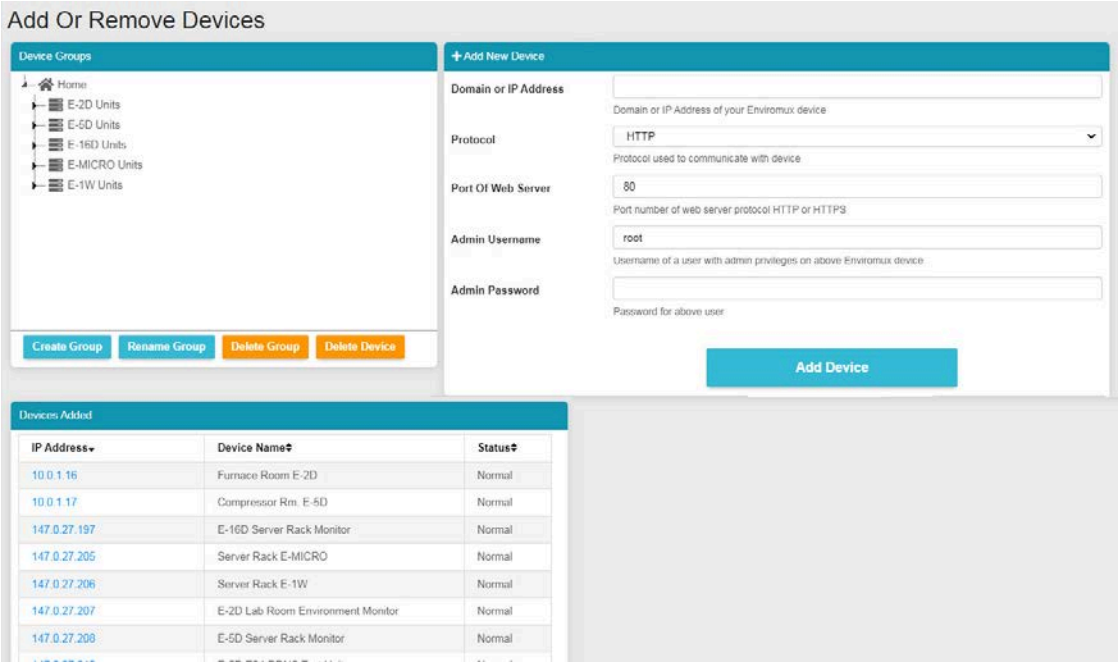


Figure 33- Add or Remove Devices

Lastly, use the "Maps" page to upload an unlimited number of images of a map, building, or server room (for example). 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.

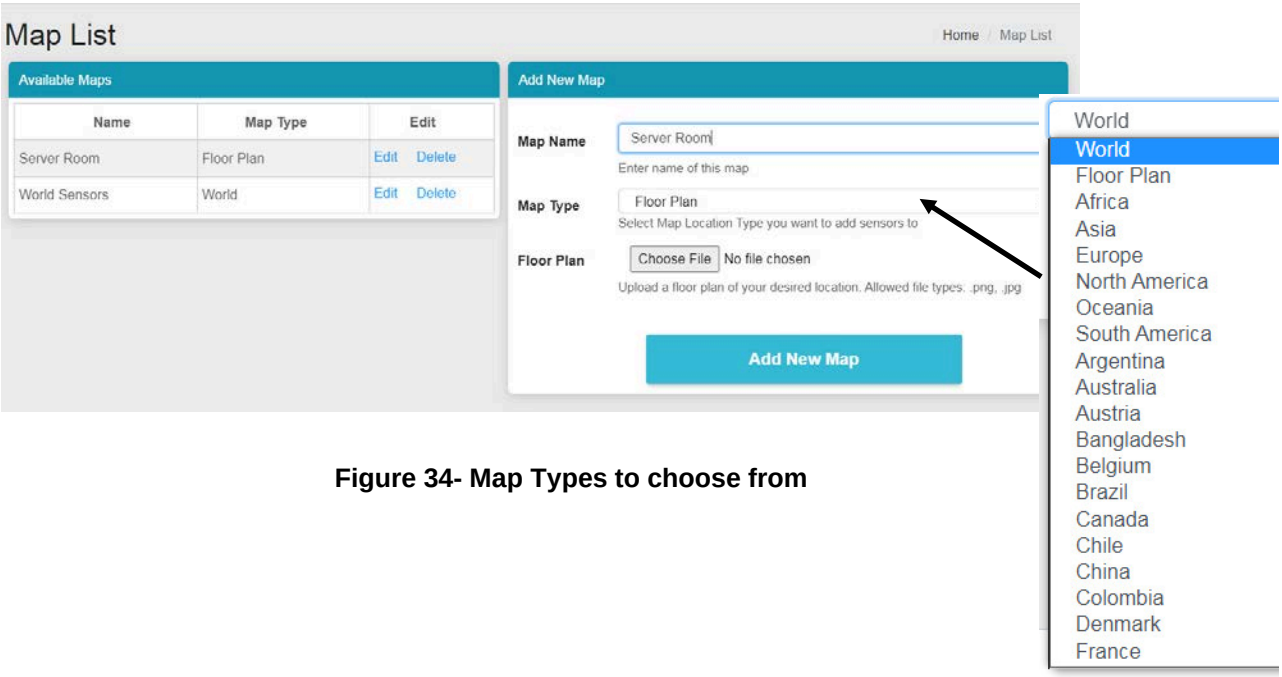


Figure 34- Map Types to choose from

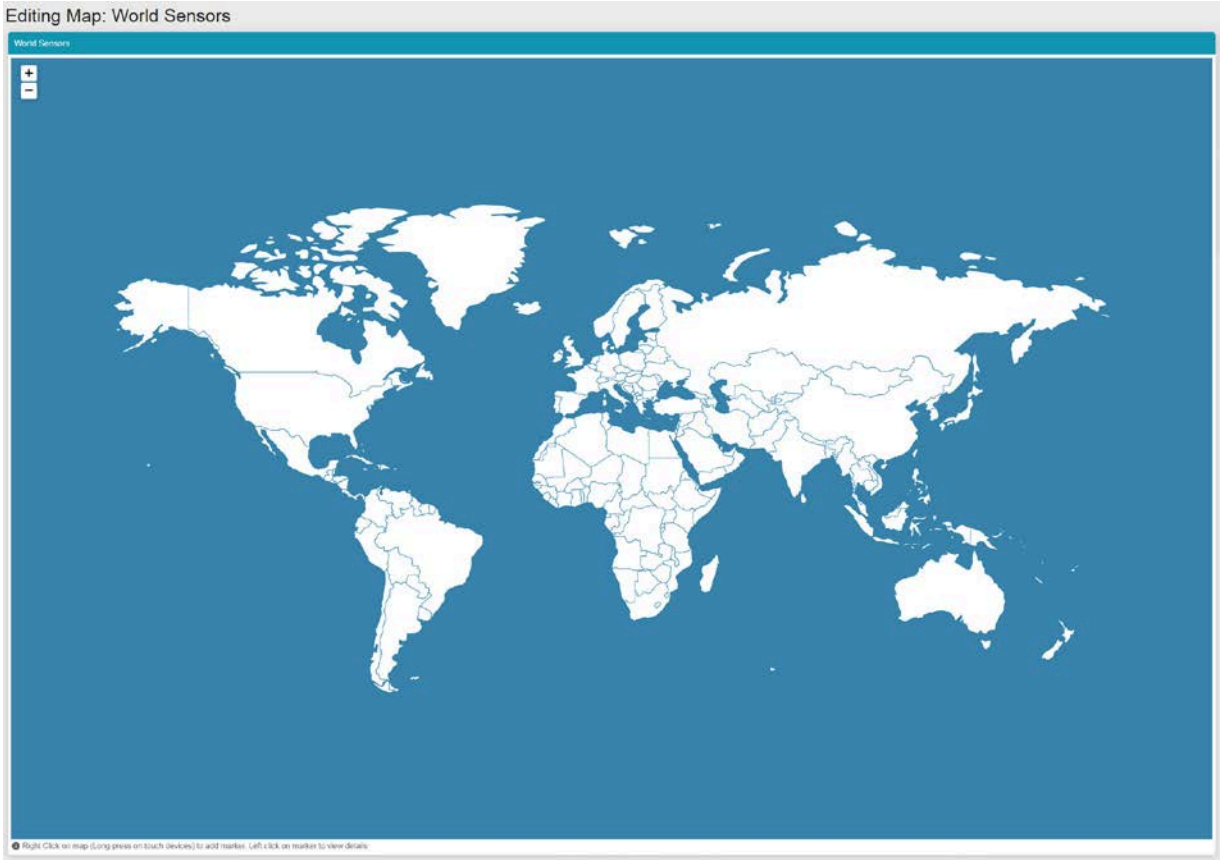


Figure 35- World map provided

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.

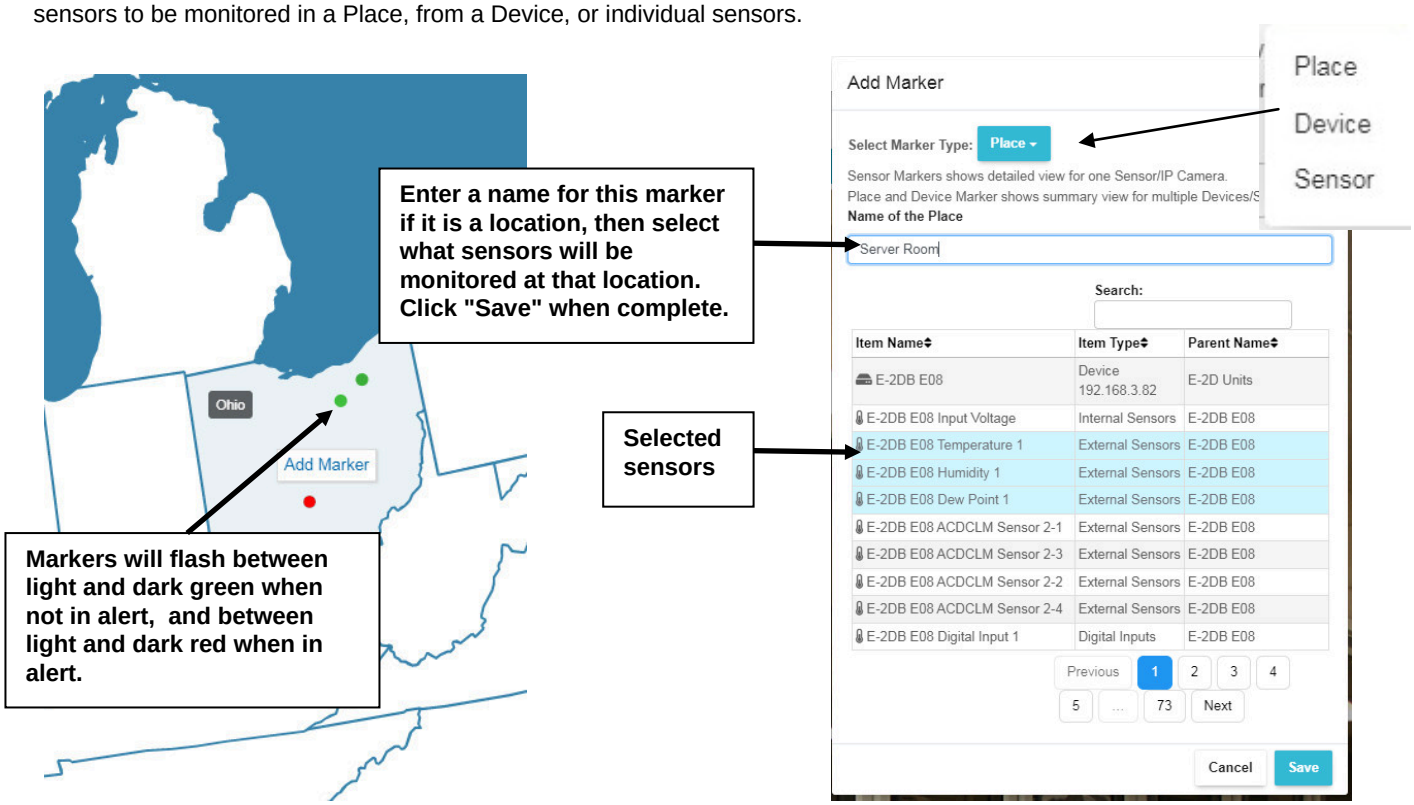


Figure 36- Loading maps and placing markers

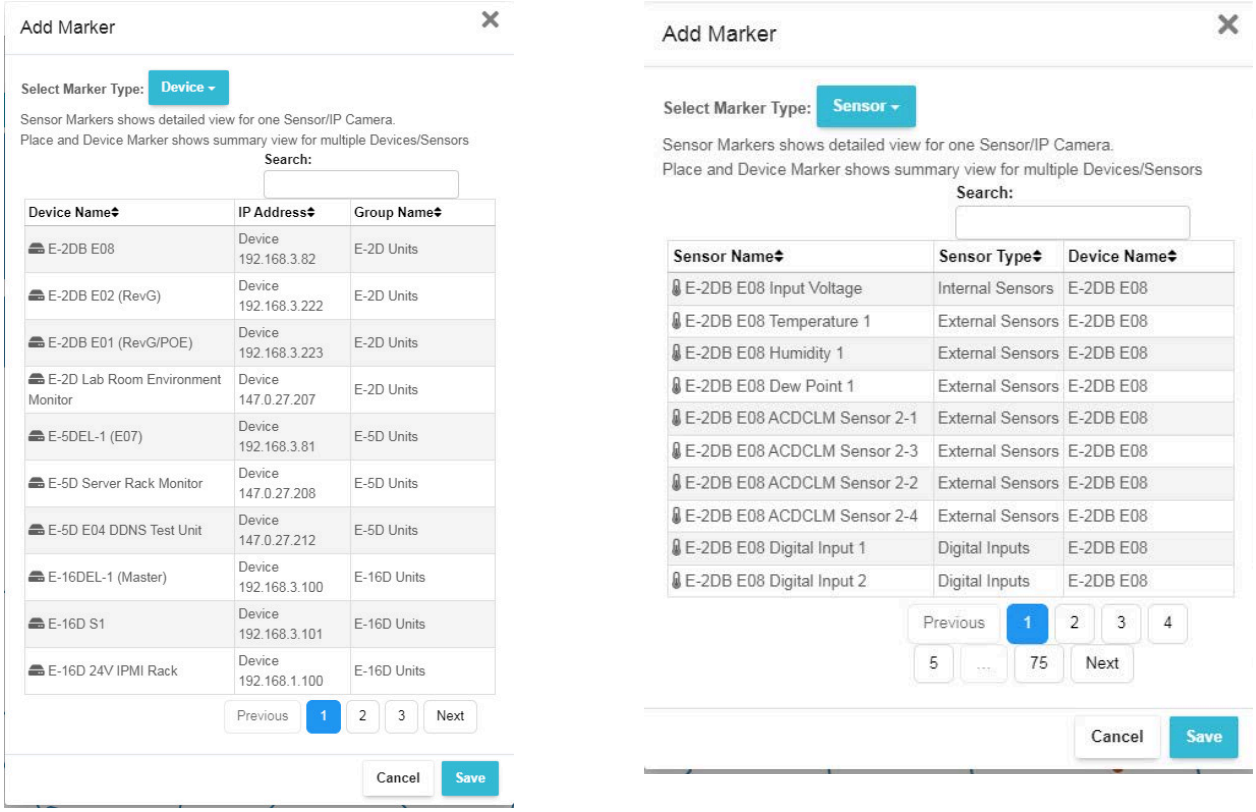


Figure 37- Markers for Device or Sensor

With your maps and markers defined, you can create a Dashboard and add your map to it (see page 36) .

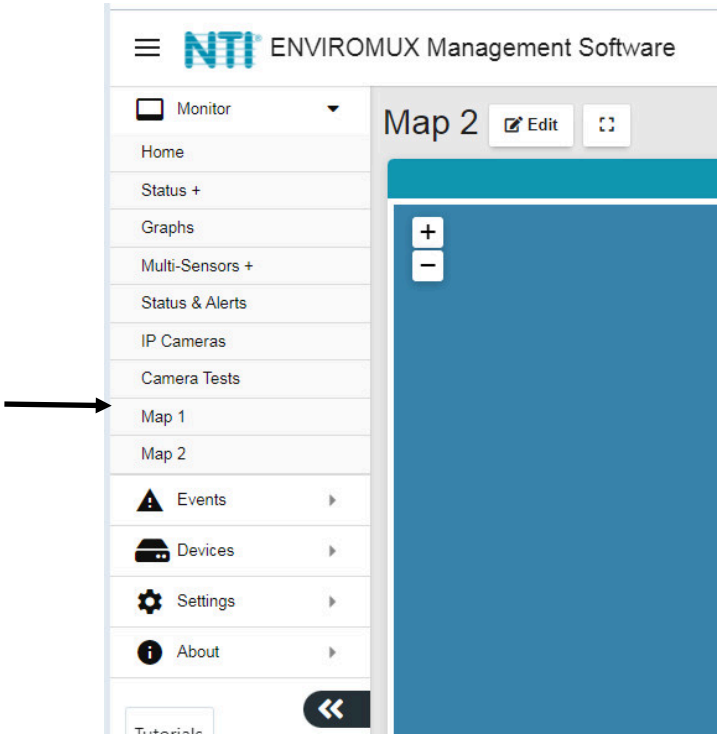


Figure 38- Use a configured map to monitor select sensors

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.

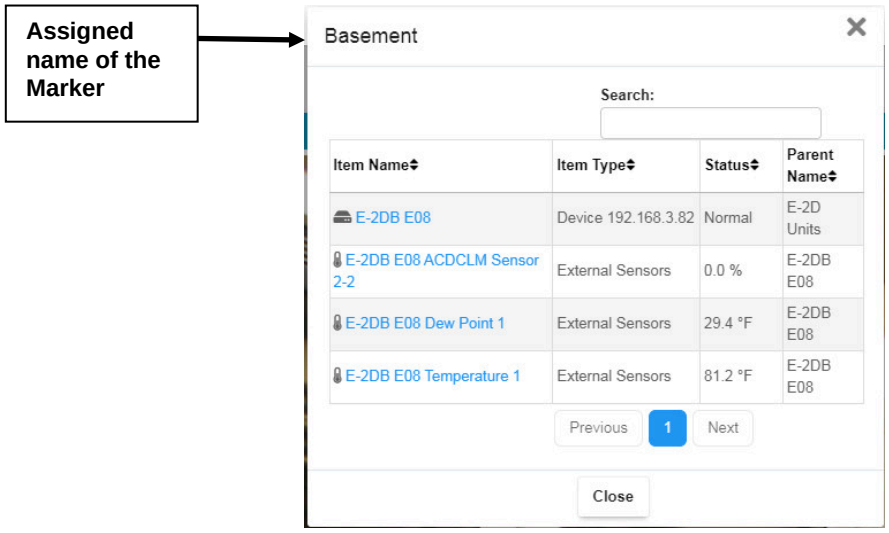


Figure 39- Sensor status at location "Basement"

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 32) to identify them (provided they are all connected to the same LAN).

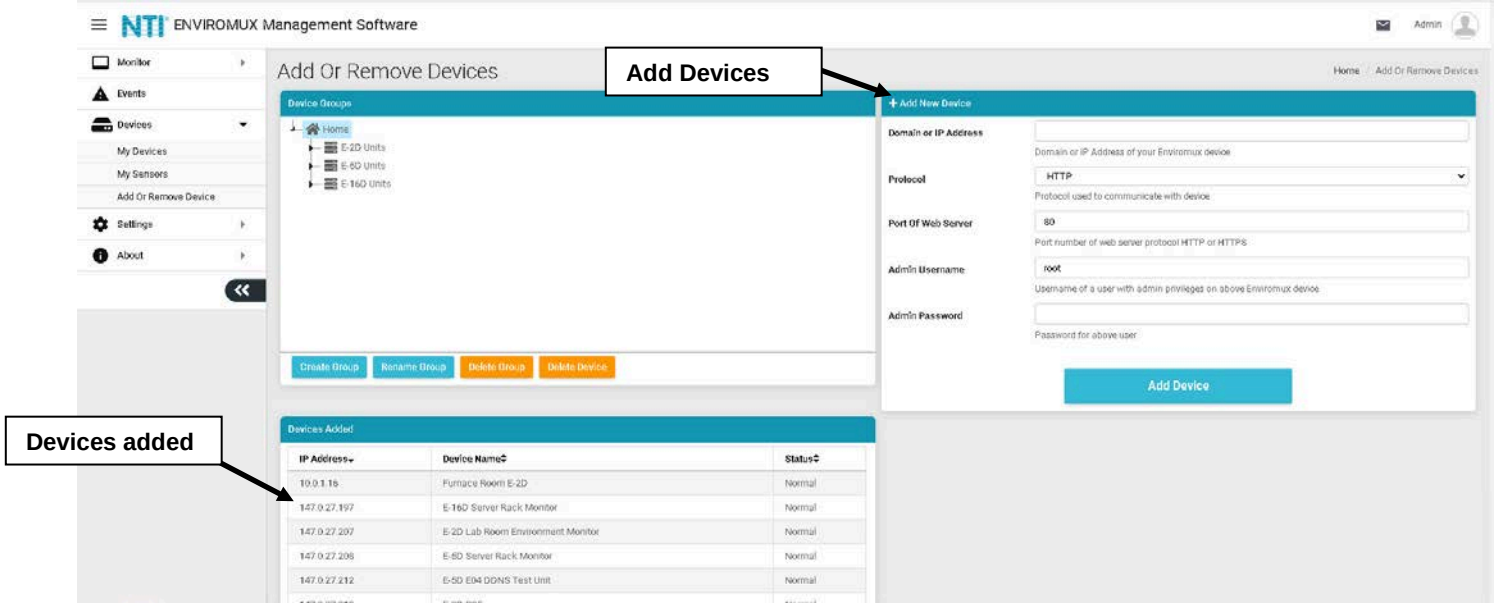


Figure 40- Add Devices to monitor

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.

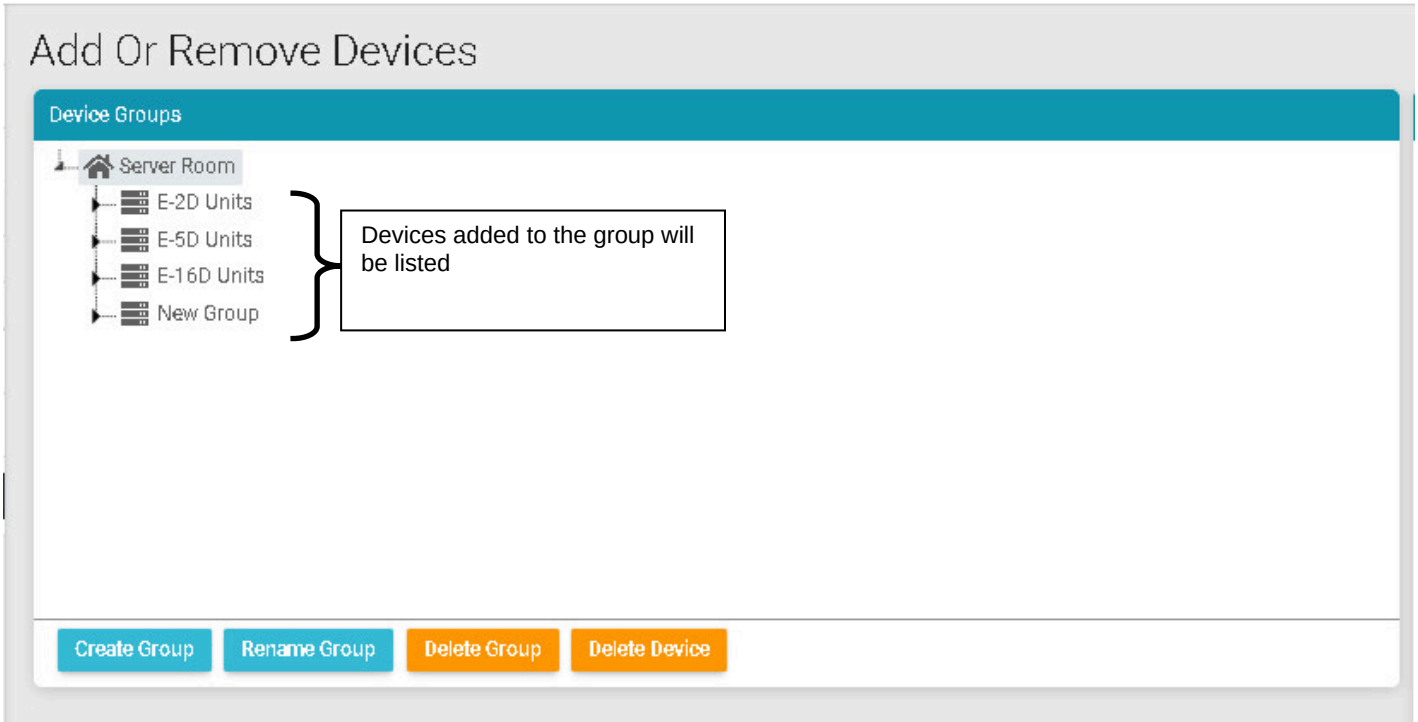


Figure 41- Primary group, and New Group added

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".

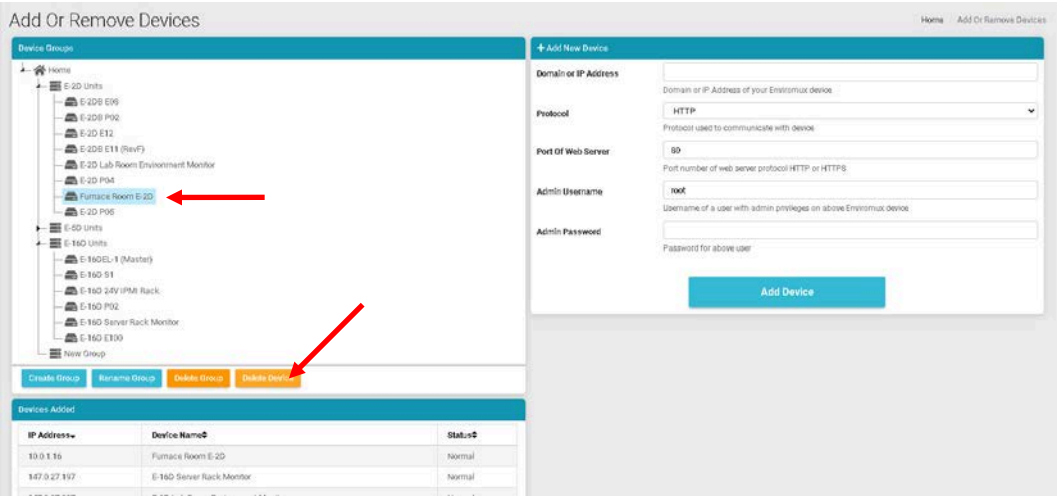


Figure 42- Select Device to delete

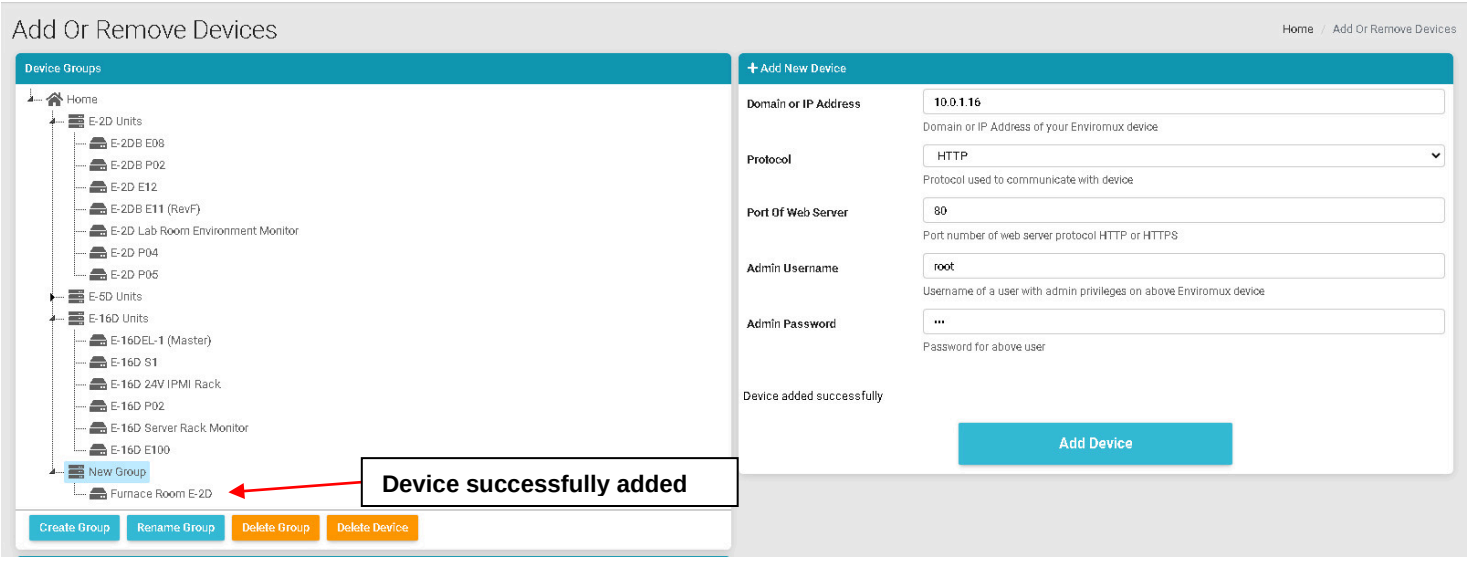


Figure 43- Device moved/added to New Group

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 32) 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.

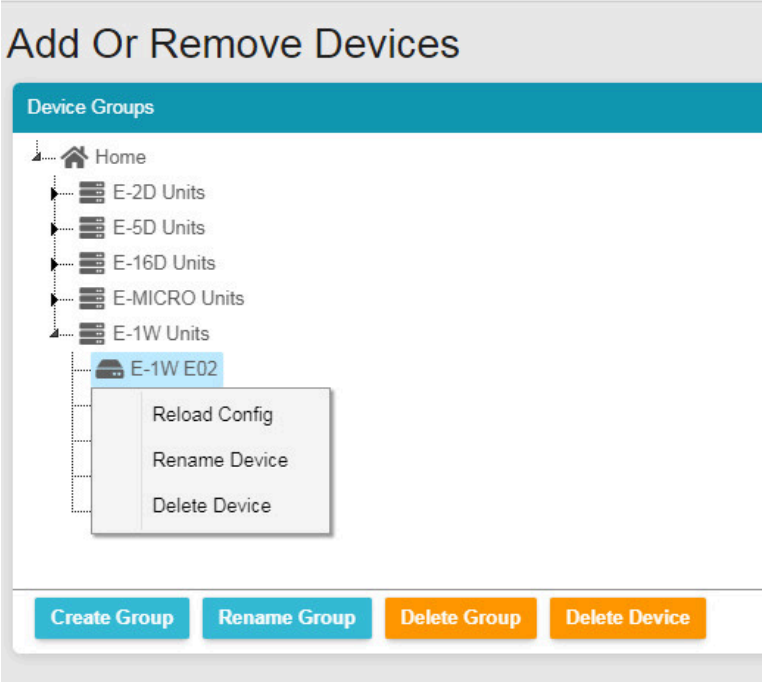


Figure 44- Additional features from Add Devices menu

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.

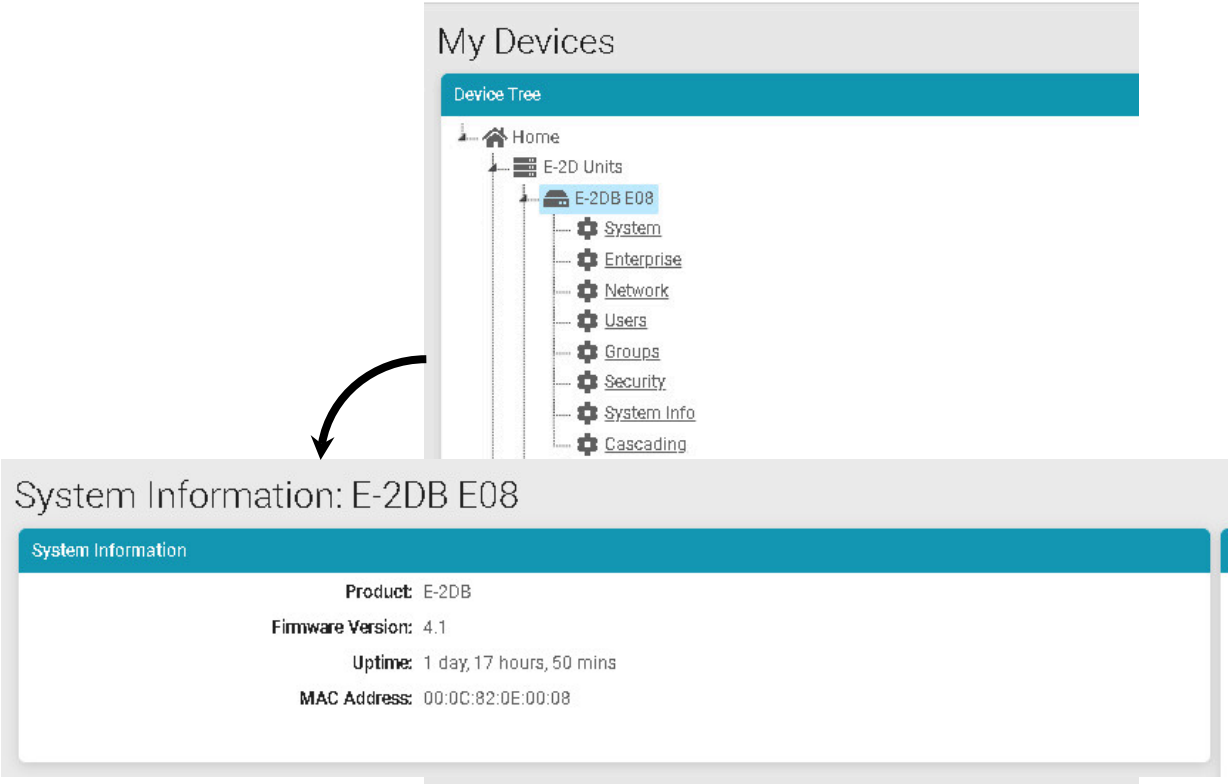


Figure 45- System Info page for the Device

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.

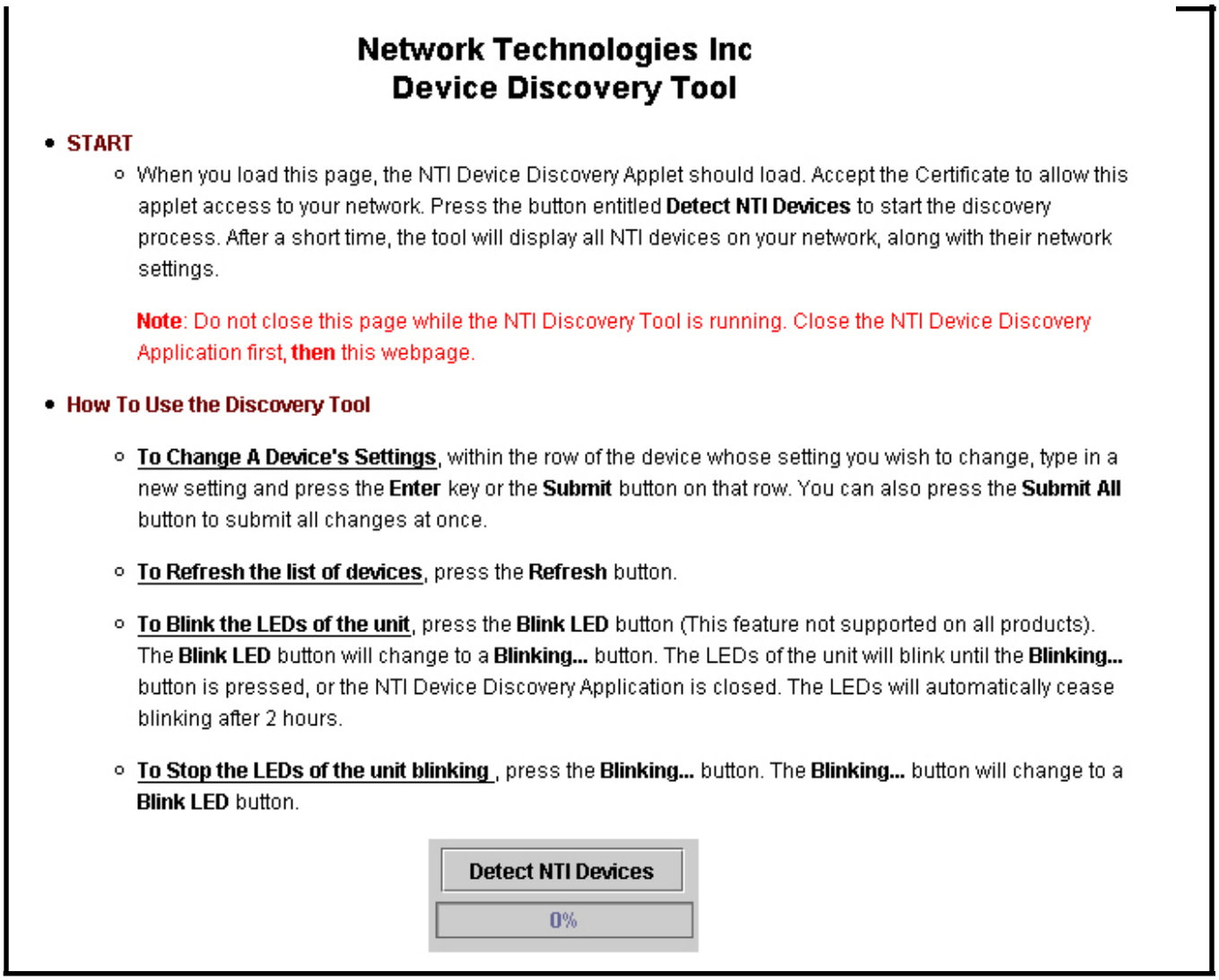
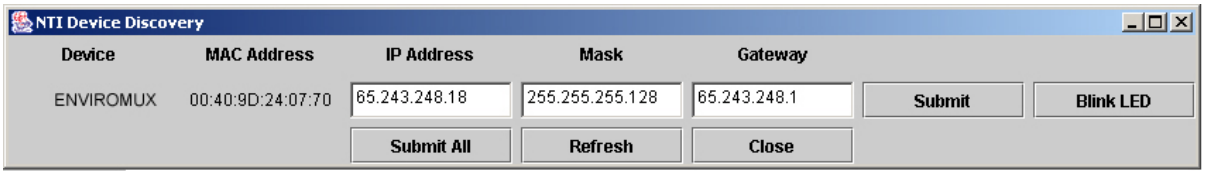


Figure 46- Device Discovery Tool page

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.

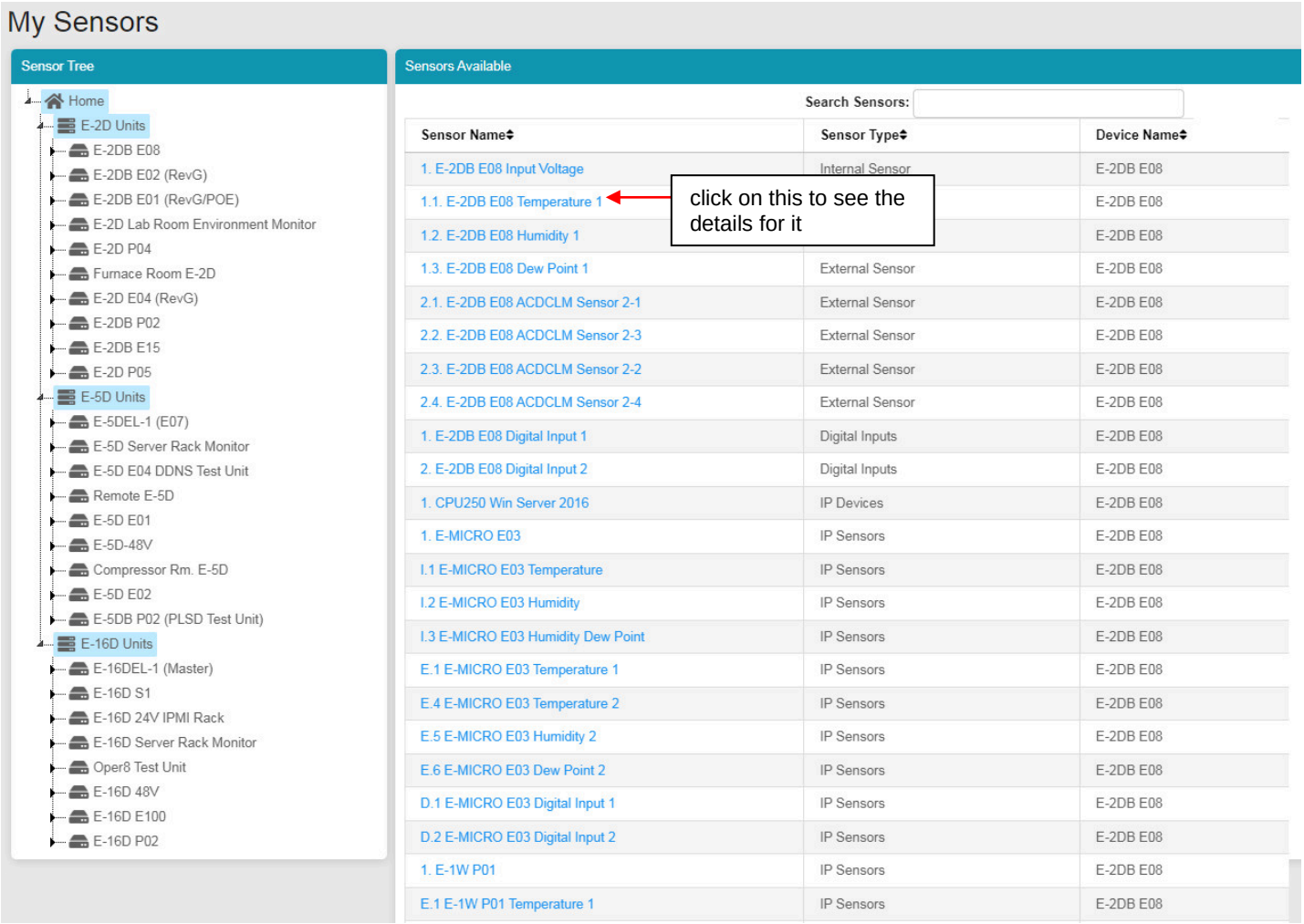


Figure 47- Sensors being monitored

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.

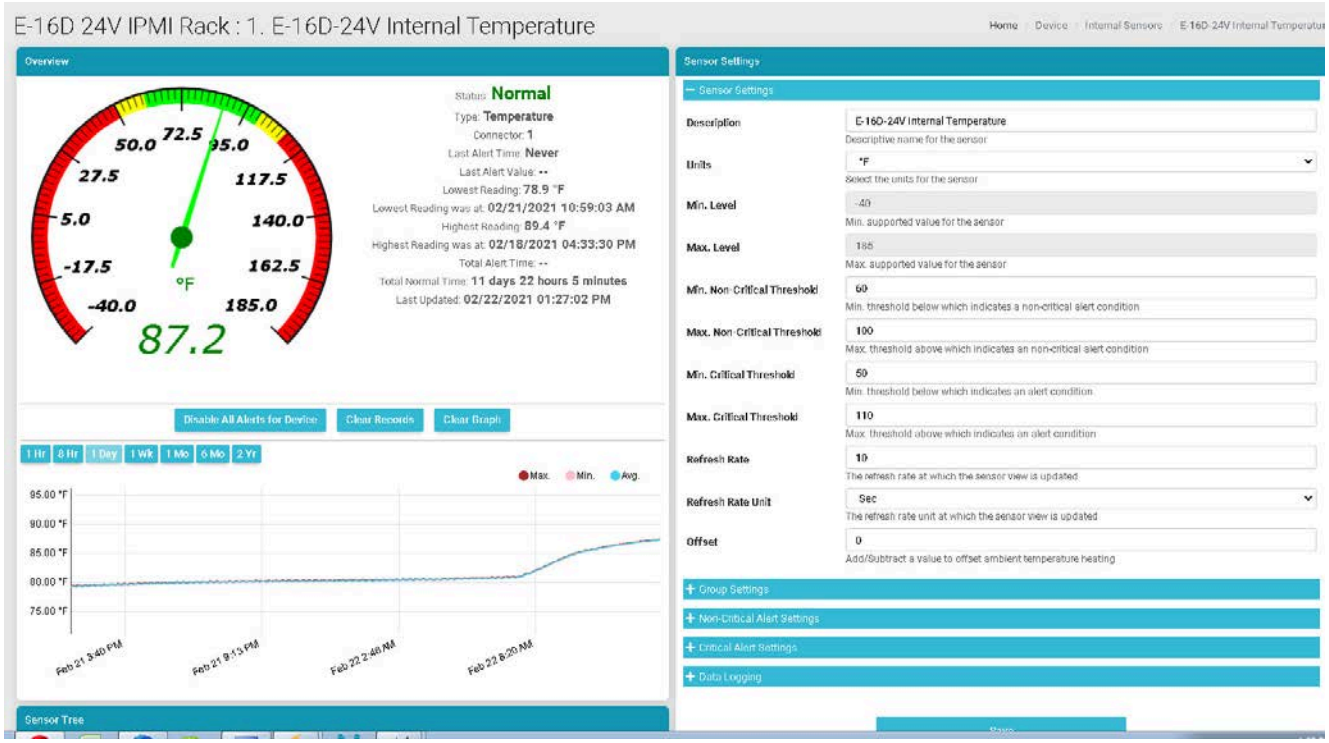
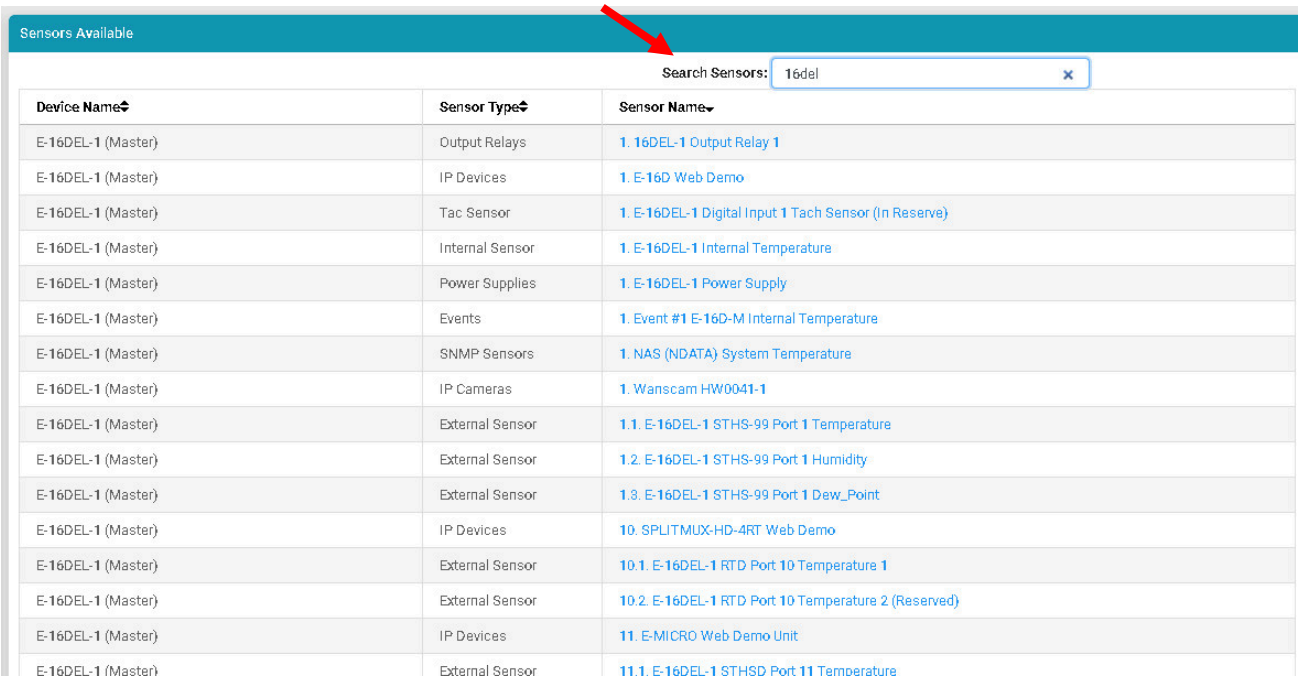


Figure 48- Details for Internal Temperature Sensor

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 49- Use Search Sensors box

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

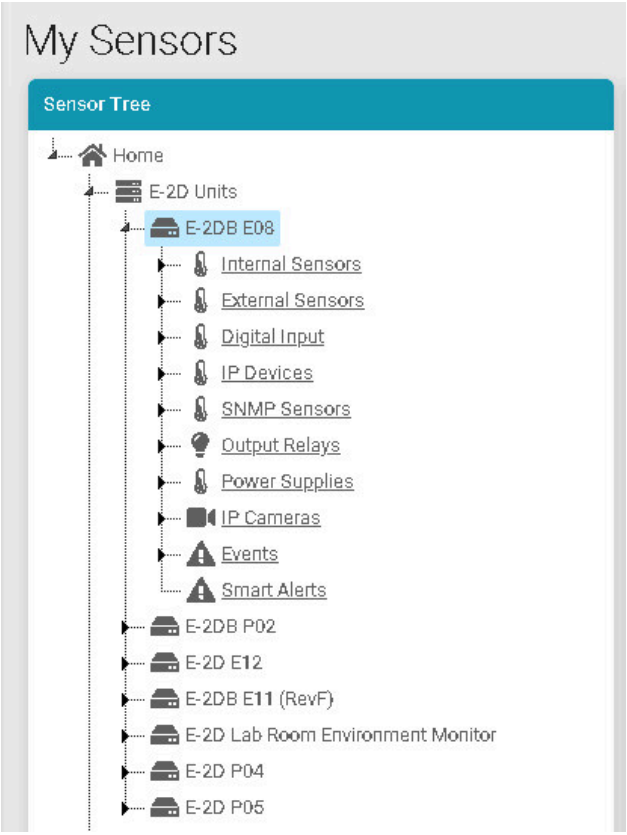


Figure 50- Sensors, relays, IP Cameras etc attached to a specific Device

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

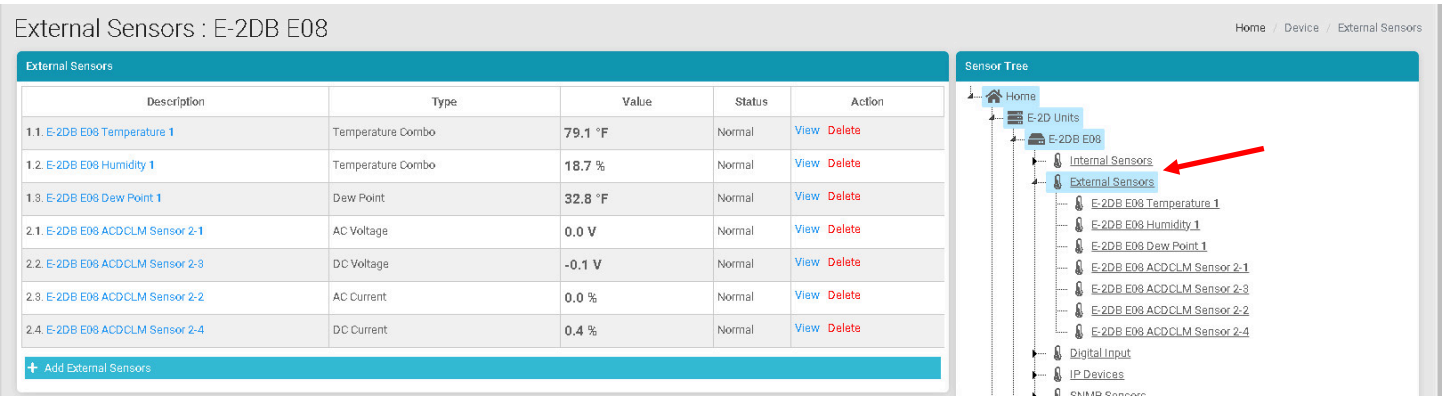


Figure 51- External Sensors connected to specific Device

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".

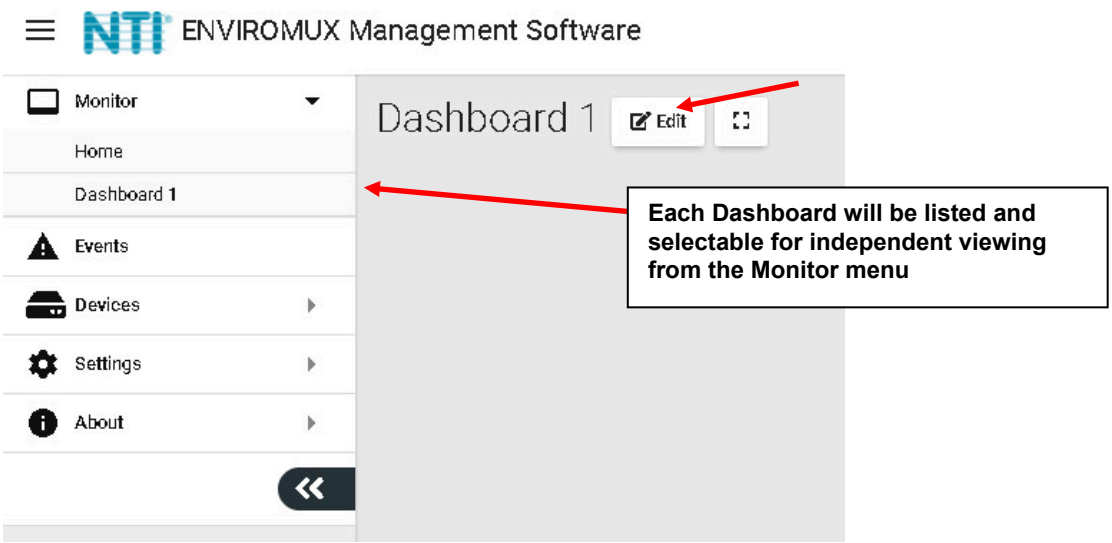


Figure 52- Initial Monitoring Dashboard menu

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, change Auto Scroll settings for the 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.

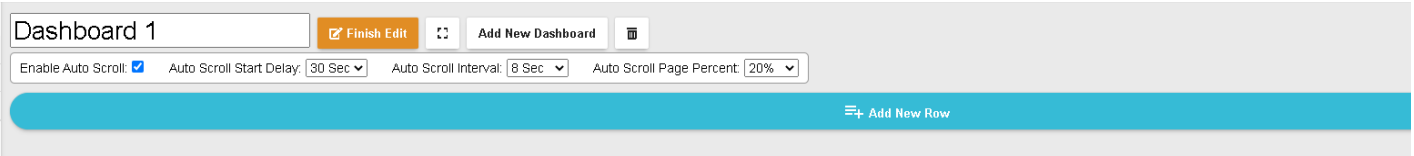


Figure 53- Dashboard options

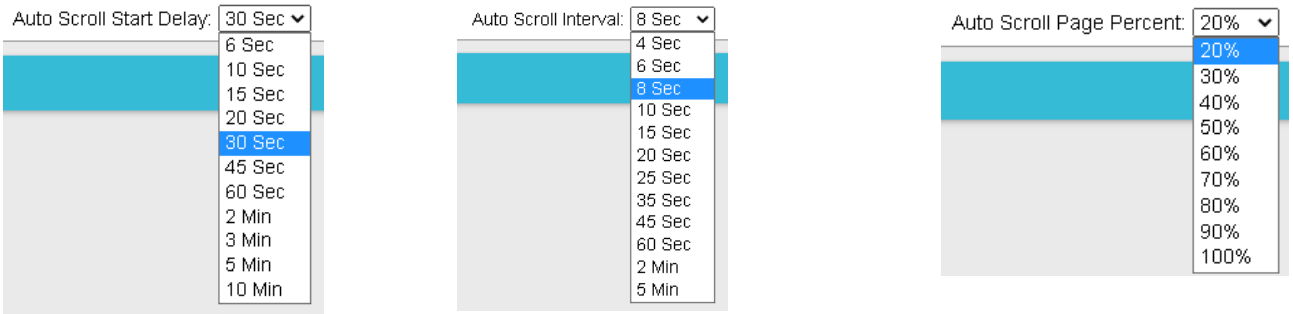


Figure 54- Auto Scroll settings

Auto Scroll is particularly helpful when you have many rows in the Dashboard and the monitor is not capable of displaying all content without scrolling. Auto scroll will start after the configured “Start Delay” period during which keyboard and mouse should be idle. You can set what percentage of page to scroll at a time from 20% to 100% of page. You can repeat to scroll this much of page every few seconds as set in Scroll Interval.

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

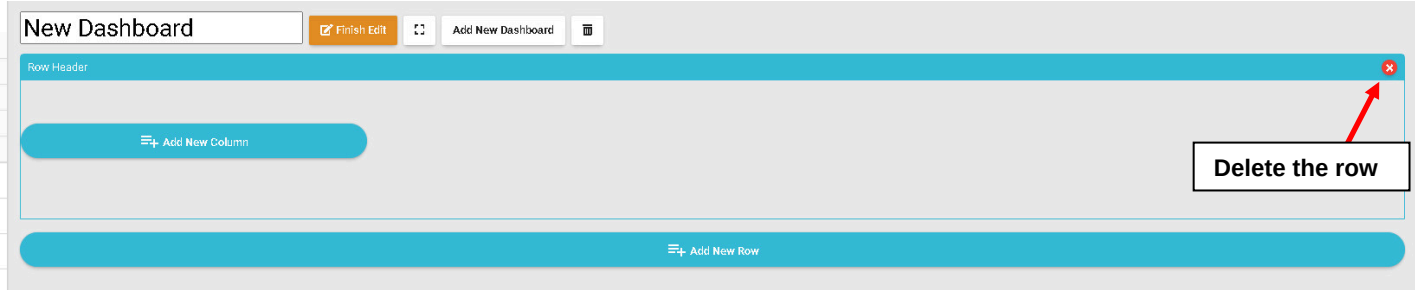


Figure 55- How to add Columns or delete Rows

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 39) .

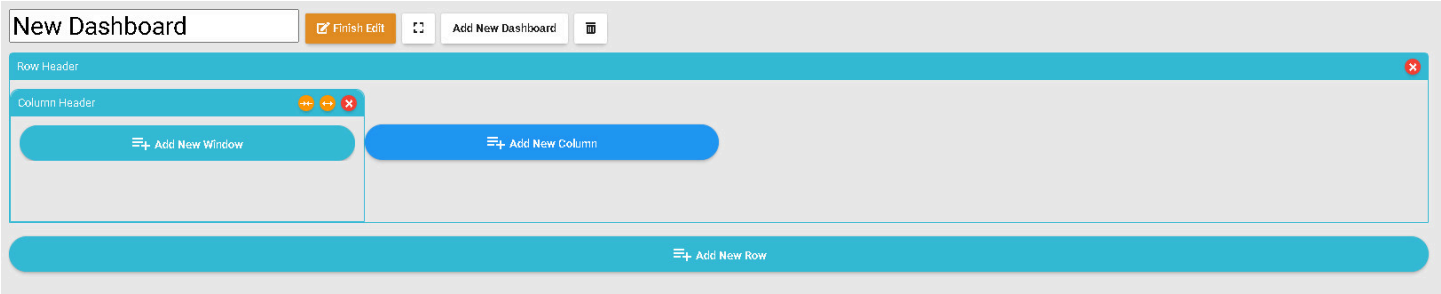


Figure 56- Ready to add a sensor window

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.

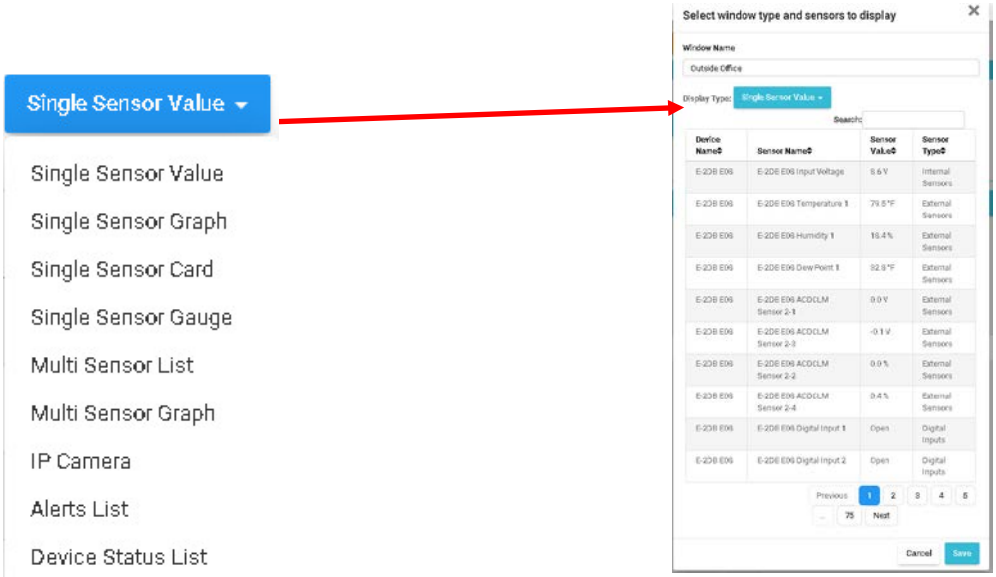


Figure 57- Select sensors to view

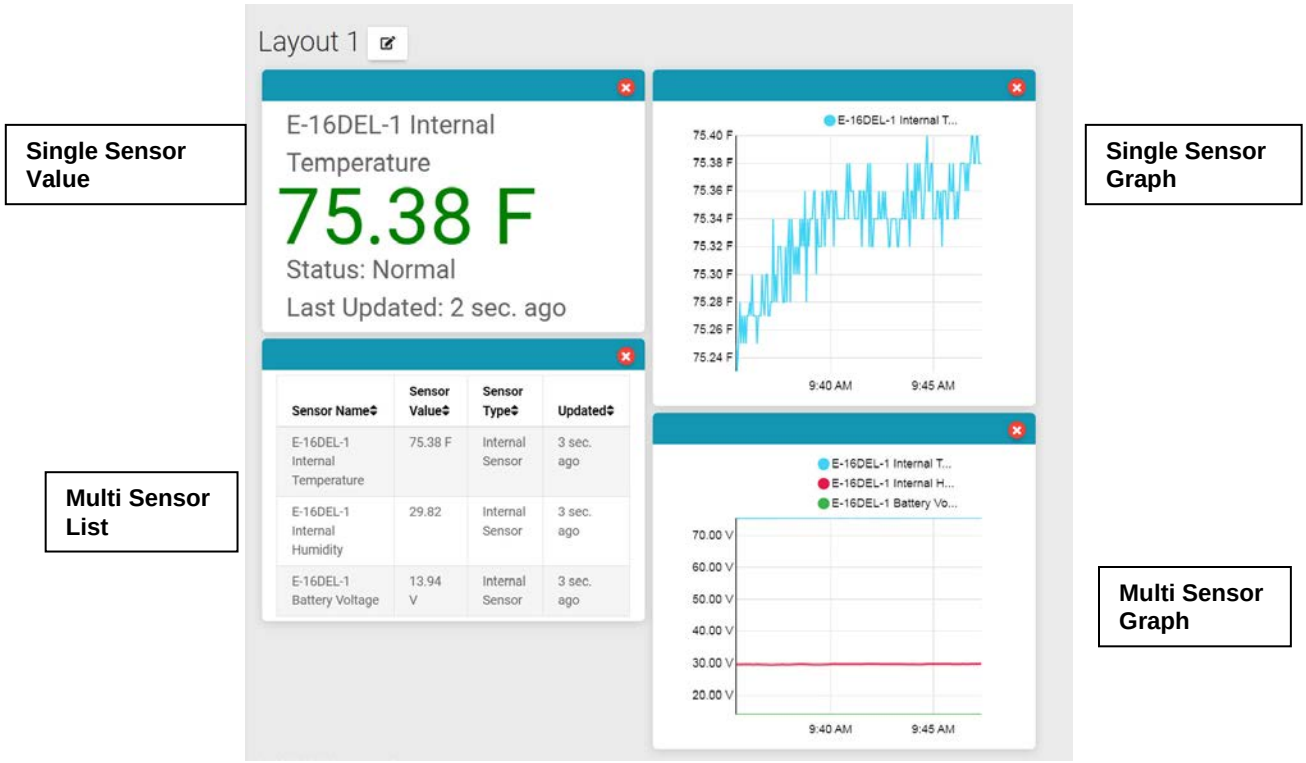


Figure 58- Multiple types of views available

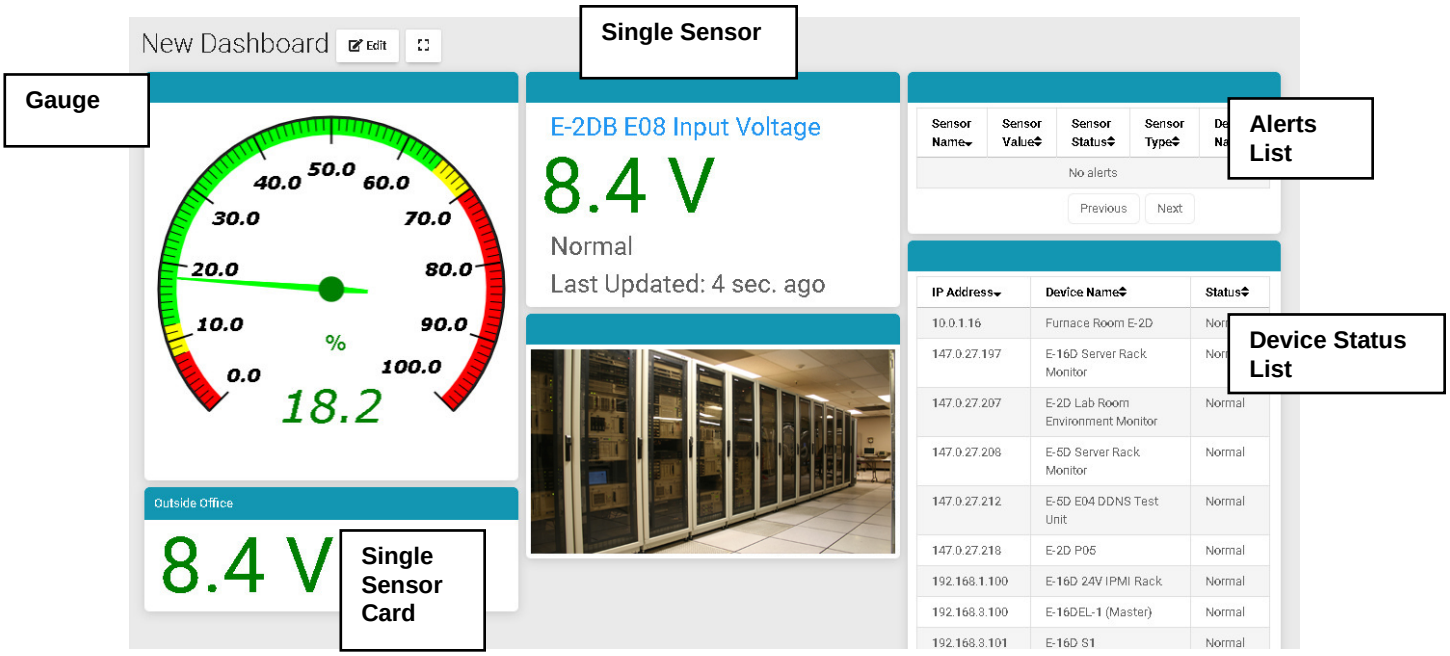


Figure 59- More types of views

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.

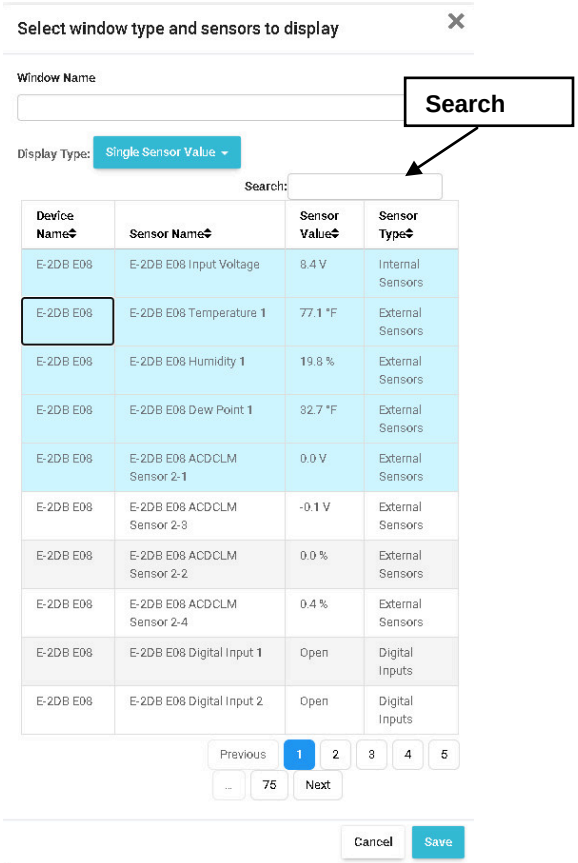


Figure 60- Select one or more sensors

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.

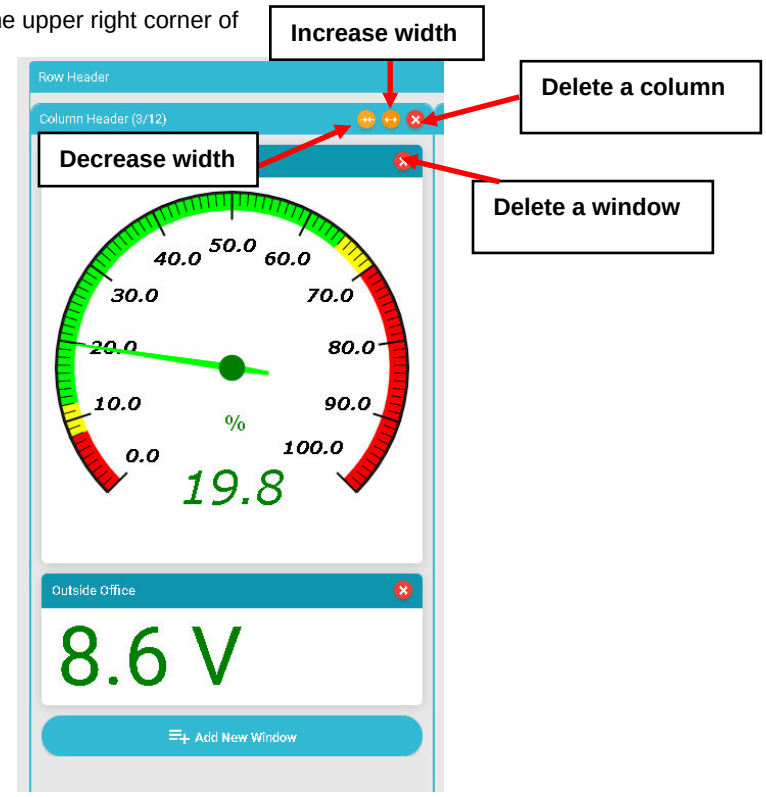


Figure 61- Change the width of a column

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

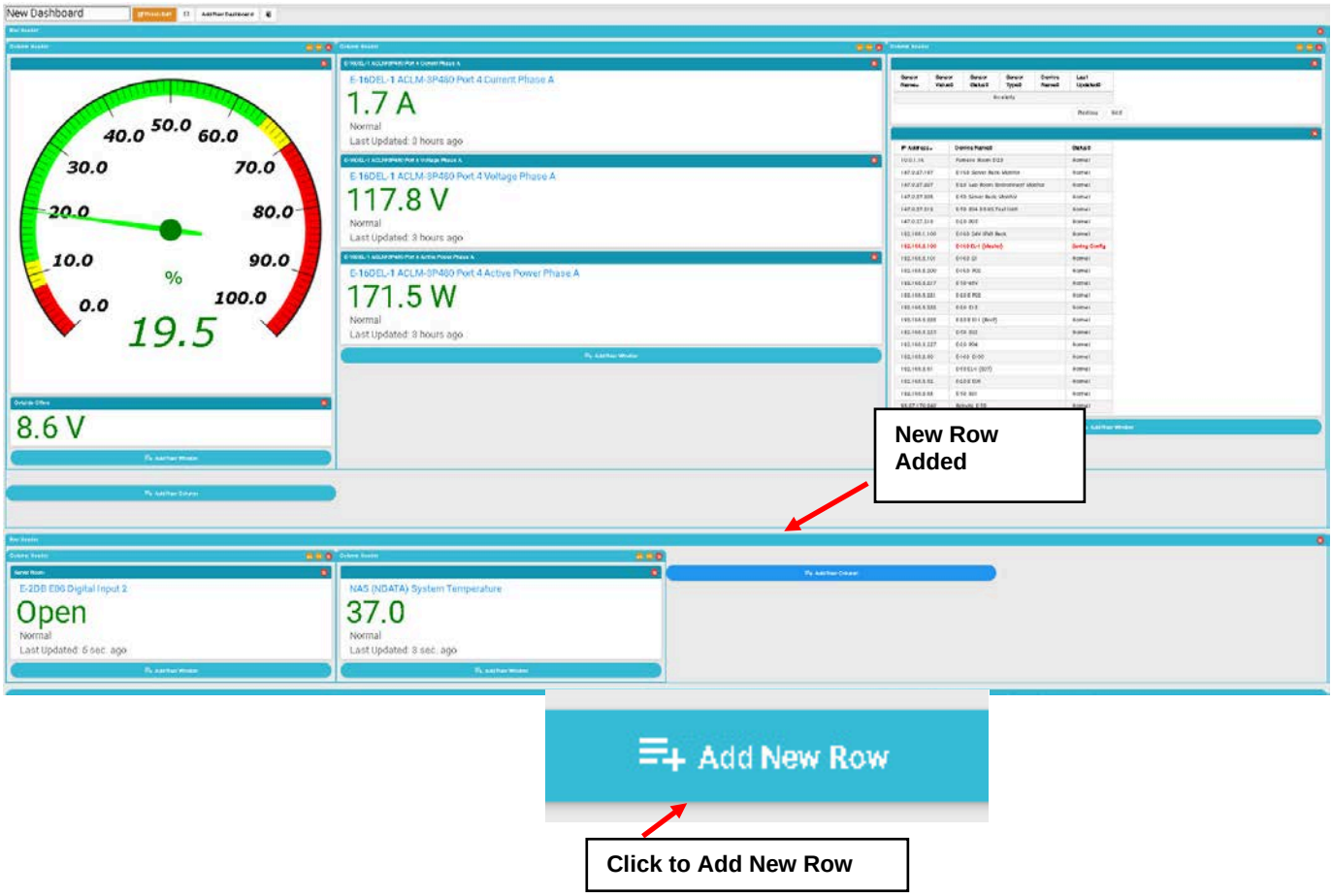


Figure 62- Add a new row of sensors

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

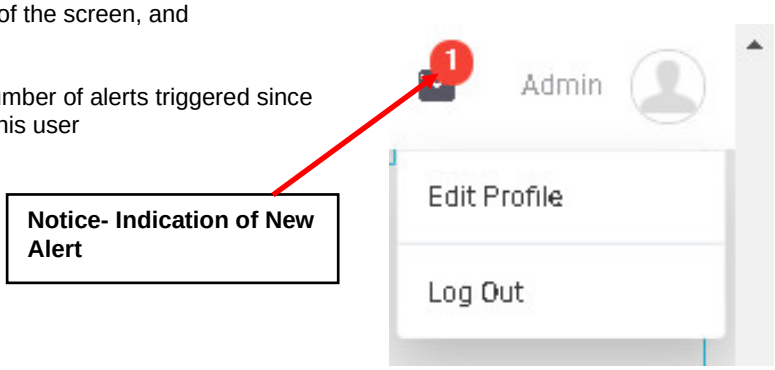


Figure 63- Log out

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 64- Dashboard setup to display specific content

The data from those graphs can also be downloaded for future reference. Click on "Download Graph Data" to download a text file with the information you need.

Note: Downloading before the graph is loaded using HTTP API will throw an HTTP response code 204.

- ***Graph data will contain data for all periods in different rows.***
- ***A value of -999999 indicates a value is not available.***

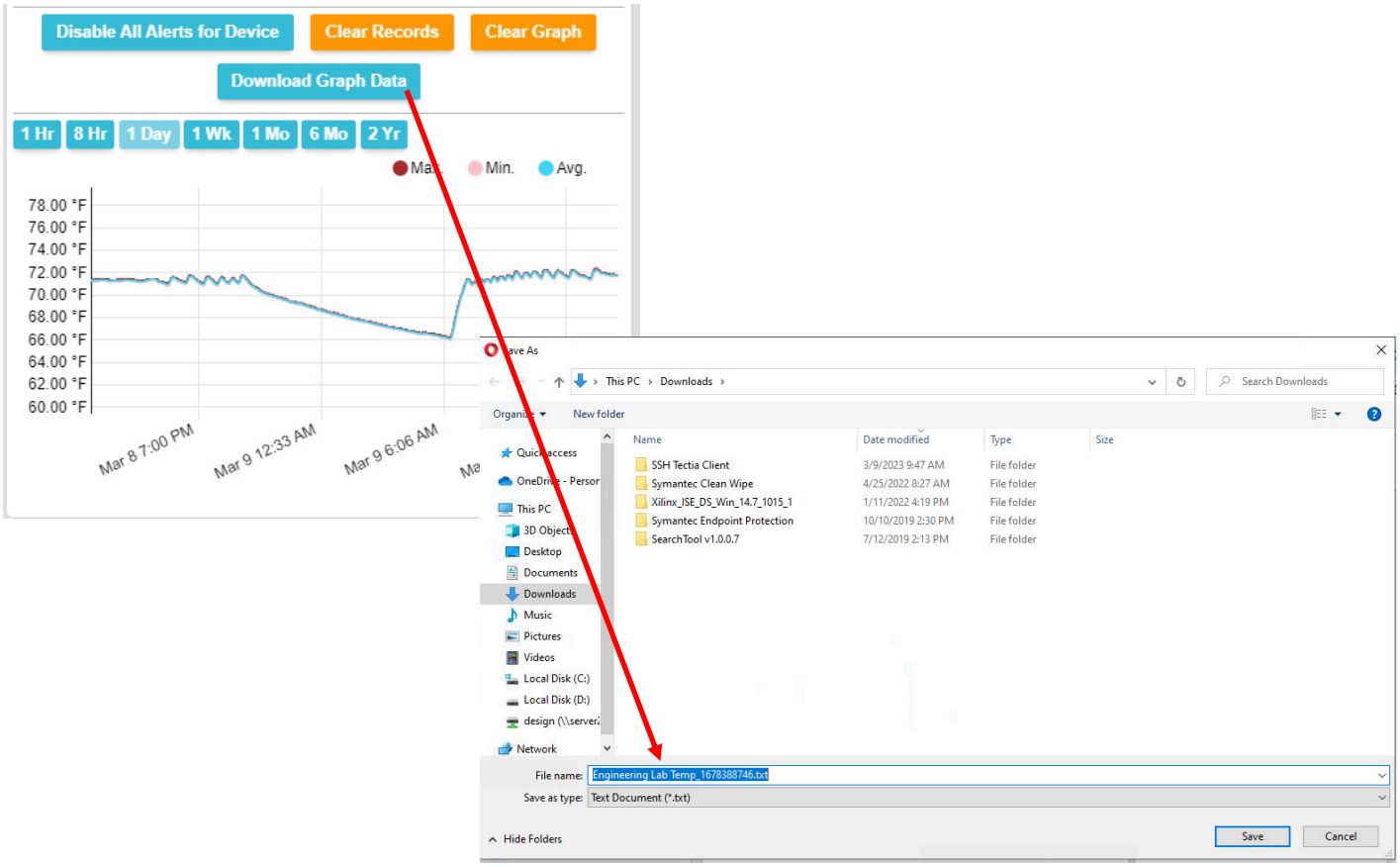
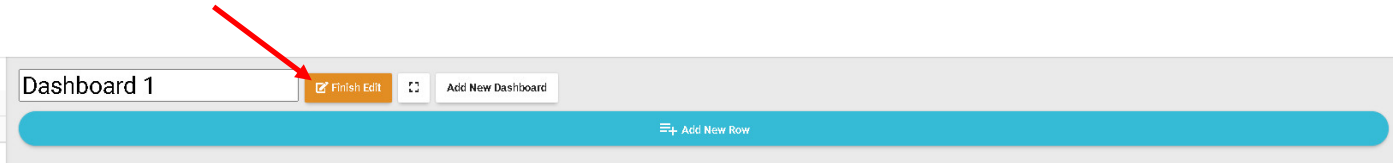


Figure 65- Download Graph Data to text file

Once you are finished editing a Dashboard, click "Finish Edit".



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.

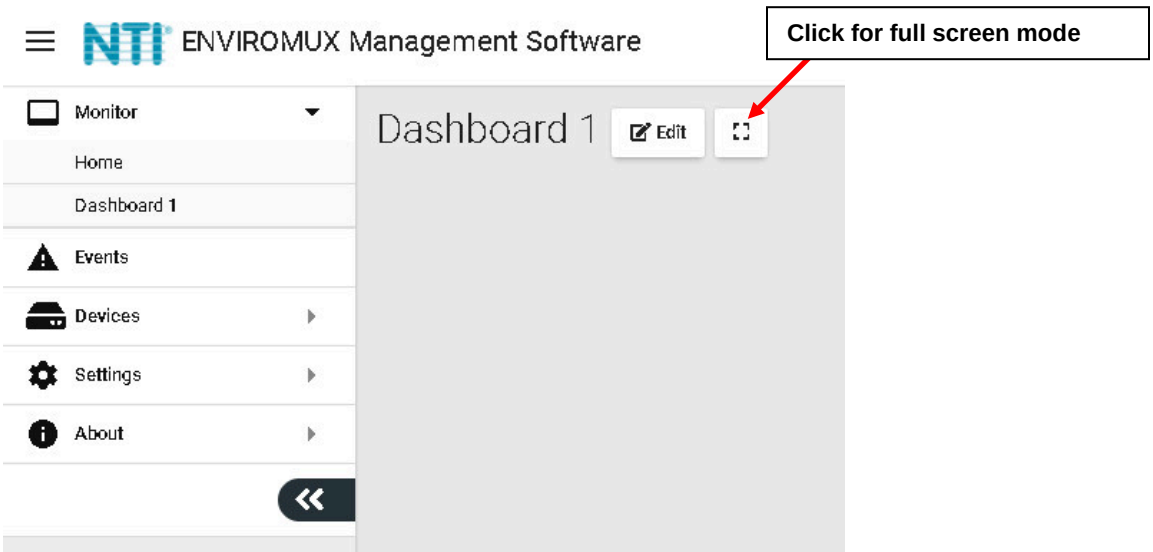


Figure 66- Enable full screen view

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 (pdf format) will provide includes 1) sensor or device summary, 2) the combined number of alerts that have been generated by each selected sensors/device's sensors/markers in the maps and 3) 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.

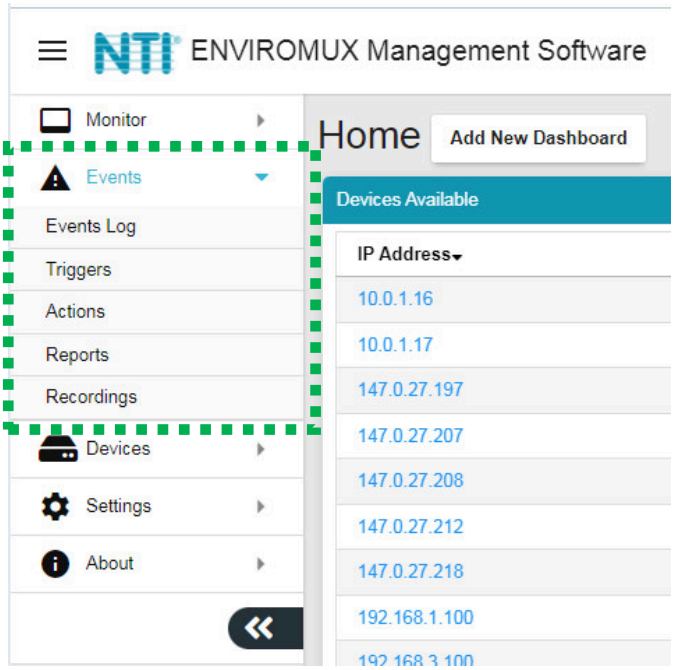


Figure 67- Events Menu

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.

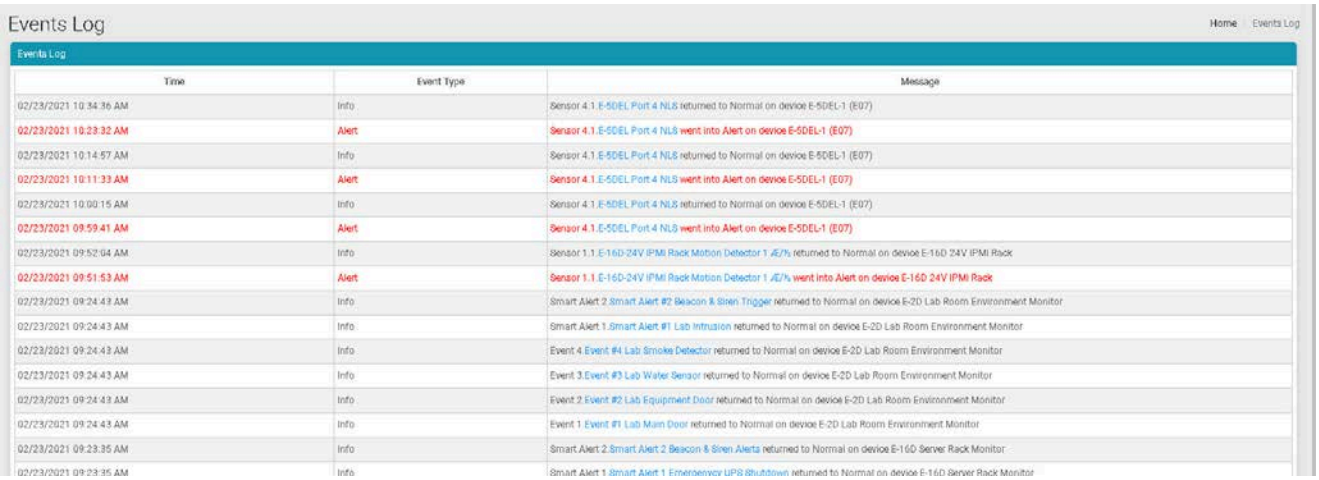


Figure 68- Events Log

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

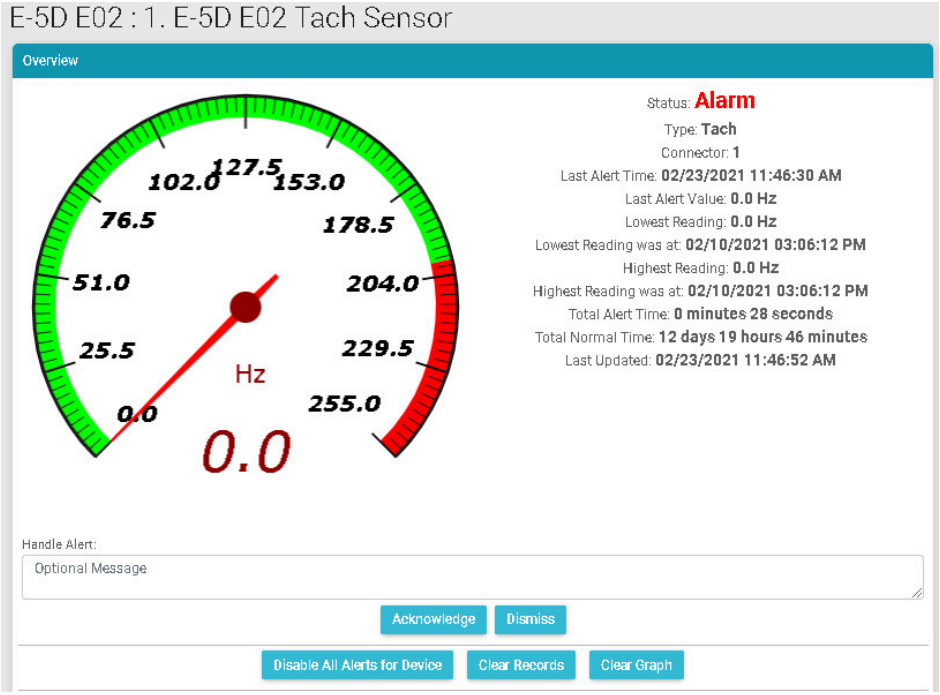


Figure 69- Connect directly to acknowledge or dismiss alert

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.

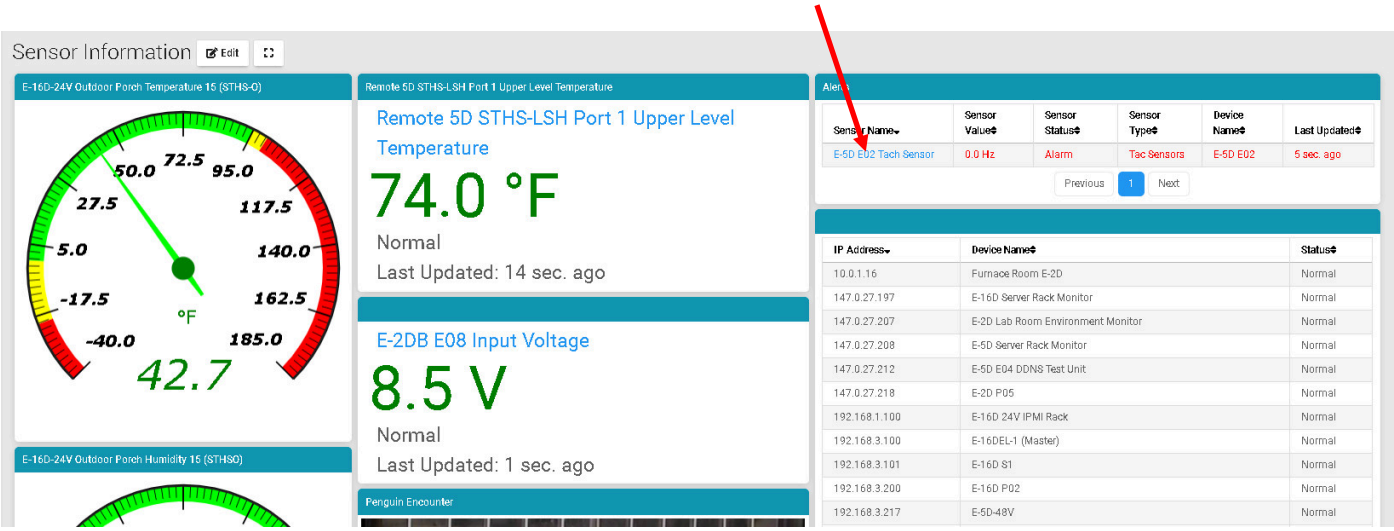


Figure 70- View and connect directly with sensor through the Dashboard

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

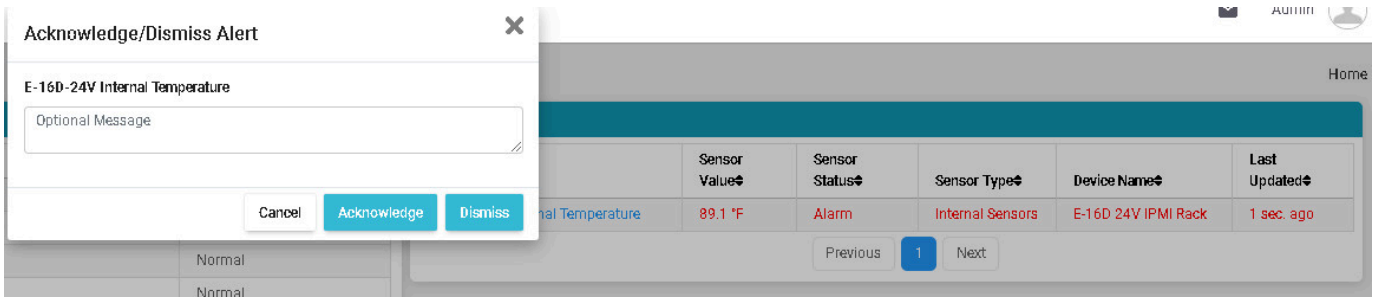


Figure 71- Acknowledge or Dismiss alert pop-up

If, at some point, you want to remove all the listed event log entries and start from scratch, you can click on "Clear All Entries" and let the list start over. If you want to save the logs for future reference, click "Download All Entries" first and save the file to a .txt file somewhere on your computer. This file is tab delimited with the first row having column names. Please note messages are in HTML format. You can use this file to filter by devices or sensors.

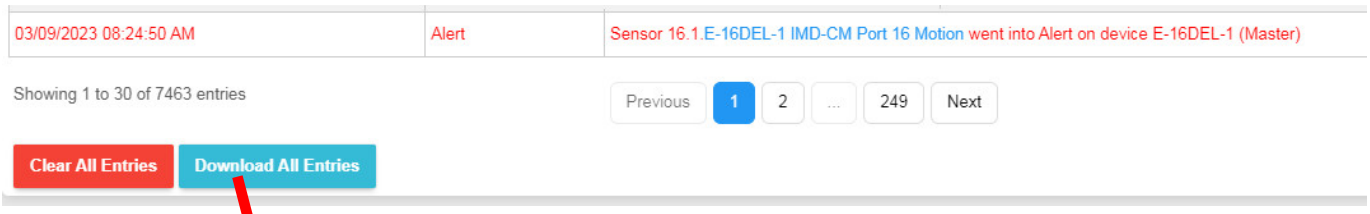


Figure 72- Clear or Download Event Log Entries

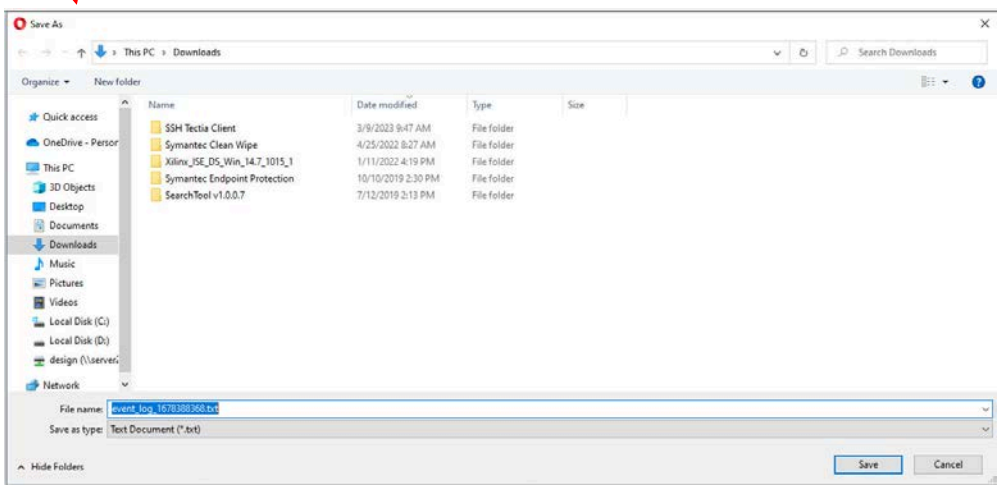


Figure 73- Save Event Log as text file

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. First you must configure the 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.

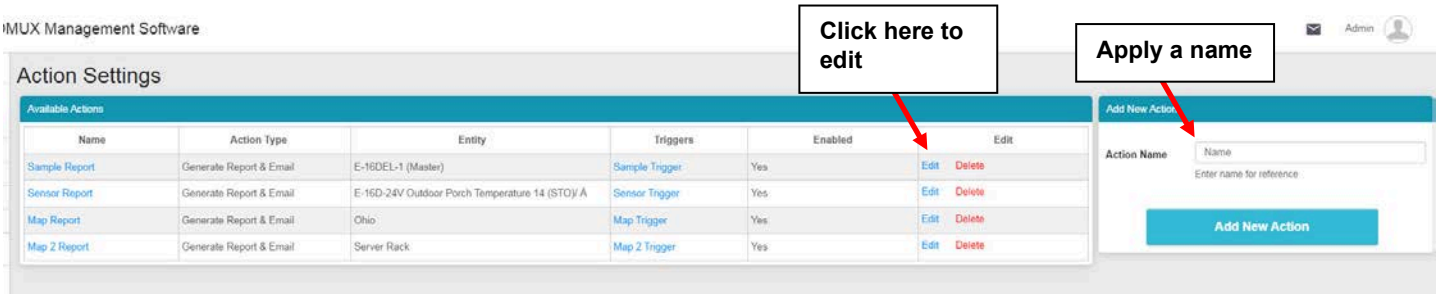


Figure 74- Action List

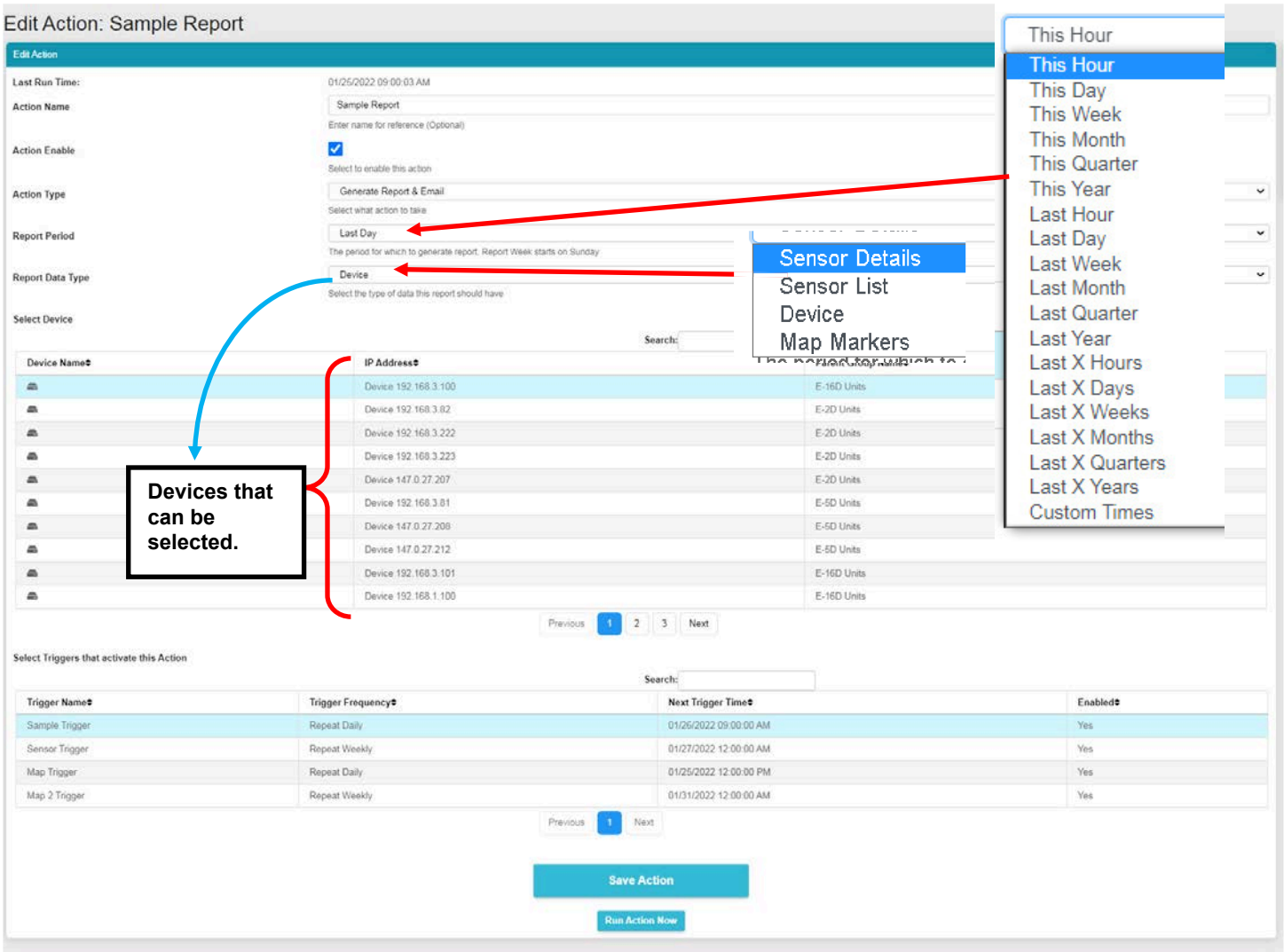


Figure 75- Action Options

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

For Action Type, select from the drop down list.

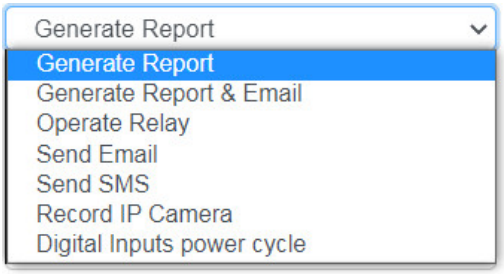


Figure 76- More Action Options

Generate Reports & Email

If you select "Generate Report & Email" then all users with "Email Alerts" selected (Figure 30) will receive reports via email. Select "Generate Report" to have generated reports saved in the Report List (page 61). A Report can include sensor details, a sensor list, devices being monitored, or a list of configured map markers.

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 a summary of sensors or devices, alerts from multiple specific sensors, alerts from all sensors that are of a specific type.

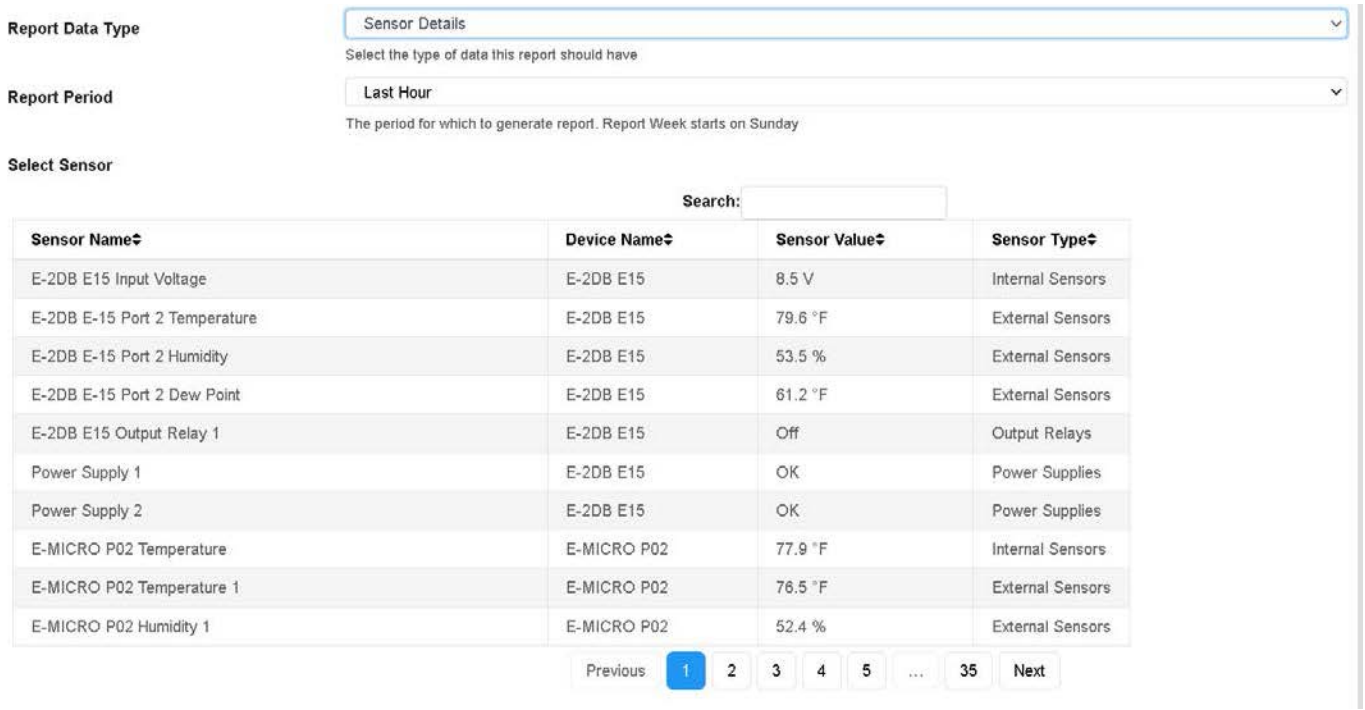


Figure 77- Report Data Type- Sensor Details

Sensor details will provide a graph of sensor values, alerts trend and sensor records of each selected sensor.

A sensor list report will provide a list of the details shown in the image above, as shown on the next page.

Sensor List Report

Report Date: 05/08/2025 04:01:56 PM

No.	Description	Value		Type	Device
E.2.1	E-2DB E-15 Port 2 Temperature	77.9	°F	Temperature Combo	E-2DB E15
E.2.2	E-2DB E-15 Port 2 Humidity	42.2	%	Humidity Combo	E-2DB E15
E.2.3	E-2DB E-15 Port 2 Dew Point	53.1	°F	Dew Point	E-2DB E15
O.1	E-2DB E15 Output Relay 1	Off		Output Relay	E-2DB E15
P.1	Power Supply 1	OK		Power Supply	E-2DB E15
P.2	Power Supply 2	OK		Power Supply	E-2DB E15
I.1	E-2DB E08 Input Voltage	8.4	V	Voltage	E-2DB E08
E.1.1	E-2DB E08 Temperature 1	80.7	°F	Temperature Combo	E-2DB E08
E.1.2	E-2DB E08 Humidity 1	34.0	%	Humidity Combo	E-2DB E08

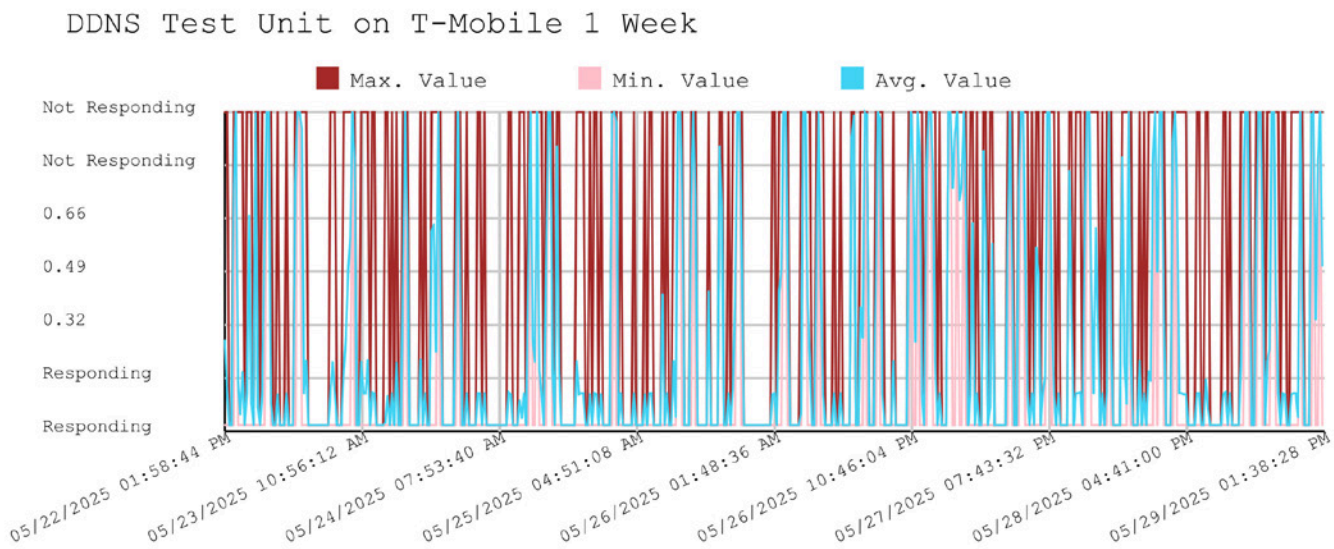
NTI ENVIROMUX Management Software

Figure 78- Report for Sensor List

Device Report

Report Period: Last 5 Days

Report Date: 05/29/2025 01:53:47 PM



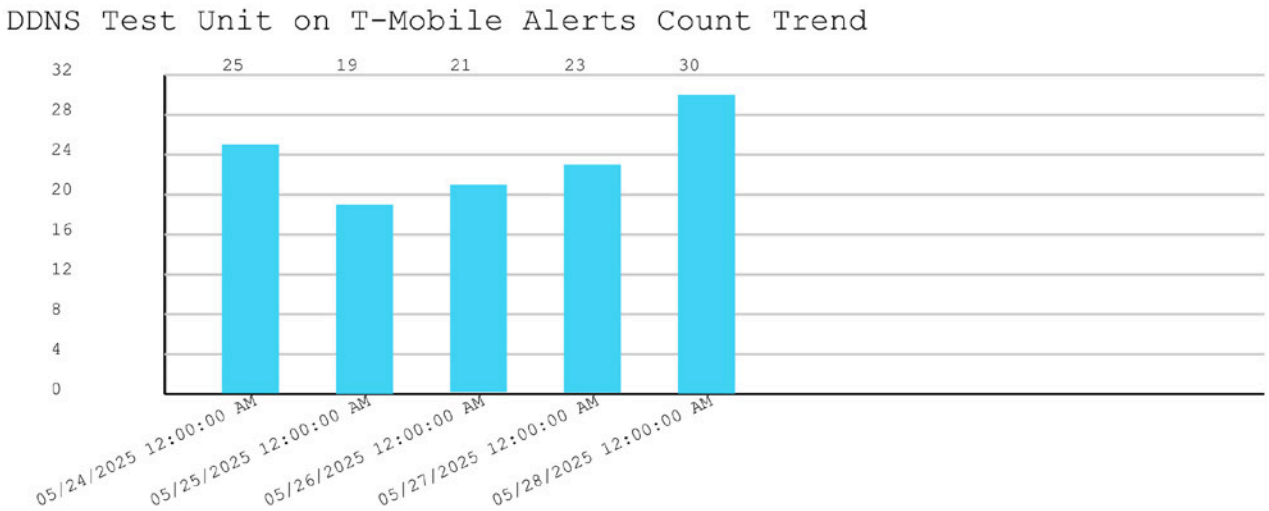


Figure 79- Report for Device

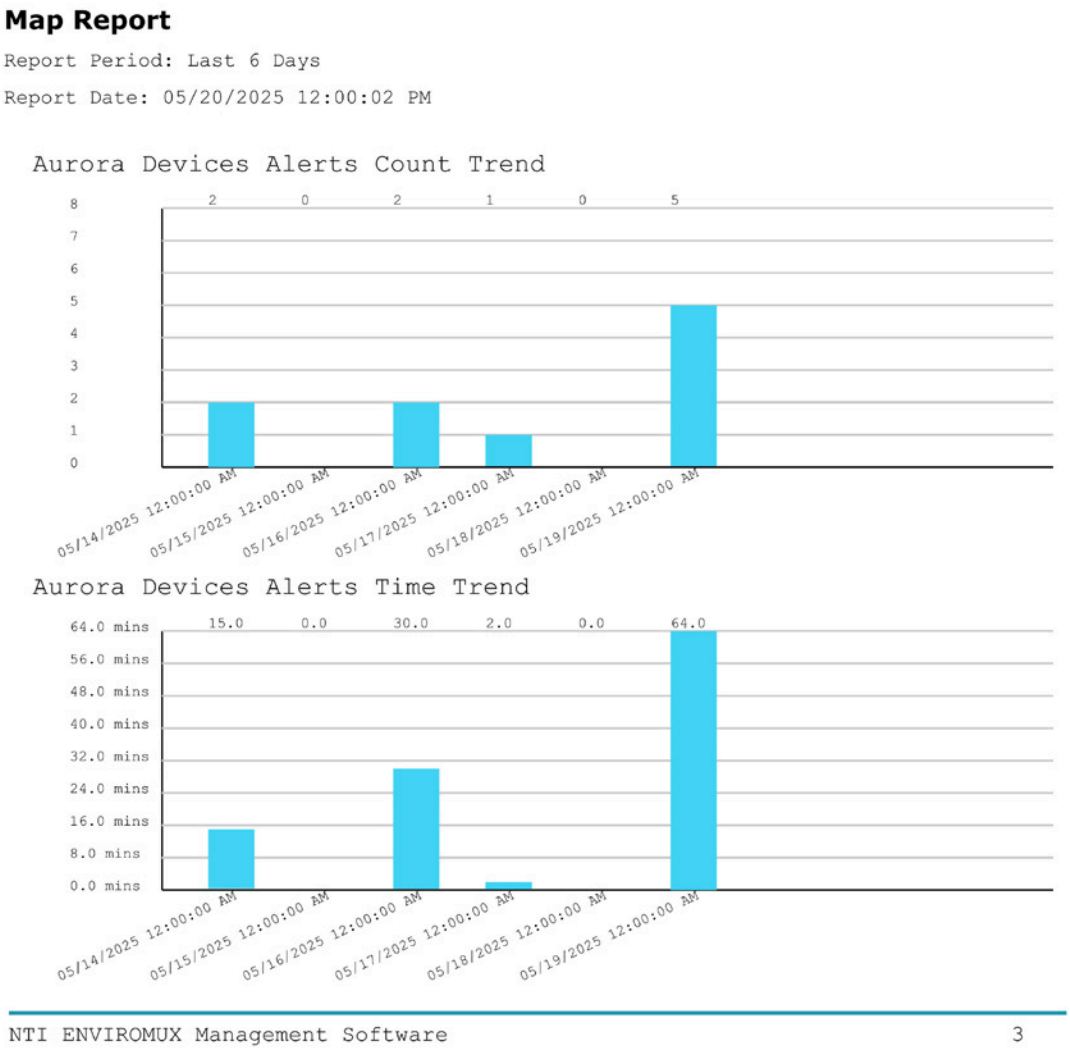


Figure 80- Report for Map Markers

Available selections will adjust depending upon what **Report Data Type** you select. Multiple sensors, devices or markers can be selected and reported in a single report.

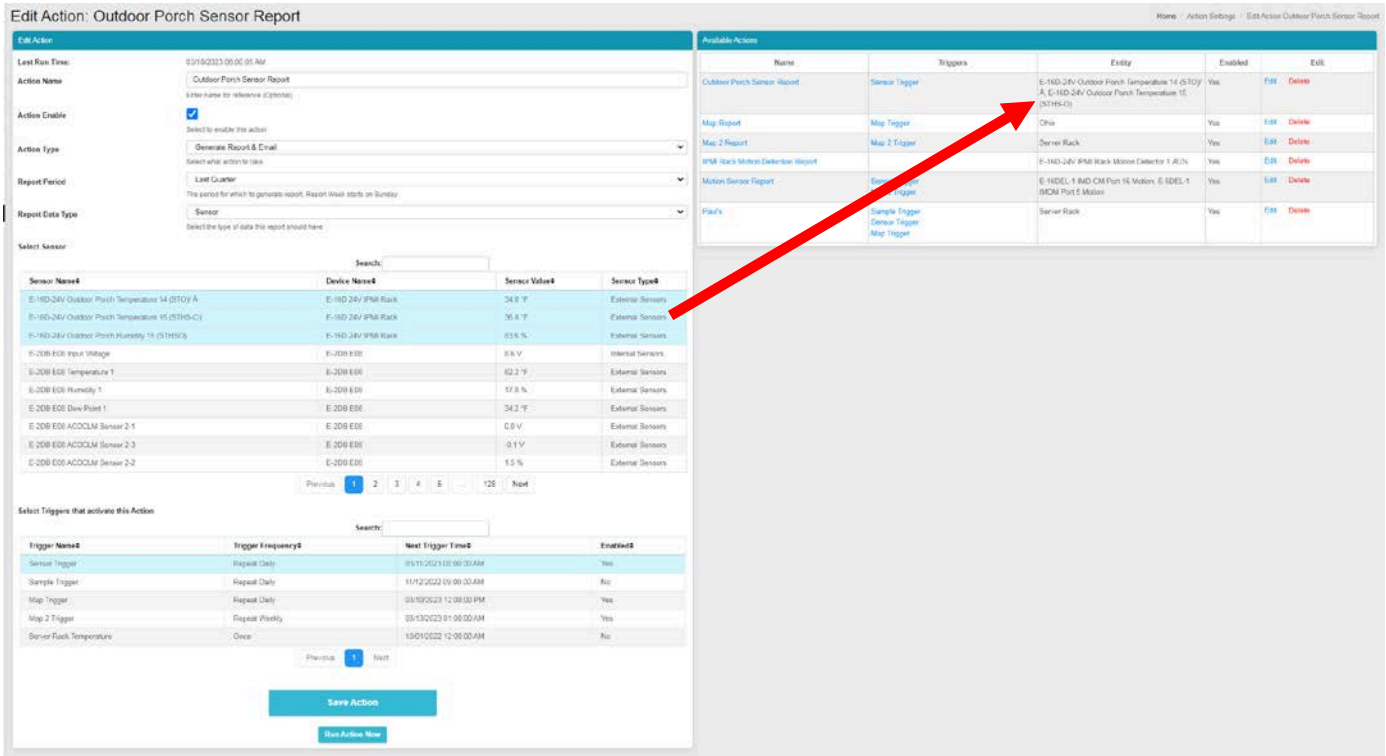


Figure 81- Reports can show multiple devices, sensors or markers

Operate Relay

When "Operate Relay" is selected, all relays found on the ENVIROMUX's monitored by the Management Software will be listed. One or more relays can be selected. For Output Relay Status, select the status the relay should switch to once an Action is Triggered.

Output Relays can be used to control beacons(E-BCN), sirens (E-SRN), automatic voice dialers(E-AVDS), electric strikes (E-EDR-SF), etc.

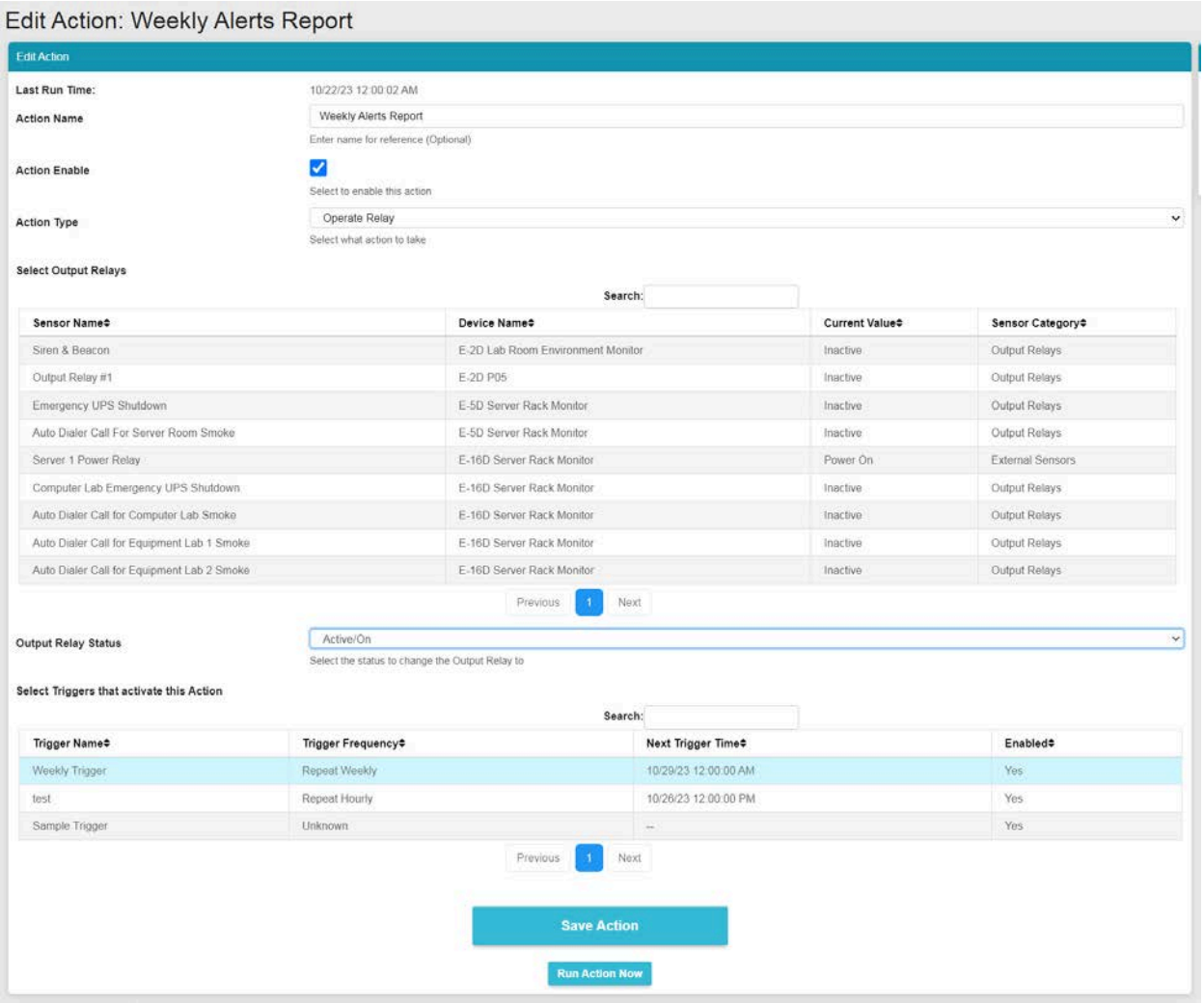


Figure 82- Action Type "Output Relay"

Send Email

When "Send Email" is selected, a text box is presented to enter an email message to be sent to all registered users of the Management Software with email alerts enabled. The message can be either plain text or a template and can include a variety of template variables to make it easy to identify the Trigger source, device information etc. Available template variables are listed below.

Variable	Description
%triggered_sens_val%	Sensor Value
%triggered_sens_name%	Sensor Name
%triggered_sens_cat_name%	Sensor Category Name
%triggered_sens_pos%	Sensor Position within the Sensor Category
%triggered_dev_name%	Device Name corresponding to sensor triggered
%triggered_dev_loc%	Device Location corresponding to sensor triggered (Available for E-xD only)
%triggered_dev_branch%	Device Branch corresponding to sensor triggered (Available for E-xD only)
%triggered_dev_rack%	Device Rack corresponding to sensor triggered (Available for E-xD only)
%triggered_dev_phone%	Contact Phone Number of Device corresponding to sensor triggered (Available for E-xD only)
%triggered_dev_email%	Contact Email of device corresponding to sensor triggered (Available for E-xD only)
%triggered_dev_mac%	Device MAC address corresponding to sensor triggered
%triggered_dev_ip%	Device IP Address corresponding to sensor triggered
%triggered_dev_model%	Device Model corresponding to sensor triggered
%current_date_time%	Current Date and Time
%sensor_name_<ID>%	Sensor Name of a specific sensor identified by its EMNG Sensor ID. Example %sensor_name_23%
%sensor_val_<ID>%	Sensor Value of a specific sensor identified by its EMNG Sensor ID. Example %sensor_val_23%.
%triggered_root_sens_name%,	These variables are available only if the Trigger is activated by an Event/Smart Alert with OR Logic and refers to Event/Smart Alert's root sensor.
%triggered_root_sens_val%,	
%triggered_root_sens_cat_name%	

EMNG Sensor ID is available on each sensors page within the Management Software

Please note all triggered_* template variables work only if the Trigger Logic is OR. If the logic for Trigger is something else (like AND) then multiple sensors combine to activate a Trigger and no single sensor can be provided for the template. In such case triggered_* variables will be replaced by a "- ".

Example message: %triggered_sens_name% went into alert on device %triggerred_dev_name% . Contact %triggered_dev_phone% to resolve .

An Email Subject can also be entered.

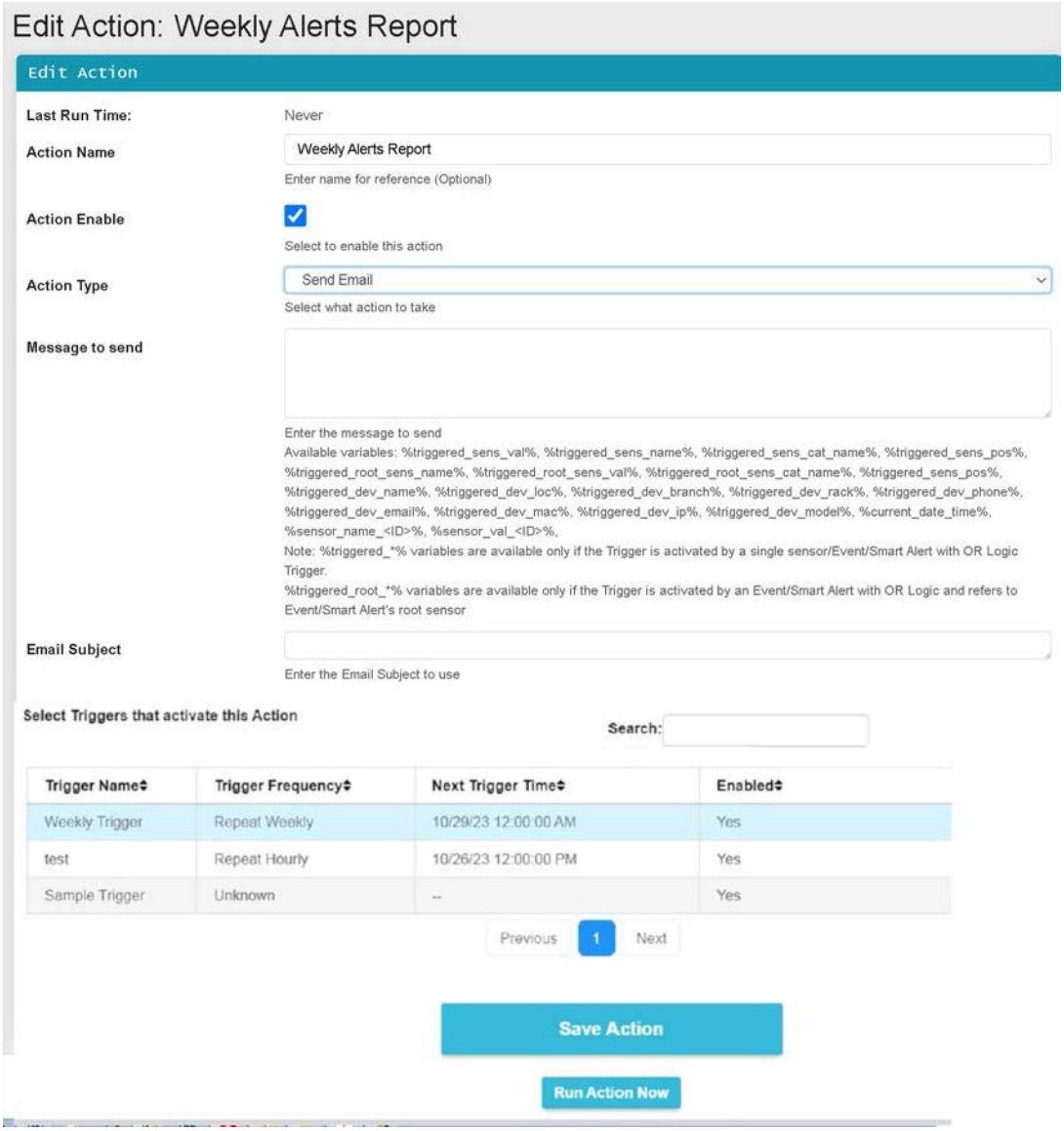


Figure 83- Action Type "Send Email"

Send SMS

Selecting "Send SMS" will have the same message format options as "Send Email" except for the "Email Subject" option. All users with configured phone numbers will receive a message when the action is initiated.

Note: Please restrict the SMS length to be under the limit provided by your SMS provider.

Record IP Camera

When "Record IP Camera" is selected, the user is provided with a list of IP cameras that are monitored by the connected ENVIROMUX's. Any of these can be selected to record video as the action taken. The length of time of the recording can be selected from 5 seconds to up to 10 minutes.

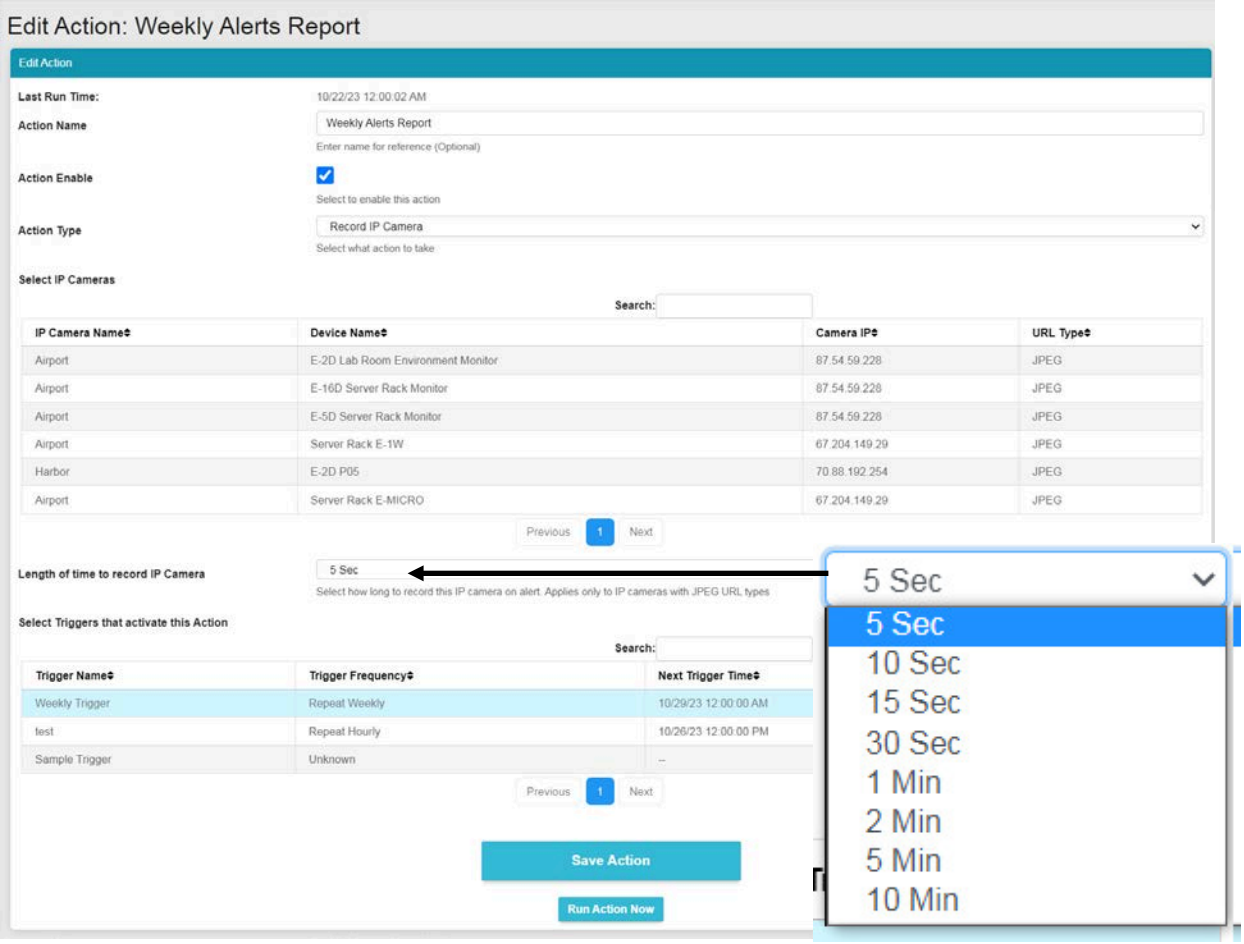


Figure 84-Action Type "Record IP Camera"

Digital Inputs Power Cycle

When "Digital Inputs power cycle" is selected, a list of all digital inputs being monitored by the ENVIROMUX's will be presented. Any of these can be selected to be power cycled by the ENVIROMUX when a trigger occurs.

Note: If the device connected to the Digital Input on the ENVIROMUX is not being powered by that ENVIROMUX, the power cycle action will have no effect on that device. See "Cycle Sensor Power" section in the E-xD product manual.

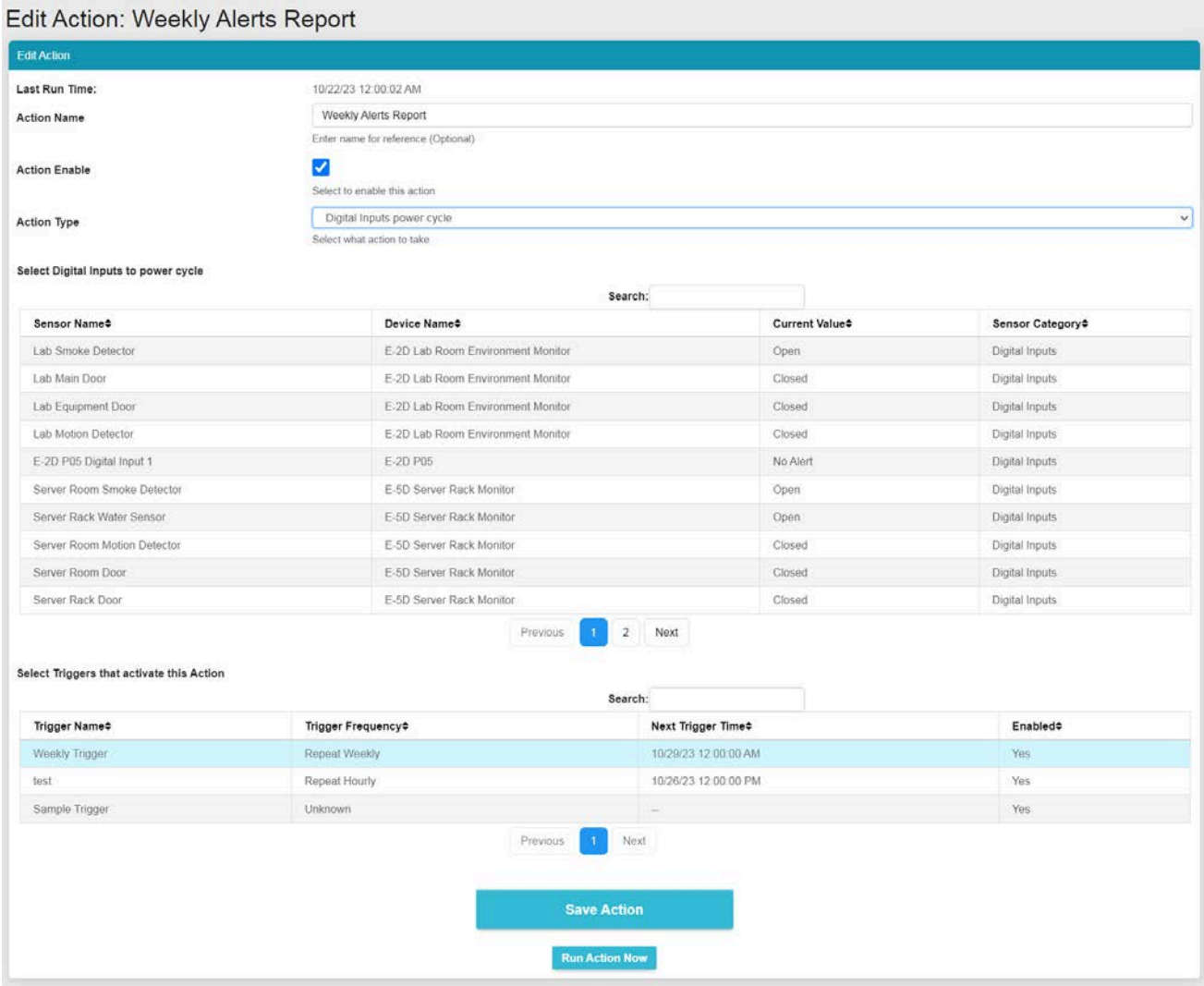


Figure 85-Action Type "Digital Inputs power cycle"

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 an existing Trigger to cause the Action to occur, 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". If the Action selected is a Report, then the Report generated by that action will appear under Reports, and if you have selected it, each user with Email Alerts enabled will also receive a pdf copy of the report. If the Action Type is any other (Operate Relay, Record IP Camera, Digital Inputs power cycle) then watch for the appropriate Action to be executed.

Triggers

Triggers determine when and how often a particular Action will be executed. For example, a Trigger for Report generation Action determines when and how often a Report gets generated. The same Trigger can be used repeatedly for as many Actions as needed.
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.

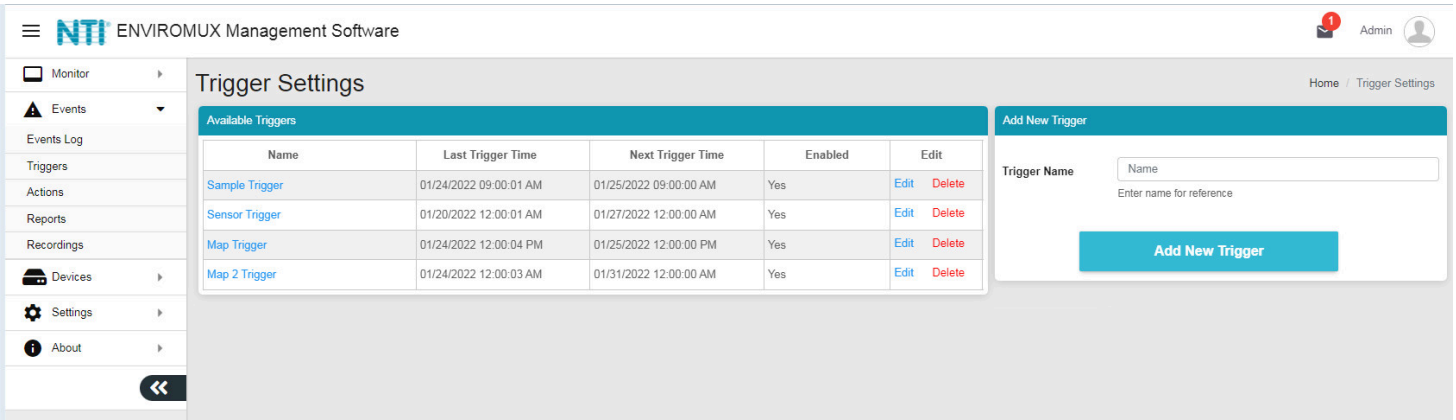


Figure 86- Trigger List

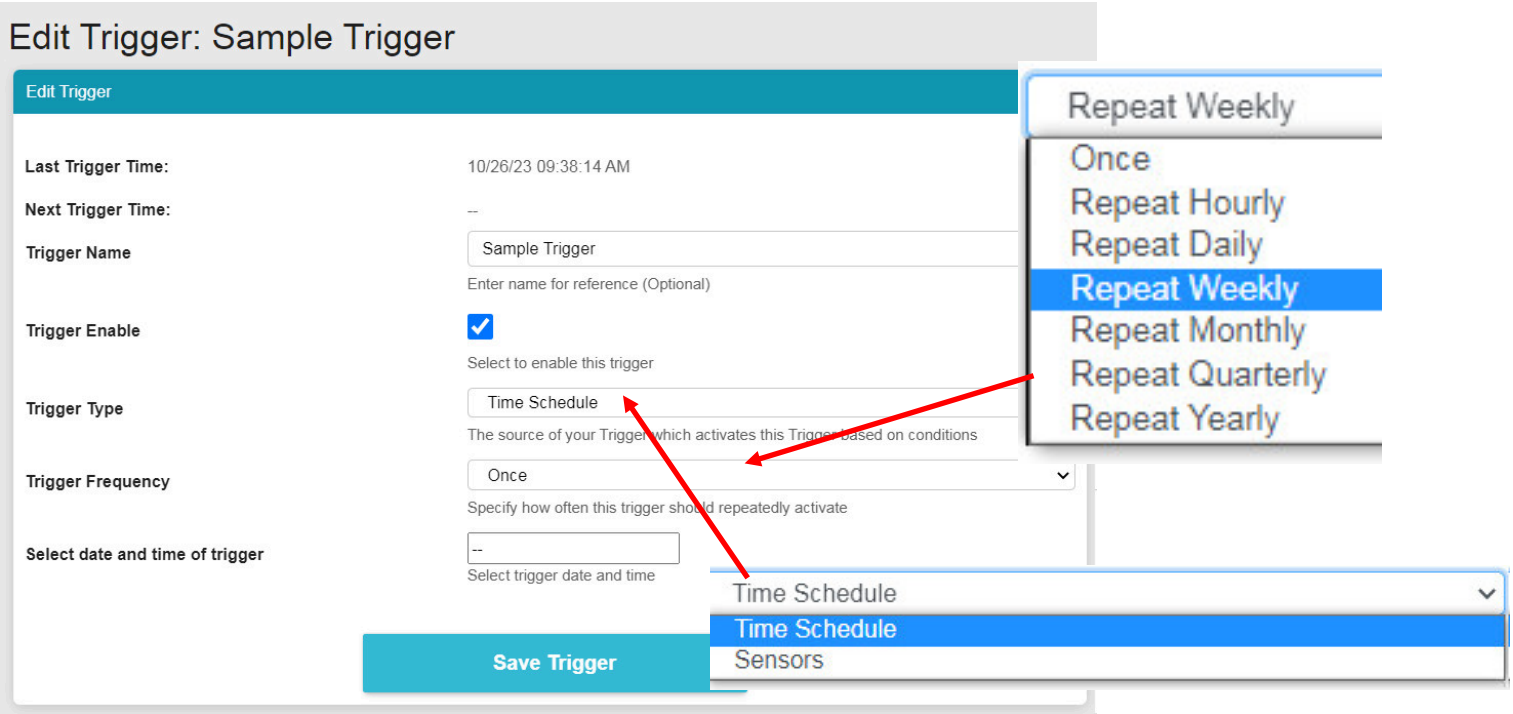


Figure 87- Trigger Options for Time Schedule Type Trigger

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.

Choose the type of trigger that will be used, one based on a Time Schedule, or one caused by the status of a sensor.

If Trigger Type is set as Time Schedule, 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 image below)

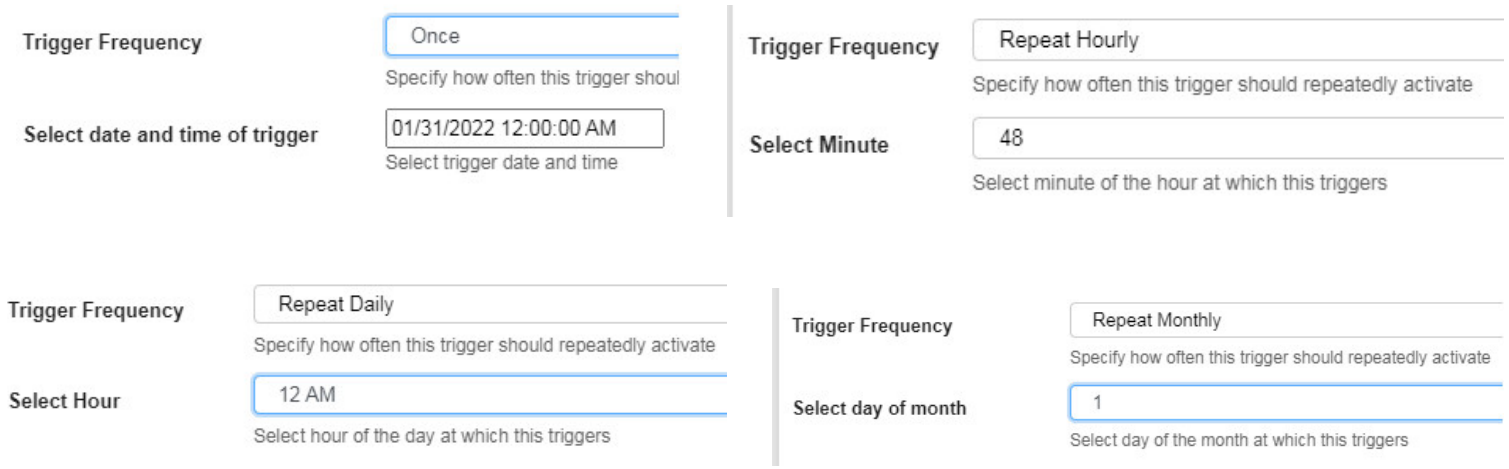


Figure 88- Option detail for Trigger Frequency

When the trigger type is set as "Sensors" (see Figure 89), the options change to sensors that are being monitored by the E-MNG-SH.

In "Select Sensor Type", choose the type of sensor (from the drop down list) to filter the selections in the list below.

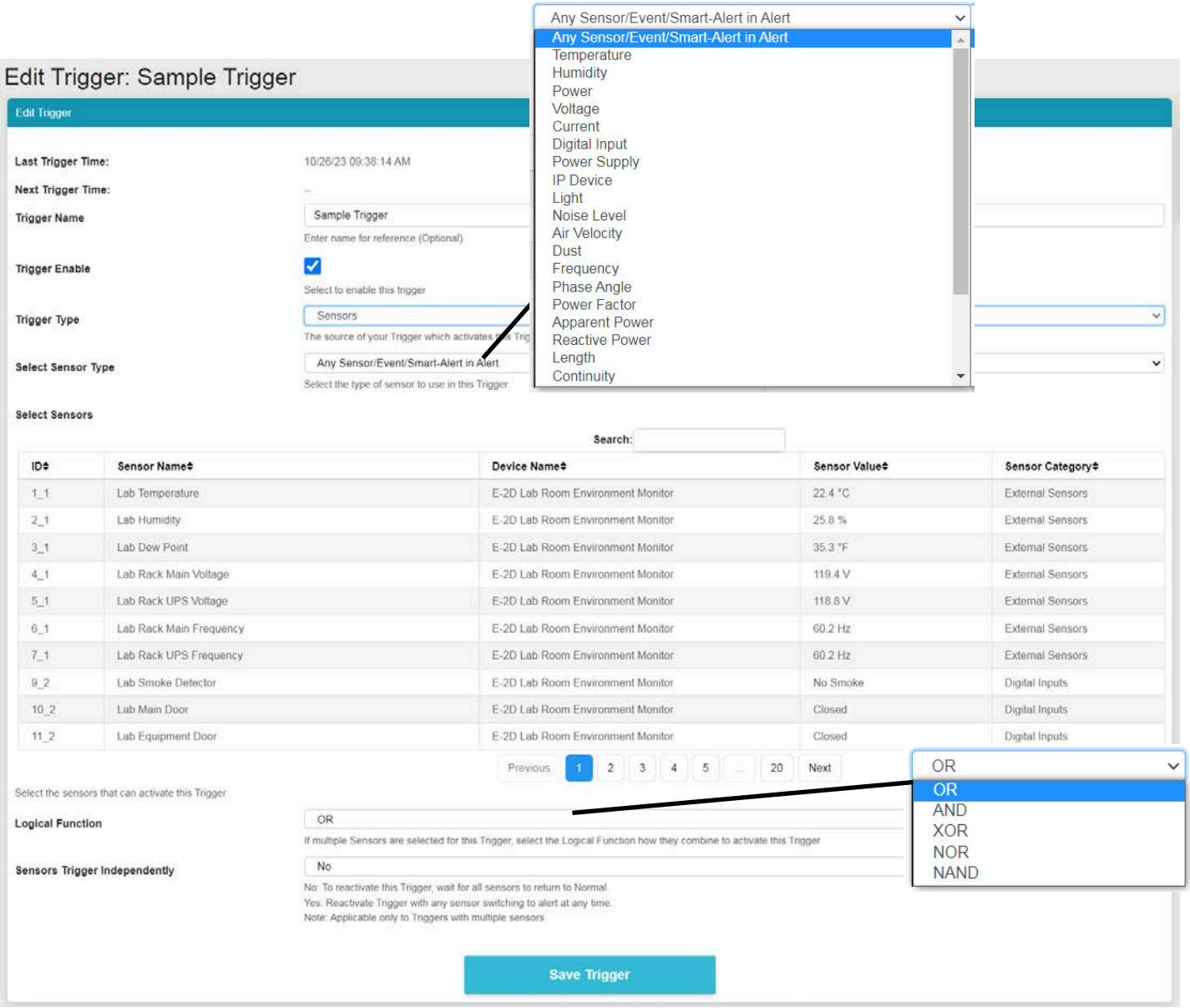
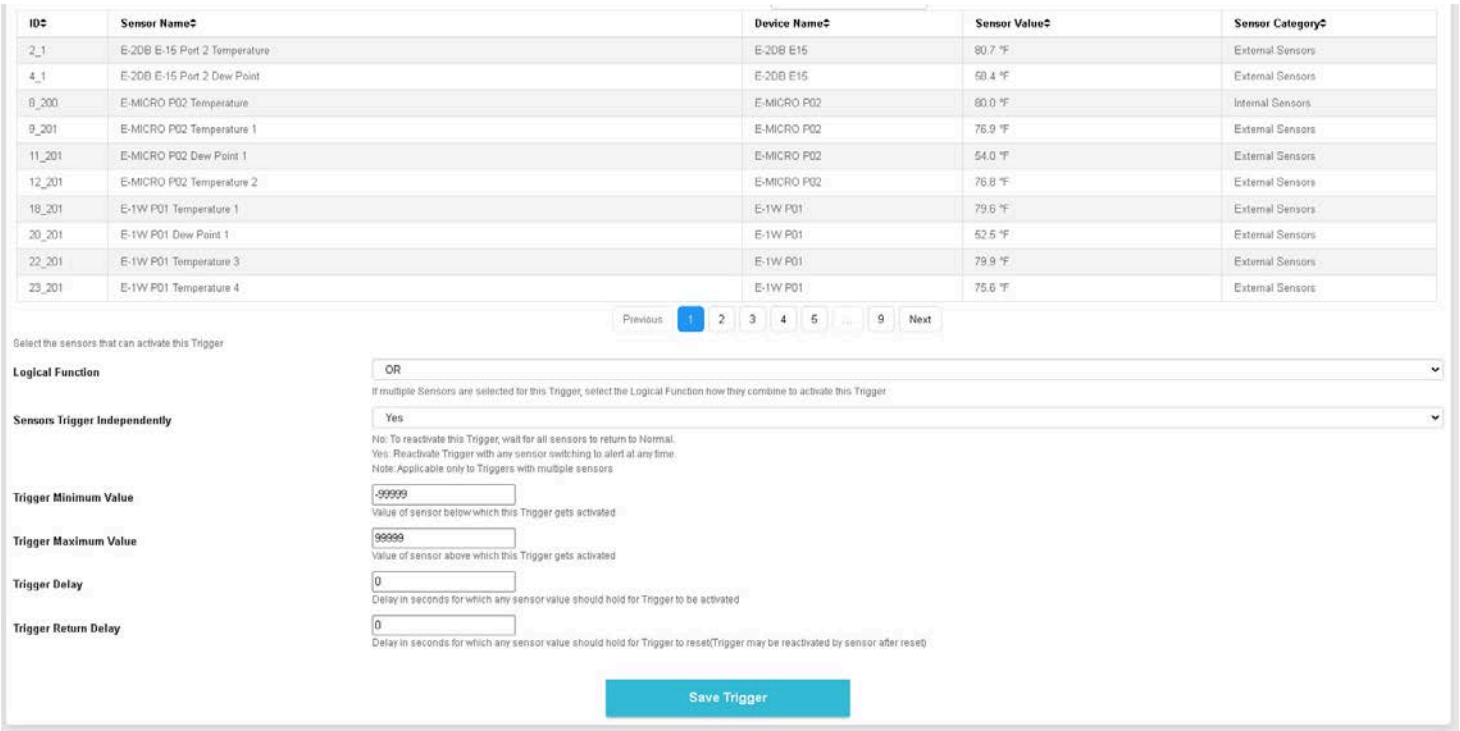


Figure 89- Trigger set as Sensor Trigger Type

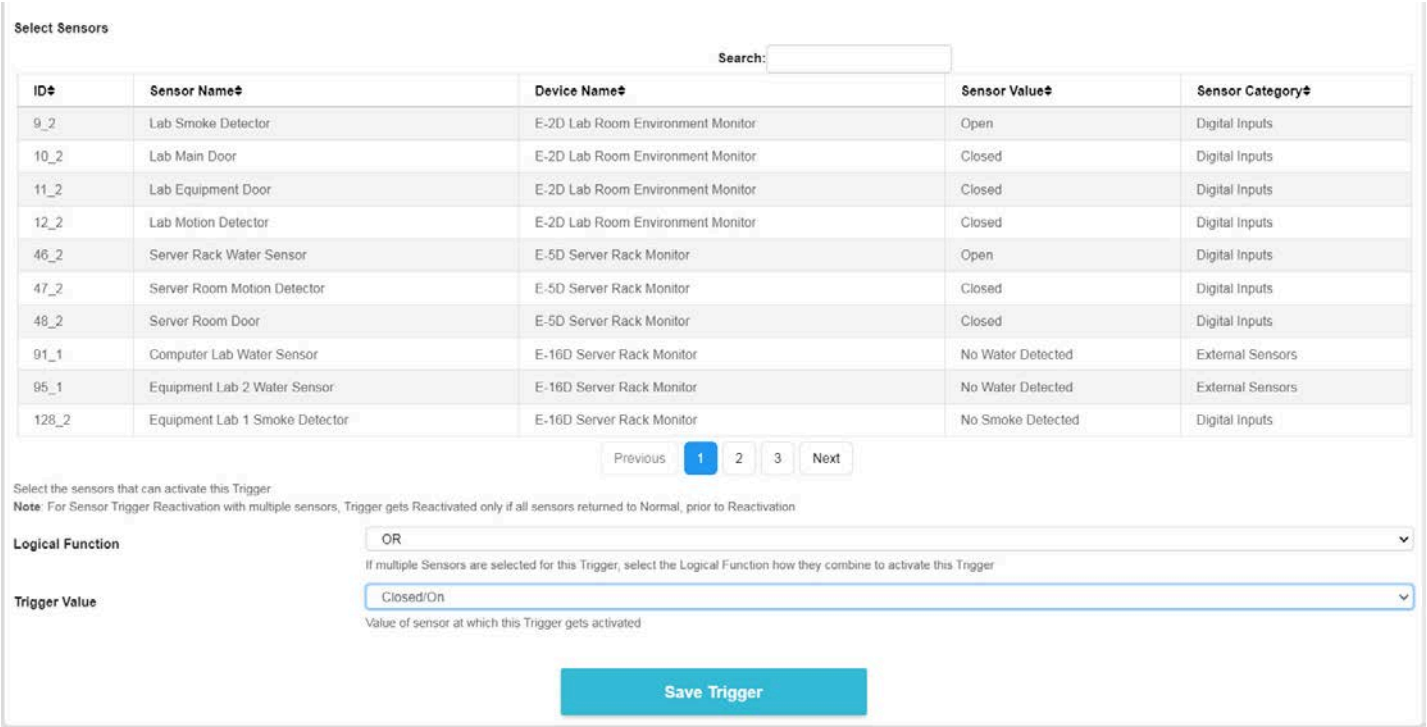
If Sensor Type selected is "Any Sensor/Event/Smart-Alert in Alert" then appropriate Sensor has to go into Alert (applicable for E-2D/5D/16D only) or appropriate Event/Smart Alert has to go into Alert on the device depending on threshold settings set on the device. If Sensor Type selected is any particular Sensor Type depending on availability on E-xD/E-MICRO-TRH(P)/E-1W, then you can set the threshold for this directly in the Management Software.

With the sensor type selected, an option will be presented to either apply the minimum or maximum value from that sensor that will trigger the action when the sensor has a range of reported values, or an on/off value to trigger the action when the sensor type is a contact sensor type. A delay can be added so that Trigger gets activated only when sensor value crosses the threshold and stays there for the time of Delay. This can be used to avoid spurious alerts when value hovers near the threshold value. A similar Delay is available when Trigger returns to normal with “Trigger Return Delay”.



ID	Sensor Name	Device Name	Sensor Value	Sensor Category
2_1	E-2DB E-15 Port 2 Temperature	E-2DB E15	80.7 °F	External Sensors
4_1	E-2DB E-15 Port 2 Dew Point	E-2DB E15	58.4 °F	External Sensors
8_200	E-MICRO P02 Temperature	E-MICRO P02	80.0 °F	Internal Sensors
9_201	E-MICRO P02 Temperature 1	E-MICRO P02	76.9 °F	External Sensors
11_201	E-MICRO P02 Dew Point 1	E-MICRO P02	54.0 °F	External Sensors
12_201	E-MICRO P02 Temperature 2	E-MICRO P02	76.8 °F	External Sensors
18_201	E-1W P01 Temperature 1	E-1W P01	79.6 °F	External Sensors
20_201	E-1W P01 Dew Point 1	E-1W P01	52.5 °F	External Sensors
22_201	E-1W P01 Temperature 3	E-1W P01	79.9 °F	External Sensors
23_201	E-1W P01 Temperature 4	E-1W P01	75.6 °F	External Sensors

Figure 90- Sensor Type Selected with a Range of Values



ID	Sensor Name	Device Name	Sensor Value	Sensor Category
9_2	Lab Smoke Detector	E-2D Lab Room Environment Monitor	Open	Digital Inputs
10_2	Lab Main Door	E-2D Lab Room Environment Monitor	Closed	Digital Inputs
11_2	Lab Equipment Door	E-2D Lab Room Environment Monitor	Closed	Digital Inputs
12_2	Lab Motion Detector	E-2D Lab Room Environment Monitor	Closed	Digital Inputs
46_2	Server Rack Water Sensor	E-5D Server Rack Monitor	Open	Digital Inputs
47_2	Server Room Motion Detector	E-5D Server Rack Monitor	Closed	Digital Inputs
48_2	Server Room Door	E-5D Server Rack Monitor	Closed	Digital Inputs
91_1	Computer Lab Water Sensor	E-16D Server Rack Monitor	No Water Detected	External Sensors
95_1	Equipment Lab 2 Water Sensor	E-16D Server Rack Monitor	No Water Detected	External Sensors
128_2	Equipment Lab 1 Smoke Detector	E-16D Server Rack Monitor	No Smoke Detected	Digital Inputs

Figure 91- Selected Sensor Type is Digital Input

With either type of sensor selected, more than one sensor in the list can be selected to trigger the action. When more than one is selected, a Logical Function should be selected to control how the sensor values will impact the trigger. Select between OR, AND, XOR, NOR and NAND logical functions.

OR - a status change in any selected senor will trigger the action
AND- a trigger will occur only if all selected sensors have a status change
XOR- a trigger will occur if one selected sensor has a status change, but not more than one sensor
NOR- a trigger will occur only if more than one selected sensor has a status change
NAND- a trigger will occur if only one sensor has a status change, or if no sensor has a status change, but it will not occur is more than one sensor has a status change.

Be sure to click "**Save Trigger**" to retain your changes.

If the Logical Function for the Trigger is OR (see Figure 89), there is another option of "Sensors Trigger Independently". Enable this setting if you like the sensors to Trigger when each and any sensor crosses threshold every time. In this case the Trigger does NOT wait for all sensors to return to normal. If this setting is disabled, the Trigger waits for all sensors to return to Normal to reactivate the trigger for any new sensor alert.

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

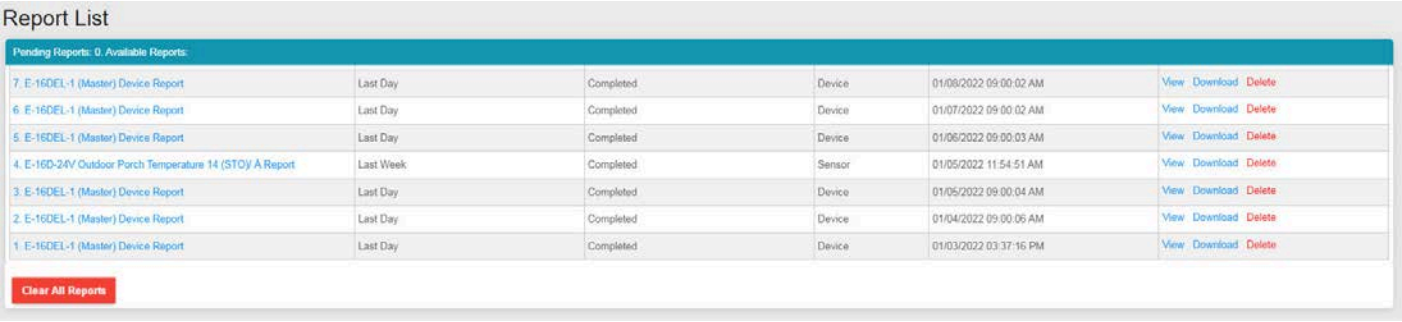


Figure 92- Reports list

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. To remove all reports at once, click "Clear All Reports"

The sensor report will provide (for one or more sensors) 1) a graph containing minimum, maximum and average sensor values, 2) a bar chart indicating the total number of alerts generated by a sensor and 3) the total length of time that sensor was in alert. The graph will contain data for the time period setup in the Report Period under Actions (page 47).

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

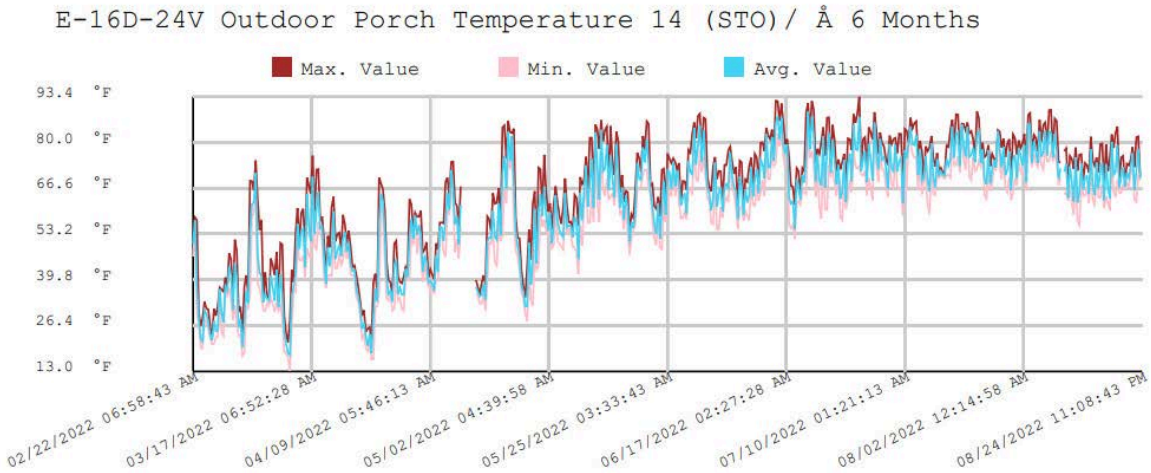
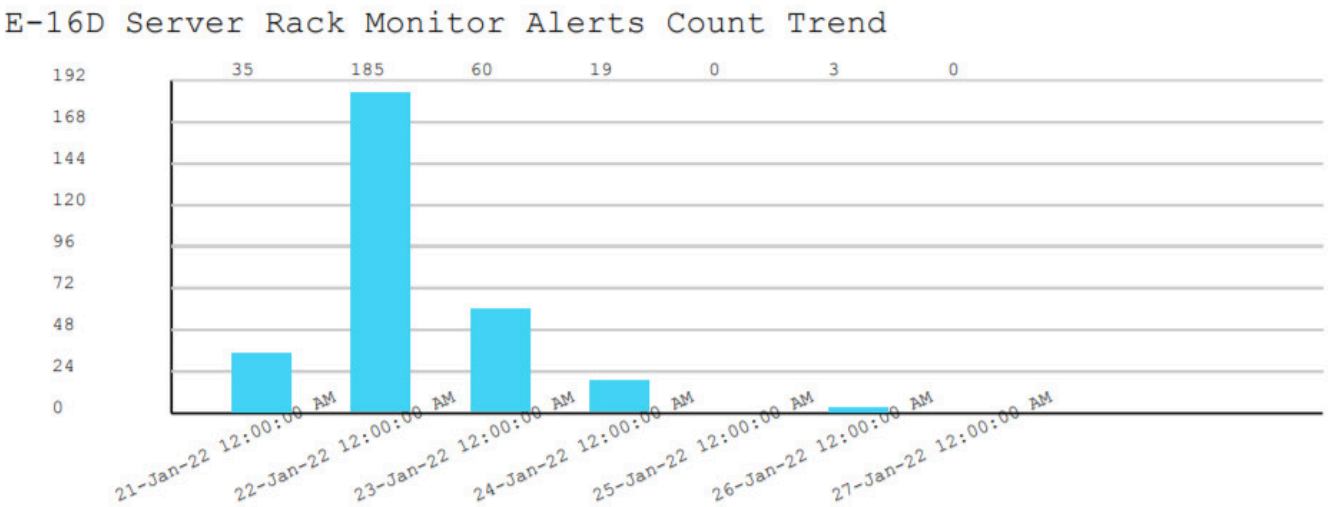


Figure 93- Report graph of an individual sensor



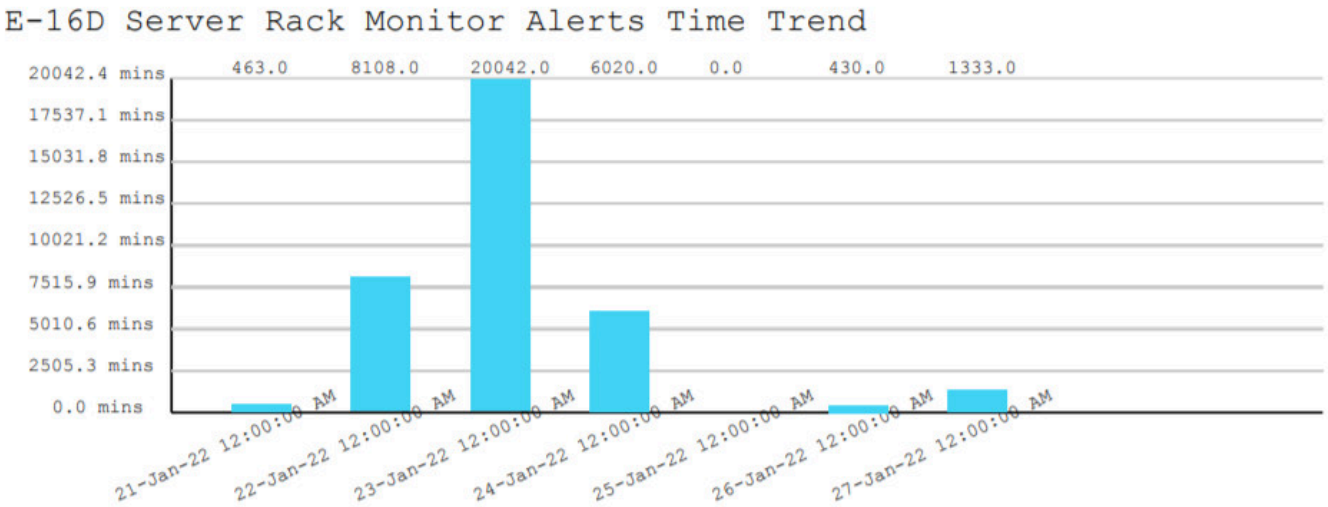


Figure 94- Report showing sensor alert trends

Current Value:	68.9 °F
Status:	Normal
Device Name:	E-16D 24V IPMI Rack
Last Alert Time:	Never
Last Alert:	--
Overall Lowest Reading:	-6.2 °F
Lowest Reading Time:	01/22/2022 05:03:23 AM
Overall Highest Reading:	93.9 °F
Highest Reading Time:	06/29/2021 02:34:22 PM
Total Alert Time:	--
Total Normal Time:	1 year 5 months 23 days
Last Update:	08/25/2022 12:00:03 AM

Figure 95- Report summary data for a sensor

Sounds

The E-MNG-SH will let you know when an sensor or device is in alert with a sound that can be heard over any speaker connected to the computer where the E-MNG-SH is being monitored. Alert warning sounds will be heard when the user is at any dashboard page that has alerts or device status windows and will sound every 120 seconds until the alert is cleared or acknowledged.

Warning sounds will not be heard if you are on the home page of the E-MNG-SH or if "Sound Alerts" is disabled in the User Setting page.

If the user has NOT used a dashboard page upon opening the tab, (for example NOT clicking or NOT scrolling on this page,) the browser may not play the alert sound. This is due to a browser restriction to prevent auto sound playback on auto-opened pages. Click on "**Enable Alert Sound**" that shows up on the dashboard page when this happens and sound alert will auto play going forward on this page.

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.

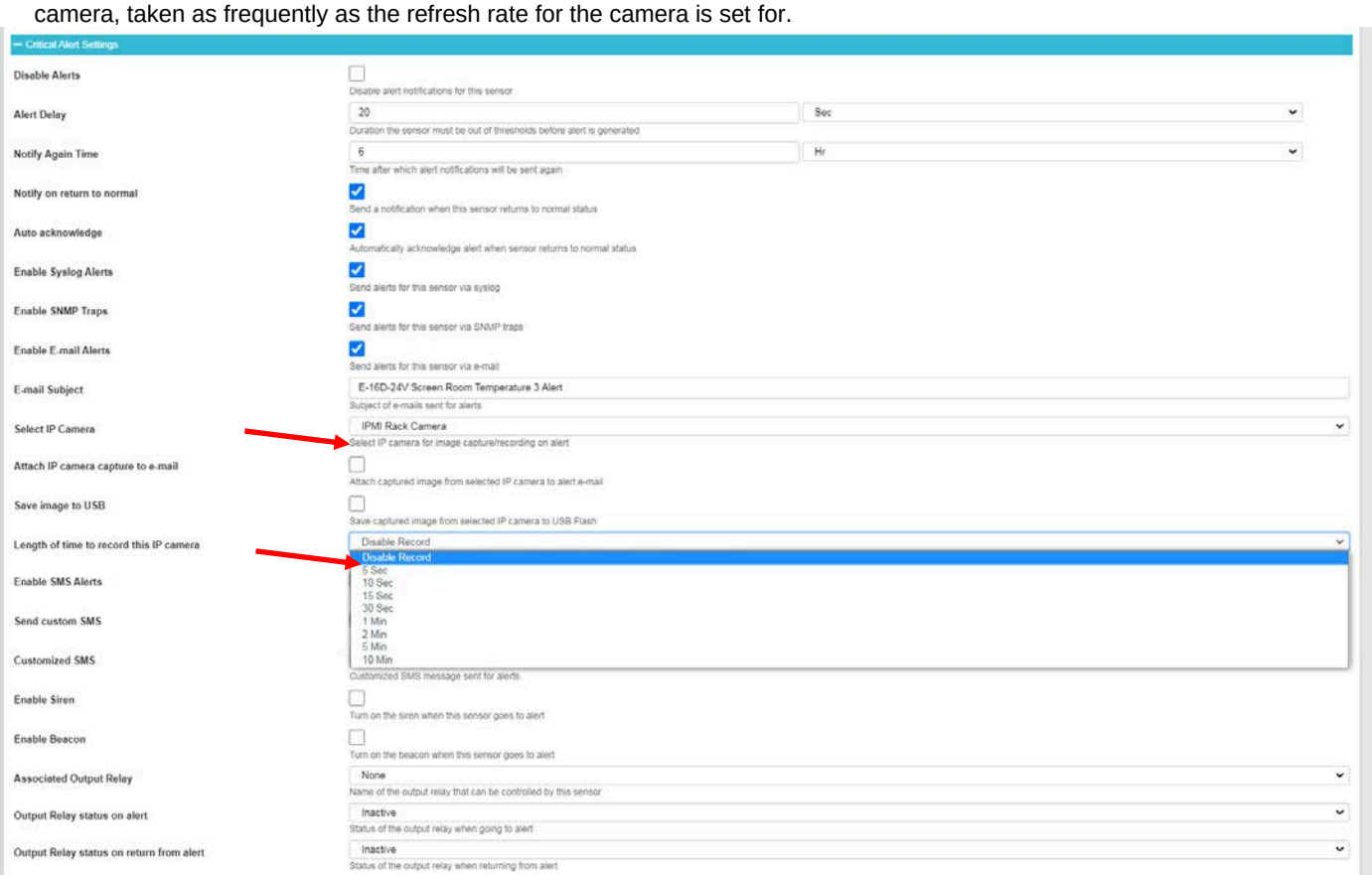


Figure 96- User settings to enable Recording

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. To clear all recordings, click “Clear All Recordings”.

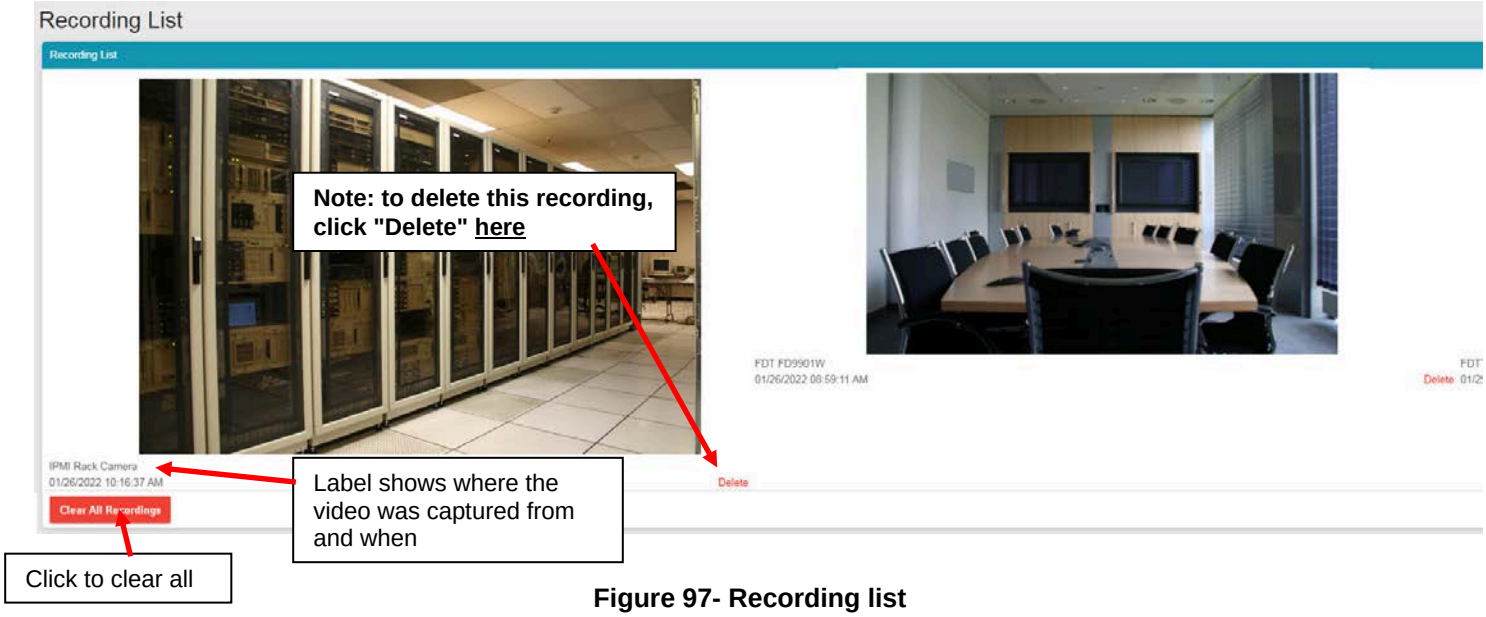


Figure 97- Recording list

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.

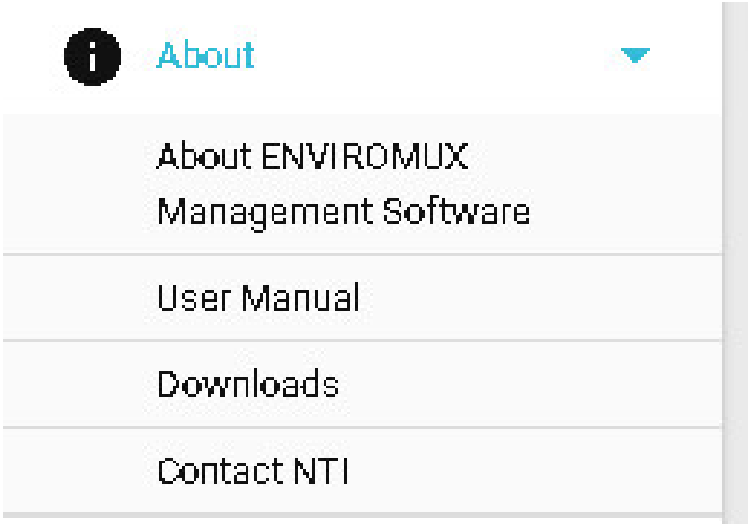
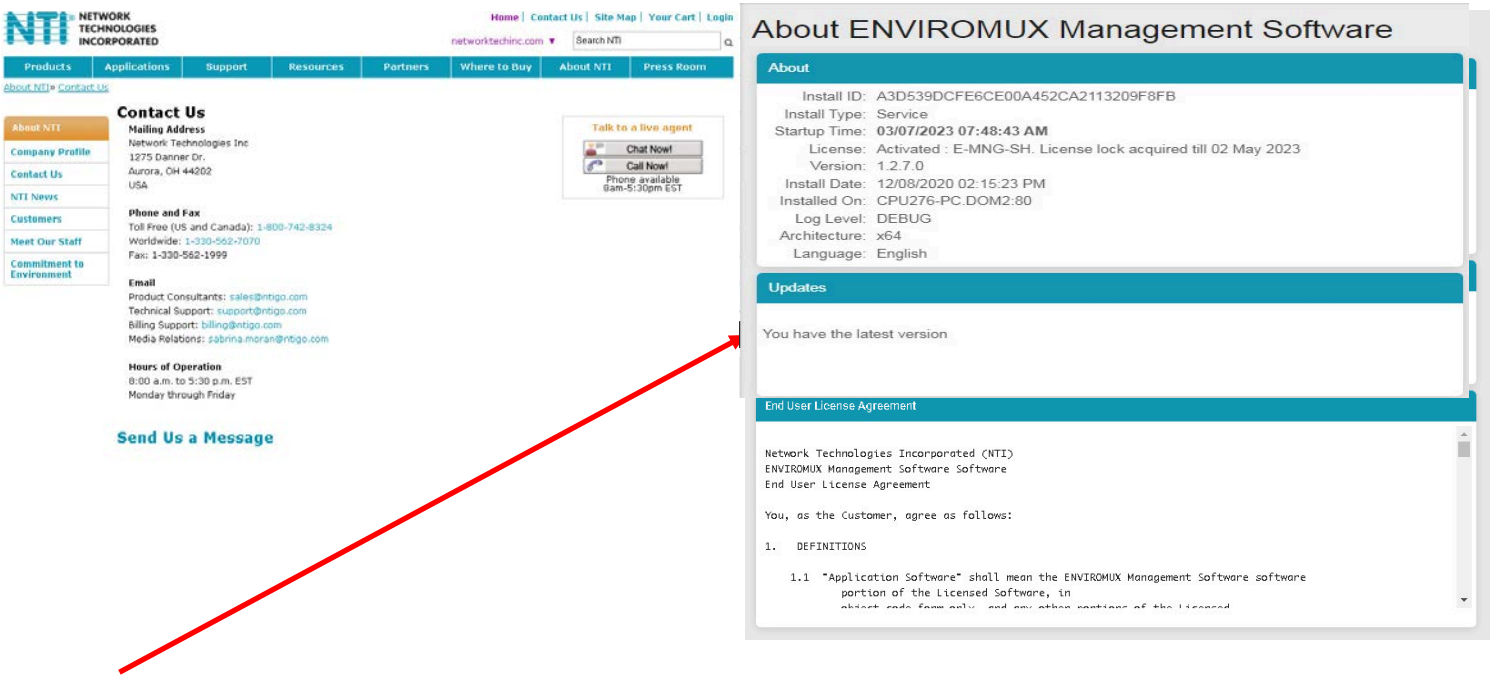


Figure 98- About menu



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

The following applies only if the software is installed as a User Application.

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

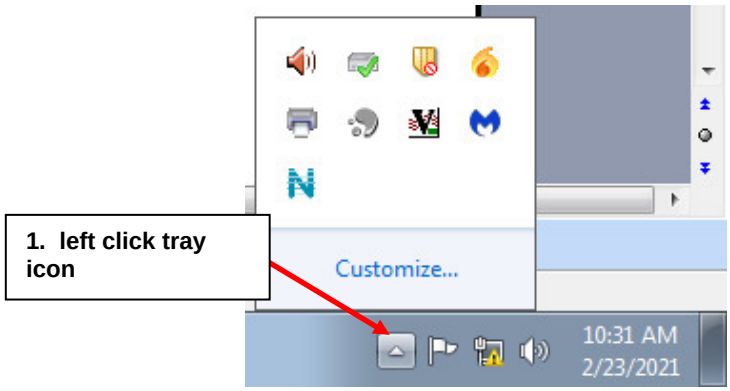


Figure 99- Click on Tray icon

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

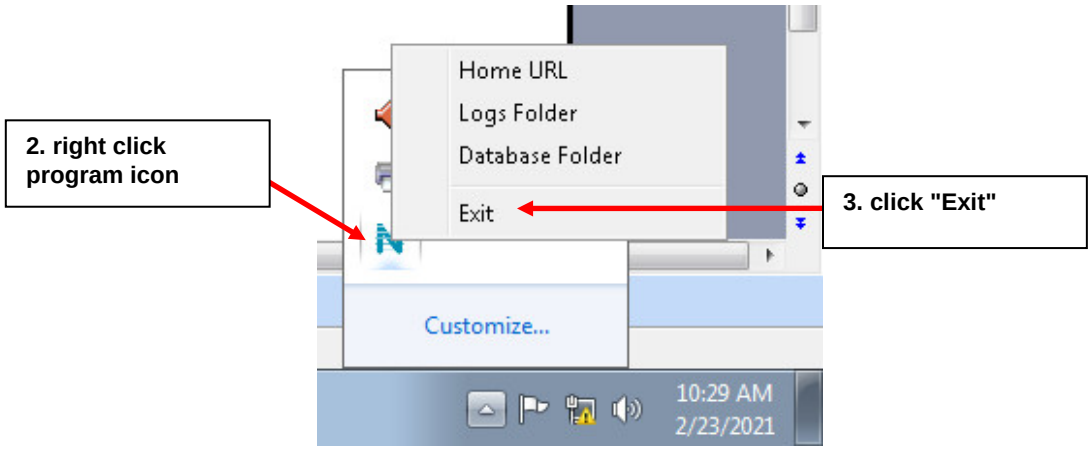


Figure 100- Exit the program

If the software is installed as a Service, the following applies.

Please open the Services application on your PC and navigate to "NTI ENVIROMUX Management Software" entry.

Right click on **Shutdown** or **Restart** as desired.

The opening and closing Tray Icon Application does not have any effect on the status of the Service in case of a "Service" Install.

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).

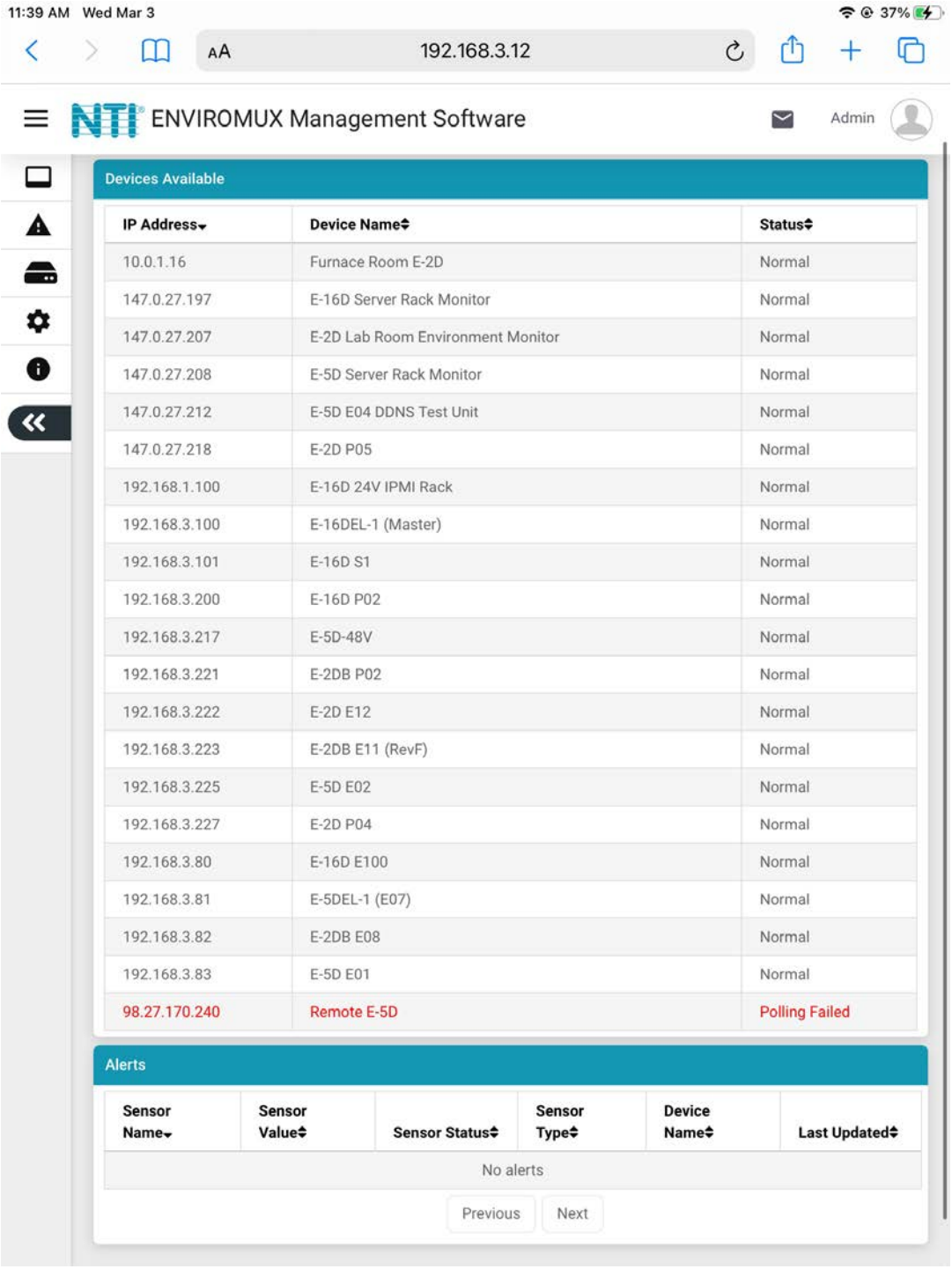


Figure 101- Screenshot from an iPad

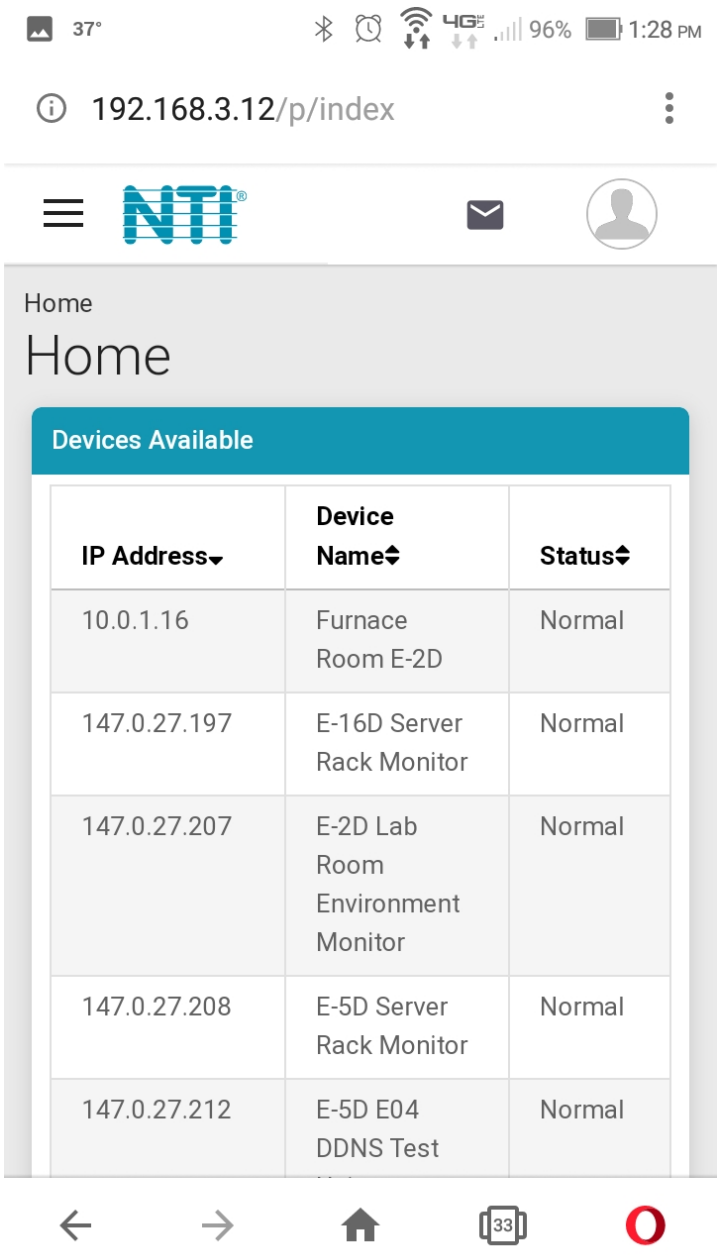


Figure 102- Screenshot from a smartphone

USER PASSWORD RESET

Any user password can be reset following the below procedure. If you are able to login as a Super Admin and want to change the password of any other users, this can be done by the Super Admin user in the User Settings page.

1. Navigate to DB folder by clicking on the tray icon for ENVIROMUX Management Software. If you have the Management Software installed in Service mode and do not see a tray icon, then you will have to start the application for the tray icon to show up.
2. Right click on the icon and Open the “Database” folder.
3. Open the **settings.db** file in a sqlite editor like “DB Browser”
4. Navigate to the “Browse Data” Tab and select Table “EMANAGER_USERS”.
5. Locate the user you want to update the password for. Set your desired password in the “PASSWORD” column in plain text.
6. Set the “PASSWORD_TYPE” column to 0.
7. Click on “Write Changes” in the menu bar above. If you are running in Service mode, you may see an error “Unable to write to file”. This error is because service writes to a protected folder. Please refer to Step 9 to solve this.
8. If you are running in Application mode, please restart the application for the new password to take effect and skip step 9.
9. If you are running in Service mode and want to write to the **settings.db** file as above, copy the **settings.db** file to the Documents folder first. Edit this **settings.db** file using steps 3-7 and “Write Changes”. Open a command prompt in Administrator mode and use the copy command to copy **settings.db** file from the Documents to the Database folder.
10. Now restart the service.
11. When the service or software is restarted, it auto encrypts the password in the Database folder and you can login with the new password.

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. Click 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.

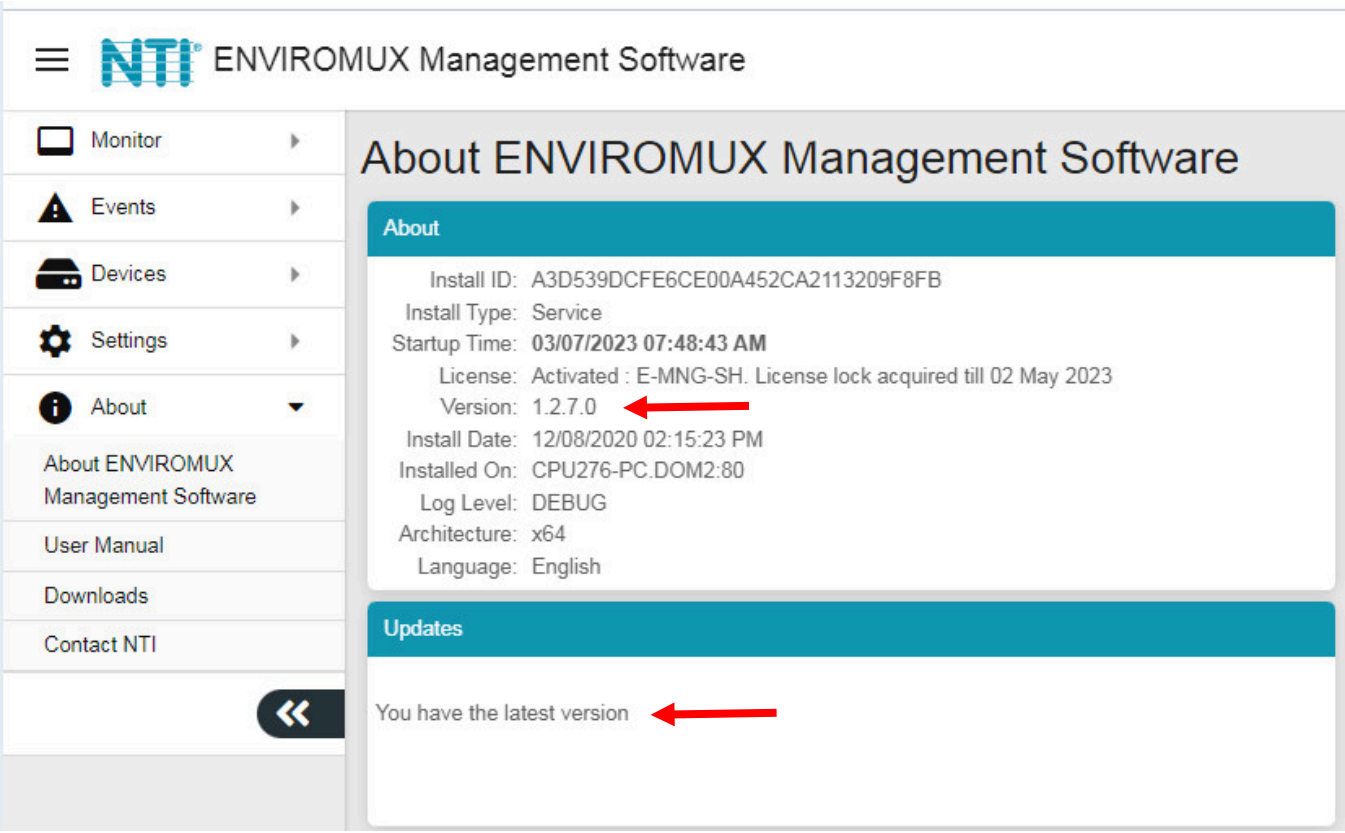


Figure 103-About page

HTTP REST API SUPPORT

Support has been built into the ENVIROMUX firmware to use JSON API to poll sensors using HTTP protocol like cURL command. To automate the interface between servers and the ENVIROMUX and provide data, the following instruction is provided.

E-MNG-SH supports the following API's that can be used to get all relevant data from the E-MNG-SH server instead of each individual device. You have to use the Login API to get the session ID first.

1. **Login API**
2. **Get Sensor List API**
3. **Get Device List API**
4. **Download Events Log API**
5. **Download Sensor Graph API**

Login API

Type: HTTP POST

Endpoint: "/api/u/login"

POST Body: email=<email>&password=<password>

Response on success: NTI session id in "Set-Cookie" HTTP Header and JSON response with code 200 and relevant success message

Response on error: JSON response with non 200 response code and error message in "msg"

Example:

Curl -vk -X POST "https://192.168.1.100/api/u/login" -d "email=guest@enviromux.com&password=guest"

Response:

HTTP/1.1 200 OK

Transfer-Encoding: chunked

Set-Cookie: **ntisid=fkal9sjks0kU02js9edjd0Jhals9qj09LSDFG24S98LsAs**; Expires=Sat, 02 Dec 2022 14:15:39 GMT; path=/; HttpOnly

Content-Type: application/json

{"code": **200**, "msg": "**Logged In..**", "data": {}}

Get Sensor List API:

Type: HTTP GET

Endpoint: "/api/u/sensor/brieflist"

Requires HTTP "Cookie" header with value "ntisid=<sid>"

Content-Type: application/json

JSON Response code if successful: 200

Response data will have array list as follows

[<Sensor_id>, <sensor_category_ID>, <Device_name>, <Sensor_name>, <current_sensor_value>, <sensor_category_name>]

Example:

curl -vk -X GET "https://192.168.1.100/api/u/sensor/brieflist" -H "Cookie: ntisid=fkal9sjks0kU02js9edjd0Jhals9qj09LSDFG24S98LsAs"

Response:


```
{
        "code": 200,
        "data":  [
                [ 14, 0, "E-2DB E08", "E-2DB E08 Input Voltage", "8.6 V", "Internal Sensors"],
                [ 20,  1, "E-2DB E08", "E-2DB E08 Temperature 1", "81.7 ◦F", "External Sensors"],
                …
        ],
        "msg": "request successful"
}
```


Sensor ID will be unique ID across all sensors of all devices except when sensor category ID is Event or Smart Alert.

Sensor ID will be unique among all Events of all devices

Sensor ID will be unique among all Smart Alerts of all devices

Sensor Category ID List:

NTI_SENSOR_CATEGORY_INVALID = -10,

NTI_SENSOR_CATEGORY_EXD_INTERNAL = 0,

NTI_SENSOR_CATEGORY_EXD_EXTERNAL = 1,

NTI_SENSOR_CATEGORY_EXD_DIGITAL_INPUT = 2,

NTI_SENSOR_CATEGORY_EXD_IP_DEVICE = 3,

NTI_SENSOR_CATEGORY_EXD_SNMP = 4,

NTI_SENSOR_CATEGORY_EXD_IP_SENSOR = 7,

NTI_SENSOR_CATEGORY_EXD_IP_INT_SENSOR = 8,

NTI_SENSOR_CATEGORY_EXD_IP_SENSOR = 8,

NTI_SENSOR_CATEGORY_EXD_IP_EXT_SENSOR = 9,

NTI_SENSOR_CATEGORY_EXD_IP_DIGINP_SENSOR = 10,

NTI_SENSOR_CATEGORY_EXD_TAC = 12,

NTI_SENSOR_CATEGORY_EXD_OUTPUT_RELAY = 100,

NTI_SENSOR_CATEGORY_EXD_POWER = 101,

NTI_SENSOR_CATEGORY_IP_CAMERA = 103,

NTI_SENSOR_CATEGORY_EXD_EVENTS = 104,

NTI_SENSOR_CATEGORY_EXD_SMART_ALERTS = 105,

NTI_SENSOR_CATEGORY_EXD_SENSOR_HUB = 106,

NTI_SENSOR_CATEGORY_EMICRO_1W_INTERNAL = 200,

NTI_SENSOR_CATEGORY_EMICRO_1W_EXTERNAL = 201,

NTI_SENSOR_CATEGORY_EMICRO_1W_DIGITAL_INPUT = 202,

NTI_SENSOR_CATEGORY_EMICRO_1W_IP_DEVICE = 203,

NTI_SENSOR_CATEGORY_EMICRO_1W_EVENTS = 204,

NTI_SENSOR_CATEGORY_EMICRO_1W_SMART_ALERTS = 205,

NTI_SENSOR_CATEGORY_MAP = 300,

Get Device List API

Type: HTTP GET

Endpoint: "/api/u/monitor/getwindeviceslist"

Requires HTTP "Cookie" header with value "ntisid=<sid>"

Content-Type: application/json

JSON Response code if successful: 200

Response "data" will have an "sdata" array list as follows

[<Device_IP_Address_in_anchor_tag>, <Device Name>, <Device_Status>]

Example:

curl -vk -X GET "https://192.168.1.100/api/u/monitor/getwindeviceslist" -H "Cookie: ntisid=fkal9sjks0kU02js9edjd0Jhals9qj09LSDFG24S98LsAs"

Response:

{

"code": 200,

"data": {

"id_window": 0,

"sdata": [

["192.168.1.100", "E-2DB- E08", "Normal"],

["192.168.1.101", "E-16DB- D05", "Alert"],

…

]

},

"msg": "request successful"

}

Download Events Log API

Type: HTTP GET or HTTP HEAD

Endpoint: "/api/u/events/log/download"

Requires HTTP "Cookie" header with value "ntisid=<sid>"

Content-Type: application/octet-stream

Content-Disposition: attachment;filename="event_log_<timestamp>.txt

If successful HTTP Response code: 200 followed by tab delimited event log data:

<Time>\t<Record Type>\t<Message>\t<Log Level>\t<Device>\t<Sensor>\t<Unix Timestamp>

HTTP Response code if error: 401

Example:

curl -vk -X GET "https://192.168.1.100/api/u/events/log/download" -H "Cookie: ntisid=fkal9sjks0kU02js9edjd0Jhals9qj09LSDFG24S98LsAs"

Response:

HTTP/1.1 200 OK

Transfer-Encoding: chunked

Content-Type: application/octet-stream; name="event_log_1688938293.txt"

Content-Disposition: attachment;filename="event_log_1688938293.txt"

Time Record Type Message Log Level Device Sensor Unix Timestamp

07/05/2022 04:39:55 PM <\t> Alert <\t> Sensor 2. E-16D E100 on 4G went into Alert on device Remote E-5D <\t> 3 <\t>Remote E-5D<\t>E-16D E100 on 4G <\t> 1688928394894<\r\n>

Download Sensor Graph API

Type: HTTP GET or HTTP HEAD

Endpoint: "/api/u/device/sensors/getgraph"

Requires HTTP "Cookie" header with value "ntisid=<sid>"

Requires HTTP GET variables: "period_index =1&cat_type=<Sensor_category_ID>&emng_id_sensor=<Sensor_ID>"

Period Index is the period for which to download this sensor graph for. Period index can be selected from list below:

Graph Periods Available:

PERIOD_1HR = 0,

PERIOD_8HR = 1,

PERIOD_2D = 2,

PERIOD_1WK = 3,

PERIOD_1MO = 4,

PERIOD_6MO = 5,

PERIOD_2YR = 6

cat_type is the sensor category ID shown in Get All Sensor List API

emng_id_sensor is the sensor ID that is unique to all sensors

Example response with graph data loaded:

Response Content-Type: application/json

If successful JSON response code will be 200 otherwise it will have appropriate response code along with error message like 401 for invalid credentials

Even if JSON response code is 200, graph data may not have loaded in response.

To confirm if data was loaded please check the response variable [‘data’][‘loaded’].

If this is true, data was available when API was called and [‘data’][‘sdata’] now contains sensor graph data for selected period

If [‘data’][‘loaded’] is false, this sensor’s graph data was not loaded to memory at the time of request. However this auto triggers a load request. So please try again in 3-5 seconds by which time graph data would have been loaded.

Format of sensor data is as below. ‘sdata’ key will have 3 arrays each for Maximum, Minimum and Average values within that period of time slice. As in example below, [‘data’][‘sdata’][0][‘values’] will have an array of dictionary of x to timestamp and y to Maximum sensor values


```
{
    "code": 200,
    "data": {
        "high_label": "Triggered",
        "loaded": true,
        "low_label": "Normal",
        "sdata": [{
            "area": false,

            "color": "brown",
            "key": "Max.",
            "max_val": 114.2,
            "min_val": 119.4,
```

```
                "unit": " V",
                "values": [{"x":1690542680206, "y": 114.2}, {"x":1690542737806, "y": 114.1} ….]
            }, {
                "area": false,
                "color": "pink",
                "key": "Min.",
                "max_val": 117.2,

                "min_val": 0,
                "unit": " V",
                "values": [{"x":1690542680206, "y": 117.2}, {"x":1690542737806, "y": 117.0} ….]
            }, {
                "area": false,
                "color": "#42d4f4",
                "key": "Avg.",
                "max_val": 121.2,
                "min_val": 120.4,
                "unit": " V",
                "values": [{"x":1690542680206, "y": 121.0}, {"x":1690542737806, "y": 120.9} ….]
            }],
            "tick_format": 1,
            "valtype": 3
        },
        "msg": "request successful"
}
```


Example response with graph NOT loaded:

curl -vk -X GET "https://192.168.1.100/api/u/device/sensors/getgraph?period_index=1&cat_type=2&emng_id_sensor=14" -H "Cookie: ntisid=fkal9sjks0kU02js9edjd0Jhals9qj09LSDFG24S98LsAs"

Response:

HTTP/1.1 200 OK

Content-Type: application/json


```
{
        "code": 200,
        "data": {
            "high_label": "Triggered",
```

```
                "loaded": false,
                "low_label": "Normal",
                "sdata": [{
                        "area": false,
                        "color": "brown",
                        "key": "Max.",
                        "max_val": -899998.2000000001,
                        "min_val": 899999.10,
                        "unit": " V",
                        "values": null
                }, {
                        "area": false,
                        "color": "pink",
                        "key": "Min.",
                        "max_val": -899998.2000000001,
                        "min_val": 899999.10,
                        "unit": " V",
                        "values": null
                }, {
                        "area": false,
                        "color": "#42d4f4",
                        "key": "Avg.",

                        "max_val": -899998.2000000001,
                        "min_val": 899999.10,
                        "unit": " V",
                        "values": null
                }],
                "tick_format": 1,
                "valtype": 3
        },
        "msg": "request successful"
}
```

INDEX

Man372 Rev 5/15/25