nLight Operation, Programming and Maintenance Manual

Project Name:
Project Location:
Acuity Agency:
Order #:
PO #:
Project ID:
Date:

Controls Tech Support:

1-800-535-2465 - option 1: nLight; option 2: SSI; option 3: Fresco; option 4: Synergy; option 5: LC&D/Bluebox; option 6 ROAM

To preschedule a call with tech support (providing a 4-hour business lead time) go to the following link: http://www.acuitybrands.com/resources/schedule-support-request

Additional Technical Literature:
https://www.acuitybrands.com/products/controls/nlight

Table of Contents

HARDWARE MANUAL

nLIGHT®

sensorswitch

An Acuity Brands Company

nLIGHT®

CONTENTS

1 nLIGHT® CONTROL SYSTEM OVERVIEW

1 INTRODUCTION

What is nLight?

nLight is a technology that integrates time-based, occupancy-based, daylight-based, and manual lighting control.

How does nLight work?

nLight works by establishing a digital communication network between intelligent lighting control devices, including: occupancy sensors, photocells, power/relay packs, wall switches, panels and dimmers. This creates a system with distributed intelligence, as well as enables global access to the building's lighting system via web-based management software calledSensorView.

What is Distributed Intelligence?

Distributed intelligence means that all lighting control actions, such as turning on/off or dimming lights, are carried out locally within each individual lighting zone. This feature reduces the wiring requirements and associated labor costs. Additionally, distributed intelligence enables each zone of nLight devices to self-commission and function independently, while still benefiting from being part of a larger networked system.

OCCUPANCY + DAYLIGHTING + TIME-BASED + MANUAL = nLIGHT®

How are nLight devices similar to other Sensor Switch sensors?

All occupancy and daylighting features from Sensor Switch's standard (non-nLight) product lines have been integrated into corresponding nLight devices. This includes Passive Infrared and Microphonics occupancy detection technologies, 0-10 VDC dimming control, stepped dimming control, automatic photocell set-point programming, 100 hr burn-in control, etc.

1.2 SYSTEM ARCHITECTURE

The nLight architecture is based on the five underlying concepts defined in this section:

- nLight Enabled Device
- nLight Control Zone
- nLight Channels
- nLight Operational Modes
- nLight Backbone

1.2.1 nLIGHT ENABLED DEVICE

DEFINITION
A device having the ability to communicate over an nLight network.

nLight Enabled devices are the most basic elements in the nLight architecture and have model numbers beginning with the letter “n” (e.g., **nCM9**).

Types of nLight Enabled devices include occupancy sensors, photocell sensors, power/relay packs, relay/dimming panels, WallPods, and luminaires.

All nLight Enabled devices are equipped with RJ-45 communication ports.

All devices consist of one or more basic lighting control components.

- Occupancy sensor
- Photocell
- Manual Switch
- Dimmer
- Relay
- Interface Devices (for luminaires)

See reference section for detailed feature descriptions of all nLight enabled devices.

1.2.2 **nLIGHT® CONTROL ZONE**

DEFINITION
A collection of nLight Enabled devices that function together in order to control a distinct space's lighting

An example of a typical nLight zone is an office lobby with an nLight Enabled occupancy sensor, power/relay pack, and WallPod controlling the lighting.

Zones…

…may consist of a single device, several different device types, or multiple devices of the same type.

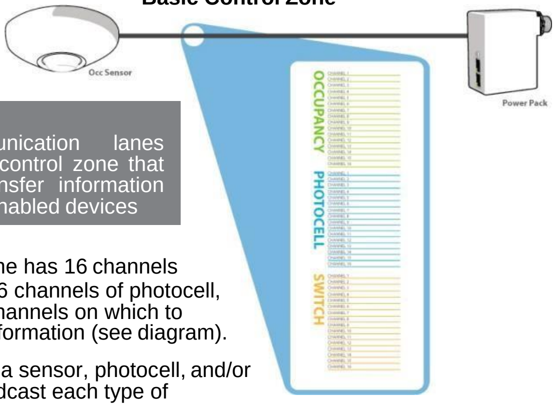
…use CAT5e cables to interconnect devices (daisy chained in any order).

…may have 1,500 ft of total cable length.,

…can function stand-alone if disconnected from Gateway/SensorView.

1.2.3 nLIGHT® CHANNELS

Basic Control Zone



DEFINITION
Distinct communication lanes within an nLight control zone that are used to transfer information between nLight enabled devices

Every nLight zone has 16 channels of occupancy, 16 channels of photocell, and 16 switch channels on which to communicate information (see diagram).

Any device with a sensor, photocell, and/or switch can broadcast each type of information on one respective channel.

For Example:

- An occupancy sensor (e.g., nCM 9) can broadcast its occupancy information on an occupancy channel (1-16).
- A combined occupancy sensor and photocell (e.g., nCM 9 P) can broadcast its occupancy information on an occupancy channel (1-16) and its photocell information on a photocell channel (1-16).
- WallPods can broadcast manual switches on a switch channel (1-16).

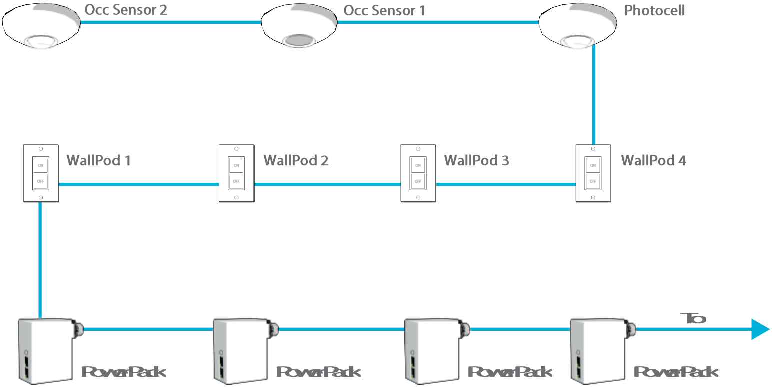
Any device with a relay and/or dimming output can listen (track) on one or more of each information type's channels simultaneously.

By default all broadcasting and tracking settings are set to channel 1. Two pole units default to channels 1 & 2, scene controller buttons default to 1-4.

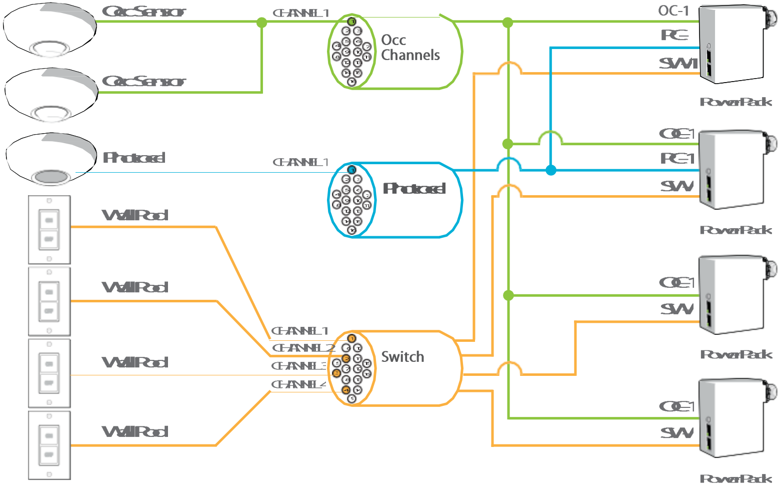
Example Zone Using Multiple Channels

- Classroom with 4 circuits of lights (3 main light rows, 1 white board light)
- Two occupancy sensors both broadcasting on occupancy channel OC-1
- Four WallPods broadcasting on switch channels SW-1, SW-2, SW-3, and SW-4 respectively
- One photocell broadcasting on photocell channel PC-1
- Four power packs tracking on occupancy channel OC-1, each tracking a different switch channel (SW-1, SW-2, SW-3, SW-4), and two tracking photocell channel PC-1

Physical Device Connections



Logical Channel Connections



1.2.4 nLIGHT OPERATIONAL MODES

DEFINITION
The behavior of relays and/or dimming outputs when events such as occupancy, daylight, or manual switching occur

Operational Modes are defined by device settings (see list and definitions below) that can be programmed via SensorView or device push-button. The default operational mode of a device is stored within each device, however temporary modes can be enabled on demand from SensorView or via a time-based profile.

NORMAL

The name of the state where a device's relay and/or dimming output is not overridden and therefore will react according to the other operational mode settings. When all devices are running their factory defaults, the following operation results:

Automatic On

Zones with occupancy sensors automatically turn lights on when occupant is detected

Automatic Off

Zones with occupancy and/or photocell sensors turn lights off when vacancy or sufficient daylight is detected

Permanent Off

Pressing the switch will turn lights off. The lights will remain off regardless of occupancy until switch is pressed again, restoring the sensor to Automatic On functionality

OVERRIDE ON

Forces a device's relay closed and/or dimming output to maximum

OVERRIDE OFF

Forces a device's relay open and/or dimming output to minimum

OCCUPANCY BROADCASTING (Enabled/Disabled)
Indicates whether a sensor is allowed to communicate its occupancy information to the rest of its zone

PHOTOCELL BROADCASTING (Enabled/Disabled)
Indicates whether a sensor is allowed to communicate its photocell information to the rest of its zone

SWITCH BROADCASTING (Enabled/Disabled)
Indicates whether a device w/ a manual switch is allowed to communicate its switch status to the rest of its zone

OCCUPANCY TRACKING (Enabled/Disabled)
Indicates whether a device's relay or dimming output will react to occupancy information

PHOTOCELL TRACKING (Enabled/Disabled)
Indicates whether a device's relay or dimming output will react to photocell information

SWITCH TRACKING (Enabled/Disabled)
Indicates whether a device's relay or dimming output will react to manual switching information

SPECIAL MODES
Pre-defined behavior for relay and/or dimming outputs. Special Modes are selectable via SensorView or device push-button.

Auto to Override On:

- Changes Override setting from Normal to Override On after occupancy is first detected
- Override On can be set to expire after a timer expires
- Related Settings: Timed Override Delay (5 min, 10 min, 15 min, 20 min, 25 min, 30 min, 45 min, 1 hr,1.5 hr, 2 hr, 3 hr, 6 hr, 9 hr, 12 hr, Infinite)

SPECIAL MODES CONT

Manual to Override On:

- Changes Override setting from Override Off to Override On
- Override On can be set to expire after a timer expires
- Related Setting: Timed Override Delay (5 min, 10 min, 15 min, 20 min, 25 min, 30 min, 45 min, 1 hr,1.5 hr, 2 hr, 3 hr, 6 hr, 9 hr, 12 hr,Infinite)

Manual On to Fully Automatic:

- Changes Override setting from Override Off to Normal after switch is first used

Semi-Automatic (Manual On):

- Changes Override setting from Override Off to Normal after each time switch is first used and from Normal to Override Off after sensor times out

Predictive Off:

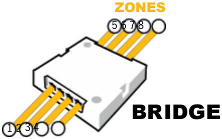
- After switch is pressed, lights turn off and a short “exit timer” begins. After timer expires, sensor scans the room to detect whether occupant is still present. If no occupancy is detected, zone returns toauto-on

1.2.4 nLIGHT® BACKBONE

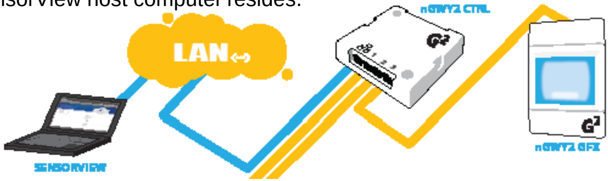
DEFINITION:
The communication network which interconnects nLight zones and the SensorView software

An nLight network backbone consists of special nLight Enabled devices called “Bridges” and “Gateways” that work together to transport and route information between control zones and the SensorView software.

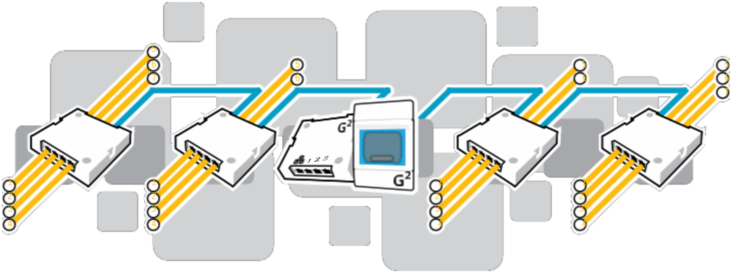
Within a typical nLight network, multiple zones are wired individually to a Bridge. Bridges act as hubs by aggregating communication traffic from these connected zones and placing it onto the backbone. They also act as routers by forwarding information from the backbone out to the applicable zones.



The second type of device on the nLight network backbone is the Gateway. The Gateway links the backbone to an Ethernet network where the SensorView host computer resides.



An nLight network backbone can consist of multiple Bridges and one Gateway deployed in virtually any physical topology. Communication between backbone devices is done over wired CAT5e connections.



BRIDGES (nBRG8)

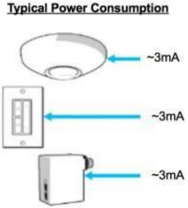
- Increases number of lighting zones (128 devices per port)
- Acts as both a hub and router of information between zones and Gateway
- Redistributes power between zones (covered in system powering section)

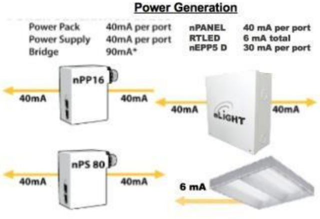
GATEWAYS (nGWY2, nGWY2 400)

- Links Ethernet to nLight network
- Stores profiles created by SensorView
- Sends out new profile settings to specified devices at specified times
- Enables profiles to be run on-demand
- Maintains time clock

1.3 SYSTEM POWER

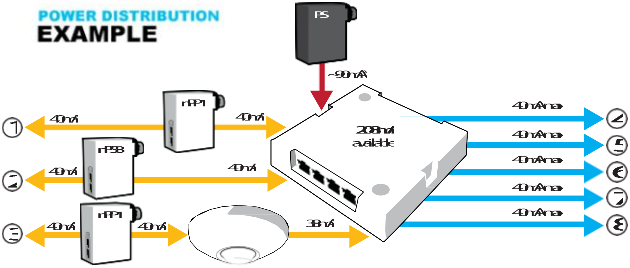
All non-backbone device and communication power is delivered via the CAT5e bus that interconnects zones and Bridges. Power to the bus is supplied from power/relay packs (nPP 16), power supplies (nPS 150), Bridges, and Acuity Luminaires.





Bridges combine system power from zones that are net contributors of power (i.e. those with downstream power packs and power supplies) and distribute it to zones that are net consumers of power (i.e. those with only sensors and WallPods).

Zones with power packs can run independently, even if communication with a Gateway or Bridge is lost or not present by design. Zones without power packs will function as long as communication with a Bridge is present.



*An external power supply provides power to a Bridge, 80mA of which is available for distribution to zones

1.4 SYSTEM CONTROL

nLight provides users both local control (via a WallPod or nGWY2) and remote control (via Virtual WallPod for PC/iOS or SensorView software)

WallPod®

The simplest level of user control is via WallPod. These single gang devices are found within a lighting zone, providing manual control of a zone's lighting.

Virtual WallPods

With the Virtual WallPod applications, users can control their lighting from their desktop or iOS mobile device. Designed to look like WallPods®, these applications are an excellent alternative to remote controls, which are often lost and require battery replacement. Simple user permissions provide facility managers necessary administrative control.

nGWY2

In addition to its role in nLight network communication, the Gateway provides a local user interface for accessing any of its up to 1500 downstream devices. Via its LCD panel and touch controls, device inventory and status information is made available. Preset profiles can also be implemented on demand from a Gateway.

SensorView™

The most powerful method of nLight control is via the SensorView Lighting Control Software. This browser-based application provides complete system administration in an easy-to-use graphical interface. SensorView requires a single installation onto a host server computer. Multiple users can then access the program via a standard web browser with network access to that server. Account permissions of varying degrees are available for assignment to each user.

SensorView features a network device tree and pages that provide individual device information, such as properties, settings, and status information. Additionally, SensorView gives the user the ability to create lighting control profiles, apply them to lighting zones, and schedule their implementation.

2 HARDWARE INSTALLATION

Since nLight systems are networked, hardware installation should follow approved nLight layouts. These drawings should indicate which devices should be installed in each lighting zone and the approximate location for occupancy sensors and photocell sensors there in. Generally, the location of the Gateway and Bridge devices in the nLight Backbone is flexible and therefore location can be determined by the installer.

The following is the recommended procedure for installing nLight network hardware.

1 Install Backbone (Gateways & Bridges)

2 Install Zones w/ Power Packs

3 Install Zones w/o Power Packs

4 Complete nLight Installation Worksheet

WARNING

It is critical that every CAT5e cable be tested with a cable tester to verify correctly wired terminations. Either T568A or T568B pin-pair assignment can be utilized as long as terminations are consistent.

2.1 INSTALL BACKBONE

GATEWAY (nGWY2)

a Mount Gateway power supply (**PS150**) and make all class 1wire connections according to device datasheet

b Mount Gateway (**nGWY2**)

c Connect Gateway & power supply via terminal connections on rear of unit

d Connect Gateway (via port labeled “Ethernet”) to Ethernet LAN (if available) w/ CAT5e cable

e Apply power and verify that Gateway is functioning (LCD screen will turn on). The nLight logo will appear on the screen.

BRIDGE

a Mount power supply (**PS 150**) and make all class 1 wire connections according to device datasheet

b Mount Bridge (**nBRG8**)

c Connect class 2 power wires from power supply to Bridge terminal connections located on side of unit

d Apply power and verify Bridge operation by observing LED blinking

e Connect to Gateway (or nearest Bridge) with CAT5e cable according to network design

f Verify communication between Gateway and newly installed Bridge (Device count on Gateway LCD screen should increment one)

g Repeat steps a-f for interconnecting additional Bridges

2.2 INSTALL ZONES W/ POWER PACKS

a Mount devices and make all class 1 and class 2 wire connections according to device datasheets
b Interconnect all devices (in any order) within zone using CAT5ecabling
c Apply power
d After a few seconds, zone should become functional and run according to defaults*
e Verify electrical control of lights by using any/all of the 3 methods below that apply:

> **Method 1** (requires WallPod): Toggle lights on/off or dim lights up/down by pressing WallPod.
>
> **Method 2** (requires Occupancy Sensor): Vacate zone and wait for occupancy sensor to time-out. Default time delay is 10 minutes. Note sound will reset time delay on dual technology (-PDT) sensors.
>
> **Method 3** (requires Photocell w/ Dimming): Shine flashlight into Photocell. LED will blink rapidly and lights will begin to dim. After 20 min of blinking, lights will turn off.

f Using CAT5e cable, connect zone into backbone via available port on closest Bridge or Gateway
g Write name of zone on line for corresponding port on the Bridge label and on Bridge Commissioning Card
h *****Optional**: Record one serial number of device ingroup
i Verify correctly incremented device count on Gateway

*All device tracking/broadcasting settings start in enabled state and all channels settings use Channel 1 initially (except 2-Pole units and Scene Controllers)

2.3 INSTALL ZONES w/o POWER PACKS

a Mount devices and make all class 1 and class 2 wireconnections according to device datasheets
b Interconnect all devices (in any order) within zone using CAT5ecabling
c Using CAT5e cable, connect zone into backbone via available port on closest Bridge, or Gateway
d Apply power to connected Bridge
e After a few seconds, zone should become functional and run according to defaults
f Verify electrical control of lights by using any/all of the 3 methods below that apply:

> **Method 1** (requires WallPod): Toggle lights on/off or dim lights up/down by pressing WallPod.
>
> **Method 2** (requires Occupancy Sensor): Vacate zone and wait for occupancy sensor to time-out. Default time delay is 10 minutes. Note sound will reset time delay on dual technology (-PDT) sensors.
>
> **Method 3** (requires Photocell w/ Dimming): Shine flashlight into Photocell. LED will blink rapidly and lights will begin to dim. After 20 min of blinking, lights will turn off.

g Write name of zone on line for corresponding port on the Bridge label and on Bridge Commissioning Card
h ******Optional:*** Record one serial number of device ingroup
i Verify correctly incremented device count on Gateway

2.4 MANUAL UNIT IDENTIFICATION

All nLight Devices can be manually labeled with a number (1-9) via the push-button. Number will appear as the first character in the default name visible through the SensorView software or local Gateway. See Manual Programming section B function 1 (Name Unit with Number).

2.5 COMPLETE nLIGHT INSTALLATION WORKSHEET

Worksheet is to be completed by the installer prior to any visits by start-up or programming agents. Every nLight system is shipped with multiple copies. Worksheet also available online at:

http://docs.nlightcontrols.com

3 MANUAL PROGRAMMING (LOCAL)

The programming phase for an nLight system should begin once the hardware has been properly installed and proper operation has been documented on the nLight Control System Installation Worksheet.

An nLight device's settings can be accessed remotely through the SensorView software and/or locally from the device. The following sections provide instructions for local programming.

3.1 SENSORS, POWER PACKS, & nIOS

The following instructions and tables contain the complete list of push-button codes for sensor, power pack, & nIO devices.

- Not all settings are applicable for every device
- Settings are organized into three levels (A, B, & C), each consisting of multiple functions that can be programmed with several values
- Settings changes made through the push-button will show up as changes to the default settings in SensorView.
- To access/edit a particular setting, one of two programming procedures (depending on the device, setting level, and function) must be followed

STANDARD METHOD

Please read all 3 steps before programming

1 Enter a programming function by pressing button the number of times as the desired function number from the following tables (e.g., press twice for function 2, time delay).

2 LED will flash back the selected function's current setting (e.g., 5 flashes for 10 minute time delay). To change setting, proceed to step 3 before flash back sequence repeats 3 times. To exit the current function or to change to a different function, wait for sequence to repeat 3 times then return to step

3 Press button the number of times indicated in the particular function's detailed table for the NEW desired setting (e.g., press 3 times for 5 min). As confirmation of setting change, LED flashes back the NEW setting 3 times before exiting.

PRESS & HOLD METHOD

Note: required for all nWSD and nWSX products and A Level Functions 1,9,10, 11, 13, 18, 20, 22
Please read all 7 steps before programming

1 Enter programming mode by pressing & holding button until LED flashes rapidly. Release button.

2 Enter a specific programming function by pressing button the number of times as the desired function number from the tables to the right (e.g., press twice for function 2, time delay).

3 LED will flash back the selected function's current setting (e.g., 5 flashes for 10 minute time delay). To change setting, proceed to step 4 before flash back sequence repeats 10 times. To exit the current function or to change to a different function, wait for sequence to repeat 10 times then return to step 3.

4 Press button the number of times indicated in the particular function's detailed table for the NEW desired setting (e.g., press 3 times for 5 min). As confirmation of setting change, LED flashes back the NEW setting 10 times before exiting.

5 Exit programming mode by pressing and holding button again until LED flashes rapidly. Release button.

6 Re-enter function number as final confirmation that its setting changed.

7 LED will flash twice indicating acceptance of NEW settings. If two flashes are not seen, repeat 7 step process.

A LEVEL PUSH-BUTTONFUNCTIONS

1 POLE SELECTION / BUTTON MODE[2]

For 2-Pole devices: functions 2 ,5, 6, and 8 can be programmed differently for each pole. The selections for the Pole Selection function determine which pole's settings are to be modified by subsequent programming. Button Mode overrides a device and enables its push-button to toggle the device's internal relay(s) or dim level

1 1st Pole[1] **3** Copy Pole 1's settings to Pole 2 **5** Enable ButtonMode
2 2nd Pole **4** Disable Button Mode

2 TIME DELAY

The length of time an occupancy sensor will keep the lights on after it last detects occupancy

STANDARD
1 30 sec **3** 5.0 min **5** 10.0 min[1] **7** 15.0 min **9** 20.0 min
2 2.5 min **4** 7.5 min **6** 12.5 min **8** 17.5 min

EXTENDED
1 30 sec **3** 30 min **5** 60 min **7** 90 min **9** 120min
2 15 min **4** 45 min **6** 75 min **8** 105 min

3 IDLE TIME UNTIL DIM

The length of time after last detected occupancy that a sensor will reduce lighting to unoccupied dim level.

STANDARD
3 30 sec **3** 5.0 min **5** 10.0 min **7** 15.0 min **9** 20.0 min
4 2.5 min **4** 7.5 min[1] **6** 12.5 min **8** 17.5 min **10** Disable

EXTENDED
1 30 sec **3** 30 min **5** 60 min **7** 90 min **9** 120 min
2 15 min **4** 45 min **6** 75 min **8** 105 min **10** Disable

3 START TO HIGH

Lights go to full bright for 20 minutes upon initial power up

5 Disabled[1] **2** Enabled

4 AUTO SET-POINT / 100 HOUR BURN-IN

100 HOUR BURN-IN: Overrides relays on (typically for lamp seasoning)
AUTO SET-POINT: Photocell calibration procedure for detecting optimum lighting control level

1 Disabled[1] **3** Enabled then run Auto-Setpoint **5** Blink backSet-Point[3]
2 Enabled **4** Run Auto Set-Point

[1] DEFAULT SETTING

[2] REQUIRES **PRESS & HOLD METHOD**

5 TEN’S DIGIT OF SET-POINT

The ten’s digit of the target light level that is to be maintained by the device (in foot-candles)

1	10 fc	**3**	30 fc	**5**	50 fc	**7**	200 fc	**10**	0 fc[1]
2	20 fc	**4**	40 fc	**6**	100 fc	**8**	Disable		

6 ONE’S DIGIT OF SET-POINT

The one’s digit of the target light level that is to be maintained by the device (in foot-candles)

1	1 fc	**3**	3 fc	**5**	5 fc[1]	**7**	7 fc	**9**	9 fc
2	2 fc	**4**	4 fc	**6**	6 fc	**8**	8 fc	**10**	0 fc

7 SUNLIGHT DISCOUNT FACTOR

Value used to improve the tracking accuracy of a photocell during periods of high daylight. Decreasing the value will lower the controlled level of the lights

1	x/1[1]	**3**	x/3	**5**	x/5	**7**	x/7	**9**	x/9
2	x/2	**4**	x/4	**6**	x/6	**8**	x/8	**10**	x/10

8 INCREMENTAL SET-POINT ADJUSTMENT

Alters the target light level that is to be maintained by the device (in foot-candles)

1	Decrease 1 fc	**2**	Increase 1 fc

9 RESTORE FACTORY DEFAULTS[2]

1	Maintain Current	**2**	Restore Defaults

10 TIME DELAY SCHEME[2]

Selects the range of time delay values available for use by function 2, Time Delay.

	POLE 1	POLE 2		POLE 1	POLE 2
1	Standard	Standard	**3**	Extended	Standard
2	Standard	Extended	**4**	Extended	Extended

11 PHOTOCELL MODE[2]

Indicates a photocell sensors method of operation. One mode enables the sensor to turn the lights both on and off while the other mode can only inhibit (prevent) the lights from turning on

1	Full On/Off Control[1]	**2**	Inhibit Only Control

[3] The LED will blink back the ten’s digit, then pause, then blink back the one’s digit. For a “0” the LED will blink very rapidly. The sequence is repeated 3 times.

11 DUAL ZONE PHOTOCELL MODE[2] (DZ Models Only)

Indicates a Dual Zone photocell sensor's method of operation

STEPPED DIMMING (DUO) MODE :
Mode where the appropriate on/off combination of the two associated relays is maintained in order to always meet the photocell set-point requirements

STEPPED DIMMING (DUO) MODE – NEVER OFF:
Mode where the appropriate on/off combination of the two associated relays (except both off) is maintained in order to always meet the photocell set-point requirements.

DUAL ZONE OFFSET MODE : Mode where Zone 2's set-point is a selected percentage higher than Zones 1's set-point

DUAL ZONE FAN MODE : Mode where Zone 2's photocell control is disabled

1 Duo[1] **2** Duo-Never Off **3** Offset **4** Fan Mode **5** Inhibit

12 DUAL TECHNOLOGY (MICROPHONICS™)

A second method of occupancy detection that allows the sensor to hear occupants

1 Normal[1] **2** Off **3** Medium **4** Low

13 MICROPHONE GRACE PERIOD TIME[2]

The time period after lights are automatically turned off that they can be voice reactivated

1 0 **3** 20 **5** 40 **7** 60
2 10[1] **4** 30 **6** 50

15 PHOTOCELL DIMMING RANGE (HIGH)

The maximum output level (0-10 VDC) up to which an automatic dimming photocell will control

1 Off **3** 2 Volts **5** 4 Volts **7** 6 Volts **9** 8 Volts **11**10 Volts[1]
2 1 Volt **4** 3 Volts **6** 5 Volts **8** 7 Volts **10**9 Volts

16 PHOTOCELL DIMMING RANGE (LOW)

The minimum output level (0-10 VDC) down to which an automatic dimming photocell will control

1 Off[1] **3** 2 Volts **5** 4 Volts **7** 6 Volts **9** 8 Volts **11**10 Volts
2 1 Volt **4** 3 Volts **6** 5 Volts **8** 7 Volts **10** 9 Volts

[1] DEFAULT SETTING [2] REQUIRES **PRESS & HOLD METHOD**

6 DEFAULT SETTING FOR **ADC**

17 DUAL ZONE OFFSET

Fixed voltage increase of Zone 2’s dimming output from Zone 1’s dimming output (Dual Zone photocell applications only)

1	-10 Volts	**5**	-6 Volts	**9**	-2 Volts	**13**	2 Volts[1]	**17**	6 Volts	**21**	10 Volts
2	-9 Volts	**6**	-5 Volts	**10**	-1 Volt	**14**	3 Volts	**18**	7 Volts		
3	-8 Volts	**7**	-4 Volts	**11**	0 Volts	**15**	4 Volts	**19**	8Volts		
4	-7 Volts	**8**	-3 Volts	**12**	1 Volt	**16**	4 Volts	**20**	9 Volts		

18 DUAL ZONE OFF POINT[2]

Zone 2’s set-point as a percentage of Zones 1’s set-point (Dual Zone photocell applications only)

1	110%	**3**	130%	**5**	150%[1]	**7**	170%	**9**	190%
2	120%	**4**	140%	**6**	160%	**8**	180%	**10**	200%

19 DIMMING RATE

The speed at which automatic changes to the light level occur

1	700 sec	**2**	350 sec	**3**	70 sec[1]	**4**	35 sec	**5**	7 sec

20 LED[2]

Indicates the behavior of a device’s LED

7	Normal[1]	**2**	Inhibited

21 PHOTOCELL TRANSITION OFF TIME

The time period for which a photocell must measure a light level above the set-point before it will turn the lights off

1	45 sec	**3**	5 min[1]	**5**	15 min	**7**	25 min
2	2 min	**4**	10 min[3]	**6**	20 min		

22 PHOTOCELL TRANSITION ON TIME[2]

The time period for which a photocell must measure a light level below the set-point before it will initiate the lights on

1	45 sec[1]	**3**	5 min	**5**	15 min	**7**	25 min
2	2 min	**4**	10 min	**6**	20 min		

23 OCCUPIED BRIGHT LEVEL

The output level (0-10 VDC) that a dimming sensor sets the light to when occupancy is detected (not applicable if photocell is enabled)

1	1 Volt	**3**	3 Volts	**5**	5 Volts	**7**	7 Volts	**9**	9 Volts
2	2 Volts	**4**	4 Volts	**6**	6 Volts	**8**	8 Volts	**10**	10 Volts[1]

24 UNOCCUPIED DIM LEVEL

The output level (0-10 VDC) a dimming sensor sets the lights after the idle time until dim timer expires

1 1 Volt[1]
2 2 Volts
3 3 Volts
4 4 Volts
5 5 Volts
6 6 Volts
7 7 Volts
8 8 Volts
9 9 Volts
10 10 Volts

25 nIO INPUT MODE

Indicates a nIO's method of operation

SCENE TOGGLE : Mode where preprogrammed settings are run on devices within a local zone when an open/close style switch is sensed from the connected device

SCENE MOMENTARY : Mode where preprogrammed settings are run on devices within a local zone when a pulse style switch is sensed from the connected device

WALLPOD TOGGLE : Mode that creates an equivalent WallPod signal when an open/close style switch is sensed from the connected device

WALLPOD MOMENTARY : Mode that creates an equivalent WallPod signal when a pulse style switch is sensed from the connected device

SWEEP TOGGLE : Mode that sets the remaining time delay for all devices on Gateway when an open/close style switch is sensed from the connected device

SWEEP MOMENTARY : Mode that sets the remaining time delay for all devices on Gateway when a pulse style switch is sensed from the connected device

BROADCAST ANALOG INPUT : Input mode that senses a 0-10 VDC input

1 Disabled[1]
2 Scene Toggle
3 Scene Momentary
4 WallPod Toggle
5 WallPod Momentary
6 Sweep Toggle
7 Sweep Momentary
8 Broadcast Analog Input

26 FOLLOW PHOTOCELL MODE

Instructs how a device's dimming output reacts relative to a dimming photocell

1 Disabled[1]
2 Enabled Negative Only
3 Enabled Both Positive and Negative

27 SWEEP EXIT TIME

The time period before a sweep is executed

1 0 sec
2 15 sec[1]
3 30 sec
4 45 sec
5 1 min
6 2 min
7 3 min
8 4 min
9 5 min

28 SWEEP GRACE PERIOD

The remaining time delay after a sweep is executed

1 0 sec
2 5 sec[1]
3 10 sec
4 15 sec
5 30 sec
6 1 min

[1] DEFAULT SETTING

[2] REQUIRES **PRESS & HOLD METHOD**

B LEVEL PUSH-BUTTON FUNCTIONS

Entered by holding down button until rapid flash, release, then hold down again until rapid flash, release, then proceed using standard programming method.

1 NAME UNIT WITH NUMBER

Name Unit with Number

1	1	**3**	3	**5**	5	**7**	7	**9**	9
2	2	**4**	4	**6**	6	**8**	8	**10**	Unassigned[1]

2 SEMI-AUTO GRACE PERIOD

The time period after lights are automatically turned off that they can be reactivated with movement

1	0 sec	**3**	10 sec[1]	**5**	2 hour	**7**	8 hour
2	5 sec	**4**	1 hour	**6**	4 hour		

3 PREDICTIVE EXIT TIME

The time period after manually switching lights off for the occupant to leave the space (Predictive Off mode only)

1	5 sec	**3**	7 sec	**5**	9 sec	**7**	15 sec	**9**	30 sec
2	6 sec	**4**	8 sec	**6**	10 sec[1]	**8**	20 sec		

4 PREDICTIVE GRACE TIME

The time period after the Predictive Exit Time that the sensor rescans the room for remaining occupants (Predictive Off mode only)

1	0 sec	**3**	10 sec	**5**	30 sec	**7**	50 sec
2	5 sec[1]	**4**	20 sec	**6**	40 sec	**8**	60 sec

5 POLE 1 OCCUPANCY BROADCASTING

Indicates whether a sensor will transmit its occupancy information to the rest of its zone

1	Enable[1]	**2**	Disable

6 POLE 1 OCCUPANCY BROADCAST CHANNEL

The channel on which a sensor transmits its occupancy information

1	Channel 1[1]	**4**	Channel 4	**7**	Channel 7	**10**	Channel 10	**13**	Channel 13	**16**	Channel16
2	Channel 2	**5**	Channel 5	**8**	Channel 8	**11**	Channel 11	**14**	Channel 14		
3	Channel 3	**6**	Channel 6	**9**	Channel 9	**12**	Channel 12	**15**	Channel 15		

7 POLE 1 PHOTOCELL BROADCASTING

Indicates whether a sensor will transmit its photocell information to the rest of its zone

1	Enable[1]	**2**	Disable

8 POLE 1 PHOTOCELL BROADCAST CHANNEL

The channel on which a sensor transmits its photocell information

1	Channel 1[1]	**4**	Channel 4	**7**	Channel 7	**10**	Channel 10	**13**	Channel 13	**16**	Channel16
2	Channel 2	**5**	Channel 5	**8**	Channel 8	**11**	Channel 11	**14**	Channel 14		
3	Channel 3	**6**	Channel 6	**9**	Channel 9	**12**	Channel 12	**15**	Channel 15		

9 POLE 1 SWITCH BROADCASTING

Indicates whether a device w/ a manual switch and/or dimmer will transmit events to the rest of its zone

1 Enable[1] **2** Disable

10 POLE 1 SWITCH BROADCAST CHANNEL

The channel on which a device with a manual switch and/or dimmer transmits

1	Channel 1[1]	**4**	Channel 4	**7**	Channel 7	**10**	Channel 10	**13**	Channel 13	**16**	Channel16
2	Channel 2	**5**	Channel 5	**8**	Channel 8	**11**	Channel 11	**14**	Channel 14		
3	Channel 3	**6**	Channel 6	**9**	Channel 9	**12**	Channel 12	**15**	Channel 15		

11 POLE 1 OCCUPANCY TRACKING

Indicates whether a device's relay and/or dimming output will react to occupancy information

1 Disable **2** Enable[1] **3** Enable and Ignore Remote

12 POLE 1 OCCUPANCY TRACKING CHANNEL

The channel on which a relay and/or dimming output receives occupancy information

1	Channel 1[1]	**4**	Channel 4	**7**	Channel 7	**10**	Channel 10	**13**	Channel 13	**16**	Channel16
2	Channel 2	**5**	Channel 5	**8**	Channel 8	**11**	Channel 11	**14**	Channel 14		
3	Channel 3	**6**	Channel 6	**9**	Channel 9	**12**	Channel 12	**15**	Channel 15		

13 POLE 1 PHOTOCELL TRACKING

Indicates whether a device's relay and/or dimming output will react to photocell information

1 Disable **2** Enable[1] **3** Enable and Ignore Remote

14 POLE 1 PHOTOCELL TRACKING CHANNEL

The channel on which a relay and/or dimming output receives photocell information

1	Channel 1[1]	**4**	Channel 4	**7**	Channel 7	**10**	Channel 10	**13**	Channel 13	**16**	Channel16
2	Channel 2	**5**	Channel 5	**8**	Channel 8	**11**	Channel 11	**14**	Channel 14		
3	Channel 3	**6**	Channel 6	**9**	Channel 9	**12**	Channel 12	**15**	Channel 15		

15 POLE 1 SWITCH TRACKING

Indicates whether a device's relay and/or dimming output will react to manual switching or dimming events

1 Disable **2** Enable[1] **3** Enable and Ignore Remote

16 POLE 1 SWITCH TRACKING CHANNEL

The channel on which a relay and/or dimming output receives manual switching or dimming events

1 Channel 1[1]
2 Channel 2
3 Channel 3
4 Channel 4
5 Channel 5
6 Channel 6
7 Channel 7
8 Channel 8
9 Channel 9
10 Channel 10
11 Channel 11
12 Channel 12
13 Channel 13
14 Channel 14
15 Channel 15
16 Channel 16

17 POLE 1 OVERRIDE

Indicates whether a device’s relay is forced on/off and/or dimming output is forced to maximum/minimum

1 Disable[1]
2 Override On Enabled
3 Override Off Enabled

18 POLE 1 SPECIAL MODE

See page 11-12 for detailed definition

1 Normal[1]
2 Semi-Auto
3 Auto to Override On
4 Manual On to FullAuto
5 Predictive Off

19 INVERT POLE 1 RELAY LOGIC

Reverses functionality of relays

1 Normal Logic[1]
2 Inverse Logic

C LEVEL PUSH-BUTTON FUNCTIONS

Entered by holding down button until rapid flash, release, then hold down again until rapid flash, release, hold down until rapid flash, then proceed using standard programming method.

1 POLE 2 OCCUPANCY BROADCASTING

Indicates whether a sensor will transmit occupancy info to the rest of its zone

1 Enable[1]
2 Disable

2 POLE 2 OCCUPANCY BROADCAST CHANNEL

The channel on which a sensor transmits its occupancy info

1 Channel 1
2 Channel 2[1]
3 Channel 3
4 Channel 4
5 Channel 5
6 Channel 6
7 Channel 7
8 Channel 8
9 Channel 9
10 Channel 10
11 Channel 11
12 Channel 12
13 Channel 13
14 Channel 14
15 Channel 15
16 Channel 16

3 POLE 2 PHOTOCELL BROADCASTING

Indicates whether a sensor will transmit photocell information to the rest of its zone

1 Enable[1]
2 Disable

4 POLE 2 PHOTOCELL BROADCAST CHANNEL

The channel on which a sensor transmits its photocell information

1 Channel 1
2 Channel 2[1]
3 Channel 3
4 Channel 4
5 Channel 5
6 Channel 6
7 Channel 7
8 Channel 8
9 Channel 9
10 Channel 10
11 Channel 11
12 Channel 12
13 Channel 13
14 Channel 14
15 Channel 15
16 Channel 16

5 POLE 2 SWITCH BROADCASTING

Indicates whether a device w/ a manual switch and/or dimmer will transmit events to the rest of its zone

1 Enable[1]
2 Disable

6 POLE 2 SWITCH BROADCAST CHANNEL

The channel on which a device with a manual switch and/or dimmer transmits

1 Channel 1
2 Channel 2[1]
3 Channel 3
4 Channel 4
5 Channel 5
6 Channel 6
7 Channel 7
8 Channel 8
9 Channel 9
10 Channel 10
11 Channel 11
12 Channel 12
13 Channel 13
14 Channel 14
15 Channel 15
16 Channel 16

7 POLE 2 OCCUPANCY TRACKING

Indicates whether a device's relay and/or dimming output will react to occupancy information

1 Disable
2 Enable[1]
3 Enable and Ignore Remote

8 POLE 2 OCCUPANCY TRACKING CHANNEL

The channel on which a relay and/or dimming output receives occupancy information

1 Channel 1

2 Channel 2[1]

3 Channel 3

4 Channel 4

5 Channel 5

6 Channel 6

7 Channel 7

8 Channel 8

9 Channel 9

10 Channel 10

11 Channel 11

12 Channel 12

13 Channel 13

14 Channel 14

15 Channel 15

16 Channel 16

9 POLE 2 PHOTOCELL TRACKING

Indicates whether a device's relay and/or dimming output will react to photocell information

1 Disable

2 Enable[1]

3 Enable and Ignore Remote

10 POLE 2 PHOTOCELL TRACKING CHANNEL

The channel on which a relay and/or dimming output receives photocell information

1 Channel 1

2 Channel 2[1]

3 Channel 3

4 Channel 4

5 Channel 5

6 Channel 6

7 Channel 7

8 Channel 8

9 Channel 9

10 Channel 10

11 Channel 11

12 Channel 12

13 Channel 13

14 Channel 14

15 Channel 15

16 Channel 16

11 POLE 2 SWITCH TRACKING

Indicates whether a device's relay and/or dimming output will react to manual switching or dimming events

1 Disable

2 Enable[1]

3 Enable and Ignore Remote

12 POLE 2 SWITCH TRACKING CHANNEL

The channel on which a relay and/or dimming output receives manual switching or dimming events

8 Channel 1

9 Channel 2[1]

10 Channel 3

4 Channel 4

5 Channel 5

6 Channel 6

7 Channel 7

8 Channel 8

9 Channel 9

10 Channel 10

11 Channel 11

12 Channel 12

13 Channel 13

14 Channel 14

15 Channel 15

16 Channel 16

13 POLE 2 OVERRIDE

Indicates whether a device's relay is forced on/off and/or dimming output is forced to maximum/minimum

1 Disable[1]

2 Override On Enable

3 Override Off Enable

14 POLE 2 SPECIAL MODE

See page 11-12 for detailed definition

1 Normal[1]

2 Semi-Auto

3 Auto to Override On

4 Manual On to Full Auto

5 Predictive Off

15 INVERT POLE 2 RELAY LOGIC

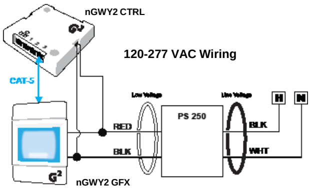
Reverses functionality of relays

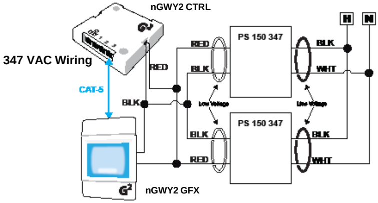
11 Normal Logic[1] **2** Inverse Logic

MANUAL PROGRAMMING

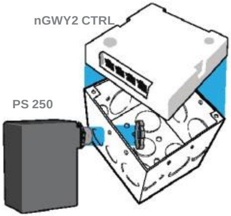
3.2 GATEWAY LCD SCREEN & TOUCH CONTROLS

The **nGWY2 CTRL** and **nGWY2 GFX** units are powered via a **PS 250** power supply wired via each unit's power terminal connectors. **Note:** For 347 VAC powering, dual **PS 150 347** power supplies are provided. Be sure to connect the red power output wires from the **PS 150 347** supplies together and then wire to both the **nGWY2 GFX** and **nGWY2 CTRL** units.



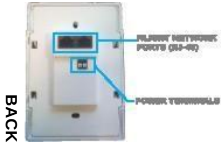


INSTALLATION



Control Unit and Power Supply

1. Mount power supply to a 4" x 4" square junction box (through a 1/2" knockout)
2. Connect the supplys' class 1 line voltage wires
3. Mount **nGWY2 CTRL** unit to top of same junction box
4. Connect the power supplys' class 2 low voltage wires to the **nGWY2 CTRL's** terminal connectors (polarity insensitive)
5. Unit's LEDs will flash indicating power up.



Gateway Touch Screen

1. Before mounting Gateway Touch Screen (**nGWY2 GFX)**, connect Class 2 low voltage wires from power supplies to unit's power terminal connections (polarity insensitive
2. Verify unit has power by observing screen and/or LED
3. Connect CAT-5 cable(s) from **nGWY2 CTRL** to one of the RJ-45 port(s) on rear of **nGWY2 GFX** unit
4. Verify units are communicating (indicated by on-screen blinking heart icon)
5. Mount unit to standard single gang switch box (screws provided)
6. Pressing reset button twice is equivalent to repowering unit

Note – to reset touch screen calibration, press reset button (located on left side of unit) 3x to restart unit in screen-calibration mode.

OVERVIEW

The touch screen on the Gateway (nGWY2 GFX) can be used to perform many tasks, including:

- View/Edit Gateway device settings
- View complete network tree of downstream nLight Enabled devices
- View operational status of any connected nLight-enable device
- View complete list of control profiles
- View list of currently running control profiles
- Run a control profile on demand

DEFAULT LCD SCREEN SECURITY PIN NUMBER [1] [2] [3] [4]

MANUAL PROGRAMMING

3.4 *nPOD*

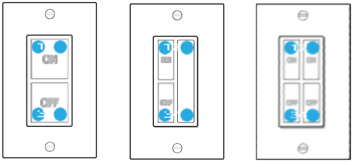
A WallPod's broadcasting channel setting(s) can be changed manually. The following instructions apply to all WallPods except the Scene Controller (**nPODS**).

VERIFY CURRENT CHANNEL:

Using a steady cadence press the corners of the button portion of the WallPod in the following sequence:

3, 4, 3, 4, 1, 2, 1, 2

Wait approximately 3 seconds and the light will cycle (flash) the number of times indicating the current channel setting. (i.e., Lights will cycle twice if current setting is channel 2)



CHANGE CURRENT CHANNEL:

Using a steady cadence press the corners of the button portion of the **nPOD** in the following sequence:

3, 4, 3, 4, 1, 2, 1, 2

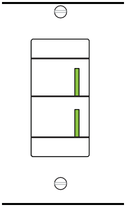
Wait approximately 3 seconds and the light will cycle (flash) the number of times indicating the current channel setting (i.e., Lights will cycle twice if current setting is channel 2).

Immediately after the lights cycle the current settings, select the corner corresponding to the channel on which you would like the WallPod to broadcast (i.e., bottom left for channel 3). The lights will then cycle according to the channel that has been selected.

nPODM PROGRAMMING INSTRUCTIONS

PLEASE READ ALL 4 STEPS BEFORE PROGRAMMING

1. Enter B-Level programming mode by holding down uppermost left button until LED flashes rapidly, release, then hold down until rapid flash again, release, then immediately enter programming function as described in step 2.
2. Enter a programming function by pressing button the number of times as the desired function number from the B-Level function table below (e.g., press ten times for function 10, Switch Broadcast Channel – Pole 1).
3. The selected function's current setting will then be read out in a sequence of LED flashes (e.g., one flash for Channel 1). To change setting, proceed to step 4 before sequence repeats 3 times.
4. While the sensor is flashing back current setting, interrupt it by pressing button the number of times for the new desired setting as indicated in the particular function's detailed table (e.g., press twice for Channel 2). Sensor will begin to flash new setting as confirmation.



Note: To exit B-Level programming mode or to change to a different function, wait for blink back sequence to repeat 3 times then return to step 1.

For more manual programming, refer to the nLight Push-Button WallPod Programming Instruction Card:

http://www.sensorswitch.com/instructionfiles/IN-11.1.pdf

12 REMOTE PROGRAMMING VIA SENSORVIEW™

SensorView is used to perform the following start-up tasks:

- Verify discovery of Gateway and all devices
- Set-up user accounts
- Label ports with zone names
- Edit active defaults in units (time delays, set-points, modes)
- Perform any necessary firmware updates (extended time may be required)
- Create Groups/Profiles per customer requests
- Print Inventory and Profile reports
- Perform system backup

To install SensorView, download and follow the SensorView Installation Guide:

http://docs.nlightcontrols.com/installation/sensorview

13 HARDWARE TROUBLESHOOTING AIDS

SENSOR LEDS

- If no LED flashes are present (even when push-button is pressed) there is no sensor power. Check CAT5e cable for connectivity.
- If LED repeatedly rapid flashes, and then blinks 2 times, power is present but communication is not present. Check CAT5e cable for connectivity.
- One second of rapid flashing followed by four blinks: Legacy device in local zone which is not compatible with this device.

BRIDGE PORT LEDS

- No LED blinks indicates bad cabling
- Rapid blinks indicates discovery is occurring
- Persistent and/or periodic rapid flashing means communications issue is present (short, cross)
- **Activity Mode** (default)
  - **a** Single blink indicates normal polling traffic of zone
  - **b** Double blink indicates upstream Gateway
  - **c** 3 blinks indicates upstream Bridge
  - **d** 4 blinks indicates downstream Bridge
  - **e** 5 blinks indicates that discovery on a port has been locked out due to inconsistent communication with a downstream device
  - **f** 6 blinks indicates there is a local wiring loop between bridge ports (Bridge discovered itself)
- Device Count Mode (press button once to toggle between modes) Number of detected devices is blinked out in two digits (fast blinking is zero)

POWER PACK LEDS

- Interior LED will be solid if it is polling the zone (e.g., Gateway or Bridge not connected)
- Only one per zone at any time should be polling
- Exterior LED will blink at regular pace to indicate communication
- If either port repeatedly rapid flashes, and then blinks 3 times, there is low voltage on the connected cable (commonly caused by miswiring)
- If interior LED repeatedly rapid flashes, and then blinks 2 times, communication is not present

GATEWAY

Rediscovery

Gateway can be manually forced to rediscover all network devices

a From LCD screen on Gateway (Main Menu > Commissioning):

- Press the Lock button
- Type [1][2][3][4] then hit Enter
- Gateway Setup
- Rediscover all devices

or

b Cycle power then disconnect Power Supply

BRIDGE RESET

a Press and hold button for 6 seconds

or

b Cycle power (unplug all ports first) then disconnect Power Supply

POWER PACK SHUT DOWN MODE

If a CAT5e is wired incorrectly such that a power line is connected to a data line, an nPP-16 power pack will go into a protective shut down mode and will appear dead. Once both the incoming CAT5e connections have been cable tested and the initial miswiring problem is fixed, the power pack can only be brought back to life by removing line voltage from it (either disconnecting it, or by resetting the circuit). Both should be done with no CAT5e connections present so that it is assured that no power is being supplied from another device.

BUTTON MODE

- Enables a device's push-button to toggle the device's internal relay(s) or change the dim level from full bright to full dim
- Mode is present in any device with a relay (power packs, line voltage sensors, etc.) and any device with a dimming output (**nCM ADC**, **nCM PDT D**, **nPODM DX**, **nIO D, etc.**)

To Enable

1 Push button down until LED flashes rapidly.
2 Release Button.
3 Press Button 1 time.
4 Short pause (2 seconds), then press button 5 times to enable toggle switch mode.
5 Press Button down until LED Flashed Rapidly.
6 Release Button.
7 Press Button 1 time.
8 The LED will flash twice indicating acceptance of NEW Setting.

To Disable

1 Push button down until LED flashes rapidly.
2 Release Button.
3 Press Button 1 time.
4 Short pause (2 seconds), then press button 4 times todisable toggle switch mode.
5 Press Button down until LED Flashes Rapidly.
6 Release Button.
7 Press Button 1 time.
8 The LED will flash twice indicating acceptance of NEW Setting.

Note: When button mode is enabled, it may take several seconds for the lights to respond to the on/off command.

sensorswitch

An Acuity Brands Company

System Backbone IT Information

Overview

nLight by Acuity Controls is a digitally addressable, networked lighting control system that can operate without requiring a connection to the facility LAN. However, in many applications it may be desirable to connect the nLight system to a facility's building infrastructure IP network to provide additional functionality. For example, these features require the system to be networked to facility LAN:

- Using SensorView software to manage the lighting control system from a non-dedicated computer/workstation, such as a building engineer or facility manager's computer
- System integration with a Building Management System (BMS) via BACnet/IP protocol
- System integration with an electrical utility OpenADR server via nADR client
- Using Virtual Wallpod control applications from iOS devices or PC workstations
- Remote support and diagnostics

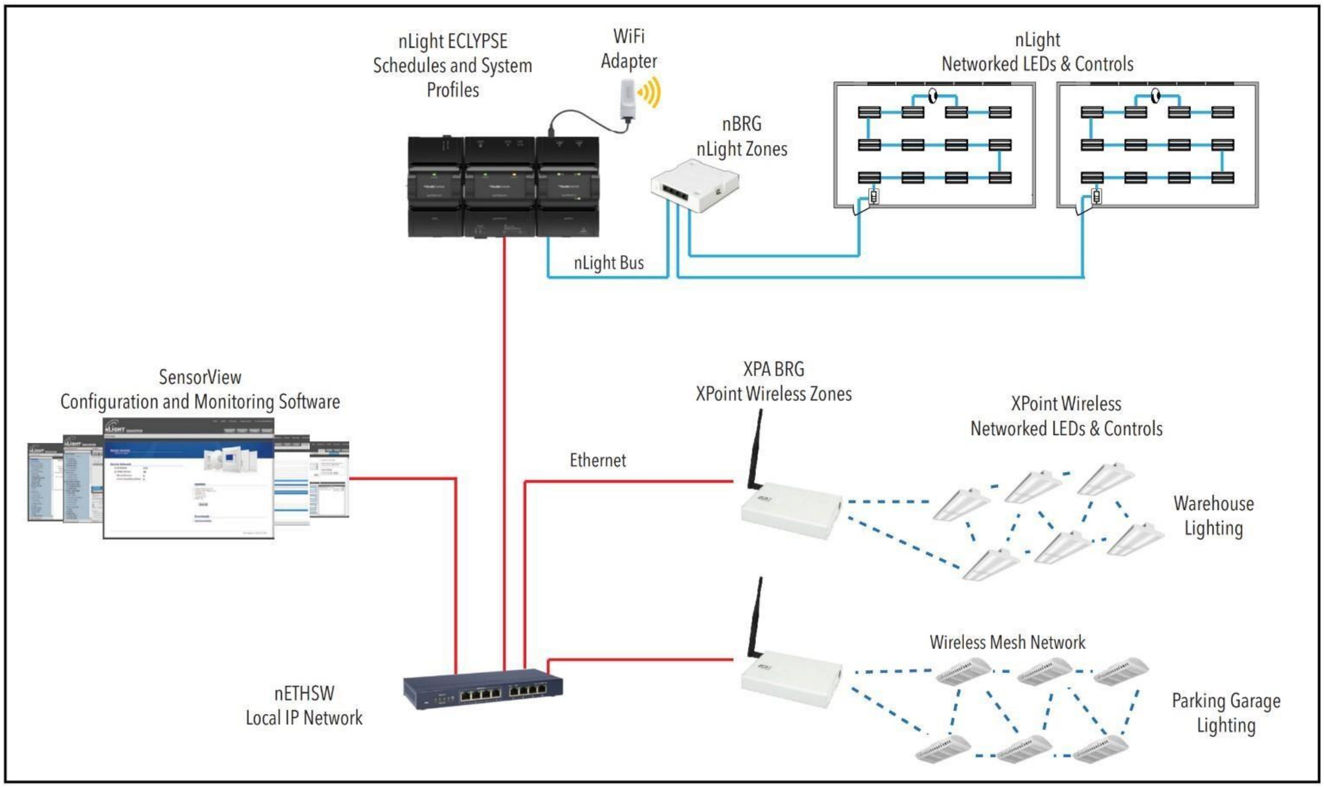


Figure 1 - Example Typical nLight System Riser Diagram

A simplified system riser diagram for a typical nLight installation, including XPoint Wireless by Acuity Controls, is shown in Figure 1. Each component shown connected with red wiring connections to the "nETHSW" is a device that requires an IP address and communication to other system devices via Ethernet. Note that there are parts of the nLight system that use proprietary communication protocols & addressing schemes and do not require IP addresses, the nLight device connections (also known as "SensorNet" and shown in blue wires) and the XPoint Wireless Mesh network (shown in dashed blue lines). In a typical "isolated" application, the IP networked devices are set up with local static IP addresses and software connections can be made through a dedicated PC/workstation or a temporary connection into the lighting control Ethernet switch (shown as nETHSW). In a typical "LAN integrated" application, the lighting control Ethernet switch may be connected to the facility LAN's IP backbone and also, may be provided by others.

The following types of nLight system backbone devices require an Ethernet connection and IP address:

1. **Client Web Browser (not shown, provided by others)**, used to access SensorView host via HTTP protocol, may be operated directly from SensorView host PC/Server (see next). Refer to SensorView Specification Sheet for supported browsers and clients.
2. **SensorView host PC/Server (provided by others)**, used to host SensorView IIS web application and communicate with all IP networked devices. Refer to SensorView Specification Sheet and Installation Instructions for specific host machinerequirements.
3. **nLight ECLYPSE™ Controller (nECY)**, used to provide timeclock, master system control, and device information cache for nLight and XPoint Wireless devices. This is also optionally used to provide protocol translation between BACnet/IP or BACnet MSTP building automation protocol and nLight system protocol.
4. **XPoint Wireless Bridge (XPA BRG)**, used to provide media/protocol translation between XPoint Wireless mesh network devices and nLight system protocol.
5. **nADR (not shown)**, used as a client to electrical utility OpenADR Demand Response Automation Server (DRAS).

Notes:

- CAT5e or higher wiring is required for all Ethernet and nLight device connections.
- Ethernet switches may be provided by others.
- All devices and TCP/UDP ports should be accessible to each other via the same LAN subnet (with the exception of the connection between Client Web Browser and SensorView PC host).
- All IP networked devices may be configured using static or dynamic (DHCP) IP address assignments (static IP addresses are recommended).
- There may be multiple quantities of each of these listed devices installed in a project; please review project Bill of Materials and system riser diagram for exact quantity of devices requiring IP addresses and connections.
- XPA BRG supports being powered from PoE network switches (IEEE 802.3af, requires PoE adapter to be specified with XPA BRG).

Wireless Mesh Network Overview

XPoint Wireless uses a low duty cycle, narrow-band, Zigbee®-based 2.4 GHz wireless protocol that is not known to interfere with your 2.4 GHz Wi-Fi or other systems. The low communication duty cycle, combined with clear-to-send back off capability from the IEEE802.15.4 radio, typically does not produce measurable impact to Wi-Fi performance and is usually difficult to observe in an RF spectrum analyzer. Each XPoint Wireless Bridge and associated mesh network (typically up to 250 wireless devices) can also be programmed to use a specific Zigbee RF channel to avoid co-channel interference with other installed 2.4 GHz equipment. Zigbee channels 11-26, corresponding with 5 MHz-wide frequency bands from 2.405 GHz to 2.480 GHz may be assigned to specific wireless mesh networks.

The wireless communication is secured and encrypted using AES 128-bit encryption. The network protocol includes "replay" protection, where each wireless message is uniquely encoded such that it cannot be recorded and replayed at a later time.

Additional Notes:

- Maximum RF power output is +18 dBm for Zigbee Channels 11-25, 0 dBm for Channel 26. Output power is typically attenuated 2-20 dB by LED luminaire housing.
- The wireless mesh network does not support integration with non-Acuity, Zigbee or Zigbee-based wireless devices.

Network Ports and Usage

To ensure proper system operation the network ports and protocols listed in Table 1-1 must be open for communication between nLight backbone devices.

Table 1-1: Required network ports and usage

Protocol	Port	nLight Devices	Usage	Security
TCP	22	• XPA BRG	SSH, factory service and diagnostics of this device (inbound)	TLS
UDP	67	• SensorView • nECY • XPA BRG • nADR	DHCP (outbound)	None, does not contain sensitive data
UDP	68	• SensorView • nECY • XPA BRG • nADR	DHCP (inbound)	None, does not contain sensitive data
TCP	80	• SensorView • XPA BRG • nADR	SensorView device configuration data (inbound/outbound)	None, does not contain sensitive data. Configuration is read only.
TCP	443	• nECY • XPA BRG • nADR	XPA BRG: Factory service and diagnostics of this device (inbound);	TLS

Protocol	Port	nLight Devices	Usage	Security
			nADR: Electrical utility Open ADR protocol (outbound)	
TCP	5000	• XPA BRG	Factory service and diagnostics (outbound)	None, does not contain sensitive data. Configuration is read only.
TCP	5551	• SensorView • nECY • nADR	System configuration (inbound/outbound)	AES-128 for nECY
UDP	7	• SensorView • nECY • nADR	Device identification on local subnet	None, does not contain sensitive data
UDP	123	• SensorView • nECY • nADR	NTP time synchronization (outbound)	None, does not contain sensitive data
UDP	5551	• SensorView • nECY • XPA BRG	nLight Protocol over IP	None, should be protected by LAN routing/firewall
UDP	5555	• SensorView • nECY • XPA BRG	Device identification on local subnet	None, does not contain sensitive data
UDP	5556	• SensorView • nECY • XPA BRG	nLight Protocol over IP	None, should be protected by LAN routing/firewall
UDP	29292	• XPA BRG	Factory service and diagnostics (outbound)	None, does not contain sensitive data. Configuration is read only.
UDP	47808	• nECY	BACnet over IP protocol	None, BACnet standard, should be protected by LAN routing/firewall

Network Data Capacity

Data capacity considerations must also be made depending on how often SensorView is used, as well as the type of devices on the network. The main cases are:

1) SensorView used only for initial system programming an ongoing maintenance/changes
2) SensorView with Plugins Modules (GreenScreen, Virtual WallPod)
3) XPoint Wireless Bridge connections to XPoint Wireless devices. Approximate bandwidth usage is provided in Table 1-2.
4) nLight system integration appliances/clients (e.g. nADR)

Table 1-2: Approximate bandwidth consumption

Application Use	Network Consumption per LAN Component (nECY, XPA BRG, nADR)
SensorView Configuration	< 0.2kbps (when SensorView is actively inuse)
SensorView Plugins	< 0.2kbps (Assuming GreenScreen and Virtual WallPod are active simultaneously)
XPoint Wireless Devices	< 0.1kbps
System Integration Appliances (e.g.nADR)	< 0.2kbps

ECLYPSE™

User Reference Guide

Table of Contents

CHAPTER 1

INTRODUCTION

This section provides an overview of the user guide.

Topics

Overview

This document describes best practices, specifications, wiring rules, and application information to implement robust and reliable communications net- works.

About the NECY Series Controller

The NECY Series Controller is a modular and scalable platform that is used to control a wide range of HVAC applications. It uses IP protocol to communicate on wired Ethernet networks and Wi-Fi to communication on wireless net-works.

This user guide also explains how to connect to the nLIGHT ECLYPSE controller's configuration interfaces.

About the IP Protocol Suite

Distech Controls' nLight ECLYPSE Series controllers use a widely used IP protocol to communicate with each other and with other applications for control and supervision. What is commonly referred to as IP is actually a multi-layered protocol suite that reliably transmits data over the public Internet and privately firewalled-off intranets. As integral part of our interconnected world, this proto- col is used by applications such as the World Wide Web, email, File Transfer Protocol (FTP), datashares, and so on.

nLight ECLYPSE Series controllers are able to work across geographic boundaries as a unified entity for control and administration purposes.

About BACnet®

The BACnet® ANSI/ASHRAE™ Standard 135-2008 specifies a number of Local Area Network (LAN) transport types. Distech Controls' controllers sup- port both BACnet/IP and BACnet Master-Slave/Token-Passing (MS/TP) com- munications data bus (based on the EIA-485 medium) as a local network for inter-networking of supervisory controllers and field controllers.

About This User Guide

Purpose of the User Guide

⚠ This user guide does not provide and does not intend to provide instructions for safe wiring practices. It is the user's responsibility to adhere to the safety codes, safe wiring guidelines, and safe working practices to conform to the rules and regulations in effect in the job site jurisdiction. This user guide does not intend to provide all the information and knowledge of an experienced HVAC technician or engineer.

This user guide shows you how to integrate nLight ECLYPSE controllers into your IP
network environment while enforcing standard network security practices.

Referenced Documentation

The follow documentation is referenced in this document.

- Controller Hardware Installation Guides: These documents are available at www.acuitybrands.com

nLIGHT ECLYPSE Introduction

The nLight ECLYPSE series is a modular and scalable platform that is used to control a wide range of HVAC applications. It supports BACnet/IP communication and is a listed BACnet Building Controller(B-BC).

The nECY Series Controller consists of an automation and connectivity server, power supply, and I/O extension modules.

This programmable Connected System Controller provides advanced functionality such as customizable control logic, Web-based design and visualization interface (ENVYSION embedded), logging, alarming, and scheduling.

This user guide also explains how to configure the nLight ECLYPSE controller's con- figuration interfaces.

Network Security

Maintaining the highest level of network security, especially when IP devices are connected to the Internet requires specially-trained personnel who are aware of the necessary techniques to ensure continued protection. This must include the implementation of a Virtual Private Network (VPN) to connect with IP controllers over the Internet. It is also important to coordinate with Information Technology (IT) department personnel the use of shared network resources.

At the first connection to an nLight ECLYPSE Controller you will be forced to change the password to a strong password for the admin account to protect access to the controller.

Intended Audience

This user guide is intended for system designers, integrators, electricians, and field technicians who have experience with control systems, and who want to learn about how to make a successful IP network installation. It is recommended that anyone installing and configuring the devices specified in this user guide have prior training in the usage of these devices.

Conventions Used in this Document

Notes

This is an example of Note text. Wherever the note-paper icon appears, it means the associated text is giving a time-saving tip or a reference to associated information of interest.

Cautions and Warnings

This is an example of Caution or Warning text. Wherever the exclamation icon appears, it means that there may be an important safety concern or that an action taken may have a drastic effect on the device, equipment, and/or network if it is improperly carried out.

Acronyms and Abbreviations Used in this Document

Acronym	Definition
ASHRAE	American Society of Heating, Refrigeration, and Air-Conditioning Engineers
AP	Access Point
APDU	Application Protocol Data Units
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BACnet®	Building Automation and Control Networking Protocol
BAS	Building Automation System
B-BC	BACnet Building Controller
BBMD	BACnet/IP Broadcast Management Device
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EOL	End Of Line
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilating, and Air Conditioning
ID	Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MB	Megabyte
MHz	Megahertz

Acronym	**Definition**
MS/TP	Master-Slave/Token-Passing
NAT	Network Address Translation
NTP	Network Time Protocol
PC	Personal Computer
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
RTU	*Remote Terminal Unit (for Modbus)*
SSID	Service Set IDentification
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web

CHAPTER 2

INTERNET PROTOCOL SUITE FUNDAMENTALS

This chapter describes the Internet protocol operating principles necessary to configure the IP parameters of an IP controller.

Topics

About the Internet Network

The Internet is the world-wide interconnection of networks. At its root however, it is not one big network, but a group of networks that communicate between each other by using standard protocols and by using gateways between these networks called routers.

The structure of the Internet is decentralized and non-hierarchical. On the Internet, all communication uses the Internet Protocol (IP) to communicate and all connected devices are identified by their IP address. An Internet Registry allocates IP addresses to internet service providers to be used by their users.

Data is sent across the network in packets. Each packet has a header that identifies the sender’s and intended receiver’s IP addresses.

Internet Protocol Suite Overview

Internet Protocol (IP) is part of a multi-layered suite that together enables data communication. The following descriptions are an overview of the IP suite protocol layers as used by IPdevices:

- Physical layer (bits): This is the physical and device-to-device electrical connection layer otherwise known as Ethernet. This layer defines:
    - The requirements for the physical connection between devices (the signal medium). For example, RJ-45 connectors (attachedper TIA/ EIA-568-A,), using Cat 5e data cable. The maximum cable length between devices is 328 ft. (100 m) at 100 MB/s datarate.
    - The electrical signal requirements for data packettransport.
    - The data packet structure including data payload and the source and destination device's MAC addresses.

In the case of Wi-Fi connected devices, the link layer is the air interface defined by the Wi-Fi standard, such as radio frequencies, data rates, authentication, data channel encryption, and so on.

- Data Link layer: This layer implements the ability for two devices to exchange data with each other.
- Network layer: This layer implements the ability to connect multiple distinct networks with each other. It provides the internetworking methods that allow data packets to travel from the source device to a destination device across network boundaries, such as a router through the use of an IP address. See
- Transport Layer (segments): This layer provides end-to-end communication data stream connection between two or more devices through a variety of protocols. However
- , it is the Transmission Control Protocol (TCP), the most commonly used internet transport protocol that is used by Distech Controls IP controllers to communicate with each other. TCP creates a connection-oriented channel between two applications; that is to say the data stream is error-checked, is sorted into the correct sequence (missing data packets are re-transmitted) and this data stream has a port number for addressing a specific application at the destination hostcomputer.
- Session layer (data): This layer implements the protocol to open, close, and manage a session between applications such that a dialog can occur.
- Presentation layer: This layer implements the display of media such as images and graphics.
- Applications layer: This layer implements the process-to-process communications protocol that includes among other services the BACnet/IP protocol, programming, debugging, WWW, and soon.

All of the above IP suite protocol layers must be fully functional for any two devices or controllers to communicate with each other.

CHAPTER 3

IPv4 Communication Fundamentals

This chapter describes IPv4 Communication operating principles.

Topics

DHCP versus Manual Network Settings
Networking Basics
About Routers, Switches, and Hubs

DHCP versus Manual Network Settings
About Routers, Switches, and Hubs

The differences between a hub, switch, and router are discussed in the table below.

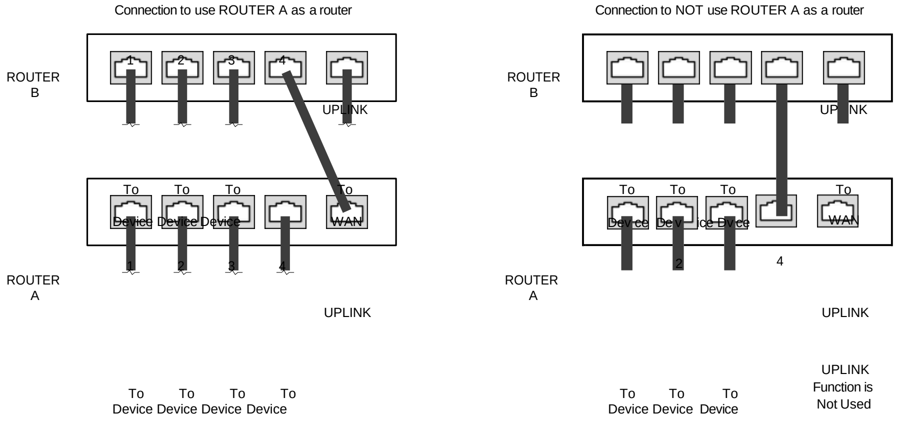
Table 1: Difference between a Hub, Switch, and Router

Device Type	Description
Hub	Every incoming data packet is repeated on every other port on the device. Due to this, all traffic is made available on all ports which increase data packet collisions that affect the entire network, thus limiting its data carrying capacity.
Switch	A switch creates a one-to-one virtual circuit that directs IP packets directly to the port that the destination computer is connected to. A switch maintains a lookup table that contains the MAC addresses of all the devices that are connected to the switch ports. The switch always refers to its lookup table before it forwards data packets to the destination devices.
Router	Like a switch, a router learns the IP addresses of all devices connected to any of its RJ-45 ports to create a routing table. If a data packet arrives at the router's port with a destination IP address that is: • Found in the router's routing table, the router forwards the data packet to the appropriate port for the device that has this IP address. • For a network with a different network ID than the current network ID, the router forwards the data packet to the uplink port where the next router will again either recognize the network ID and route the data packet locally or again forwards the data packet to the uplink port. By being exposed to traffic, a router adds to its routing table the pathways necessary to resolve a data packet's pathway to its final destination, by passing through one or more routers if necessary.

Connecting a Router

The way a router is connected to other devices changes its function.

Figure 2: The Way a Router is Connected Changes its Function



On some routers, the uplink port is marked as WAN (Wide Area Network) and the numbered ports are to be connected to the LAN (Local Area Network) devices.

Network Address Translation / Firewall

A router’s uplink port provides Network Address Translation (NAT) and firewall functions.

NAT is a method to hide the private IP addresses of a range of devices (connected to LAN ports) behind a single IP address presented at the WAN uplink port. NAT uses a mechanism to track requests to WAN IP addresses and readdresses the outgoing IP packets on exit so they appear to originate from the router itself. In the reverse communications path, NAT again readdresses the IP packet’s destination address back to the original source private IP address.

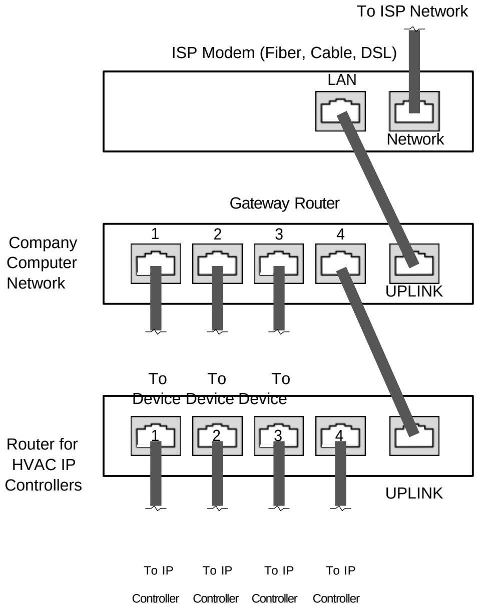
Due to this tracking mechanism, only requests originating from the LAN side can initiate communications. A request from the WAN to the router cannot be mapped into a private address as there is no outbound mapping for the router to use to properly readdress it to a private IP address. This is why a NAT acts as a firewall that blocks unsolicited access to the router’s LAN side.

Most routers allow you to open a port in the firewall so that WAN traffic received at a specific port number is always forwarded to a specific LAN IP address. The standard port numbers used by nLight ECLYPSE controllers is explained in chapter *nLight ECLYPSE Controller IP Network Protocols and Port Numbers.*

IP Network Segmentation

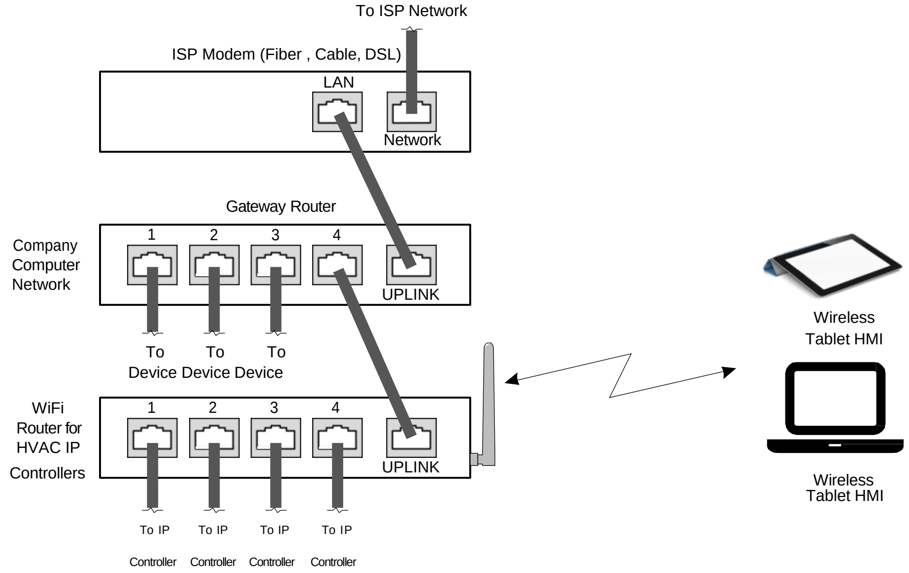
For efficient network planning, normally the IP controllers will be assigned to their own network segment of an IP network or subnetwork. This is done as shown in the figure below.

Figure 3: Network Segment for HVAC IP Controllers



For certain wireless topologies, a wireless router can be used to connect nLight ECLYPSE controller. In this scenario, a wireless operator interface (laptop or tablet) can be used for commissioning as shown in the figure below. If the lap- top has a Supervisor installed, it can be used to program ECB series controlers connected to the RS-485 port of the Connected System Controller.

Figure 4: Network Segment for HVAC IP Controllers with a Wireless Access Point



If a wireless router is unavailable or is out-of-range, an nLight ECLYPSE Wi-Fi adapter can be connected to an nLight ECLYPSE controller's USB port to add wire- less connectivity. See *Wireless NetworkConnection*.

CHAPTER 4

nLight ECLYPSE CONTROLLER IP NETWORK PROTOCOLS AND PORT NUMBERS

This chapter describes the IP Network Protocols and Port Numbers used by the nLight ECLYPSE controller.

Topics

About Port Numbers

In an IP packet, a port number is an extension of the packet's IP address and completes the destination address for a communications session. By convention, the packet's port number is associated with a protocol used between software applications and is used to uniquely identify a communications endpoint for a specific application or process running on a computer. This allows a multitude of applications to share a single physical connection to the Internet while allowing distinct communication channels between different applications.

For example, your web browser listens to port 80 on your computer to receive HTML web pages sent from a web server on port 80.

The standard port numbers used by nLight ECLYPSE controllers is explained in *nLight ECLYPSE IP Network Port Numbers and Protocols.*

Sometimes, two applications might use the same port number to communicate. To sort out this conflict, the following methods can be used.

- In the configuration of some applications, the port number can be changed from its default setting. Should you change it, you must also change it on the corresponding application also so that the port numbers will match.
- Routers have features such as port forwarding that can change an incoming packet's port number coming from the Wide Area Network (WAN) to another port number on the Local Area Network or vice versa.

nLight ECLYPSE IP Network Port Numbers and Protocols

nLight ECLYPSE uses the following IP Network Protocols to communicate over IPv4 networks. The corresponding default in-bound port number is also shown.

Service	Default Port Number (Protocol)	Description	Where can this port number be changed?
SMTP	25 (TCP)	Outgoing Email server port number.	See the EC-gfx Program User Guide, Resources Configuration.
DNS	53 (TCP, UDP)	Domain Name Server URL lookup.	–
DHCP	67 (UDP)	The router's DHCP service that allows a device to auto-configure a devices' IP settings.	–
HTTP	80 (TCP)	**EC-gfx Program Debugging Values (REST service)**: After the control logic or code has been sent to the controller, a live debugger allows programmers to execute code, view input/output values, and troubleshoot errors in real-time. **ENVYSION**: The ENVYSION server presents system status, trending visualization, real-time equipment visualization, schedule configuration, alarm monitoring, and dashboard functions to a Web browser operator interface. **Web Configuration Interface**: This is the network configuration interface for wired and wireless IP network interfaces.	See *System Settings*. If this is used with EC-Net, this parameter can be changed in the **RestService** and **WebService**.

Service	Default Port Number (Protocol)	Description	Where can this port number be changed?
HTTPS	443 (TCP)	**Secure EC-gfx Program Debugging Values (REST service)**: After the control logic or code has been sent to the controller, a live debugger allows programmers to execute code, view input/output values, and troubleshoot errors in real-time. **Secure ENVYSION**: The ENVYSION server presents system status, trending visualization, real-time equipment visualization, schedule configuration, alarm monitoring, and dashboard functions to a Web browser operator interface. Secure Web Configuration Interface: This is the network configuration interface for wired and wireless IP network interfaces.	See *System Settings*. If this is used with EC-Net, this parameter can be changed in the **RestService** and **WebService**.
Radius Server	1812 (UDP)	**Authentication Port**: This is the port on which authentication requests are made.	
Radius Server	1813 (UDP)	**Accounting Port**: This is the port on which accounting requests are made. This is only used to receive accounting requests from other RADIUS servers.	
Radius Server	1814 (UDP)	**Proxy Port**: This is an internal port used to proxy requests between a local server and a remote server.	See *User Management*. If this is used with EC-Net, these parameters must be set in the RadiusService.
BACnet/IP	47808 (UDP)	The BACnet over IP protocol.	See *BACnet Settings*
MQTT	8883(TCP)	SecureMQTelemetryTransport.Thisis an internal port that facilitates communication with the nLight Gateway.	

nLight ECLYPSE Services that Require Internet Connectivity

In order to operate, the following out-bound services require:

- A working DNS. See *Domain Name System (DNS).*
- The default gateway / router to be configured. See *Default Gateway.*
- Internet connectivity.

The corresponding default out-bound port number is also shown.

Service	Default Port Number (Protocol)	Description
SMTP	25 (TCP)	Outgoing Email server port number.
Network Time Protocol (NTP)	123 (UDP)	Used to set the controller's real time clock.
DNS server	53 (UDP, TCP)	Used to provide URL name resolution. The controller by default uses an internet DNS. If the local network has a DNS, set its IP address in *Network Settings*.

CHAPTER 5

CONNECTING IP DEVICES TO AN IP NET
WORK

An IP network requires infrastructure such as Ethernet cable, routers, switches, or Wi-Fi hotspots in order to work. The following topics discuss the fundamentals of such a network.

Topics

Connecting the IP Network

There are two methods to connect a device to an IP Network:

- Wired (Ethernet connection with the PRI and SEC ports).
- Wireless (when the nLight ECLYPSE Wi-Fi Adapter is connected to the controller).

Wired Network Cable Requirements

Wired networks use commonly available Cat 5e structural cabling fitted with RJ-45 connectors. If you make your own patch cable, use Category 5e cable and crimp the RJ-45 connectors at both ends of the cable either as T568A or T568B.

Table 2: Wired Network Cable Physical Specifications and Requirements

Parameter	Details
Media	Cat 5e Cable; four (4) pairs of wires with RJ-45 Connectors (standard straight patch cable)
RJ-45 Pin Configuration	Straight-through wiring. Crimp connectors as per T568A or T568B (both cable ends must be crimped the same way).
Characteristic impedance	100-130 Ohms
Distributed capacitance	Less than 100 pF per meter (30 pF per foot)
Maximum Cat 5e Cable length between IP devices	328 ft. (100 m) maximum. See *About the Integrated Ethernet Switch*.
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections) nLight ECLYPSE IP devices have two RJ-45 female RJ-45 connectors that provide IP packet switching to support follow-on devices.
Daisy-chain limit, Connected System Controllers	Up to 20 devices can be daisy-chained per network switch port.
Daisy-chain limit, Connected VAV Controllers	Up to 50 devices can be daisy-chained per network switch port.
EOL terminations	Not applicable
Shield grounding	Not applicable

.

Table 3: Distech Controls Recommended Cable Types to use for the Cat 5e Cable Subnetwork Bus

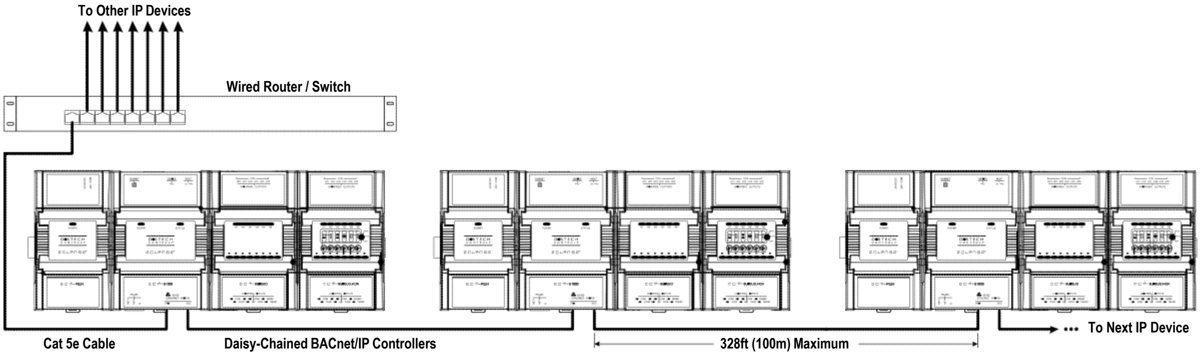
Bus and Cable Types	**Non-Plenum Applications (Use in Conduit - FT4)**		**Plenum Applications (FT6)**	
	Part Number	**O.D. (Ø)[1]**	**Part Number**	**O.D. (Ø)[1]**
300 m (1000 feet), Cat 5e Yellow Jacket Cable - Without Connectors	CB-W244P-1446YLB	4.6mm (0.18in.)	CB-W244P-2175YEL	4.6mm (0.18in.)
100 Crimp RJ 45 Connectors	CB-W5506E	N/A	CB-W5506E	N/A

[1] Outer cable diameter – This does not take into account the RJ-45 connector.

About the Integrated Ethernet Switch

The 2-port wired interface uses a switch to forward packets addressed to downstream IP devices connected to it. This allows controllers to be daisy-chained together to extend the IP network’s physical range and to reduce the amount of network cable required as each controller no longer has to make a home run to the network switch

Figure 5: Wired Network Connection: Daisy-Chained nLight ECLYPSE Controllers

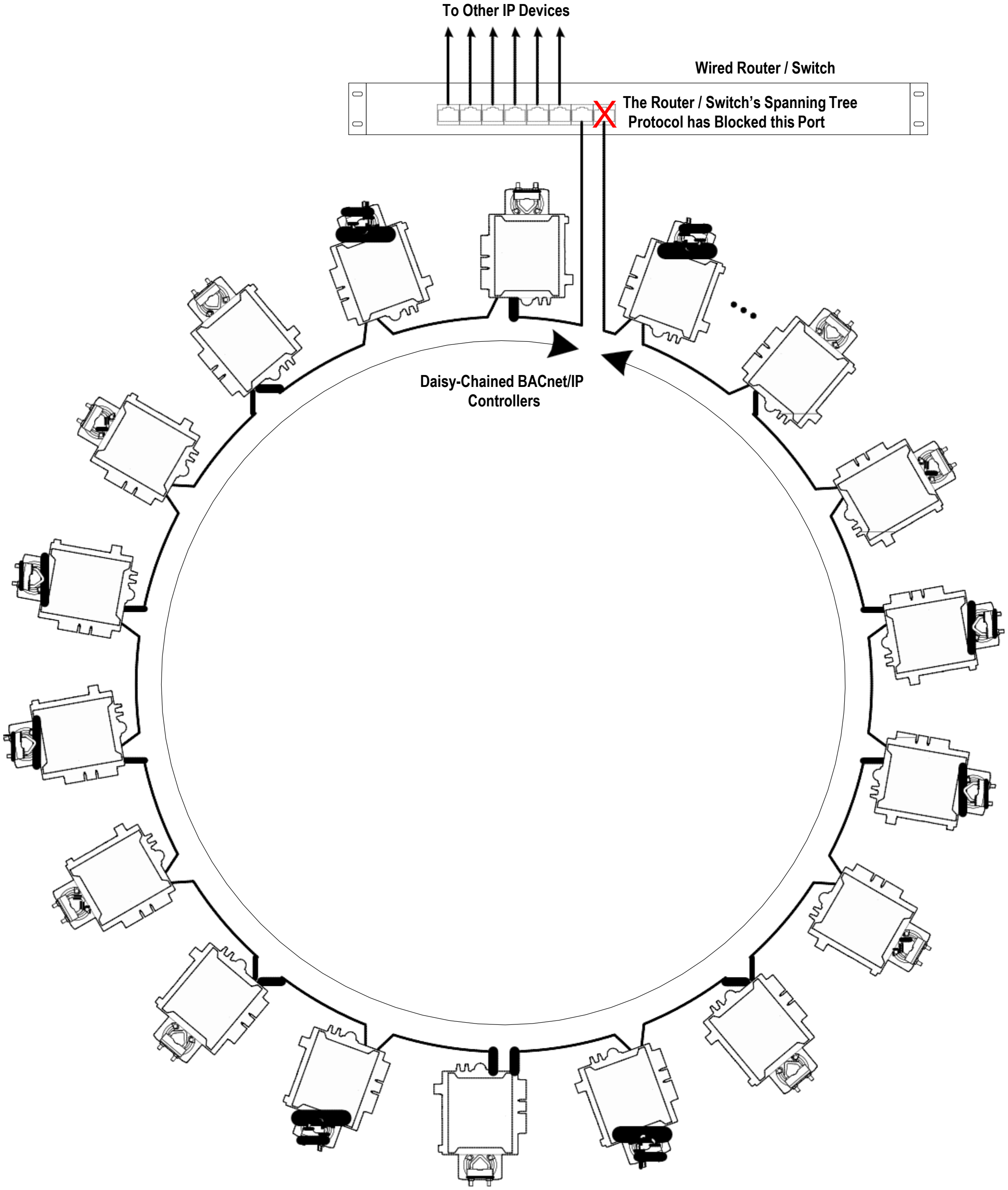


Spanning Tree Protocol

Switches and routers that support Spanning Tree Protocol (are IEEE 802.1D certified) are able to detect and eliminate a loop from being formed on the network by disabling any port on the router that is causing a loop. Such switches can be used to enhance network availability by allowing you to create a ring network of controllers that is resistant to a single point network failure (a cut wire for example).

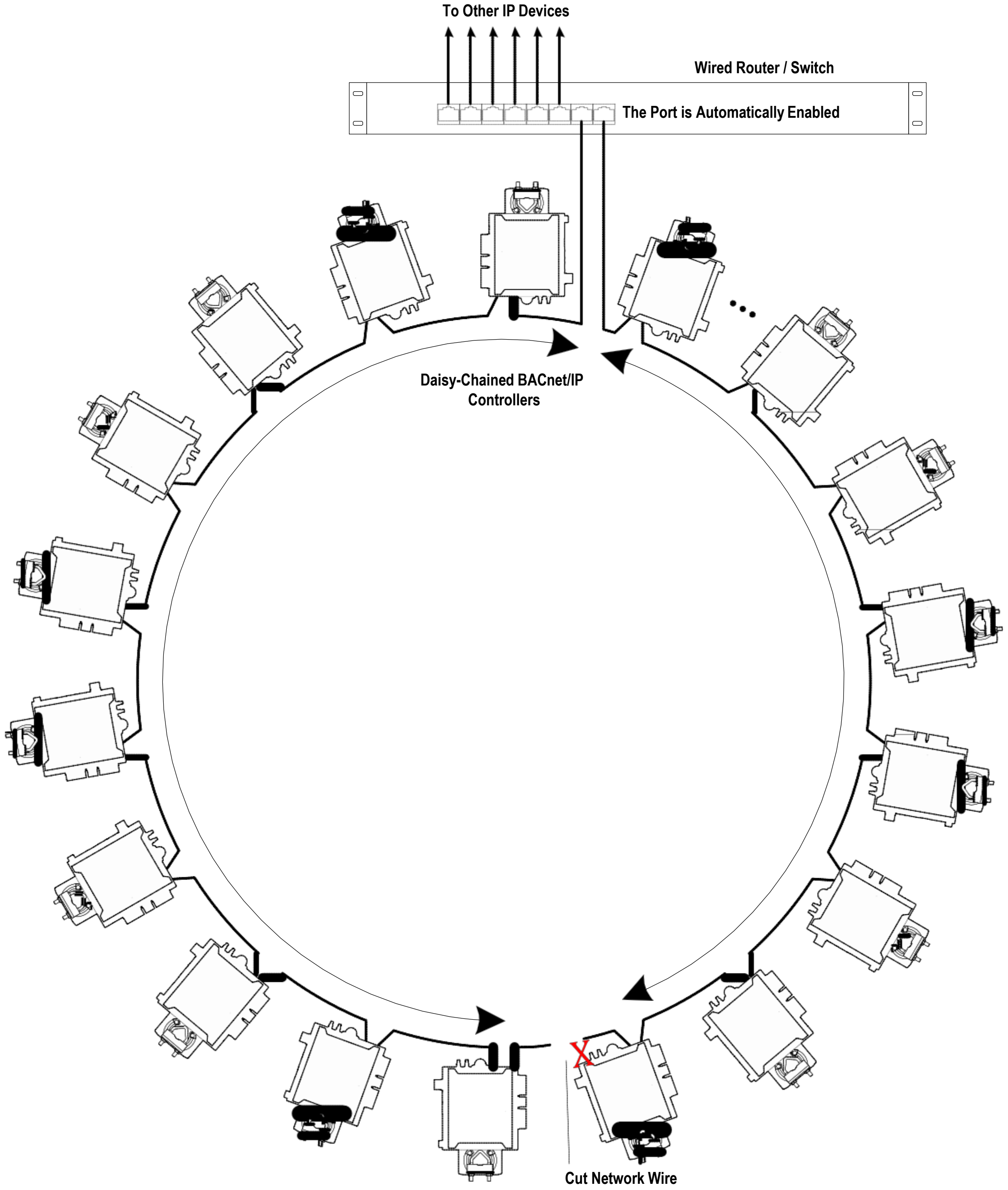
In this scenario, controllers are connected in a loop (or ring) such that the last controller is connected back to the switch / router. Under normal operation, the switch / router disables one of the ports to prevent a packet storm. This is shown below.

Figure 7: Wired Network Connection: Spanning Tree Protocol – Normal Operation


To Other IP Devices
Wired Router / Switch
X
The Router / Switch's Spanning Tree Protocol has Blocked this Port
Daisy-Chained BACnet/IP Controllers

When a network wire is cut, the ring is split into two – the switch / router automatically enables the port to maintain service. This is shown below.

Figure 8: Wired Network Connection: Spanning Tree Protocol – Failover Operation


To Other IP Devices
Wired Router / Switch
The Port is Automatically Enabled
Daisy-Chained BACnet/IP Controllers
Cut Network Wire

The switch / router can be configured to send an email message when port blocking is disabled thus signaling that a network wire has been cut.

Connecting the Network Cable to the nLight ECLYPSE Controller

To connect controllers to an Ethernet network and then discover them, see chapter *First Time Connection to an nLight ECLYPSE Controller*.

Wireless Network Connection

The nLight ECLYPSE Wi-Fi adapter connects to an nLight ECLYPSE controller's USB port.

Figure 9: nLight ECLYPSE Wi-Fi Adapter

It adds wireless IP connectivity to nLight ECLYPSE controllers and it can be used in a number of wireless topologies and applications.

Recommendations are provided regarding the radio signal obstructions and factors that should be avoided to obtain the best Wi-Fi radio signal transmission and reception. Walls attenuate radio wave propagation by an amount that varies with the construction materials used. See *Radio Signal Transmission Obstructions* for more information on wall materials that can reduce range transmission.

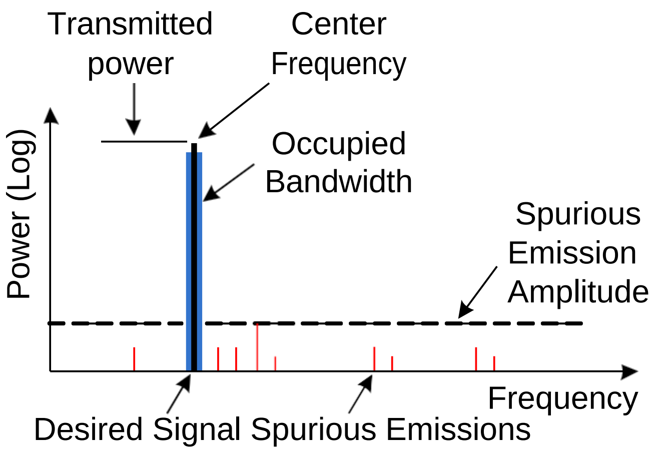
About the 2.4 GHz ISM band

The 2.4 GHz ISM (Industrial, Scientific and Medical) band has been allocated worldwide for the use of radio frequency energy by industrial, scientific, and medical purposes as part of the device's method of internal operation and as such may have powerful emissions that cause interference to radio communications.

For example, microwave ovens operate in the 2.4 GHz ISM band with about 1000W emitted power and a fraction of a percent of that energy does leak from the oven. While this is not a health risk, Wi-Fi networks operate at even lower power levels to communicate and can be overwhelmed by this source of interference.

When setting up a 2.4 GHz band Wi-Fi network, you must take into consideration any equipment that operates in the 2.4 GHz ISM band such as medical and laboratory equipment. Other sources of interference are other telecommunications equipment such as cell phones, GSM/DECT, cordless phones, RFID reader, Bluetooth devices, walkie-talkies, baby monitors, and so on. Note that equipment that transmits in other frequency bands do emit spurious emissions at low levels over a wide spectrum so that a radio transmitter in close proximity to the nLight ECLYPSE Wi-Fi adapter can cause interference, even if its operating frequency is 1.9 GHz for example.

Figure 10: Typical Radio Transmitter Spurious Emissions



Distance between nLight ECLYPSE Wi-Fi Adapter and Sources of Interference

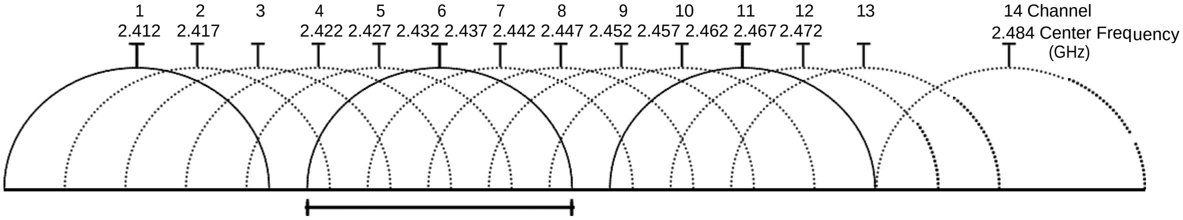
Unrelated transmitters should be more than 6.5 feet (2 m) away from the nLight ECLYPSE Wi-Fi Adapter to avoid possible interference.

About Wi-Fi Network Channel Numbers

Wi-Fi communications use a slice of radio spectrum or channel width for data transmission. In general terms, the amount of channel width required is proportional to the data transmission rate. Wi-Fi networks operate in a number of different frequency ranges or bands such as the 2.4 GHz band. Each band is divided into a number of industry-standard channels that represent a center frequency for data transmission. In practice, the center frequency is the midpoint between the upper and lower cutoff frequencies of the channel width.

When the channel width is larger than the channel spacing (the space between channels), overlap between the channels can occur, resulting in inter-channel interference that lowers overall network throughput. This is shown in the diagram below. For example, in the 2.4 GHz band using 802.11 g, the channel width is 20 MHz while the channel spacing is 5 MHz. If one Wi-Fi network is using channel 1 that is in close proximity to another Wi-Fi network that is using channel 2, there will be significant inter-channel overlap and interference. Data throughput is reduced as a result.

Figure 11: 2.4 GHz Band 802.11g Radio Spectrum Showing Inter-Channel Overlap



For a 20 MHz channel width in the 2.4 GHz band using 802.11g, the best channels to use to avoid inter-channel overlap are channels 1, 6, and 11. For a 40 MHz channel width in the 2.4 GHz band using 802.11g, the best channels to use to avoid inter-channel overlap are channels 3 and 11.

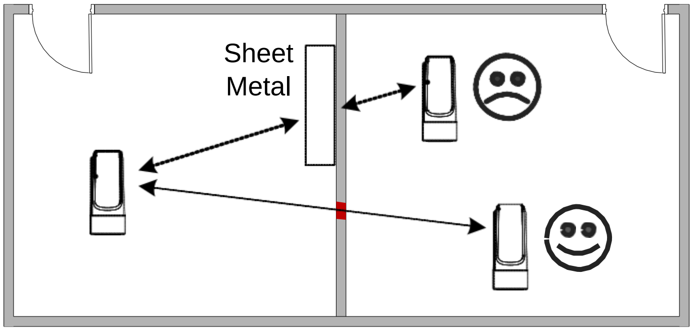
For a 20 MHz channel width in the 2.4 GHz band using 802.11n, the best channels to use to avoid inter-channel overlap are channels 1, 6, and 11. For a 40 MHz channel width in the 2.4 GHz band using 802.11g, the best channel to use to avoid inter-channeloverlap is channel 3.

For industrial / commercial environments, it is recommended to avoid using a 40 MHz channel width in the 2.4 GHz band as it occupies a large part of the available radio spectrum. This means that it will be difficult to co-exist with other networks while avoiding interference, especially from devices that use mixed mode 802.11 b/g which significantly degrades 802.11n performance. One solution is to disable the 802.11 b/g mode on all hotspots to force all wireless clients to 802.11n mode, thereby forbidding the use of legacy devices.

Radio Signal Range
Radio Signal TransmissionObstructions
Where to Locate Wireless Adapters

When installing the wireless adapter, it is important to ensure that distances and obstructions do not impede transmission. Metallic parts, such as steel reinforcement in walls, machinery, office furniture, etc. are major sources of field strength dampening. Furthermore, supply areas and elevator shafts should be considered as complete transmission screens, see following figure.

Figure 12: Screening of Radio Waves

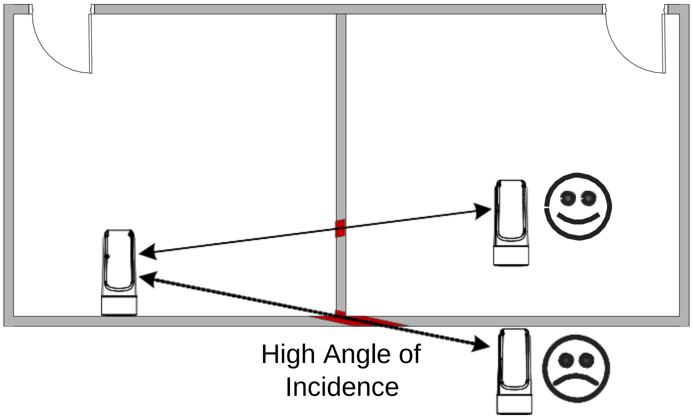


Transmission Obstructions and Interference

One way to get around an obstruction, such as a duct, is to place the wireless adapter on the side of the obstruction that is nearer to the coordinating wireless device, even if the controller is on the opposite side of the obstruction. But always keep in mind that the wireless adapter performs best when it is away from metal objects or surfaces (more than 1" (2.5 cm)).

In addition to obstructions, the angle with which the transmission travels through the obstruction has a major influence on the field strength. The steeper the angle through an obstruction, the radio wave has to travel through more material resulting in the field strength reduction (See *Figure 13*.). Therefore, it is preferable that the transmission be arranged so that it travels straight and perpendicularly through the obstruction.

Figure 13: Angle of Radio Waves



A solution to avoid an obstruction is to add another wireless router located closer to the controller(s).

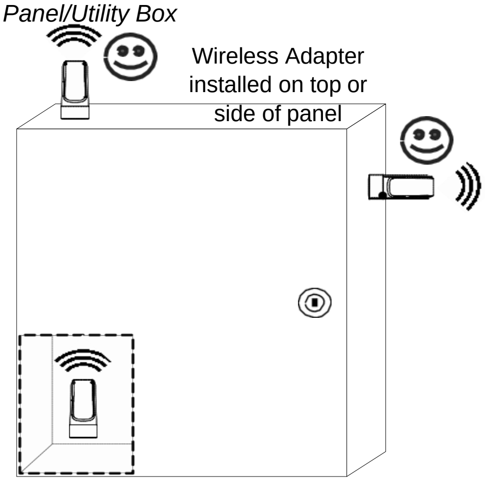
nLight ECLYPSE Wi-Fi Adapter MountingTips

This section provides information and examples on how to properly position the nLight ECLYPSE Wi-Fi Adapter to ensure reliable wireless communication. The most common guidelines to remember when installing the nLight ECLYPSE Wi-Fi Adapter is to keep it at least 1” (2.5 cm) away from metal, and never install the nLight ECLYPSE Wi-Fi Adapter inside a metal enclosure (relay panels, junction box, etc.).

Typical Metal Relay Panel/ Utility Box Installation

The following image shows where to install an nLight ECLYPSE Wi-Fi Adapter on a metal relay panel or utility box with a controller inside the panel/box. To maxi- mize wireless range, the nLight ECLYPSE Wi-Fi Adapter must be installed on the top or side of the panel.

Figure 16: nLight ECLYPSE Wi-Fi Adapter Position with Metal Relay Panel/Utility Box



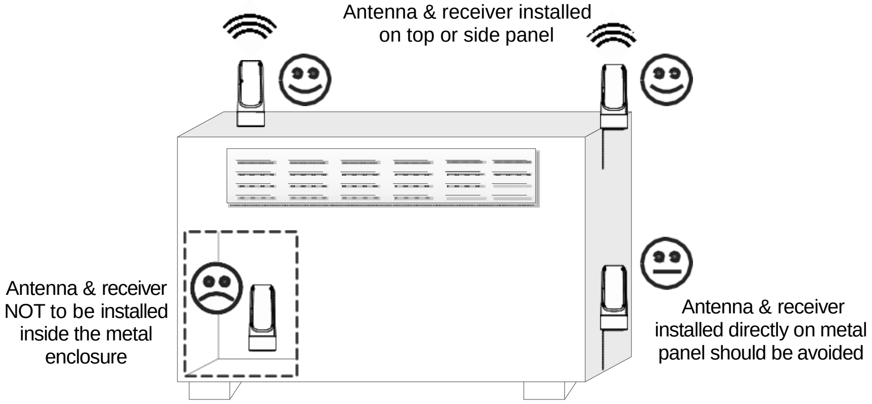
☹ Wireless Adapter
NOT to be installed
inside the panel

Typical Fan Coil Unit Installation

The following example shows where to install an nLight ECLYPSE Wi-Fi Adapter on a fan coil unit with a controller inside the unit.

must be installed on the top or side of the unit with the antenna straightened out and away from the metal. The nLight ECLYPSE Wi-Fi Adapter and antenna should never be installed inside the metal enclosure.

Figure 17: nLight ECLYPSE Wi-Fi Adapter Position on Fan Coil Unit

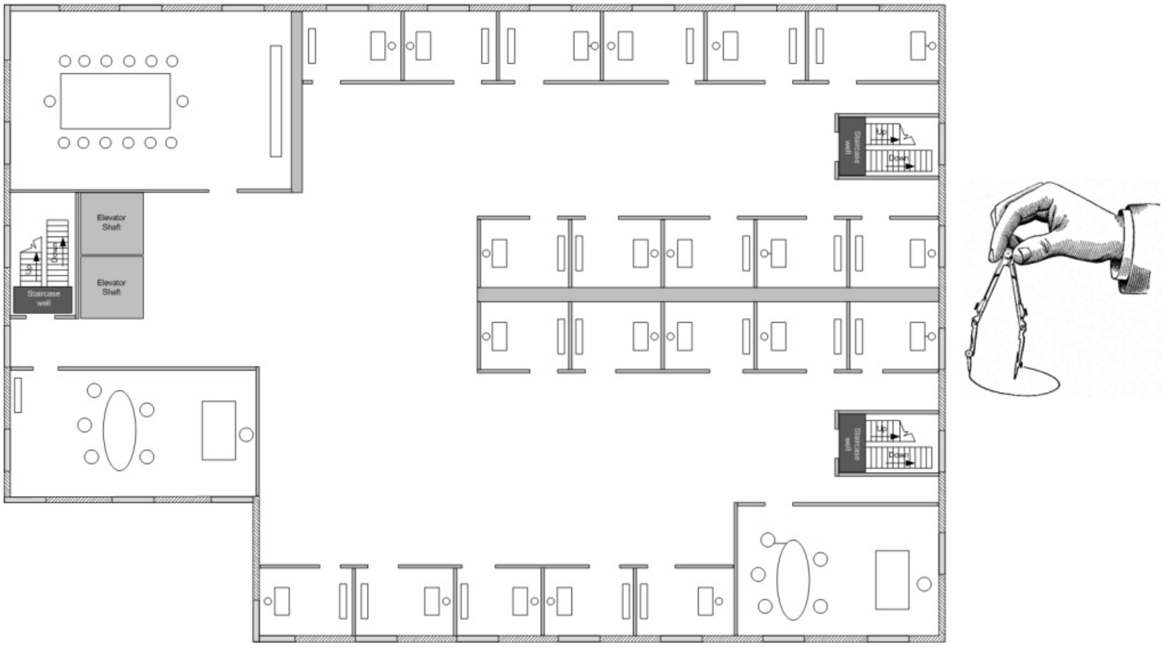

Antenna & receiver installed on top or side panel
Antenna & receiver NOT to be installed inside the metal enclosure
Antenna & receiver installed directly on metal panel should be avoided

Planning a Wireless Network

A wireless network can be installed in many different types of floor spaces, large or small: office space, commercial space, residential space, etc. The following provides an example on how to start planning a wireless network such as a large office space. This type of planning can also be used with smaller areas.

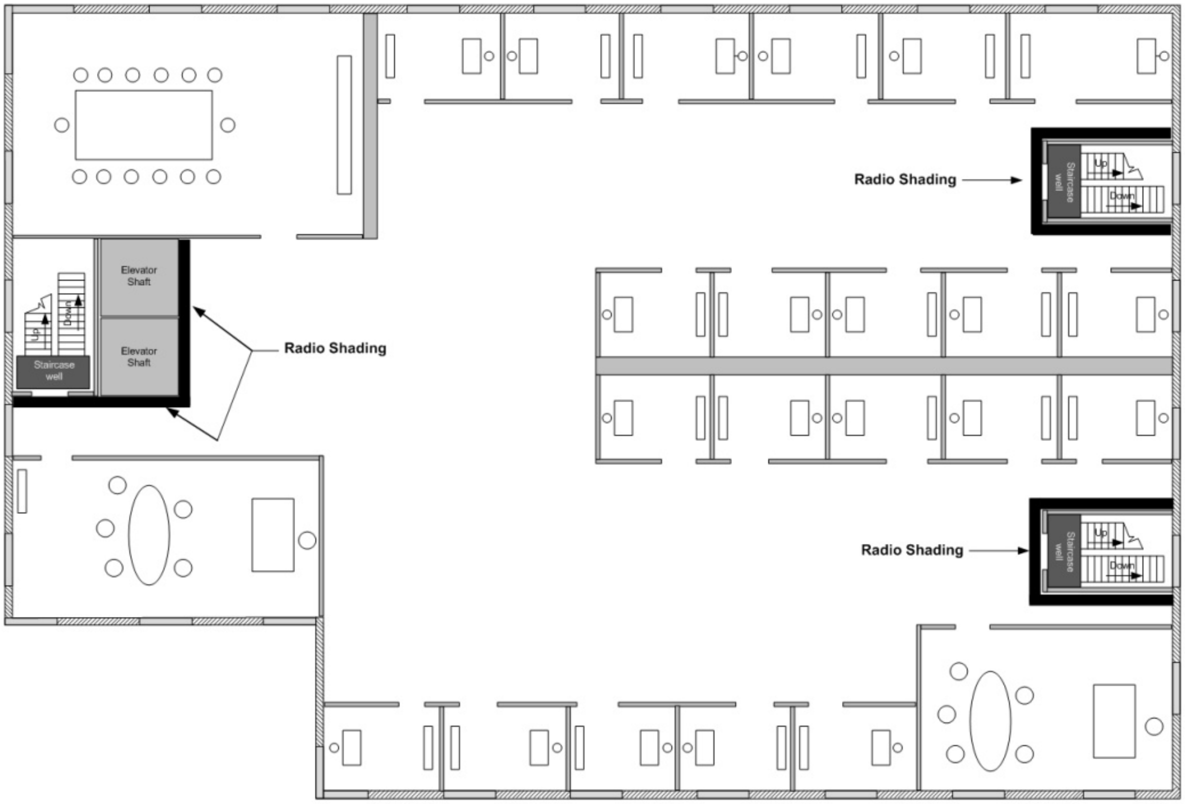
1. Retrieve a copy of your floor plans and a compass.

Figure 18: Copy of floor plan and a compass



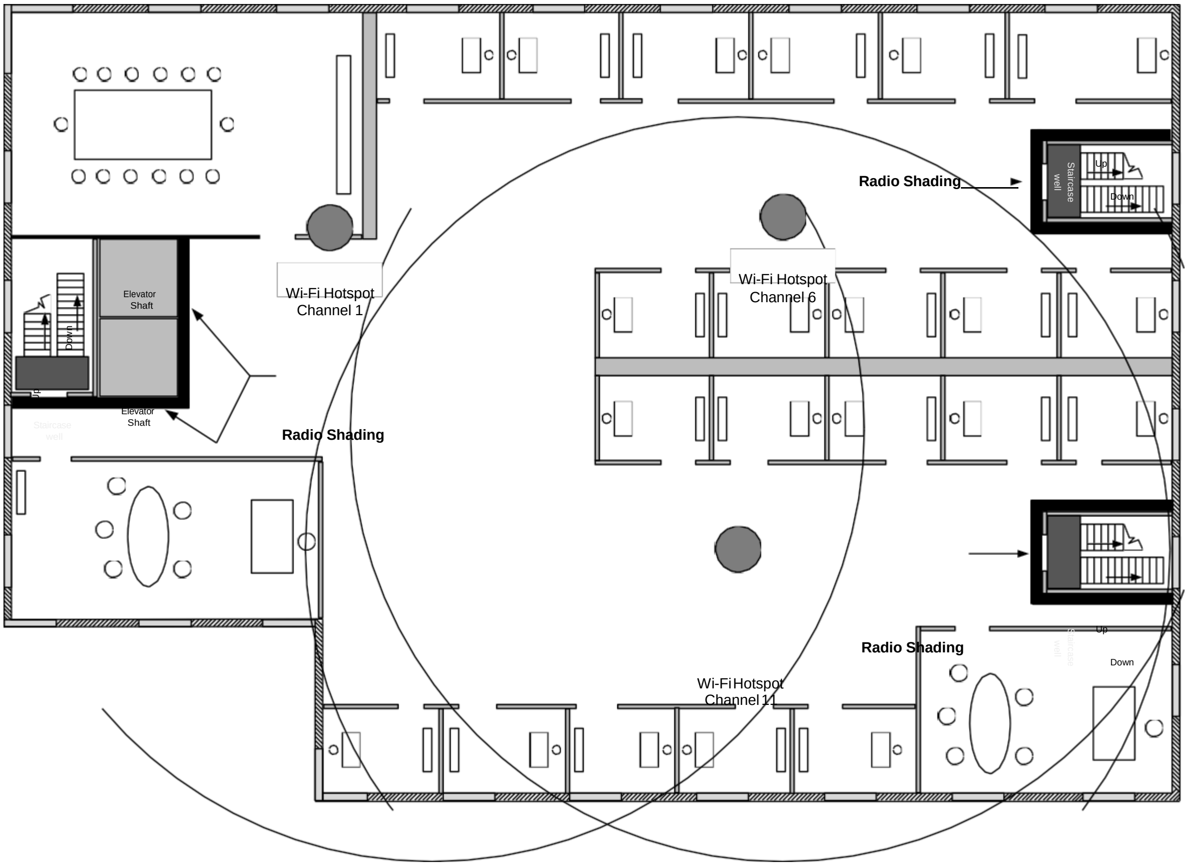
2. Mark relevant radio shadings into floor plan such as: fire protection walls, lavatories, staircases, elevator shafts and supply areas.

Figure 19: Mark relevant radio shadings



3. Draw circles to locate the ideal positions for your nLight ECLYPSE Wi-Fi Adapter as shown below:

Figure 20: Radio nLight ECLYPSE Wi-Fi Adapter Location



Make sure that the nLight ECLYPSE Wi-Fi Adapter is positioned in a way such that no screens block the connection to any corner inside the fire safety section (potential sensor positions).

For reliable range planning, the unfavorable conditionsshould be detected at the beginning but often come from later changes to the environment (room filled with people, alteration of partition walls, furniture, room plants, etc.).

Even after careful planning, range and signal tests should be done during installation to verify proper reception at the nLight ECLYPSE Wi-Fi Adapter positions. Unfavorable conditions can be improved by changing the antenna position or by adding a router closer to the controller(s).

nLight ECLYPSE Wi-Fi Adapter ConnectionModes

nLight ECLYPSE Wi-Fi adapter supports a number of connection modes shown in the table below:

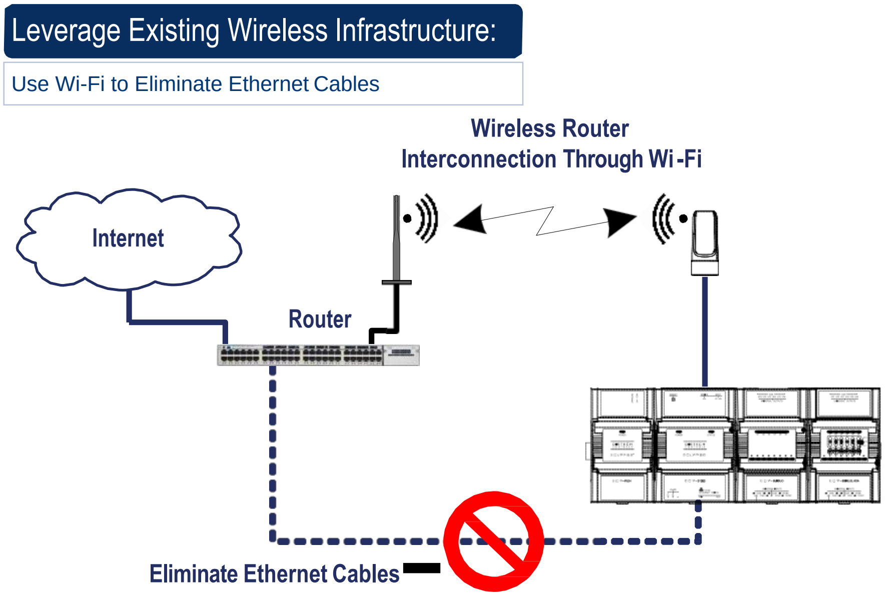
Connection Mode	Description	Max Number of Wireless Clients or Nodes
Client	This sets the mode of the nLight ECLYPSE Wi-Fi adapter to connect the controller as a client of a Wi-Fi access point. This interface can auto-configure its IP parameters when the connected network that has a DHCP server. When an nLight ECLYPSE controller is a Wi-Fi client, the Ether- net ports can be used to provide network connectivity to another nLight ECLYPSE controller or to a laptop for example. Each connected device counts towards the “Maximum Number of Wireless Clients or Nodes”. See *Wireless Bridge* for more information.	16
Access Point	This sets the mode of the nLight ECLYPSE Wi-Fi adapter to be a Wi-Fi access point. This access point operates off of the same subnetwork and has the same IP connectivity that the controller has with its wired network connection. For example, if the controller’s wired connection is to a net- work that has an active DHCP server, access point clients can also use this DHCP server to automatically configure their IP connection parameters.	16
Hotspot (default)	This sets the mode of the nLight ECLYPSE Wi-Fi adapter to be a Wi-Fi hotspot with a router. This puts the hotspot into a separate subnetwork with a DHCP server to provide IP addresses to any connected device. Wide area network (WAN) connectivity is through the wired connection.	16

Typical application examples are shown below.

Wi-Fi Client Connection Mode

Cut installation costs by leveraging existing wireless infrastructure and by eliminating the need for Ethernet cables. This architecture is characterized by the point-to-point connection between an access point and a client-controller.

Figure 21: Leveraging Existing Wireless Infrastructure by Eliminating Ethernet Cables

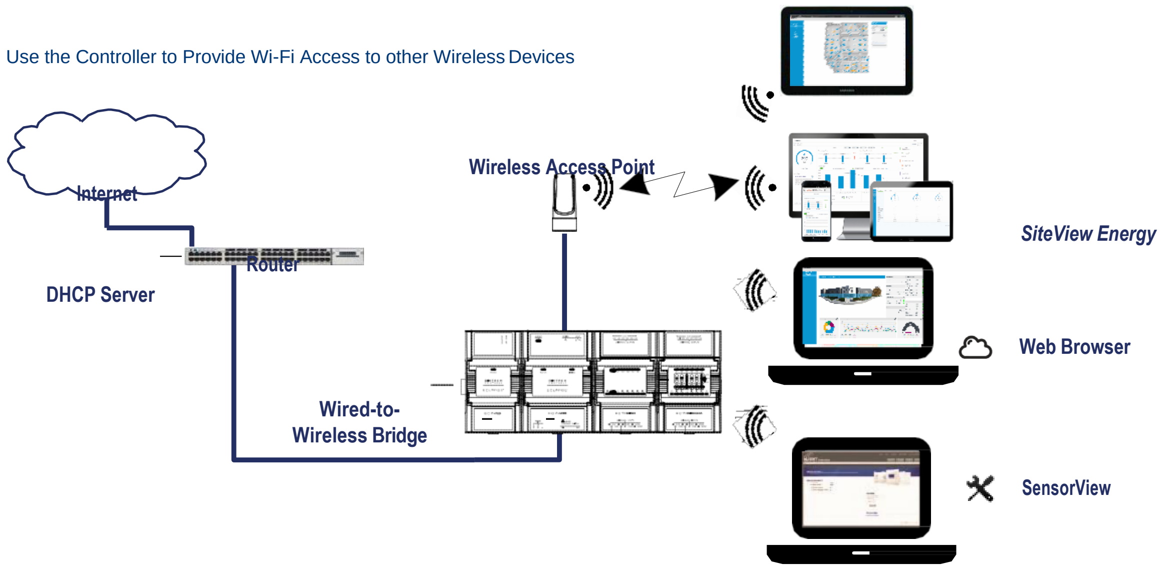

Leverage Existing Wireless Infrastructure:
Use Wi-Fi to Eliminate Ethernet Cables
Wireless Router
Interconnection Through Wi-Fi
Internet
Router
Eliminate Ethernet Cables

To configure the Wi-Fi client connection mode, see *Setting up a Wi-Fi Client Wireless Network*.

Wi-Fi Access Point

Should there be no available access point; an nLight ECLYPSE controller can be configured as a wired-to-wireless bridge to create an access point which can provide Wi-Fi access to other Wi-Fi enabled clients. This access point operates off of the same subnetwork and has the same IP connectivity that the controller has with its wired network connection. The nLight ECLYPSE Wi-Fi adapter can also be temporarily added to an nLight ECLYPSE controller for wireless commissioning purposes. A variety of software applications are available for system monitoring and override, commissioning, configuration and programming.

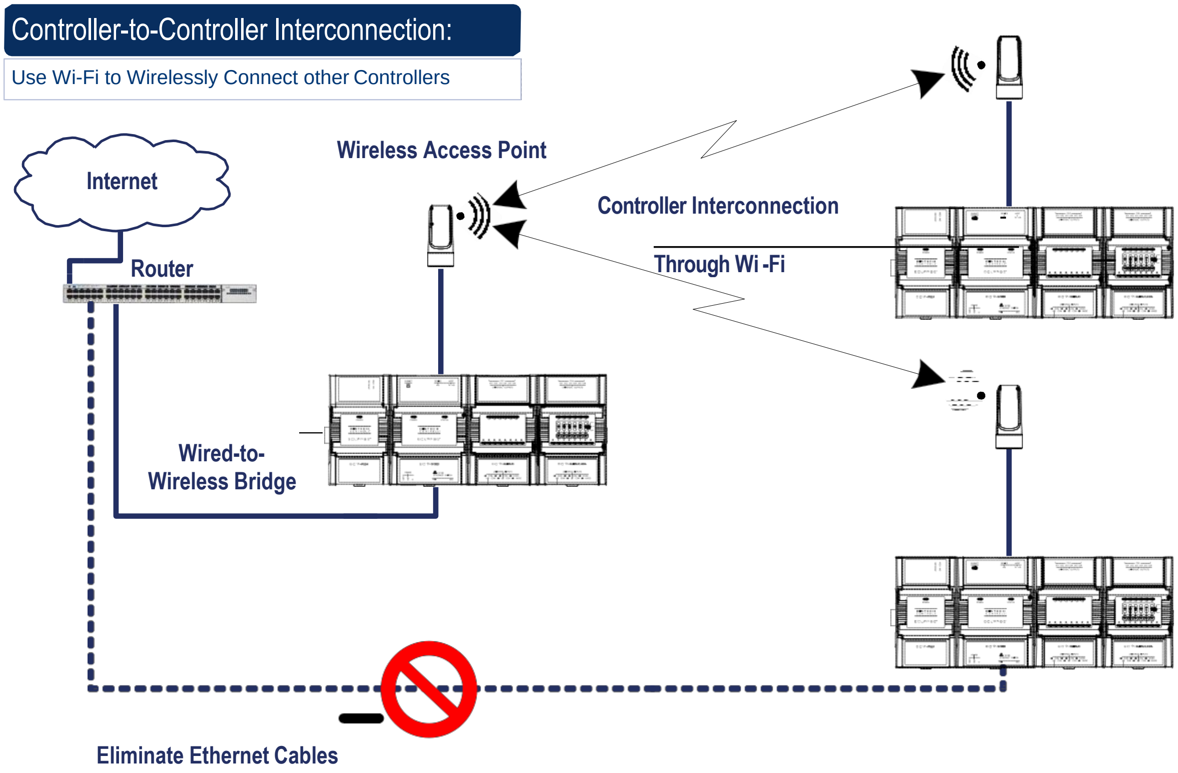
Figure 22: Using an nLight ECLYPSE Controller Create an Access Point



A second nLight ECLYPSE controller can be configured as a wireless client. This can be used as a solution to 'jump' architectural features that are not compatible with wires such as glass atrium and the like. To configure the Wi-Fi client connection mode, see *Setting up a Wi-Fi Client Wireless Network*.

An access point can provide Wi-Fi access to other Wi-Fi enabled clients and controllers.

Figure 23: Using an nLight ECLYPSE Controller as a Wireless Bridge

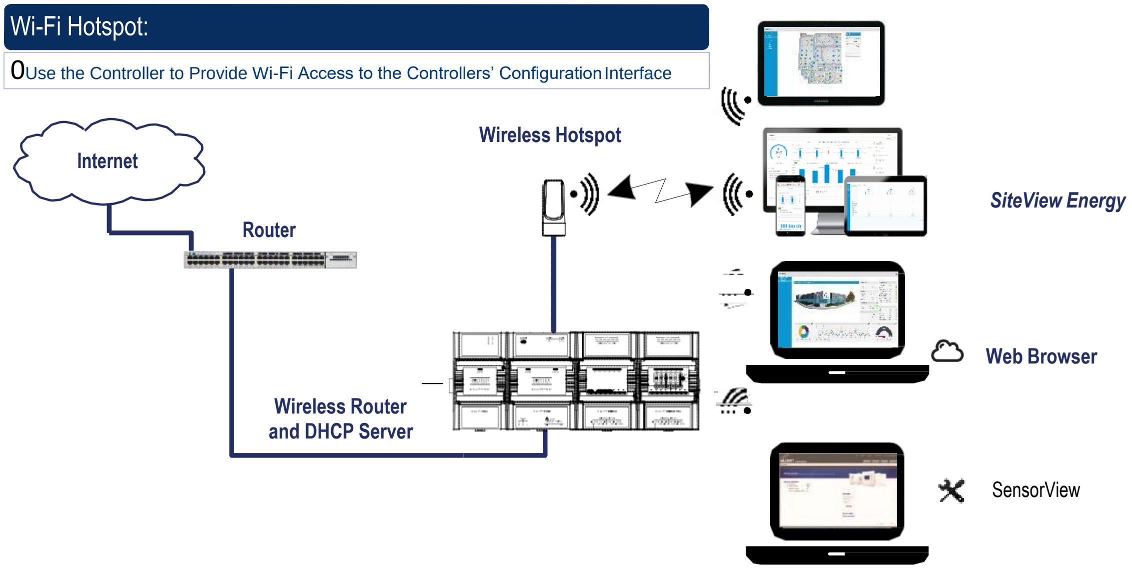

Controller-to-Controller Interconnection:
Use Wi-Fi to Wirelessly Connect other Controllers
Internet
Router
Wireless Access Point
Controller Interconnection
Through Wi -Fi
Wired-to-
Wireless Bridge
Eliminate Ethernet Cables

Wi-Fi Hotspot

Should the wired network not use a DHCP server (uses fixed IP addresses); an nLight ECLYPSE controller can be configured to create a hotspot with a router that creates its own subnet and DHCP server which can provide Wi-Fi access to other Wi-Fi enabled clients. This is the default connection method when an nLight ECLYPSE Wi-Fi adapter is connected to an nLight ECLYPSE controller. The nLight ECLYPSE Wi-Fi adapter can also be temporarily added to an nLight ECLYPSE controller for wireless commissioning purposes. A variety of software applications are available for system monitoring and override, commissioning, configuration and programming.

A hotspot creates a subnetwork. As a result, any connected BACnet device will not be able to discover BACnet devices on any other LAN subnetwork.

Figure 24: Using an nLight ECLYPSE Controller Create a Hotspot

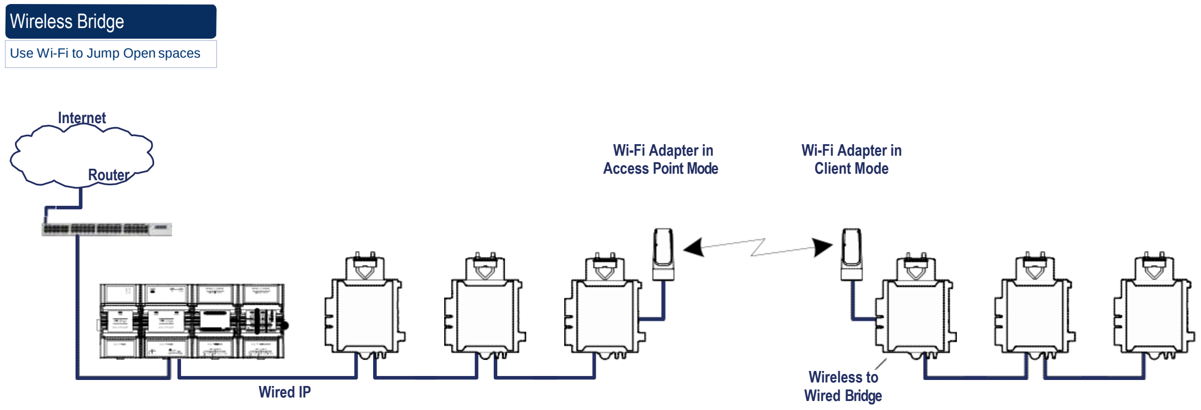


Wireless Bridge

A second nLight ECLYPSE controller can be configured as a wired-to-wireless bridge to allow the connection of wired IP devices to the bridged controller's Ethernet ports. This can be used as a solution to 'jump' architectural features that are not compatible with wires such as glass atrium and the like.

The access point / hotspot can provide Wi-Fi access to other Wi-Fi enabled clients.

Figure 25: Using an nLight ECLYPSE Controller as a Wireless Bridge

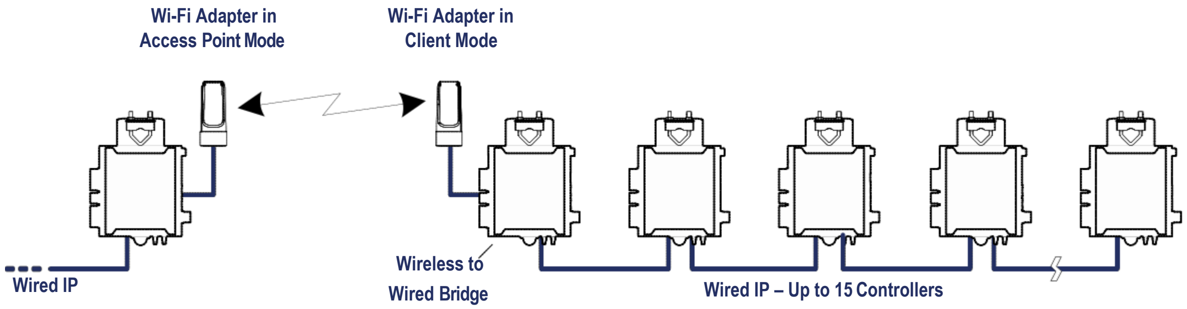


Maximum Number of Wireless Clients or Nodes for an Access Point

A wireless access point can service a maximum of 16 clients or nodes in total. The following examples show what this limit can be composed of:

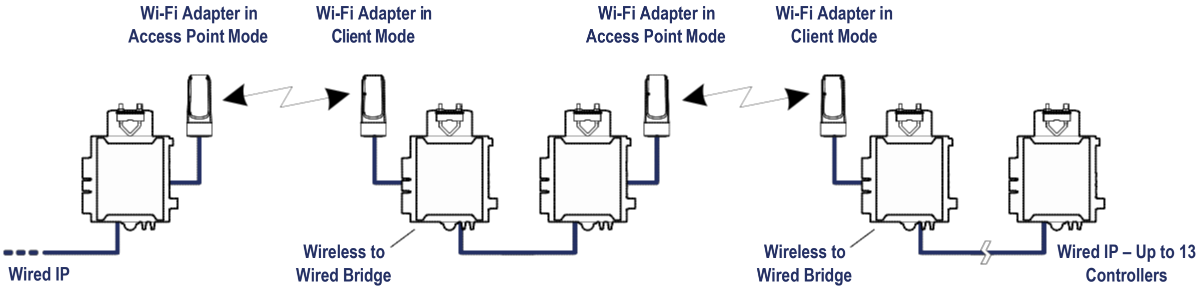
- One wireless bridged controller is connected to as many as 15 daisy-chained wired devices.

Figure 26: Using an nLight ECLYPSE Controller as a Wireless Bridge



- One wireless bridged controller is connected to one wired controller that is wirelessly connected to one wireless bridge that is then connected 13 daisy chained wired devices.

Figure 27: Using an nLight ECLYPSE Controller as a Wireless Bridge



If the access point is a Wi-Fi router:

1. The number of devices is limited by the total number of clients the router is able to support.
2. It can support many controllers acting as wireless to wired bridges.
3. Each wireless to wired bridge controller can support up to 15 controllers.

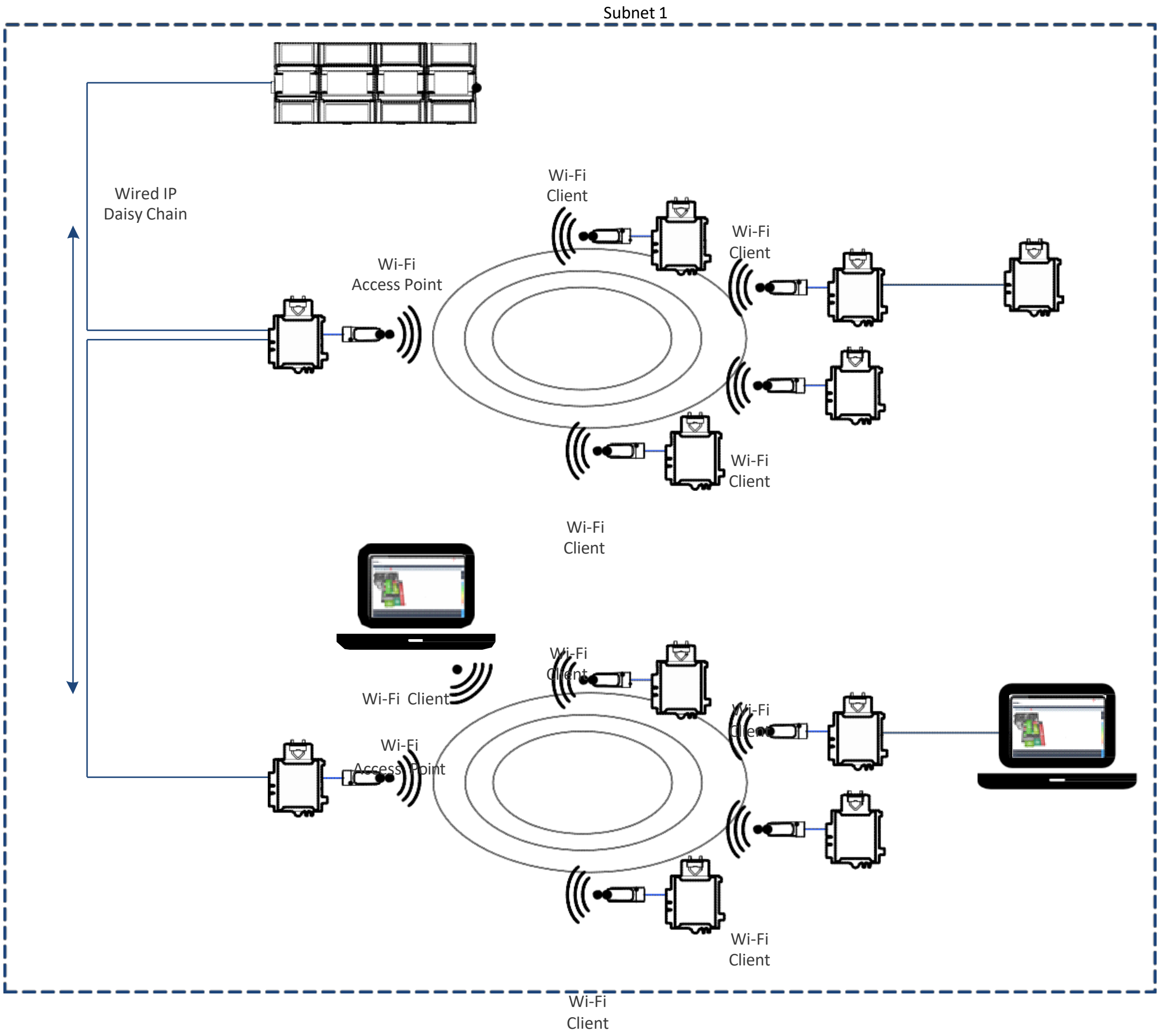
Wireless Network Commissioning Architectures

Client to Access Point Configuration

A laptop is connected through Wi-Fi, as a Wi-Fi client, to any ECLYPSE Controller that has its wireless settings configured as an Access Point. The other ECLYPSE Controllers are configured as Wi-Fi Clients and are wirelessly connected to the same Access Point.

With this configuration, the laptop and all the nLight ECLYPSE controllers are on the same subnet, so either laptop user has access to all networked nLight ECLYPSE controllers.

Figure 28: Client to Access Point Configuration



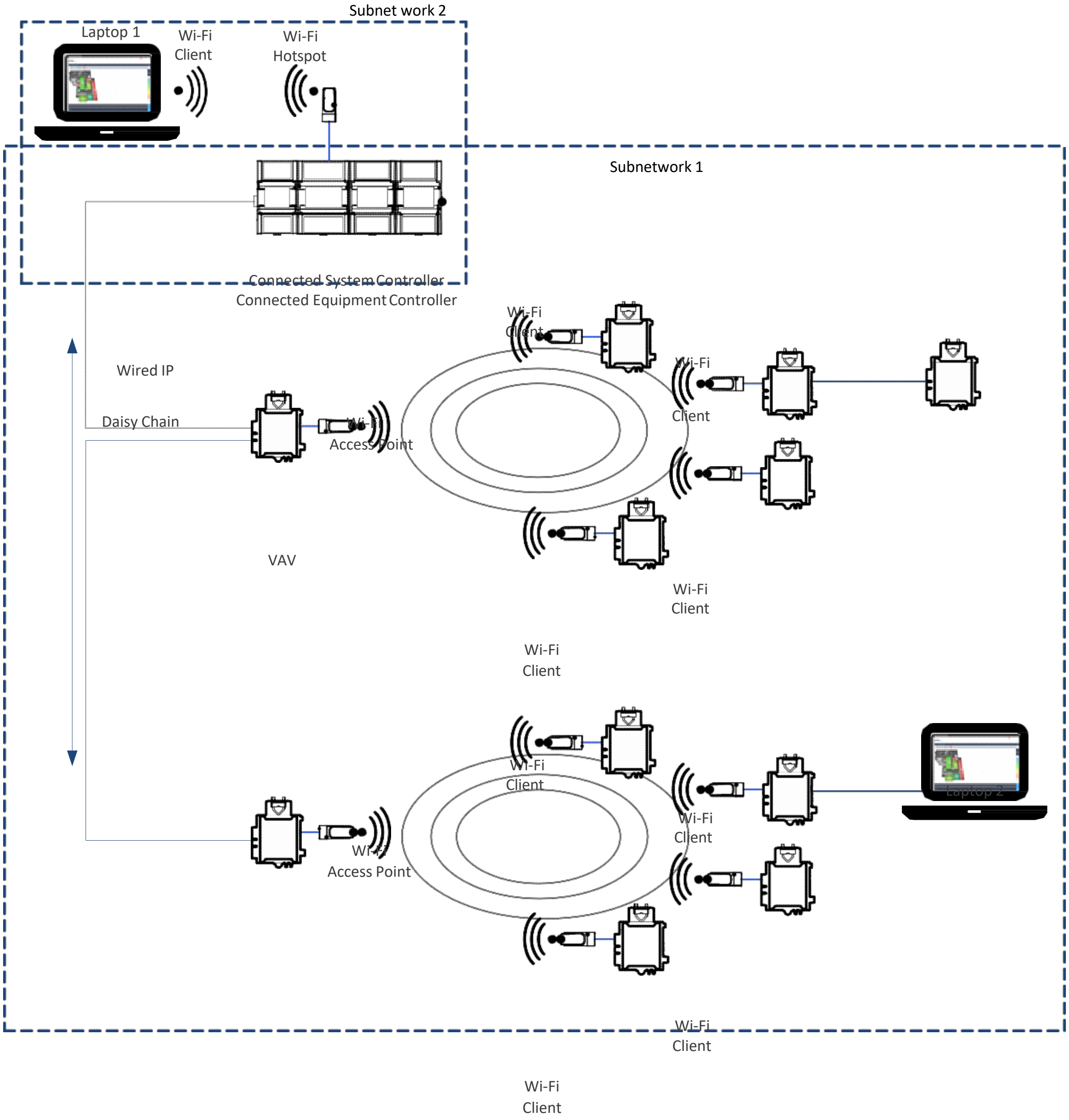
Client to Hotspot Configuration

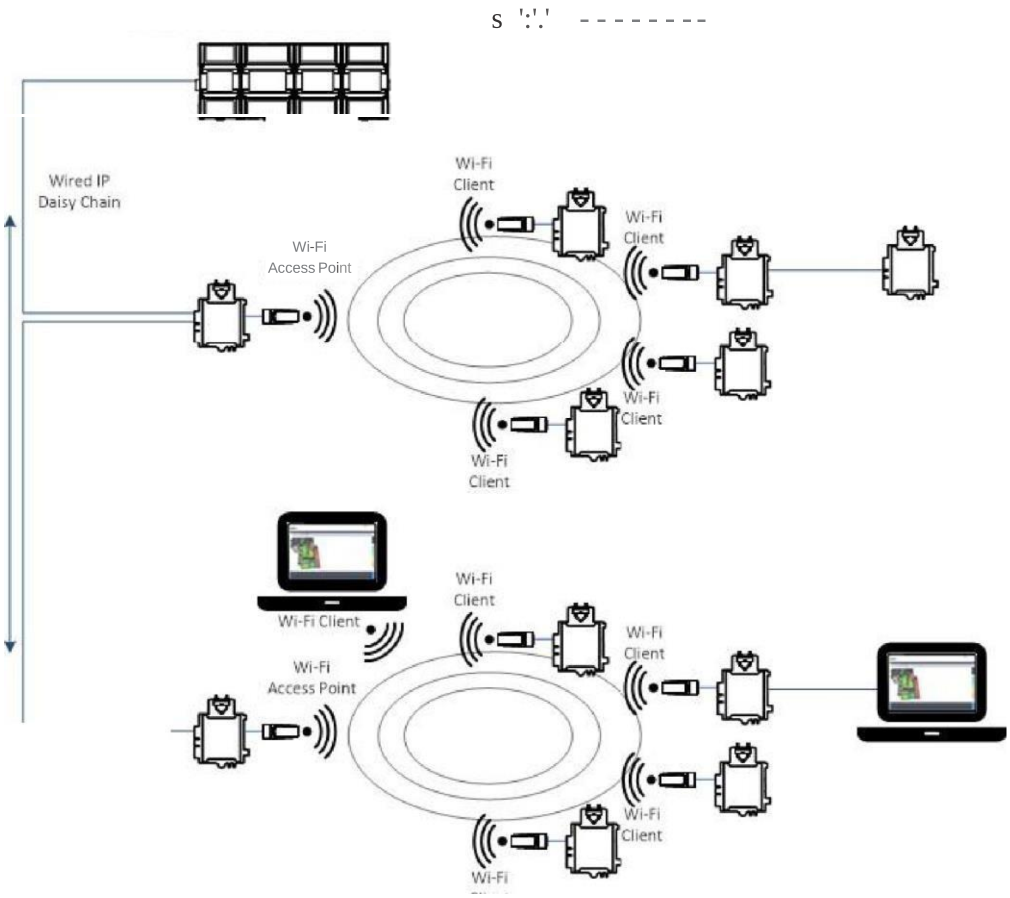
Laptop 1 is connected as a Wi-Fi client to a Connected System Controller that has its wireless settings configured as a Hotspot (Subnetwork 2). The ECLYPSE Controllers that are part of the wired network are configured, on their wireless side as a Wi-Fi Access Point (Subnetwork 1).

The remaining ECLYPSE Controllers are configured as a Wi-Fi Client and are wirelessly connected to a VAV controller's Access Point.

With this configuration, laptop 1 is on the same subnet as the Connected System Controller (Subnetwork 2 created by the Hotspot), but all the Connected VAV Controllers are on a different Subnet (Subnetwork 1), so the laptop 1 user only has access to the Connected System Controller. This is because BACnet/IP broadcast discovery messages such as "Who-Is" do not pass through network routers that separate subnetworks. In the example shown below, the Connected System Controller acts as a router between the Wi-Fi hotspot clients and the wired network. This means that BACnet/IP controllers on different subnetworks will not normally communicate with each other. The laptop 2 user has access to both the ECLYPSE controllers and the Connected System Controller. A solution is to use BBMD on both Laptop 1 (using EC-Net for example) and on the Connected System Controller. See *BACnet/IP Broadcast Management Device Service (BBMD)*.

Figure 29: Client to Hotspot Configuration




S ':'.' --------
Wired IP
Daisy Chain
Wi-Fi
Client
Wi-Fi
Access Point
Wi-Fi
Client
Wi-Fi
Client
Wi-Fi
Client
Wi-Fi Client
Wi-Fi
Client
Wi-Fi
Access Point
Wi-Fi
Client
Wi-Fi
Client
Wi-Fi

CHAPTER 6

FIRST TIME CONNECTION TO AN nLight ECLYPSE CONTROLLER

This paragraph is here to introduce the topics that will be discussed in the chapter. Following it should be a Topics paragraph.

Topics

Connecting to the Controller

When connecting to the controller for the first time, the goal is to gain access to the controller so that you can configure it to work in its future network environment. To do so, you must connect the controller to form a network.

There are two networking methods to connect to a controller:

- Wired (Ethernet connection) with a PC.
- Wireless (when the nLight ECLYPSE Wi-Fi Adapter is connected to the control- ler) with a PC. See *Wi-Fi Network Connection.*

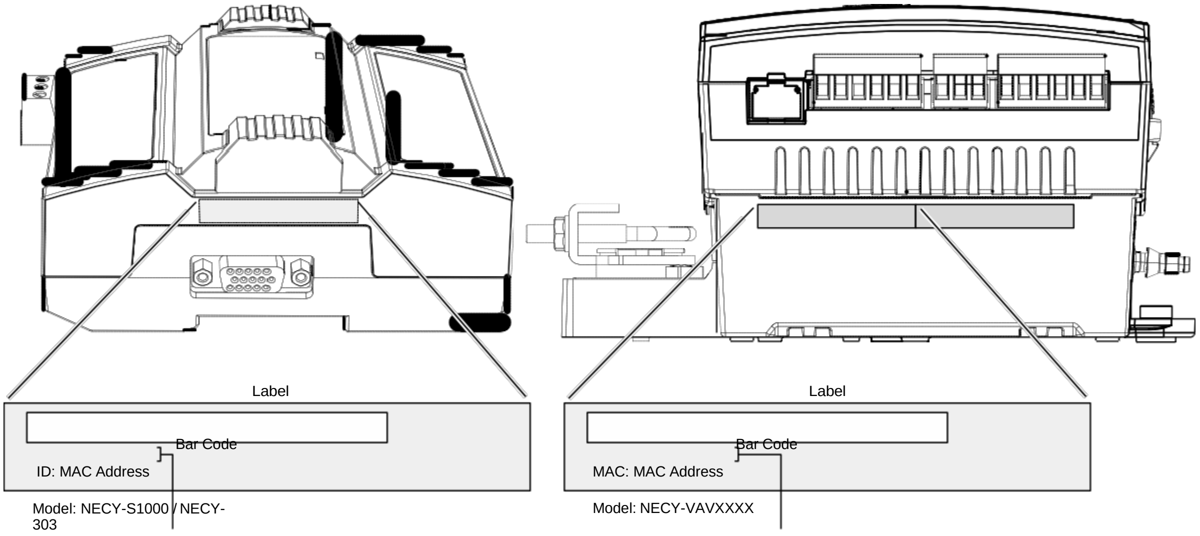
Once you have connected the controller(s) to a network, configure the controller. See *Configuring the Controller.*

Controller Identification

Controllers are uniquely identified on the network by their MAC address. This identifier is printed on a label located on the side of the controller and another is on the controller’s box. Get a printed copy of the building’s floor plan. During controller installation, peel the MAC address sticker off of the controller’s box and put it on the floor plan where the controller has been installed.

This MAC address is used as part of the controller’s factory-default Wi-Fi access point name and its hostname.

Figure 30: Finding the Controller's MAC Address



For example, for a MAC Address of : 76:a5:04:cd:4a:d1
The factory-default name for the Wi -Fi access point is **nLightECLYPSE-CD4AD1**
The factory-default hostname is **nLight ECLYPSE-cd4ad1.local**

For example, for a MAC Address of : 76:a5:04:cd:4a:d1
The factory-default name for the Wi -Fi access point is **nLight ECLYPSE-CD4AD1**
The factory-default hostname is **nLight ECLYPSE-cd4ad1.local**

Depending on the controller model, the way the controller is connected to the network will change according to whether the controller is a Power over Ethernet (PoE) model or not.

- For non-PoE controller models, see *Network Connections for NECY Series Controllers.*
- For the NECY-VAV-PoE controller, see *Network Connections for NECY-VAV- PoE Model Controllers.*.

See also *Connecting IP Devices to an IP Network* for network wir- ing considerations.

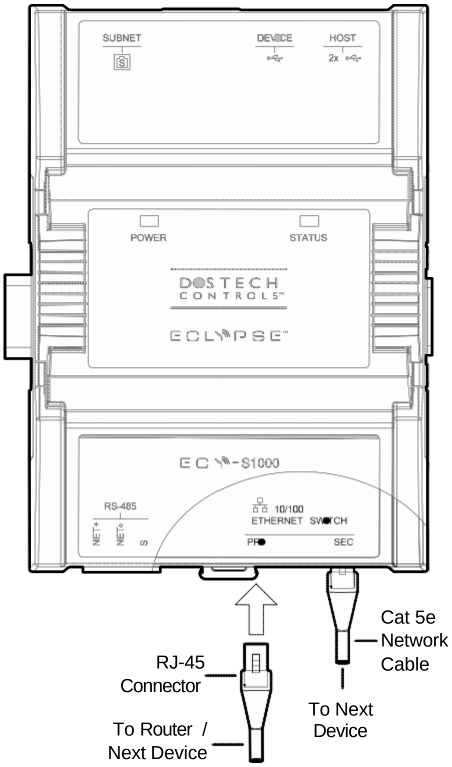
Network Connections for NECY Series Controllers

Connect the controller to the network as follows:

1. Connect your PC’s network card to the controller’s **PRI** Ethernet port using a Category 5e Ethernet cable.

If you are commissioning more than one controller, connect the controllers and PC to a network switch. Two or more controllers can be connected to the network by daisy-chaining them together by using Cat 5e network Cables to connect the **Ethernet Switch Sec**(ondary) connector of one controller to the **Ethernet Switch Pri**(mary) connector of the next controller.

Figure 31: nLight ECLYPSE Wired Network Connection: Cat 5e Cables with RJ-45 Connectors are used



2. Connect power to the controller(s). See the controller's Hardware Installation Guide for how to do so.

Wi-Fi Network Connection

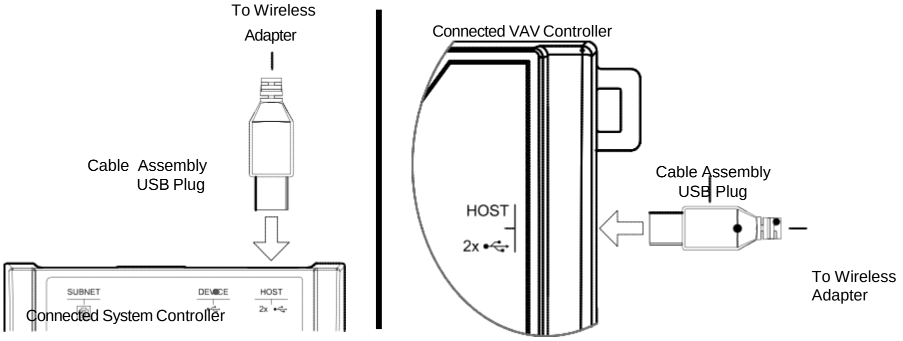
Once the nLight ECLYPSE Wi-Fi Adapter has been connected to a powered controller, a Wi-Fi hotspot becomes available that allows you to connect to the controller’s configuration Web interface with your PC.

On your PC’s wireless networks, look for an access point named nLight **ECLYPSE- XXYYZZ** where **XXYYZZ** are the last 6 hexadecimal characters of the control- ler’s MAC address.

To find the controller’s MAC address, see *Controller Identification*.
The default password for the wireless network is: **ECLYPSE1234**

Either of the controller’s two USB HOST ports can be used to connect the wireless adapter.

Figure 34: Connecting the Wireless Adapter to the Controller’s USB HOST Port



Configuring the Controller

Any of the following methods can be used to connect to the controller’s interface in order to configure it:

- Using the controller’s factory-default Hostname in the Web browser
- Using the controller’s IP address in the Web browser

Using the Controller’s Factory-default Hostname in the Web Browser

Controllers have a factory-default hostname that you can use instead of an IP address to connect to it[1]. The hostname can be used in a Web browser’s address bar. Then install The Bonjour service. The Bonjour service must be installed on your PC to allow your PC to discover controllers by their hostname.

If your PC is unable to resolve the controller’s hostname, you must connect your PC to the controller through Ethernet or Wi-Fi so that your PC only sees the controller network. For example, in this case, your PC must be disconnected from all other networks such as a corporate network or the Internet. If necessary, temporarily disconnect your PC’s network cable from its Ethernet port.

The controller’s factory-default hostname is **ECLYPSE-xxxxxx.local** where **xxxxxx** is the last 6 characters of the MAC address printed on a sticker located on the side of the controller. See *Controller Identification.*

For example, the sticker on the side of a controller shows that its MAC address is 76:a5:04:cd:4a:d1. Connect to the controller’s Web interface as follows:

1. Open your Web browser.

2. In the Web browser’s address bar, type **https://nLight ECLYPSE-cd4ad1.local**
and click go.

3. Login to the controller. Then set the controller’s configuration parameters in the controller’s configuration Web interface. See *Connecting to the Controller’s Configuration Web Interface.*

The Hostname can be changed in the *System Settings.*

Using the Controller’s IP Address in the Web Browser

Connect to a controller through its IP address as follows:

For a Wi-Fi network connection

1. Open your Web browser.

2. In the Web browser’s address bar, type **https://192.168.0.1** (the controller’s factory-default wireless hotspot IP address) and click go.

3. Login to the controller. Then set the controller’s configuration parameters in the controller’s configuration Web interface. See *Connecting to the Controller’s Configuration Web Interface.*

[1] Not all smart phones/mobile devices have the Bonjour service installed and thus cannot use the hostname mechanism.

For an Ethernet network connection

You must know the controller’s current IP address (from the DHCP server for example).

1. Open your Web browser.

2. In the Web browser’s address bar enter the controller’s IP address and click go.

3. Login to the controller. Then set the controller’s configuration parameters in the controller’s configuration Web interface. See *Connecting to the Controller’s Configuration Web Interface.*

Connecting to the Controller’s Configuration Web Interface

The nLight ECLYPSE Series Controller configuration can be made through the controller’s configuration Web interface to set all the controller’s configuration parameters including the controller’s IP address according to your network planning.

At the first connection to an nLight ECLYPSE Controller you will be forced to change the password to a strong password for the admin account to protect access to the controller.

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. Remove the factory default admin account as this is a commonly known security breech (only the password for this user account needs to be compromised). See *User Management*, *Securing an nLight ECLYPSE Controller*, and *Supported RADIUS Server Architectures*.

Next Steps

In Network Settings, configure the controller’s network parameters so that they are compatible with your network. See *nLight ECLYPSE Web Interface.*

CHAPTER 7

nLight ECLYPSE WEB INTERFACE

This chapter describes the nLight ECLYPSE controller's Web interface.

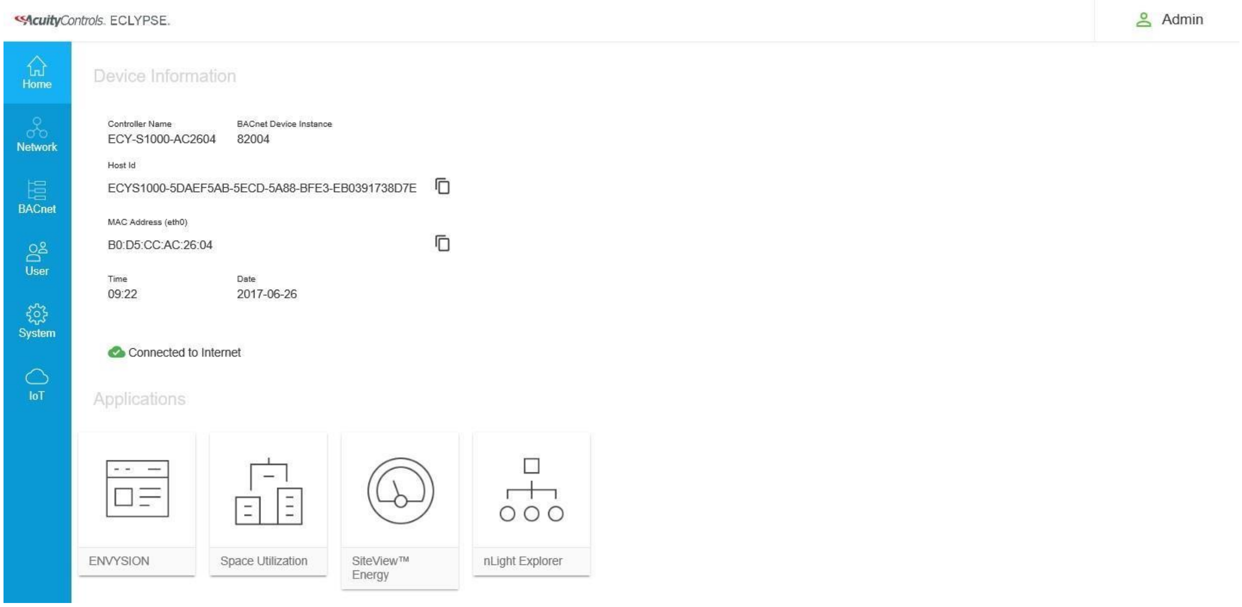
Topics

Overview

The nLight ECLYPSE controller has a web-based interface that allows you to view system status, configure the controller, update the controller's firmware, and access different applications associated to your projects.

Note that if you intend on enabling FIPS 140-2 mode, it should be done prior to configuring the controllers. See *FIPS 140-2 Mode.*

Figure 41: nLight ECLYPSE Controller's Web Interface Welcome Home Page



Device Information

Controller Name: ECY-S1000-AC2604

BACnet Device Instance: 82004

Host Id: ECYS1000-5DAEF5AB-5ECD-5A88-BFE3-EB0391738D7E

MAC Address (eth0): B0:D5:CC:AC:26:04

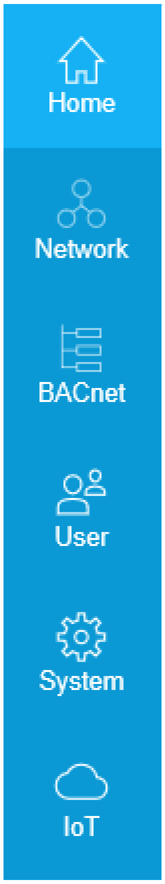
Time: 09:22

Date: 2017-06-26

Connected to Internet

Configuration Menu

The sidebar contains the Configuration menus that allow you to view and set the controller's configuration settings including its IP address, Wi-Fi settings, and to update the controller's firmware. The menus may vary according to the associated device licenses and the user's access level. These configuration parameters are password protected.



- *IPS Luminaires*
- *Home Page*
- *Network Settings*
- *BACnet Settings*
- *User Management*
- *System Settings*

HomePage

Themainareaofthehomepageconsistsofthefollowingitems:

Item	Description
Device Information	This section provides basic information on the device such as controller name, device instance, host ID, MAC address, time, and date.
⧉	The Copy icon allows you to copy the Host Id and/or the MAC address of the device to that you can quickly paste elsewhere as needed.
Connected to Internet	This indicates whether the nLight ECLYPSE controller is connected to the Internet or not.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Applications</td><td>To access different applications associated toyour projects and controller license such as the following:
<table>
<tr><td>SiteView™ Energy</td><td>The energy metering edge application gives building owners real-time, actionable data about their facility’s energy consumption and makes it easier to identify usage trends and savings</td></tr>
<tr><td>nLight Explorer</td><td>An edge application that gives a general system overview and a look at the system health of connected nLight devices</td></tr>
<tr><td>Space Utilization</td><td>The Space Utilization edge application allows building owners and property managers to analyze where occupants spend their time throughout the day, and make data-driven decisions for renovation, space planning and other expansions</td></tr>
<tr><td>ENVYSION</td><td>The responsive, web-based design and visualization interface that delivers actionable, graphical data</td></tr>
</table></td></tr>
</table>

User Profile and Login Credentials

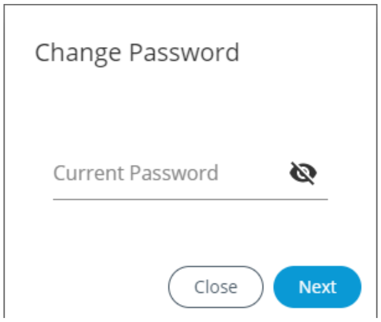
Click the profile box to change your password and logout.

AtthefirstconnectiontoannLight ECLYPSEControlleryouwillbe forcedto change the password to a strong password for the *admin* account to protect access to the controller.Itisimportanttocreatenewuseraccountswithstrongpasswords to protect the controller from unauthorized access.

See *User Management*, *Securing an nLight ECLYPSE Controller*, and *Supported RADIUS Server Architectures*.

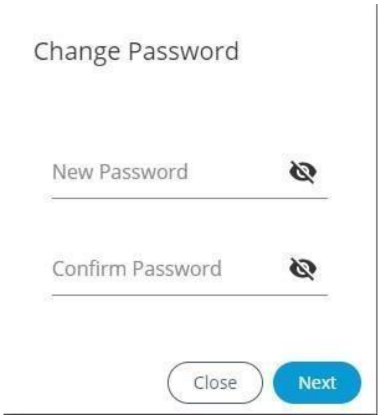
Tochangeyour password

1. To change your password, click the profile icon and select **Change Password**.



Change Password

2. Enter your current password and click **Next**.



3. Enter the new password twice to confirm and click **Next**.Your password is changed.

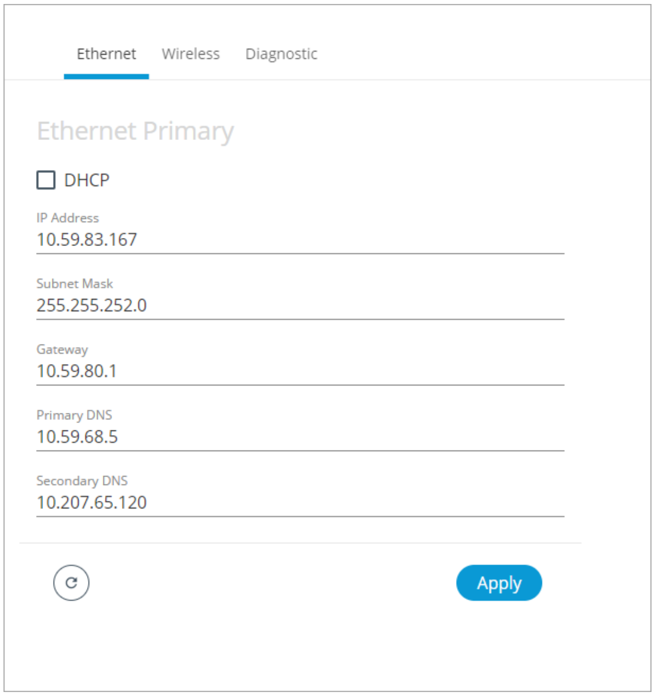
NetworkSettings

The **Network** menu is used to configure the nLight ECLYPSE controller's network interface and set up the wired and wireless network configuration parameters. The available menus are:

- Ethernet
- Wireless
- Diagnostic

Ethernet

The Ethernet screen is used for any wired IP connections that are made through either one of the controller's **Ethernet Switch Pri**(mary) connector or **Ethernet Switch Sec**(ondary) connector. See *Figure 31* and *Figure 32*. The Wired IP parameters can be auto-configured when the connected network has a working DHCP server. The alternative is to manually configure the controller's IP parameters.



Ethernet Primary

□ DHCP

IP Address
10.59.83.167

Subnet Mask
255.255.252.0

Gateway
10.59.80.1

Primary DNS
10.59.68.5

Secondary DNS
10.207.65.120

Option	DHCP Client: Enabled	DHCP Client: Disabled
DHCP	If the controller is connected to a network that has an active DHCP server, enabling this option will automatically configure the Wired IP connection parameters. The Wired IP parameters shown below are read only (presented for information purposes only).	If you want to manually configure the controller's network settings (to have a fixed IP address for example) or in the case where the network does not have a DHCP server, disable this option. In this case, you must set the Wired IP connection parameters shown below to establish network connectivity. See also *DHCP versus Manual Network Settings*
IP Address	This is the IP Address provided by the network's DHCP server.	Set the IP address for this network device. See *IPv4 Communication Fundamentals* Ensure that this address is unique from all other device on the LAN including any used for a hot spot's IP addressing.
Subnet Mask	This is the subnet mask provided by the network's DHCP server.	Set the connected network's subnetwork mask. See *About the Subnetwork Mask*
Gateway	This is the gateway IP Address provided by the network's DHCP server.	The IP address of the default gateway to other networks. This is usually the IP address of the connected network router. See *Default Gateway*
Primary DNS Secondary DNS	This is the primary and secondary DNS IP Address provided by the network's DHCP server.	The connected network's primary and secondary IP address of the DNS servers. See *Domain Name System (DNS)*

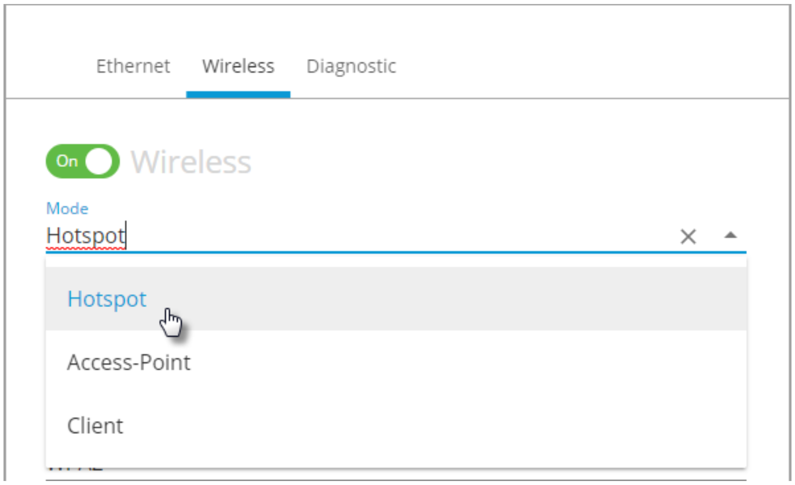
When making changes to the network settings, click **Apply** to apply and save the changes. You can click refresh to refresh the information in the screen.

Wireless Configuration

This configuration interface is for any nLight ECLYPSE Wi-Fi Adapter connected to the **HOST** connector.

A hotspot creates a subnetwork. As a result, any connected BACnet device will not be able to discover BACnet devices on any other LAN subnetwork.

Figure 42: The Wi-Fi network operating modes: Hotspot, Access-Point, or Client.



Mode
Hotspot

The Wireless connection parameters can be set as follows.

Item	Description
On / Off On Off	This enables/disables the controller's wireless features.
Wireless Mode	Select the Wi-Fi network operating mode: Hotspot, Access-Point, or Client. • **Hotspot**:This creates a Wi-Fi hot spot with a router. See *Setting up a Wi-Fi Hotspot Wireless Network* for how to configure this mode. • **Access-Point**:This creates a Wi-Fi access point. See *Setting up a Wi-Fi Access Point Wireless Network* for how to config- ure this mode. • **Client**: this connects the controller as a client of a Wi-Fi access point. See *Setting up a Wi-Fi Client Wireless Network* for how to configure this mode. See also *nLight ECLYPSE Wi-Fi Adapter Connection Modes.*
Network Name	The network name is the Service Set IDentification (SSID) for a Wi-Fi hotspot. This parameter is case sensitive. When this controller's active mode is configured as a: • For **Hotspot**: set a descriptive network name that other wireless clients will use to find this hotspot. • For **Client**: select an available hotspot from the lists of access point connections that are within range. Click the Wi-fi icon 📶 to select an available Wi-Fi network from thelistof access points that are within range.

Item	Description
Encryption	Set the encryption method to be used by the Wi-Fi network: • Open: this option should be avoided as it does not provide any wireless security which allows any wireless client to access the LAN. • WPA2: select the Wi-Fi Protected Access II option to secure the Wi-Fi network with a password.
Password	When encryption is used, set the password to access the Wi-Fi network as a client or the password other clients will use to access this hotspot. Passwords should be a long series of random alphanumeric characters and symbols that are hard to guess. This parameter is case sensitive.
👁̸ 👁	Click to show or hide the password.
IP Address	This is the IP address for a Hotspot (or gateway address that wireless clients will connect to). Ensure that this address is: • Not in the range of IP address set by **First Address** and **Last Address**. • Not the same as the **IP address** set under IP Configuration for the wired network.
Subnet Mask	The hotspot's subnetwork mask. See *About the Subnetwork Mask* .
First Address Last Address	This defines the range of IP addresses to be made available for Hotspot clients to use. The narrower the range, the fewer hotspot clients will be able to connect due to the lack of available IP addresses. For example, a range where First Address = 192.168.0.22 and Last Address = 192.168.0.26 will allow a maximum of 5 clients to connect to the hotspot on a first-to-connect basis.
Advanced	When a Hotspot or Access-point is configured,this sets the channel width and number the hot spot is to use. The wireless mode can also be set. See below.
ChannelNumber	This sets the center frequency of the transmission. If there are other Wi-Fi networks are nearby, configure each Wi-Fi network to use different channel numbers to reduce interference and network drop-outs. **Note**: The range of available channels may vary from country to country.
Wi-FiMode	This sets the wireless mode (wireless G or wireless N). Wireless N mode is backwards compatiblewith wireless GandB.Wireless Gmodeisback- wards compatible with wireless .B
SSIDHidden	For a Client hot spot,hide or show the Service Set IDentification(SSID).

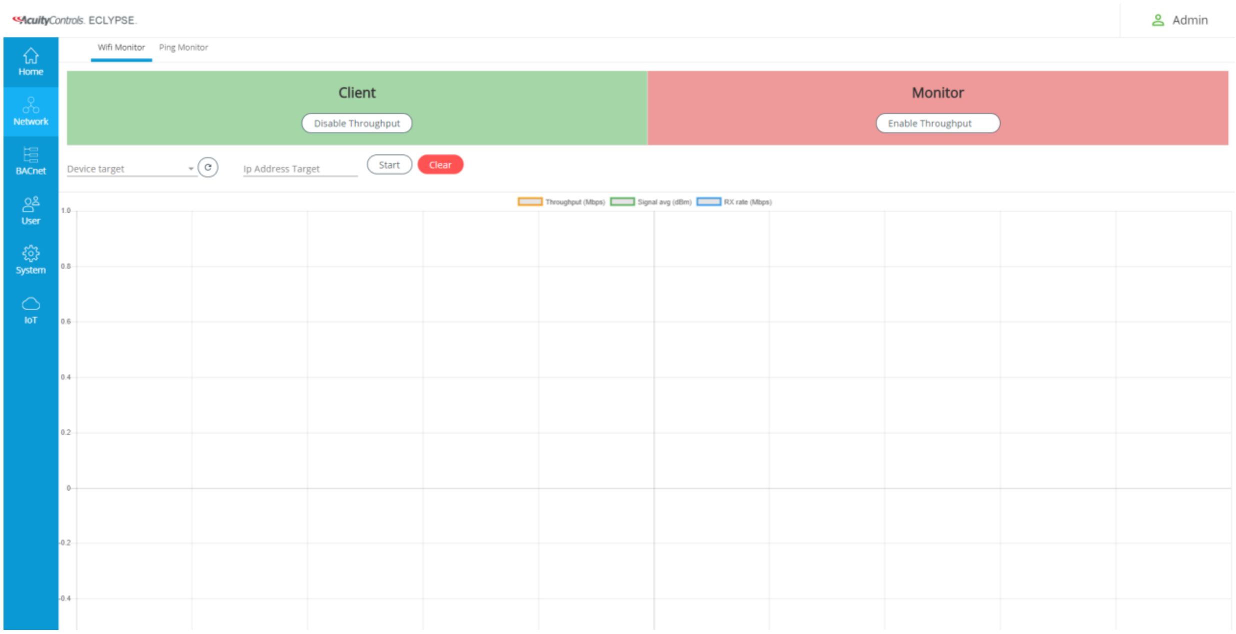
Item	Description
↻	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

Network Diagnostics

The **Diagnostic** menu provides a number of tools to diagnose network connectivity issues between controllers.

- **Wi-Fi Monitor**: shows the current performance of a Wi-Fi connection with another controller.
- **Ping Monitor**: shows the round trip time it takes for a ping packet to go to an IP address and come back.

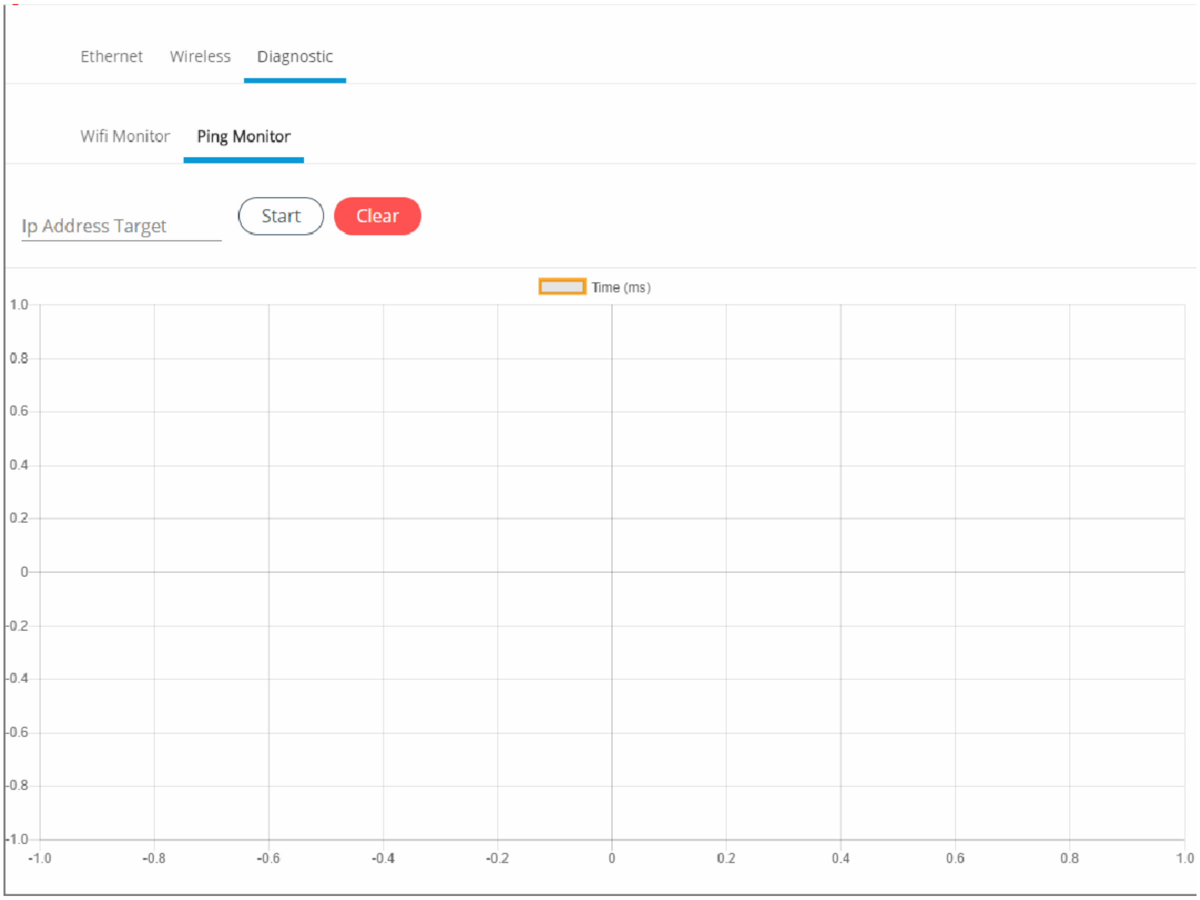
Figure 43: Network Diagnostics: Wi-Fi Monitor



Item	Description
DisableThroughput	This disables the Wi-Fi Monitoring throughput client service.For Wi-Fi monitor to work, this must be started.
EnableThroughput	This activates the Wi-Fi Monitoring throughput client service.For Wi-Fi monitor to work, this must be started.

Item	**Description**
Device Target	Select the corresponding controller’s MAC address in the **Device Target** list.
Ip Address Target	Enter the corresponding controller’s IP address for its Wi-Fi interface in **Ip Address Target**.
↻	Click to refresh the information in the **Device Target** list.
Start	Starts graphing the monitored data.
Clear	Clears the graph.
Throughput (Mbps)	The transmit datarate to the target.
Signal avg (dBm)	The current average receive signal strength. **Note**: Signal strength is measured in negative units where the stronger the signal, the closer it is to zero. A weaker signal strength will have a more negative number. For example, a receive signal strength of -35 dBm is much stronger than a receive signal strength of -70 dBm.
RX rate (Mbps)	The receive datarate from the target.

Figure 44: Network Diagnostics - Ping Monitor



Item	Description
Ip AddressTarget	Enter the corresponding controller’s IP address for its Wi-Fi interface in **Ip AddressTarget**.
Start	Starts graphing the monitored data.
Clear	Clears the graph.

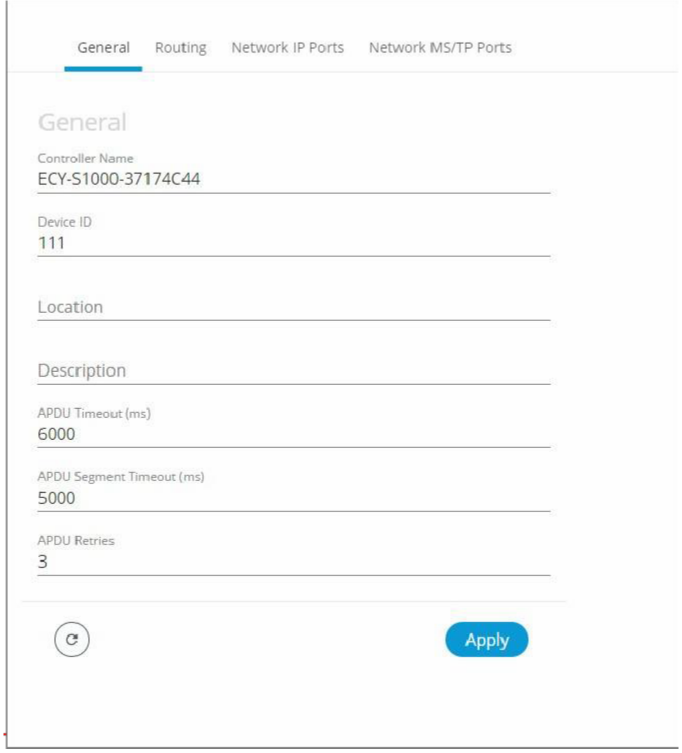
BACnet Settings

This is where the BACnet interface parameters are set.

General

This sets the controller’s BACnet network parameters.

Figure 45: General BACnet Settings



Controller Name
ECY-S1000-37174C44

Device ID
111

Location

Description

APDU Timeout (ms)
6000

APDU Segment Timeout (ms)
5000

APDU Retries
3

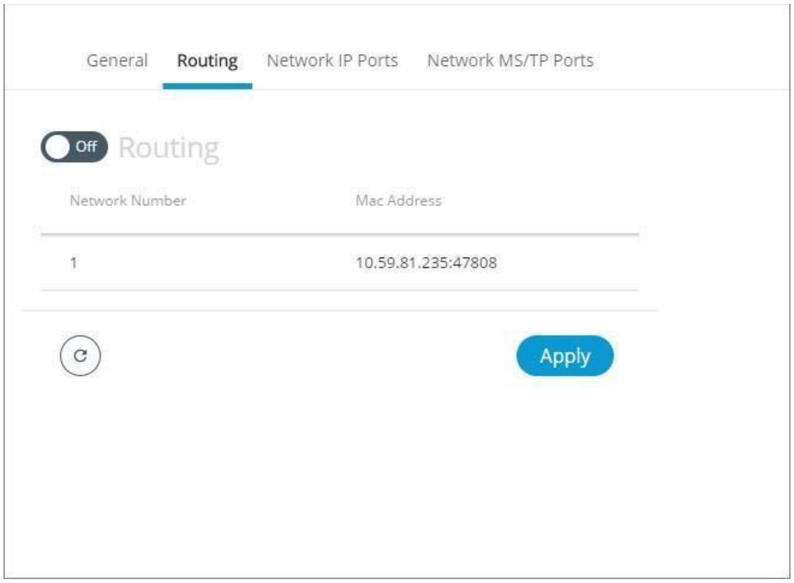
Item	Description
Controller Name	Set a descriptive name by which this controller will be known to other BACnet objects.
Device ID	Each controller on a BACnet intra-network (the entire BACnet BAS network) must have a unique Device ID. Refer to the NetworkGuide for more information.
Location	The current controller’s physical location. This is exposed on the BACnet network as a device object property.
Description	A description of the controller’s function. This is exposed on the BACnet network as a device object property.
APDU Timeout (ms)	The maximum amount of time the controller will wait for an acknowledgment response following a confirmed request sent to a BACnet device before re-sending the request again or moving onto the next request. This property is exposed on the BACnet network as a device object property.

Item	Description
APDU Segment Timeout(ms)	The maximum amount of time the controller will wait for an acknowledgment response following a confirmed segmented request sent to a BACnet device before re-sending the segmented request again or moving onto the next request. This property is exposed on the BACnet network as a device object property.
APDU Retries	This sets the number of times to retry a confirmed request when no acknowledgment response has been received. This property is exposed on the BACnet network as a device object property.
↻	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

Routing

This enables the routing of BACnet packets between BACnet MS/TP controllers connected to the nLight ECLYPSE Connected System Controller’s RS-485 port and BACnet/IP controllers connected to the nLight ECLYPSE Connected System Controller’s Ethernet Switch ports. For example, routing must be enabled for EC-Net to discover the BACnet MS/TP controllers connected to the nLight ECLYPSE Connected System Controller’s RS-485 port.

Figure 46: BACnet Routing Configuration



Off Routing

Network Number	Mac Address
1	10.59.81.235:47808

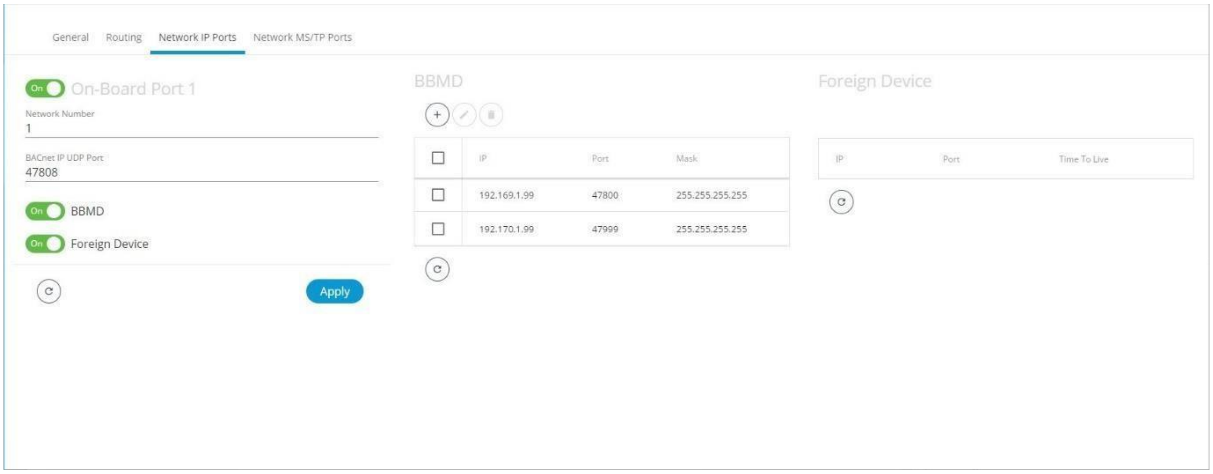
Item	Description
On Off	This enables/disables the routing of BACnet packets between BACnet MS/TP controllers connected to the nLight ECLYPSE ConnectedSystem Controller’s RS-485 port and BACnet/IP controllers connected to the nLight ECLYPSE Connected System Controller’s EthernetSwitchports.

Item	Description
Network Number	A network number identifies a LAN for routing purposes.All controllers with the same network number are members of the same logical BACnet network.See*Device Addressing*.
Mac Address	The device Mac address.
↻	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes.

Network IP Ports

This sets the IP network configuration parameters (on-boardport)aswellas the BACnet Broadcast Management Device (BBMD) and Foreign Device for intranetwork connectivity.

Figure 47: BACnet IP Configuration - Network IP Ports



On On-Board Port 1

Network Number: 1

BACnet IP UDP Port: 47808

On BBMD

On Foreign Device

□	IP	Port	Mask
□	192.169.1.99	47800	255.255.255.255
□	192.170.1.99	47999	255.255.255.255

IP	Port	Time To Live

On-BoardPort

Item	Description
On/Off On Off	This enables/disables the routing of BACnet packets between BACnet MS/TP controllers connected to the nLight ECLYPSE Connected System Controller’s RS-485 port and BACnet/IP controllers connected to the nLight ECLYPSE Connected System Controller’s Ethernet Switch ports.
Network Number	A network number identifies a LAN for routing purposes. All controllers with the same network number are members of the same logical BACnet network. See *Device Addressing.*
BACnet IP UDP Port	This is the standard BACnet/IP port number (UDP 47808) used by BACnet devices to communicate.

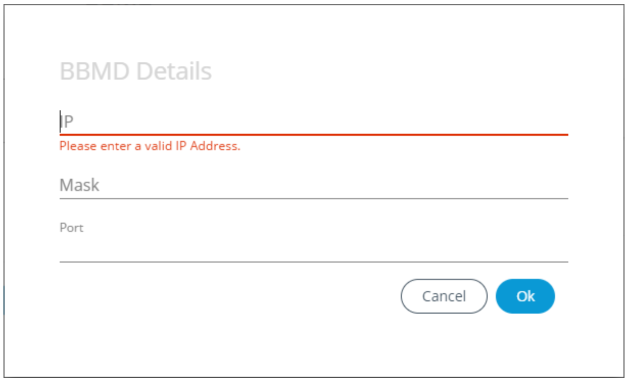
Item	Description
Enable BBMD	BBMD allows broadcast message to pass through a router. See *BBMD Settings.* To enable this feature, set **Enable BBMD** on only one device on each subnet.
Enable Foreign Devices	Foreign Device Registration allows a BACnet/IP device to send broadcast messages to a device with BBMD enabled. See *Foreign Device Settings.* To enable this feature, set **Enable Foreign Devices** on only one device on each subnet.
↻	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

BBMD Settings

BACnet/IP devices send broadcast discovery messages such as “Who-Is” as a means to discover other BACnet devices on the network. However, when there are two or more BACnet/IP subnetworks, broadcast messages do not pass through network routers that separate these subnetworks.

BBMD allows broadcast message to pass through a router: on each subnet, a single device has BBMD enabled. Each BBMD device ensures BACnet/IP connectivity between subnets by forwarding broadcast messages found on its subnetwork to each other, and then onto the local subnetwork as a broadcast message.

In the BBMD table, add the BBMD-enabled controllers located on other subnetworks.

Item	Description
⊕	Add another subnetwork's BBMD to this controller's a Broadcast Distribution Table. To add a BBMD: **1.** Click ⊕. *Figure 48: Adding a BBMD*  BBMD Details IP Please enter a valid IP Address. Mask Port Cancel Ok **2.** In the **IP** field, enter IP address of the BBMD located on the other subnetwork. **3.** In the **Mask** field, enter the subnetworkmask for the other subnetwork. **4.** In the **Port** field, enter the port number for the BACnet service of the BBMD located on the other subnetwork. **5.** Click **OK**.
✎	Edit a BBMD's information. This icon is displayed only when one or more BBMD is selected ☑ from thelist.
🗑	Remove a BBMD from this controller's Broadcast Distribution Table. This icon is displayed only when one or more BBMD is selected ☑ from the list.
⟳	Click to refresh the information in the list.

Foreign Device Settings

Some BACnet/IP devices also support a feature called Foreign Device Registration (FDR). FDR allows a BACnet/IP device to send broadcast messages to a device with BBMD enabled. The BBMD-enabled device will then forward these broadcast messages to all other BBMDs and onto all other FDR devices. If a subnet has only FDR supported devices then it does not need a local BBMD. These devices can register directly with a BBMD on another subnetwork.

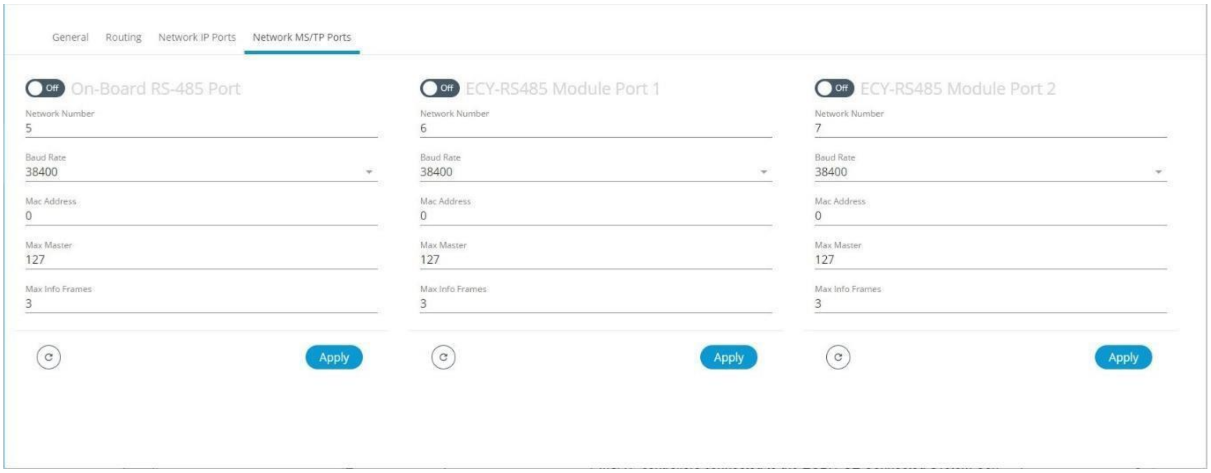
Item	Description
Ip	The IP address of a controller (foreign device) located on another subnetwork.
Mask	The port number for the BACnet service of the controller located on the other subnetwork.
Port	This is the delay after which the foreign device is forgotten.
↻	Click to refresh the information in the list.

Network MS/TP Ports

Some controller models support up to three RS-485 ports. Some controllers only support Modbus RTU on its RS-485 port. See the controller's datasheet for more information.

BACnet MS/TP and Modbus RTU communications are made by connecting directly to separate RS-485 ports. **On-board RS-485 Port** is the controller's onboard RS-485 port. When an NECY-RS485 expansion module is attached to the controller, **NECY-RS485 Module Port 1** is port #1 and **NECY-RS485 Module Port 2** is port #2 on that module. The following network configuration parame- ters are for an RS-485 port that is used to communicate with BACnet MS/TP controllers.

Figure 49: Network MS/TP Ports



General | Routing | Network IP Ports | Network MS/TP Ports

Off On-Board RS-485 Port
Network Number: 5
Baud Rate: 38400
Mac Address: 0
Max Master: 127
Max Info Frames: 3

Off ECY-RS485 Module Port 1
Network Number: 6
Baud Rate: 38400
Mac Address: 0
Max Master: 127
Max Info Frames: 3

Off ECY-RS485 Module Port 2
Network Number: 7
Baud Rate: 38400
Mac Address: 0
Max Master: 127
Max Info Frames: 3

Item	Description
On/Off On Off	This enables/disables the controller's BACnet MS/TP connection. If the controller has been configured to use Modbus RTU, this option cannot be enabled. First disable Modbus RTU in EC-*gfx* Program.

Item	**Description**
Network Number	A network number identifies a LAN for routing purposes. All controllers with the same network number are members of the same logical BACnet network. See *Device Addressing.*
Baud Rate	The recommended baud rate setting is 38 400. See *Baud Rate.*
Mac Address	The NECY series controller’s MAC Address on the BACnet MS/TP Data Bus.
Max Master	When commissioning a BACnet MS/TP Data Bus, it is useful to start with the **Max Master** set to 127 so as to be able to discover all devices connected to the data bus. Then, once all devices have been discovered and the MAC Addressing is finalized by eliminating any gaps in the address range, set the **Max Master** (the highest MAC Address) to the highest Master device’s MAC Address number to optimize the efficiency of the data bus. See *Setting the Max Master and Max Info Frames*.
Max Info Frames	For the NECY series controller, this should be set to 20. See *Setting the Max Master and Max Info Frames.*
↻	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

User Management

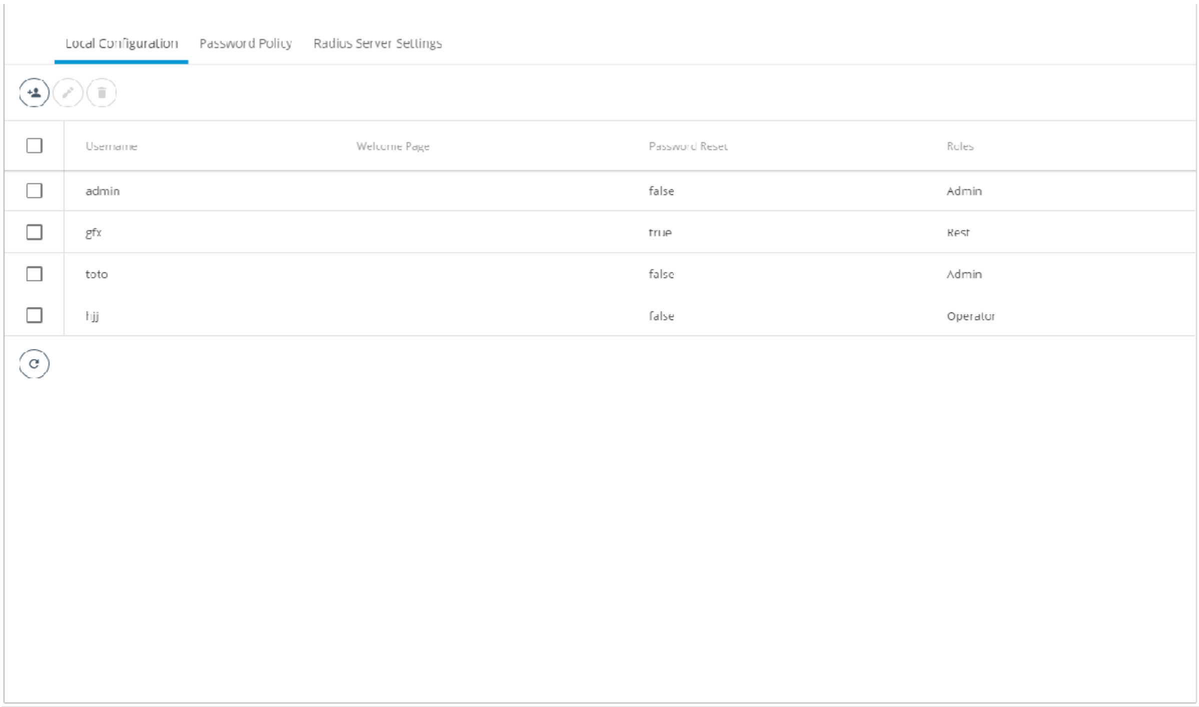
User management is the control of who can access the controller by enforcing the authentication credentials users need to access the controller. User management can either be locally managed or remotely managed. If there is more than one nLight ECLYPSE controller on the network, it is best to centralize access management .

User management can also set the welcome page a user will land on when they connect to the controller.

Local Configuration

User access to this controller and to other controllers that are using this controller as their RADIUS server are managed by adding them to the **Local User Management** shown below.

Figure 50: Local Configuration User Management



□	Username	Welcome Page	Password Reset	Roles
□	admin		false	Admin
□	gfx		true	Rest
□	toto		false	Admin
□	hjj		false	Operator

Item	Description
Add	Add a new user to user management. See *Adding a User.* These users will have login access to the controller. It is important to cre- ate new user accounts with strong passwords to protect the controller from unauthorized access. See *Securing an nLight ECLYPSE Controller.*

Item	Description
Edit	Edit a user’s information. When editing user information, the user password is not shown therefore the field appears empty. You can leave the password as is or assign a new one
Remove	Remove a user from user management. Remove the factory default admin account as this is a commonly known security breech (only the password for this user account needs to be compromised). Proceed as follows. **1.** Create a new user account with administrative rights for yourself. **2.** Logout of the **admin** account and then login to the user account you have created. **3.** Remove the factory default **admin** account.

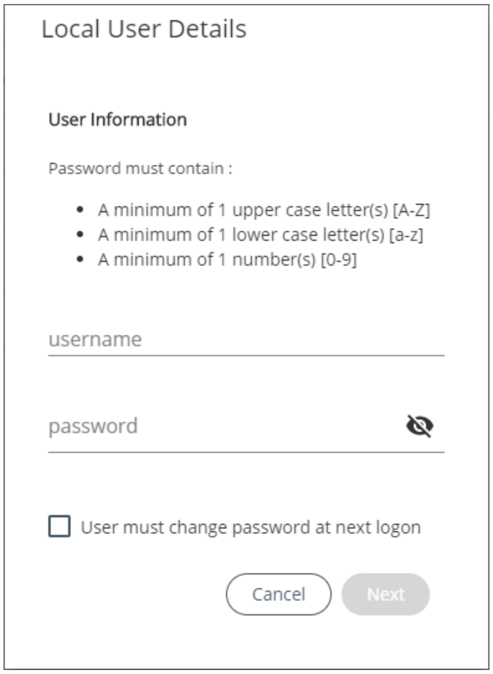
Adding a User

Adding a user creates a user profile that allows a person to login to the controller with a username / password combination and to have access to certain controller software interfaces. When this controller is used as a RADIUS server by other controllers, users connecting to those controllers will have access to those controllers as defined by their user profile.

User management can also set the welcome page a user will land on when they connect to the controller with the **Welcome Page** setting.

1. Click to add a new user or to edit an existing user. The **Local User Details** window is displayed.

Figure 51: Adding a User



Local User Details

User Information

Password must contain :

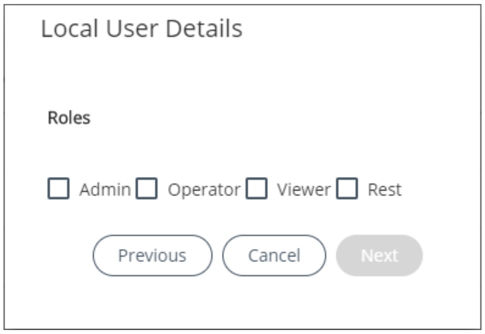
- A minimum of 1 upper case letter(s) [A-Z]
- A minimum of 1 lower case letter(s) [a-z]
- A minimum of 1 number(s) [0-9]

□ User must change password at next logon

2. Enter the information as shown below:

Item	Description
Username	The user’s login credential.
Password	The user’s password credential.
👁̸ 👁	Show/Hide the user’s password credential.
User must change password at next login	Select to force user to change their password at the next login.

3. Click **Next**.The **Roles** options are displayed.



Local User Details

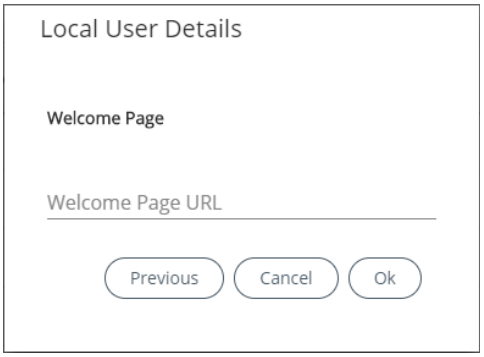
Roles

☐ Admin ☐ Operator ☐ Viewer ☐ Rest

4. Select the access levels the user will be able to use.Set one or more options according to the user’s role:

Admin	Allows user access to the ENVYSION studio and viewer. The user can also view and modify all configuration interface parameters and program the controller with EC-*gfx*Program.
Operator	Allows user access to the ENVYSION interface in viewing mode as well as gives partial access to the nLight ECLYPSE Web Configuration Interface. Certain configuration interface screens are unavailable such as User Management, Viewer Information, etc.
Viewer	Allows user access to the ENVYSION interface in Viewing mode. The user is not allowed to access the nLight ECLYPSE Web Configuration Interface.
Rest	Allows a user to program the controller with EC-*gfx*Program. This user does not have access to the nLight ECLYPSE Web Configuration Interface or ENVYSION.

5. Click **Next**.The **Welcome Page** screen is displayed where you can set the landing page that will be displayed to individual users when they login to the controller.



Local User Details

Welcome Page

Welcome Page URL

6. Enter the URL of the web page found after the controllers' IP address or hostname.This should be copied from your Web browser’s address bar when you have navigated to the target page.

   For example, the address for the user default web page is **HOSTNAME/nLightECLYPSE/envysion/viewer.html?proj=ENVYSION_PROJECT_NAME**or

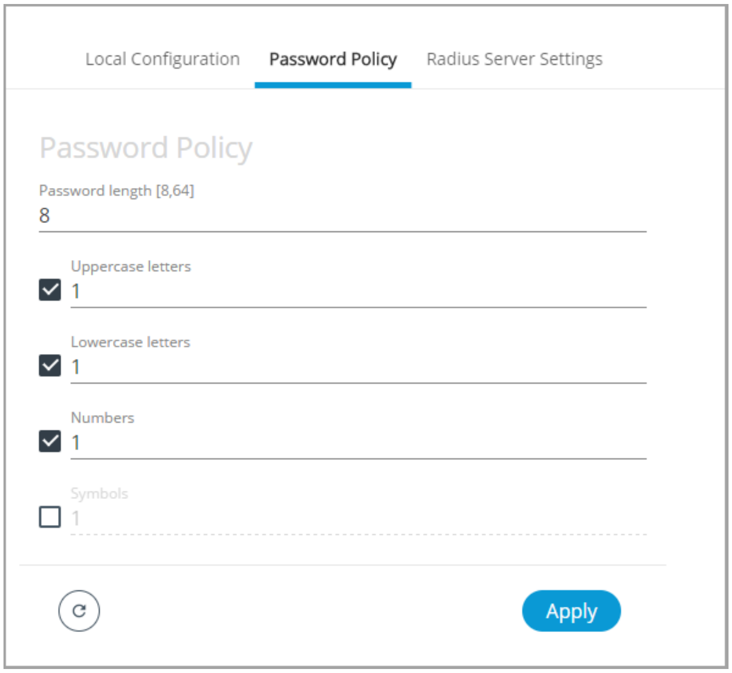
192.168.0.1/config/bacnet.html, remove the hostname or IPAddress so that theURLbecomes**/config/bacnet.html**.See*User Management.*

7. Click **OK**,and because authentication is required,enter your username and password.

Password Policy

The password policy sets the minimum requirements for a valid password to help prevent common password cracking techniques. By requiring long passwords with a well-rounded composition of elements (uppercase and lowercase letters, numbers, and symbols) makes the password harder to guess and makes a brute force attack less effective.

Select the **Password Policy** tab to display the password options:



Password Policy

Password length [8,64]
8

☑ Uppercase letters
1

☑ Lowercase letters
1

☑ Numbers
1

□ Symbols
1

Item	Description
Password length (>8)	The minimum password length. See also *FIPS 140-2 Mode* for password settings.
Uppercase letters	The minimum number of uppercase letters (A to Z) required to compose the password.
Lowercase letters	The minimum number of lowercase letters (a to z) required to compose the password.
Numbers	The minimum number of numbers (0 to 9) required to compose the password.

Item	Description
Symbols	The minimum number of symbols (for example, =, +, &, ^, $, etc.) required to compose the password.
↻	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

System Settings
CHAPTER 8

CONFIGURING THE nLight ECLYPSE WI-FI ADAPTER WIRELESS NETWORKS

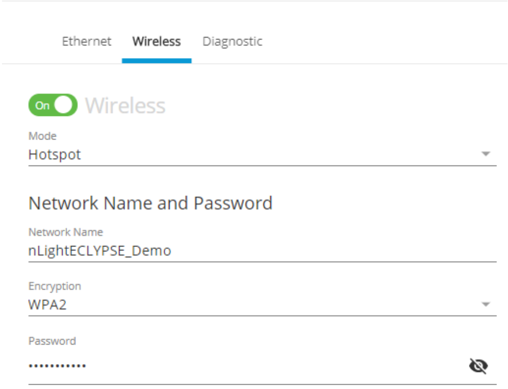
nLight ECLYPSE Wi-Fi Adapter supports a number of wireless network connection modes. This chapter describes how to configure a controller's wireless net- work. See also *nLight ECLYPSE Wi-Fi Adapter Connection Modes*.

Topics

Setting up a Wi-Fi Client Wireless Network

This connects the controller as a client of a Wi-Fi access point. See *Wi-Fi Client Connection Mode* for more information.

Figure 66: Client Wireless Network Settings



On Wireless

Mode
Hotspot

Network Name and Password

Network Name
nLightECLYPSE_Demo

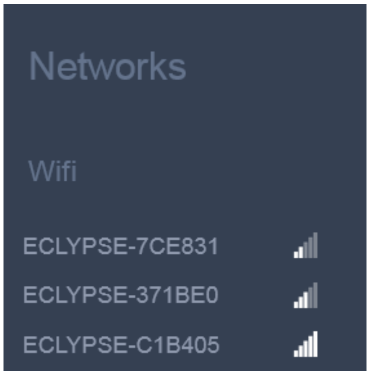
Encryption
WPA2

Password
•••••••••••

Configure the controller's nLight ECLYPSE Wi-Fi adapter mode as a Wi-Fi client as follows.

1. Set **On**.
2. Set the **Mode** to **Client**.
3. Click for ((•)) the controller to search for available access points that are within range. The access points are listed on the right.

Figure 67: List of Available Access Points to Pair With



Networks

Wifi

ECLYPSE-7CE831

ECLYPSE-371BE0

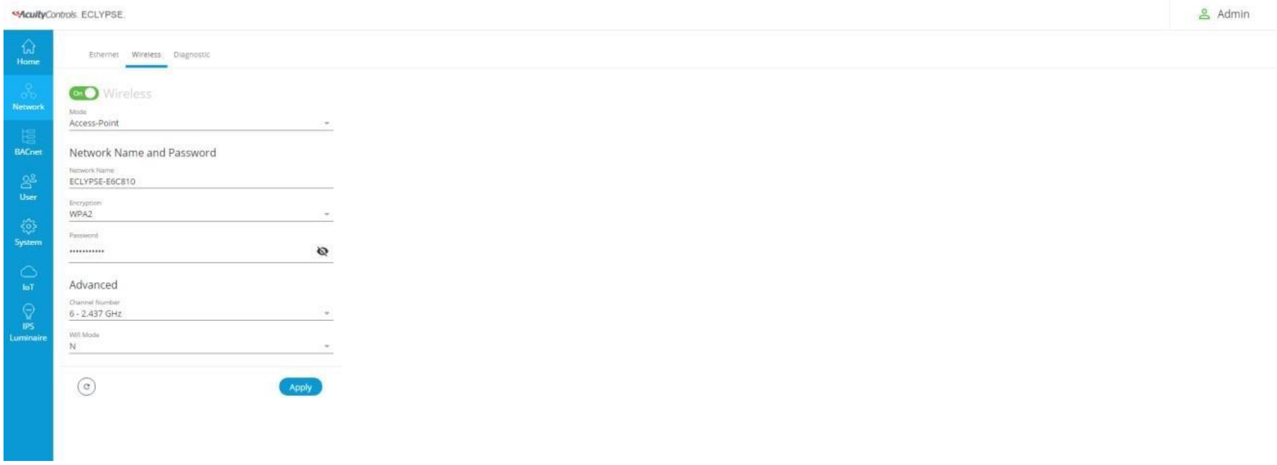
ECLYPSE-C1B405

4. Select an access point to pair with from the access point list. The **Encryption** mode is provided by the access point.
5. Set the access point's authentication password in
6. **Password**. This password is set in the access point's (or wireless router's) configuration.
7. Click **Apply**.

Setting up a Wi-Fi Access Point Wireless Network

This turns the controller into a Wi-Fi access point that other wireless clients can use to have network access. This access point operates off of the same subnetwork and has the same IP connectivity that the controller has with its wired network connection. For example, if the controller's wired connection is to a network that has an active DHCP server, access point clients can also use this DHCP server to automatically configure their IP connection parameters. See *Wi-Fi Access Point* for more information.

Figure 68: Access Point Wireless Network Settings



On Wireless

Mode
Access-Point

Network Name and Password

Network Name
ECLYPSE-E6C810

Encryption
WPA2

Password
•••••••••••

Advanced

Channel Number
6 - 2.437 GHz

Wifi Mode
N

Configure the controller's nLight ECLYPSE Wi-Fi adapter mode as a Wi-Fi access point as follows.

1. Under **Wireless Configuration**, set **Enabled**.
2. Set the **Active mode** to **Hotspot/AP**.
3. Set the name for this access point by which wireless clients will identify it in **Network Name**.
4. Set the encryption mode to be used by this access point in **Encryption**:
   - **None: this option should be avoided** as it does not provide any wireless security which allows any wireless client to access the LAN.
   - **WPA2**: select the Wi-Fi Protected Access II option to secure the Wi-Fi network with a password.
   - **WPA2 Enterprise**: Use this option if you are connecting to an enterprise network that has a working RADIUS authentication server. This RADIUS server provides user authentication.
5. Set the access point's authentication password in **Password.** This is the password wireless clients will need to know in order to connect to this access point.
6. Under **Hotspot Configuration**, disable **Enabled**.

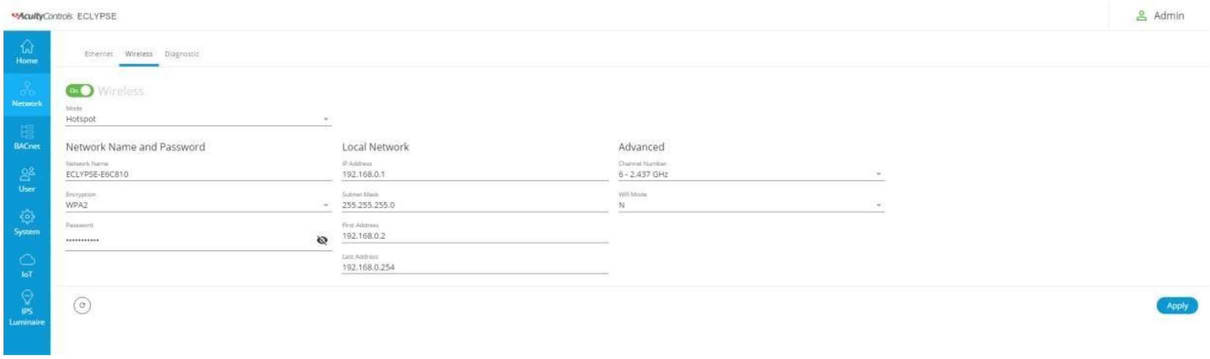
7. Under **Advanced**, set the **Channel Width**, **Channel Number**, and **Wi-Fi Mode**. See *BACnet Settings* for an explanation of theseparameters.
8. Click **Apply**.

Setting up a Wi-Fi Hotspot Wireless Network

This turns the controller into a Wi-Fi hotspot with a router. This puts the hotspot into a separate subnetwork with a DHCP server to provide IP addresses to any connected device. See *Wi-Fi Hotspot* for more information.

Wide area network (WAN) connectivity is through the wired connection. See *Network Address Translation / Firewall*. Though BACnet/IP uses IP protocol to communicate, this hotspot acts as an IP router; it does not for- ward broadcast messages which are important in BACnet to identify services that are available within the BACnet internetwork. See *BACnet/IP Broadcast Management Device Service (BBMD)*.

Figure 69: Hotspot Wireless Network Settings



Wireless: On

Mode: Hotspot

Network Name and Password

Network Name: ECLYPSE-E6C810

Encryption: WPA2

Password: ••••••••••••

Local Network

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

First Address: 192.168.0.2

Last Address: 192.168.0.254

Advanced

Channel Number: 6 - 2.437 GHz

WiFi Mode: N

Configure the controller’s nLight ECLYPSE Wi-Fi adapter mode as a Wi-Fi hotspot as follows.

1. Under **Wireless Configuration**, set**Enabled**.
2. Set the **Active mode** to**Hotspot/AP**.
3. Set the name for this access point by which wireless clients will identify it in **Network Name**.
4. Set the encryption mode to be used by this hotspot in **Encryption**:
   - **None**: **this option should be avoided** as it does not provide any wireless security which allows any wireless client to access the LAN.
   - **WPA2**: select the Wi-Fi Protected Access II option to secure the Wi-Fi network with a password.
   - **WPA2 Enterprise**: Use this option if you are connecting to an enterprise network that has a working RADIUS authentication server. This RADIUS server provides user authentication.
5. Set the hotspot’s authentication password in **Password**. This is the password wireless clients will need to know in order to connect to this hotspot.
6. Under **Hotspot Configuration**, set**Enabled**.

7. Set the hotspot’s IP address that wireless clients will connect to in **Ip Address**. Ensure that this address is:

    - Not in the range of IP address set by **First Address** and **Last Address**.
    - Not the same as the **IP address** set under IP Configuration for the wired network.

8. Set the hotspot’s subnet mask in **Subnet Mask**. See *About the Subnetwork Mask*.

9. Set the hotspot’s addressing range in **First Address** and **Last Address**. This defines the range of IP addresses to be made available for hotspot clients to use. The narrower the range, the fewer hotspot clients will be able to connect due to the lack of available IP addresses. For example, a range where First Address = 192.168.0.22 and Last Address = 192.168.0.26 will allow a maximum of 5 clients to connect to the hotspot on a first-to-connect basis.

10. Under **Advanced**, set the **Channel Width**, **Channel Number**, and **Wi-Fi Mode**. See *BACnet Settings* for an explanation of these parameters.

11. Click **Apply**.

CHAPTER 9

SECURING AN nLight ECLYPSE CONTROLLER

This chapter describes how to harden an nLight ECLYPSE controller from unauthorized access and use.

Topics

Introduction

This chapter describes how to implement best security practices for nLight ECLYPSE controllers. Security is built up layer upon layer to make the system more resistant to attacks. This involves taking simple but effective steps to implement built-in security features.

Passwords

A username / password combination (or credentials) authenticates a user’s access rights to a controller. If an attacker gains access to a user’s password, the attacker has access to carry out any action on the controller that is allowed by that user’s permissions.

Change the Default Platform Credentials

At the first connection to an nLight ECLYPSE Controller you will be forced to change the password to a strong password for the admin account to protect access to the controller.

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. Remove the factory default admin account as this is a commonly known security breach (only the password for this user account needs to be compromised). The username / password can be changed in *User Management* and see also *Supported RADIUS Server Architectures.*

Use Strong Passwords

Passwords should be hard to guess. Avoid birth dates and common keyboard key sequences. A password should be composed of a random combination of 8 or more uppercase and lowercase letters, numbers, and special characters.

If FIPS 140-2 mode is enabled, password must be a random combination of 14 or more uppercase and lowercase letters, numbers, and special characters. The controller will reset to a default username and password when FIPS 140-2 is enabled, and the user will then be prompted to reset both. See *FIPS 140-2 Mode.*

Do not allow a browser to remember a user’s login credentials

When logging into an nLight ECLYPSE controller with certain browsers, the browser asks to remember a user’s login credentials. When this option is set, the next time the user logs in, the credentials will automatically be filled in. While this is convenient, anyone with access to the computer can login using those cre- dentials. Do not set this option for administrator accounts or when accessing an account from an unsecure computer.

Account Management and Permissions

User accounts must be properly managed to make it harder for an attacker to compromise security, and to make it easier to detect that an attack has occurred. To set user account parameters, see *User Management.*

FIPS 140-2 Mode

Enabling FIPS 140-2 mode has an effect on account management and permissions. Once FIPS 140-2 mode is enabled, several controller settings are reset. Therefore, it is best to enable FIPS 140-2 mode before creating accounts and assigning permissions. See *FIPS 140-2 Mode.*

Use a Different Account for Each User

Each user account should represent an individual user. Multiple users or user groups should not share an account.

Suspending an account shuts-off a single user’s access to the controller – it does not disrupt many users.

Permissions can be tailored to the needs of each user. A shared account may have more permissions than all users should have.

A shared account has a shared password which is more likely to be leaked.

It is harder to implement password expiration requirements.

Use Unique Service Type Accounts for Each Project

System integrators should use different credentials for each job they do. Should an attacker gain access to one system, they cannot readily access all systems installed by the same system integrator.

Disable Known Accounts When Possible

Create a new user admin account with new credentials then delete the default admin account. It is easier to attack the default admin account when an attacker only has to guess the password.

Assign the Minimum Required Permissions

When creating a new user account, give that account only the minimum rights to access or modify the system needed for that user.

Use Minimum Possible Number of Admin Users

A compromised admin account can be disastrous as it allows complete access to everything. Only give a user admin privileges only when absolutely necessary.

HTTPS Certificates

HTTPS is a protocol which encrypts HTTP requests and their responses. This ensures that if someone were able tocompromise the network, theywould notbe able to listen in or tamper with the communications.

Make sure that HTTPS is enabled.For more information on how to enable HTTPS,see*Web Server Access.*

Certificates

Generate and install a signed SSL certificate. Refer to *Web Server Access* for information on how to import a custom certificate.

Additional Measures

Update the nLight ECLYPSE Controller’s Firmwareto the Latest Release

Always keep the nLight ECLYPSE controller’s firmware up-to-date. The most recent firmware has the latest bug fixes and stability enhancements.

External Factors

Install nLight ECLYPSE Controllersin a Secure Location

Ensure that the nLight ECLYPSE Controller is installed in a physically secure loca- tion, under lock and key. Through physical access, an attacker can take over the controller to do with it what theyplease.

For example, the reset button can be used to reset the controller to its factory default settings. If FIPS 140-2 mode has been enabled on the controller, resetting a controller to its factory default settings will turn FIPS 140-2 mode off.

Make Sure that nLight ECLYPSE Controllers Are Behind a VPN

For off-site connections, ensure that users access the controllers through a Virtual Private Network (VPN). This helps to prevent an attack through eaves-dropping on the communications channel to steal user credentials.

CHAPTER 10

BACnet MS/TP Communication Data Bus Fundamentals

This chapter describes the BACnet MS/TP Communications Data Bus operating principles.

Topics

BACnet MS/TP Data Transmission Essentials

Certain nLight ECLYPSE controller models support BACnet MS/TP to BACnet/IP routing according to the controller model purchased. See the Controller’s datasheet for more information. To enable BACnet MS/TP to BACnet/IP rout- ing, see *Routing.*

The BACnet MS/TP or Modbus RTU network option is selected in the controller’s web interface. BACnet MS/TP and Modbus RTU communications are made by connecting directly to separate RS-485 ports. The Connected System Controller integrates up to three RS-485 ports when equipped with one NECY-RS485 extension module allowing the controller to support more than one trunk or communication protocol at a time. When the NECY Series Control- ler is configured for BACnet MS/TP, values from the connected BACnet MS/ TP controllers can be used in ENVYSION graphics hosted on the NECY Series Controller. Furthermore, the NECY Series Controller acts as a BACnet/IP to BACnet MS/TP bridge that allows BACnet objects to be shared among BAC- net intra-networks through BBMD. See *BACnet/IP Broadcast Management Device Service (BBMD).*

The BACnet MS/TP data bus protocol is part of the BACnet® ANSI/ ASHRAE™ Standard 135-2008 that uses the EIA-485 (RS-485) physical layer standard for data transmission (herein called the data bus). Multiple data buses can be logically tied together as each BACnet MS/TP data bus is assigned a unique Network Instance that distinguishes it from other data buses in the BACnet MS/TP Local Area Network (LAN).

EIA-485 is a standard that defines the electrical characteristics of the receivers and drivers to be used to transmit data in a differential (balanced) multipoint data bus that provides high noise immunity with relatively long cable lengths which makes it ideal for use in industrial environments. The transmission medium is inexpensive and readily-available twisted pair shielded cable.

While there are many possible LAN topologies for an EIA-485 data bus, only devices that are daisy-chained together are allowed with BACnet MS/TP (see *Figure 74*). A spur is only permitted when it is connected to the data bus through a repeater (see *Using Repeaters to Extend the Data Bus.)*

End-of-line (EOL) terminations are critical to error-free EIA-485 data bus operation. The impedance of the cable used for the data bus should be equal to the value of the EOL termination resistors (typically 120 ohms). Cable impedance is usually specified by the cable manufacturer.

BACnet MS/TP data bus is polarity sensitive

The polarity of all devices that are connected to the two-wire BACnet MS/TP data bus must be respected. The markings to identify the polarity can vary by manufacturer. The following table summarizes the most common identification labels for BACnet MS/TP data bus polarity.

Table 4: Common Identification Labels for BACnet MS/TP Data Bus Polarity for Distech Controls' Products

Acuity Controls and Distech Controls Product	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
ECB Series Controllers	NET –	NET +	24V COM
ECB-PTU Series Line-Powered Controllers	NET –	NET +	COM
ECLYPSE Series Controllers	NET –	NET +	S
Thermostat	–	+	Ref
Repeater	Data– Data1–	Data+ Data1+	N/A
BACnet/IP to MS/TP Adapter	RT–	RT+	COM
BACnet/IP to MS/TP Router	–	+	SC

⚠ Except for an ECB-PTU Line-Powered Controllers and NECY Series Controllers, never connect the shield of the BACnet MS/TP data bus to the Reference terminal. See *Data Bus Shield Grounding Requirements* for moreinformation.

Table 5: Common Identification Labels for BACnet MS/TP Data Bus Polarity for other Manufacturers

Device Manufacturer	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
Common identification labels for BACnet MS/TP data bus polarity by other Manufacturers	B	A	SC
	–	+	G
	TxD–/RxD–	TxD+/RxD+	GND
	U–	U+	COM
	RT–	RT+	REF
	Sig–	Sig+	S
	Data–	Data+	

⚠ When interfacing with BACnet MS/TP devices from other manufacturers, refer to the documentation provided with the device to correctly wire the device.

Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate

The following technical parameters limit the number of devices on a BACnet MS/TP Data Bus Segment.

- The BACnet MS/TP Data Bus Segment has a hard limit on the number of devices that can communicate due to the device addressing scheme (the MAC Address Range for BACnet MS/TP Devices). See *Data Bus Segment MAC Address Range for BACnet MS/TP Devices.*
- Each device presents an electrical load on the BACnet MS/TP Data Bus Segment. This is called *device loading*. The number of devices that can be connected to a BACnet MS/TP Data Bus Segment is limited by the loading of each device. See *Device Loading.*
- Choosing a low baud rate can cause BACnet MS/TP Data Bus congestion that can limit the amount of data that can be efficiently exchanged between devices connected to the BACnet MS/TP Data Bus. For example, at 9600 baud, the maximum number of devices is reduced to 25 due to the increased time it takes for token passing between devices. The recommended baud rate is 38 400. See *BaudRate*.
- Distech Controls recommends that you connect no more than 50 of our ⅛ or ½-load devices on a single BACnet MS/TP Data Bus Segment when a baud rate of 19 200 or higher is used (preferably 38 400 baud). This is to ensure that the BACnet MS/TP Data Bus has enough bandwidth to efficiently communicate network variables betweencontrollers.

These parameters are described in greater detail below.

Data Bus Segment MAC Address Range for BACnet MS/TP Devices

The BACnet MS/TP data bus supports up 255 devices:

- Up to 128 devices (with device MAC addresses in the range of 0 to 127) that are BACnet MS/TP Masters (that can initiate communication).
- Up to 128 devices (with device MAC addresses in the range of 128 to 255) that are BACnet MS/TP Slaves (cannot initiate communication).

However, it is recommended that any given data bus segment have no more than 50 devices, when a baud rate of 19 200 or higher is used for the BACnet MS/TP Data Bus. A repeater counts as a device on each data bus segment to which it is connected.

All Distech Controls' devices are categorized as BACnet MS/TP Masters, that is, their device MAC address can be set in the range of 0 to 127 only.

Device Loading

Each device presents an electrical load on the BACnet MS/TP Data Bus Segment. This is called *device loading*. The use of full load devices limits the number of devices connected to a BACnet MS/TP Data Bus Segment to 32 devices. Distech Controls' BACnet MS/TP devices are ⅛-load devices and ½-load devices, which allows more devices to be connected to the BACnet MS/TP Data Bus Segment, as compared to full load devices.

Table 6: Device Loading

Manufacturer	**Device load on the attached BACnet MS/TP Data Bus**
Distech Controls' ECB and ECLYPSE Series controllers Distech Controls' ECB-PTU Series Line-Powered Controllers	⅛-load devices
Distech Controls' BACnet MS/TP Thermostats	½-load devices
Other manufacturers	Refer to their documentation

However, if a data bus segment is interoperating with devices that are full-load, ½-load, ¼-load, or ⅛-load, then the device that supports the fewest devices on the same data bus is the one that sets the limit for the maximum total number of devices for that data bus segment. For example, you plan to put on one data bus the following devices:

Table 7: Device Loading Example

Manufacturer	**Quantity of devices (example)**	**Equivalent full-load devices**	**Maximum devices supported by the manufacturer**
Distech Controls' devices (⅛-load devices)	8	1	128[1] Maximum 50 recommended
Distech Controls' BACnet MS/TP Thermostats (½-load devices)	14	7	64 Maximum 50 recommended
Manufacturer Y (full load devices)	26	26	32
Total Full-Load Devices		34	There are too many devices on the data bus. It is limited to a maximum of 32 devices by Manufacturer's Y devices.

[1] This is limited by the maximum number of master devices allowed on a BACnet MS/TP Data Bus.

The solution for the above example is to create two data bus segments connected together by a repeater and then split up the devices between the data bus segments, ensuring again that the maximum number of devices on each separate data bus is not exceeded. See *Using Repeaters to Extend the Data Bus.*

Baud Rate

Most devices will have a range of baud rate settings and possibly an AUTO setting that detects the baud rate of other devices transmitting on the data bus and adjusts the baud rate of the device accordingly. Typical baud rates are 9600, 19 200, 38 400, and 76 800. The baud rate setting determines the rate at which data is sent on the BACnet MS/TP data bus.

⚠ At 9600 baud, the maximum number of devices is reduced to 25 due to the increased time it takes for token passing between devices.

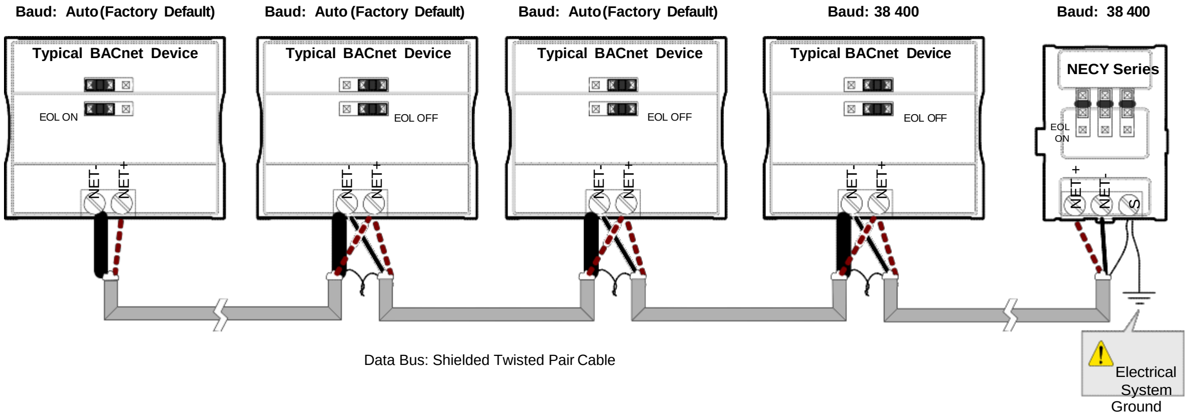
All devices on the data bus must be set to the same baud rate. Therefore, the chosen baud rate must be supported by all devices connected to the data bus.

The recommended baud rate for Distech Controls' devices is 38 400.

We recommend that you:

- Set the baud rate of two controllers on a BACnet MS/TP Data Bus Segment to the same baud rate to provide failoverprotection.
- For example, set the baud rate of the NECY Series Controller (if equipped) and one other controller to 38 400 baud. If the NECY Series Controller *becomes* unavailable and there is a power cycle, the ECB controller will set the baud rate for the BACnet MS/TP Data Bus.
- Set all other devices to automatically detect the baud rate, if this option is available.

Figure 70: Setting the Baud rate on two Controllers on a BACnet MS/TP Data Bus Segment for Failover Protection



To set the baud rate for:

- NECY Series Controllers, see *NetworkSettings.*
- ECB Series controllers, see the controller's hardware installation guide or the NetworkGuide.

Data Bus Physical Specifications and Cable Requirements

Cables composed of stranded conductors are preferred over solid conductors as stranded conductor cable better resist breakage during pulling operations. Distech Controls strongly recommends that the following data bus segment cable specifications be respected.

Table 8: BACnet MS/TP Data Bus Segment Physical Specifications and Cable Requirements

Parameter	Details
Media	Twisted pair, 24 AWG (see also *Metric Conversions for Wire Gauge*)
Shielding	Foil or braided shield
Shield grounding	The shield on each segment is connected to the electrical system ground at one point only; see *Data Bus Shield Grounding Requirements.*
Characteristic impedance	100-130 Ohms. The ideal is 100-120 Ohms.
Distributed capacitance between conductors	Less than 100 pF per meter (30 pF per foot). The ideal is less than 60 pF per meter (18 pF per foot).
Distributed capacitance between conductors and shield	Less than 200 pF per meter (60 pF per foot).
Maximum length per segment	1220 meters (4000 feet)
Data Rate	9600, 19 200, 38 400, and 76 800 baud
Polarity	Polarity sensitive
Multi-drop	Daisy-chain (no T-connections)
EOL terminations	120 ohms at each end of each segment
Data bus bias resistors	510 ohms per wire (max. of two sets per segment)

Shielded cable offers better overall electrical noise immunity than non-shielded cable. Unshielded cable or cable of a different gauge may provide acceptable performance for shorter data bus segments in environments with low ambient noise.

Table 9: Distech Controls Recommended Cable Types for BACnet MS/TP Data Buses

Cable Type	Part Number	O.D. (Ø)
300 meters (1000 feet), 24 AWG Stranded, Twisted Pair Shielded Cable – FT6, Rated for Plenum Applications	CB-BACN6BL1000	3.75mm (0.148 in.)

Distech Controls BACnet cable offers the best performance over the full range of baud rates, cable lengths, and number of connected devices. This is primarily due to lower conductor-to-conductor capacitance of this cable.

Data Bus Topology and EOL Terminations

Function of EOL Terminations

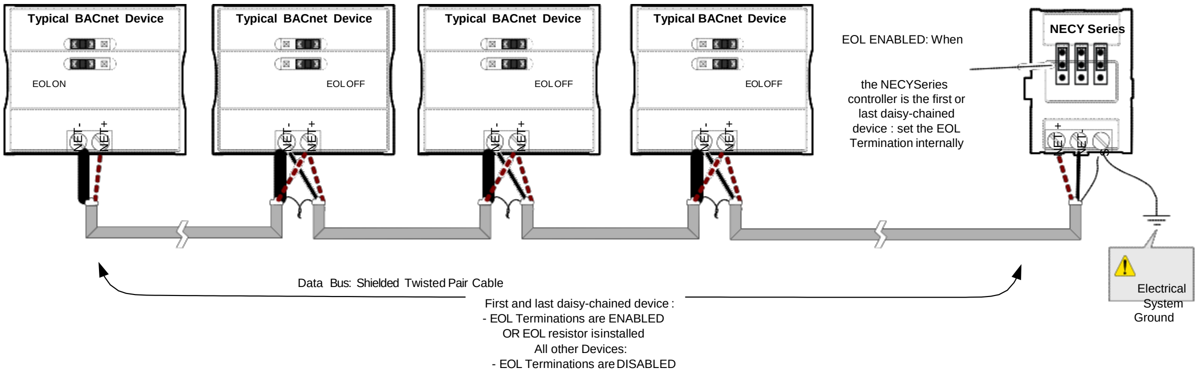
The first and last device on the data bus must have End-of-Line (EOL) termination resistors connected across the two data lines/wires of the twisted pair. These resistors serve the following purposes:

- EOL terminations dampen reflections on the data bus that result from fast-switching (high-speed rising and falling data edges) that otherwise would cause multiple data edges to be seen on the data bus with the ensuing data corruption that may result. The higher the baud rate a data bus is operating at, the more important that EOL terminations be properly implemented. Electrically, EOL terminations dampen reflections by matching the impedance to that of a typical twisted pair cable.
- EIA-485 data bus transmitters are tri-state devices. That is they can electrically transmit 1, 0, and an idle state. When the transmitter is in the idle state, it is effectively off-line or disconnected from the data bus. EOL terminations serve to bias (pull-down and pull-up) each data line/wire when the lines are not being driven by any device. When an un-driven data bus is properly biased by the EOL terminations to known voltages, this provides increased noise immunity on the data bus by reducing the likelihood that induced electrical noise on the data bus is interpreted as actual data.

When to Use EOL Terminations

EOL terminations should only be enabled / installed on the two devices located at either end of the data bus. All other devices must not have the EOL terminations enabled/installed.

Figure 71: EOL Terminations Must be Enabled at Both the First and Last Device on the Data Bus


Typical BACnet Device
EOL ON
NET -
NET +
Typical BACnet Device
EOL OFF
NET -
NET +
Typical BACnet Device
EOL OFF
NET -
NET +
Typical BACnet Device
EOL OFF
NET -
NET +
EOL ENABLED: When
the NECYSeries controller is the first or last daisy-chained device : set the EOL Termination internally
NECY Series
NET +
NET -
S
Electrical System Ground
Data Bus: Shielded Twisted Pair Cable
First and last daisy-chained device :
- EOL Terminations are ENABLED
OR EOL resistor isinstalled
All other Devices:
- EOL Terminations are DISABLED

Devices with built-in EOL terminations are factory-set with the EOL termination disabled by default.

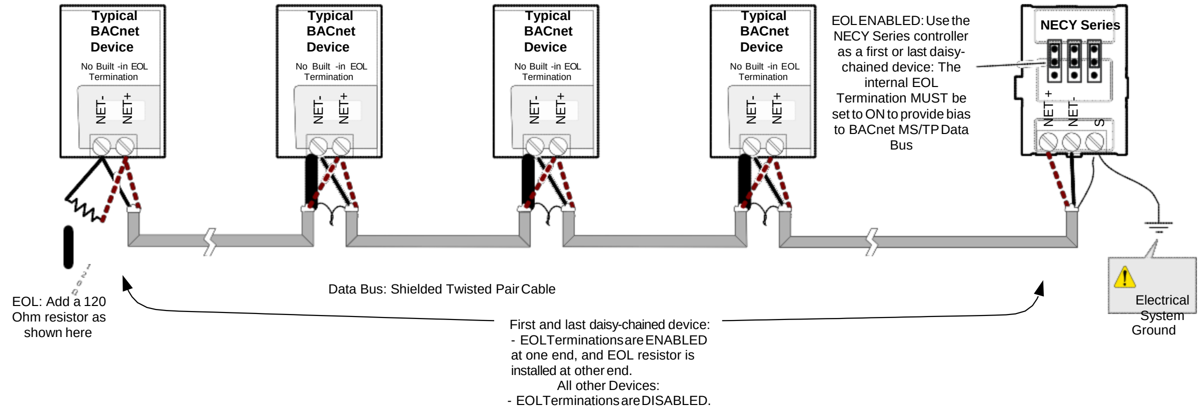
The *BACnet/IP to MS/TP Adapter* does not have EOL Termination (and BACnet MS/TP Data Bus biasing) capabilities to be used at the end of a BACnet MS/TP data bus. Instead, use the *BACnet/IP to MS/TP Router* for this application.

When to use EOL Terminations with BACnet MS/TP Thermostats

BACnet MS/TP thermostats support external EOL termination resistors only. When a BACnet MS/TP thermostat is the first or last daisy-chained device, add a 120 Ohm resistor across the – and + BACnet MS/TP data bus connections.

The BACnet MS/TP data bus must be biased. This bias can only be provided by built-in EOL termination resistors (ones set with jumpers or DIP switches – refer to the controller's Hardware Installation Guide for how to identify and set a controller's built-in EOL terminations). If a BACnet MS/TP data bus has a BACnet MS/TP thermostat at one end of the BACnet MS/TP data bus and an NECY Series Controller at the other end, you must set the built-in EOL termina- tion in the NECY Series Controller so that proper biasing is provided to the BACnet MS/TP data bus.

Figure 72: Typical EOL Terminations with BACnet MS/TP Thermostats with Biasing Provided by the NECY Series Controller's Built-in EOL Termination set to ON

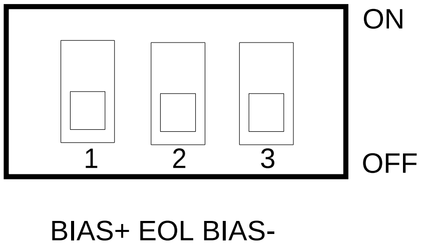


Typical BACnet Device
No Built -in EOL Termination
NET-
NET+
Typical BACnet Device
No Built -in EOL Termination
NET-
NET+
Typical BACnet Device
No Built -in EOL Termination
NET-
NET+
Typical BACnet Device
No Built -in EOL Termination
NET-
NET+
EOL ENABLED: Use the NECY Series controller as a first or last daisy-chained device: The internal EOL Termination MUST be set to ON to provide bias to BACnet MS/TP Data Bus
NECY Series
NET+
NET-
S
EOL: Add a 120 Ohm resistor as shown here
Data Bus: Shielded Twisted Pair Cable
First and last daisy-chained device:
- EOL Terminations are ENABLED at one end, and EOL resistor is installed at other end.
All other Devices:
- EOL Terminations are DISABLED.
Electrical System Ground

About Setting Built-in EOL Terminations

NECY Series Controllers have built-in EOL terminations. These Controllers use jumpers or DIP switches to enable the EOL resistors and biasing circuitry. These controllers have separate bias and EOL termination settings. This is useful in the following scenario: the NECY series controller is located in the middle of the data bus and either one or both controllers at the data bus ends do not have biasing or EOL terminations. In this situation, set the bias on the NECY series controller and set the EOL termination on the controllers at the end of the data bus. If a controller at the end of the data bus does not have a built-in EOL termination, then add a 120 Ohm resistor across the device's terminals as shown at the left side of *Figure 72*.

Figure 73: Typical nLight ECLYPSE Controller with Separate EOL Termination and Bias Configuration Settings



ECB-PTU Series Line-Powered Controllers use DIP switches (found alongside those DIP switches used to set the MAC address) to enable the build-in EOL resistors and biasing circuitry.

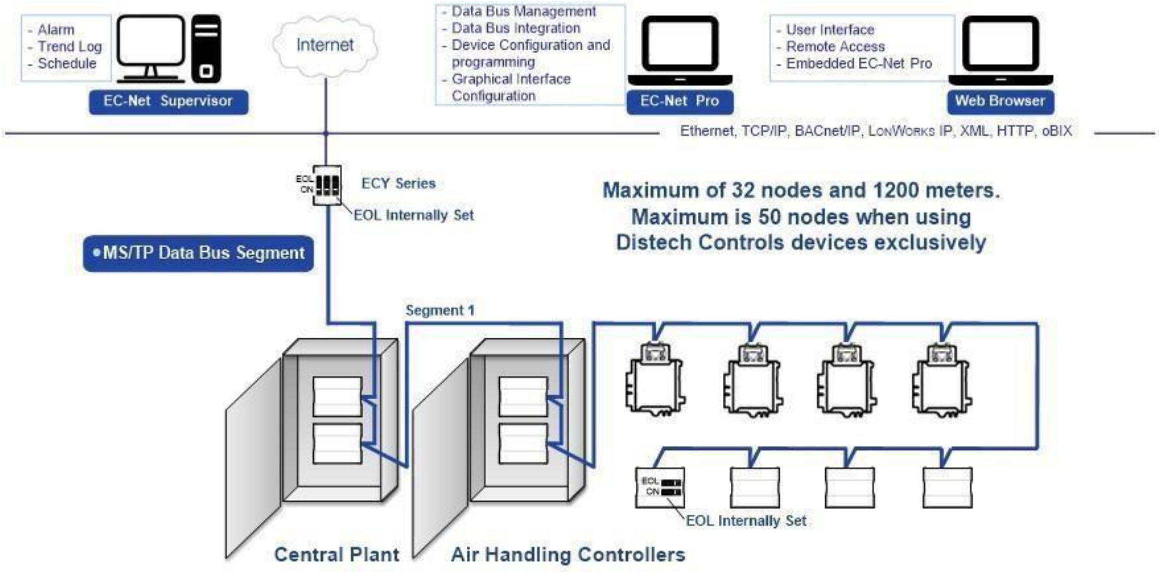
ECB Series 24V-Powered Controllers have built-in EOL terminations. These Controllers use jumpers to enable the EOL resistors and biasing circuitry.

Refer to the controller's Hardware Installation Guide for how to identify and set a controller's built-in EOL terminations.

Only a Daisy-Chained Data Bus Topology is Acceptable

Use a daisy-chained BACnet MS/TP data bus topology only. No other data bus topology is allowed.

Figure 74: Typical BACnet MS/TP LAN Topology Showing How Devices are Daisy-Chained Together to Form One Data Bus Segment



⚠ Only linear, daisy-chained devices provide predictable data bus impedances required for reliable data bus operation.

Only a daisy-chained data bus topology should be specified during the planning stages of a project and implemented in the installation phase of the project.

A spur is only permitted when it is connected to the data bus through a repeater (see *Using Repeaters to Extend the Data Bus*).

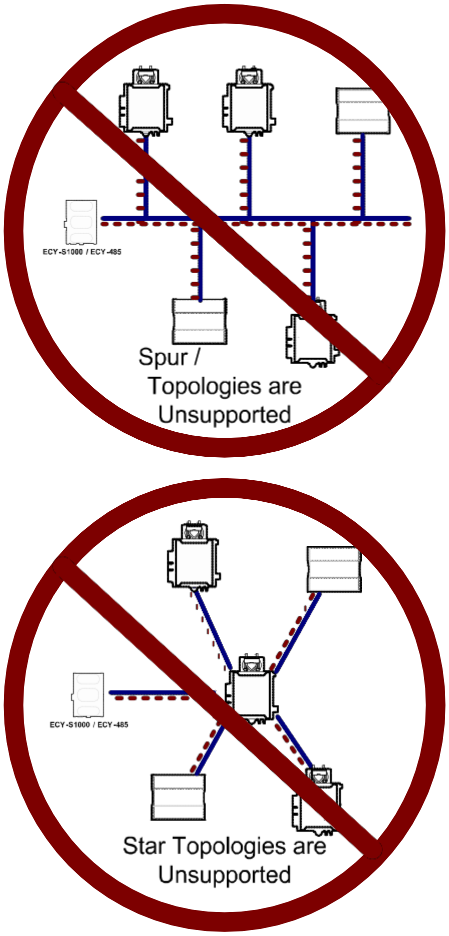


Figure 75: Unsupported BACnet MS/TP LAN Topologies

Data Bus Shield Grounding Requirements

The EIA-485 data bus standard requires that the data bus must be shielded against interference. A BACnet MS/TP data bus must also be properly grounded.

For ECB Series 24V-Powered Controllers: The data bus' cable shields must be twisted together and isolated with electrical tape at each device. Note that for ECB 24V-Powered Controllers, the power supply transformer's secondary that is connected to the 24V COM terminal is grounded. This provides the ground reference for the data bus (see *BACnet MS/TP is a Three-Wire Data Bus*). If the controller is at the end of the BACnet MS/TP data bus, simply isolate the data bus shield with electrical tape.

For ECB-PTU Series Line-Powered Controllers: The data bus' cable shields must be twisted together and connected to the **COM** terminal ateach ECB-PTU Line-Powered Controller. Keep the cable shield connections short and take steps at each device to isolate the cable shield from touching any metal surface by wrapping them with electrical tape, for example. Note that for ECB-PTU Line-Powered Controllers, the data bus' cable shield provides the ground reference for the data bus (see *BACnet MS/TP is a Three-Wire Data Bus*). If the controller is at the end of the BACnet MS/TP data bus, simply connect the data bus shield to the **COM**terminal.

ECLYPSE Series Controller: The data bus' cable shields must be twisted together and connected to the **S** terminal at each ECLYPSE Series Controller. Keep the cable shield connections short and take steps at each device to isolate the cable shield from touching any metal surface by wrapping them with electrical tape, for example. Note that for ECLYPSE Series Controller, the data bus' cable shield provides the ground reference for the data bus (see *BACnet MS/TP is a Three-Wire Data Bus*). If the controller is at the end of the BAC- net MS/TP data bus, simply connect the data bus shield to the **S** terminal.

⚠ Grounding the shield of a data bus segment in more than one place will more than likely reduce shieldingeffectiveness.

ECB 24V-Powered Controller Data Bus Shield Grounding Requirements

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the NECY Series Controller, as shown below in *Figure 76* and *Figure 77*.

Series Controller located at the End of the Data Bus

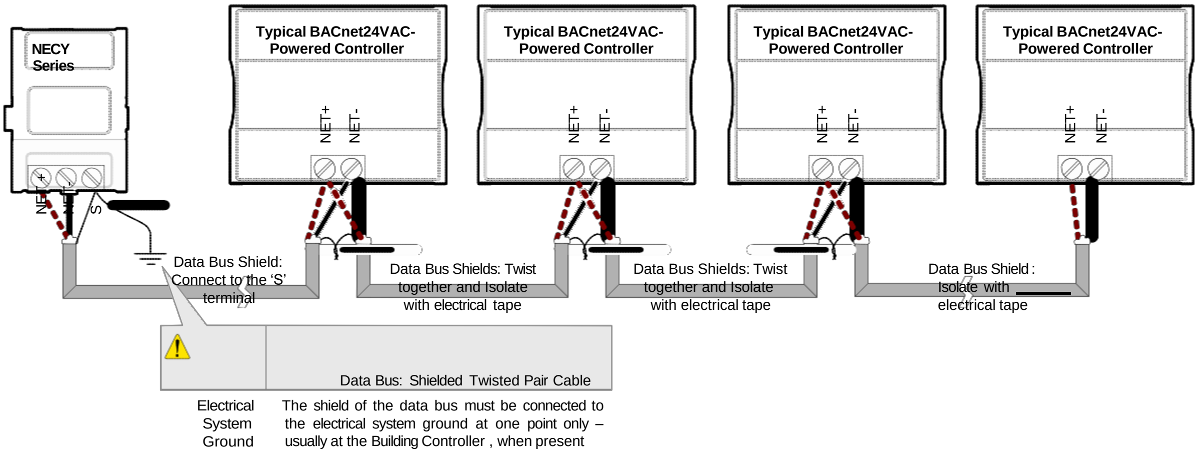
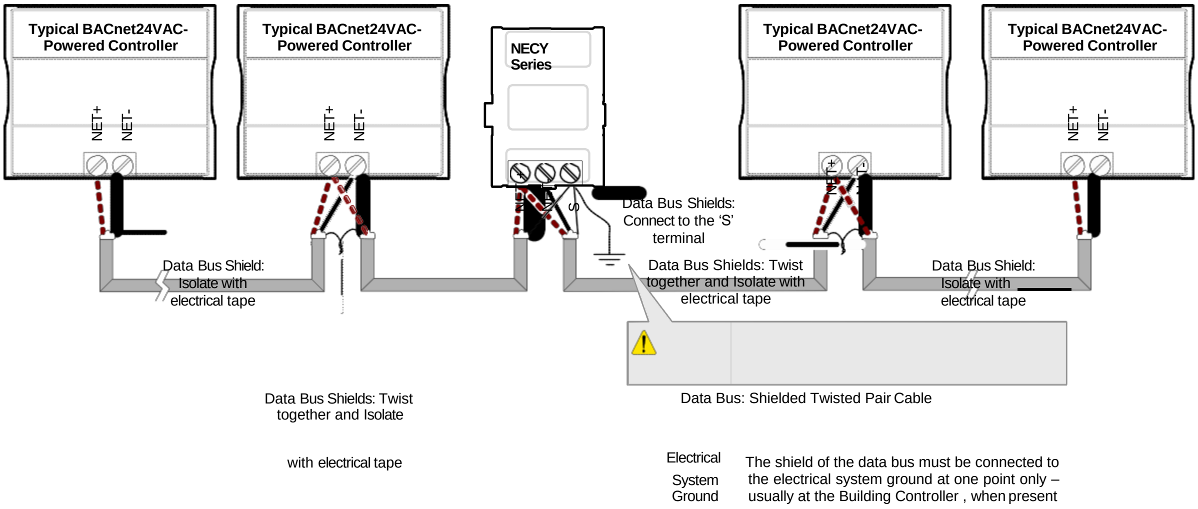

NECY
Series
NET+
NET-
S
Typical BACnet24VAC-Powered Controller
Typical BACnet24VAC-Powered Controller
Typical BACnet24VAC-Powered Controller
Typical BACnet24VAC-Powered Controller
NET+
NET-
NET+
NET-
NET+
NET-
NET+
NET-
Data Bus Shield: Connect to the 'S' terminal
Data Bus Shields: Twist together and Isolate with electrical tape
Data Bus Shields: Twist together and Isolate with electrical tape
Data Bus Shield : Isolate with electrical tape
Data Bus: Shielded Twisted Pair Cable
Electrical System Ground
The shield of the data bus must be connected to the electrical system ground at one point only – usually at the Building Controller , when present

Figure 77: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an NECY Series Controller located in the Middle of the Data Bus


Typical BACnet24VAC-Powered Controller
Typical BACnet24VAC-Powered Controller
NECY
Series
Typical BACnet24VAC-Powered Controller
Typical BACnet24VAC-Powered Controller
NET+
NET-
NET+
NET-
NET+
NET-
S
NET+
NET-
NET+
NET-
Data Bus Shields: Connect to the 'S' terminal
Data Bus Shield: Isolate with electrical tape
Data Bus Shields: Twist together and Isolate with electrical tape
Data Bus Shield: Isolate with electrical tape
Data Bus Shields: Twist together and Isolate
with electrical tape
Data Bus: Shielded Twisted Pair Cable
Electrical System Ground
The shield of the data bus must be connected to the electrical system ground at one point only – usually at the Building Controller , when present

ECB-PTU Line-Powered Data Bus Controller Shield Grounding Requirements

The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the NECY Series Controller, as shown below *Figure 78* and *Figure 79*.

Figure 78: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an NECY Series Controller located in the End of the Data Bus

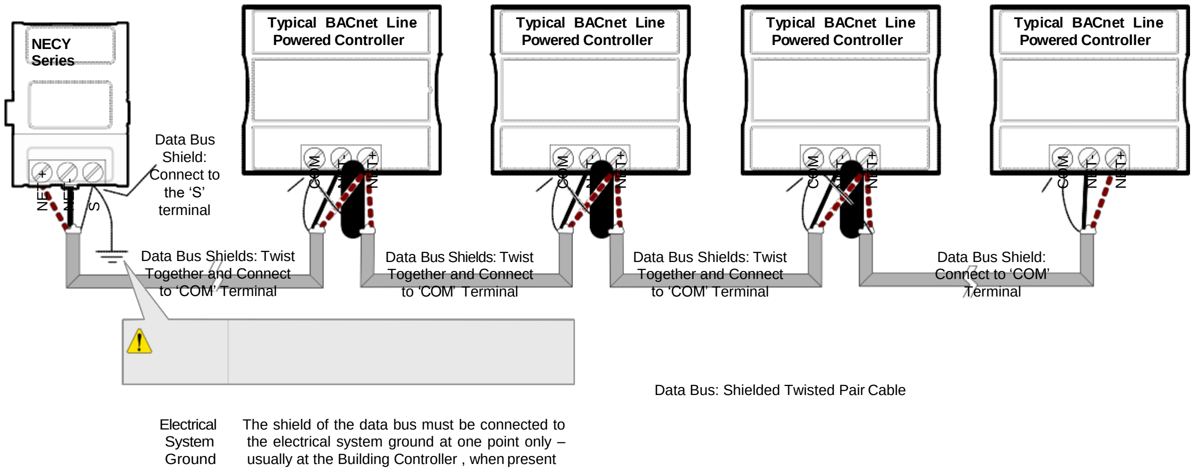
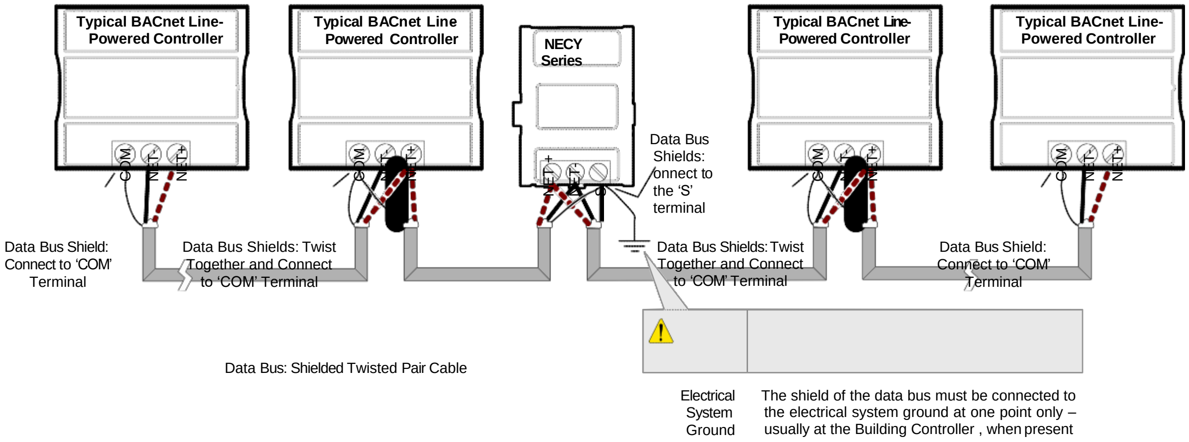

NECY Series
Typical BACnet Line Powered Controller
Typical BACnet Line Powered Controller
Typical BACnet Line Powered Controller
Typical BACnet Line Powered Controller
NET+
NET-
S
COM
NET-
NET+
Data Bus Shield: Connect to the 'S' terminal
Data Bus Shields: Twist Together and Connect to 'COM' Terminal
Data Bus Shields: Twist Together and Connect to 'COM' Terminal
Data Bus Shields: Twist Together and Connect to 'COM' Terminal
Data Bus Shield: Connect to 'COM' Terminal
Data Bus: Shielded Twisted Pair Cable
Electrical System Ground
The shield of the data bus must be connected to the electrical system ground at one point only – usually at the Building Controller , when present

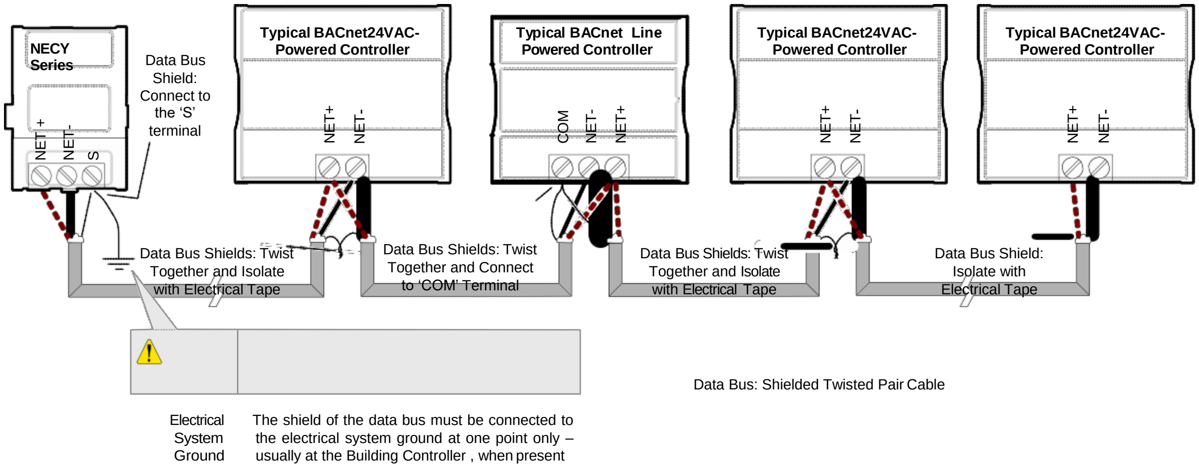
Figure 79: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an NECY Series Controller located in the Middle of the Data Bus


Typical BACnet Line-Powered Controller
Typical BACnet Line Powered Controller
NECY Series
Typical BACnet Line-Powered Controller
Typical BACnet Line-Powered Controller
COM
NET-
NET+
Data Bus Shields: onnect to the 'S' terminal
Data Bus Shield: Connect to 'COM' Terminal
Data Bus Shields: Twist Together and Connect to 'COM' Terminal
Data Bus Shields: Twist Together and Connect to 'COM' Terminal
Data Bus Shield: Connect to 'COM' Terminal
Data Bus: Shielded Twisted Pair Cable
Electrical System Ground
The shield of the data bus must be connected to the electrical system ground at one point only – usually at the Building Controller , when present

Data Bus Shield Grounding Requirements When Mixing Both ECB 24V-Powered Controllers and ECB-PTU Line-Powered Controllers

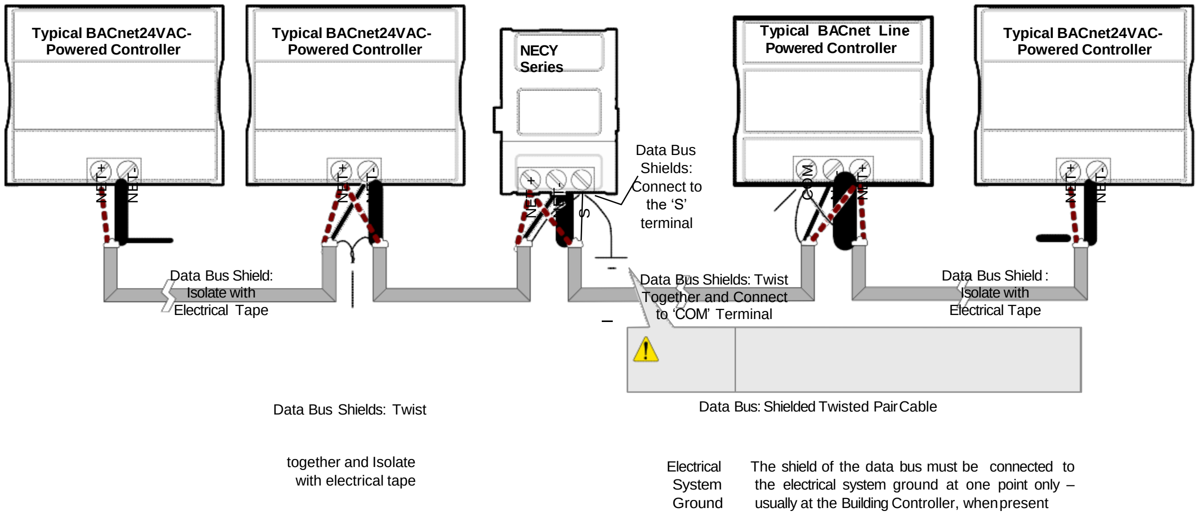
The shield on each data bus segment must be connected to the electrical system ground at one point only, for example, at the NECY Series System Controller, as shown below *Figure 80* and *Figure81*.

Series Controller located in the End of the Data Bus



The shield of the data bus must be connected to the electrical system ground at one point only – usually at the Building Controller , when present

Figure 81: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an NECY Series Controller located in the Middle of the Data Bus



The shield of the data bus must be connected to the electrical system ground at one point only – usually at the Building Controller, when present

Using Repeaters to Extend the Data Bus

A BACnet MS/TP data bus segment can be up to 1220 meters (4000 feet) long with up to a maximum of 50 devices. When a greater length is required, a solution is to use a repeater. A repeater increases the maximum length of the data bus.

Using a Repeater to Extend the Length of the BACnet MS/TP Data Bus

Repeaters can be used to extend a BACnet MS/TP data bus up to 3660 meters maximum total length. Do not use more than two repeaters on a BACnet MS/TP LAN.

A BACnet MS/TP repeater is a bi-directional device that regenerates and strengthens the electrical signals that pass through it. It creates two electrically-isolated BACnet MS/TP data bus segments that transparently enable devices on one side of the repeater to communicate with any device on the other side. The two BACnet MS/TP data bus segments have the same requirements of an ordinary BACnet MS/TP data bus segment; that is, each BACnet MS/TP data bus segment:

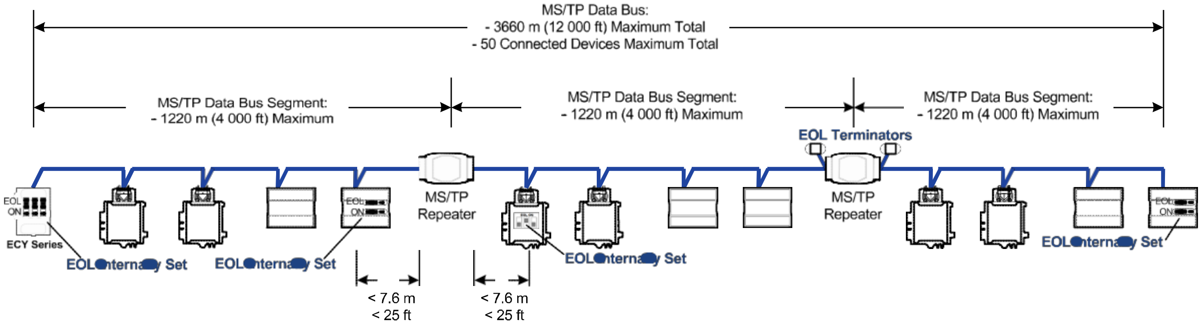
- Can be up to 1220 meters (4000 feet) long.
- The first and last device on the data bus must have End-of-Line (EOL) termination resistors connected across the two data lines/wires of the twisted pair.
- Must respect the maximum limit for *Device Loading.*
- Will have the same network number as they remain part of the same network or LAN.

It is recommended that you connect no more than 50 of our ⅛ or ½-load devices on all BACnet MS/TP Data Bus repeater segments when a baud rate of 19 200 or higher is used (preferably 38 400 baud). This is to ensure that the BACnet MS/TP Data Bus has enough bandwidth to efficiently communicate network variables between controllers.

⚠ Do not use more than two repeaters on a BACnet MS/TP data bus. A repeater can only connect two BACnet MS/TP data bus segments even if it has ports to support more than two BACnet MS/TP data bus segments.

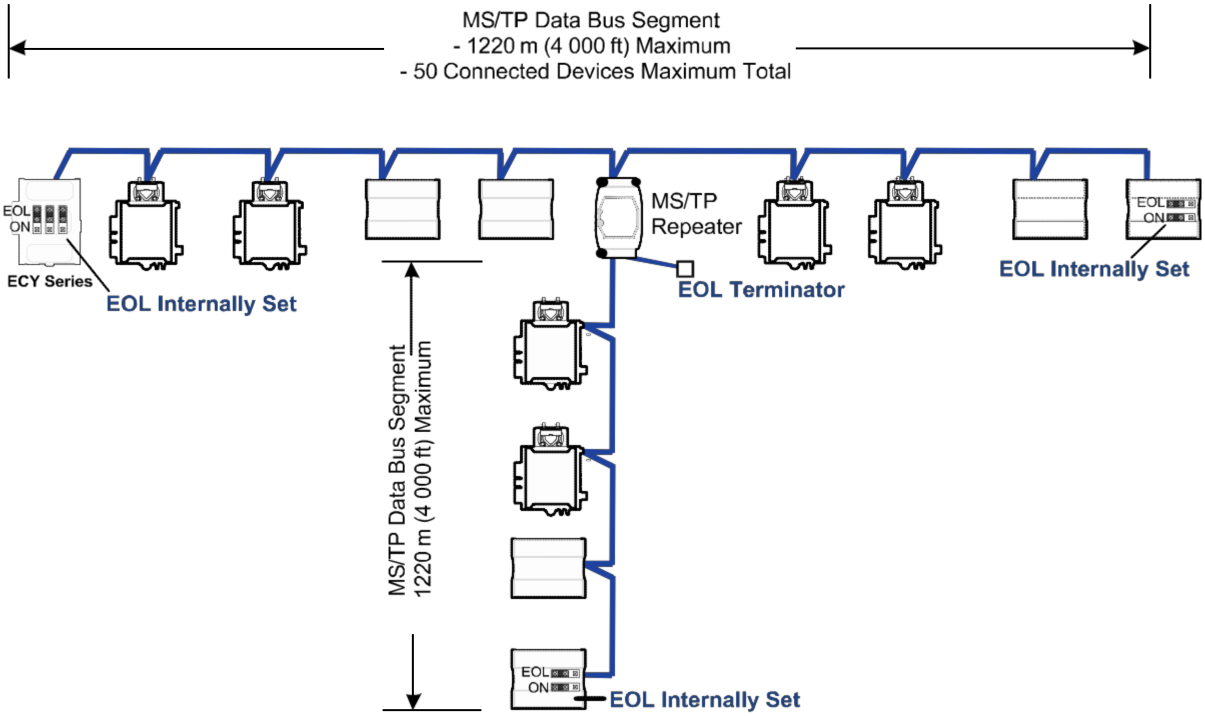
A repeater can be added anywhere to a data bus segment including the end of the segment as shown below.

Figure 82: Using a Repeater to Extend the Range of the LAN



A repeater can be used to create a spur as shown below.

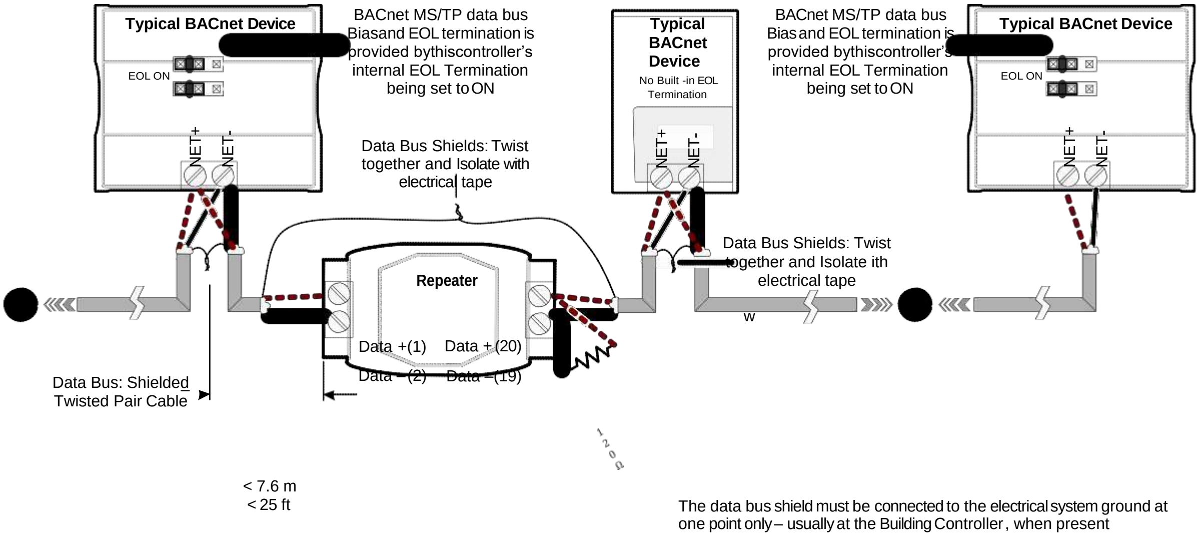
Figure 83: Adding a Spur by Using a Repeater



A repeater is counted as a device on each data bus to which it is connected.

When third party devices are connected to a data bus segment, the number of devices that can be connected to that data bus segment may be reduced. See *Device Loading.*

Figure 84: Repeater Connections when it is the First or Last Device on its Respective Data Bus Segment


Typical BACnet Device
EOL ON
NET+
NET-
BACnet MS/TP data bus Biasand EOL termination is provided bythiscontroller's internal EOL Termination being set to ON
Typical BACnet Device
No Built -in EOL Termination
NET+
NET-
BACnet MS/TP data bus Bias and EOL termination is provided bythiscontroller's internal EOL Termination being set to ON
Typical BACnet Device
EOL ON
NET+
NET-
Data Bus Shields: Twist together and Isolate with electrical tape
Data Bus Shields: Twist together and Isolate ith electrical tape
Repeater
Data +(1)
Data +(20)
Data −(2)
Data −(19)
w
Data Bus: Shielded Twisted Pair Cable
1 2 0 Ω
< 7.6 m
< 25 ft
The data bus shield must be connected to the electrical system ground at one point only – usually at the Building Controller, when present

The BACnet MS/TP Data Bus must be biased. This bias can only be provided by built-in EOL termination resistors (ones set with a jumper or DIP switch). When a repeater is the first or last device on its respective data bus segment, use the following methods to provide MS/TP Data Bus biasing and EOL termination as applicable to your situation:

1. On the BACnet MS/TP data bus segment □ shown in *Figure 84*, bias and EOL termination is provided by a controller's built-in EOL termination being set to ON. In this case the connection to the repeater cannot be more than 7.6 meters (25 feet) from this controller.
2. On the BACnet MS/TP data bus segment □ shown in *Figure 84*, a 120Ω EOL Termination resistor is added to the repeater's terminals. Biasing for this BACnet MS/TP data bus segment is provided by the built-in EOL termination being set to ON at the last controller at the other end of this data bus.

See *When to Use EOL Terminations* for more information. The shield of one data bus must be grounded at one point as specified in *Data Bus Shield Grounding Requirements*. The shields of the two data buses must be connected together and isolated with electrical tape as shown in *Figure 84*. Refer to the controller's Hardware Installation Guide for how to identify and set a controller's built-in EOL terminations.

Device Addressing

Device addressing allows the coordinated transfer of messages between the intended devices on the BACnet MS/TP data bus and with devices connected to the internetwork. For this, each device connected to the BACnet MS/TP data bus is identified by a MAC address, a Device Instance number, and a Network Number:

- The MAC Address uniquely identifies a device on a Network (identified by a Network Number). Devices on another Network can have the same MAC Address as messages are not passed at the internetwork level using the MAC Address. The MAC Address also defines the devices on the data bus that are Masters and Slaves, among other categories (see *Table 10*). The MAC Address is also used to share data bus bandwidth between devices through token passing between Masterdevices.
- The Device Instance uniquely identifies a device across the BACnet internetwork. The Device Instance is any number between 0 and 4 194 303. It is with the Device Instance that messages are exchanged between BACnet devices. The Device Instance is also used by routers to forward messages to devices located elsewhere in the internetwork. Unlike a MAC Address, a Device Instance cannot be reused elsewhere in the BACnet internetwork (it must be unique for the entirenetwork).
- The Network Number is any number between 1 and 65 534. A network number identifies a LAN for routing purposes.

Both the MAC Address and the Device Instance must be set for each device and are essential for proper BACnet LAN operation.

For an example of how MAC address, Device Instance number, and Network Number apply to a typical BACnet network, see *Figure 86*.

About the MAC Address

The MAC Address is a number from 0 to 255; however, we recommend reserving some MAC Addresses for common commissioning and maintenance tasks. For example, when a portable adapter is set to use one of these reserved MAC Addresses, it can be temporarily connected with certainty to any BACnet MS/TP data bus of any site without conflicting with other devices already connected to the BACnet MS/TP data bus. We strongly recommend that the MAC address of NECY Series Controller’s MS/TP port be always set to
0.

MAC Addresses should be used as shown in the following table.

Table 10: Recommended BACnet MS/TP Bus MAC Address Values / Ranges for BACnet MS/TP Data Bus Devices

MAC Address Value / Range	Usage	Devices
0	Data Bus Master (NECY Series Control- ler)	This address is invalid for Distech Controls' ECB series devices
1	Temporary commissioning connection	This address is invalid for Distech Controls' ECB series devices
2	Reserved	Other
3-127	Master Range	Master devices: All Distech Controls' devices are master devices and should be in this MAC Address range
128-254	Slave Range	Slave devices and network sensors
255	Broadcast	Do not apply address 255 to any device

BACnet MS/TP Data Bus Token-Passing Overview

The BACnet MS/TP data bus protocol is a peer-to-peer, multiple-master protocol that shares data bus bandwidth by passing a token between Master devices on the data bus that authorizes the device that is holding the token to initiate communications on the data bus. Once the device has completed its request(s), it closes the communications channel, passes the token to the next Master device (making it the current Master), and liberates the data bus.

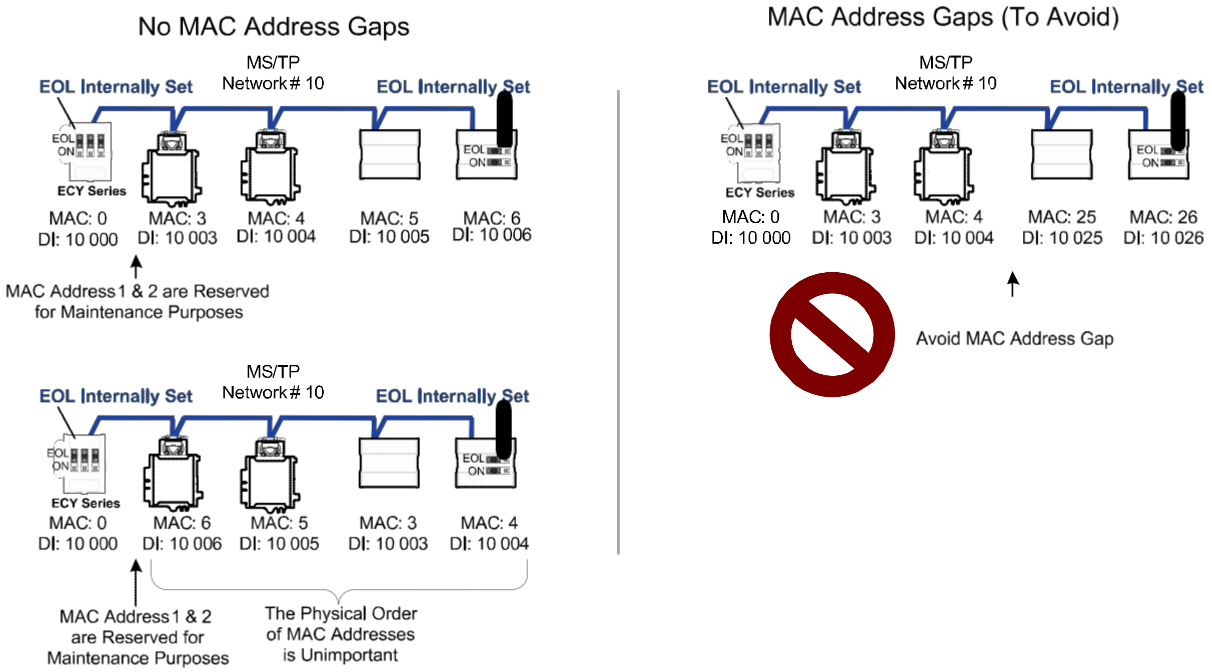
The token is passed through a short message from device to device on the BACnet MS/TP data bus in consecutive order starting from the lowest MAC address (MAC Address = 0) to the next MAC Address.

Gaps or pockets of unassigned device MAC Addresses should be avoided as this reduces data bus performance. Once a master has finished making its requests, it must poll for the next master that may exist on the Data Bus. It is the timeout for each unassigned MAC Address that slows down the data bus.

The way MAC Addresses are assigned is not a physical requirement: Devices can be daisy-chained on the data bus in any physical order regardless of their MAC Address sequence. The goal is to avoid gaps in the device MAC Address range.

Slave devices cannot accept the token, and therefore can never initiate communications. A Slave can only communicate on the data bus to respond to a data request addressed to it from a Master device. Gaps in slave device MAC Addressing have no impact on BACnet MS/TP data bus performance.

Figure 85: Setting the Max Master on the NECY Series Controller to the Highest MAC Address Used on the BACnet MS/TP Data Bus



About Tuning the Max Info Frames Parameter

Once a device has the token, it can make a number of information requests to other devices on the BACnet intranetwork. The maximum number of requests is limited by the **Max Info Frames** parameter. Once the device has made the maximum number of requests it is permitted to make according to the **Max Info Frames** parameter, the device passes the token to the following device with the next higher MAC address. This makes the BACnet MS/TP Data Bus more reactive for all devices by preventing a device from hanging on to the token for too long. Ordinary BACnet MS/TP devices should have the **Max Info Frames** parameter set to between 2 and 4. The Data Bus Master (NECY Series Controller) should have the **Max Info Frames** parameter set to 20.

About Tuning the Max Master Parameter

To prevent the passing of the token to unused MAC Addresses situated after the final Master device, the Max Master parameter must be set. By default, the Max Master for an NECY Series Controller or a Supervisor is set to 127 which allows for the theoretical maximum of 127 devices besides the Data Bus Master to be connected to the data bus.

In practice, the actual number of devices connected to a data bus is far less, resulting in a gap between the highest MAC Address of any device connected to the data bus and the value set for Max Master. This gap unnecessarily slows-down the data bus with Poll for Masterrequests.

When commissioning a BACnet MS/TP Data Bus, it is useful to start with the Max Master set to 127 so as to be able to discover all devices connected to the data bus. Then, once all devices have been discovered and the MAC Addressing is finalized by eliminating any gaps in the address range, set the **Max Master** (maximum MAC Address) in the NECY Series Controller and in the Supervisor to the highest Master device's MAC Address number to optimize the efficiency of the data bus.

Setting the Max Master and Max Info Frames

The **Max Master** and **Max Info Frames** are parameters used to optimize a BACnet MS/TP Data Bus. This is set in the NECY Series Controller and sepa- rately with the Supervisor for each connected BACnet MS/TP device.

For the NECY Series Controller, set the **Max Info Frames** to 20 in the screen shown in **BACnet Settings** of the *Network MS/TP Ports* as this is a device that will make more requests for service from other devices on the network. In general, according to the way a device is programmed, the **Max Info Frames** may have to be set to a higher value than for other devices. For example, when Roof Top Unit Controllers are used with VAV controllers that use *gfx*Applications code, they should also have their **Max Info Frames** set to a higher value such as 5, as Roof Top Unit Controllers will poll many VAV controllers for information.

To set the **Max Master** and **Max Info Frames** for BACnet MS/TP devices (for example, an ECB series controller), use a Supervisor to do so. See the NetworkUserGuide for more information.

Default Device Instance Number Numbering System for Acuity Controls' controllers

By default, controllers from Distech Controls automatically self-assign a Device Instance number generated from the unique MAC Address assigned to the controller during installation. The Device Instance number is calculated as follows:

Device Instance number = 364 X 1000 + MAC Address

Where 364 is Distech Controls unique BACnet Manufacturer ID.

This Numbering system is sufficient for a BACnet network that has only one NECY Series Controller. For larger BACnet networks that have more than one NECY Series Controller (to form a BACnet intranetwork), set the MAC Addresses, Device Instance Numbers and Network Numbers according to the numbering scheme below.

Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers

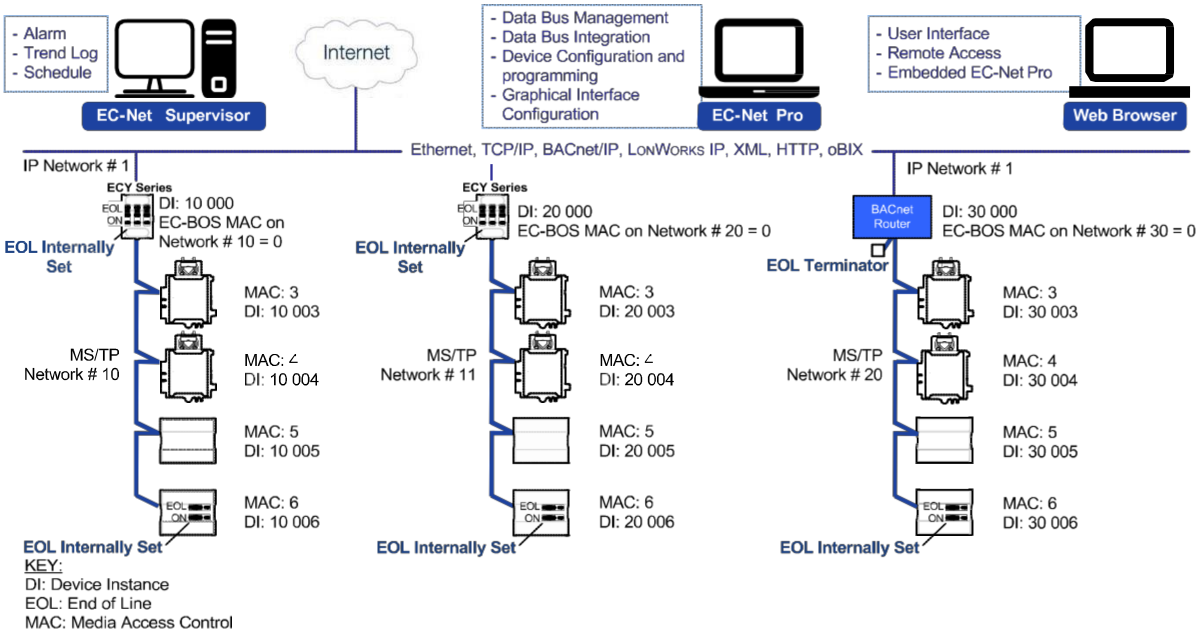
Good network planning requires a well-thought-out numbering scheme for device MAC Addresses, Device Instance Numbers (DI), and Network Numbers. We recommend the following scheme, as it reuses the MAC Address and Network Number in the Device Instance number to make it easier for a network administrator to know where a device is located in the network. This is shown below.

Table 11: Recommended Numbering Scheme for MAC Addresses, Instance Numbers, and Network Numbers

Description	Range	Example
BACnet/IP Network Number	0 to 65 534	1
NECY Series Controller BACnet/IP Device Instance Numbers: Multiples of 10 000	10 000 to 4 190 000	10 000 20 000
BACnet MS/TP Network Number: NECY Series Controller BACnet/IP Device Instance Num- ber/1000 + 0,1,2,3,4 (for each LAN)	10 to 4190	10 20 30
BACnet MS/TP Device Instance Number = NECY Series Controller BACnet MS/TP Net- work Number * 1000 + MAC Address	10 000 to 4 190 256	10 006 where MAC = 6

An example of this numbering system is shown below.

Figure 86: BACnet MS/TP Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers



⚠ When discovering devices with EC-Net which has the routing option configured, it will discover all BACnet devices connected to all NECY Series Controllers when routing is enabled (see *Routing*). Make sure to add only the devices connected to the MS/TP port of the specific NECY Series Controller being configured. Using this numbering system will greatly help to identify those devices that should be added to a given NECY Series Controller.

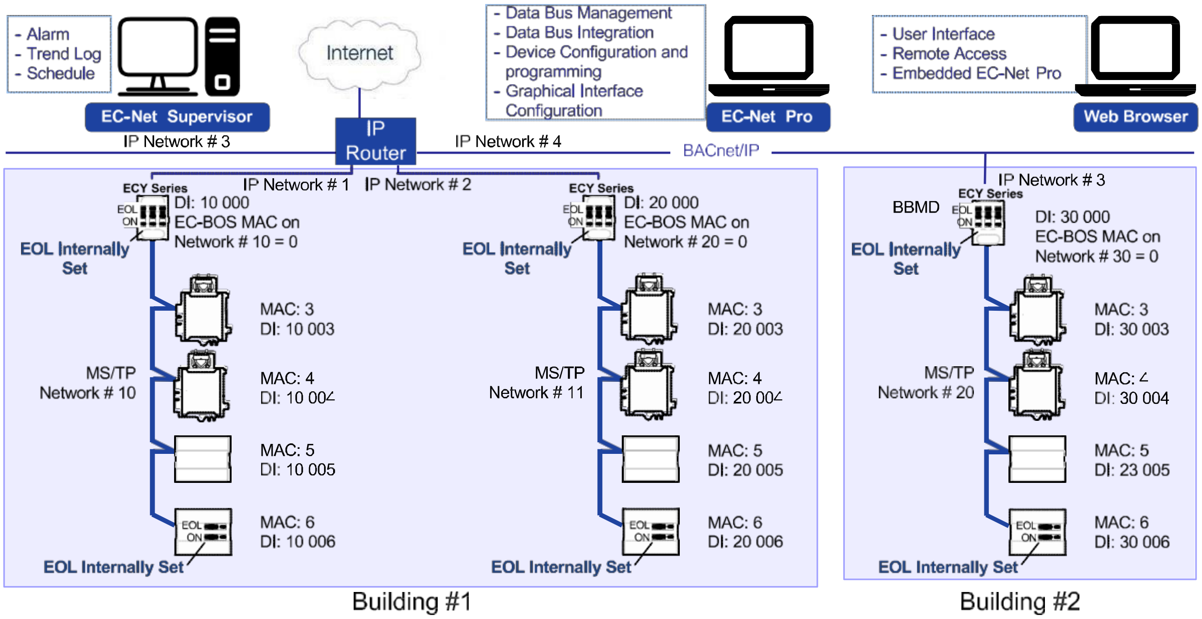
Setting the NECY Series Controller's MAC Address

The NECY Series Controller's MAC address can be set in **BACnet Settings** of the *nLight ECLYPSE Web Interface.*

Inter-Building BACnet Connection

BACnet network connections between buildings must be made using BACnet/IP as shown below.

Figure 87: Typical Inter-Building Connection Using BACnet/IP or FOX



KEY:
DI: Device Instance
EOL: End of Line
MAC: Media Access Control

BACnet/IP Broadcast Management Device Service (BBMD)

Though BACnet/IP uses IP protocol to communicate, a standard IP router does not forward broadcast messages which are important in BACnet to identify services that are available within the BACnet internetwork.

When two NECY Series Controllers communicate to each other over a standard IP connection that is separated by an IP router, both NECY Series Control- lers need the BACnet/IP Broadcast Management Device (BBMD) service to be configured and operational.

The BBMD service identifies BACnet messages on the BACnet MS/TP network that are intended for a device located on another BACnet network. The BBMD service encapsulates these messages into an IP message to the appropriate BBMD service of the other BACnet MS/TP network(s). The BBMD service on these networks strips out the encapsulation and sends the BACnet message on to the appropriate devices.

When sending BACnet messages across a standard IP connection that has an IP router, there must be one BBMD service running on each BACnet MS/TP network.

Power Supply Requirements for 24VAC-Powered Controllers

BACnet MS/TP is a Three-Wire Data Bus

Even though data is transmitted over a 2-wire twisted pair, all EIA-485 transceivers interpret the voltage levels of the transmitted differential signals with respect to a third voltage reference common to all devices connected to the data bus (signal reference). In practice, this common signal reference is provided by the building's electrical system grounding wires that are required by electrical safety codes worldwide. Without this signal reference, transceivers may interpret the voltage levels of the differential data signals incorrectly, and this may result in data transmission errors.

PS100-240 Power Supply is a double-insulated device and therefore is not grounded. The reference for the BACnet MS/TP data bus is made by connecting the shield of the BACnet MS/TP data bus to the ECLYPSE Series Controller's **S** terminal to provide a sig- nal reference. This shield is grounded at one point only – see *Data Bus Shield Grounding Requirements.*

Avoid Ground Lift

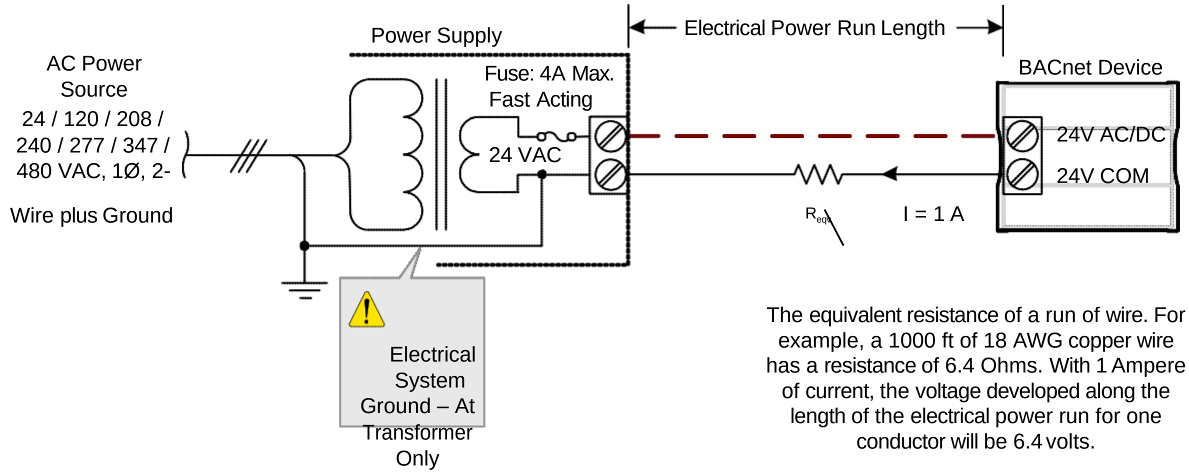
24V Power wiring runs should not be too long, nor have too many devices connected to it. Wiring used to supply power to devices has a resistance that is proportional to the length of the wiring run (See *Table 12*.).

Table 12: Resistance of Common Copper Wire Sizes

AWG	Diameter		Area		Copper wire resistance	
	Range	(mm)	(kcmil)	(mm^2)	(Ω/km)	(Ω/1000 ft.)
14	0.0641	1.628	4.11	2.08	8.286	2.525
16	0.0508	1.291	2.58	1.31	13.17	4.016
18	0.0403	1.024	1.62	0.823	20.95	6.385

If the power run from the power supply is relatively long and it supplies power to many devices, a voltage will develop over the length of wire. For example, a 1000 ft. of 18 AWG copper wire has a resistance of 6.4 Ohms. If this wire is supplying 1 Ampere of current to connected devices (See *Figure 88*.), the voltage developed across it will be 6.4 volts. This effect is called ground lift.

Figure 88: Ground Lift from a Long Power Run with a 24VAC Device


Power Supply
Electrical Power Run Length
AC Power Source
24 / 120 / 208 / 240 / 277 / 347 / 480 VAC, 1Ø, 2- Wire plus Ground
Fuse: 4A Max. Fast Acting
24 VAC
BACnet Device
24V AC/DC
24V COM
Req
I = 1 A

Electrical System Ground – At Transformer Only

The equivalent resistance of a run of wire. For example, a 1000 ft of 18 AWG copper wire has a resistance of 6.4 Ohms. With 1 Ampere of current, the voltage developed along the length of the electrical power run for one conductor will be 6.4 volts.

Because the 24V COM terminal on ECB series controllers is the signal reference point for the data bus, ground lift offsets the data bus voltage reference that is used to interpret valid data levels sent on the data bus. If the ground lift is more than 7 volts peak, there is a risk of data corruption and offline events due to the device being incapable of correctly reading data signals from the data bus. **Thus it is important to keep the power supply (transformer) as close to the controller as possible.**

Techniques to Reduce Ground Lift

Reduce the impact of ground lift as follows:

- Use a heavier gauge wire.
- Add more wire runs. Connect these wire runs to the power supply in a star pattern.
- For controllers that accept DC power (that is, models without triac outputs): Specify a 24VDC power supply. The continuous and evenvoltage of a DC power supply makes more efficient use of the power handling capabilities of a power run. A 24VDC power supply eliminates the 2.5 multiplication factor associated with the peak AC current being 2.5 times the average RMSAC current. See below.

About External Loads

When calculating a controller’s power consumption to size the 24VAC transformer, you must also add the external loads the controller is going to supply, including the power consumption of any connected subnet module (for example, for Allure series communicating sensors). Refer to the respective module’s datasheet for related power consumption information.

A controller can support a maximum of two Allure series sensor models equipped with a CO_2 sensor. See *Subnetwork Module Compatibility and Supported Quantity Charts* for how many Allure series communicating sensors are supported by a given controller model. The remaining connected Allure series sensor models must be without a CO_2 sensor.

24VAC Power Supply Connection

Use an external fuse on the 24VAC side (secondary side) of the transformer, as shown in *Figure 89*, to protect all controllers against power line spikes.

The ECLYPSE Controller uses the **S** terminal as the signal reference point for the data bus (see *Table 4* for common device terminal labels).

CHAPTER 11

Resetting or Rebooting the Controller

This chapter describes how to recover control over the controller by resetting it to the factory default settings.

Topics

Resetting or Rebooting the Controller

The reset button is located between the RS-458 and Ethernet connectors on connected system controllers and underneath the cover on connected VAV controllers. Depending on the amount of time the reset button is held down, different actions are taken by the controller.

Hold reset for	To
5 seconds	Restart / reboot the controller.
10 seconds	Reset both Ethernet and Wi-Fi IP addresses back to factory default settings.
20 seconds	Reset the controller to its factory default settings. User accounts (user names and passwords) will also be reset to the factory default settings and the controller's license and HTTPS security certificates will be cleared. If FIPS 140-2 mode has been enabled on the controller, this will turn FIPS 140-2 mode off.

⚠ Always backup the controller's license through the controller's Web interface before you hold the controller's reset button for 20 seconds. Once the controller reboots, you will have to install the license through the controller's Web interface.

To backup and install the license, see *System Settings*. Click **Export To PC** to backup the controller's license to your PC. Click **Import From PC** to restore the controller's license file from your PC.

After you hold the controller's reset button for 20 seconds, the controller's HTTPS security certificates will be regenerated. If you use HTTPS to connect to the controller, you will no longer be able to connect to the controller from any PC that was used in the past to connect to the controller unless you delete the old HTTPS security certificate from these PCs. See *Removing a Certificate*.

CHAPTER 16

NECY CONTROLLER TROUBLESHOOTING

You can use this Troubleshooting Guide to help detect and correct issues with the nLight ECLYPSE Series controllers.

Table 27: Troubleshooting NECY Controller Symptoms

Symptom	Possible Cause	Solution
Controller is powered but does not turn on	Fuse has blown (for 24V controllers)	Disconnect the power. Check the fuse integrity. Reconnect the power.
	Power supply polarity	Verify that consistent polarity is maintained between all controllers and the transformer. Ensure that the COM terminal of each controller is connected to the same terminal on the secondary side of the transformer. See *DHCP versus Manual Network Settings*
	The device does not have power / poor-quality power (for 24V controllers)	Verify that the transformer used is powerful enough to supply all controllers. See *Transformer Selection and Determining the Maximum Power Run Length*

Table 27: Troubleshooting NECY Controller Symptoms

Symptom	Possible Cause	Solution
Device does not communicate on the BACnet MS/TP network	Absent or incorrect supply voltage (for 24V controllers)	1. Check power supply voltage between 24VAC/DC and 24VCOM pins and ensure that it is within acceptable limits (±15% for 24V controllers). 2. Check for tripped fuse or circuit breaker.
	Overloaded power transformer (for 24V controllers)	Verify that the transformer used is powerful enough to supply all controllers. See *Transformer Selection and Determining the Maximum Power Run Length*
	Network not wired properly	Double check that the wire connections are correct.
	Absent or incorrect network termination	Check the network termination(s).
	Max Master parameter	Configure the **Max Master** to the highest MAC Address of any device on the MS/TP data bus. See *Setting the Max Master and Max Info Frames*
	There is another controller with the same MAC Address on the BACnet MS/TP data bus	Each controller on a BACnet MS/TP data bus must have a unique MAC Address. Look at the MAC Address DIP switch on the faceplate of each controller. If it is set to 0 (all off), use an Allure EC-Smart-Vue sensor to check the MAC Address.
	There is another controller with the same Device ID on the BACnet intranetwork	Each controller on a BACnet intranetwork (the entire BACnet BAS network) must have a unique Device ID. Use an Allure series communicating sensor to check the Device ID of each controller. See *Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers*
	BACnet data bus polarity is reversed.	Ensure the polarity of the BACnet data bus is always the same on all devices. See *BACnet MS/TP data bus is polarity sensitive*
	Cut or broken wire.	Isolate the location of the break and pull a new cable.
	The BACnet data bus has one or more devices with the same MAC Address.	See *Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers*
	The baud rate for all devices are set to AUTO	At least one device must be set to a baud rate, usually the data bus master. See *Baud Rate*
	The device is set to a MAC Address in the range of 128 to 255.	See if the STATUS LED on the device is showing a fault condition. See *Table 28* for a list of fault codes. This range is for slave devices that cannot initiate communication. All Distech Controls' devices are master devices and must their MAC Address set accordingly. See *Device Addressing*
	The maximum number of devices on a data bus segment has been exceeded.	Use a repeater to extend the BACnet data bus. See *Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate*
The STATUS LED is blinking	The device has auto-diagnosed a fault condition	See *Table 28* for a list of fault codes.

Table 27: Troubleshooting NECY Controller Symptoms

Symptom	Possible Cause	Solution
Controller communicates well over a short network BACnet MS/TP network, but does not communicate on large network	Network length	Check that the total wire length does not exceed the specifications of the Network Guide. See *Data Bus Physical Specifications and Cable Requirements*
	Wire type	Check that the wire type agrees with the specification of the Network Guide: See *Data Bus Physical Specifications and Cable Requirements*
	Network wiring problem	Double check that the wire connections are correct.
	Absent or incorrect network termination	Check the network termination(s). Incorrect or broken termination(s) will make the communication integrity dependent upon a controller's position on the network.
	Number of controllers on network segment exceeded	The number of controllers on a channel should never exceed 50. Use a router or a repeater: See *Data Bus Segment MAC Address Range for BACnet MS/TP Devices*
	Max Master parameter	Configure the maximum number of master device on the MS/TP network in all devices to the controller's highest MAC address used on the MS/TP trunk. *BACnet MS/TP Data Bus Token-Passing Overview*.
Hardware input is not reading the correct value	Input wiring problem	Check that the wiring is correct according to the module's hardware installation manual and according to the peripheral device's manufacturer recommendations.
	Open circuit or short circuit	Using a voltmeter, check the voltage on the input terminal. For example, for a digital input, a short circuit shows approximately 0V and an open circuit shows approximately 5V. Correct wiring if at fault.
	Configuration problem	Using the controller configuration wizard, check the configuration of the input. Refer to the controller's user guide for more information.
	Over-voltage or over-current at an input	An over-voltage or over-current at one input can affect the reading of other inputs. Respect the allowed voltage / current range limits of all inputs. Consult the appropriate datasheet for controller input range limits.
Hardware output is not operating correctly	Fuse has blown (Auto reset fuse, for 24V controllers)	Disconnect the power and outputs terminals. Then wait a few seconds to allow the auto-reset fuse to cool down. Check the power supply and the output wiring. Reconnect the power.
	Output wiring problem	Check that the wiring is correct according to the module's hardware installation manual and according to the peripheral device's manufacturer.
	Configuration problem	With EC-*gfx*Program, check the configuration of the output; for example, is it enabled? Refer to the EC-gfxProgram User Guide for more information.
	0-10V output, 24VAC powered actuator is not moving	Check the polarity of the 24VAC power supply connected to the actuator while connected to the controller. Reverse the 24VAC wire if necessary.

Table 28: LED Fault Condition Interpretation for ECB Devices

ECB Device LED Interpretation	Description	Solution
RX LED not blinking	Data is not being received from the BACnet MS/TP data bus.	If there is no communication, see *Table 27* - Troubleshooting NECY Controller Symptoms.
TX LED not blinking	Data is not being transmitted onto the BACnet MS/TP data bus.	
POWER constant on	Power is available at the device. However this does not mean that the quality of supplied power is good. See *Power Supply Requirements for 24VAC-Powered Controllers*.	If not lit, see *Power Supply Requirements for 24VAC-Powered Controllers* for the power requirements.
STATUS blinking	See following table.	-

Table 29: STATUS LED Interpretation for Normal Operation with ECB Devices

Device STATUS LED blink patterns	Status	Description
One fast blink	Initialization	The device is starting up.
The STATUS LED is always OFF (Not applicable to ECB-PTU Series)	No anomaly	Normal operation.

Table 30: Verify that the Following Recommendations have been Carried Out Before Calling Technical Support

Properly terminate the BACnet MS/TP data bus	EOL terminations must be enabled / installed at either end of the data bus only. See *Figure 71*.
Avoid duplicate MAC Addresses	Verify that no device has a duplicate MAC Address by checking the MAC Address DIP switch settings on all devices on the data bus, including segments connected by a repeater. If necessary, isolate devices from the data bus to narrow-down the number of devices that may be at fault.

Table 30: Verify that the Following Recommendations have been Carried Out Before Calling Technical Support

All devices must be set to the same baud rate	When all devices are set to AUTO baud rate, at least one device must be set to a baud rate, usually the data bus master. See *Maximum Number of BACnet MS/TP Devices on a Data Bus Segment and Baud Rate*
The data bus is polarity sensitive	Ensure that the polarity of all data bus wiring is consistent throughout the network. See *BACnet MS/TP data bus is polarity sensitive*
Do not overload the data bus with Change of Value (COV) reporting	COV reports create the most traffic on the BACnet MS/TP data bus. Set the COV report rate to the largest value that provides acceptable performance. Only map COV reports for values that are necessary. For mapped analog points that are continuously changing, try increasing the COV increment on these points or set the COV minimum send time flag to true to send the value at a regular frequency.
Do not leave address holes in the device's MAC Address range	Assign MAC Address to device starting at 3, up to 127. Do not skip addresses. Set the maximum MAC Address in the NECY Series Controller to the final MAC Address number actually installed. NOTE: The physical sequence of the MAC Address of the devices on the data bus is unimportant: For example, the MAC Address of devices on the data bus can be 5, 7, 3, 4, 6, and 8.
Only daisy-chained devices are acceptable	Eliminate T-taps and star configurations. Use a router to connect a data bus spur.
Connect no more than five devices to a power supply transformer (for 24V controllers)	BACnet MS/TP devices require good power quality. See *Power Supply Requirements for 24VAC-Powered Controllers*

CHAPTER 18

WI-FI NETWORK TROUBLESHOOTING GUIDE

Any wireless system consists of two or more Wi-Fi transceivers and a radio propagation path (Radio Path). Problems encountered can be any of the following.

Symptoms	Probable Causes	Corrective Actions
Wi-Fi communications are inexistent or intermittent	Presence of a low power jammer	If the low power jammer is close to the transceiver antenna, move low power jammer (PC, telephone, etc.) at least 6.5 feet (2 m) away from transceiver antenna.
		Change the Wi-Fi channel on the router. Use a Wi-Fi surveying or Wi-Fi stumbling tool on a laptop computer to identify unused Wi-Fi channels that may provide a better interference-free radio path.
		Move the nLight ECLYPSE Wi-Fi Adapter's position where it has a clear line of sight to the router.
		Move the wireless router's position. Try moving the router to the center of the room where it has a clear line of site to each wireless device.
	Presence of a high power jammer	Remove high power jammer if possible. If not, you will have to accept strong range reduction or add another wireless router closer to the controller(s).
		Use a wired Ethernet connection to the controller.
	Defective nLight ECLYPSE Wi-Fi Adapter	Exchange the wireless dongle with another nLight ECLYPSE Wi-Fi Adapter. If the dongle is found to be defective, replace the dongle.
	The maximum wireless operating range has been exceeded	Add another wireless router closer to the controller(s).
	The controller has a known technical issue	Upgrade the controller's firmware. See *User Management*
The nLight ECLYPSE Wi-Fi Adapter has been tested functional and there is no jammer in the field to interfere with the signal.	Radio signal path might be obstructed	If a new screening or metal separation wall has been installed since the network was set up, try moving the receiver to see if the issue is corrected.
	Router may have a known technical issue	Upgrade the router's firmware. See the manufacturer's Website.

Document Revision History

1. Version 0.1 - December 2014 - BetaRelease
2. Version 1.0 - January 2015 - Release toMarket
3. Version 1.1 - February 2015 - Updated Web Interface Information
4. Version 1.2 - September 2015 - Added the NECY-VAV series controllers, BACnet MS/TP, Modbus RTU, and Modbus TCP networksupport
5. Version 1.3 - October 2015 - Added Wi-Fi Mesh and Smart Room Control support
6. Version 1.4 - December 2015 - Clarified the number of Allure EC-Smart-Air and Allure EC-Smart- Comfort that are supported by a given controller model.
7. Version 1.5 - May 2016 - Added information for the ECx-Display
8. Version 1.6 - October 2016 - Minorupdates
9. Version 1.7 - March 2017:
   - New Applications tile in Web Configuration Interface
   - Update password information when FIPS 140-2 isenabled.
   - XpressNetwork Companion mobile appsupport
   - Updated Foreign Device Settings
10. Version 1.8 - June 2017 - Removed Wi-Fi mesh, added GSA support, new screenshots for the nLight ECLYPSE Web Interface, new backup & restore feature.

SENSORVIEW
INSTALLATION OVERVIEW

IMPORTANT

The following items should be available to ensure a successful SensorView Installation

- Computer meeting hardware/software requirements
- Windows Installation Disk
- Active Internet Connection
- SensorView Registration Key (provided in each Gateway box)
- Cross wired CAT-5(e) cable pg 18

step 1

SENSORVIEW REQUIREMENTS

Depending on the intended usage of SensorView, there are two sets of computer hardware/software requirements.

Single-user / Commissioning Installation:	**See Manual**
Multi-user Installation:	**See Manual**

step 2

PRE-INSTALLATION

The following Windows software components (as listed in SensorView hardware/software specifications) are required prior to SensorView installation.

.NET Framework **See Manual**

- Available for download (free) from Windows Updates web page

IIS (Internet Information Services):

IIS 5.0 XP Pro (32 bit)	**See Manual**
IIS 6.0 Windows Small Business Server 2003 (32b)	**See Manual**
IIS 6.0 Windows Server 2003 (32 bit)	**See Manual**
IIS 6.0 Windows Server 2003 (64 bit)	**See Manual**
IIS 7.0 Windows Server 2008 (32 bit)	**See Manual**
IIS 7.0 Windows Vista / 7 (32 bit)	**See Manual**
IIS 7.0 Windows Vista / 7 (64 bit)	**See Manual**

- Both Win XP & Server 2003 require Windows installation disks and are not downloadable from the web

NOTE: Both of these components must be installed prior to running the SensorView installation

step 3

SENSORVIEW INSTALLATION **See Manual**

The SensorView installation application is downloaded from the Internet.

- SensorView Installation will not proceed prior installation of both Windows components listed in the Pre-Installation section above were not completed.

step 4

CONNECTION TO GATEWAY

The Gateway uses its port labeled “Ethernet” to communicate with the computer running the SensorView software.

Direct Connection	**See Manual**
LAN/WAN Connection	**See Manual**
Crossover Cable Reference	**See Manual**

http://www.sensorswitch.com/install/setup.zip

SensorView Manual

Using SensorView

SensorView provides a large variety of configuration options to fine tune the connected nLight network. This section covers common configuration and management tasks that arise when setting up and maintaining the network over time; as well as step by step instructions for accomplishing a given task.

The Device Tree: The Device Tree is the foundation for navigating through SensorView and easily locating a specific device, profile, etc. It is always located in the far left side of the screen, and works in the same fashion as standard collapsing menus do in other programs. Select which feature of the Device Tree you wish to learn more about

- □ **Device Tree Overview**
- □ **Tree Layout**
- □ **Search / Filter / Locate Device**
- □ **View Device State**
- □ **View Device Status**
- □ **Selecting Multiple Devices**

FloorPlan: A feature providing a visual layout of the space for the purposes of device and zone selection and interaction. Contact us to have a layout produced for your nLight installation.

Once a layout is produced and you have received the layout (.mvdb) file, it can be imported into SensorView by going to Admin > Map and clicking the “Import” button, then browsing to and selecting the file.

Software and Firmware Updates

- **Updating Sensorview:** This process walks you through upgrading to the latest version of SensorView, and ensures you are running on the latest build, including the newest patches, compatibility fixes, and features. This process can only be run by authorized administrators of SensorView’s host machine, they cannot be performed via the web interface.
- □ **Updating Device Firmware:** Each nLight device has internal software that can be updated, usually to add new functionality. This process will ensure your devices are all running on up-to-date firmware, and can only be performed by authorized nLight network administrators.

Common Procedures: The menu items on the left are the procedures most commonly asked about using SensorView. If a procedure you are trying to perform is not included in this list, please contact us at [redacted] and we will look into adding it for future revisions.

- □ **Logging in**
- □ **Administrative Tasks**
  - ○ **Creating Users**
  - ○ **Modifying Users**
  - ○ **Gateway Page**
  - ○ **Location Page**
- □ **View Device Properties**
- □ **Viewing / Editing Device Settings**
  - ○ **Normal Devices**
  - ○ **Scene Selectors / nIOs**

Admin: The Admin tabs are for administrators only, and will not be accessed by a day to day end user.

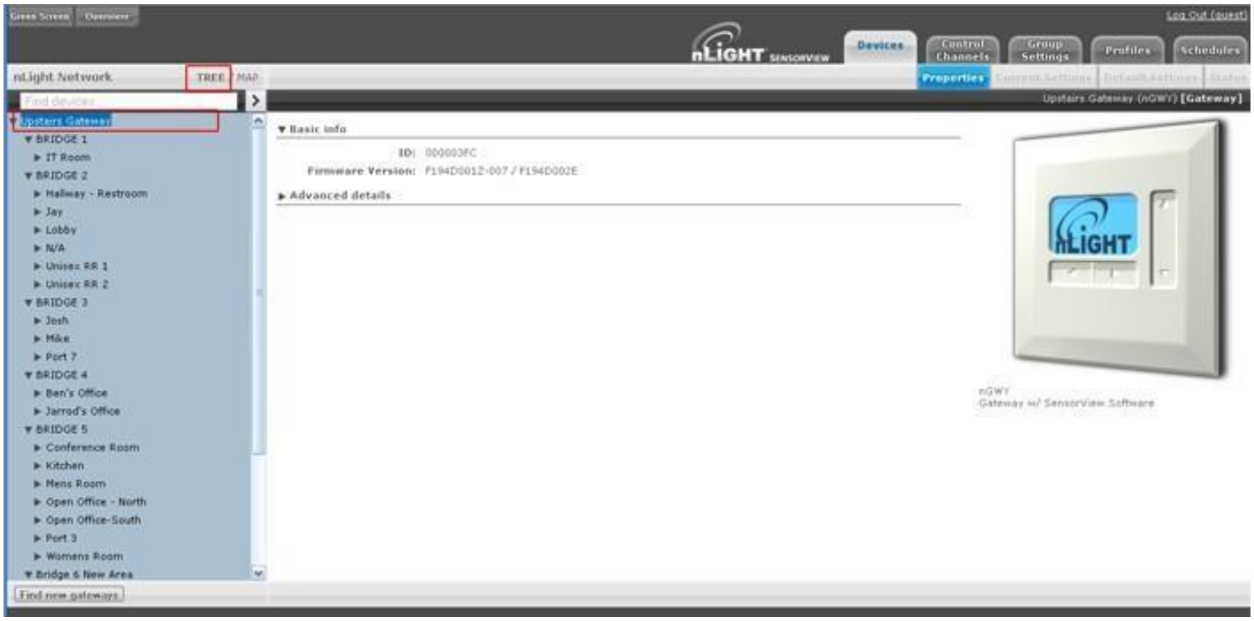
Navigation Tabs: Across the top of all pages within SensorView are the **Navigation Tabs**. Depending on a user's permissions only some of these may be available. To learn more about each tab, click from the list below:

- **Devices**
- **Control Channels**
  - **Local Channels**
  - **Global Channels**
- **Group Settings**
- **Profiles**
- **Schedules**
- **Users**

Glossaries

- **SensorView Terms**
- **Status Icons**

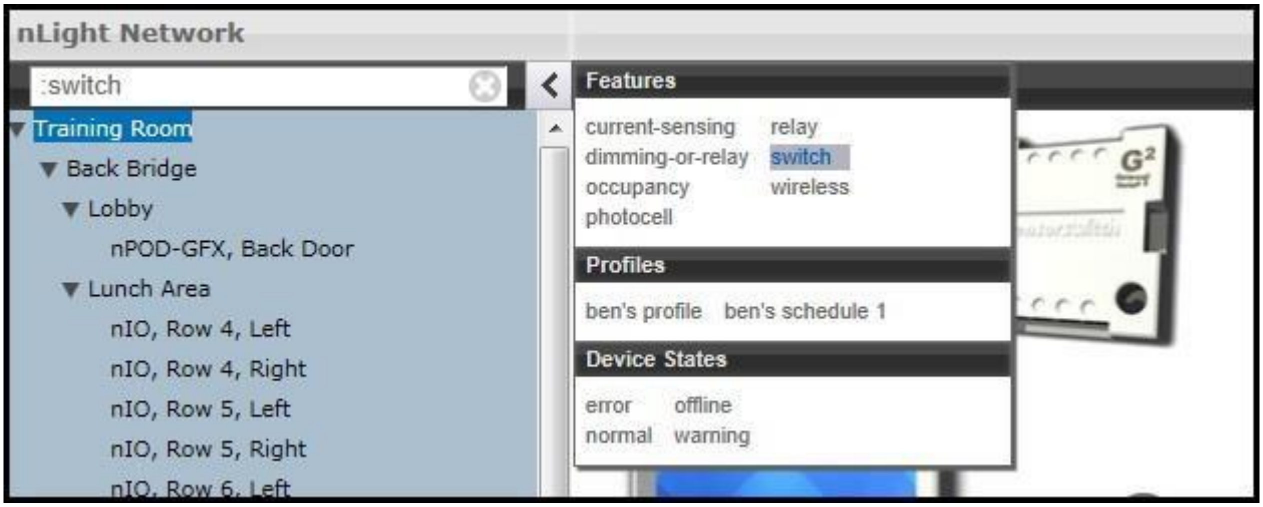
Device Tree Overview



ID: 000003FC

Firmware Version: F194D0012-007 / F194D002E

The Device Tree Menu, available from the arrow to the right of the search textbox, contains selection features that aid in the location / selection of devices. Three primary types of search features exist: Features, Profiles, and Device States. Features allows for selecting / searching of the tree based on predefined characteristics of the device, such as whether it has a relay or occupancy sensor; available options are: current-sensing, occupancy, daylighting, relay, dimming, switch, dimming-or-relay.

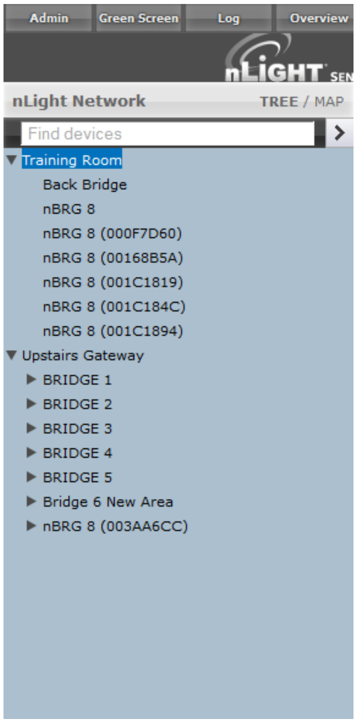


Profiles locates or selects devices that are in a particular profile; this is useful when creating a new profile that operates on all the devices already in an existing profile. As profiles are added or removed from the system the contents of this selections will change. Device States allows for searching or selecting devices depending on their current state.

Tree Layout

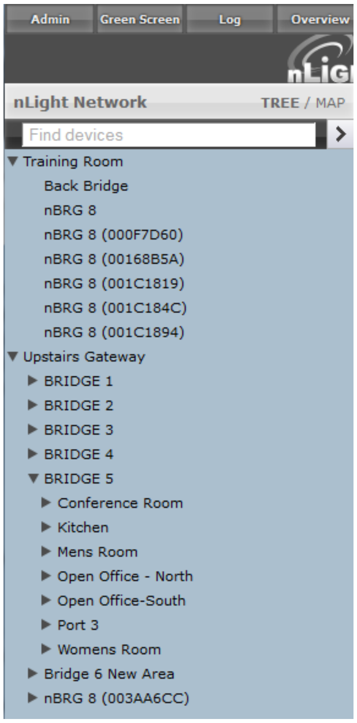
The layout of the SensorView device tree corresponds closely with the actual wiring of the devices, with a few notable exceptions:

Bridges are not nested within their parents



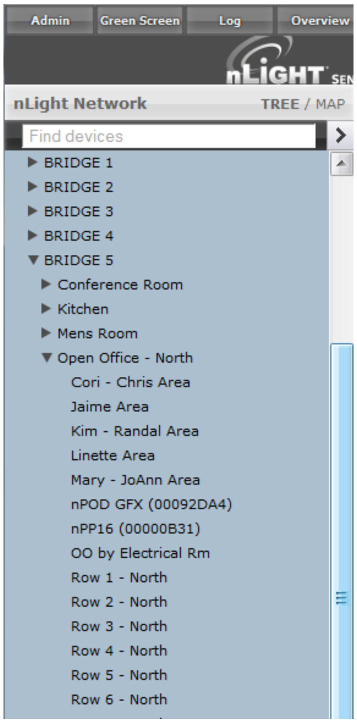
- ▼ Training Room
  - Back Bridge
  - nBRG 8
  - nBRG 8 (000F7D60)
  - nBRG 8 (00168B5A)
  - nBRG 8 (001C1819)
  - nBRG 8 (001C184C)
  - nBRG 8 (001C1894)
- ▼ Upstairs Gateway
  - ▶ BRIDGE 1
  - ▶ BRIDGE 2
  - ▶ BRIDGE 3
  - ▶ BRIDGE 4
  - ▶ BRIDGE 5
  - ▶ Bridge 6 New Area
  - ▶ nBRG 8 (003AA6CC)

Zones off a bridge are displayed in ascending alphabetical order



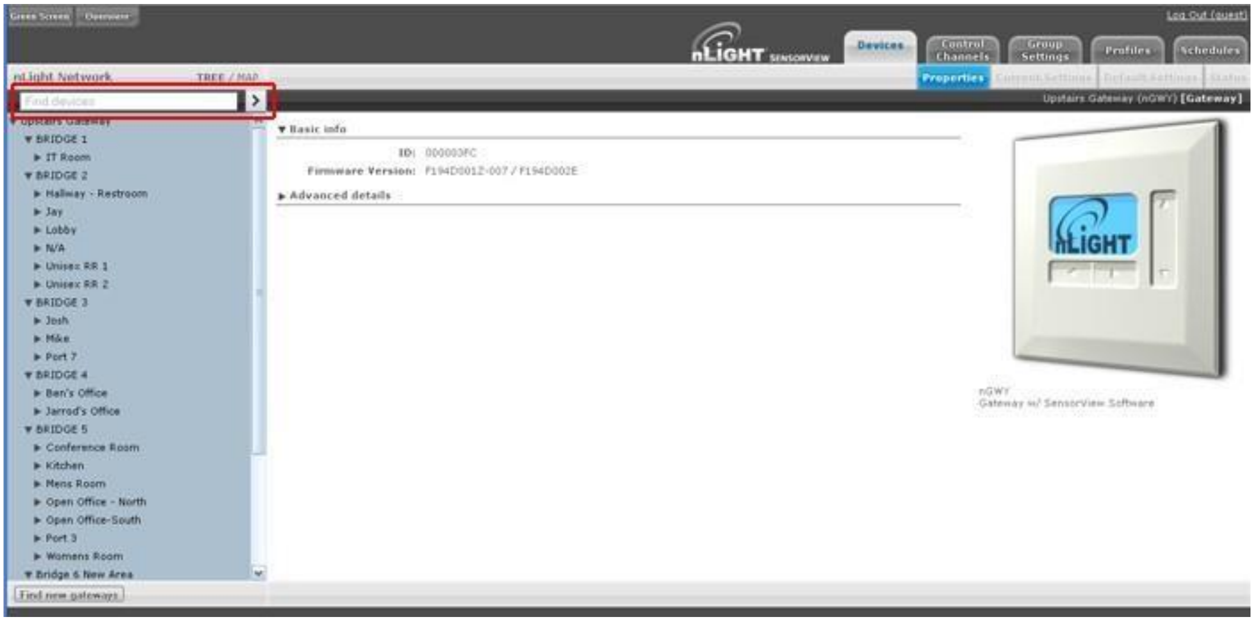
- ▼ Training Room
  - Back Bridge
  - nBRG 8
  - nBRG 8 (000F7D60)
  - nBRG 8 (00168B5A)
  - nBRG 8 (001C1819)
  - nBRG 8 (001C184C)
  - nBRG 8 (001C1894)
- ▼ Upstairs Gateway
  - ▶ BRIDGE 1
  - ▶ BRIDGE 2
  - ▶ BRIDGE 3
  - ▶ BRIDGE 4
  - ▼ BRIDGE 5
    - ▶ Conference Room
    - ▶ Kitchen
    - ▶ Mens Room
    - ▶ Open Office - North
    - ▶ Open Office-South
    - ▶ Port 3
    - ▶ Womens Room
  - ▶ Bridge 6 New Area
  - ▶ nBRG 8 (003AA6CC)

Devices in a zone are displayed in alphabetical order, not wiring order



- ▶ BRIDGE 1
- ▶ BRIDGE 2
- ▶ BRIDGE 3
- ▶ BRIDGE 4
- ▼ BRIDGE 5
  - ▶ Conference Room
  - ▶ Kitchen
  - ▶ Mens Room
  - ▼ Open Office - North
    - Cori - Chris Area
    - Jaime Area
    - Kim - Randal Area
    - Linette Area
    - Mary - JoAnn Area
    - nPOD GFX (00092DA4)
    - nPP16 (00000B31)
    - OO by Electrical Rm
    - Row 1 - North
    - Row 2 - North
    - Row 3 - North
    - Row 4 - North
    - Row 5 - North
    - Row 6 - North

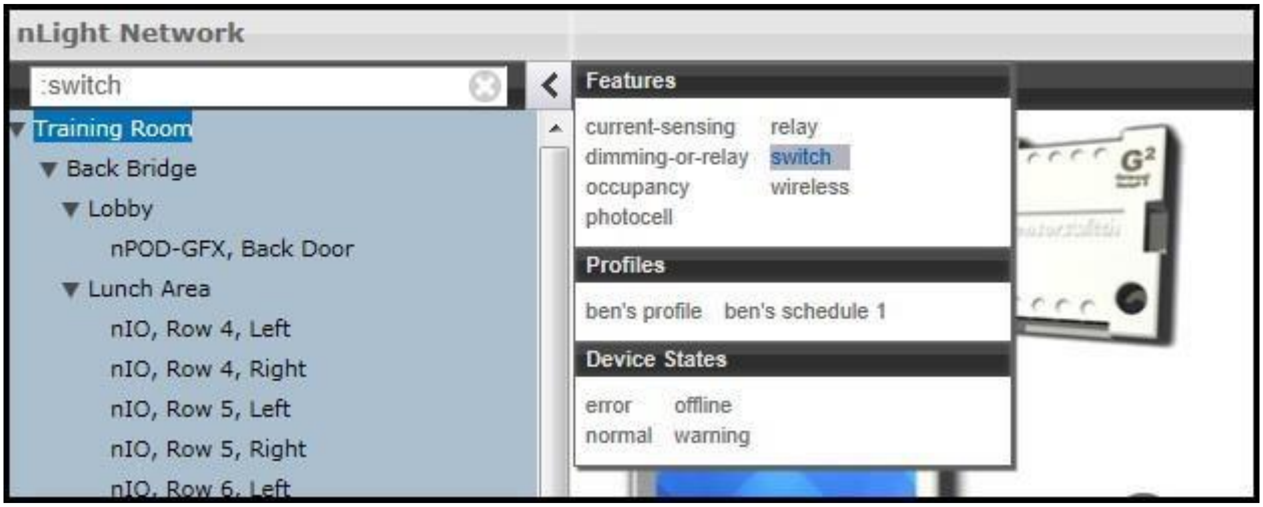
Search / Filter / Locate Device



ID: 000003FC

Firmware Version: F194D001Z-007 / F194D002E

The SensorView tree allows for the user to **select or search for devices** based on a variety of parameters. The Device Tree Menu contains numerous options for searching for (“finding”) devices based on predetermined characteristics (such as device state, or features the device has). The text field above the device tree also allows for **free text search over the devices**. A user can type any value into the field and the tree will automatically begin filtering to display devices with label(s), model(s), or device ID(s) matching the entered value(s).



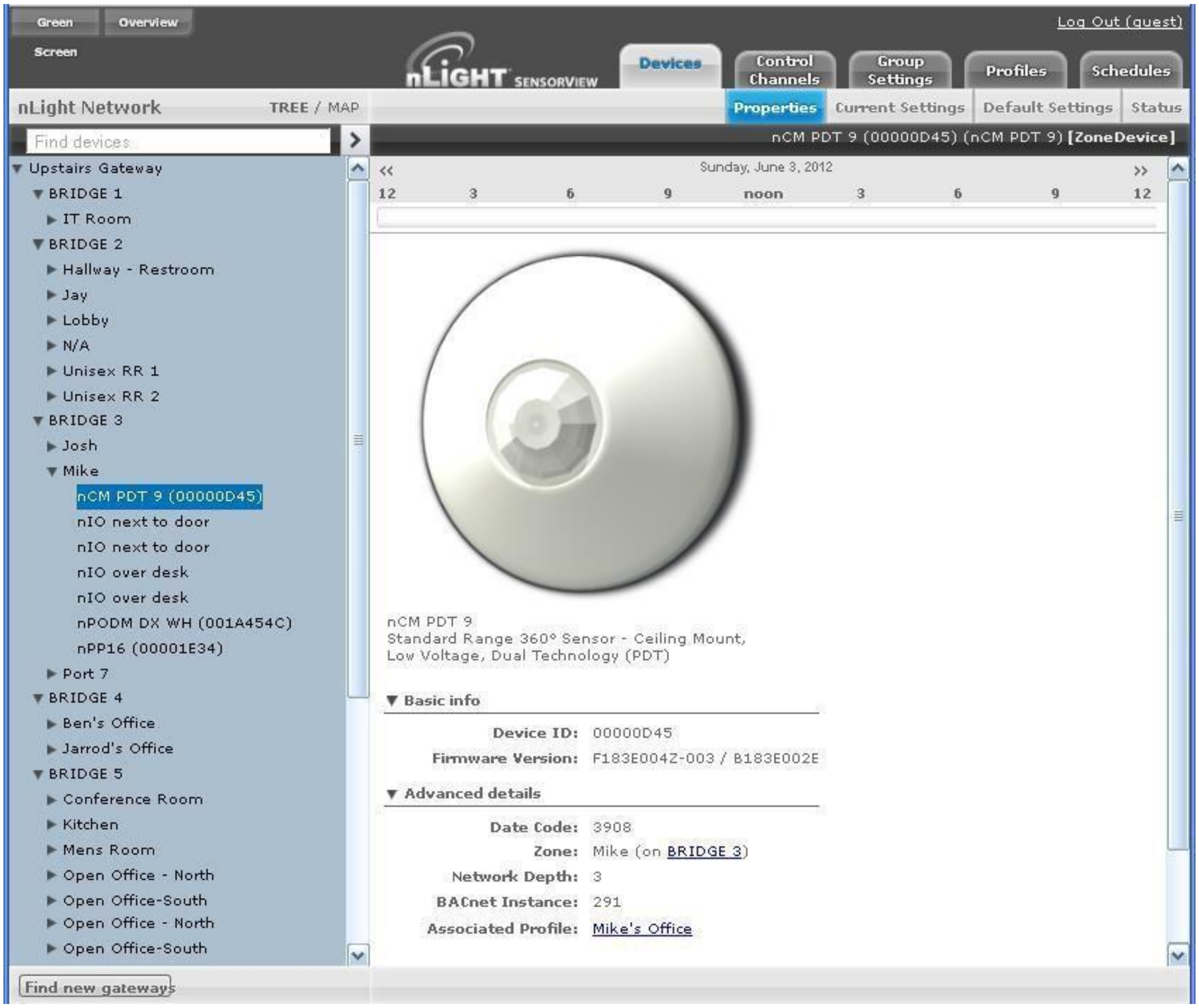
There are two primary ways to quickly locate a device: use the device **Search**, or the **prebuiltFeatures**.

1. **Device search (filter)** allows a user to immediately begin typing to search for the device (over device ID, model, or custom label), while
2. **Features** allows for a user to search for a device based on its
    - Hardware capabilities:
        - current-sensing, dimming-or-relay, occupancy, photocell, relay, switch, wireless
    - Profiles
        - Select by Profile name
    - Device state
        - error, normal, offline, warning

Note that any device matched and displayed will automatically cause the parent zone, bridge, and gateway to be displayed. When operating in MultiSelect (link) mode, clicking on the parent nodes will select all the currently visible child nodes, and will omit the ones that have been filtered out.

View Device State

For any device selected from the Device Tree (left), SensorView displays data in real time by selecting one of the available tabs: **Properties**, **Current Settings**, **Default Settings**, and **Status**. This example shows the readings from one of the **n**Light **C**eiling-**M**ount, **P**assive **D**ual-**T**echnology sensors covering approximately an area of **9** meters in diameter (**nCM PDT 9**) in the Zone called “Mike”, which has been selected from the device tree menu.



nCM PDT 9
Standard Range 360° Sensor - Ceiling Mount,
Low Voltage, Dual Technology (PDT)

▼ Basic info

Device ID: 00000D45
Firmware Version: F183E004Z-003 / B183E002E

▼ Advanced details

Date Code: 3908
Zone: Mike (on BRIDGE 3)
Network Depth: 3
BACnet Instance: 291
Associated Profile: Mike's Office

There are 6 possible states that an nLight device can be in. These different generally indicate some sort of operational problem with a device.

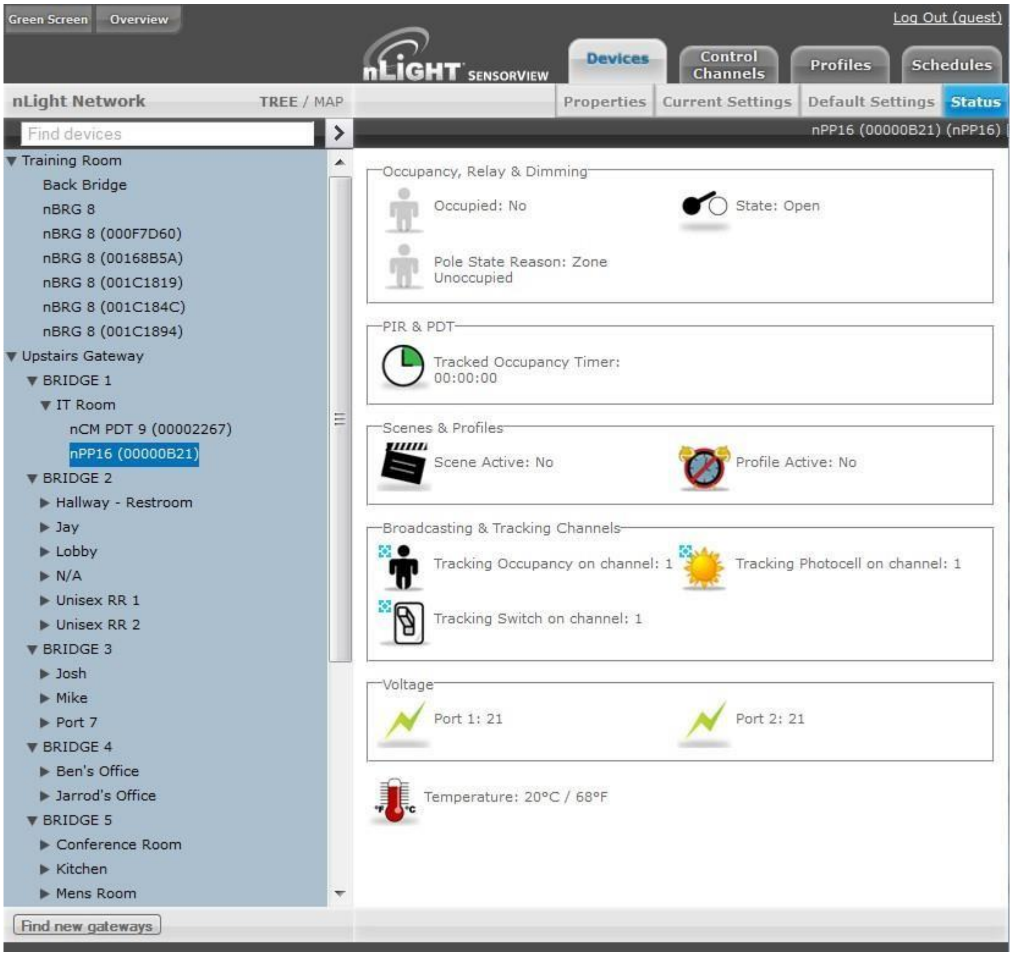
Note: *“Device State” (shown below) is not the same as Device Status. Individual device types can have various “status” conditions, depending on their functions.*

- **Offline** – The device is no longer online, check that the device is properly connected

- **Out of Range** – The device is online, but communication is restricted due to insufficient signal strength. This applies to **nWiFi** devices only. Signal strength for wireless may vary under certain conditions. Devices downstream from an **nWiFi** device may also appear Out of Range, if the parent is.
- **Bootstrap** – The device failed a firmware update and is in bootloader. Any relay or dimming output will be toggled on, but the device will not respond to any operational changes. Update the device to resolve this.
- **Misread** – Some properties of the device were not read by the gateway. To resolve state, goto the device and select "Rediscover" or use Group Select->Rediscover
- **Incompatible** – SensorView is not compatible with this device and is unable to configure it. Upgrade the device to resolve this.
- **Mismatched** – SensorView has detected that the devices' settings do not match what is expected. Synchronize the device (either using SensorView or device's settings) to resolve.

View Device Status

The **Status Screen** displays the present state of any device selected in the left tree menu. Device types have different functions. The status pages display parameters specific to the type of device selected, indicated by icons easily seen at glance.



Occupancy, Relay & Dimming

Occupied: No

State: Open

Pole State Reason: Zone Unoccupied

PIR & PDT

Tracked Occupancy Timer: 00:00:00

Scenes & Profiles

Scene Active: No

Profile Active: No

Broadcasting & Tracking Channels

Tracking Occupancy on channel: 1

Tracking Photocell on channel: 1

Tracking Switch on channel: 1

Voltage

Port 1: 21

Port 2: 21

Temperature: 20°C / 68°F

The current state of the device for each parameter (icon) is also displayed in readable text, which may include additional information on the particular status of the parameter within the selected device.

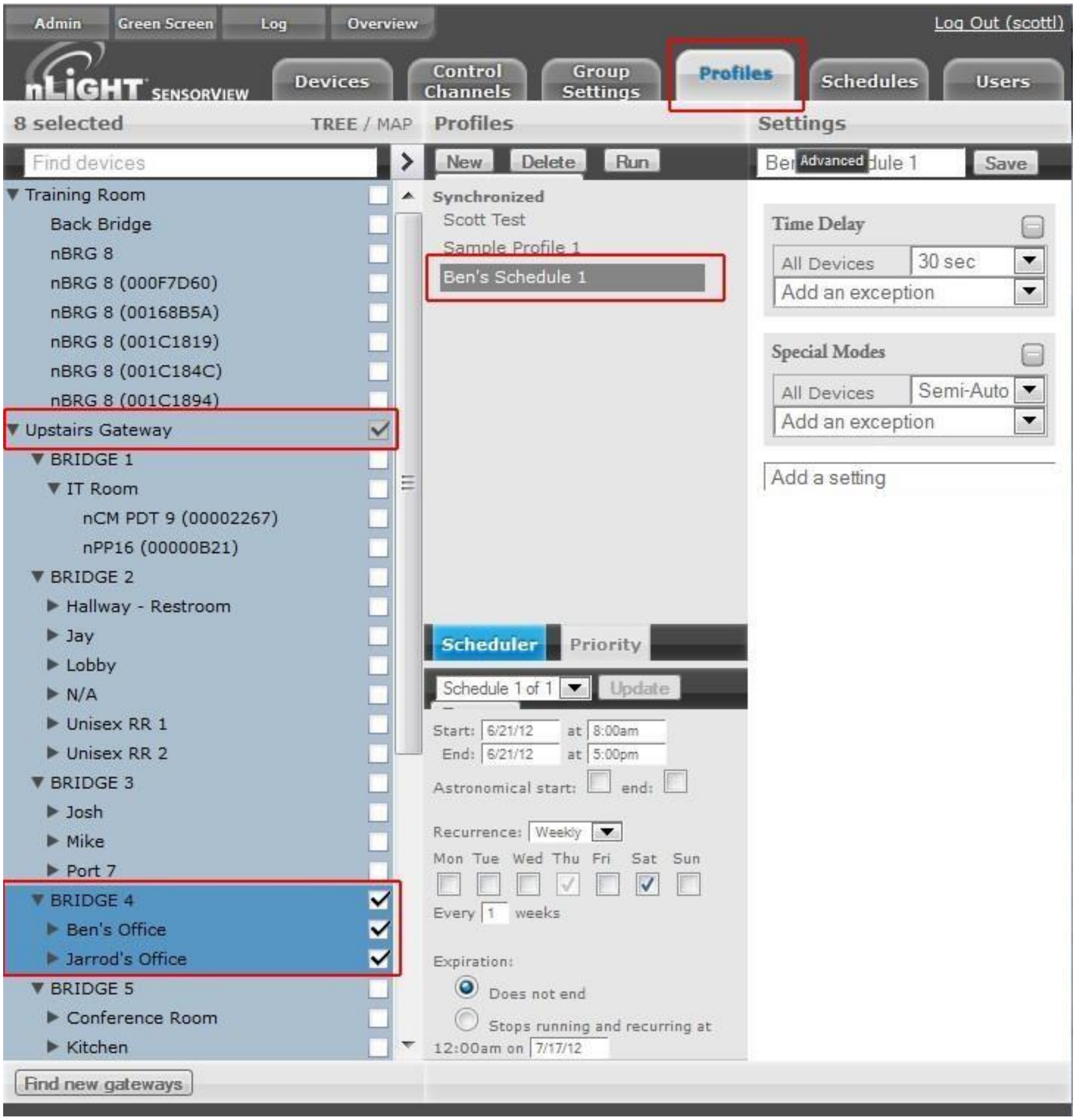
For a complete guide to Status Icons or possible conditions for a given device parameter, visit the Status Icon Glossary.

Selecting Multiple Devices

In certain contexts the Device Tree will allow for users to select multiple devices, rather than just one. This mode of selection is available on **Group Settings**, **Profiles**, **Global Channels**, or **Users**. This mode of selection greatly enhances the ability to quickly create system schedules, permissions, or make wholesale changes to device settings.

To select multiple devices:

- □ Check multiple boxes, each new device will be added to the selection. Checking a selected device a second time will remove it from the grouping.
- □ Check a Zone / Bridge / Gateway to select all of the devices within that group. Check that grouping structure a second time to deselect all devices within that Zone / Bridge / Gateway group.



Ben's Schedule 1

Time Delay: All Devices 30 sec

Special Modes: All Devices Semi-Auto

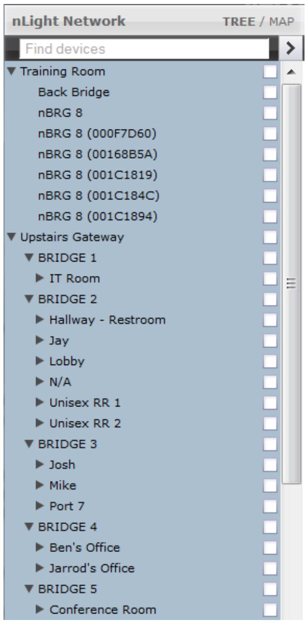
Start: 6/21/12 at 8:00am
End: 6/21/12 at 5:00pm
Astronomical start: □ end: □

Recurrence: Weekly
Mon □ Tue □ Wed □ Thu □ Fri □ Sat ☑ Sun □
Every 1 weeks

Expiration:
● Does not end
○ Stops running and recurring at 12:00am on 7/17/12

Selecting multiple devices is useful when large amounts of devices are to be operated on simultaneously. **Profiles, Users**, **Group Settings** and **Global Channels** all support multiple device selection. All other modes operate in single select, such that selecting any item in the tree displays information specific to that device.

None Selected (empty Checkboxes)

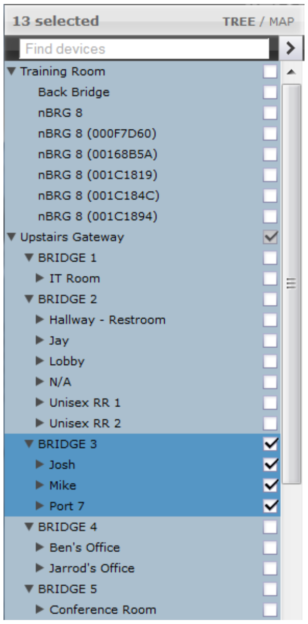


nLight Network TREE / MAP

Find devices

- ▼ Training Room ☐
  - Back Bridge ☐
  - nBRG 8 ☐
  - nBRG 8 (000F7D60) ☐
  - nBRG 8 (00168B5A) ☐
  - nBRG 8 (001C1819) ☐
  - nBRG 8 (001C184C) ☐
  - nBRG 8 (001C1894) ☐
- ▼ Upstairs Gateway ☐
  - ▼ BRIDGE 1 ☐
    - ▶ IT Room ☐
  - ▼ BRIDGE 2 ☐
    - ▶ Hallway - Restroom ☐
    - ▶ Jay ☐
    - ▶ Lobby ☐
    - ▶ N/A ☐
    - ▶ Unisex RR 1 ☐
    - ▶ Unisex RR 2 ☐
  - ▼ BRIDGE 3 ☐
    - ▶ Josh ☐
    - ▶ Mike ☐
    - ▶ Port 7 ☐
  - ▼ BRIDGE 4 ☐
    - ▶ Ben's Office ☐
    - ▶ Jarrod's Office ☐
  - ▼ BRIDGE 5 ☐
    - ▶ Conference Room ☐

Bridge Selected (Parent gateway checked in gray)

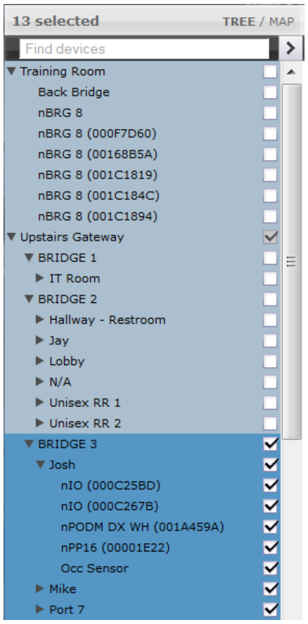


13 selected TREE / MAP

Find devices

- ▼ Training Room ☐
  - Back Bridge ☐
  - nBRG 8 ☐
  - nBRG 8 (000F7D60) ☐
  - nBRG 8 (00168B5A) ☐
  - nBRG 8 (001C1819) ☐
  - nBRG 8 (001C184C) ☐
  - nBRG 8 (001C1894) ☐
- ▼ Upstairs Gateway ☑
  - ▼ BRIDGE 1 ☐
    - ▶ IT Room ☐
  - ▼ BRIDGE 2 ☐
    - ▶ Hallway - Restroom ☐
    - ▶ Jay ☐
    - ▶ Lobby ☐
    - ▶ N/A ☐
    - ▶ Unisex RR 1 ☐
    - ▶ Unisex RR 2 ☐
  - ▼ BRIDGE 3 ☑
    - ▶ Josh ☑
    - ▶ Mike ☑
    - ▶ Port 7 ☑
  - ▼ BRIDGE 4 ☐
    - ▶ Ben's Office ☐
    - ▶ Jarrod's Office ☐
  - ▼ BRIDGE 5 ☐
    - ▶ Conference Room ☐

Zone expanded. All zone devices checked

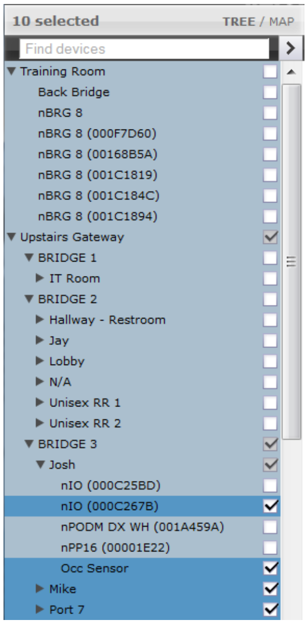


13 selected TREE / MAP

Find devices

- ▼ Training Room ☐
  - Back Bridge ☐
  - nBRG 8 ☐
  - nBRG 8 (000F7D60) ☐
  - nBRG 8 (00168B5A) ☐
  - nBRG 8 (001C1819) ☐
  - nBRG 8 (001C184C) ☐
  - nBRG 8 (001C1894) ☐
- ▼ Upstairs Gateway ☑
  - ▼ BRIDGE 1 ☐
    - ▶ IT Room ☐
  - ▼ BRIDGE 2 ☐
    - ▶ Hallway - Restroom ☐
    - ▶ Jay ☐
    - ▶ Lobby ☐
    - ▶ N/A ☐
    - ▶ Unisex RR 1 ☐
    - ▶ Unisex RR 2 ☐
  - ▼ BRIDGE 3 ☑
    - ▼ Josh ☑
      - nIO (000C25BD) ☑
      - nIO (000C267B) ☑
      - nPODM DX WH (001A459A) ☑
      - nPP16 (00001E22) ☑
      - Occ Sensor ☑
    - ▶ Mike ☑
    - ▶ Port 7 ☑

Specific zone devices unchecked



10 selected TREE / MAP

Find devices

- ▼ Training Room ☐
  - Back Bridge ☐
  - nBRG 8 ☐
  - nBRG 8 (000F7D60) ☐
  - nBRG 8 (00168B5A) ☐
  - nBRG 8 (001C1819) ☐
  - nBRG 8 (001C184C) ☐
  - nBRG 8 (001C1894) ☐
- ▼ Upstairs Gateway ☑
  - ▼ BRIDGE 1 ☐
    - ▶ IT Room ☐
  - ▼ BRIDGE 2 ☐
    - ▶ Hallway - Restroom ☐
    - ▶ Jay ☐
    - ▶ Lobby ☐
    - ▶ N/A ☐
    - ▶ Unisex RR 1 ☐
    - ▶ Unisex RR 2 ☐
  - ▼ BRIDGE 3 ☑
    - ▼ Josh ☑
      - nIO (000C25BD) ☐
      - nIO (000C267B) ☑
      - nPODM DX WH (001A459A) ☐
      - nPP16 (00001E22) ☐
      - Occ Sensor ☑
    - ▶ Mike ☑
    - ▶ Port 7 ☑

Updating SensorView

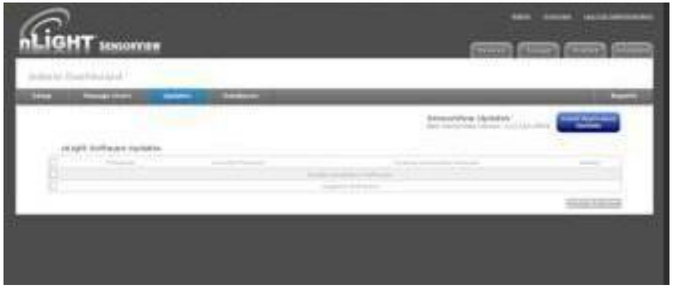
Please note that the following procedure *must* be done from the SensorView host computer, and cannot be initiated over the web; administrator credentials on the host are also required.

Note: *Always retrieve the latest installer to perform the actual update, on occasion SensorView updates will require subsequent device updates, should this occur the installer will warn you before proceeding with the update.*

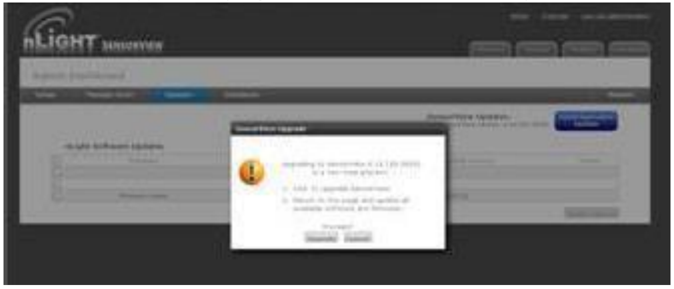
Depending on the currently installed version of SensorView the steps to update the software may vary, for all versions less than 7.0, follow steps **A** and **B**. Otherwise, proceed to step **B**.

A. Updating to 6.14:

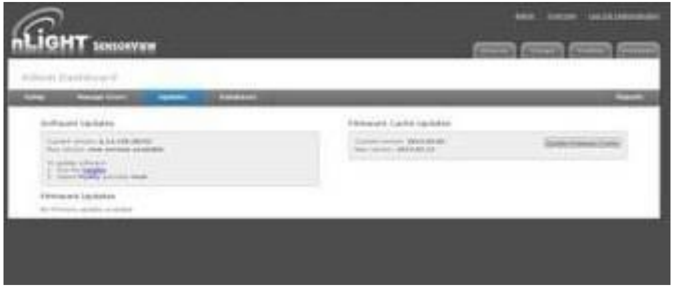
1. Visit **Updates** page in SensorView & initiate upgrade to *6.12.xx:*



2. Return to the **Updates** page & initiate upgrade to *6.14.xx.*
3. Return to **Updates** page & run all available updates on firmware:

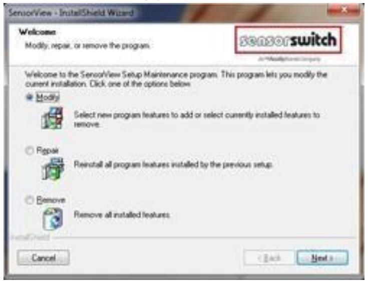


4. Return to **Updates** page & follow instructions to update to *7.x.x*:



B. Updating to the latest version:

1. Download SensorView installer and run *Setup.exe*
2. Select ***Modify*** when offered and follow the prompts.

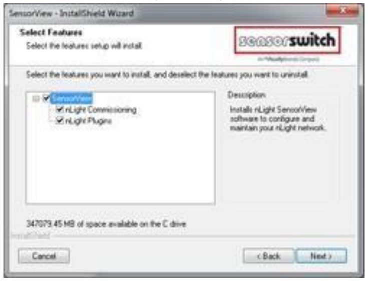

SensorView - InstallShield Wizard
Welcome
Modify, repair, or remove the program.
sensorswitch
Cancel
< Back
Next >

Welcome to the SensorView Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

● Modify
Select new program features to add or select currently installed features to remove.

○ Repair
Reinstall all program features installed by the previous setup.

○ Remove
Remove all installed features.

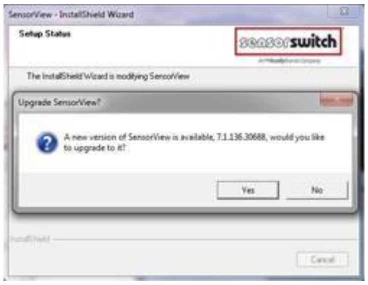

SensorView - InstallShield Wizard
Select Features
Select the features setup will install.
sensorswitch
Cancel
< Back
Next >

Select the features you want to install, and deselect the features you want to uninstall.

☑ SensorView
☑ nLight Commissioning
☑ nLight Plugins

Description
Installs nLight SensorView software to configure and maintain your nLight network.

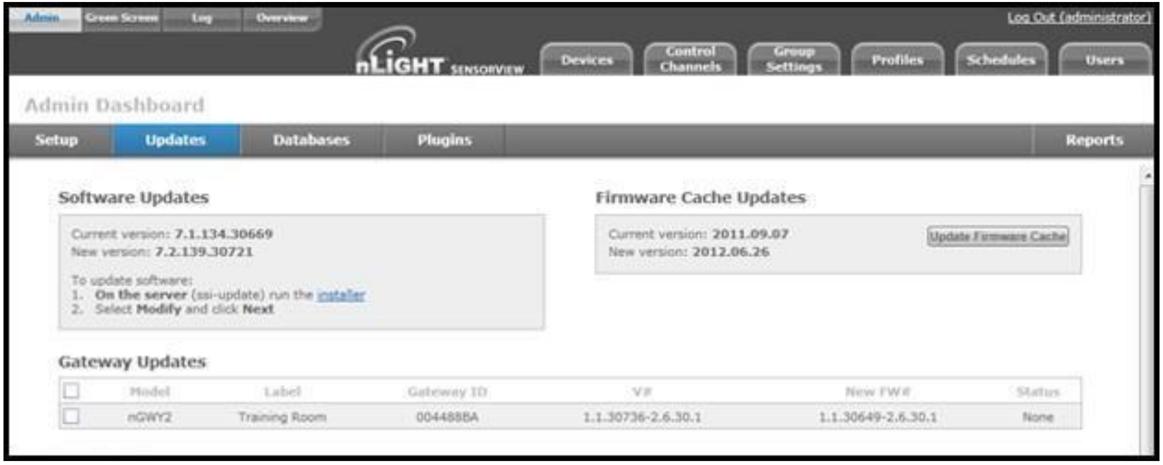
347079.45 MB of space available on the C drive



The InstallShield Wizard is modifying SensorView

A new version of SensorView is available, 7.1.136.30688, would you like to upgrade to it?

3. Return to **Updates** page & run all available firmware updates.



Software Updates

Current version: **7.1.134.30669**
New version: **7.2.139.30721**

To update software:
1. **On the server** (ssi-update) run the installer
2. Select **Modify** and click **Next**

Firmware Cache Updates

Current version: **2011.09.07**
New version: **2012.06.26**

Gateway Updates

□	Model	Label	Gateway ID	V#	New FW#	Status
□	nGWY2	Training Room	004488BA	1.1.30736-2.6.30.1	1.1.30649-2.6.30.1	None

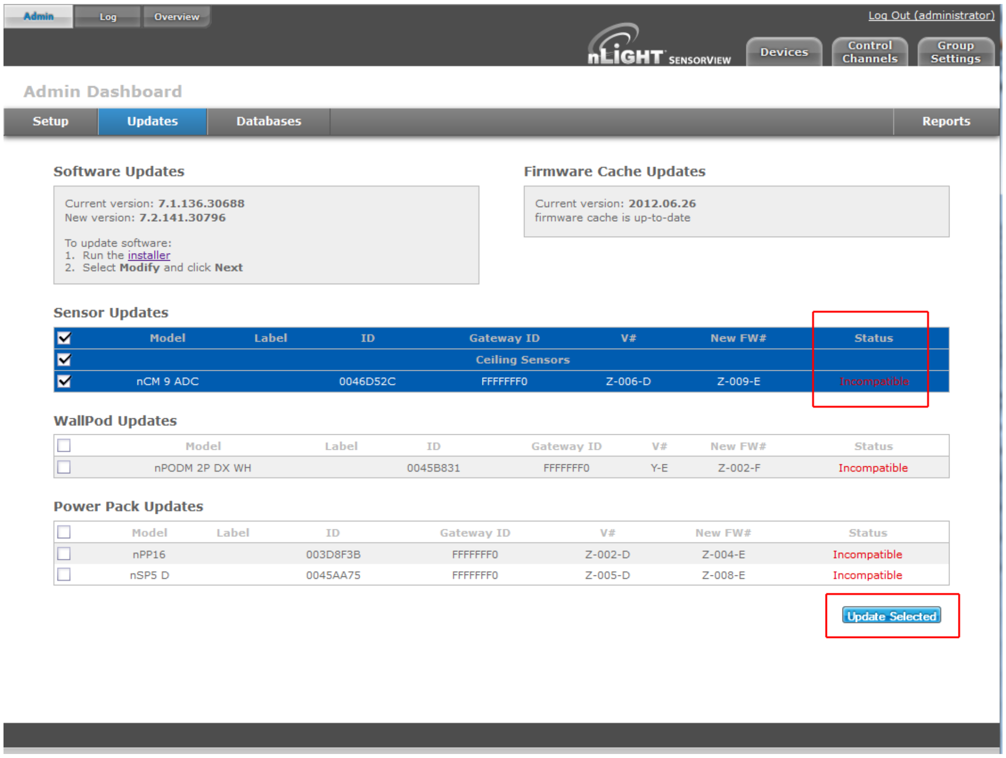
Downgrading to Version 6.12.x

If you need to return to SensorView Version 6.12 for any reason, run the 6.12.x installer. Note that you will have to uninstall the current version of SensorView beforehand.

Updating Device Firmware

Select the **Admin** button at upper left, then select the **Updates** tab to view all available updates. Devices will be omitted from the listing if they are currently up to date.

SensorView will retrieve the latest firmware for each device from the internet. If youare not going to have internet then download and install the firmware cache (top right), which will allow firmware updates to be performed offline.



Software Updates

Current version: **7.1.136.30688**
New version: **7.2.141.30796**

To update software:
1. Run the installer
2. Select **Modify** and click **Next**

Firmware Cache Updates

Current version: **2012.06.26**
firmware cache is up-to-date

Sensor Updates

☑	Model	Label	ID	Gateway ID	V#	New FW#	Status
☑	Ceiling Sensors						
☑	nCM 9 ADC		0046D52C	FFFFFFF0	Z-006-D	Z-009-E	Incompatible

WallPod Updates

□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□	nPODM 2P DX WH		0045B831	FFFFFFF0	Y-E	Z-002-F	Incompatible

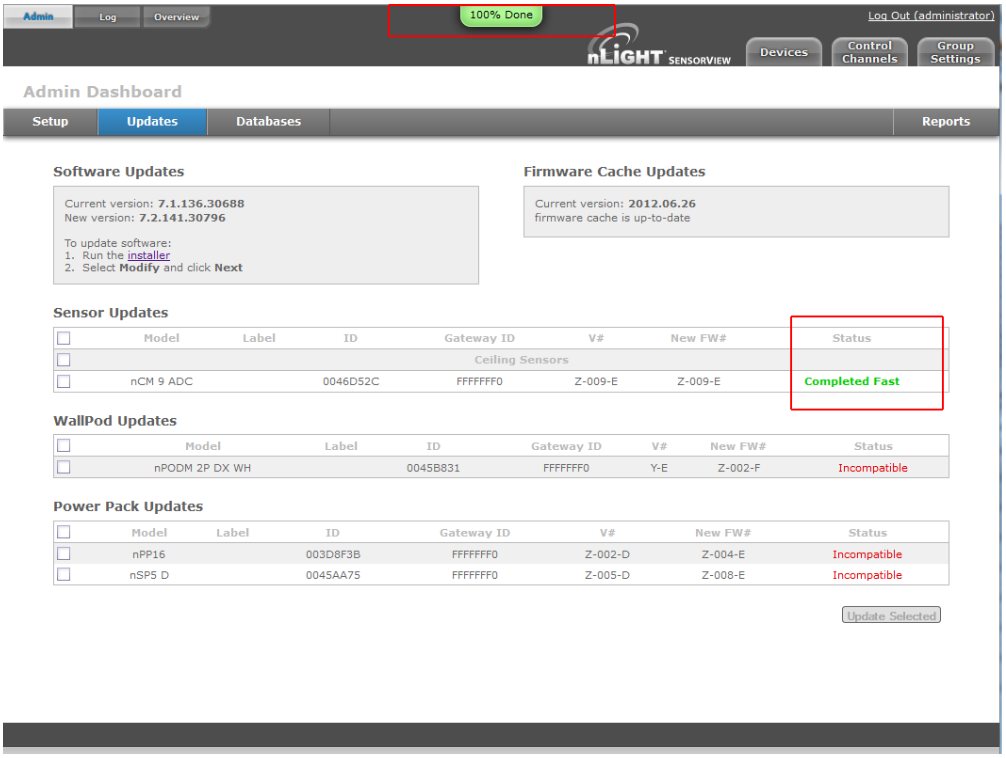
Power Pack Updates

□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□	nPP16		003D8F3B	FFFFFFF0	Z-002-D	Z-004-E	Incompatible
□	nSP5 D		0045AA75	FFFFFFF0	Z-005-D	Z-008-E	Incompatible

The status of the update is displayed in the rightmost column of the blue Status bars, and also at the top center of the screen:

1. Status: **Pending** while "**Preparing to update firmware …**"
2. Status: **In Progress** while "**Updating firmware: X% done**"
3. Status: **Completed Fast** when "**100% Done**"

While firmware is being updated by the system, the actual physical device will display a very fast blink of its green status light, as well as closing relays and dimming to full bright, as appropriate. As the process nears completion, the device will display a slow, blinking pattern. After a few minutes, the device status light will return to normal.



Admin Dashboard

Software Updates

Current version: **7.1.136.30688**
New version: **7.2.141.30796**

To update software:
1. Run the installer
2. Select **Modify** and click **Next**

Firmware Cache Updates

Current version: **2012.06.26**
firmware cache is up-to-date

Sensor Updates

□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□				Ceiling Sensors			
□	nCM 9 ADC		0046D52C	FFFFFFF0	Z-009-E	Z-009-E	Completed Fast

WallPod Updates

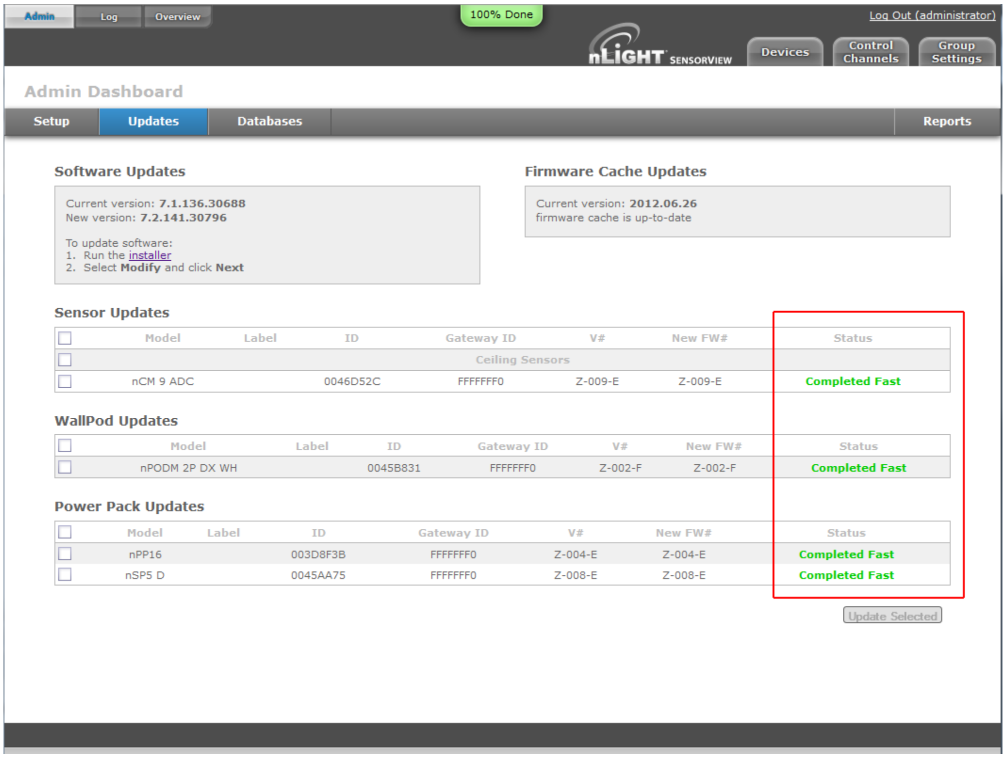
□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□	nPODM 2P DX WH		0045B831	FFFFFFF0	Y-E	Z-002-F	Incompatible

Power Pack Updates

□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□	nPP16		003D8F3B	FFFFFFF0	Z-002-D	Z-004-E	Incompatible
□	nSP5 D		0045AA75	FFFFFFF0	Z-005-D	Z-008-E	Incompatible

Repeat this process for all devices by selecting any and all (at once) which require firmware updates.

When all devices have been updated, the red Incompatible conditions on the screen will bereplaced by **Completed Fast**.



Software Updates

Current version: **7.1.136.30688**
New version: **7.2.141.30796**

To update software:
1. Run the installer
2. Select **Modify** and click **Next**

Firmware Cache Updates

Current version: **2012.06.26**
firmware cache is up-to-date

Sensor Updates

□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□	Ceiling Sensors						
□	nCM 9 ADC		0046D52C	FFFFFFF0	Z-009-E	Z-009-E	Completed Fast

WallPod Updates

□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□	nPODM 2P DX WH		0045B831	FFFFFFF0	Z-002-F	Z-002-F	Completed Fast

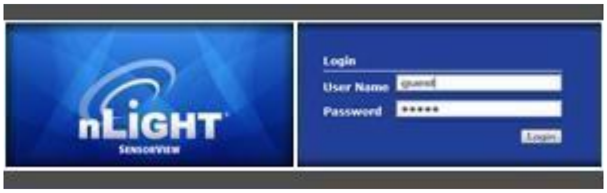
Power Pack Updates

□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□	nPP16		003D8F3B	FFFFFFF0	Z-004-E	Z-004-E	Completed Fast
□	nSP5 D		0045AA75	FFFFFFF0	Z-008-E	Z-008-E	Completed Fast

Logging in

Navigate to the SensorView login screen via the Start Menu, desktop shortcut, or by directly typing the address into the web browser (note: address requires entering the Host Specific Computer Name, which is installation specific):

http://<Host Computer Name>/SensorView



Login
User Name: guest
Password: *****

Enter your *case sensitive* username and password. Default login is:
Username: **administrator**
Password: **admin**

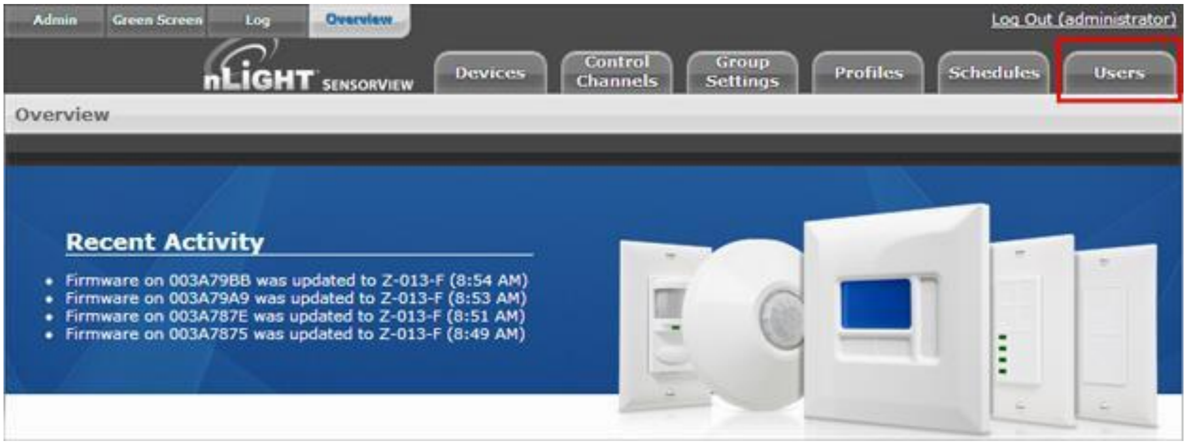
If you have forgotten or do not have your login information, please contact your network administrator.

Administrative Tasks

Only administrative users have authority to perform these tasks, which involve modifying / creating users, as well as modifying properties on the Gateway & Location pages.

Creating:

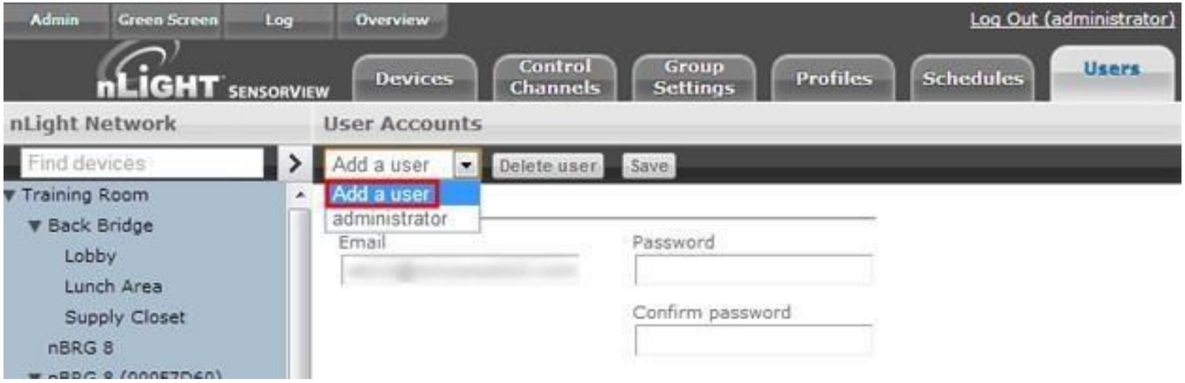
1. Click the ***Users*** tab



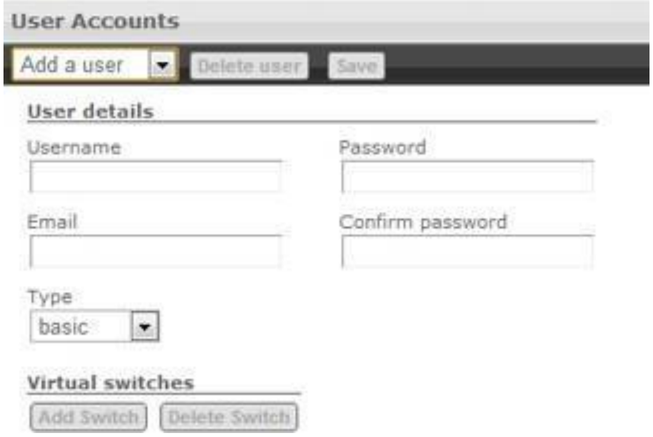
Recent Activity

- Firmware on 003A79BB was updated to Z-013-F (8:54 AM)
- Firmware on 003A79A9 was updated to Z-013-F (8:53 AM)
- Firmware on 003A787E was updated to Z-013-F (8:51 AM)
- Firmware on 003A7875 was updated to Z-013-F (8:49 AM)

2. Select ***Add a User*** from the dropdown



3. Fill out all fields, making sure to set the appropriate access level.



Username

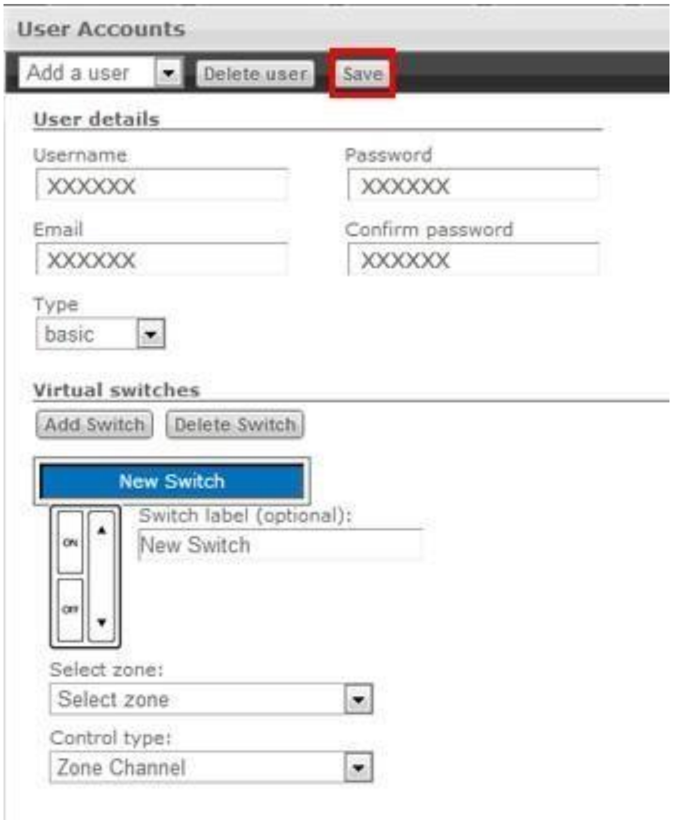
Password

Email

Confirm password

Type: basic

4. Click ***Save***



Username: XXXXXX

Password: XXXXXX

Email: XXXXXX

Confirm password: XXXXXX

Type: basic

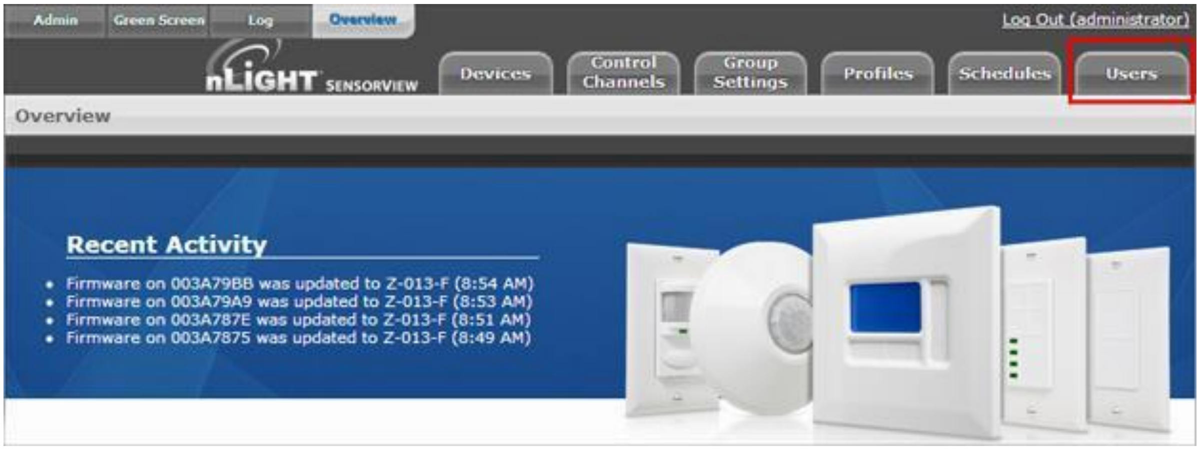
Switch label (optional): New Switch

Select zone: Select zone

Control type: Zone Channel

Modifying:

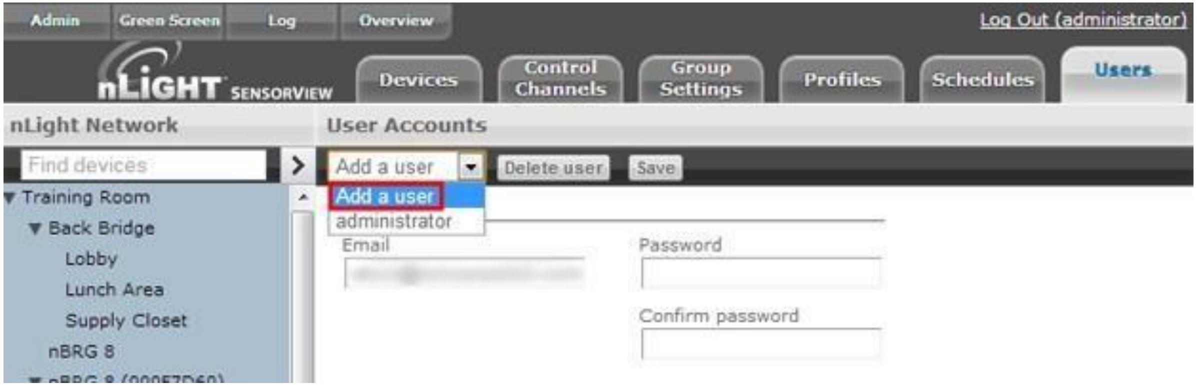
1. Click the ***Users*** tab



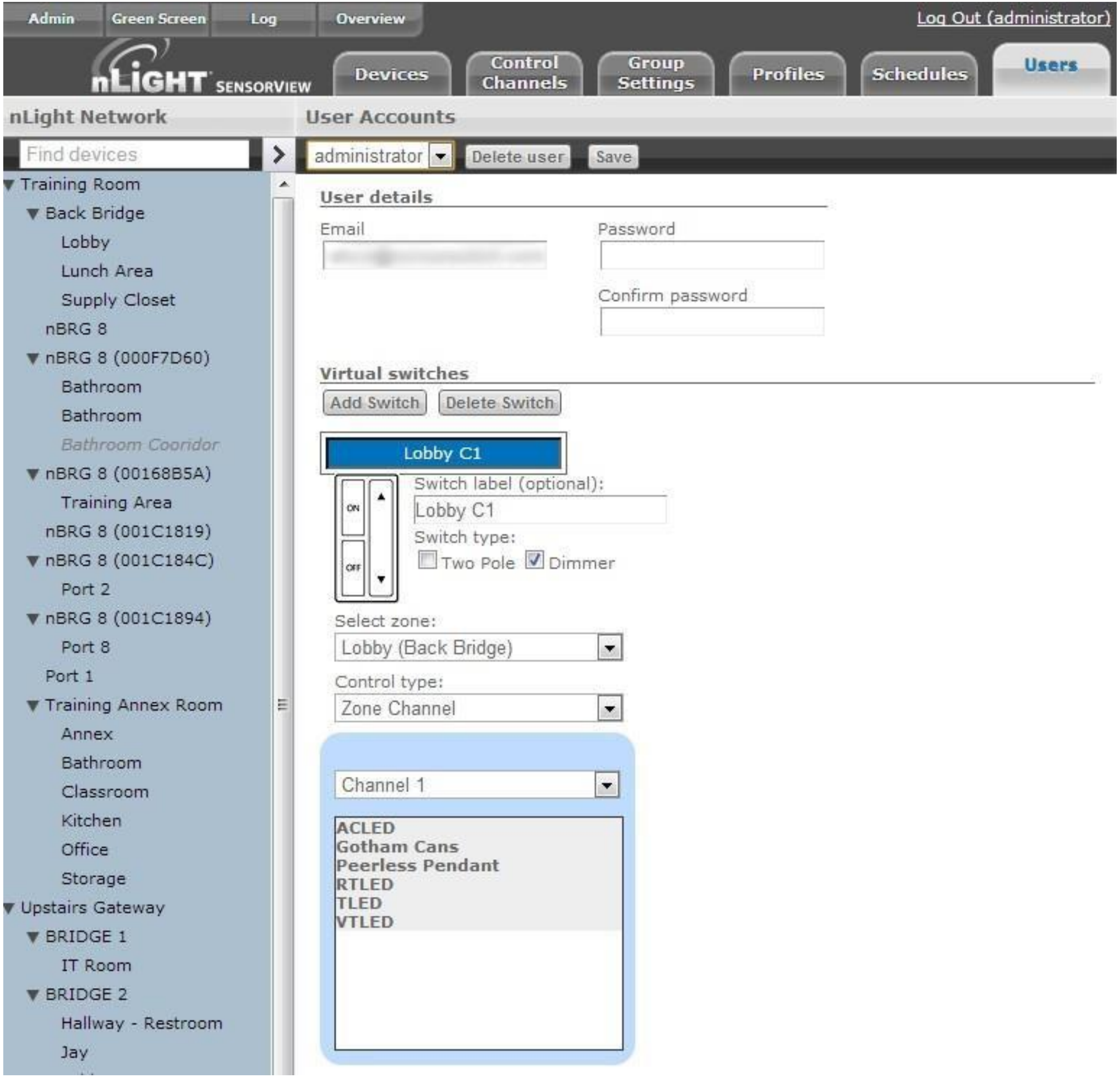
Recent Activity

- Firmware on 003A79BB was updated to Z-013-F (8:54 AM)
- Firmware on 003A79A9 was updated to Z-013-F (8:53 AM)
- Firmware on 003A787E was updated to Z-013-F (8:51 AM)
- Firmware on 003A7875 was updated to Z-013-F (8:49 AM)

2. Select user from the dropdown



3. Change the appropriate information



Training Room
Back Bridge
Lobby
Lunch Area
Supply Closet
nBRG 8
nBRG 8 (000F7D60)
Bathroom
Bathroom
Bathroom Cooridor
nBRG 8 (00168B5A)
Training Area
nBRG 8 (001C1819)
nBRG 8 (001C184C)
Port 2
nBRG 8 (001C1894)
Port 8
Port 1
Training Annex Room
Annex
Bathroom
Classroom
Kitchen
Office
Storage
Upstairs Gateway
BRIDGE 1
IT Room
BRIDGE 2
Hallway - Restroom
Jay

administrator

User details

Email: [redacted]

Password:

Confirm password:

Virtual switches

Lobby C1

Switch label (optional): Lobby C1

Switch type: □ Two Pole ☑ Dimmer

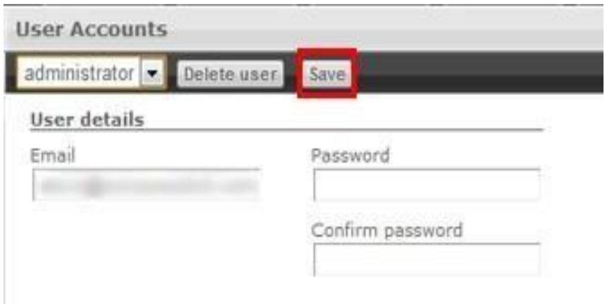
Select zone: Lobby (Back Bridge)

Control type: Zone Channel

Channel 1

ACLED
Gotham Cans
Peerless Pendant
RTLED
TLED
VTLED

4. Click ***Save***



administrator

User details

Email: [redacted]

Password:

Confirm password:

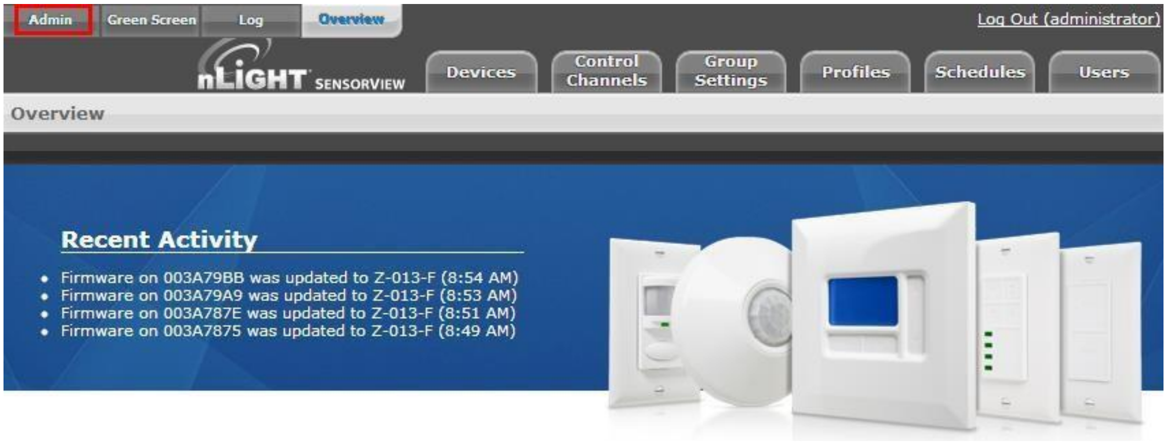
Gateway Page

The Gateways tab allows operators to manage the nGWY devices that are currently managed by SensorView. nGWY devices running on the same IP Subnet will be discovered automatically by SensorView; any nGWYs that reside on different segments of the IP network can be added by simply entering their IP address on the Gateways tab.

Note: Discovering nGWY devices on different segments of the IP network may require for firewalls and routers to be updated to allow access to the necessary ports.

Including / Excluding Gateways:

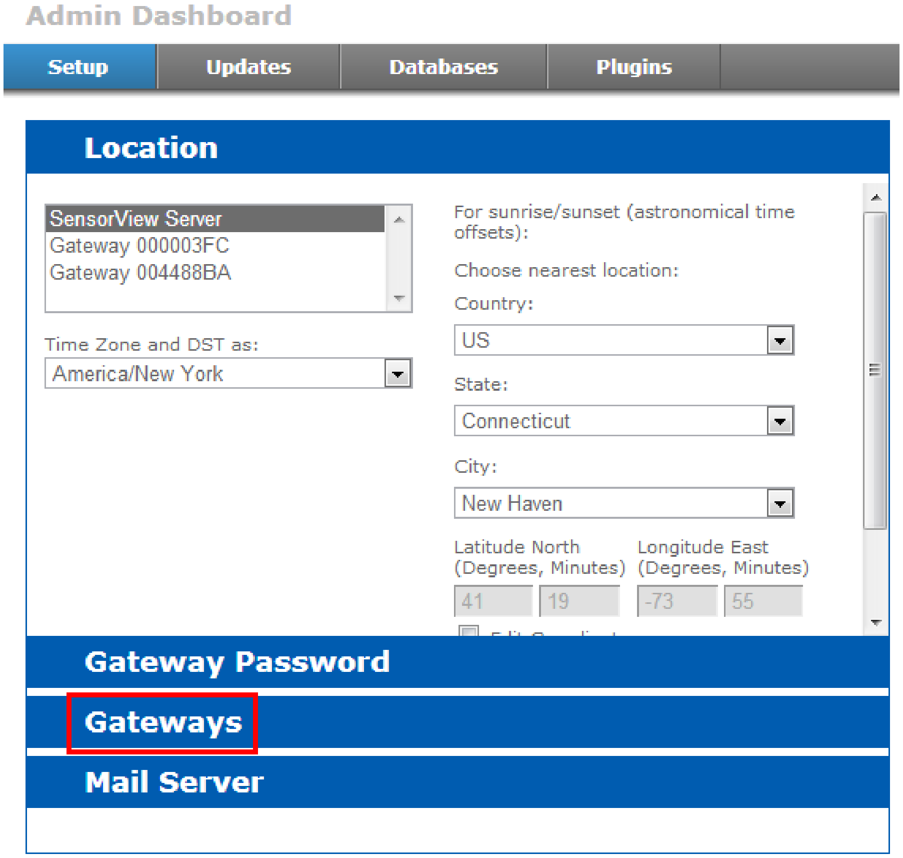
1. Click the ***Admin*** tab



Recent Activity

- Firmware on 003A79BB was updated to Z-013-F (8:54 AM)
- Firmware on 003A79A9 was updated to Z-013-F (8:53 AM)
- Firmware on 003A787E was updated to Z-013-F (8:51 AM)
- Firmware on 003A7875 was updated to Z-013-F (8:49 AM)

2. Click the ***Gateways*** section to expand it



SensorView Server
Gateway 000003FC
Gateway 004488BA

Time Zone and DST as: America/New York

For sunrise/sunset (astronomical time offsets):

Choose nearest location:

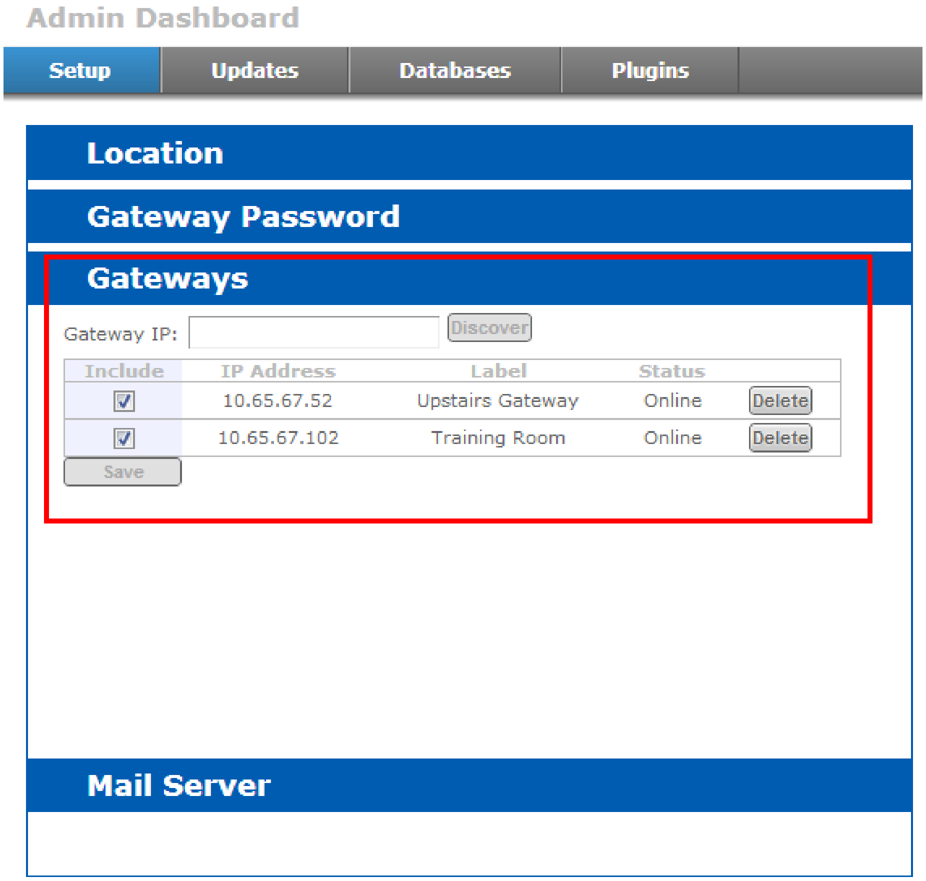
Country: US

State: Connecticut

City: New Haven

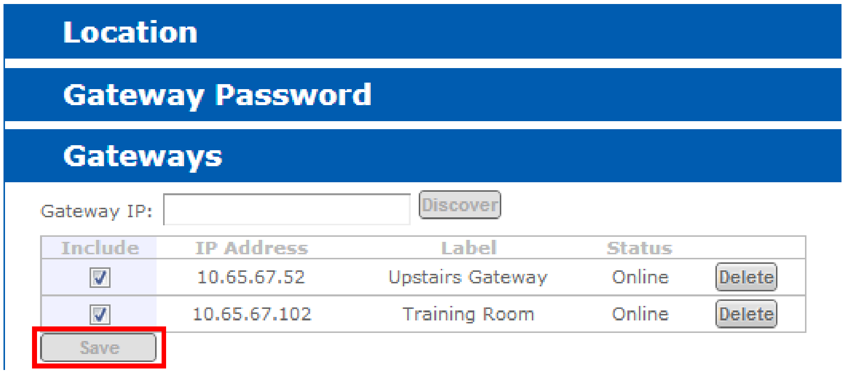
Latitude North (Degrees, Minutes)		Longitude East (Degrees, Minutes)	
41	19	-73	55

3. Make any changes to the existing list, such as whether or not to include a particular Gateway



Include	IP Address	Label	Status	
☑	10.65.67.52	Upstairs Gateway	Online	Delete
☑	10.65.67.102	Training Room	Online	Delete

4. Add IP addresses of any required Gateways not auto-detected (requires IP address).
5. Click ***Save*** to apply your changes



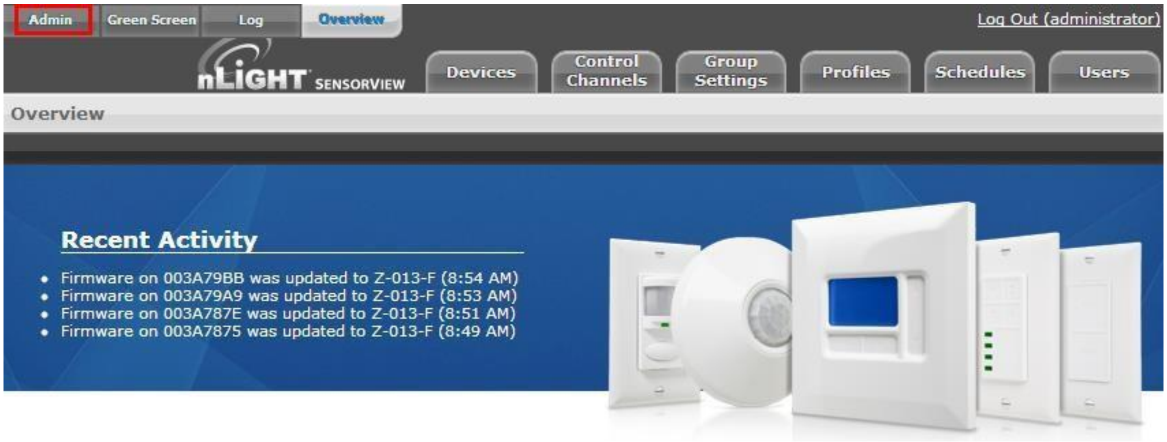
Include	IP Address	Label	Status	
☑	10.65.67.52	Upstairs Gateway	Online	Delete
☑	10.65.67.102	Training Room	Online	Delete

Location Page

Properly configuring the location for all nGWY devices and the SensorView host is required to ensure that all profiles will run at the proper time. Setting the time zone allows the nGWY devices to properly update their time throughout the course of the year as Daylight Savings Time comes into effect. The location parameters allow the nGWY devices and SensorView to properly compute the correct Sunrise and Sunset times for a given day.

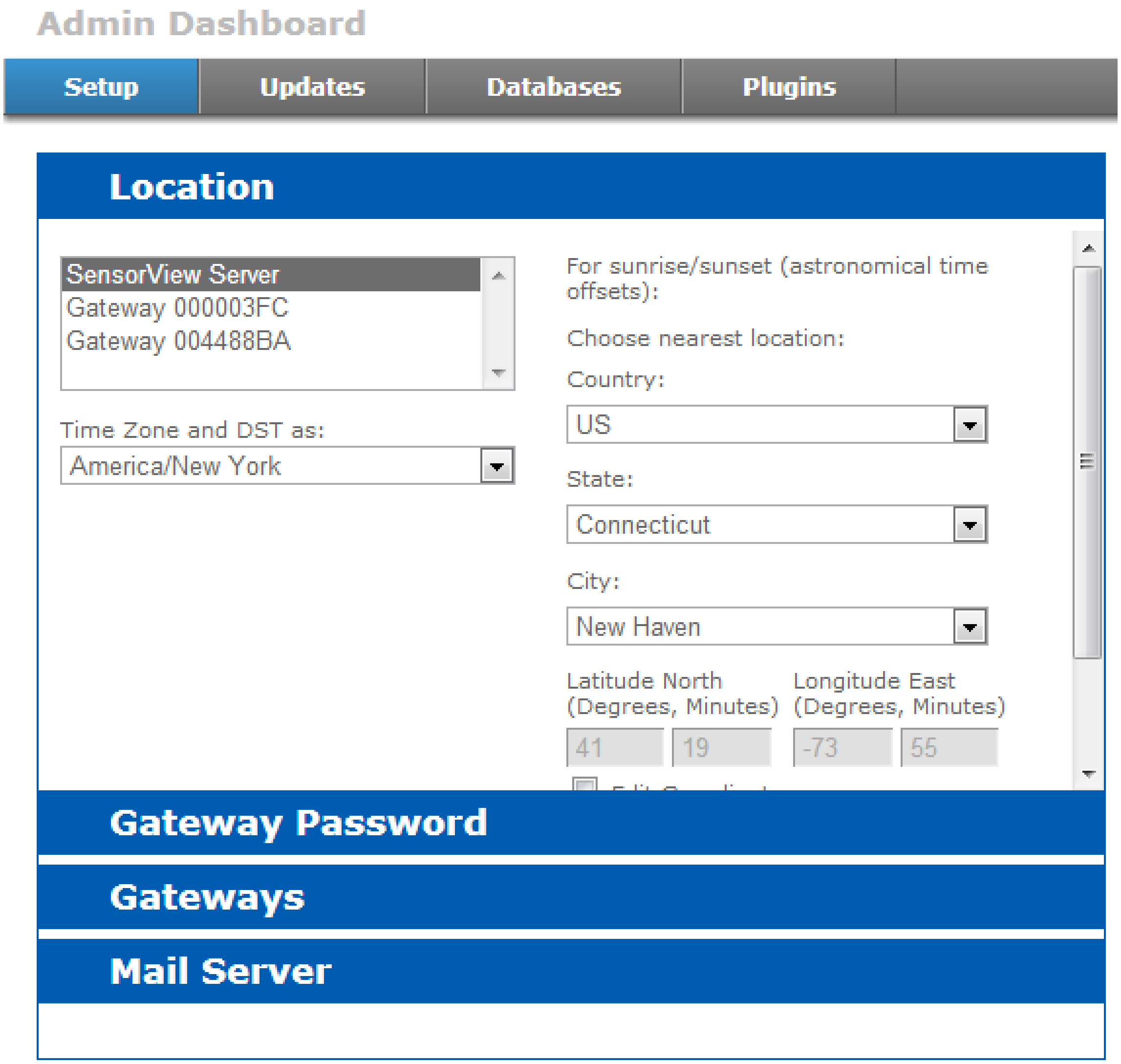
Viewing/Editing Gateway & Server Locations:

1. Click the ***Admin*** tab



- Firmware on 003A79BB was updated to Z-013-F (8:54 AM)
- Firmware on 003A79A9 was updated to Z-013-F (8:53 AM)
- Firmware on 003A787E was updated to Z-013-F (8:51 AM)
- Firmware on 003A7875 was updated to Z-013-F (8:49 AM)

2. The ***Setup*** tab should automatically load with the Location section expanded



SensorView Server
Gateway 000003FC
Gateway 004488BA

Time Zone and DST as: America/New York

For sunrise/sunset (astronomical time offsets):

Choose nearest location:

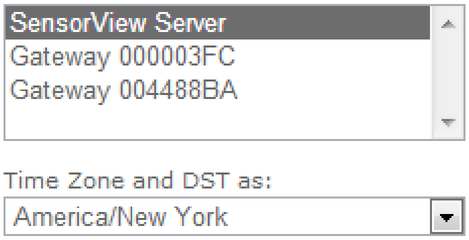
Country: US

State: Connecticut

City: New Haven

Latitude North (Degrees, Minutes)		Longitude East (Degrees, Minutes)	
41	19	-73	55

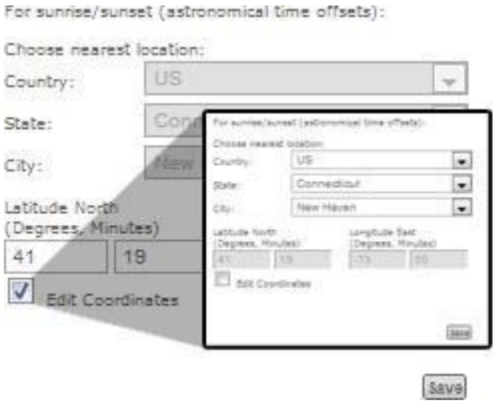
3. Click the Server or Gateway you wish to edit



SensorView Server
Gateway 000003FC
Gateway 004488BA

Time Zone and DST as: America/New York

4. Uncheck the ***Edit Coordinates*** box to edit the Country/State/City fields



For sunrise/sunset (astronomical time offsets):

Choose nearest location:

Country: US

State: Con

City: New

Latitude North (Degrees, Minutes): 41 19

☑ Edit Coordinates

For sunrise/sunset (astronomical time offsets):

Choose nearest location:

Country: US

State: Connecticut

City: New Haven

Latitude North (Degrees, Minutes): 41 19

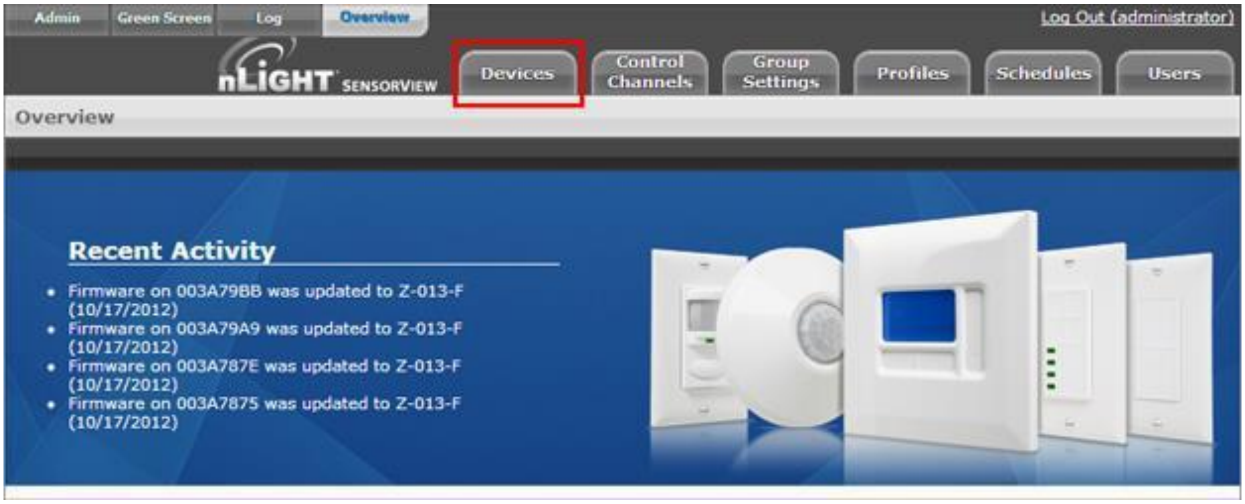
Longitude East (Degrees, Minutes): -73 55

□ Edit Coordinates

5. Click ***Save*** to apply your changes

View Device Properties

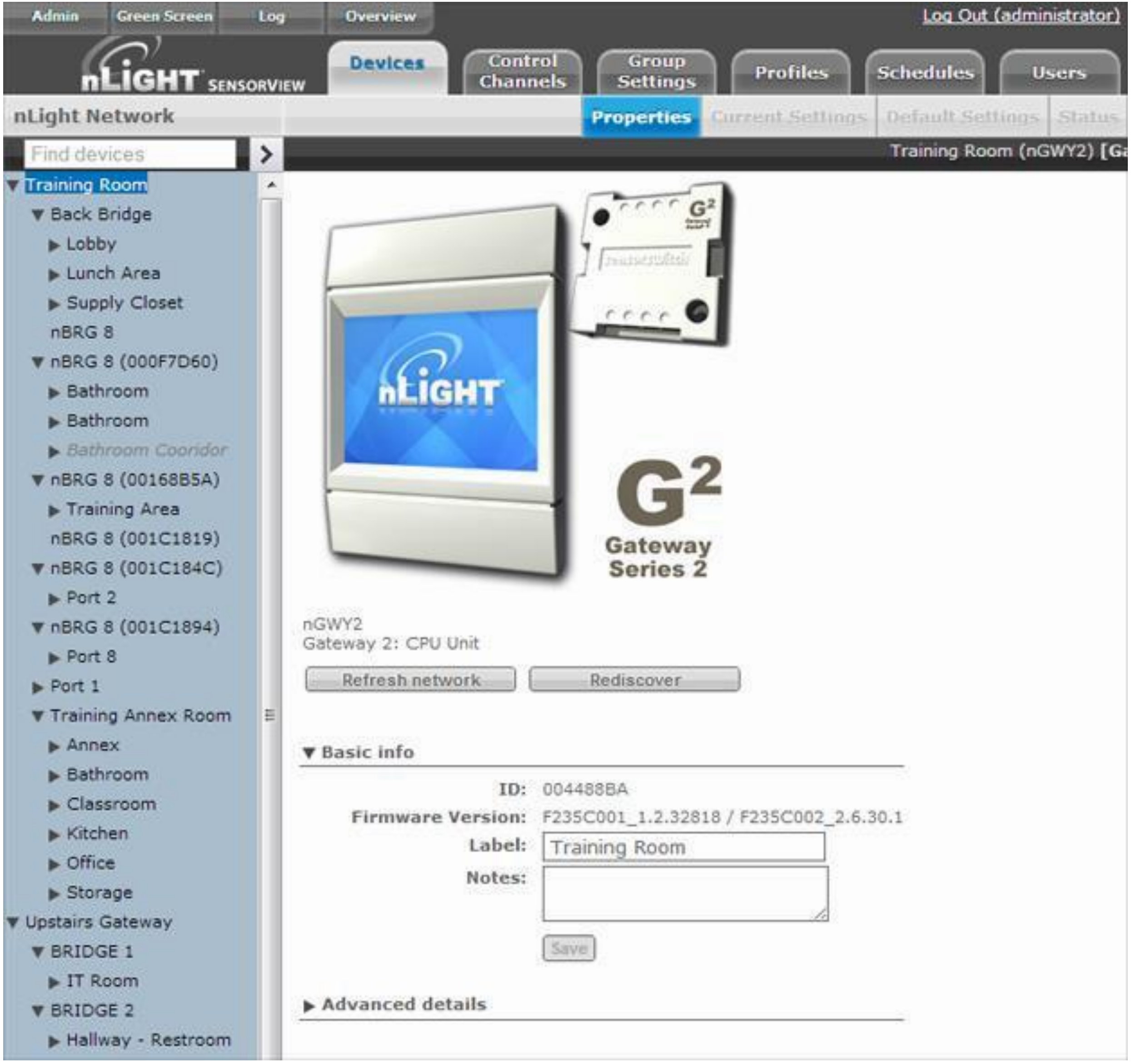
1. Click the ***Devices*** tab



Recent Activity

- Firmware on 003A79BB was updated to Z-013-F (10/17/2012)
- Firmware on 003A79A9 was updated to Z-013-F (10/17/2012)
- Firmware on 003A787E was updated to Z-013-F (10/17/2012)
- Firmware on 003A7875 was updated to Z-013-F (10/17/2012)

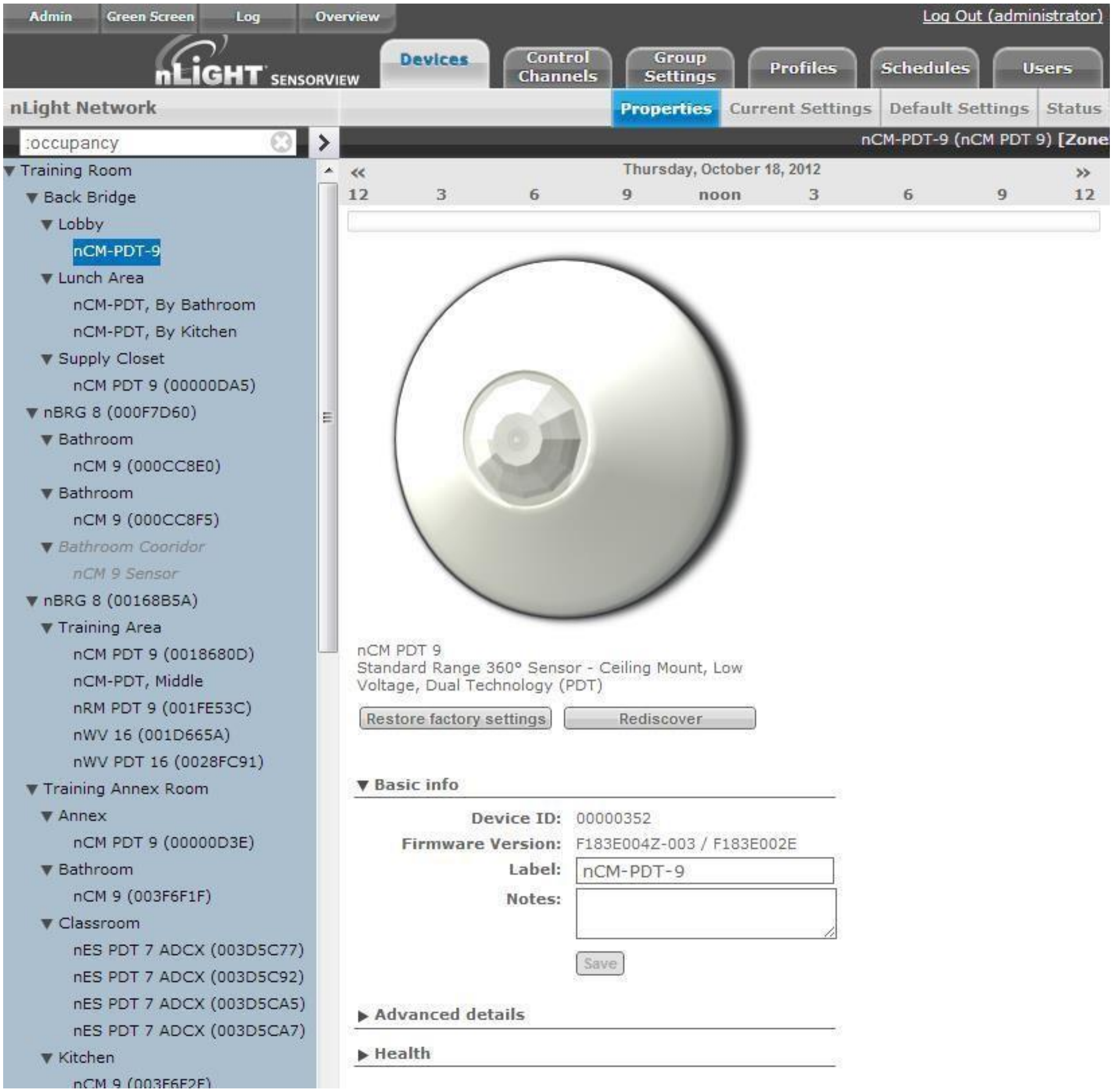
2. Using the nLight Network tree to the left, find the device you wish to view



nGWY2
Gateway 2: CPU Unit

ID: 004488BA
Firmware Version: F235C001_1.2.32818 / F235C002_2.6.30.1
Label: Training Room
Notes:

3. Click the desired device; the properties will populate the Devices area to the right

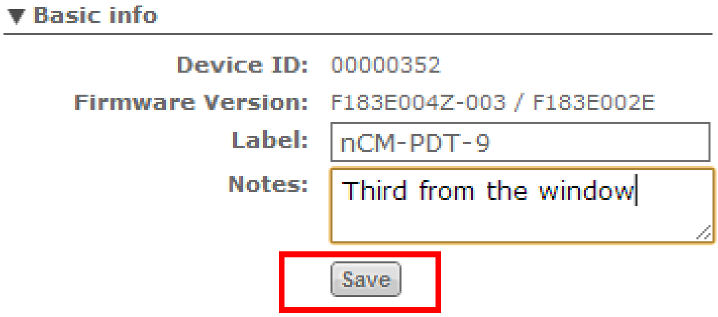


nCM PDT 9
Standard Range 360° Sensor - Ceiling Mount, Low Voltage, Dual Technology (PDT)

Device ID: 00000352
Firmware Version: F183E004Z-003 / F183E002E
Label: nCM-PDT-9
Notes:

4. Change the Label, Notes, and other areas to your requirements

5. Click ***Save*** to apply your changes

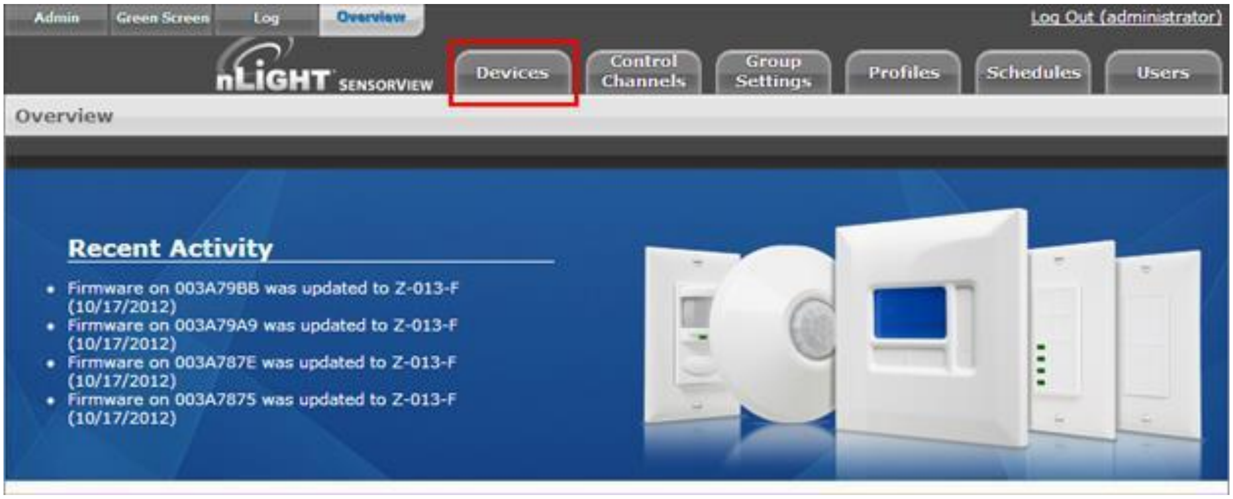


▼ Basic info

Device ID:	00000352
Firmware Version:	F183E004Z-003 / F183E002E
Label:	nCM-PDT-9
Notes:	Third from the window

Viewing / Editing Normal Device Settings: Sensors/WallPods/Power Packs

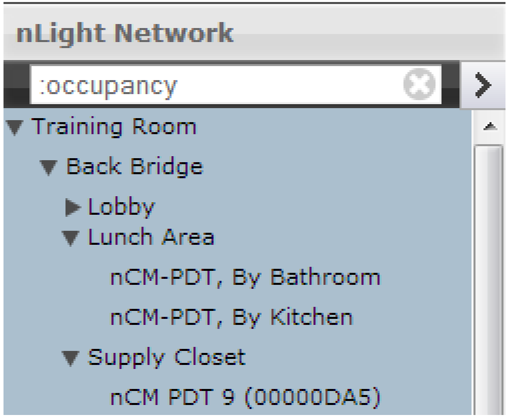
1. Click the ***Devices*** tab



Recent Activity

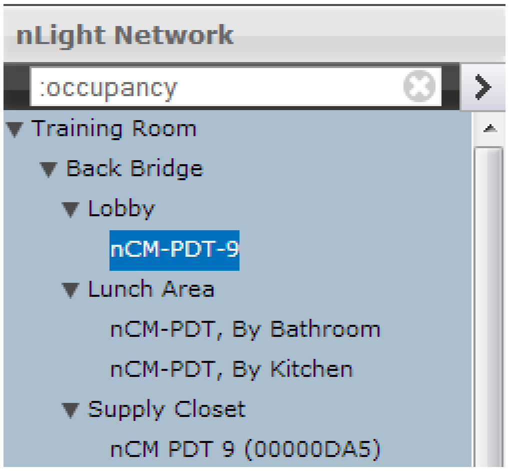
- Firmware on 003A79BB was updated to Z-013-F (10/17/2012)
- Firmware on 003A79A9 was updated to Z-013-F (10/17/2012)
- Firmware on 003A787E was updated to Z-013-F (10/17/2012)
- Firmware on 003A7875 was updated to Z-013-F (10/17/2012)

2. Using the Device tree to the left, find the device you wish to view



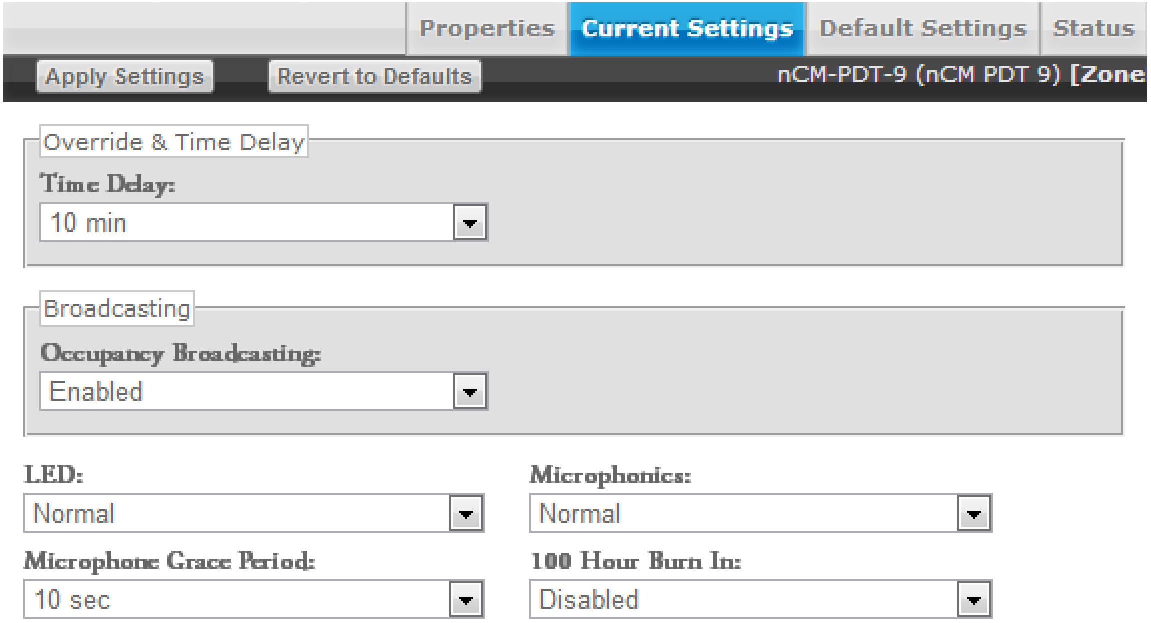
- Training Room
  - Back Bridge
    - Lobby
    - Lunch Area
      - nCM-PDT, By Bathroom
      - nCM-PDT, By Kitchen
    - Supply Closet
      - nCM PDT 9 (00000DA5)

3. Click the desired device



- Training Room
  - Back Bridge
    - Lobby
      - nCM-PDT-9
    - Lunch Area
      - nCM-PDT, By Bathroom
      - nCM-PDT, By Kitchen
    - Supply Closet
      - nCM PDT 9 (00000DA5)

4. Click the ***Current Settings*** tab (if it’s grayed out, settings aren’t applicable to the current selection, & you need to pick another device)



Override & Time Delay

Time Delay:

10 min

Broadcasting

Occupancy Broadcasting:

Enabled

LED:

Normal

Microphonics:

Normal

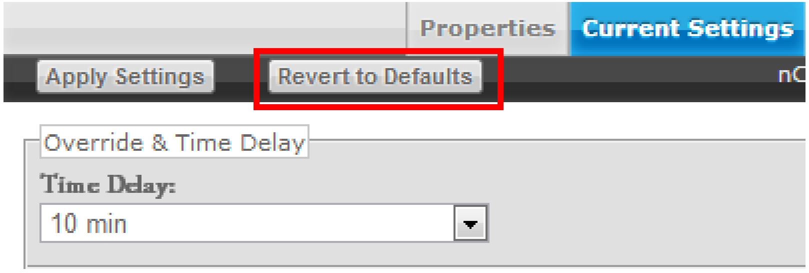
Microphone Grace Period:

10 sec

100 Hour Burn In:

Disabled

5. Your device’s specific settings (varies from device to device) will show
6. Modify the settings in the dropdown/checkbox fields to your specifications (You may also revert to device defaults by clicking the button at the top)

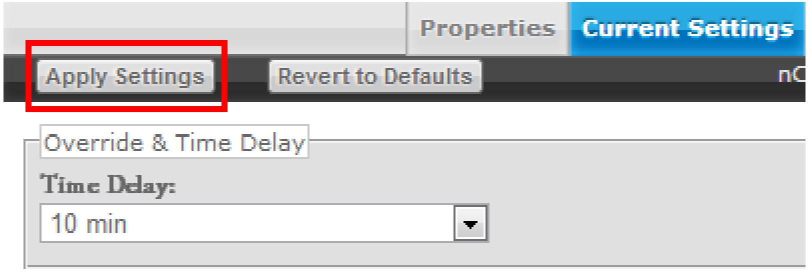


Override & Time Delay

Time Delay:

10 min

7. After you’ve made your changes, click the ***Apply Settings*** button to save your modifications

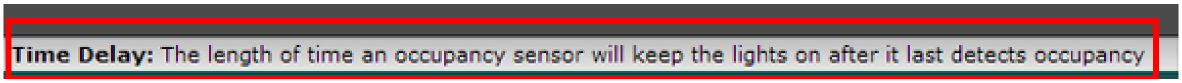


Override & Time Delay

Time Delay:

10 min

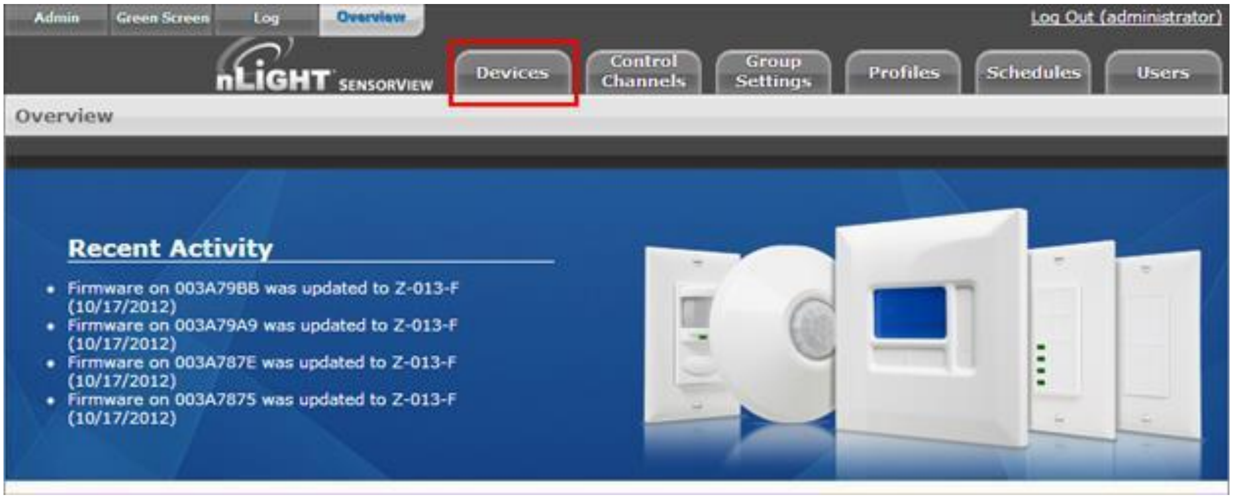
Note: hovering over a setting will cause its definition to appear in the information pane at the bottom of the page. The SensorView Terms Glossary also lists these definitions.



Time Delay: The length of time an occupancy sensor will keep the lights on after it last detects occupancy

Viewing / Editing Scene Selector / nIO Settings:

1. Click the ***Devices*** tab

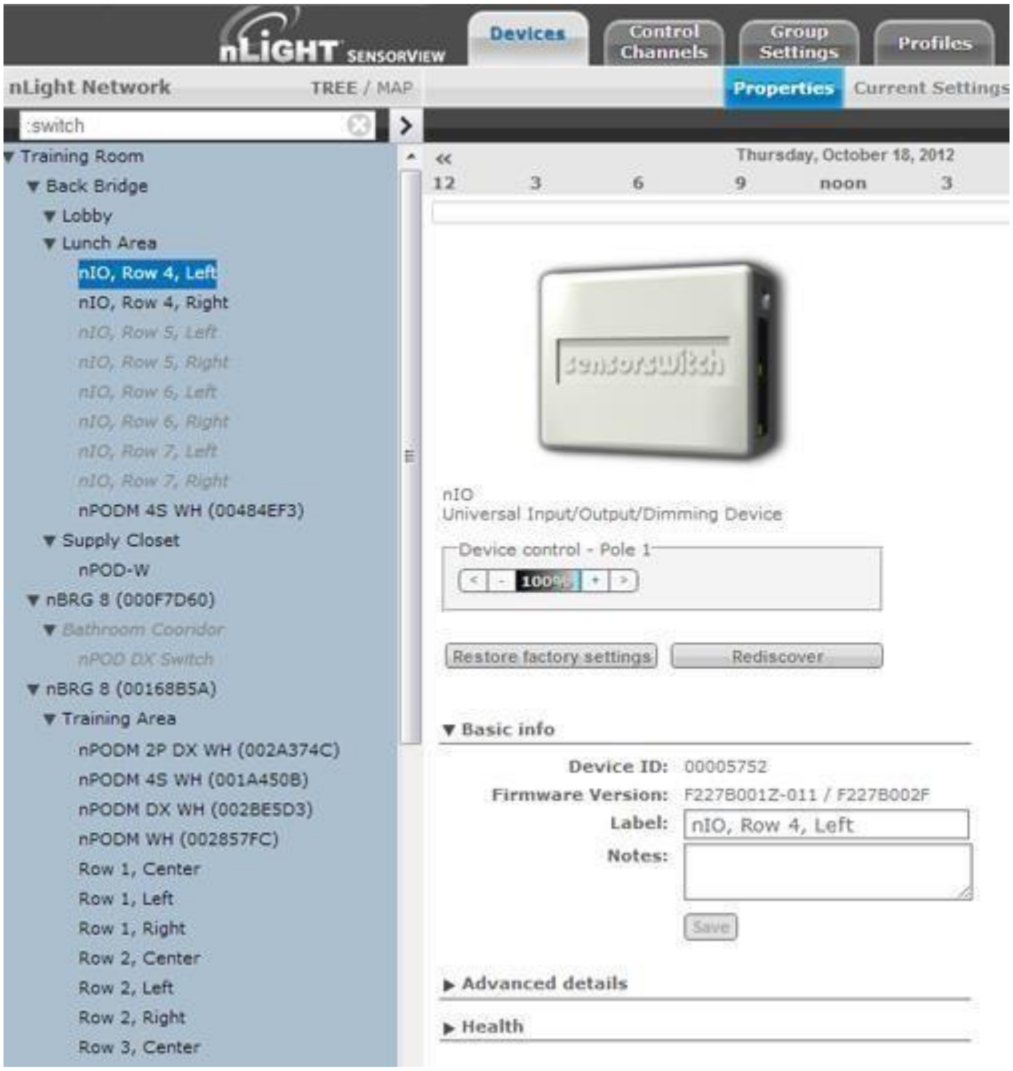


Recent Activity

- Firmware on 003A79BB was updated to Z-013-F (10/17/2012)
- Firmware on 003A79A9 was updated to Z-013-F (10/17/2012)
- Firmware on 003A787E was updated to Z-013-F (10/17/2012)
- Firmware on 003A7875 was updated to Z-013-F (10/17/2012)

2. Using the nLight Network tree to the left, find a Scene Selector or nIO

3. Click the desired device

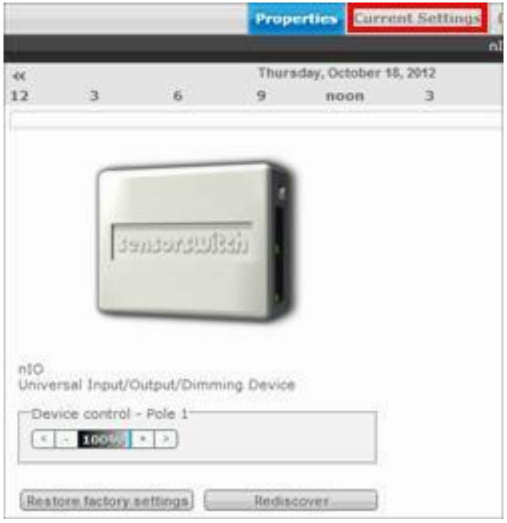


nIO
Universal Input/Output/Dimming Device

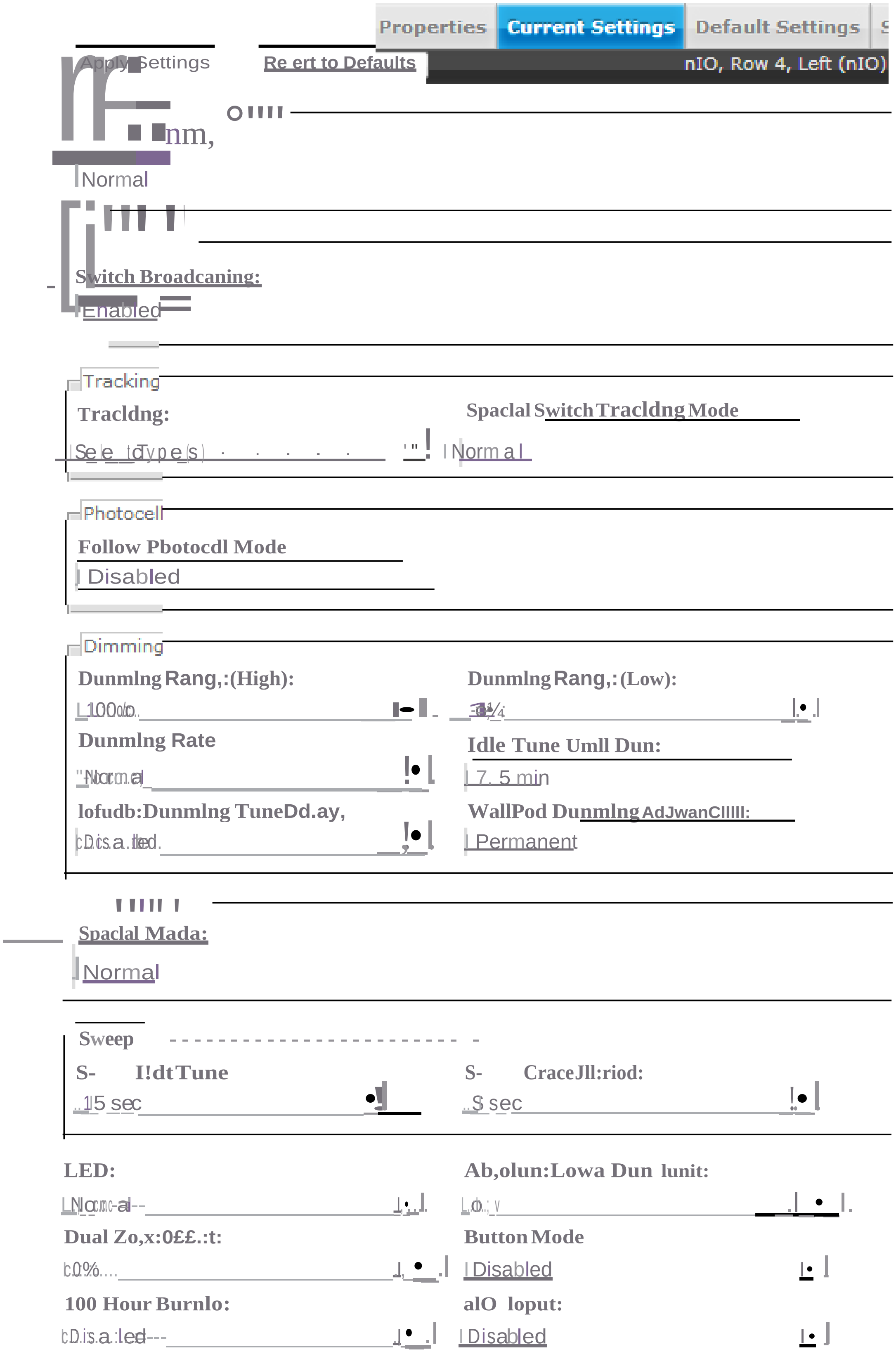
Basic info

Device ID: 00005752
Firmware Version: F227B001Z-011 / F227B002F
Label: nIO, Row 4, Left
Notes:

4. Click the ***Current Settings*** tab (if it's grayed out, settings aren't applicable, & you need to pick another device)



5. For Scene Selectors, the currently assigned action for each of the four control mode buttons is displayed. Change settings for each button via the dropdowns. Click ***Apply Settings*** to save.



nIO, Row 4, Left (nIO)

nm,

Normal

Switch Broadcaning:

Enabled

Tracking

Tracldng:

Sele_td Type(s)

Spaclal Switch Tracldng Mode

Normal

Photocell

Follow Pbotocdl Mode

Disabled

Dimming

Dunmlng Rang,:(High):

100%

Dunmlng Rang,:(Low):

3¼

Dunmlng Rate

Normal

Idle Tune Umll Dun:

7.5 min

lofudb:Dunmlng TuneDd.ay,

Disabled

WallPod Dunmlng AdJwanClllll:

Permanent

Spaclal Mada:

Normal

Sweep

S- I!dtTune

15 sec

S- CraceJll:riod:

5 sec

LED:

Normal

Ab,olun:Lowa Dun lunit:

Low

Dual Zo,x:0££.:t:

0%

Button Mode

Disabled

100 Hour Burnlo:

Disabled

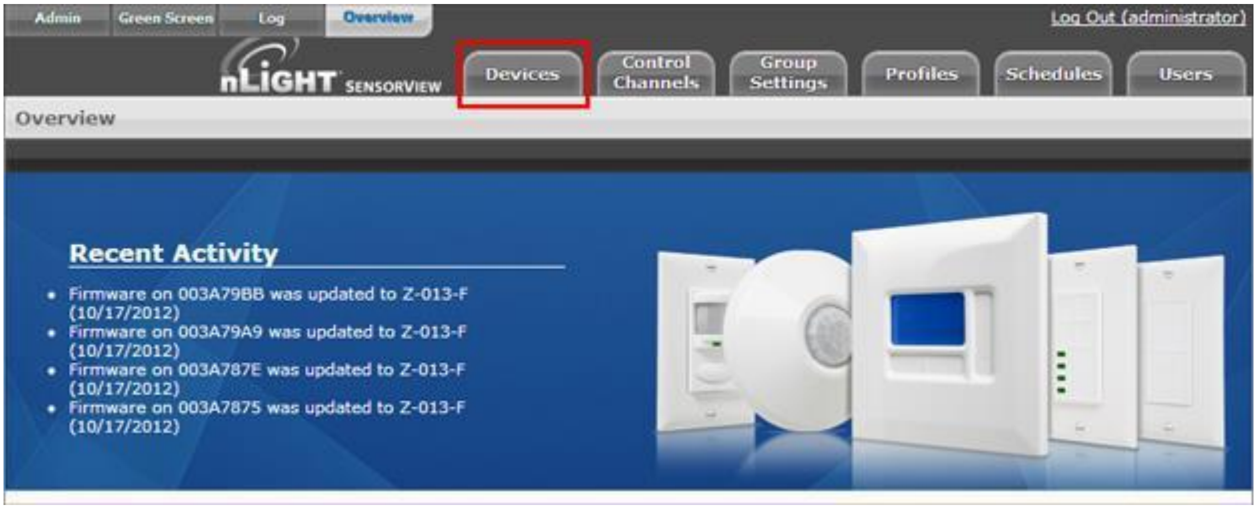
alO loput:

Disabled

Control Mode Options (triggered through a button push or nIO input event):
Scene Control – Initiates corresponding scene outlined in Default Settings
Wallpod – On/Off functionality for the associated lights
Sweep – Initiates sweep for the corresponding number in Default Settings
Disabled – Disables the corresponding button

To create Scene Selector / nIO Scenes & Profiles:

1. Click the ***Devices*** tab

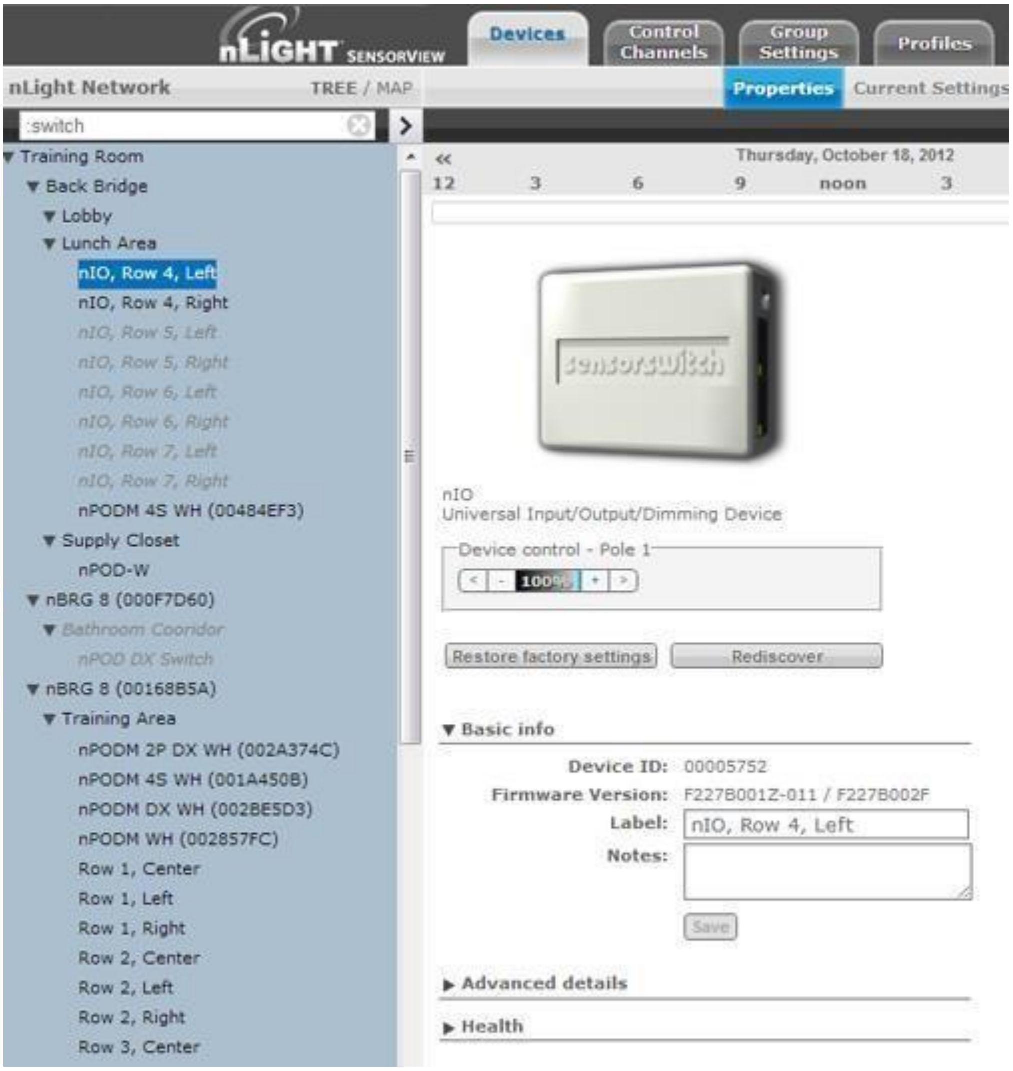


Recent Activity

- Firmware on 003A79BB was updated to Z-013-F (10/17/2012)
- Firmware on 003A79A9 was updated to Z-013-F (10/17/2012)
- Firmware on 003A787E was updated to Z-013-F (10/17/2012)
- Firmware on 003A7875 was updated to Z-013-F (10/17/2012)

2. Using the nLight Network tree to the left, find a Scene Selector or nIO

3. Click the desired device



- Training Room
  - Back Bridge
    - Lobby
    - Lunch Area
      - nIO, Row 4, Left
      - nIO, Row 4, Right
      - nIO, Row 5, Left
      - nIO, Row 5, Right
      - nIO, Row 6, Left
      - nIO, Row 6, Right
      - nIO, Row 7, Left
      - nIO, Row 7, Right
      - nPODM 4S WH (00484EF3)
    - Supply Closet
      - nPOD-W
  - nBRG 8 (000F7D60)
    - Bathroom Cooridor
      - nPOD DX Switch
  - nBRG 8 (00168B5A)
    - Training Area
      - nPODM 2P DX WH (002A374C)
      - nPODM 4S WH (001A450B)
      - nPODM DX WH (002BE5D3)
      - nPODM WH (002857FC)
      - Row 1, Center
      - Row 1, Left
      - Row 1, Right
      - Row 2, Center
      - Row 2, Left
      - Row 2, Right
      - Row 3, Center

nIO
Universal Input/Output/Dimming Device

Device control - Pole 1

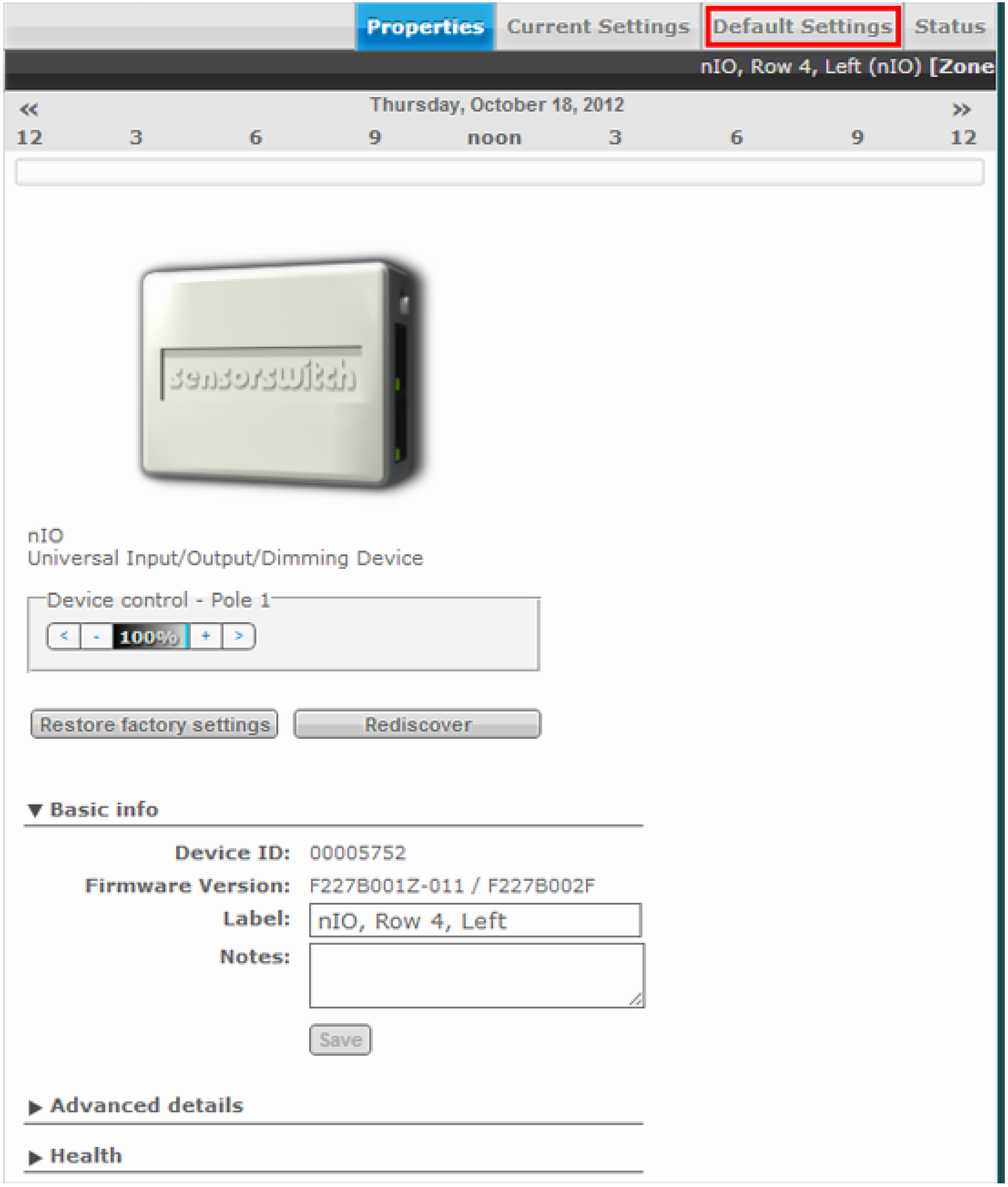
▼ Basic info

Device ID: 00005752
Firmware Version: F227B001Z-011 / F227B002F
Label: nIO, Row 4, Left
Notes:

▶ Advanced details

▶ Health

4. Click the ***Default Settings*** tab (if grayed out, settings aren’t applicable to the current choice, & you need to pick a new device)



nIO, Row 4, Left (nIO) [Zone

nIO
Universal Input/Output/Dimming Device

100%

Device ID: 00005752

Firmware Version: F227B001Z-011 / F227B002F

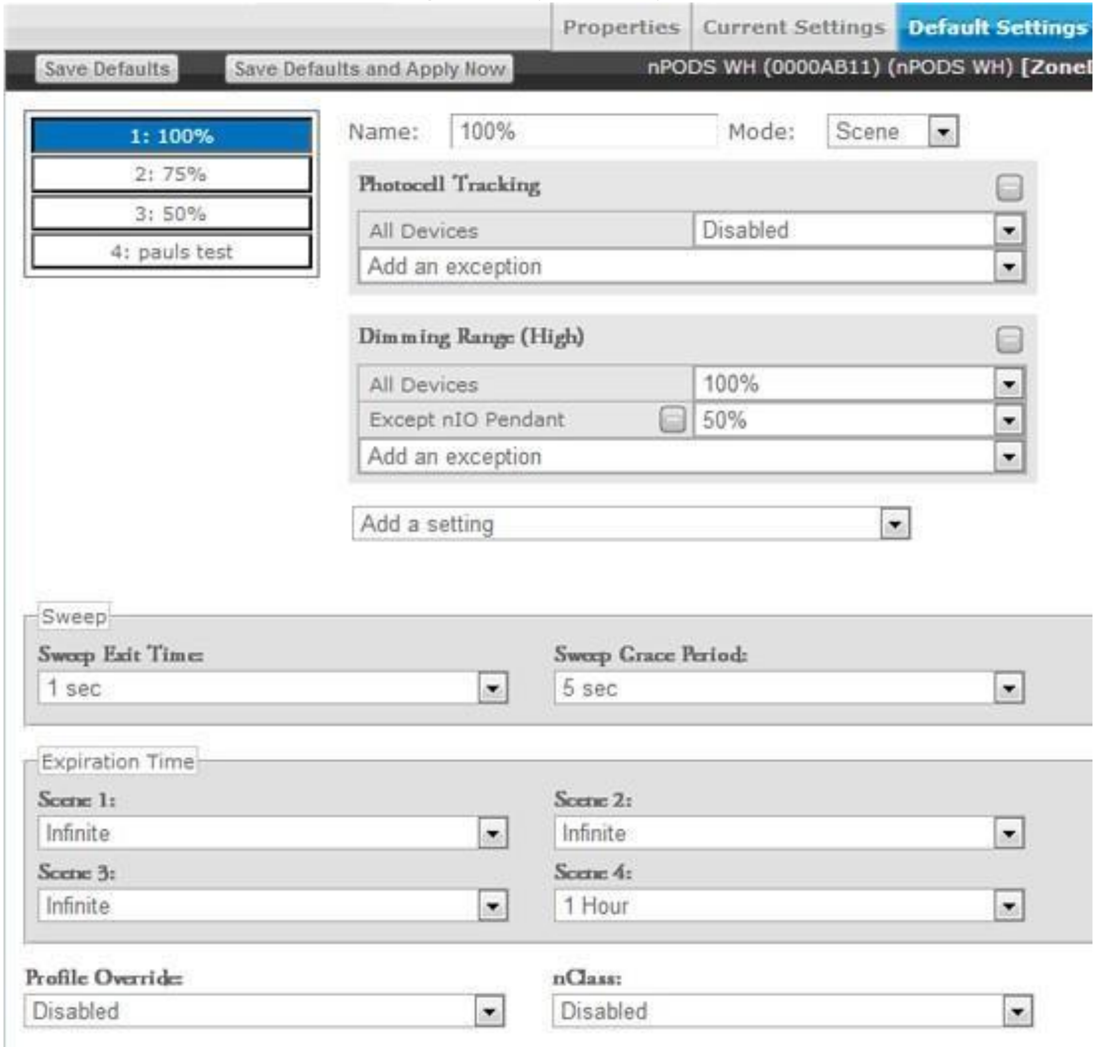
Label: nIO, Row 4, Left

Notes:

5. Select a button, type a name to associate with it, then select which mode you wish to run in:
Wallpod – Assigns on/off control to button
Scene – Assigns created scene to button
Profile – Assigns an existing profile to button
Sweep – Assigns sweep to selected button

For buttons designated with Scene Mode:

Create a scene via the device settings & exceptions dropdowns.



Name: 100% Mode: Scene

Photocell Tracking

All Devices	Disabled
Add an exception	

Dimming Range (High)

All Devices	100%
Except nIO Pendant	50%
Add an exception	

Add a setting

Sweep

Sweep Exit Time: 1 sec

Sweep Grace Period: 5 sec

Expiration Time

Scene 1: Infinite

Scene 2: Infinite

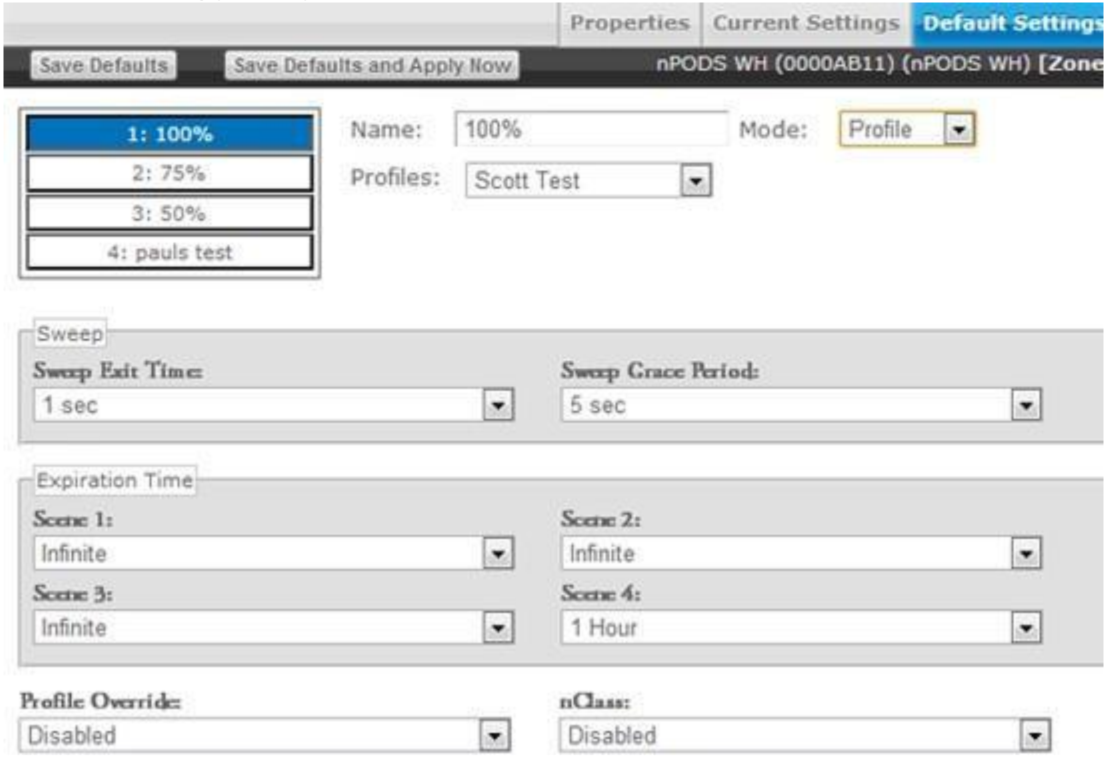
Scene 3: Infinite

Scene 4: 1 Hour

Profile Override: Disabled

nClass: Disabled

For buttons designated with Profile Mode:
Select an existing profile you wish to attach to the selected button.



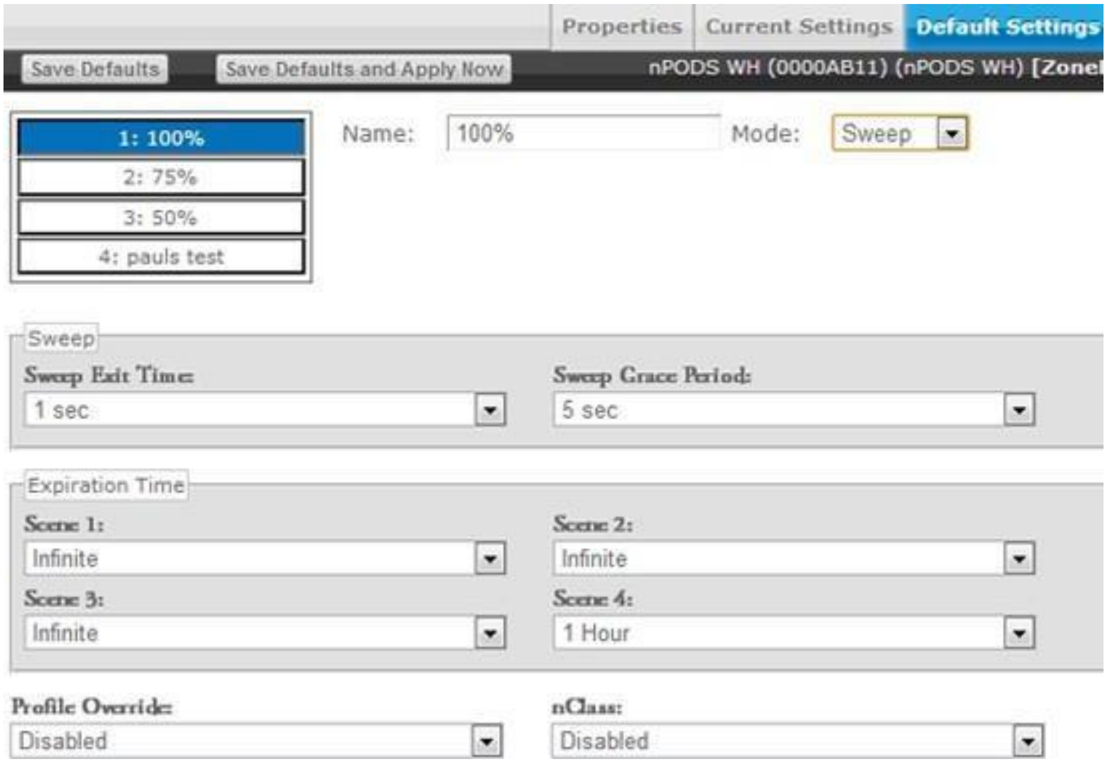
Name: 100%
Mode: Profile
Profiles: Scott Test

Sweep
Sweep Exit Time: 1 sec
Sweep Grace Period: 5 sec

Expiration Time
Scene 1: Infinite
Scene 2: Infinite
Scene 3: Infinite
Scene 4: 1 Hour

Profile Override: Disabled
nClass: Disabled

For buttons designated with Sweep Control Mode:
The Sweep Exit and Sweep Grace Period dropdowns allow you to set a time delay, after which the value of the remaining time delay in all applicable devices will be changed to the input value. This is helpful if you wish to quickly turn all the lights in a zone or building off without affecting any of the device settings.



nPODS WH (0000AB11) (nPODS WH) [Zone

1: 100%
2: 75%
3: 50%
4: pauls test

Name: 100%
Mode: Sweep

Sweep

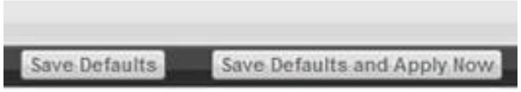
Sweep Exit Time: 1 sec
Sweep Grace Period: 5 sec

Expiration Time

Scene 1: Infinite
Scene 2: Infinite
Scene 3: Infinite
Scene 4: 1 Hour

Profile Override: Disabled
nClass: Disabled

6. Click ***Save Defaults and Apply Now*** to save, then click another number to change its settings.



Viewing / Editing Zone Settings

1. Click the ***Group Settings*** tab
2. Using the nLight Network tree to the left, click the checkbox next to the desired Zone to select all devices within the zone.
   Note: Each port of a Bridge is considered a zone
3. Create the list of settings to be modified by selecting settings one at a time from the provided dropdown field
4. To prevent a device from having a particular setting apply, create an exception
5. After you've made your changes, click the ***Save Defaults*** button to save your modifications
6. Refer to the Appendix for specific details regarding each setting's meaning

Managing Profiles

The Profiles page provides the ability to create, edit, and delete all Profiles configured within the system. All Profiles displayed will be grouped with other Profiles sharing the same state: Synchronized, Mismatched, SensorView Only, or Gateway Only.

While creating or editing a profile the Device tree will operate in MultiSelect mode, there is no limit on how many devices can participate in a given Profile. As Devices are added to the Profile more settings may become available on the right, settings are only displayed if there is a Device selected that contains it, settings will be omitted if no Devices selected support it.

The Scheduler, visible at the bottom of the screen, controls the Schedule for the Profile. Profiles can be configured to start/stop at a particular time of day, or based on an offset from Sunrise or Sunset. Recurrences specify how often the Profile should recur in the future, available Recurrences are Daily, Weekly, Monthly, and Yearly.

The Scheduler also contains a tab for Priority, which allows specification of how Scheduling conflicts should be handled. If two, or more, Profiles' execution times overlap then the Priority determines which Profile will run on each Device. The Schedules section provides a view of exactly how Scheduling conflicts will be resolved by Priority.

Create a Profile

1. Click the ***Profiles*** tab
2. Click on **New**
3. Profile will show up under the ***SensorView Only*** header
4. Select all Devices that should be in the Profile using the Device Tree, as Devicesare added more Settings will become available in the Settings area

5. In the Scheduler/Priority section, create a schedule with any required recurrences, then click ***Create***. For additional schedules select ***New Schedule*** in the dropdown and repeat the previous process.
6. Click the ***Priority*** tab to modify the priority of the profile using the arrows. Priority will only matter if another Profile is scheduled to execute at the same time, on the same Device.
7. Select desired settings to be added / modified by the profile from the Settings dropdowns; choose values & pick exceptions, if needed.
8. Once all Settings and Schedules have been configured fill in the name for the profileand click **Save**, the Profile will then move under the **Synchronized** header.

Edit a Profile

1. Click the ***Profiles*** tab
2. Select a Profile Name
3. Edit the schedule & priority, clicking ***Update*** to save your changes when finished
4. Remove any existing settings by clicking the **–** button, modify the current values, or use the Add a Setting dropdown to add new ones
5. Repeat for each setting you wish to modify, then click ***Save***

On Demand Profiles

SensorView provides the ability to command a Profile to **Run** or **Stop** on demand. This is often utilized for standard events that don’t recur according to a specific Schedule, but requires the same lighting configuration.

When a Profile is run on demand it will not stop according to any Schedule, it must be stopped manually; other Profiles that are scheduled to run at the same time, or afterwards, will still execute normally. When a Profile is stopped on demand, and it has a schedule, it will still follow the next Recurrence of the Schedule.

To command a Profile manually:

1. Click the ***Profiles*** tab
2. Select a Profile Name
3. Click either ***Run*** or ***Stop*** to command the Profile

Delete a Profile

1. Click the ***Profiles*** tab
2. Select a Profile Name

3. Click ***Delete*** to permanently remove that profile
4. A pop-up will confirm that you wish to do this. Click ***Ok***.
5. Repeat for each profile you wish to delete
   ***Please note: deleted profiles are permanently removed. Be certain you wish to delete the profile before proceeding.*

View Reports

SensorView provides a variety of generated reports detailing all configurable aspects of the nLight network. To view a list of available reports refer to SensorView Reports.
To Generate a Report:

1. Click the ***Admin*** link
2. Click the ***Reports*** tab
3. Select the report you wish to run. Click ***Generate Report***
4. Once run, print a report using the ***Print Report*** button, supported browsers all provide the option to Print to a PDF

Upgrading Devices

1. Click the ***Admin*** link in the top right
2. Click the ***Updates*** tab (or click the "Updates" link from the Overview page)
3. Check the selected items you wish to update (unchecked items will not update)
4. Click ***Submit*** at the bottom of the page

   Downloading Firmware Cache:
   Available when internet connection is present & an updated version of SensorView is available, enabling update downloads that are made available to an offline network.

   Note: This process may be lengthy depending on the size of the network.

SensorView

Installing SensorView is a multi-step process that should only be completed by a qualified computer administrator. Before proceeding, please make the following items available to ensure a successful SensorView Installation:

- □ Windows Installation Disk (Required for Windows XP & Windows Server 2003)
- □ Active Internet Connection
- □ SensorView Registration Key (provided in each Gateway box)
- □ Cross wired CAT-5(e) cable (click here for pinouts)

nLIGHT
SENSORVIEW
REGISTRATION KEY
GK6J9J95MC6C677I
SAMPLE
For instructions on downloading and installing SENSORVIEW go to
www.sensorswitch.com/install/instructions.pdf
sensorswitch

Step 1: Requirements

There are two types of installations available for SensorView:

Single-User / Commissioning

For use with any nLight network where a single user operates or commissions the system.

MINIMUM SPECS:	SUGGESTED SPECS:
Operating System: Windows 7	**Operating System:** Windows 7 or 8
Software: IIS 6.0, .NET 4.5.1	**Software:** IIS 8.0, .NET 4.5.1
Hardware: 1 GB RAM, 2 GB Hard Drive	**Hardware:** 2 GB RAM, 30 GB Hard Drive
Browser: Firefox, Chrome, Opera, or Internet Explorer 10+	**Browser:** Firefox, Chrome, Opera, or Internet Explorer 10+

Multi-User

For use with any nLight network where multiple concurrent web sessions are desired.

MINIMUM SPECS:	SUGGESTED SPECS:
Operating System: Windows Server 2003, Windows Server Web Edition, Windows Small Business Server 2003	**Operating System:** Windows Server 2008 or 2012
Software: IIS 6.0, .NET 4.5.1	**Software:** IIS 8.0, .NET 4.5.1
Hardware: 1 GB RAM, 2 GB Hard Drive	**Hardware:** 2 GB RAM, 30 GB Hard Drive
Browser: Firefox, Chrome, Opera, or Internet Explorer 10+	**Browser:** Firefox, Chrome, Opera, or Internet Explorer 10+

Step 2: Pre-Installation

SensorView requires pre-installation of both **IIS** and the **Microsoft .NET Framework**.

.NET Framework

The .NET Framework 3.0 is automatically installed with Windows Server 2008 & Windows Vista / 7 / 8. If you are NOT running either of these operating systems, click here and follow the .NET installation instructions.

IIS

IIS (Internet Information Services) is a Windows component that allows computers to host web applications. This component is required for hosting a SensorView installation, and will allow end users to view and control their SensorView install(s) remotely.

To install IIS, please click the link to your corresponding operating system below and follow the specific information for installing this component.

Please Note: *Both Win XP & Server 2003* ***require Windows installation disks*** *and are NOT downloadable from the web. Without Windows discs to install this component, SensorView installation cannot be completed:*

- **Windows XP Pro (32 bit) – IIS 5.0**
- **Windows Small Business Server 2003 (32 bit) – IIS 6.0**
- **Windows Server 2003 (32 bit) – IIS 6.0**
- **Windows Server 2003 (64 bit) – IIS 6.0**
- **Windows Server 2008 – IIS 7.0**
- **Windows Vista / 7 / 8 – IIS 7.0**

Step 3: Installation

After completing the successful installation of IIS (and .NET), you are now ready to continue:

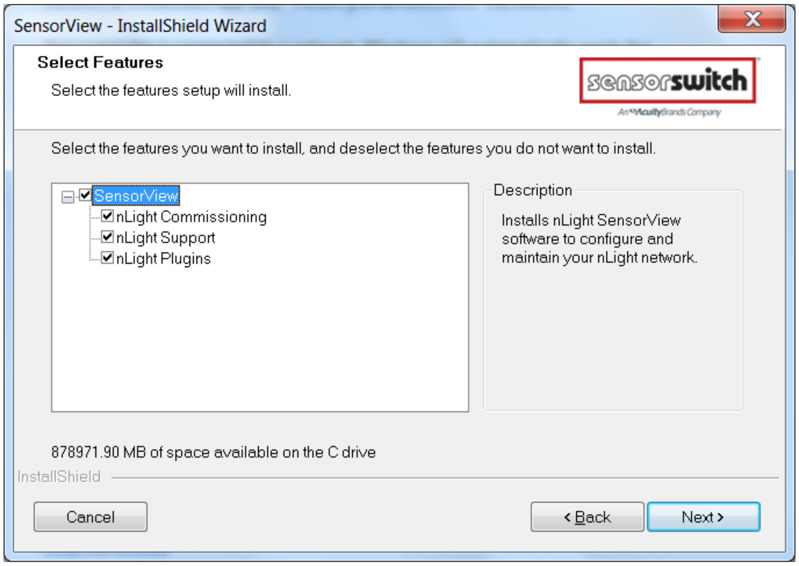
Download the **nLight SensorView installation package**:

1. Download the compressed .zip file (20 mb) from:
2. Unzip the file and run **setup.exe**.
3. Follow the instructional prompts to complete the installation of the SensorView application.

SensorView Installation Best Practices

It is recommended to do a full install of all offered features/plugins**.**

All boxes are checked by default. If they are not, please check them and click **Next**.



SensorView - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- ☑ SensorView
  - ☑ nLight Commissioning
  - ☑ nLight Support
  - ☑ nLight Plugins

Description

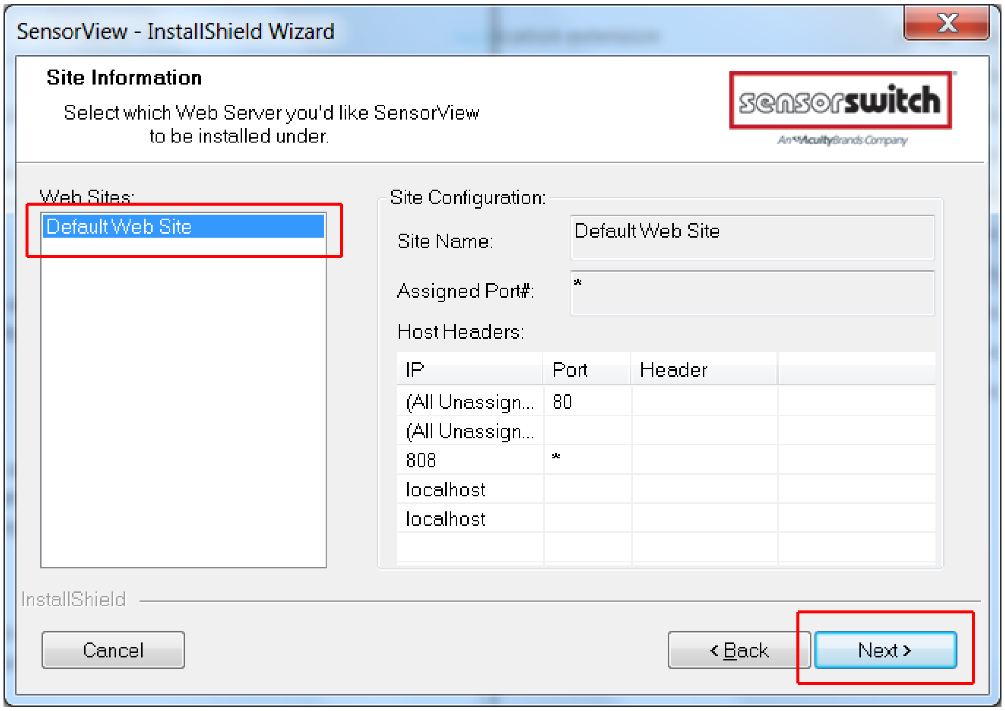
Installs nLight SensorView software to configure and maintain your nLight network.

878971.90 MB of space available on the C drive

SensorView will require registration to complete the installation process.

SensorView Registration
This includes a license key as well as information about who is installing
(the registration key is included on a small card with the gateway)

When the Install Shield wizard opens, select "**Default Web Site**" and click **Next**.



SensorView - InstallShield Wizard

Site Information

Select which Web Server you'd like SensorView to be installed under.

Web Sites:

Default Web Site

Site Configuration:

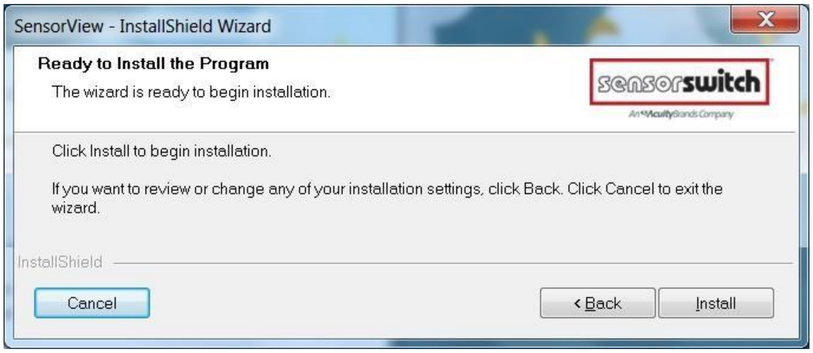
Site Name: Default Web Site

Assigned Port#: *

Host Headers:

IP	Port	Header
(All Unassign...	80	
(All Unassign...		
808	*	
localhost		
localhost		

Click **Install**



SensorView - InstallShield Wizard

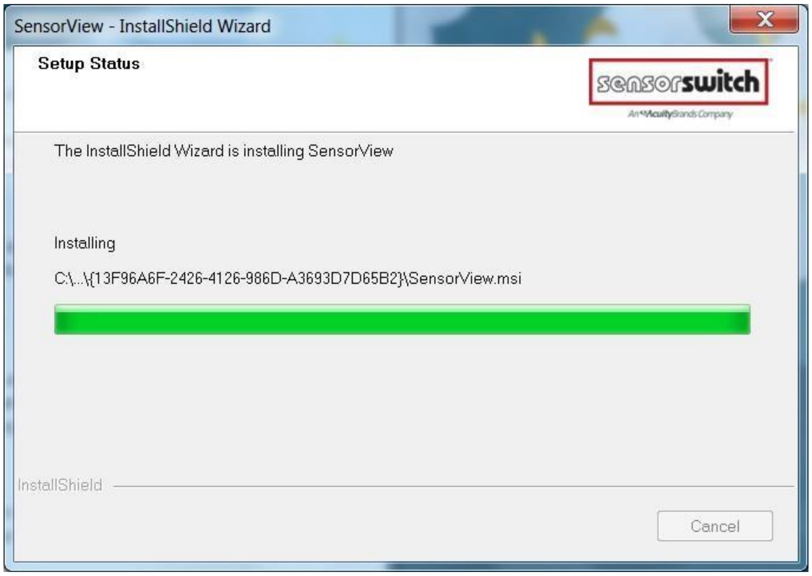
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

The install shield wizard takes a few moments to run.


SensorView - InstallShield Wizard

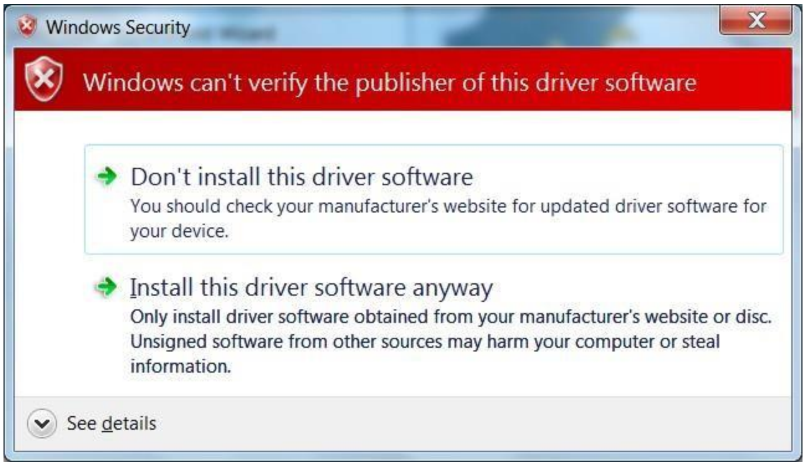
Setup Status

The InstallShield Wizard is installing SensorView

Installing

C:\...\{13F96A6F-2426-4126-986D-A3693D7D65B2}\SensorView.msi

If you see the following message, click “install this driver software anyway”.

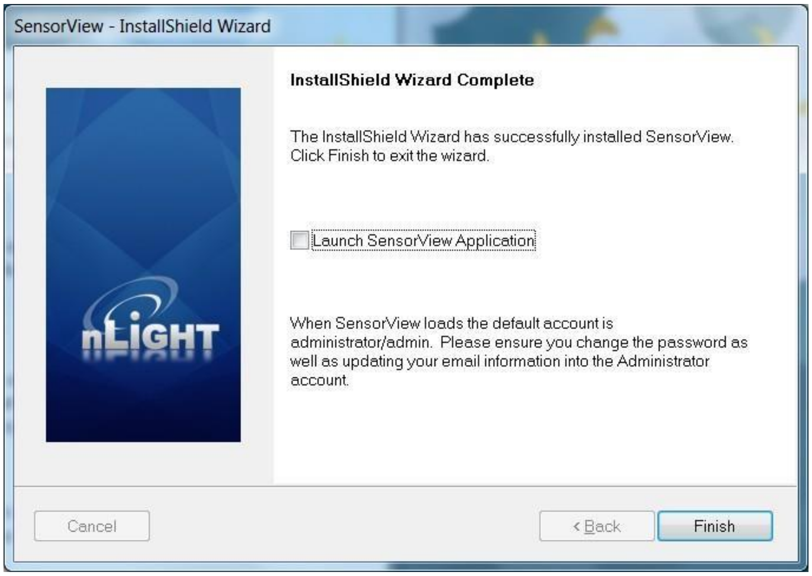

Windows Security

Windows can't verify the publisher of this driver software

Don't install this driver software
You should check your manufacturer's website for updated driver software for your device.

Install this driver software anyway
Only install driver software obtained from your manufacturer's website or disc. Unsigned software from other sources may harm your computer or steal information.

The installation is complete. Click the box to launch SensorView, or



SensorView - InstallShield Wizard

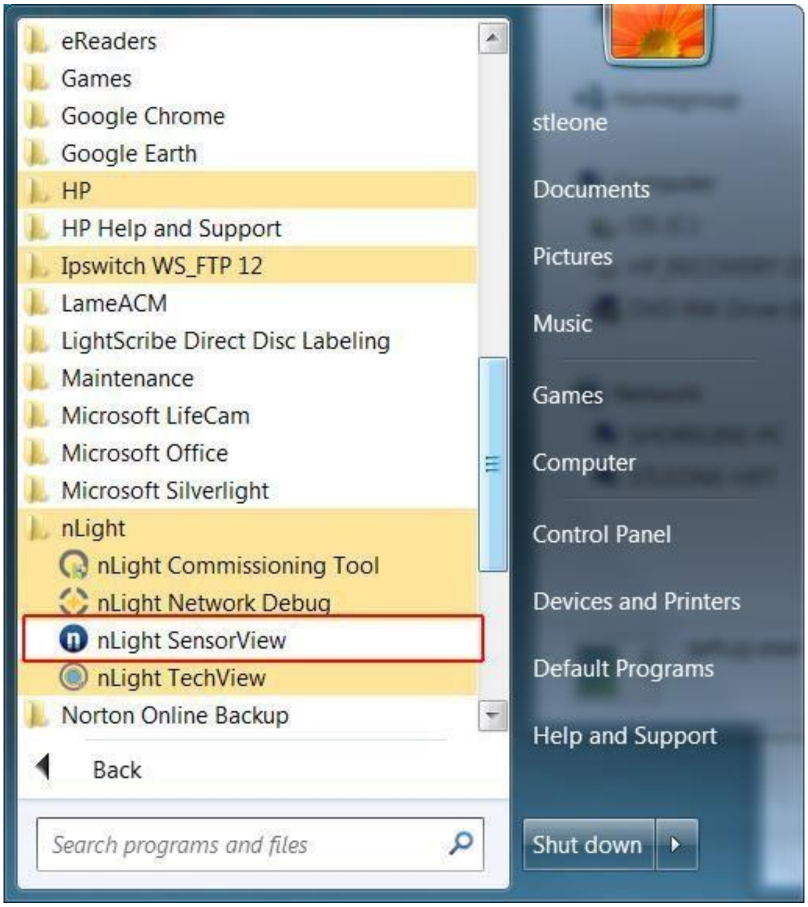
InstallShield Wizard Complete

The InstallShield Wizard has successfully installed SensorView. Click Finish to exit the wizard.

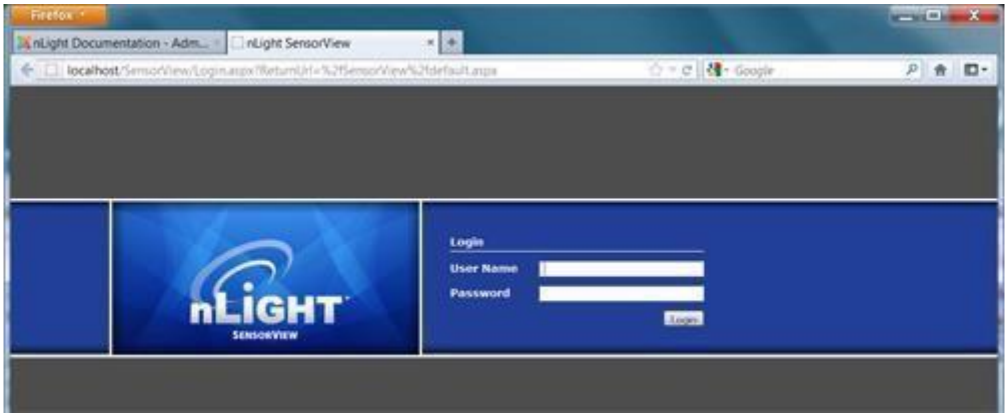
☐ Launch SensorView Application

When SensorView loads the default account is administrator/admin. Please ensure you change the password as well as updating your email information into the Administrator account.

Click **Start**, **All Programs**, Select **nLight SensorView**

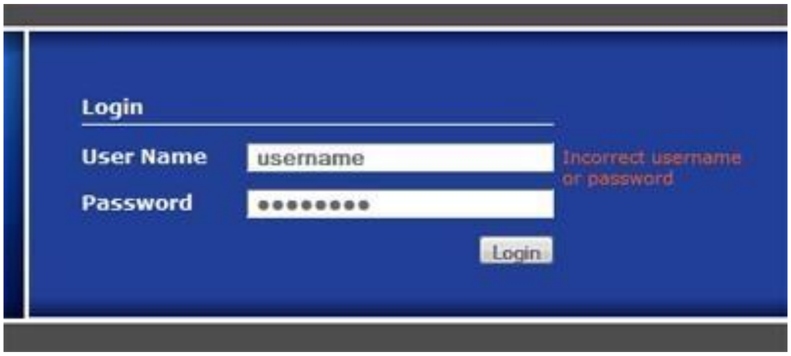


Launch SensorView on the desktop.


Firefox
nLight Documentation - Adm...
nLight SensorView
localhost/SensorView/Login.aspx?ReturnUrl=%2fSensorView%2fdefault.aspx
Google
nLIGHT
SENSORVIEW
Login
User Name
Password
Login

A username and password are required to login to SensorView. When SensorView is freshly installed, use the following:

Default User Name: **administrator**
Default Password: **admin**



User Name: username

Password: ●●●●●●●●

Incorrect username or password

Step 4: Connecting to Gateway

The Gateway uses the port labeled “Ethernet” to communicate with the computer running the SensorView software. There are several ways to connect to a gateway; please choose the method you wish to use:

Direct Connection

The following procedure will show you how to establish a direct connection between a laptop computer and a Gateway:

NOTE: a cross-wired CAT-5(e) cable is only required to connect this way to an nGWY1, nGWY2 does not require a cross-wired cable

1. If present, disable wireless networking card
2. Connect PC to Gateway’s Ethernet port with cross-wired (cross-over) CAT-5(e) cable
   NOTE: a standard patch cable (straight through wired) will not work
3. Turn off/verify DHCP on Gateway
   MENU > SETUP OPTIONS > SET [DHCP OFF]
   NOTE: if pin is required, enter 1234
4. Enter static IP address for Gateway (for example 192.168.1.2)
   MENU > SETUP OPTIONS > TCP/IP
5. Enter static IP address for Laptop (e.g., 192.168.1.5). The following instructionsare for Windows XP. Other operating systems may require different procedures for changing network address.
   1. **START > CONTROL PANEL > NETWORK CONNECTIONS >LOCAL AREA CONNECTION > PROPERTIES**
   2. Highlight Internet Protocol (TCP/IP) in box and click Properties
   3. Click the radio button for “Use the following IP address”
   4. Fill in
      IP address: 192.168.1.5
      Subnet Mask: 255.255.255.0
      Default Gateway: 192.168.1.1
   5. Click OK
6. Verify “Link Up” message on Gateway LCD screen. If “Link Up” message doesnot appear, reboot gateway
   MENU > REBOOT
7. Launch SensorView
   http://localhost/SensorView
8. Login to SensorView
   Default User Name: administrator
   Default Password: admin

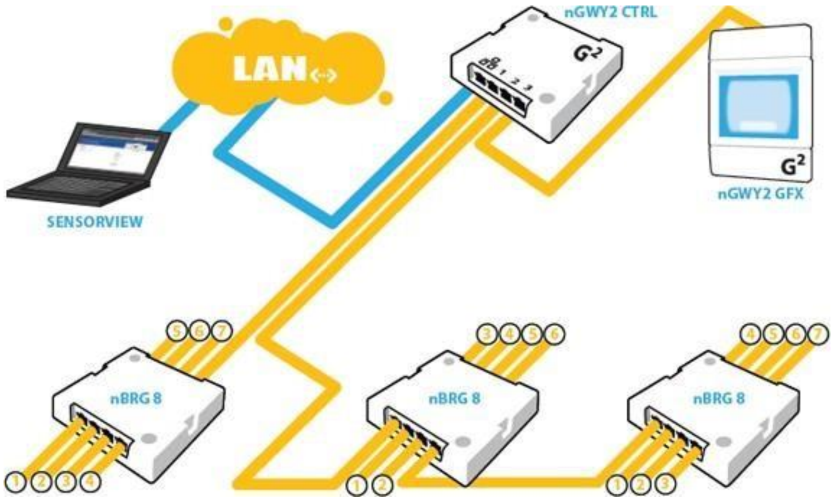
9. Once SensorView detects the Gateway it will appear in device tree
10. If Gateway does not appear in the tree, call tech support; **1.800.535.2465**

LAN Connection

The following procedure will show you how to connect to a Gateway over an existing Ethernet Local Area Network (LAN).

> **NOTE: if the computer and Gateway are located on different subnets, use the instructions for connecting over a Wide Area Network (WAN).**

1. Connect SensorView's computer to LAN using a standard patch cable
2. Connect Gateway's Ethernet port to LAN using a standard patch cable
3. If Link Up message appears on Gateway, go to step e, if not continue to next step
4. The Gateway can either use a dedicated IP address or acquire one from the network's DHCP server.
    1. To enter a dedicated IP address:
        1. Turn off DHCP on Gateway
           MENU > SETUP OPTIONS > SET [DHCP OFF]
           NOTE: if pin is required, enter 1234
        2. Enter static IP address for Gateway (for example 192.168.1.2)
           MENU > SETUP OPTIONS > TCP/IP
        3. Return to main screen and verify "Link Up" message. If "Link Up" message does not appear, reboot gateway
           MENU > REBOOT
    2. To use a DHCP assigned IP address:
        1. Turn On / Verify DHCP on Gateway
           MENU > SETUP OPTIONS > SET [DHCP ON]
           NOTE: if pin is required, enter 1234
        2. If DHCP fails, force the Gateway to acquire an address
           MENU > GET IP ADDRESS
        3. Return to main screen. Verify "Link Up" message
5. Launch SensorView
   From host computer: **http://localhost/SensorView**
   From non-host computer on LAN: **http://[enter server name]/SensorView**
6. Login to SensorView
   Default User Name: administrator
   Default Password: admin
7. Once SensorView discovers the Gateway it will appear in device tree
8. If Gateway does not appear in tree, call Sensor Switch tech support; 1.800.535.2465



WAN Connection

If you would like to connect to a Gateway over an existing Wide Area Network (WAN), please call tech support at 1.800.535.2465.

Crossover Cable Reference

Virtual WallPods

With the Virtual WallPod applications, users can control their lighting from their desktop or iOS mobile device. Designed to look like WallPods®, these applications are an excellent alternative to remote controls, which are often lost and require battery replacement. Simple user permissions provide facility managers necessary administrative control.

Configuring SensorView

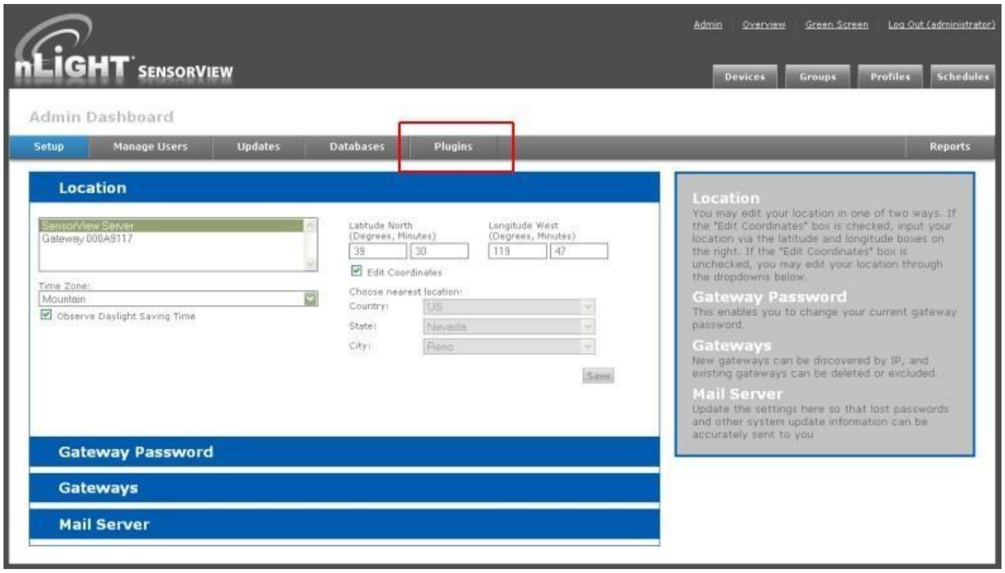
SensorView is a required component of the Virtual WallPods Plugin. It is used to setup and configure Users and the Virtual WallPods associated with them; as well as authenticate and process commands sent by Virtual WallPods.

Use of Virtual WallPods requires SensorView be online and accessible.

Update SensorView

Step 1

Before starting, log into your SensorView page and click on Admin at the top right of the screen. If you see a Plugins tab, skip Step 1 and proceed to Start the nLight Virtual WallPod Server.



Location

SensorView Server
Gateway 000A9117

Time Zone: Mountain

☑ Observe Daylight Saving Time

Latitude North (Degrees, Minutes): 39 30

Longitude West (Degrees, Minutes): 119 47

☑ Edit Coordinates

Choose nearest location:

Country: US

State: Nevada

City: Reno

Gateway Password

Gateways

Mail Server

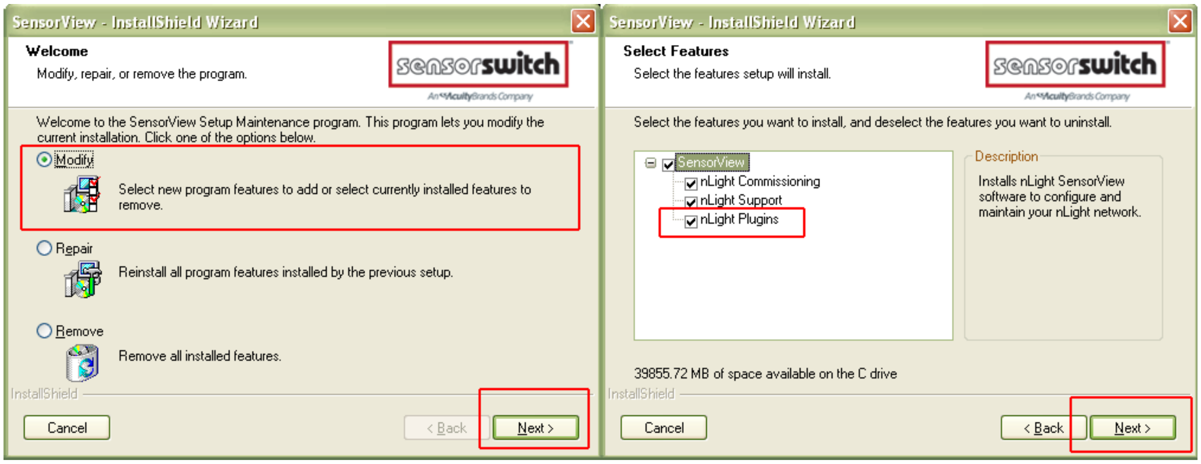
Location
You may edit your location in one of two ways. If the "Edit Coordinates" box is checked, input your location via the latitude and longitude boxes on the right. If the "Edit Coordinates" box is unchecked, you may edit your location through the dropdowns below.

Gateway Password
This enables you to change your current gateway password.

Gateways
New gateways can be discovered by IP, and existing gateways can be deleted or excluded.

Mail Server
Update the settings here so that lost passwords and other system update information can be accurately sent to you

If you do not see a Plugins tab, click the **Updates** tab and update to the latest version of SensorView. Once the SensorView application update is finished, run the install file for SensorView and select **Modify**.



Welcome

Modify, repair, or remove the program.

Welcome to the SensorView Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

● Modify
Select new program features to add or select currently installed features to remove.

○ Repair
Reinstall all program features installed by the previous setup.

○ Remove
Remove all installed features.

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you want to uninstall.

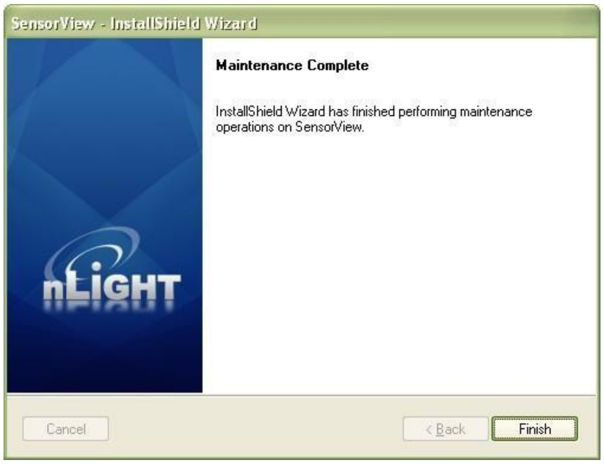
☑ SensorView
- ☑ nLight Commissioning
- ☑ nLight Support
- ☑ nLight Plugins

Description
Installs nLight SensorView software to configure and maintain your nLight network.

39855.72 MB of space available on the C drive

Click **Next**, and once the proceeding page opens check the **nLight Plugins** box, followed by **Next**.

Once the below screen appears the modification is complete, click **Finish** to close.



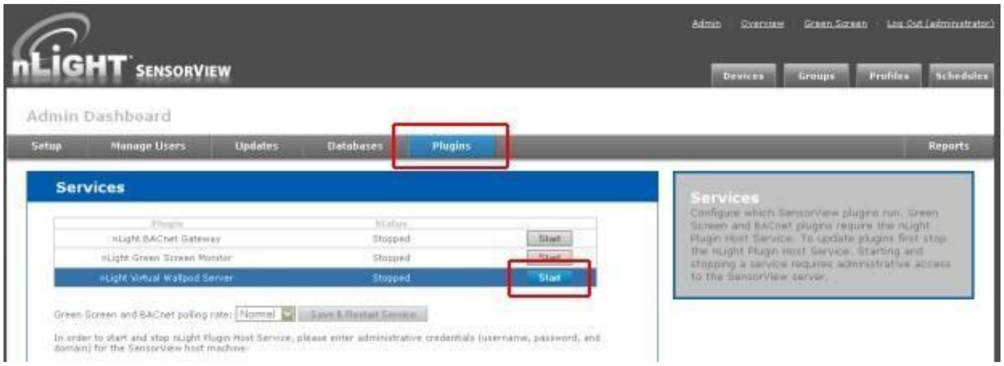
Maintenance Complete

InstallShield Wizard has finished performing maintenance operations on SensorView.

Virtual WallPod Server

Step 2

Once at the Admin Dashboard, click Plugins and Start the nLight Virtual WallPod Server.



Plugin	Status	
nLight BACnet Gateway	Stopped	Start
nLight Green Screen Monitor	Stopped	Start
nLight Virtual Wallpod Server	Stopped	Start

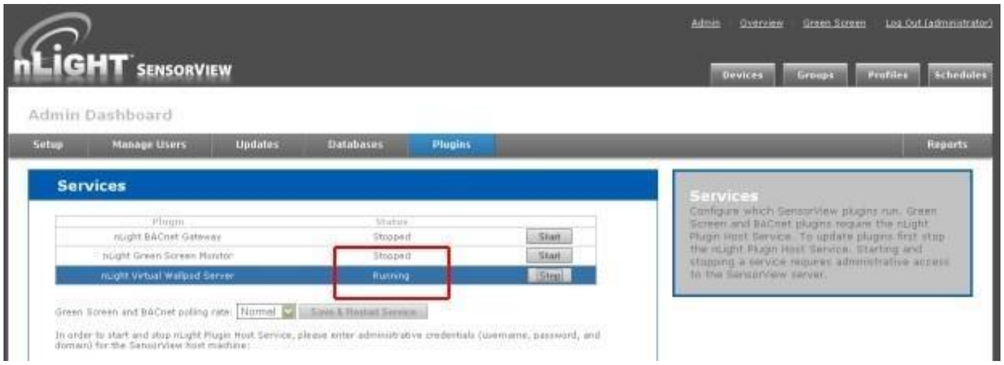
Green Screen and BACnet polling rate: Normal

In order to start and stop nLight Plugin Host Service, please enter administrative credentials (username, password, and domain) for the SensorView host machine.

Services

Configure which SensorView plugins run. Green Screen and BACnet plugins require the nLight Plugin Host Service. To update plugins first stop the nLight Plugin Host Service. Starting and stopping a service requires administrative access to the SensorView server.

Notice that stopped will change to running.



Admin Dashboard

Services

Plugin	Status	
nLight BACnet Gateway	Stopped	Start
nLight Green Screen Monitor	Stopped	Start
nLight Virtual Wallpod Server	Running	Stop

Green Screen and BACnet polling rate: Normal

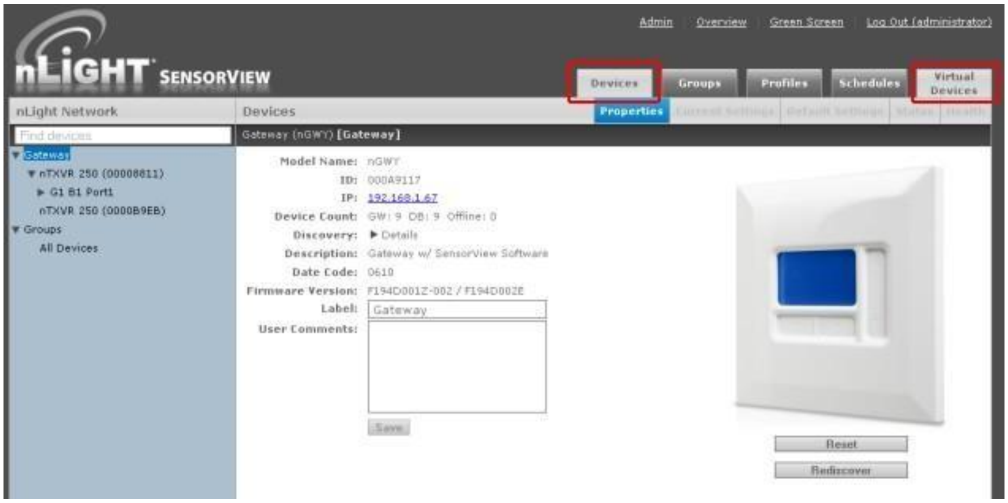
In order to start and stop nLight Plugin Host Service, please enter administrative credentials (username, password, and domain) for the SensorView host machine:

Services
Configure which SensorView plugins run. Green Screen and BACnet plugins require the nLight Plugin Host Service. To update plugins first stop the nLight Plugin Host Service. Starting and stopping a service requires administrative access to the SensorView server.

Virtual Controls

Step 3

Now that the nLight Virtual WallPod Server is running, go to the device page by clicking the **Devices** tab at the top right area of the screen. Once the devices page opens, clickon the **Virtual Devices** tab, located in the same area.



nLight Network

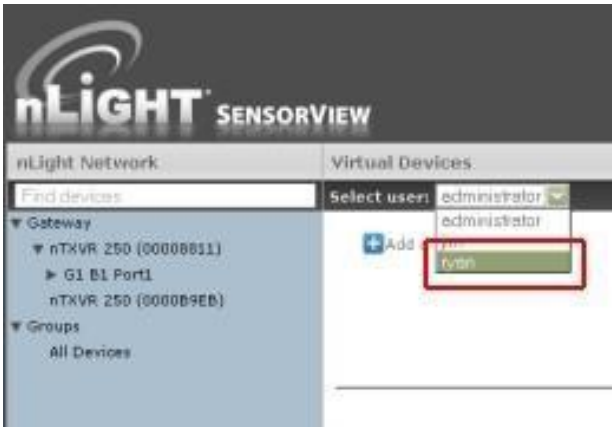
- Gateway
  - nTXVR 250 (00008811)
    - G1 B1 Port1
  - nTXVR 250 (0000B9EB)
- Groups
  - All Devices

Devices

Gateway (nGWY) [Gateway]

Model Name: nGWY
ID: 000A9117
IP: 192.168.1.67
Device Count: GW: 9 DB: 9 Offline: 0
Discovery: ▶ Details
Description: Gateway w/ SensorView Software
Date Code: 0610
Firmware Version: F194D001Z-002 / F194D002E
Label: Gateway
User Comments:

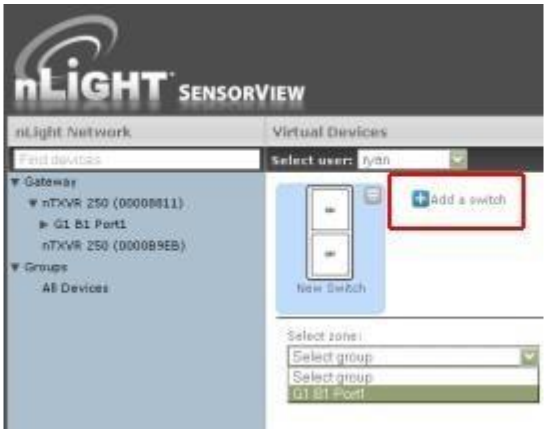
Select a user by clicking on the dropdown arrow



Virtual WallPod Switch

Step 4

Click the **Add a switch** button.



Control Zone

Step 5

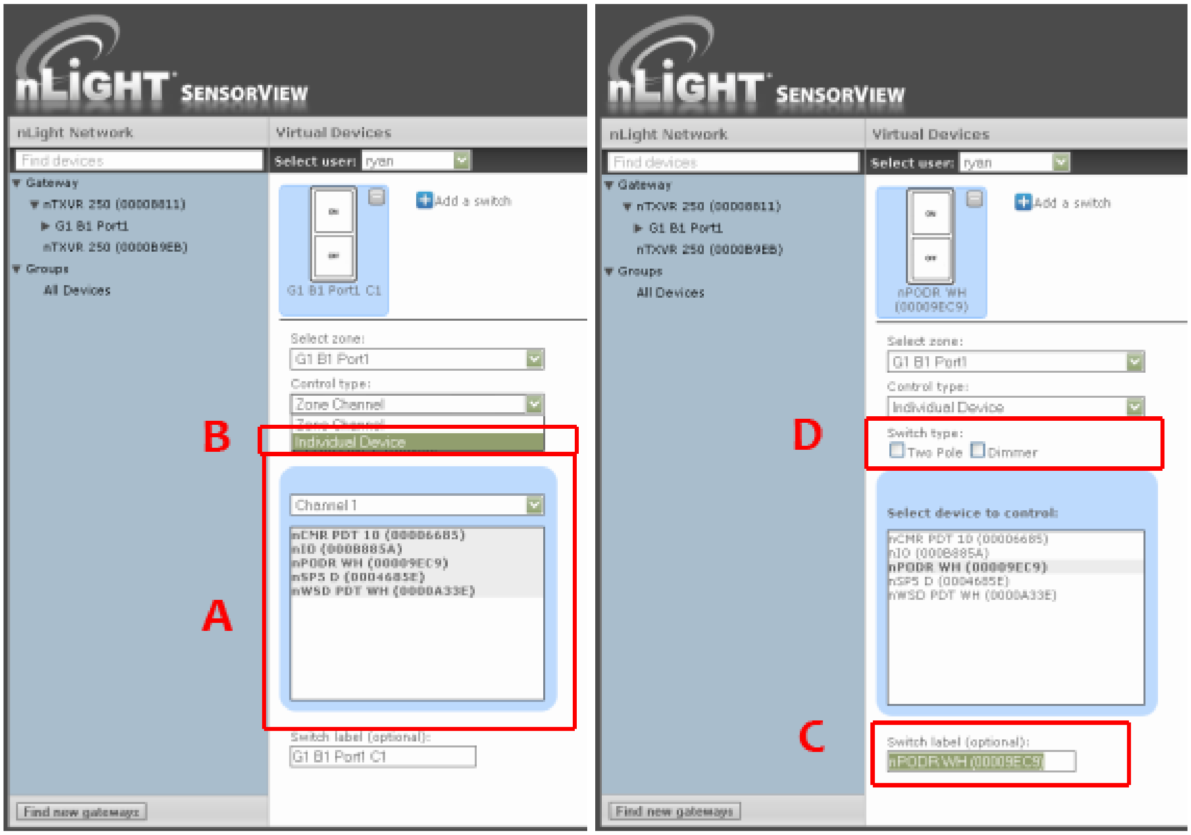
Select a zone (bridge port) to control, as well as an individual device or switch broadcasting channel. For convenience, only the switch channels that devices are tracking within the zone will appear in the channel dropdown menu.

This screen shows the nLight Virtual WallPod controlling all devices connected to the zone that are tracking switch via Channel 1 **(A)**.

To control an individual device, select “Individual Device” from the **Control Type** dropdown **(B)**.

To label the nLight Virtual WallPod, highlight the **Switch Label** box and enter the preferred Switch Label **(C)**.

If the nLight Virtual WallPod is to control dimming or a 2-Pole device, check the appropriate box **(D)**.



Select zone: G1 B1 Port1

Control type: Zone Channel

Zone Channel

Individual Device

Channel 1

nCMR PDT 10 (00006685)
nIO (0000885A)
nPODR WH (00009EC9)
nSPS D (0004685E)
nWSD PDT WH (0000A33E)

Switch label (optional): G1 B1 Port1 C1

Select zone: G1 B1 Port1

Control type: Individual Device

Switch type: □ Two Pole □ Dimmer

Select device to control:

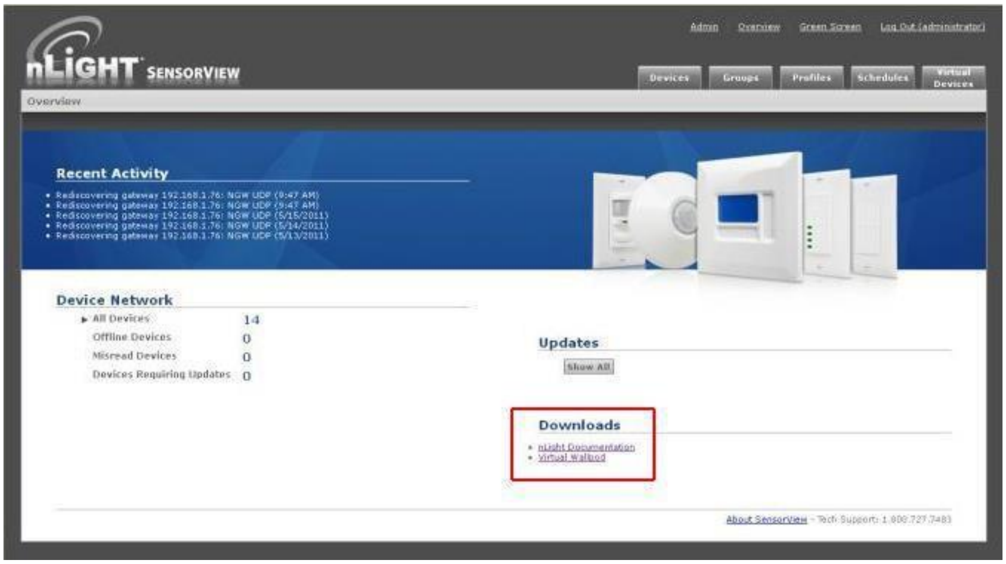
nCMR PDT 10 (00006685)
nIO (0000885A)
nPODR WH (00009EC9)
nSPS D (0004685E)
nWSD PDT WH (0000A33E)

Switch label (optional): nPODR WH (00009EC9)

Virtual WallPod Application

Download the **Virtual WallPod** application from the Overview page of SensorView. Click the **Overview** tab at the top right portion of the screen, then Virtual WallPod under the Downloads section (bottom right) to download.

Note: The download link will only be shown if the Virtual WallPod Plugin has been enabled.



Recent Activity

- Rediscovering gateway 192.168.1.76: NGW UDP (9:47 AM)
- Rediscovering gateway 192.168.1.76: NGW UDP (9:47 AM)
- Rediscovering gateway 192.168.1.76: NGW UDP (5/15/2011)
- Rediscovering gateway 192.168.1.76: NGW UDP (5/14/2011)
- Rediscovering gateway 192.168.1.76: NGW UDP (5/13/2011)

Device Network

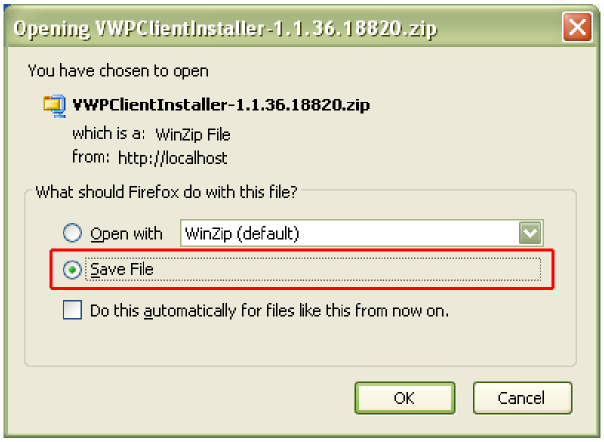
▸ All Devices	14
Offline Devices	0
Misread Devices	0
Devices Requiring Updates	0

Updates

Downloads

- nLight Documentation
- Virtual Wallpod

About SensorView - Tech Support: 1.800.727.7483


Opening VWPClientInstaller-1.1.36.18820.zip

You have chosen to open

VWPClientInstaller-1.1.36.18820.zip

which is a: WinZip File
from: http://localhost

What should Firefox do with this file?

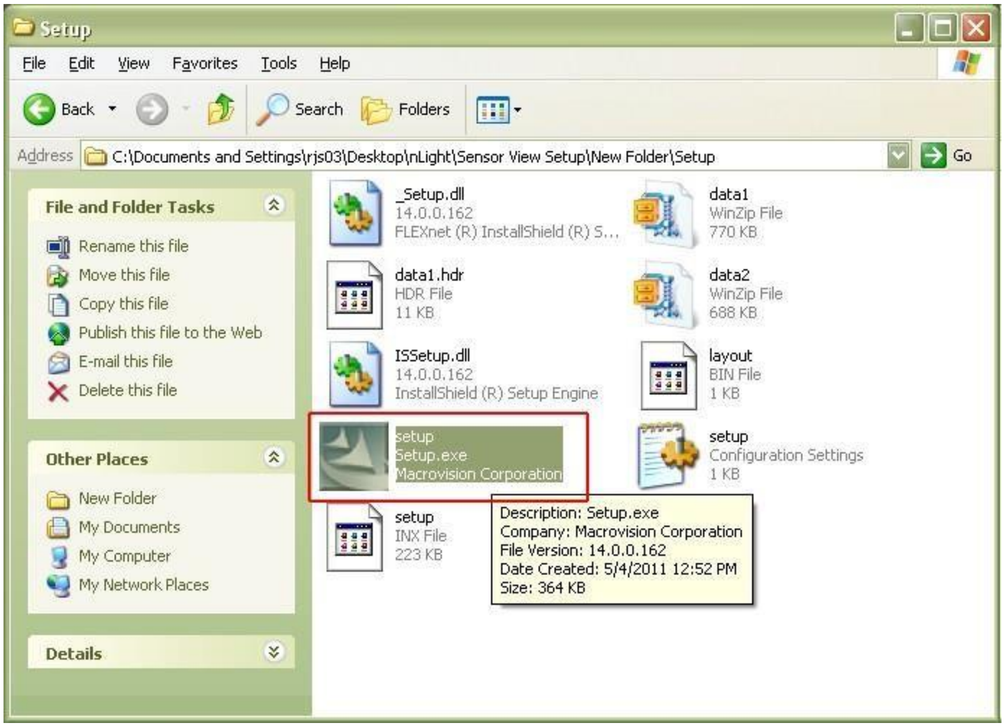
○ Open with WinZip (default)

● Save File

□ Do this automatically for files like this from now on.

It is recommended to save this file to a flash drive so that it can be installed to other machines throughout the network.

Once the files have been downloaded and extracted to a folder, locate it and run setup.exe



Address C:\Documents and Settings\rjs03\Desktop\nLight\Sensor View Setup\New Folder\Setup

_Setup.dll
14.0.0.162
FLEXnet (R) InstallShield (R) S...

data1
WinZip File
770 KB

data1.hdr
HDR File
11 KB

data2
WinZip File
688 KB

ISSetup.dll
14.0.0.162
InstallShield (R) Setup Engine

layout
BIN File
1 KB

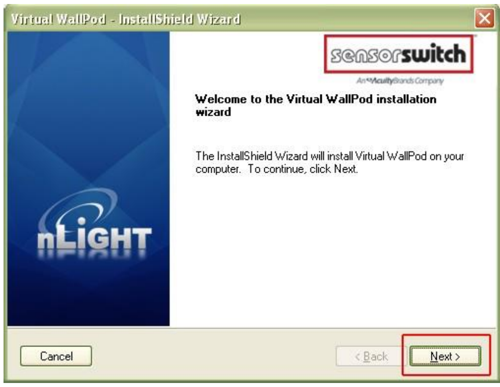
setup
Setup.exe
Macrovision Corporation

setup
Configuration Settings
1 KB

setup
INX File
223 KB

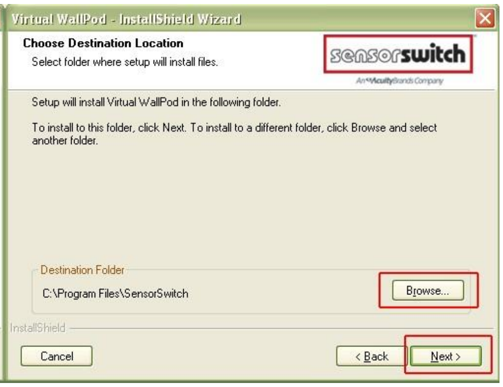
Description: Setup.exe
Company: Macrovision Corporation
File Version: 14.0.0.162
Date Created: 5/4/2011 12:52 PM
Size: 364 KB

Next, follow the setup file's installation steps.



Welcome to the Virtual WallPod installation wizard

The InstallShield Wizard will install Virtual WallPod on your computer. To continue, click Next.



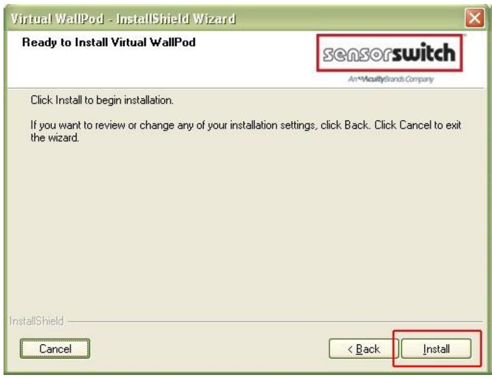
Choose Destination Location

Select folder where setup will install files.

Setup will install Virtual WallPod in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

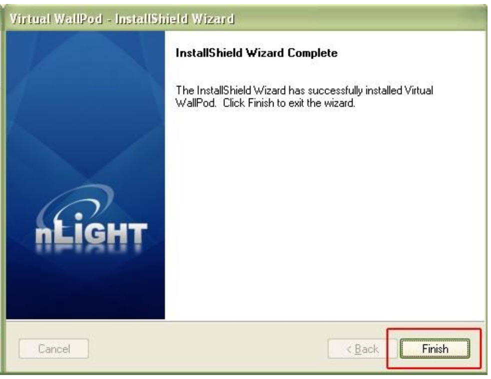
Destination Folder
C:\Program Files\SensorSwitch



Ready to Install Virtual WallPod

Click Install to begin installation.

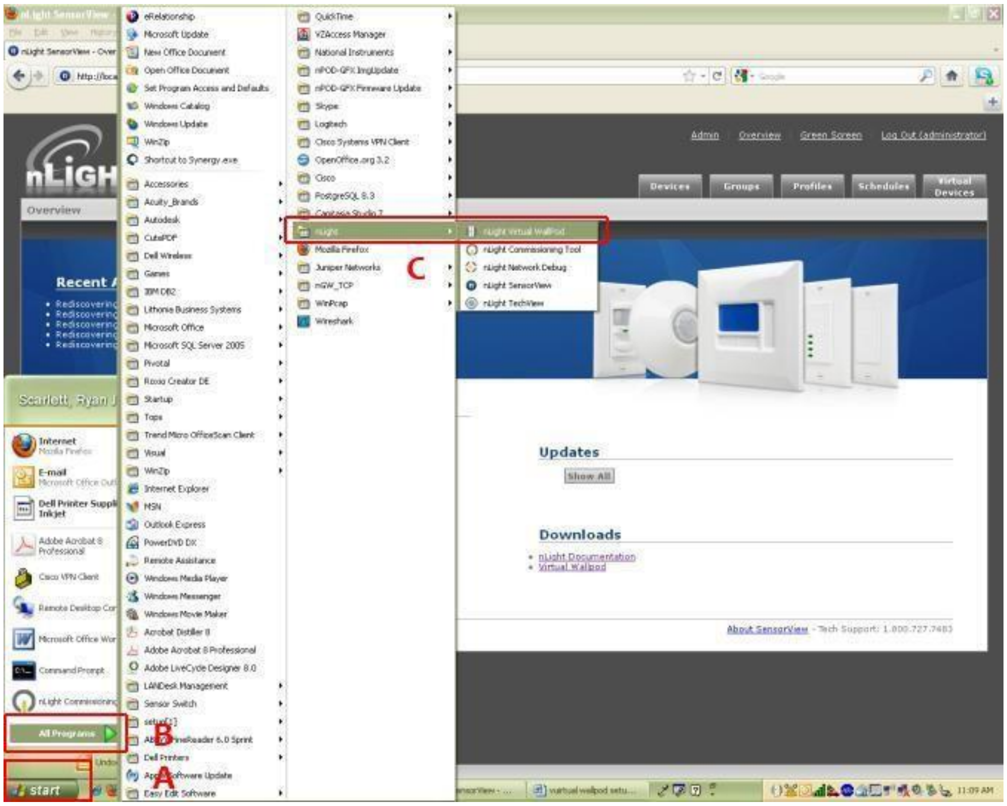
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.



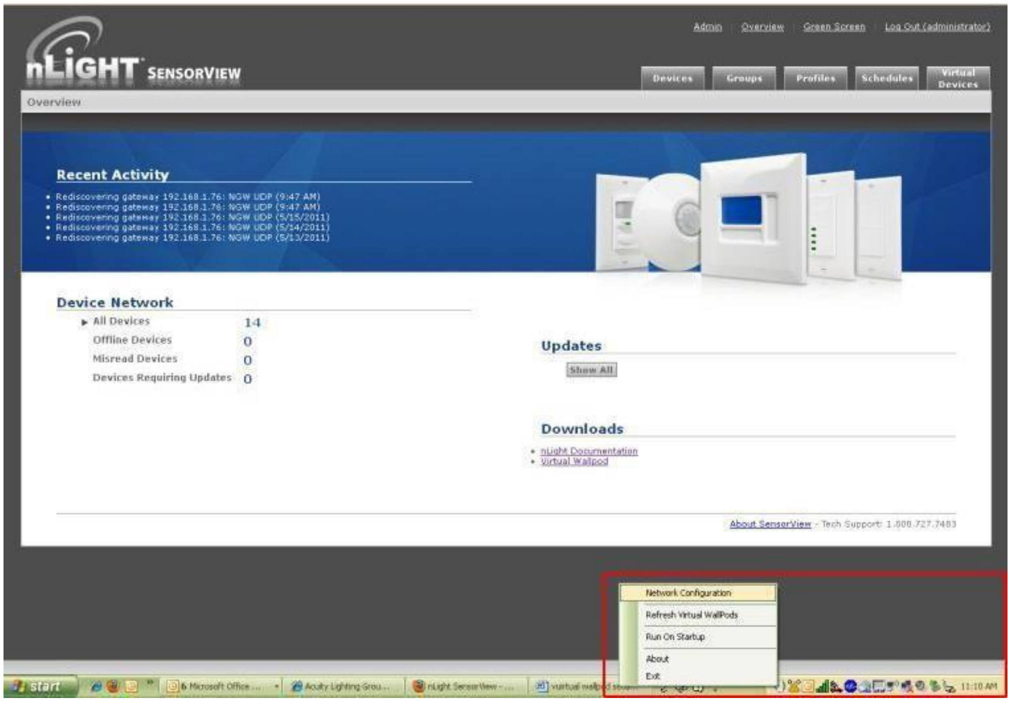
InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Virtual WallPod. Click Finish to exit the wizard.

Once the install is complete, follow the path.



Start/All Programs/nLight/nLight Virtual WallPod. (above)



Recent Activity

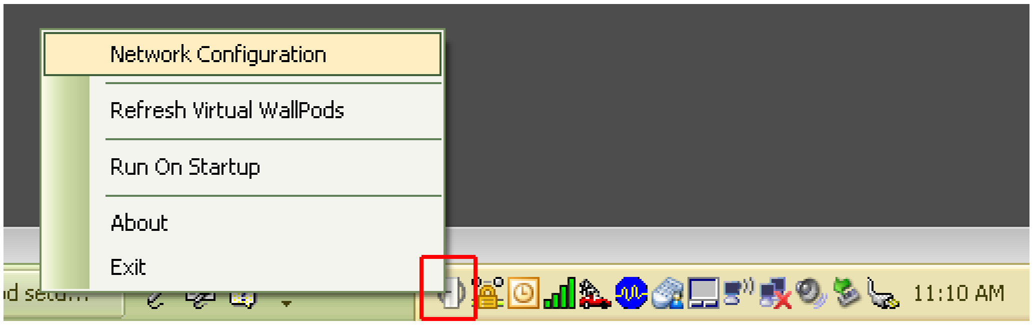
- Rediscovering gateway 192.168.1.76: NGW UDP (9:47 AM)
- Rediscovering gateway 192.168.1.76: NGW UDP (9:47 AM)
- Rediscovering gateway 192.168.1.76: NGW UDP (5/15/2011)
- Rediscovering gateway 192.168.1.76: NGW UDP (5/14/2011)
- Rediscovering gateway 192.168.1.76: NGW UDP (5/13/2011)

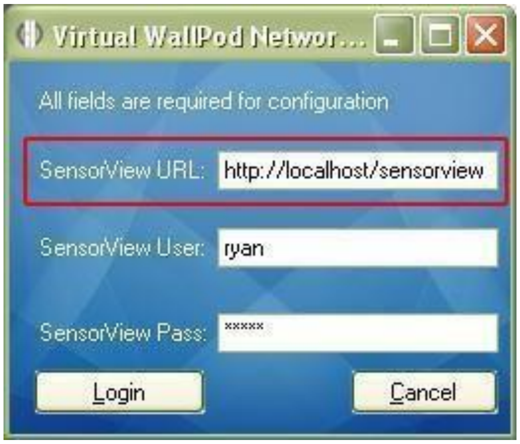
Device Network

▸ All Devices	14
Offline Devices	0
Misread Devices	0
Devices Requiring Updates	0

About SensorView - Tech Support: 1.800.727.7483

Once the icon for the nLight Virtual WallPod appears in the Taskbar, right-click it and enter the network configuration.





All fields are required for configuration

SensorView URL: http://localhost/sensorview

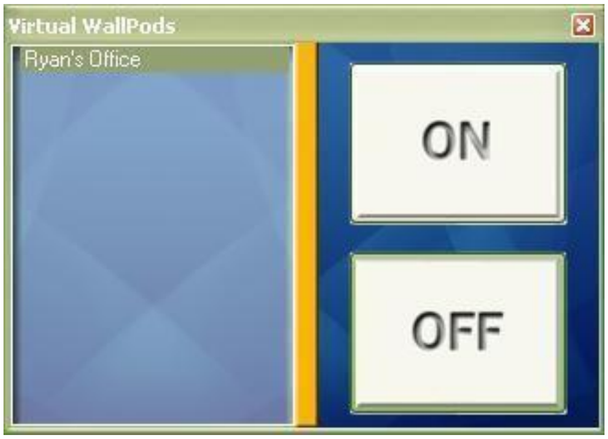
SensorView User: ryan

SensorView Pass: *****

If the nLight Virtual WallPod app is installed to the SensorView host machine, the SensorView URL will match the **(left)** screenshot.

If it is installed to a remote machine (that is on the same LAN or subnet) the SensorView URL will be: http://[host name or IP address]/sensorview
Login as a user assigned one or more Virtual WallPods in SensorView.

The nLight Virtual WallPod is now running and will control the assigned relays.

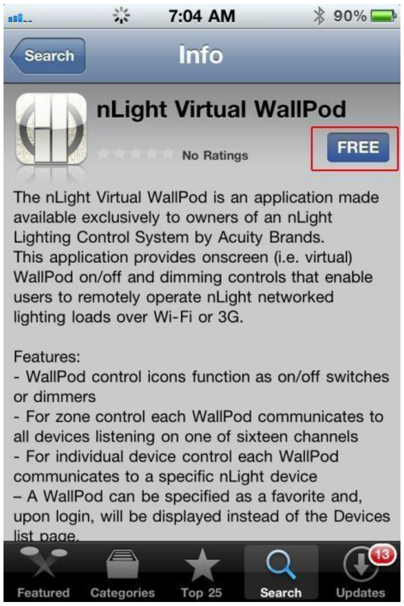


Now that setup for the host machine is complete, the iOS app can be downloaded and installed.

Virtual WallPod iOS App

This section details how to install and setup the Virtual WallPod software for iOS devices.

Download and Install iOS application



The nLight Virtual WallPod is an application made available exclusively to owners of an nLight Lighting Control System by Acuity Brands.
This application provides onscreen (i.e. virtual) WallPod on/off and dimming controls that enable users to remotely operate nLight networked lighting loads over Wi-Fi or 3G.

Features:
- WallPod control icons function as on/off switches or dimmers
- For zone control each WallPod communicates to all devices listening on one of sixteen channels
- For individual device control each WallPod communicates to a specific nLight device
– A WallPod can be specified as a favorite and, upon login, will be displayed instead of the Devices list page.

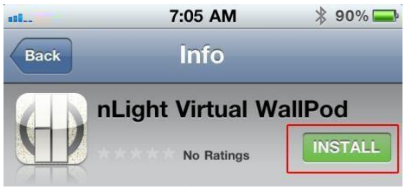
Go to the App Store on the device that will have the nLight Virtual WallPod installed.

Search for **nLight Virtual WallPod**.

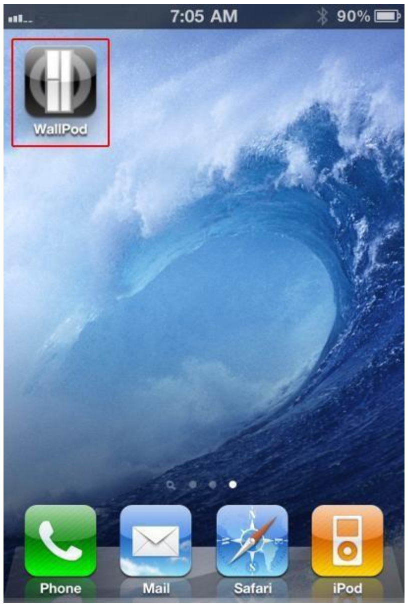
Note that the App is **free of charge**, as is all nLight software.

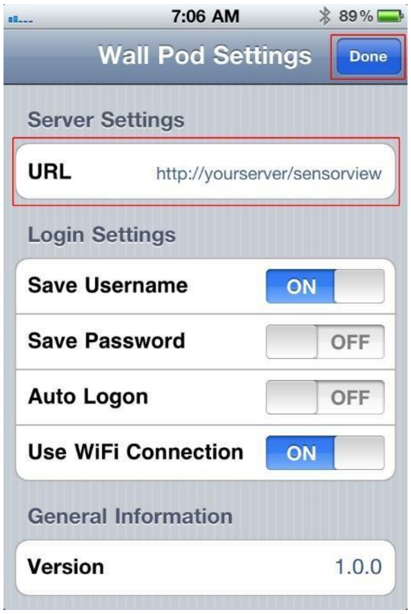
Click **FREE**, followed by the green INSTALL button that appears.

(note: an **iTunes account** is required)



Once installed, **click the WallPod App** icon to launch.





Wall Pod Settings Done

Server Settings

URL http://yourserver/sensorview

Login Settings

Save Username	ON
Save Password	OFF
Auto Logon	OFF
Use WiFi Connection	ON

General Information

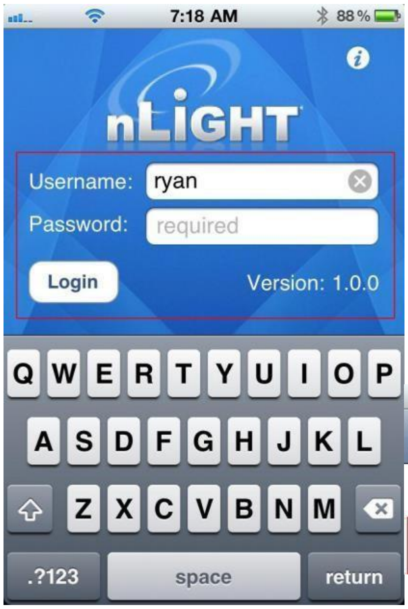
Version 1.0.0

The app will open the WallPod Settings page the first time it’s launched.

Enter the Server Settings URL (replace “yourserver” with host machine’s IP address).

Set **Save Password**
and **Auto Logon** to desired settings.

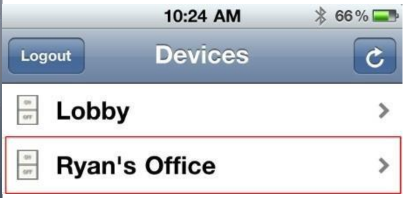
Click **Done**.



Username: ryan

Password: required

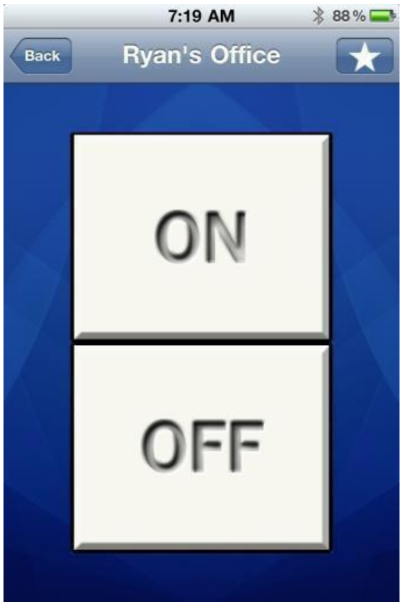
Version: 1.0.0



Login with the user credentials for the nLight Virtual WallPod you wish to control. (left)

Select a switch from the devices list. (right)

Installation is now complete.



Notice that the switch is backlit, indicating that the **relay** controlled by this nLight Virtual WallPod is **closed**, i.e., “turned on.”

Green Screen

This SensorView module logs and analyzes system and building performance. A “Savings Scorecard” calculates energy savings in kWH or dollars.

As with SensorView itself, installing the GreenScreen plug-in should be performed by authorized network administrators.

This will entail installing and setting up a database (PostgreSQL), a driver to connect to the database, a DSN for the data source, initializing the database, starting GreenScreen, and configuring GreenScreen options in SensorView.

Setting up PostgresQL

Setting up PostgreSQL on a computer requires downloading and installing the application, configuring the database to accept remote connections, and restarting the database server.

- PostgreSQL is a separate product that is maintained and developed entirely separate from SensorView and is in no way affiliated with nLight, SensorSwitch, or Acuity Brands.
- For the remainder of this document the phrase “X.Y” will refer to major and minor versions of the version of PostgreSQL being installed; for example: 9.0, 8.4.
- GreenScreen is compatible with PostgreSQL versions 8.4 or higher (9.0 recommended).

1.1 : Installing PostgreSQL

SensorView can use an existing PostgreSQL database or a dedicated one. Which option is most appropriate is at the discretion of the system owner. Download the most recent version for either Windows x86-64 (64 bit) or x86-32 (32-bit). A few notes on the installer:

Super-User Creation Screen:
The screen below configures the default super-user account for PostgreSQL, take note of these

credentials as those will be the default login account and password for the PostgreSQL database.

Port Configuration Screen:
The screen below allows for configuration of the port that PostgreSQL will use for connections. Use whatever value is required by system administrator. Note, SensorView and GreenScreen can be configured to use any port value.

Advanced Options:
The screen below allows for configuration of the locale that PostgreSQL is operating in. The default is almost always sufficient. If the installation site has specific requirements then select the most appropriate option from the drop down. The selected option does not seriously affect GreenScreen operations.

On the final screen, push “Next” to finish the installation of PostgreSQL onto the local computer.

1.2 : Allowing Remote Connections

This step is only necessary if SensorView and the PostgreSQL database reside on separate computers. By default, PostgreSQL will not allow any remote connections; to change this, administrative access to the host machine for the database is required. To setup PostgreSQL to allow remote connections, go to the directory PostgreSQL was installed at (by default C:\Program Files\PostgreSQL), from that folder open the file at X.Y\data\pg_hba.conf; this file can be opened in notepad or any generic text editor. For how to configure pg_hba.conf, as well as any questions, refer to: _______________, _______________

For all database versions, adding the following line to the bottom of the file to allow ALL remote connections to the database:

host all 0.0.0.0/0 md5

Note, allowing all connections is a potential security risk that should be weighed by system owners.

Save the changes and close the file. PostgreSQL will now accept remote connections from the configured host.

1.3 : Tuning PostgreSQL (Optional)

By default PostgreSQL is tuned for systems with low memory sets. By changing a few configuration parameters GreenScreen database queries can be significantly sped up. To change configuration options go to the directory in which PostgreSQL was installed (by default C:\Program Files\PostgreSQL). From that folder open the file X.Y\data\postgresql.conf with notepad or any generic text editor. Note that some of the following setting recommendations are based on the total system RAM available. Before entering the new values look up how much total RAM is installed in the computer (right click on My Computer and select Properties) and convert that value to MB (note that 1GB = 1024 MB).

The following changes are suggested to improve performance (note that leaving a # in front of a line denotes a comment and the value will be ignored; remove any leading # for the setting to take effect.

shared_buffers
Set to 25% of system RAM (not exceeding 512MB (256MB recommended for most installs)
default is 32MB

effective_cache_size
50-75% total RAM (in MB)
default is 128MB

After making changes to the configuration the PostgreSQL service must be restarted (1.4) before the new settings will take effect.

Note: Overall system performance may vary. Modifying values may have a result on overall system performance and stability, if problems persist revert modified settings to original values.

Sensor Switch is not responsible for any non-SensorView issues this may cause. .

1.4 : Restarting PostgreSQL

PostgreSQL must be restarted before the changes made to pg_hba.conf will take effect. If no changes were made to pg_hba.conf then this step is unnecessary. Go to Start Menu -> Control Panel -> Administrative Tools -> Services (Windows XP / Server 2003) or Start Menu -> Control Panel -> System and Security -> Administrative Tools -> Services (Windows Vista / 7 / Server 2008).

In the services window select the following service:

8.4
PostgreSQL Server 8.4

9.0
(32 bit) postgresql-9.0-PostgreSQL Server 9.0

9.0
(64 bit) Postgresql-x64-9.0

Right click on the relevant service name and select Restart; this will restart the database server.

1.5 : Firewall Setup

If the computer running PostgreSQL is a different from the computer running SensorView, then the firewall on the computer running PostgreSQL may need to be updated to allow for incoming connections on whichever port PostgreSQL was configured to listen on. This will vary depending on the firewall software in use.

Setting Up Database Connection

A connection to the database that GreenScreen will store data in must be configured. This involves downloading and installing a driver for the database and configuring a system DSN that specifies the connection parameters to SensorView and GreenScreen. Both steps 2.1 and 2.2 must be performed on the computer that is running SensorView.

2.1 : Installing a PostgreSQL Driver

For SensorView to connect and control the PostgreSQL database a driver must be installed on the machine hosting SensorView. Download the Windows driver (x32 and x64). After downloading open the zip file, run psqlodbc.msi, and install the driver.

2.2 : DSN Configuration

DSNs provide a way to configure a datasource connection in a standard consistent way that can be used throughout the machine. A DSN must be configured to allow SensorView and GreenScreen to connect to the database; this must be done on the machine running SensorView. A DSN consists of a name, database, server, port, user, password, and SSL connection requirements. Locating the correct DSN configuration tool varies depending on the specific version of Windows and whether or not it is 64 bit.

- To configure a DSN for Windows XP 32 bit / Server 2003 bit go to: **Start Menu -> Control Panel -> Administrative Tools -> Data Sources (ODBC)**
- To configure a DSN for all 64 bit variants of Windows go to: **Start Menu -> Run -> type C:\Windows\SysWOW64\odbcad32.exe and press Enter (Assuming Windows is installed to C:, otherwise substitute correct system path)**
- To configure a DSN for Windows Vista 32 bit / 7 32 bit / Server 2008 32 bit go to: **Start Menu -> Control Panel -> System and Security -> Administrative Tools ->Data Sources (ODBC)**

Once the Data Sources (ODBC) popup is open, select the tab System DSN, then press Add. Select a datasource from the list. The name of the driver will vary depending on what was installed, commonly for 32 bit the name will be “PostgreSQL Unicode”, this is the driver that was previously installed during PostgreSQL setup (2.1). Select Finish and a form will appear with additional fields to fill out.

Fill out the form with the following values:

- **Data Source:** A custom name for the DSN that will be put into SensorView
- **Database:** nlight_system_data

- **Server:** IP Address or hostname of machine running PostgreSQL server. (127.0.0.1 or localhost for local computer)
- **Port:** Port PostgreSQL was configured to run on (by default 5432)
  User name Account name for the database user
- **Password:** Account password for the database user
- **SSL Mode:** As appropriate for the database (disabled by default)

Select Save. Note, the Data Source name value as this is the field that must be entered into SensorView later. Note that pressing the Test button will fail with "database not found" until step 3.1 has been completed. For testing purposes you can change the datasource name to read 'postgres', and then test, if the connection is successful then change the datasource parameter back to nlight_system_data, otherwise check the other parameters that were entered.

Setting Up GreenScreen

In order to configure and run SensorView the plug-ins component must be installed. For new installs this can be accomplished by making sure that plug-ins is checked during the feature select portion of the SensorView install. For existing installations, run the installer and select Modify, then check plug-ins and push modify. Once the plug-in components have been installed, open SensorView and go to the Admin page and select Plug-ins.

3.1 : Administrator Email (Recommended)

GreenScreen will notify the administrator via email if it encounters any issues while attempting to start. To configure email notification the administrator use of SensorView must have an email address entered; additionally the Mail Server section (found at Admin >Setup->Mail Server) must be filled out to allow for email to be sent from SensorView. Notification emails will be sent in two specific instances, if the host Windows service crashes (and the subsequent automatic restart fails); or if, while starting up, GreenScreen is unable to start due to version requirements, improper configuration, or any unexpected error.

3.2 : Database Initialization

Once PostgreSQL, the database driver, and the system DSN have been set up and configured, the last step is to build the GreenScreen database and start the service. To build the database, in SensorView, go to Admin -> Databases. At the bottom of the screen is the GreenScreen Database Setup section. Input the name of the custom DSN that was previously configured and SensorView will build the database (upon hitting save). If the credentials supplied in the DSN do not have the create database privilege, then SensorView will prompt for credentials that do. SensorView will use those credentials to create the database and give ownership to the credentials in the DSN. Afterwards the other, higher, set of credentials will be discarded.

3.3 : Starting GreenScreen

In order to start GreenScreen, the plug-ins component must have previously been installed (3.0); if this has not been done then there will be no Plug-ins tab. Proceed to the Admin screen in SensorView and select Plug-ins. The host service should already be running; if it is not then the username, password, and domain (optional) must be filled out, then start the nLight Plug-in Host Service. Once this is running GreenScreen can be started and stopped in the top window.

3.4 : GreenScreen Operations

Within the accordion select GreenScreen; on this page options can be set that will configure how GreenScreen will compute savings and what units to display them in. Note that displaying savings in dollars requires electrical generation rate information be entered on the Admin->Plugins->GreenScreen section.

Display Options:
SensorView can be configured to show savings in dollars or kWh. For CO2 savings, the generation type for the electricity can be selected that will be used to determine CO2 savings.

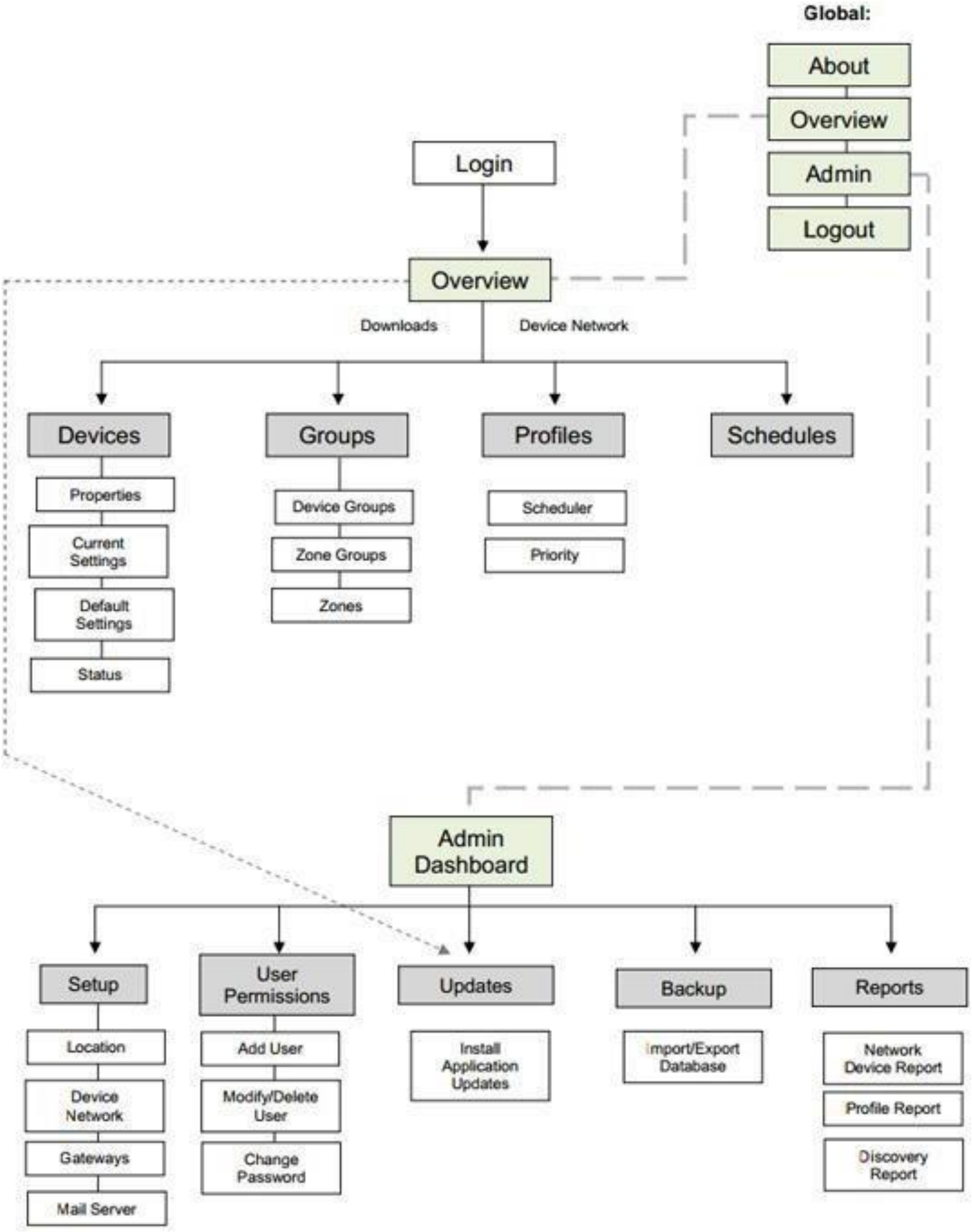
Electrical Rates:
SensorView can be configured with the building's electrical rates. Set the rate and time periods in which the rate applies. These settings will only be used if SensorView is set to display savings in dollars.

Baseline Periods:
During these periods, SensorView will assume the building is occupied. Energy savings (whether in dollars or kWh) are relative to how much energy would have been spent, with all control points in the system being on for the duration of the baseline periods. Refer to the GreenScreen data sheet for a more detailed explanation of savings analysis.

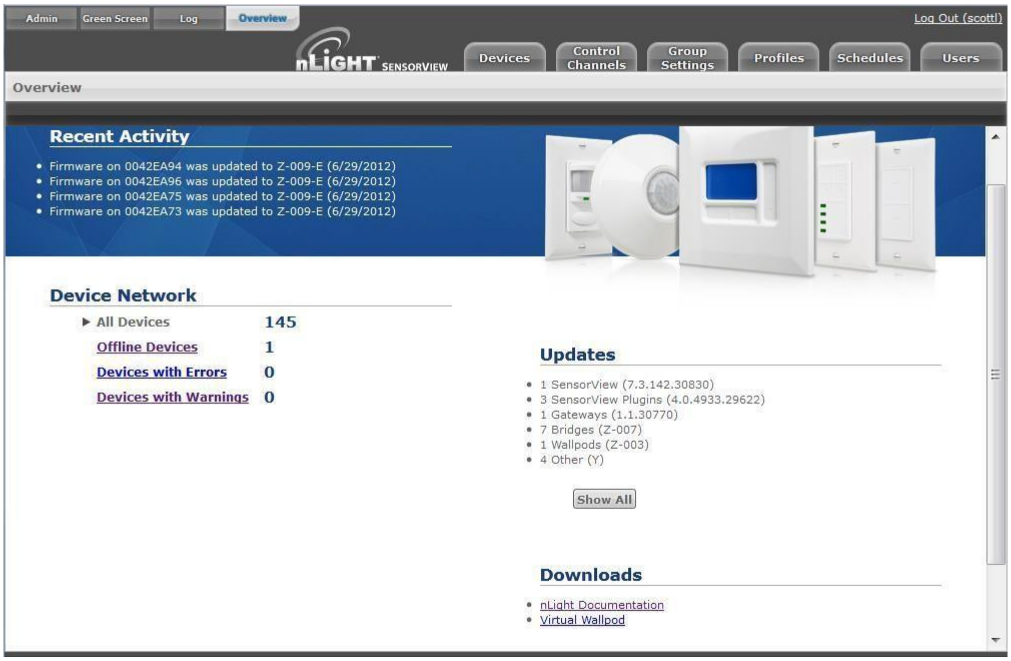
Hit **Save Settings** to save the configuration.

Once SensorView has a valid Data Source which can connect to the database, it will display the current size of the database and the state of hosting service in the bottom left corner of the screen (completed in step 3.1).

SensorView Page Mapping



Overview



Recent Activity

- Firmware on 0042EA94 was updated to Z-009-E (6/29/2012)
- Firmware on 0042EA96 was updated to Z-009-E (6/29/2012)
- Firmware on 0042EA75 was updated to Z-009-E (6/29/2012)
- Firmware on 0042EA73 was updated to Z-009-E (6/29/2012)

Device Network

▶ All Devices	145
Offline Devices	1
Devices with Errors	0
Devices with Warnings	0

Updates

- 1 SensorView (7.3.142.30830)
- 3 SensorView Plugins (4.0.4933.29622)
- 1 Gateways (1.1.30770)
- 7 Bridges (Z-007)
- 1 Wallpods (Z-003)
- 4 Other (Y)

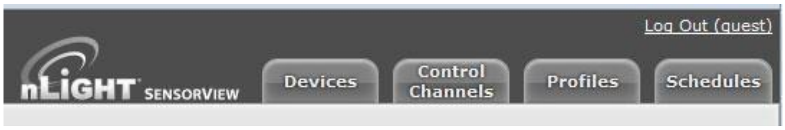
Downloads

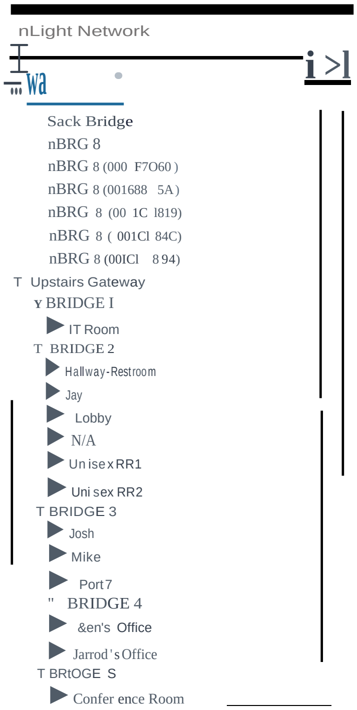
- nLight Documentation
- Virtual Wallpod

A successful login opens the **Overview** page, showing:

- a list of all recent activity, including Firmware updates (upper left)
- a **Device Network** report showing a count of offline and total devices (lower left)
- a list of all current updates available, with direct links to download and install them. (lower right)
- Upper left
    - **Admin** allows authorized administrators to setup and configure SensorView and perform updates.
    - **Green Screen** (upper left) provides a historical and real-time status on energy savings resulting from your installed nLight systems. For in-depth info: Green Screen.
    - **Log** displays troubleshooting data.
    - **Overview** returns users to the Overview Screen.

The Overview page features four clickable tabs along the top.





nLight Network

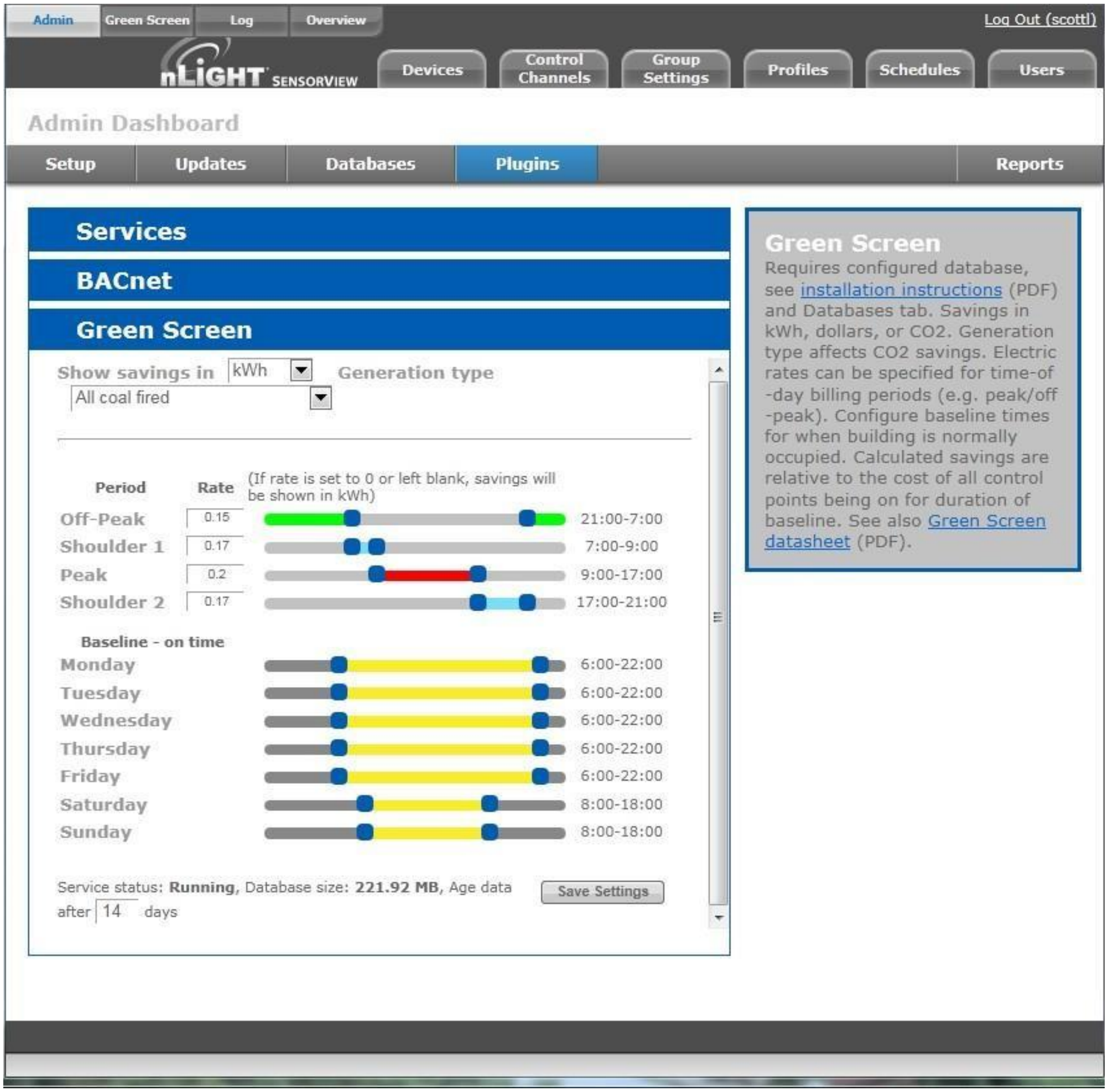
Sack Bridge
nBRG 8
nBRG 8 (000 F7O60)
nBRG 8 (001688 5A)
nBRG 8 (00 1C l819)
nBRG 8 (001Cl 84C)
nBRG 8 (00ICl 8 94)
T Upstairs Gateway
Y BRIDGE I
IT Room
T BRIDGE 2
Hallway-Restroom
Jay
Lobby
N/A
Unisex RR1
Uni sex RR2
T BRIDGE 3
Josh
Mike
Port 7
" BRIDGE 4
&en's Office
Jarrod's Office
T BRtOGE S
Confer ence Room

Green Screen

This SensorView **GreenScreen** module logs and analyzes system and building performance. A "Savings Scorecard" calculates energy savings in kWH or dollars.

Detailed graphs show performance over user selected time scales. This data can be used to monitor space and lighting usage, optimize time delays, and better utilize available daylight. Data is also provided to the user in downloadable reports.

Green Screen Admin



Show savings in kWh Generation type All coal fired

Period	Rate	(If rate is set to 0 or left blank, savings will be shown in kWh)
Off-Peak	0.15	21:00-7:00
Shoulder 1	0.17	7:00-9:00
Peak	0.2	9:00-17:00
Shoulder 2	0.17	17:00-21:00

Baseline - on time	
Monday	6:00-22:00
Tuesday	6:00-22:00
Wednesday	6:00-22:00
Thursday	6:00-22:00
Friday	6:00-22:00
Saturday	8:00-18:00
Sunday	8:00-18:00

Service status: **Running**, Database size: **221.92 MB**, Age data after 14 days

Green Screen

Requires configured database, see installation instructions (PDF) and Databases tab. Savings in kWh, dollars, or CO2. Generation type affects CO2 savings. Electric rates can be specified for time-of-day billing periods (e.g. peak/off-peak). Configure baseline times for when building is normally occupied. Calculated savings are relative to the cost of all control points being on for duration of baseline. See also Green Screen datasheet (PDF).

Green Screen requires a configured database (see installation instructions and tab).

The top pull-down allows users to select Savings in **kWh**, **dollars**, or **CO2**.

Generation type indicates a rate of CO2 production to energy consumption and affects CO2 savings.

Electric rates can be specified for time-of-day billing periods (e.g. peak/off-peak). Use the sliders to define time intervals for a specific facility using nLight devices.

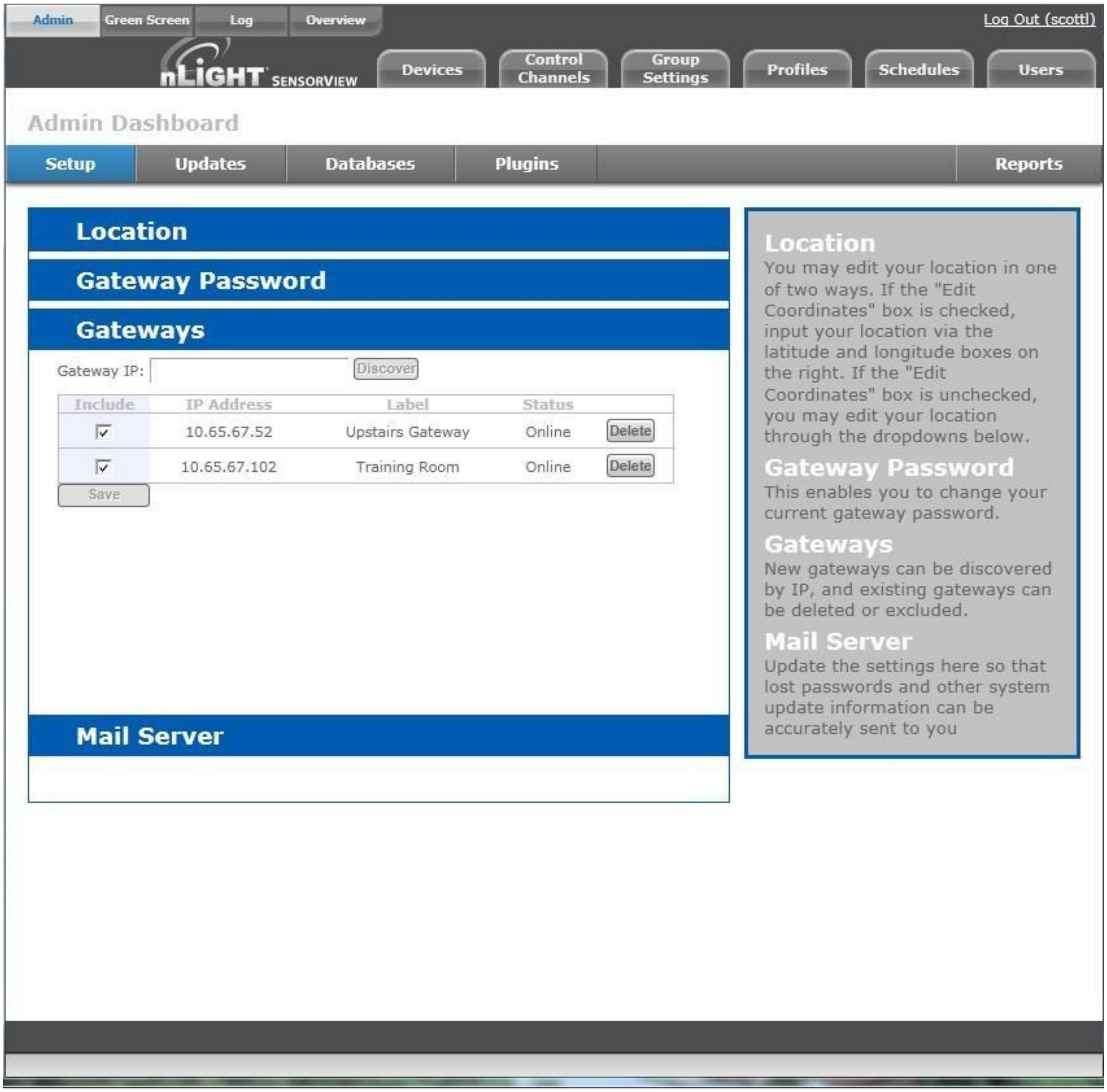
Baseline times should be configured for each day of the week, according to normal building occupancy. Calculated savings are relative to the cost of all control points being on for the duration of the baseline.

The bottom line displays basic statistics and status about GreenScreen. It provides indications about the current data aging setting, the size of the database on disk, and the current status of the GreenScreen Plugin.

When configuration or changes are completed, click **Save Settings**.

See also Green Screen datasheet (PDF).

Admin



Admin Dashboard

Location

Gateway Password

Gateways

Gateway IP:

Include	IP Address	Label	Status	
☑	10.65.67.52	Upstairs Gateway	Online	Delete
☑	10.65.67.102	Training Room	Online	Delete

Mail Server

Location
You may edit your location in one of two ways. If the "Edit Coordinates" box is checked, input your location via the latitude and longitude boxes on the right. If the "Edit Coordinates" box is unchecked, you may edit your location through the dropdowns below.

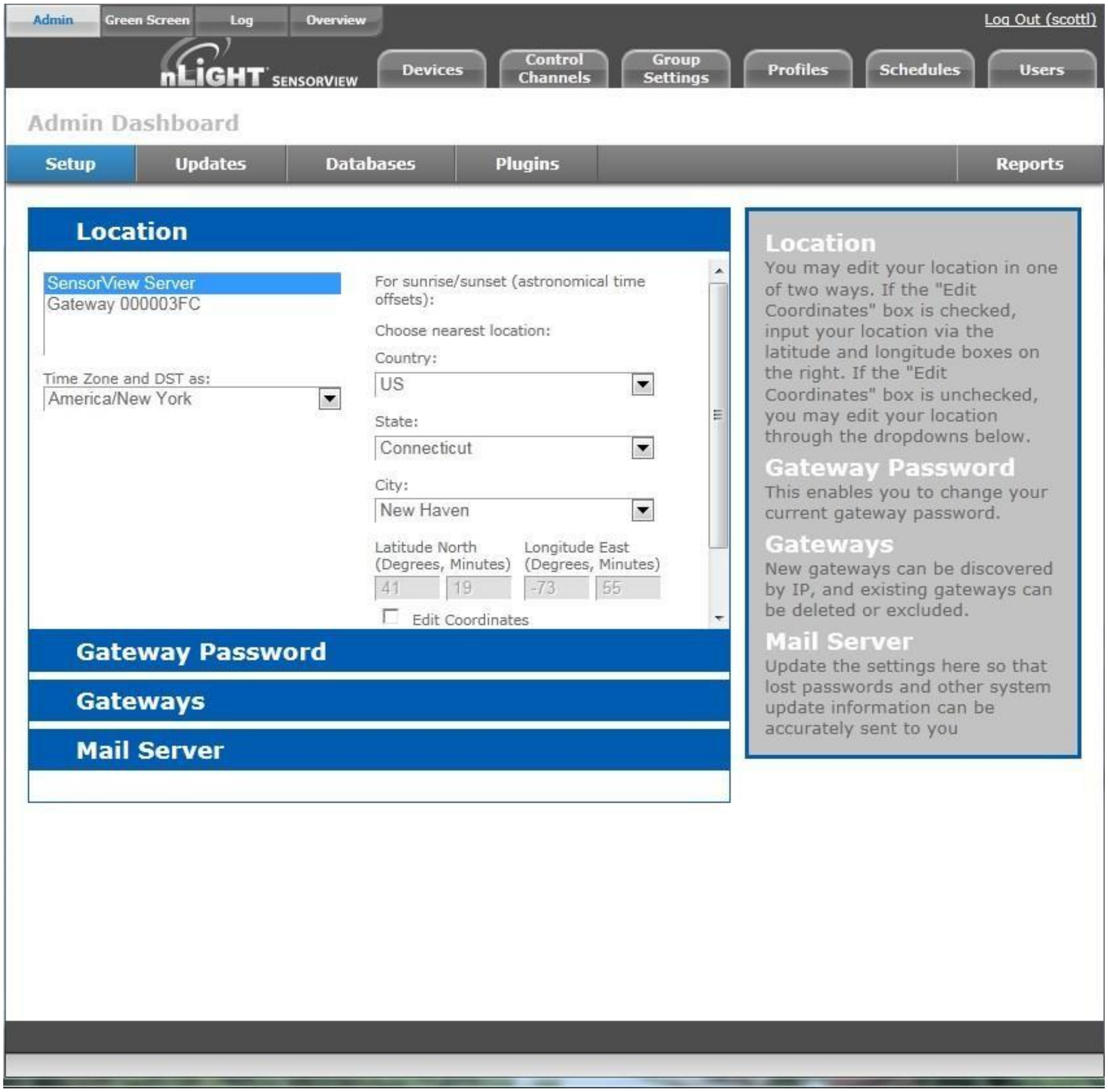
Gateway Password
This enables you to change your current gateway password.

Gateways
New gateways can be discovered by IP, and existing gateways can be deleted or excluded.

Mail Server
Update the settings here so that lost passwords and other system update information can be accurately sent to you

The Admin tabs are for administrators only, and will not be accessed by a day to day end user.

Setup



Location

SensorView Server
Gateway 000003FC

Time Zone and DST as: America/New York

For sunrise/sunset (astronomical time offsets):

Choose nearest location:

Country: US

State: Connecticut

City: New Haven

Latitude North (Degrees, Minutes): 41 19

Longitude East (Degrees, Minutes): -73 55

☐ Edit Coordinates

Gateway Password

Gateways

Mail Server

Location
You may edit your location in one of two ways. If the "Edit Coordinates" box is checked, input your location via the latitude and longitude boxes on the right. If the "Edit Coordinates" box is unchecked, you may edit your location through the dropdowns below.

Gateway Password
This enables you to change your current gateway password.

Gateways
New gateways can be discovered by IP, and existing gateways can be deleted or excluded.

Mail Server
Update the settings here so that lost passwords and other system update information can be accurately sent to you

The Admin Setup screen displays four setup categories:
Location, Gateway Password, Gateways, and Mail Server.

Location

- **Time zone** – Select Time zone from pull-down menu
- **Select Location** – Country, State, nearest City

Location settings allow a gateway to be aware of what time zone and daylight savings rules it should apply. Specifying the location also allows the gateway to determine the proper astronomical time for schedules using sunrise or sunset.

You may edit your location in one of two ways. If the “Edit Coordinates” box is checked, input your location via the latitude and longitude boxes on the right.

If the “Edit Coordinates” box is unchecked, you may edit your location through the dropdowns below.

Gateway Password

This enables authorized users to change current gateway password. Configuring a gateway password ties gateways to your particular SensorView, and prevents unauthorized users from using a different SensorView to modify the system; as well as restricting direct configuration access to the gateways.

Gateways

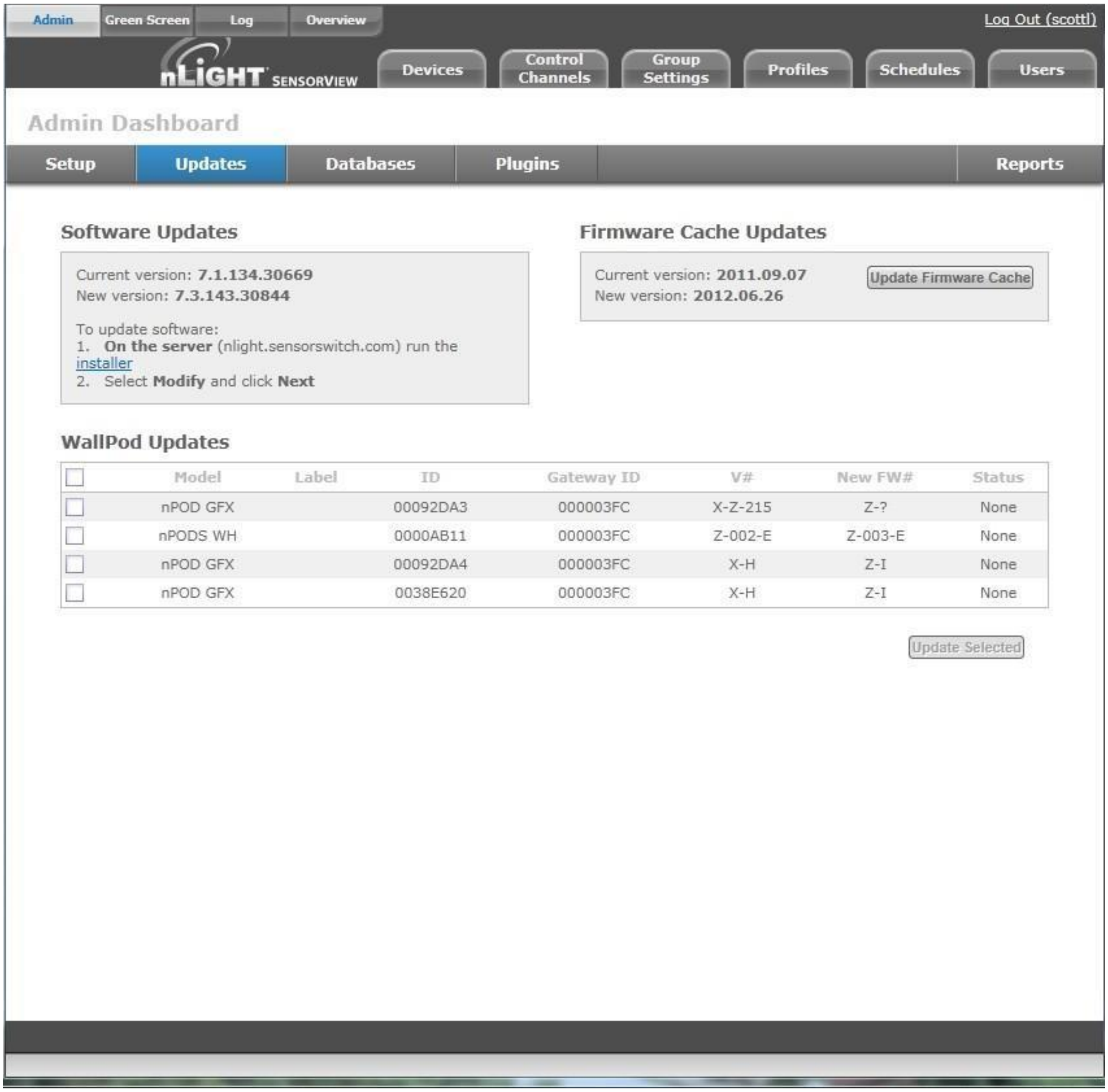
New gateways can be discovered by IP, and existing gateways can be deleted or excluded.

Mail Server

Update the settings here in order to receive important system notifications.

Updates

On this screen both software and device firmware updates are performed.



Admin Dashboard

Software Updates

Current version: **7.1.134.30669**
New version: **7.3.143.30844**

To update software:
1. **On the server** (nlight.sensorswitch.com) run the installer
2. Select **Modify** and click **Next**

Firmware Cache Updates

Current version: **2011.09.07**
New version: **2012.06.26**

WallPod Updates

□	Model	Label	ID	Gateway ID	V#	New FW#	Status
□	nPOD GFX		00092DA3	000003FC	X-Z-215	Z-?	None
□	nPODS WH		0000AB11	000003FC	Z-002-E	Z-003-E	None
□	nPOD GFX		00092DA4	000003FC	X-H	Z-I	None
□	nPOD GFX		0038E620	000003FC	X-H	Z-I	None

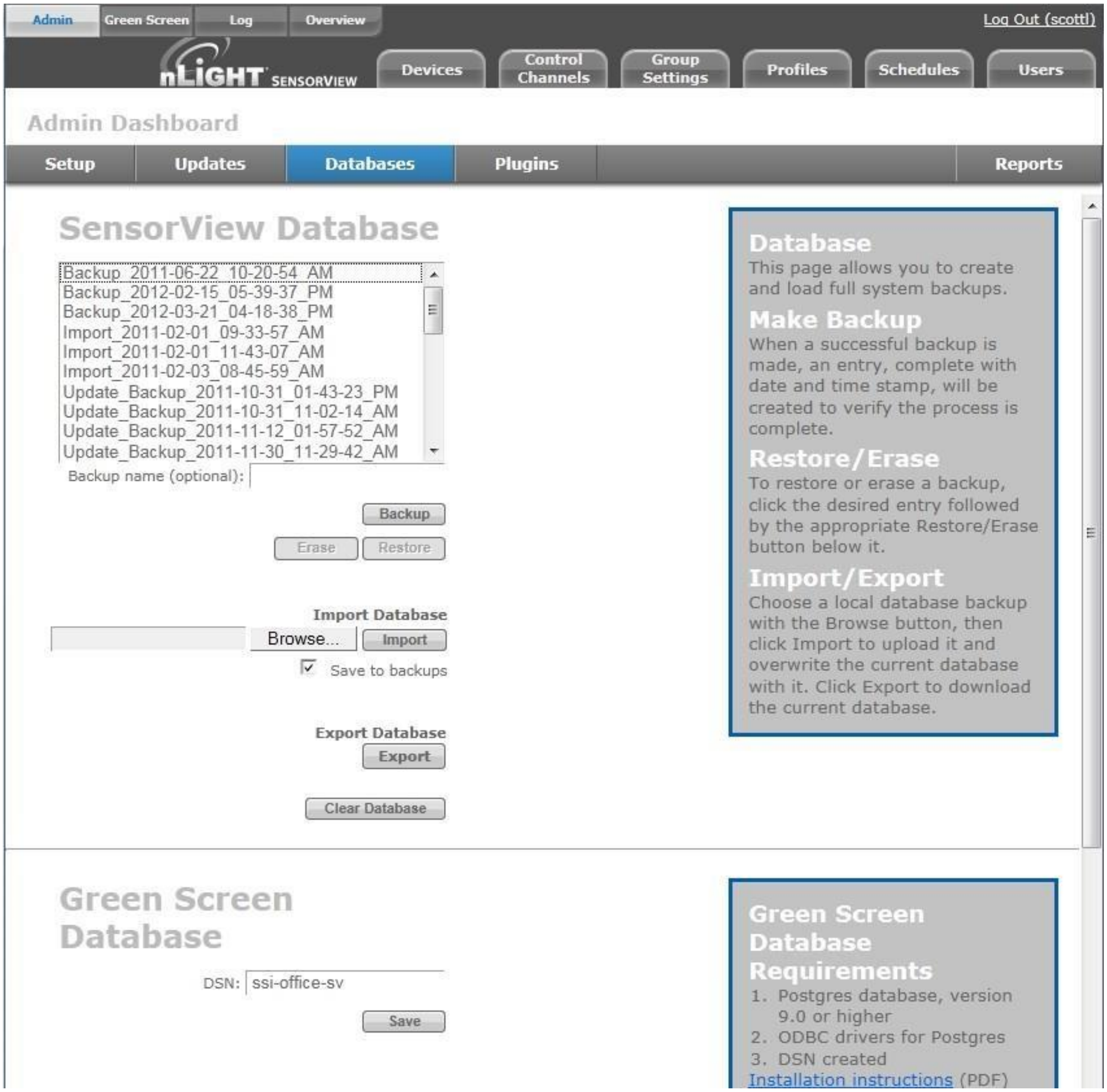
All updates are retrieved automatically from the internet and can be applied at the users' discretion. Additionally a firmware cache component is available that allows users to perform device updates without an active internet connection. Updates are only shown for components in which an update is actually available.

It is recommended that users run the latest version of SensorView and device firmware to ensure maximum efficiency and utility of nLight devices and networks.

For step by step information on how to update SensorView please see .

Databases

The Admin **Database** page allows you to create and load full system backups.



SensorView Database

Backup_2011-06-22_10-20-54_AM
Backup_2012-02-15_05-39-37_PM
Backup_2012-03-21_04-18-38_PM
Import_2011-02-01_09-33-57_AM
Import_2011-02-01_11-43-07_AM
Import_2011-02-03_08-45-59_AM
Update_Backup_2011-10-31_01-43-23_PM
Update_Backup_2011-10-31_11-02-14_AM
Update_Backup_2011-11-12_01-57-52_AM
Update_Backup_2011-11-30_11-29-42_AM

Backup name (optional):

Import Database

☑ Save to backups

Export Database

Database
This page allows you to create and load full system backups.

Make Backup
When a successful backup is made, an entry, complete with date and time stamp, will be created to verify the process is complete.

Restore/Erase
To restore or erase a backup, click the desired entry followed by the appropriate Restore/Erase button below it.

Import/Export
Choose a local database backup with the Browse button, then click Import to upload it and overwrite the current database with it. Click Export to download the current database.

Green Screen Database

DSN: ssi-office-sv

Green Screen Database Requirements
1. Postgres database, version 9.0 or higher
2. ODBC drivers for Postgres
3. DSN created

Installation instructions (PDF)

Database Selection (left side of browser) displays all databases available for your admin user account. There are multiple types of databases from which to select.

- **Automatic_Backup** – Backup of a current or formerly active database. Databases are automatically backed up daily (by default) and receive this label prefix.

- **Backup** – a backup of a database that has been created on an as-needed or as-desired basis. Administrators may backup the database at any time. To backup a database from the list, select the desired database, enter a name in the “backup name” field, and click **Backup**.
- **Import** -an imported database
- **Update** – a database backup created while updating SensorView.

Backup, Erase, Restore Buttons

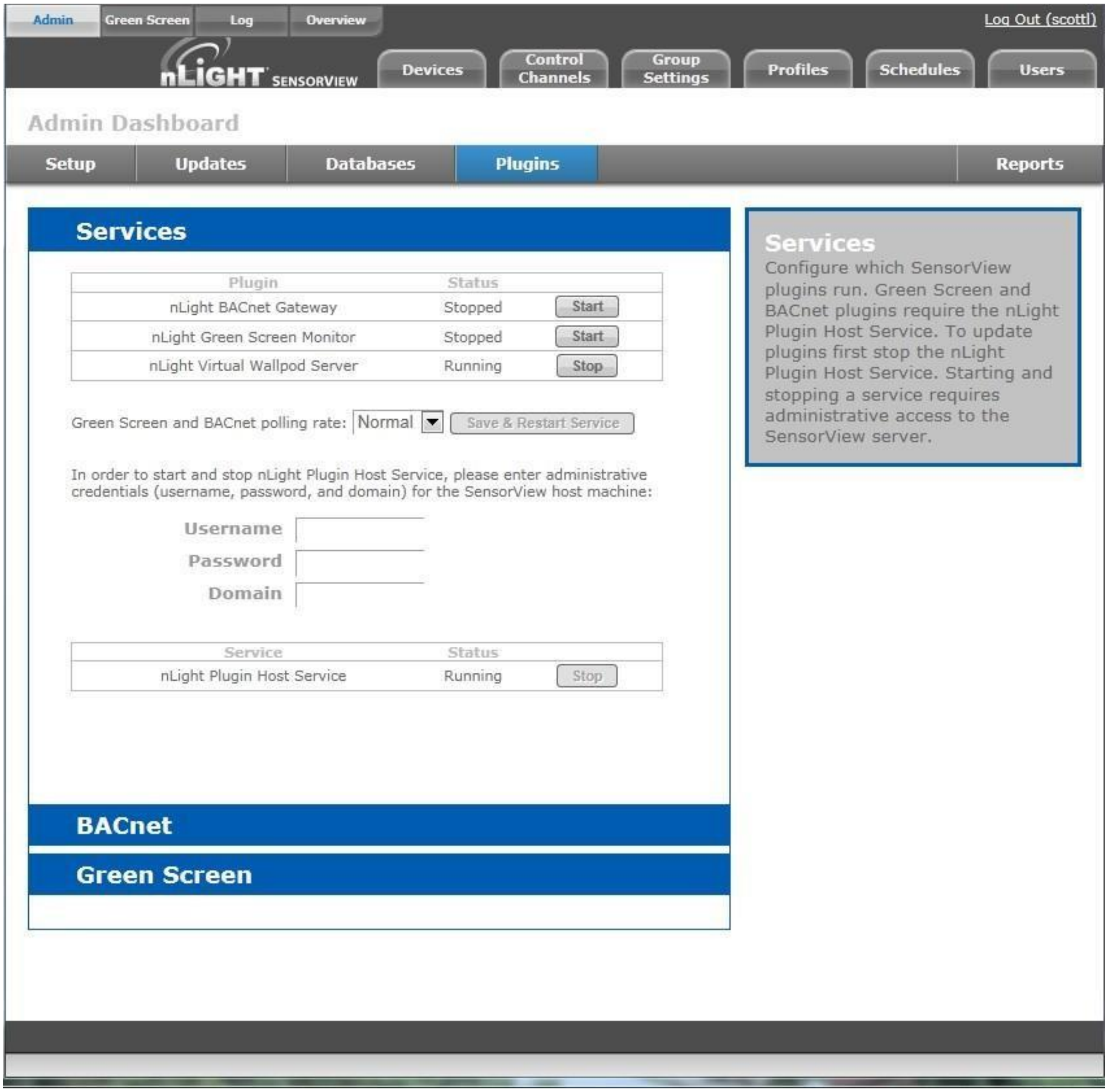
Any database selected from the list can be Backed up, Erased or Restored.

- **Make Backup** – When a successful backup is made, an entry, complete with date and time stamp, will be created to verify the process is complete.
- **Restore/Erase** – To **restore** or **erase** a backup, click the desired entry followed by the appropriate button.
- **Import** – Choose a database backup with the **Browse** button, then click **Import** to upload it and overwrite the current database.
- **Export** – Click to download the current database.

Plugins

The Admin dashboard for Plugins- **Services**, **BACnet** and **GreenScreen**.

Services



Services

Plugin	Status	
nLight BACnet Gateway	Stopped	Start
nLight Green Screen Monitor	Stopped	Start
nLight Virtual Wallpod Server	Running	Stop

Green Screen and BACnet polling rate: Normal ▾ Save & Restart Service

In order to start and stop nLight Plugin Host Service, please enter administrative credentials (username, password, and domain) for the SensorView host machine:

Username
Password
Domain

Service	Status	
nLight Plugin Host Service	Running	Stop

BACnet

Green Screen

Services
Configure which SensorView plugins run. Green Screen and BACnet plugins require the nLight Plugin Host Service. To update plugins first stop the nLight Plugin Host Service. Starting and stopping a service requires administrative access to the SensorView server.

At upper left of the Services section each **Plugin** is listed along with its current **status**, either **Running** or **Stopped**.

Green Screen and BACnet Polling rate
Controls the rate at which these plugins are being polled. Increasing the rate may allow for Change of

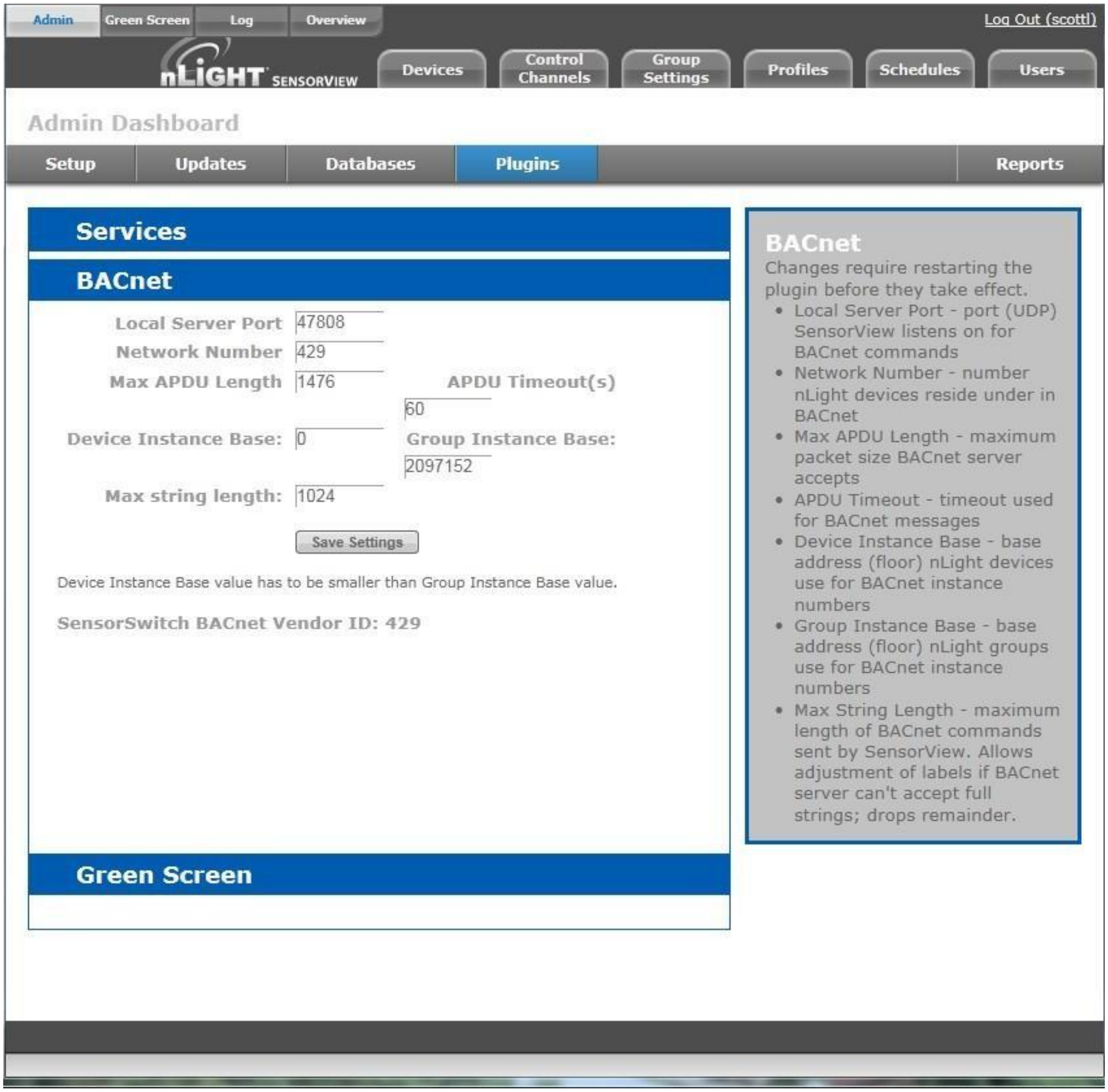
Value notifications (BACnet) and GreenScreen reporting points to increase, but will result in additional network traffic. To change the polling rate for these plugins, select a new rate, and click **Save & Restart Service**.

The nLight Plugin Host Services status (either **running** or **stopped**) is indicated in the table below.

Controlling the nLight Plugin Host Service requires system administrator credentials (not SensorView credentials). You may have to contact your local IT department to retrieve the proper set of credentials.

Administrators can enter their credentials (**Username**, **Password**, and **Domain**) for the SensorView host machine, and click **Stop** or **Start**.

BACnet Admin Screen



Admin Dashboard

Services

BACnet

Local Server Port: 47808
Network Number: 429
Max APDU Length: 1476
APDU Timeout(s): 60
Device Instance Base: 0
Group Instance Base: 2097152
Max string length: 1024

Device Instance Base value has to be smaller than Group Instance Base value.

SensorSwitch BACnet Vendor ID: 429

Green Screen

BACnet

Changes require restarting the plugin before they take effect.

- Local Server Port - port (UDP) SensorView listens on for BACnet commands
- Network Number - number nLight devices reside under in BACnet
- Max APDU Length - maximum packet size BACnet server accepts
- APDU Timeout - timeout used for BACnet messages
- Device Instance Base - base address (floor) nLight devices use for BACnet instance numbers
- Group Instance Base - base address (floor) nLight groups use for BACnet instance numbers
- Max String Length - maximum length of BACnet commands sent by SensorView. Allows adjustment of labels if BACnet server can't accept full strings; drops remainder.

BACnet administrative settings displayed are:

- **Local server port** – The port (UDP) on which SensorView receives BACnet commands
- **Network Number** – Number nLight devices reside under in BACnet. Default value is the nLight BACnet Vendor ID, 429.
- **Max APDU Length** – maximum packet size BACnet server accepts
- **ADPU timeout(s)** – timeout used for BACnet messages
  Defined by the ISO 7816 standards, the APDU (Application Protocol Data Unit) is the communication unit between a reader and a card.
- **Device Instance Base** – base address (floor) nLight **devices** use for BACnet instance numbers
- **Group Instance Base** – base address (floor) nLight **groups** use for BACnet instance numbers

- **Max String Length** – (default is 1024) maximum length of BACnet commands sent by SensorView. Allows adjustment of labels if BACnet server can't accept full strings; drops remainder.

To change these settings enter the desired value in the appropriate field(s) and click **Save Settings**. Device Instance Base must be smaller than Group Instance Basevalue.

The nLight Plugin Host Service must be restarted before the modified settings will take effect.

Reports

Linked directly to the current active SensorView database, authorized administrators can view detailed reports on the following:

Network Device Report: Creates a printable report containing basic information about the devices in the network and their basic properties, such as Label, Device ID, Firmware Version, Zone, and parent Bridge.

Profile & Scene Report: Creates a printable report describing the configuration of all profiles and scenes currently in the system.

Device Settings Report: Creates a printable report describing the default settings for all nLight devices in the system.

Global Channels / Preset Report: Creates a printable report listing all configured Global Channels along with the devices broadcasting and tracking within them. Also listed is all Global Preset configurations saved to any Global Preset capable device.

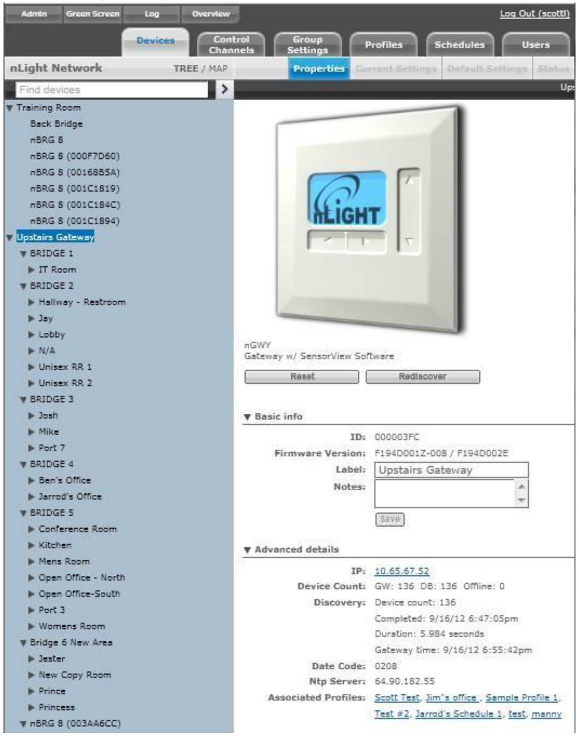
Discovery Report: Creates a printable report listing basic discovery statistics about all nGWY devices in the system. This is generally used for diagnostic purposes only.

BACnet Inventory Report: Creates a CSV report that lists all BACnet devices available in the system. It lists the Instance Numbers for all BACnet devices, as well as the instance values for all available properties. This is typically provided directly to the BACnet integrator.

Devices

On the SensorView Overview Device Properties page the user selects from the device tree. By default these devices are listed in hierarchical order: gateways are parents of bridges, which are parents of zones, each of which contain sensors, switches, relays, dimmers, or other devices.

Gateway Properties



▼ Training Room
Back Bridge
nBRG 8
nBRG 8 (000F7D60)
nBRG 8 (00168B5A)
nBRG 8 (001C1819)
nBRG 8 (001C184C)
nBRG 8 (001C1894)
▼ Upstairs Gateway
▼ BRIDGE 1
▶ IT Room
▼ BRIDGE 2
▶ Hallway - Restroom
▶ Jay
▶ Lobby
▶ N/A
▶ Unisex RR 1
▶ Unisex RR 2
▼ BRIDGE 3
▶ Josh
▶ Mike
▶ Port 7
▼ BRIDGE 4
▶ Ben's Office
▶ Jarrod's Office
▼ BRIDGE 5
▶ Conference Room
▶ Kitchen
▶ Mens Room
▶ Open Office - North
▶ Open Office-South
▶ Port 3
▶ Womens Room
▼ Bridge 6 New Area
▶ Jester
▶ New Copy Room
▶ Prince
▶ Princess
▼ nBRG 8 (003AA6CC)

nGWY
Gateway w/ SensorView Software

▼ Basic info

ID: 000003FC
Firmware Version: F194D001Z-008 / F194D002E
Label: Upstairs Gateway
Notes:

▼ Advanced details

IP: 10.65.67.52
Device Count: GW: 136 DB: 136 Offline: 0
Discovery: Device count: 136
Completed: 9/16/12 6:47:05pm
Duration: 5.984 seconds
Gateway time: 9/16/12 6:55:42pm
Date Code: 0208
Ntp Server: 64.90.182.55
Associated Profiles: Scott Test, Jim's office , Sample Profile 1, Test #2, Jarrod's Schedule 1, test, manny

Note that some items on Properties pertain only to certain types of devices and do not appear otherwise.

Basic Info:

- **ID:** An unique ID assigned to the device.
- **Firmware Version:** Indicates the firmware currently installed and running on the device. If this number does not match information in the Overview screen under "**Updates**", it may be time for a .
- **Label:** This custom label should be used to describe and represent the device.
- **Notes:** (optional) Comments on this device or the area it serves.
- **Load: (in Watts)** Shows and/or sets the load on the selected device or devices within the selected zone; used with Green Screen. Only applicable to devices containing relays or nIO LEDs.
- **Update Historical Load Data:** This indicates whether to change the load for data points previously collected for Green Screen (when checked) or leave old load values unaltered (unchecked). Only applicable to devices containing relays or nIO LEDS.

Advanced detail

- **IP:** The IP address of the selected gateway. nGWY only.
- **Device Count:** Shows the number of devices beneath this gateway in the network, including its bridges and all devices below them. DB shows the number of database records associated with the selected gateway, which should match the number of devices. Most SensorView users may ignore this data, which is primarily used for network and system diagnostics. Also indicated are the number of devices *offline*, if any. nGWY only.
- **Discovery:** Indicates the last time the selected Gateway was polled by SensorView. This occurs when an instruction to the device is sent by a SensorView user, or a firmware update. You can perform discovery any time by clicking **Rediscover**. nGWY only.
- **Date Code:** Indicates the internal lot number for the device.
- **NTP Server: Network Time Protocol (NTP)** is a protocol for synchronizing the clocks of computer systems over a network. This is used to keep times on gateways in sync, and the NTP server's IP address is listed here. nGWY2 only.
- **Parent Gateway:** The name of the Gateway directly above the selected bridge in the network hierarchy.
- **Network Depth:** The number of steps below a gateway in the network hierarchy.
- **Associated Profiles:** Profiles which include the selected device.
- **Zone:** The name of the Zone in which the selected device resides.
- **Parent Device:** The name of the device above the selected zone in the network hierarchy.
- **BACnet Instance (Number)** A device's instance number is used to uniquely identifynLight devices connected to BACnet.

The instance number is combined with other parameters in BACnet, such as Object Type or Object Name. Because BACnet services many facilities and many different companies, the instance number compensates for and eliminates any possibility of duplicate identifiers across the BACnet network. It is similar to the WHOIS function for domain names on the Internet. Requesting devices across the network can identify the device, its address information and its relative position in the network hierarchy. More information on BACnet Instance Numbers.

Output Controls

Provides convenient controls for viewing the current status of the device, as well as modifying the device's outputs (relays or dimmers as appropriate).

Health

This section provides diagnostics read-outs for nLight Engineers and Field Techs.

Control Channels

nLight Devices exchange control information via the use of Local and Global channels. Communication performed within a Zone (single nBRG port) is dictated via Local Channels; while Global Channels allow a device to receive input from any other device onthe nLight network.

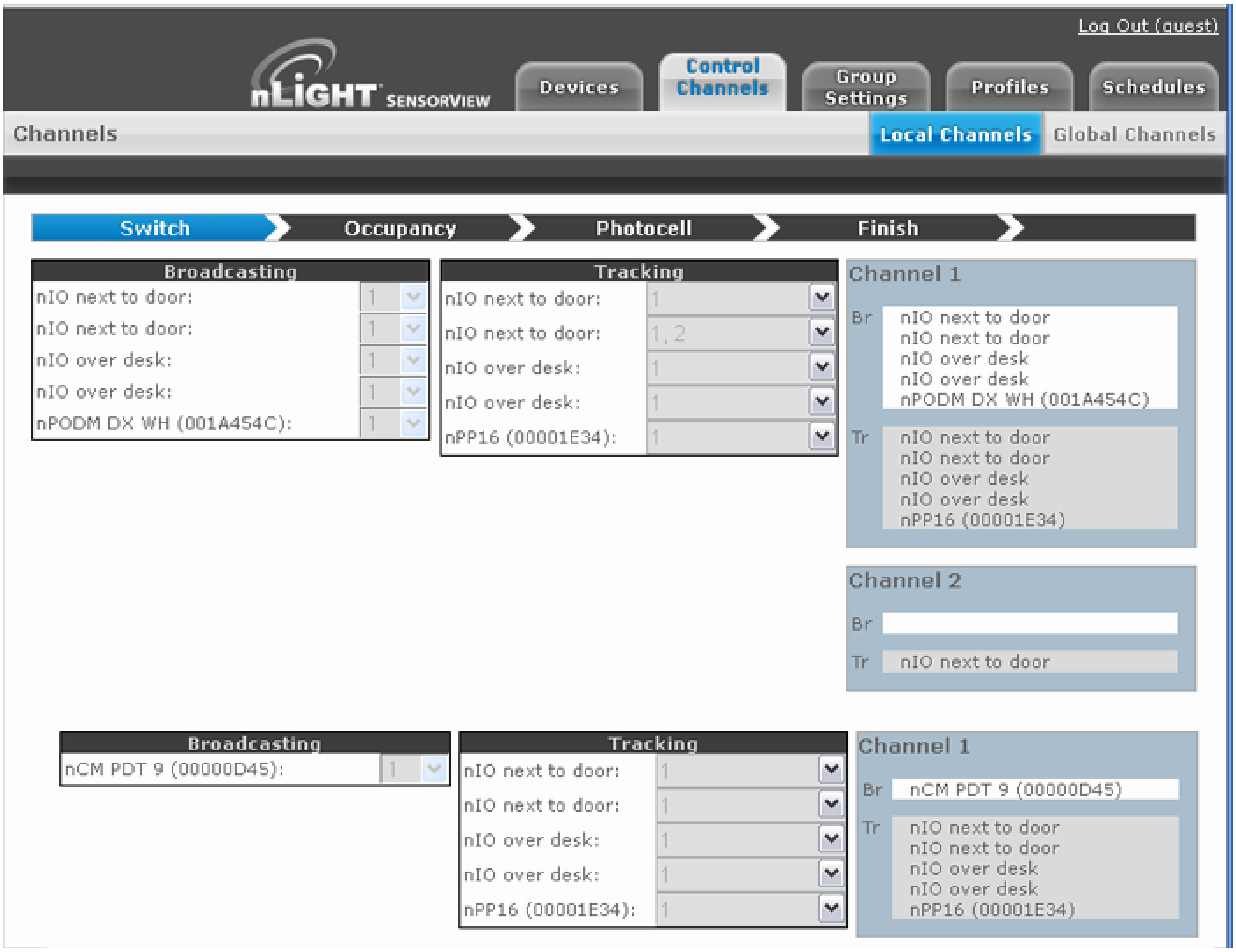
SensorView allows users to modify both Local and Global Channels to configure the control they need. Local Channels are commonly used to subdivide a single Zone and allow for switches to control individual fixtures or switch legs within a Zone, rather than all of them. Global Channels are more commonly used to provide instantaneous switch control over the entire building with a master switch.

Channels, both Global and Local, can be used to fine tune the control that one devices has over others, for Occupancy, Switching, and Daylighting.

Local Channels

SensorView’s **Local Channels** tab allows a user to specify the channeling for all devices in the selected zone. Users can configure **Switching**, **Occupancy**, and **Photocell** channels on a single screen.

Devices tracking a particular channel will respond to commands sent by any device broadcasting on that channel. To configure one device to control another simply set the broadcasting and tracking numbers for the devices to the same number. The column on the far right is a combined view, indicating all devices broadcasting and tracking on the same channel, as changes are made this column will update.



Broadcasting	
nIO next to door:	1
nIO next to door:	1
nIO over desk:	1
nIO over desk:	1
nPODM DX WH (001A454C):	1

Tracking	
nIO next to door:	1
nIO next to door:	1, 2
nIO over desk:	1
nIO over desk:	1
nPP16 (00001E34):	1

Channel 1

Br nIO next to door
nIO next to door
nIO over desk
nIO over desk
nPODM DX WH (001A454C)

Tr nIO next to door
nIO next to door
nIO over desk
nIO over desk
nPP16 (00001E34)

Channel 2

Br

Tr nIO next to door

Broadcasting	
nCM PDT 9 (00000D45):	1

Tracking	
nIO next to door:	1
nIO next to door:	1
nIO over desk:	1
nIO over desk:	1
nPP16 (00001E34):	1

Channel 1

Br nCM PDT 9 (00000D45)

Tr nIO next to door
nIO next to door
nIO over desk
nIO over desk
nPP16 (00001E34)

Start by selecting a zone from the tree. Then configure channels (eg. make this switch control only the lights at the back of the room) change the broadcasting channel of one or more devices to a new number, and add that number to the tracking channels of one or more devices the broadcaster(s) should affect. Add or remove tracking channels by expanding a drop-down and checking or unchecking the desired channels. Note that as changes to the channels are made the far right column will update to indicate which devices are tracking/broadcasting on each channel.

Global Channels

With traditional wired nLight systems, devices within a zone communicate occupancy, photocell and switch events over local channels.

With global channels, communication of this information is possible between zones as well. This provides enhanced design flexibility for applications requiring master control stations or centralized relays. Global channels are set through SensorView.

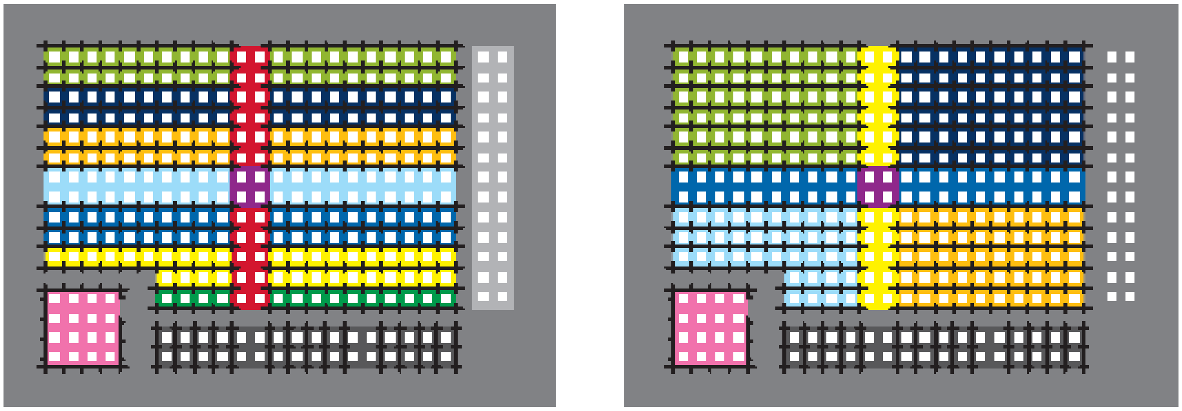
Select desired Switches from the Tree menu, and Select Switch on the Global Channels screen, and select the Global Channel on which the desired devices will operate. Click to add desired Switches (devices) to this

If no channel is yet defined, select New Channel. SensorView will display the next available Global Channel.

Devices can be added to more than one channel if desired. Click New Channel to see the next available Global Channel.

nWiFi Global Channel Functionality

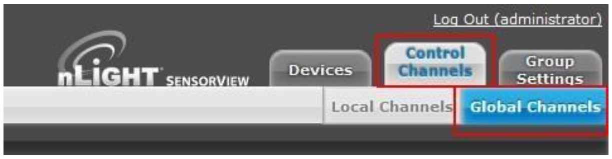
Out of the box nWiFi devices communicate with other devices directly connected to them, but when configured can use the WiFi network and global channels to link to other devices wirelessly and communicate switch, occupancy, and/or photocell events.



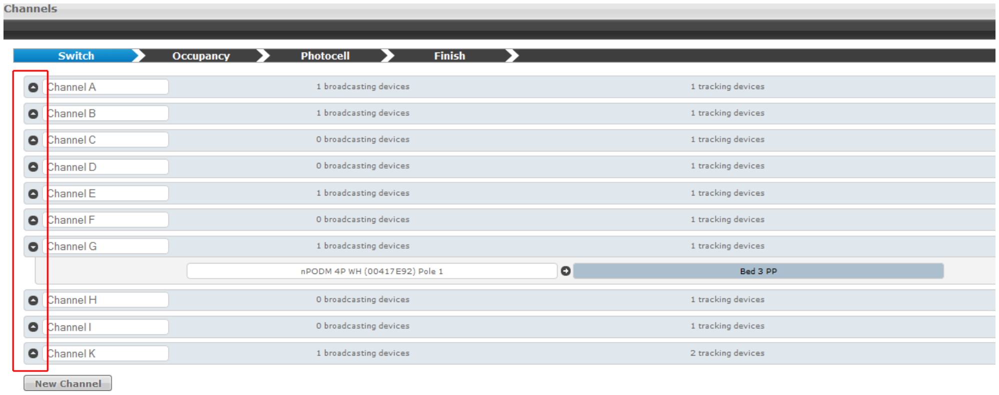
EXAMPLE: Warehouse with multiple global channel assignments per device

For example, a common global channel would be tracked by devices within each colored area above. On/Off & Dim Level control of each area is then possible via a standard WallPod. nWiFi devices can be set to track any/all of the 128 global channels – providing the flexibility to assign each device into multiple groups based on its location or type (i.e., All Rows, Columns, Alternating, Load Shed eligible, Custom, etc.). Simultaneous On/Off & Dim Level control of multiple global channel groups (referred to as "global preset") is possible via a Scene Selector WallPod.

nWiFi Global Commands

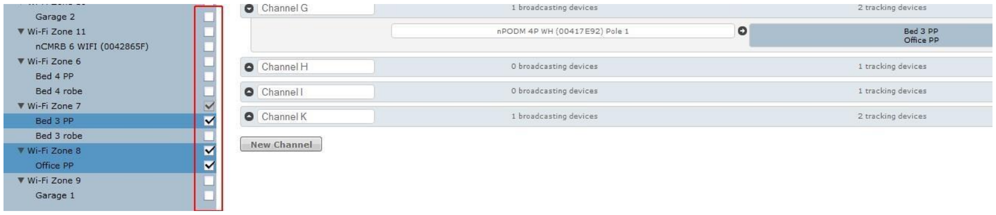


To create groups of devices that will switch on and off together, click on the Control Channels tab at the top right of the page followed by the Global Channels tab. The tree will expand and display all of the devices that can broadcast and track events over the nWIFI network.



Channel A	1 broadcasting devices	1 tracking devices
Channel B	1 broadcasting devices	1 tracking devices
Channel C	0 broadcasting devices	1 tracking devices
Channel D	0 broadcasting devices	1 tracking devices
Channel E	1 broadcasting devices	1 tracking devices
Channel F	0 broadcasting devices	1 tracking devices
Channel G	1 broadcasting devices	1 tracking devices
	nPODM 4P WH (00417E92) Pole 1	Bed 3 PP
Channel H	0 broadcasting devices	1 tracking devices
Channel I	0 broadcasting devices	1 tracking devices
Channel K	1 broadcasting devices	2 tracking devices

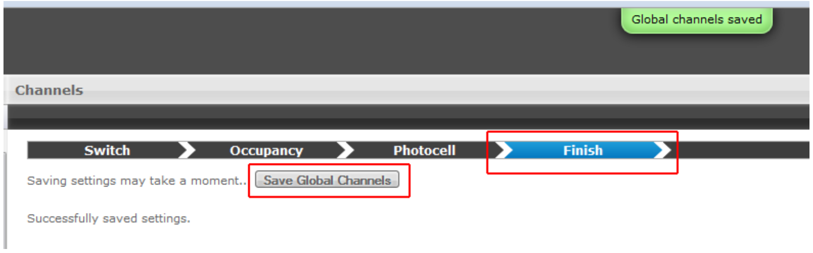
Any Global Channels that have been previously assigned will be displayed. A maximum of 128 Global Channels are available. To view or edit the devices that are part of a global channel expand the channel by clicking the arrow next to the channel name. Click the box under Broadcasting Devices or Tracking Devices to add or remove devices from that group using the device tree.



- Garage 2 □
- ▼ Wi-Fi Zone 11 □
  - nCMRB 6 WIFI (0042865F) □
- ▼ Wi-Fi Zone 6 □
  - Bed 4 PP □
  - Bed 4 robe □
- ▼ Wi-Fi Zone 7 ☑
  - Bed 3 PP ☑
  - Bed 3 robe □
- ▼ Wi-Fi Zone 8 ☑
  - Office PP ☑
- ▼ Wi-Fi Zone 9 □
  - Garage 1 □

Channel G	1 broadcasting devices	2 tracking devices
	nPODM 4P WH (00417E92) Pole 1	Bed 3 PP Office PP
Channel H	0 broadcasting devices	1 tracking devices
Channel I	0 broadcasting devices	1 tracking devices
Channel K	1 broadcasting devices	2 tracking devices

After setting up the desired channels, click Finish followed by **Save Global Channels**.

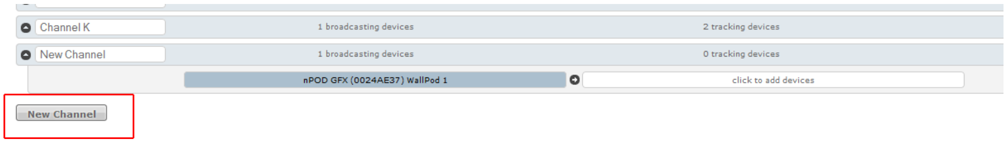

Global channels saved

Channels

Saving settings may take a moment.. Save Global Channels

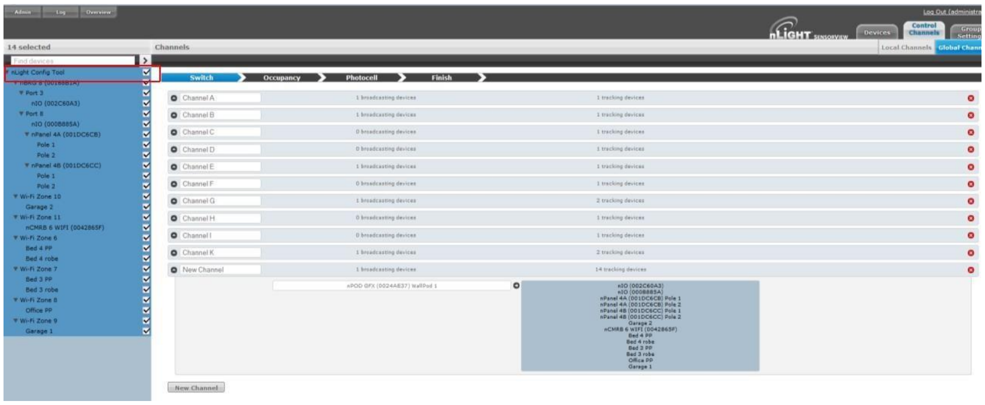
Successfully saved settings.

To create a new Global Channel click the New Channel button, change the default label if desired, and select Broadcasting or Tracking to begin adding devices from the tree.


Channel K	1 broadcasting devices	2 tracking devices
New Channel	1 broadcasting devices	0 tracking devices
	nPOD GFX (0024AE37) WallPod 1	click to add devices

New Channel

To select (or deselect) multiple devices at once in the tree click the box next to a top-level device, such as a gateway or nLight Config Tool, to affect everything below it.



14 selected

Find devices

nLight Config Tool
nBRG 8 (0018881A)
Port 3
nIO (002C60A3)
Port 8
nIO (0008885A)
nPanel 4A (001DC6CB)
Pole 1
Pole 2
nPanel 4B (001DC6CC)
Pole 1
Pole 2
Wi-Fi Zone 10
Garage 2
Wi-Fi Zone 11
nCMRB 6 WIFI (0042865F)
Wi-Fi Zone 6
Bed 4 PP
Bed 4 robe
Wi-Fi Zone 7
Bed 3 PP
Bed 3 robe
Wi-Fi Zone 8
Office PP
Wi-Fi Zone 9
Garage 1

Channels

Channel A	1 broadcasting devices	1 tracking devices
Channel B	1 broadcasting devices	1 tracking devices
Channel C	0 broadcasting devices	1 tracking devices
Channel D	0 broadcasting devices	1 tracking devices
Channel E	1 broadcasting devices	1 tracking devices
Channel F	0 broadcasting devices	1 tracking devices
Channel G	1 broadcasting devices	2 tracking devices
Channel H	0 broadcasting devices	1 tracking devices
Channel I	0 broadcasting devices	1 tracking devices
Channel K	1 broadcasting devices	2 tracking devices
New Channel	1 broadcasting devices	14 tracking devices
	nPOD GFX (0024AE37) WallPod 1	nIO (002C60A3) nIO (0008885A) nPanel 4A (001DC6CB) Pole 1 nPanel 4A (001DC6CB) Pole 2 nPanel 4B (001DC6CC) Pole 1 nPanel 4B (001DC6CC) Pole 2 Garage 2 nCMRB 6 WIFI (0042865F) Bed 4 PP Bed 4 robe Bed 3 PP Bed 3 robe Office PP Garage 1

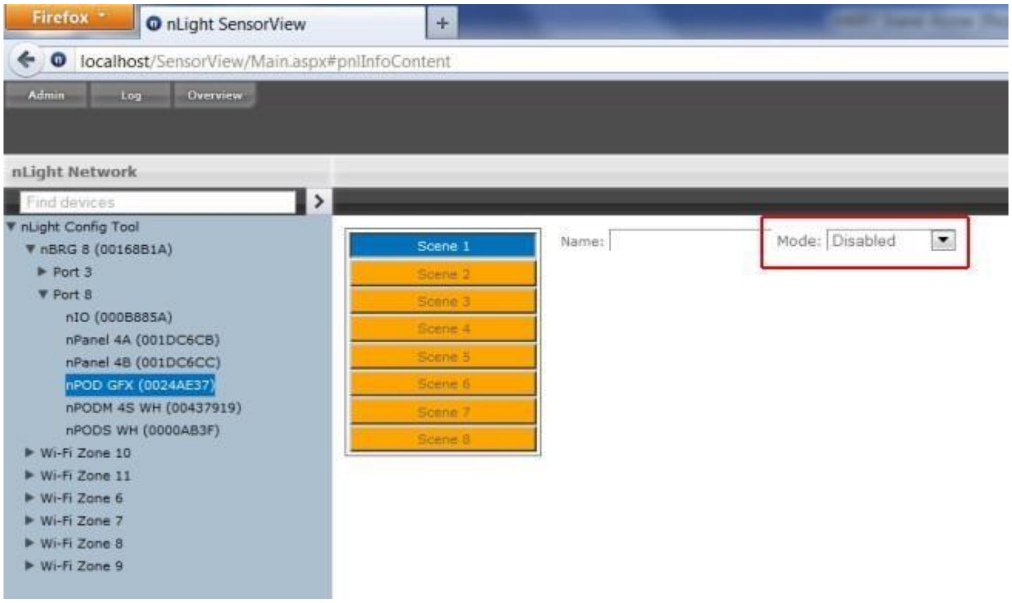
New Channel

Tip: Channels used in a global preset shouldn't contain the same devices to prevent On/Off conflicts. e.g., a preset where 50% of all lights go on and the other half go off, two global channels are required (one for the On command & the other for Off).

Global Preset: a combination of global channels commands (on/off/dim level) activated simultaneously by a device. Each global preset can feature different commands on different channels. A global preset can contain between 1 and 80 Global Channels.

For example: a Scene Selector can simultaneously send an On command to all devices tracking global channel A and an Off command to all devices tracking global channel B.

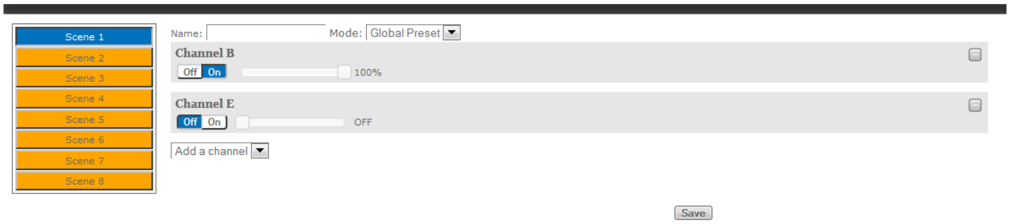
To set a Global Preset on a Graphic WallPod (nPOD GFX), find the device in the tree on the Devices page and click the Scenes tab.



Name:

Mode: Disabled

Change the mode to Global Preset Mode: Global Preset and select the desired global channels. Once they have been selected set them to On, Off, or a Dim Level (if dimming hardware is installed) and click Save.

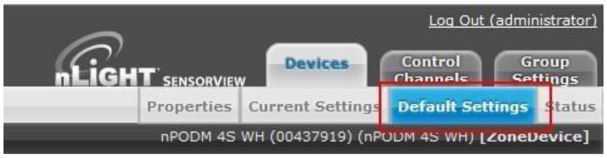


Name:

Mode: Global Preset

Channel B: Off [✓ On] 100%

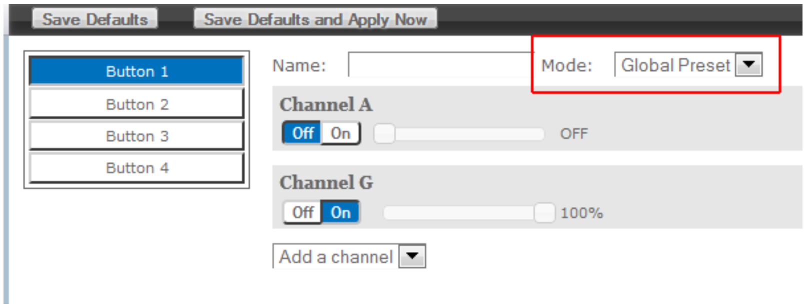
Channel E: [✓ Off] On OFF



nPODM 4S WH (00437919) (nPODM 4S WH) [ZoneDevice]

To set a Global Preset for an nPOD(M) device, find device in the tree on the Devices page and select the Default Settings tab near the top right of the page.

Change the mode to Global Preset and select the desired global channels. Once selected set them to On, Off, or a Dim Level (if dimming hardware installed) and click Save.



Name:

Mode: Global Preset

Channel A

Off On OFF

Channel G

Off On 100%

Global Presets are resent every time the button on the device is pushed; if any fixture(s) does not respond to the Global Preset, resend by pressing the button again.

Group Settings

Here default settings can be modified for many devices at once. Start by selecting devices from the tree, which will show a drop-down to add a setting. The list of settings available depends on the devices selected.

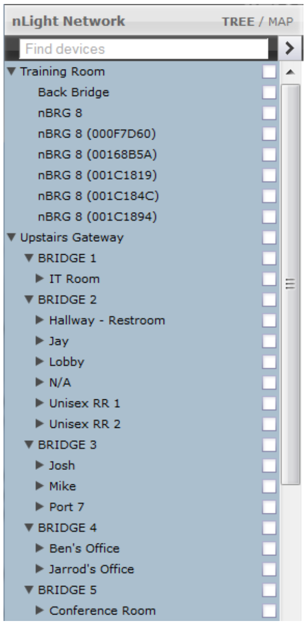
Add one or more settings, then select the desired value(s). When finished, click Save Defaults.

Selecting Multiple Devices from the Tree

MultiSelect is a selection mode offered by SensorView's tree. When operating in this mode, all line items displayed in the tree will be given a checkbox which will allow for selection. Single clicking on a device no longer displays information specific to the device, but rather selects/deselects it.

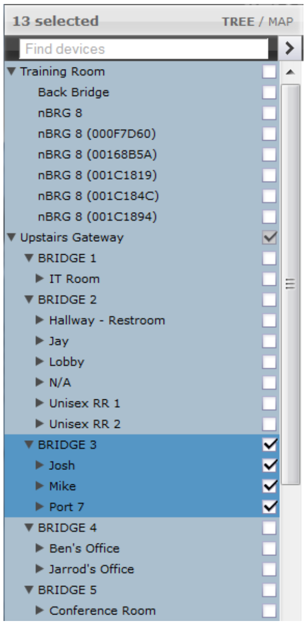
This mode of selection is used when large amounts of devices are to be operated on simultaneously.

None Selected
(empty Checkboxes)



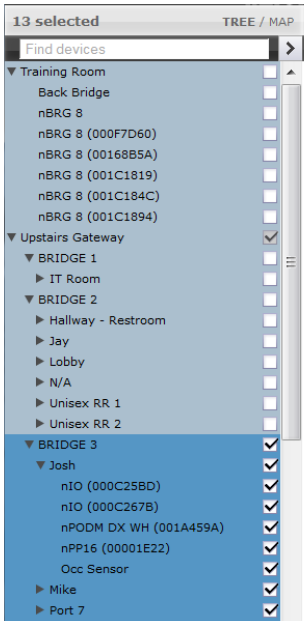
```
nLight Network                    TREE / MAP
Find devices                               >
▼ Training Room                            ☐
    Back Bridge                            ☐
    nBRG 8                                 ☐
    nBRG 8 (000F7D60)                      ☐
    nBRG 8 (00168B5A)                      ☐
    nBRG 8 (001C1819)                      ☐
    nBRG 8 (001C184C)                      ☐
    nBRG 8 (001C1894)                      ☐
▼ Upstairs Gateway                         ☐
  ▼ BRIDGE 1                               ☐
    ▶ IT Room                              ☐
  ▼ BRIDGE 2                               ☐
    ▶ Hallway - Restroom                   ☐
    ▶ Jay                                  ☐
    ▶ Lobby                                ☐
    ▶ N/A                                  ☐
    ▶ Unisex RR 1                          ☐
    ▶ Unisex RR 2                          ☐
  ▼ BRIDGE 3                               ☐
    ▶ Josh                                 ☐
    ▶ Mike                                 ☐
    ▶ Port 7                               ☐
  ▼ BRIDGE 4                               ☐
    ▶ Ben's Office                         ☐
    ▶ Jarrod's Office                      ☐
  ▼ BRIDGE 5                               ☐
    ▶ Conference Room                      ☐
```

Bridge Selected
(Parent gateway checked in gray)



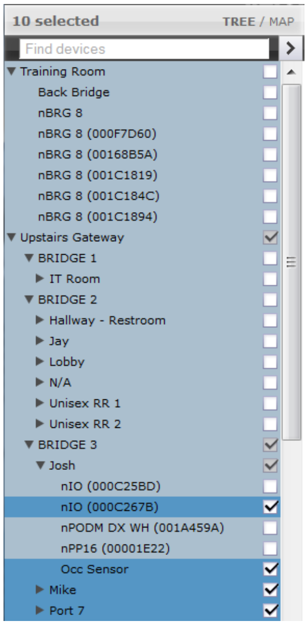
```
13 selected                       TREE / MAP
Find devices                               >
▼ Training Room                            ☐
    Back Bridge                            ☐
    nBRG 8                                 ☐
    nBRG 8 (000F7D60)                      ☐
    nBRG 8 (00168B5A)                      ☐
    nBRG 8 (001C1819)                      ☐
    nBRG 8 (001C184C)                      ☐
    nBRG 8 (001C1894)                      ☐
▼ Upstairs Gateway                         ☑
  ▼ BRIDGE 1                               ☐
    ▶ IT Room                              ☐
  ▼ BRIDGE 2                               ☐
    ▶ Hallway - Restroom                   ☐
    ▶ Jay                                  ☐
    ▶ Lobby                                ☐
    ▶ N/A                                  ☐
    ▶ Unisex RR 1                          ☐
    ▶ Unisex RR 2                          ☐
  ▼ BRIDGE 3                               ☑
    ▶ Josh                                 ☑
    ▶ Mike                                 ☑
    ▶ Port 7                               ☑
  ▼ BRIDGE 4                               ☐
    ▶ Ben's Office                         ☐
    ▶ Jarrod's Office                      ☐
  ▼ BRIDGE 5                               ☐
    ▶ Conference Room                      ☐
```

Zone expanded.
All zone devices checked



```
13 selected                       TREE / MAP
Find devices                               >
▼ Training Room                            ☐
    Back Bridge                            ☐
    nBRG 8                                 ☐
    nBRG 8 (000F7D60)                      ☐
    nBRG 8 (00168B5A)                      ☐
    nBRG 8 (001C1819)                      ☐
    nBRG 8 (001C184C)                      ☐
    nBRG 8 (001C1894)                      ☐
▼ Upstairs Gateway                         ☑
  ▼ BRIDGE 1                               ☐
    ▶ IT Room                              ☐
  ▼ BRIDGE 2                               ☐
    ▶ Hallway - Restroom                   ☐
    ▶ Jay                                  ☐
    ▶ Lobby                                ☐
    ▶ N/A                                  ☐
    ▶ Unisex RR 1                          ☐
    ▶ Unisex RR 2                          ☐
  ▼ BRIDGE 3                               ☑
    ▼ Josh                                 ☑
        nIO (000C25BD)                     ☑
        nIO (000C267B)                     ☑
        nPODM DX WH (001A459A)             ☑
        nPP16 (00001E22)                   ☑
        Occ Sensor                         ☑
    ▶ Mike                                 ☑
    ▶ Port 7                               ☑
```

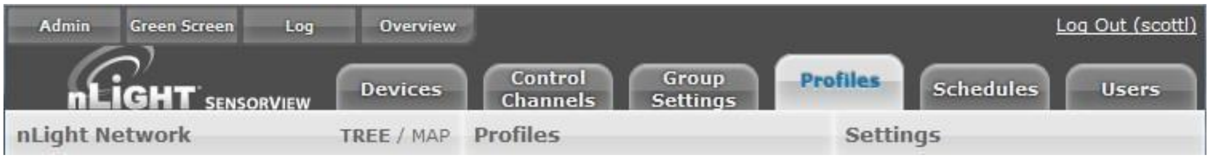
Specific zone devices
unchecked



```
10 selected                       TREE / MAP
Find devices                               >
▼ Training Room                            ☐
    Back Bridge                            ☐
    nBRG 8                                 ☐
    nBRG 8 (000F7D60)                      ☐
    nBRG 8 (00168B5A)                      ☐
    nBRG 8 (001C1819)                      ☐
    nBRG 8 (001C184C)                      ☐
    nBRG 8 (001C1894)                      ☐
▼ Upstairs Gateway                         ☑
  ▼ BRIDGE 1                               ☐
    ▶ IT Room                              ☐
  ▼ BRIDGE 2                               ☐
    ▶ Hallway - Restroom                   ☐
    ▶ Jay                                  ☐
    ▶ Lobby                                ☐
    ▶ N/A                                  ☐
    ▶ Unisex RR 1                          ☐
    ▶ Unisex RR 2                          ☐
  ▼ BRIDGE 3                               ☑
    ▼ Josh                                 ☑
        nIO (000C25BD)                     ☐
        nIO (000C267B)                     ☑
        nPODM DX WH (001A459A)             ☐
        nPP16 (00001E22)                   ☐
        Occ Sensor                         ☑
    ▶ Mike                                 ☑
    ▶ Port 7                               ☑
```

Selecting a zone device (a device that exists in a zone) only selects/deselects that device. Selecting a zone, bridge, or gateway selects/deselects children; this allows for a user to quickly select all devices in a zone, bridge, or gateway.

Profiles



The **Profiles** tab is where control modes and settings for a particular group are selected. A schedule (complete with a recurrence pattern) and priority are also chosen on this page.

Profiles are stored in the database and the Gateway, which administers profiles according to priorities. The profiles can also be activatedon demand via SensorView or the Gateway.

Click New to start creating a new profile, or the name of a profile in the list to edit an existing profile.

Add or remove devices using the checkboxes in the tree on the left. Checked devices can participate in the profile and receive applicable settings while the profileruns.

Scheduler

- Schedule date/hour/minute for any setting change or control mode
- Astronomical start/end dates include +/-180 minute deviance from Sunrise/Sunset
- Set daily/weekly/monthly/yearly recurrences; drilldown options provide more detailed patterns

Priority:

- Select the priority of the profile to change, then use the arrows to move to the appropriate position, or down into the disabled area

Unlike other systems which allow scheduling of lights on/off or on-demand dimming scene control, nLight provides users with the ability to schedule changes to almost any operational parameter. This allows for dynamic sequences of operation that can be tailored to a space across different times of day and/or dates.

Schedules

The **Schedules** tab shows all scheduled profiles for zones and devices in the nLight network, on a 24-hour schedule for a given date.

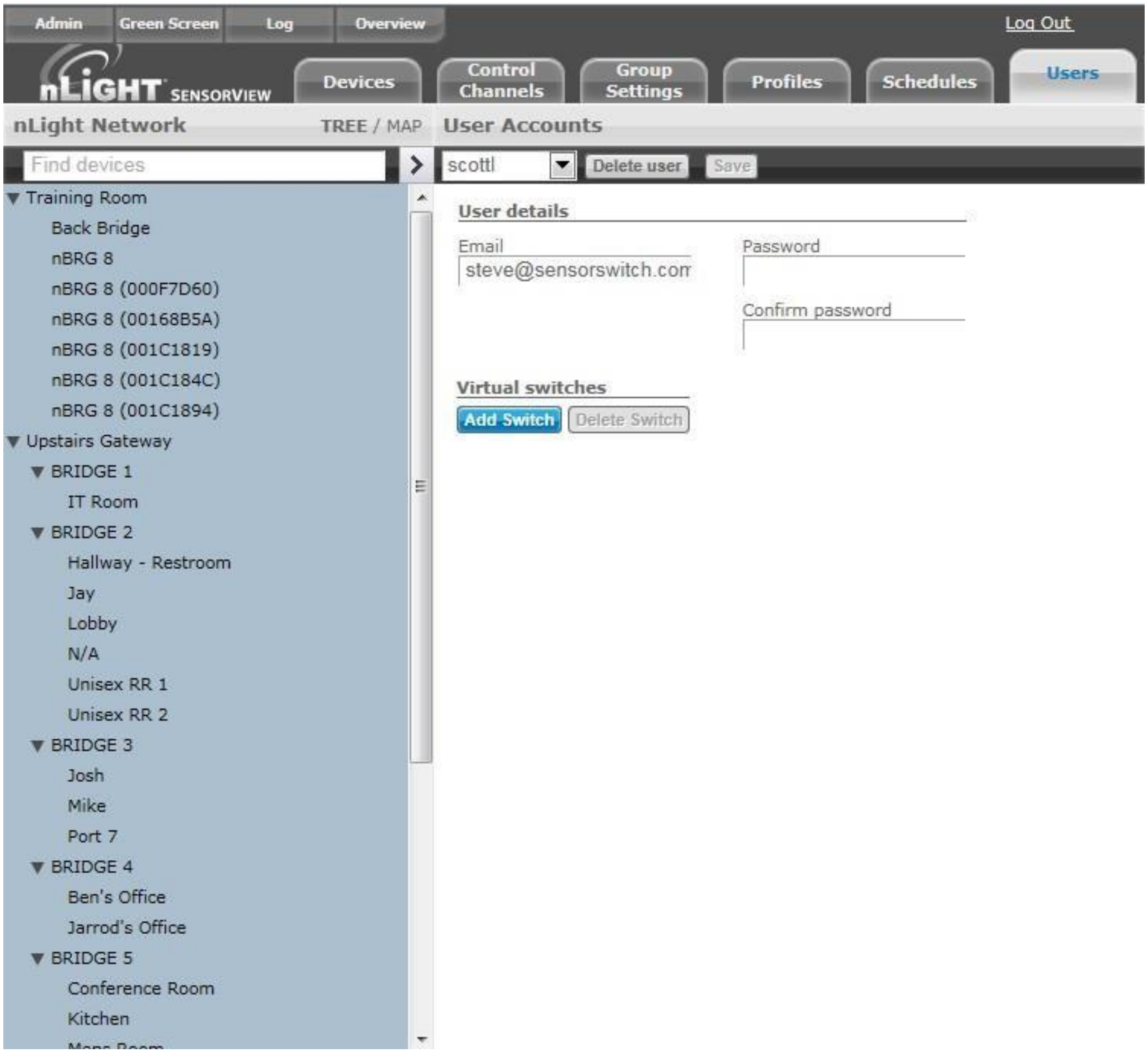
Hovering over a profile name displays the profile's begin and end times. Clicking the profile name is a shortcut to editing that profile on the Profiles tab.

When a zone is expanded, individual schedule bars for the zone's devices are generated. These bars are colored to denote a specific profile.

Clicking the header with the time markings will bring up a date picker for quick viewing of a future date.

Users

The Users tab manages users and their permissions to nLight devices and Virtual WallPods.



User Accounts

scottl

User details

Email: steve@sensorswitch.com

Password

Confirm password

Virtual switches

At the top, under User Accounts, is a drop-down that lists users. Select a user to display and edit the user's details.

You may assign one or more **Virtual Switches** to a user by clicking **Add Switch**. The newly added switch can be labeled using the text field. Select either **Zone Channel** or an **Individual device** from the Control Type drop-down.

For zone channel switches **Select Zone** from the drop-down. Individual devices associated with that zone will be displayed beneath. For individual device **Select device to control**, and it will be added to your list.

When finished click **Save**.

Adding, Modifying, and Deleting Users

To add a user select **Add a user** from the drop-down. Or select a username to edit that user. Clicking **Delete user** will delete the user selected in the drop-down.

Users you control, other than yourself, can be one of several user types, which dictates their level of capabilities within SensorView.

- **Read-only** users are only allowed to view status and current settings from the devices they are given permission to; they are not allowed to affect any sort of change to the system.
- **Basic** users are allowed to read and configure the devices within their permissions, including managing profiles for (just) those devices.
- **Administrators** have access to the Admin page. In addition to Basic User tasks for their permission set, Administrators are also allowed to run updates and manage SensorView (location, gateway passwords, mail servers, and users).

SensorView Terms

- **100 Hour Burn-In**: Overrides relay on and/or dimming output to full bright(typically used for lamp seasoning)
- **Auto Set-Point**: Photocell calibration procedure for detecting optimum lightingcontrol level
- **Auto to Override On**: Special Mode where lights are turned on initially by occupant detection but then left in the Override On state
- **BACnet Instance (Number)** A device's instance number is used to uniquelyidentify nLight devices connected to BACnet.

  The instance number is combined with other parameters in BACnet, such as Object Type or Object Name. Because BACnet services many facilities and many different companies, the instance number compensates for and eliminates any possibility of duplicate identifiers across the BACnet network. It is similar to the WHOIS function for domain names on the Internet. Requesting devices across the network can identify the device, its address information and its relative position in the network hierarchy. More information on BACnet Instance Numbers.

- **BMS (Building Management System)**
  A Building Management System (BMS) is a network which monitors and/or controls devices in a building, campus, or in multiple facilities.

  When used for **monitoring**, the BMS polls and displays information from various types of equipment. BMS may monitor alarm conditions for equipment dependent up humidity or temperature. SensorView polls nLight devices, for example, and collect sensor information on occupancy, light levels, microphonic activity, among others.

  When used as a control system, the BMS has the ability to change settings on networked devices. This can be done manually by facilities/BMS managers, or by pre-programmed conditions, where settings of devices are modified in response to readings collected by other networked devices. Slave devices pass data from sensors to the master, which processes collected data and issues instructions for any necessary settings changes. Instructions can also be issued to devices based on Profiles which may be scheduled to start at a certain time of day, or triggered by readings and thresholdsof other devices. nLight products integrate with BMSs using Internet protocols and open standards such as BACnet.

- **Broadcast Analog Input**: Input mode that senses a 0-10 VDC input
- **Button Mode**: Overrides a device and enables its push-button to toggle the device's internal relay(s) or dim level
- **Dimming Offset**: Fixed voltage difference of dimming output from dimming photocell

- **Dimming Rate**: The speed at which automatic changes to the light level occur
- **Dual Technology (Microphonics)**: A second method of occupancy detection that allows the sensor to hear occupants
- **Dual Zone Fan Mode**: Dual Zone photocell mode where Zone 2’s photocell controlis disabled
- **Dual Zone Off-Point:** Zone 2’s set-point as a percentage of Zones 1’s set-point (Dual Zone photocell applications only)
- **Dual Zone Offset**: Fixed voltage increase of Zone 2’s dimming output from Zone 1’s dimming output (Dual Zone photocell applications only)
- **Dual Zone Offset Mode**: Dual Zone photocell mode where Zone 2’s set-point isa selected percentage higher than Zones 1’s set-point
- **DZ Photocell Mode**: Indicates a Dual Zone photocell sensor’s method of operation
- **Enabled – Both Positive and Negative**: User can increase or decrease lighting level set by dimming photocell
- **Enabled – Negative Only**: User can decrease lighting level set by dimming photocell
- **Follow Photocell Mode**: Instructs how a device’s dimming output reacts relative to a dimming photocell
- **Idle Time Until Dim**: The length of time after last detected occupancy that a sensorwill reduce lighting to unoccupied dim level.
- **Incremental Set-Point Adjust**: Alters the target light level that is to be maintained by the device (in footcandles)
- **Invert Relay Logic**: Reverses functionality of relays
- **LED**: Indicates the behavior of a device’s LED
- **Local Only Occupancy Tracking**: Instructs a device with a relay and/or dimming output to react to only its internal occupancy information
- **Local Only Photocell Tracking**: Instructs a device with a relay and/or dimming output to react to only its internal photocell information
- **Local Only Switching Tracking**: Instructs a device with a relay and/or dimming output to react to only its own manual switching and/or dimming events
- **Manual On to Full Auto**: Special Mode that initially requires the occupant tomanually turn on the lights, after which the sensor assumes full on/off control
- **Manual to Override On**: Special Mode that requires the occupant to manually turn on the lights and then leaves them in the Override On state
- **Microphone Grace Period**: The time period after lights are automatically turned off that they can be reactivated by sound
- **Momentary**: Input mode that senses a pulse style switch
- **Night Light Brightness**: The percent of full brightness the push-buttons LED illuminates
- **Network Time Protocol (NTP)** is a protocol for synchronizing the clocks of computer systems over a network. nLight gateways are synchronized with an NTP Server.
- **Occupancy Broadcast Channel**: The channel on which a sensor transmits its occupancy information
- **Occupancy Broadcasting**: Indicates whether a sensor will transmit its occupancy information to the rest of its zone

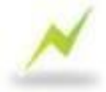
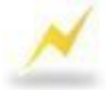
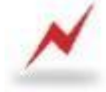
- **Occupancy Tracking**: Indicates whether a device's relay and/or dimming output will react to occupancy information
- **Occupancy Tracking Channel**: The channel on which a relay and/or dimming output receives occupancy information
- **Occupied Bright Level**: The output level (0-10 VDC) that a dimming sensor sets the lights when occupancy is detected (not applicable if photocell is enabled).
- **Override**: Indicates whether a device's relay is forced on/off and/or dimming output is forced to maximum/minimum
- **Photocell Broadcast Channel**: The channel on which a sensor transmits its photocell information
- **Photocell Broadcasting**: Indicates whether a sensor will transmit its photocell information to the rest of its zone
- **Photocell Dimming Range (High)**: The maximum output level (0-10 VDC) up to which an automatic dimming photocell will control
- **Photocell Dimming Range (Low)**: The minimum output level (0-10 VDC) down to which an automatic dimming photocell will control
- **Photocell Mode**: Indicates a photocell sensor's method of operation. One mode enables the sensor to turn the lights both on and off while the other mode can only inhibit (prevent) the lights from turning on
- **Photocell Tracking**: Indicates whether a device's relay and/or dimming output will react to photocell information
- **Photocell Tracking Channel**: The channel on which a relay and/or dimming output receives photocell information
- **Photocell Transition Off Time**: The time period for which a photocell must measure a light level above the set-point before it will turn the lights off
- **Photocell Transition On Time**: The time period for which a photocell must measure a light level below the set-point before it will initiate the lights on
- **Predictive Exit Time**: The time period after manually switching lights off for the occupant to leave the space (Predictive Off mode only)
- **Predictive Grace Period**: The time period after the Predictive Exit Time that the sensor rescans the room for remaining occupants (Predictive Off mode only)
- **Predictive Off**: When lights are switched off, this Special Mode determines whether occupants remain or left the room, so as to leave the lights in either the Override Off or Auto On state.
- **Profile Mode**: Mode that commands a Gateway to run any number of specified profiles
- **Profile Override**: Whether profiles selected via a Scene Controller button will cancel out or run concurrently with other profiles.
- **Reduced Turn-On**: Reduces the initial PIR detection strength; for use in areas where reflections are in sensor's view
- **Scene Expiration Time**: The length of time a selected scene or profile will run before automatically disengaging and reverting affected devices back to defaults

- **Scene Mode**: Mode that causes button to initiate pre-programmed settings on devices within a local zone
- ❖ **Scene Mode – Momentary**: Mode where pre-programmed settings are run on devices within a local zone when a pulse style switch is sensed from the connected device
- ❖ **Scene Mode – Toggle**: Mode where pre-programmed settings are run on devices within a local zone when an open/close style switch is sensed from the connected device
- **Semi-Auto**: Special Mode that requires the occupant to manually turn the lights on, while having them turn off automatically by a sensor
- **Semi-Auto Grace Period**: The time period after lights are automatically turned off that they can be reactivated with movement
- **Set-Point**: The target light level that is to be maintained by the device (in foot-candles)
- **Special Modes**: Unique defined behaviors for relays and/or dimming outputs
- **Start-to-High**: Lights go to full bright for 20 minutes upon initial power up
- **Stepped Dimming (DUO) Mode**: Dual Zone photocell mode where the appropriate on/off combination of the two associated relays is maintained in order to always meet the photocell set-point requirements
- ❖ **Stepped Dimming (DUO) – Never Off**: Dual Zone photocell mode where the appropriate on/off combination of the two associated relays (except both off) is maintained in order to always meet the photocell set-point requirements
- **Sunlight Discount Factor**: Value used to improve the tracking accuracy of a photocell during periods of high daylight; decreasing the value will lower the controlled level of the lights
- **Sweep Exit Time**: The time period before a sweep is executed, setting time delays on affected devices to zero
- **Sweep Grace Period**: The time delay before a sweep is executed, so a user pressing a switch to activate the sweep may exit the room or building before the sweep occurs
- **Sweep Mode**: Mode that causes a Scene Controller button to set the remainingtime delay for all devices on a gateway
- ❖ **Sweep Mode – Momentary**: Mode that sets the remaining time delay for all devices on a gateway when a pulse style switch is sensed from the connected device
- ❖ **Sweep Mode – Toggle**: Mode that sets the remaining time delay for all devices ona gateway when an open/close style switch is sensed from the connected device.
- ❖ **Switch Broadcast Channel**: The channel on which a device with a manual switch and/or dimmer transmits
- **Switch Broadcasting**: Indicates whether a device with a manual switch and/or dimmer will transmit events to the rest of its zone
- ❖ **Switch Tracking**: Indicates whether a device's relay and/or dimming output will reactto manual switching or dimming events
- **Switch Tracking Channel**: The channel on which a relay and/or dimming output receives manual switching or dimming events

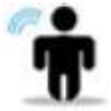
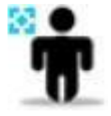
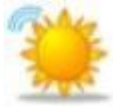
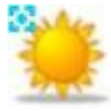
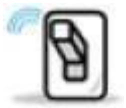
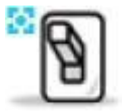
- **Timed Override Delay**: The length of time an Override On state that is initiated by a Special Mode will remain in effect
- **Toggle Mode**: Input mode of a nIO that senses an open/close style switch
- **Unoccupied Dim Level:** The output level (0-10 VDC) a dimming sensor sets the lights after the idle time until dim timer expires
- **WallPod Dimming Adjustments:** Indicates whether user adjustments to dimming levels are stored to device defaults (Permanent) or not (Temporary)
- **Wallpod Mode – Momentary**: Mode that creates an equivalent WallPod signal when a pulse style switch is sensed from the connected device.
- **Wallpod Mode – Toggle**: Mode that creates an equivalent WallPod signal when an open/close style switch is sensed from the connected device
- **WallPod Mode:** Mode that causes a Scene Controller button to function like a WallPod

Status Icons

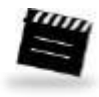
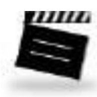
Voltage Status

Icon	Value	Description
	**Bridge / Transceiver PowerState** Power Supply Voltage: (VDC)	Device has adequate power (bridge)
	**Bridge / Transceiver PowerState** Power Supply Voltage: (VDC)	Device is close to low power condition (bridge)
	**Bridge / Transceiver Power State** Power Supply Voltage: (VDC)	Device is in low power condition (bridge)

Broadcasting & Tracking Status

Icon	Value	Description
	**Occupancy Broadcasting**	Occupancy status broadcast is active
	**Occupancy Tracking**	Occupancy status tracking is active
	**Photocell Broadcasting**	Photocell status broadcast is active
	**Photocell Tracking**	Photocell status tracking is active
	**Switch Broadcasting**	Switch status broadcast is active
	**Switch Tracking**	Switch status tracking is active

Scenes & Profiles Status

Icon	Value	Description
	**Scene States (per button/nIO)** Scene State: Active	Scene associated with button is active
	**Scene States (per button/nIO)** Scene State: Idle	Scene associated with button is not active

	Scene States (per button/nIO) Scene State: Disabled	Button is disabled
	Scene Expiration Time	Indicates when current running scene/profile will expire
	Photocell Not Inhibiting	Indicates that photocell is not preventing lights from being on
	Photocell Status (per pole) Transition time: (hh:mm:ss)	Indicates when current photocell state will change
°F °C	**Temperature**	Current temperature at the processor of the device
20	**LightLevel** Measured light level: (fc)	Current foot candle level as measured by the photocell
	Profile Active	Profile is currently active
	Profile Inactive	Profile is NOT currently active

Photocell Status

Icon	Value	Description
	Photocell Inhibiting	Indicates that photocell is preventing the lights from being on
	Photocell Not Inhibiting	Indicates that photocell is not preventing lights from being on
	Photocell Status (per pole) Transition time: (hh:mm:ss)	Indicates when current photocell state will change
20	**LightLevel** Measured light level: (fc)	Current foot candle level as measured by the photocell

PIR & PDT Status

Icon	Value	Description

🕒	**Time Delay Remaining:** (hh:mm:ss)	Indicates when current occupancy state will expire
🕒	**Tracked Occupancy Timer**	Reason why pole is open or closed
✳	**PIR Activity**	PIR Activity detected/detecting occupant motion
🚫	**PIR Activity**	No PIR Activity. PIR not currently detecting occupant motion
🔊	**Microphonic Activity**	Microphone has detected a triggering noise
🔇	**Microphonic Activity**	Microphone is not currently detecting noises

Occupancy, Relay & Dimming Status

Icon	Value	Description
🧍	**Occupied**	Room is occupied
🧍	**Vacant**	Room is not occupied
⁘	**Dimming Output (input) level: (%)**	Current % of 0-10 VDC scales
⁘	**Input Dim Level**	Follow Photocell Level: 4.9% or Input Dim Level: 100%
🧍	**Pole State Reason**	Reason why pole is open or closed
🕒	**Accumulated Hours**	Accumulated Hours: 1272
100% 80%	**Compensated Output Level**	Compensated Output Level: 0

💡		Pole State reason: Manual Switch Override Off
💡⚙		
●–●	**Relay State (per pole)**	Closed
●⁄○	**Relay State (per pole)**	Open

Wireless Status

Icon	Value	Description
📶	**Wireless Signal Strength: (1- 5)**	Indicates wireless signal strength (higher is better)
7271982	**Wireless PAN ID**	Wireless panel identification number
01100110 00110110 10011001 11101010 01100110	**Wireless Node ID**	Wireless node identification number
📡	**Wireless Channel: (11-26)**	Indicates the wireless channel currently being used
📻	**Wireless State:**	Wireless States: • Normal • Validating the network • Searching for a network that is allowing joining • Creating a new network • Allowing joining • Cloning is happening in the system • Multiple SSI networks are allowing joining • Lost a remote device during OTA cloning • Wireless device is not responding
PORT 8	**Bridge Port Information**	Port States: • Polling downstream devices • Upstream port • Commissioning tool connected • Polling downstream bridges
PORT 7		

PORT 6		• Error: Too many adds/deletes(reset bridge) • Error: Local loop • Error: Non-local loop • Error: Devices connected between bridges
PORT 5		
PORT 4		
PORT 3		
PORT 2		
PORT 1		
		Number of downstream wireless Bridges and Transceivers
PORT 2	Transceiver Port Status	Port States: • Polling downstream devices • Upstream port • Commissioning tool connected • Polling downstream bridges • Error: Too many adds/deletes(reset bridge) • Error: Local loop • Error: Non-local loop • Error: Devices connected between • bridges
PORT 1		
		Number of downstream wireless Bridges & Transceivers

ADDITIONAL nLIGHT RESOURCES

(hyperlinks provided below)

Specialty User Guides

nTune Grayscale and Color Accent User Guide
nTune Tunable White Programming Guide
nLight Relay Panel Programming Guide
nLight Programming Videos
VLP Quick-Start Guide
OpenADR Application Note
nComm Kit User Guide
Graphic Wallpod User Guide
nConfig User Guide
nLight Explorer User Guide
nLight BMS Integration Guide
nWiFi Requirement Checklist
nWiFi Commissioning Guide
nWiFi Global Commands

Programming Guides

nLight Enabled LED Luminaires
Occupancy Sensors
Photocell Sensors
Wall Switch Occupancy Sensors
Two-Pole Occupancy Sensors
Bridges
Relay Packs
Push Button Wallpods

Software Guides

SensorView Installation Guide
SensorView User Manual
SensorView Replace Functionality Tutorial
SensorView Installation Best Practices
SensorView BACnet IP Interface Statement
Green Screen Installation Guide
Virtual Wallpod Installation Guide