nLight® AIR
OPERATION, PROGRAMMING, AND MAINTENANCE MANUAL

Project Name:

Project Location:

Acuity Agency:

Order #:

PO #:

Project ID:

Date:

CONTROLS TECHNICAL SUPPORT

1-800-535-2465

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

nLight AIR O&M Table of Contents

CLAIRITY™+ Mobile App

nLight AIR

Table of Contents

Table of Contents - cont'd

Welcome

The Acuity Brands CL**AIR**ITY **+** mobile app is a one-stop resource for a variety of Acuity Brands digital solutions. CL**AIR**ITY **+** is available for both Android™ and iOS devices. This guide explains all the features and functionality within the CL**AIR**ITY **+** mobile app when selecting the nLight AIR module.

Startup Process Overview

nLight® AIR consists of fixtures (with and without integrated radios), wall switches, and sensors. There are no communication wires between the devices. Installers and other onsite personnel use the CL**AIR**ITY **+** mobile app to define how these devices interoperate to achieve the result our customers request.

An overview of the startup process we recommend you follow is shown below.

NOTE

A definition of terms section is located near the end of this guide.

1. Install and energize the equipment. You can proceed to the next step once all nLight® AIR equipment has been installed in a given functional area of the building.
2. Download the CL**AIR**ITY **+** app and select nLight AIR (first time users must follow the steps to create a user account).
3. Create the site.
4. Create the first group, identify devices, and associate with the grid.
5. Set behavior zones for each group and save to complete the commissioning process for a single group.
6. Return to step 4 when you're ready to move to the next group.

Out of Box Functionality

The devices at the site will operate under their out of box functionality but can be customized and programmed to suit the needs of the customer. Please refer to device specs sheets for specific information.

- Indoor fixtures with integrated occupancy sensors - All operate independently, and have occupancy and daylighting enabled.
- Switches - Do not control any fixtures
- Other indoor fixtures - will turn on when powered.
- Outdoor fixtures with integrated occupancy sensors - will turn on at night and off in the morning and have occupancy enabled.

Download CLAIRITY +

Start by downloading the CL**AIR**ITY **+** mobile app from the Apple App Store or Google Play Store (CL**AIR**ITY **+**). The app is no charge.

To proceed to nLight AIR, select the nLight AIR module.

Enable Bluetooth On Your Mobile Device

Once the app has downloaded, ensure that Bluetooth® is enabled on mobile device. If you're unsure, follow the steps below for either an Android or iOS device.

NOTE

Disconnect from any existing Bluetooth devices before commissioning.

For **Android** Devices:

1. Open your device's **Settings** menu.
2. Under **Wireless & Networks**, touch **Bluetooth.**
3. Touch the switch to turn Bluetooth **On.**
4. A Bluetooth icon at the top of your screen will indicate when Bluetooth is turned on.

For **iOS** Devices:

1. On your iOS device, tap **Settings >Bluetooth.**
2. Tap the switch to turn Bluetooth **On.**
3. Once complete, look for the Bluetooth icon in the status bar of your device.

Create a User Account

If this is your first time using the CL**AIR**ITY **+** app, follow the steps below to create a new user account.

1. Select nLight Products.
2. Download the CL**AIR**ITY **+ App.**
3. Tap on the **Sign Up** link on the sign in page and then select the sign up now link.
4. Enter your information, including your email address, what you'd like your password to be, first name, last name, and your display name.
5. Once complete, tap on the **Send Verification Code** button.
6. Check your email.
7. You will receive an email with a verification code.
8. Go back to the app and enter the verification code you received.
9. Click on the **Create** Button.
10. Sign into the app with your email and password (Figure 01).

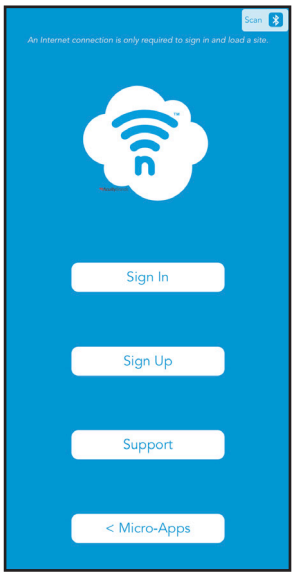


Figure 01: CLAIRITY + Sign In

Forgot My Password

If you've forgotten your password, tap on the **Can't Access My Account** link after tapping the **Sign In** button. Follow the steps to reset your password.

Sign into the App

If you already have an account, use your email address and password to sign into CL**AIR**ITY **+**.

Once you've successfully signed in, you'll see the **Sync** screen (Figure 02). While this screen is shown, the application is connecting to the cloud to retrieve your sites.

NOTE

You must have a connection to the Internet to complete this process.

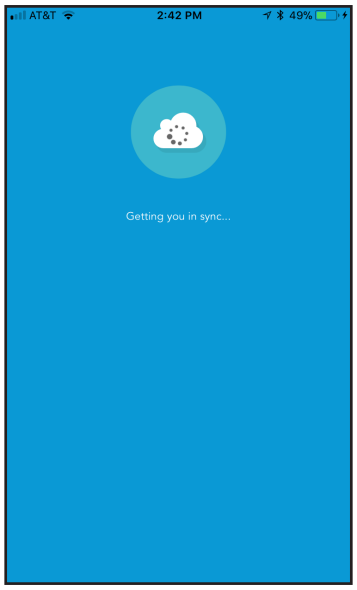


Figure 02: CLAIRITY + Sync Screen

Support

Navigate to the **Support** page from the **Sites** screen by tapping on the ☰ on the top left portion of the screen. The **Support** page (Figure 03) provides contact information for Acuity Brands, a link to a how-to video for CL**AIR**ITY **+**, a link to this user guide, a means to submit diagnostic information from your application to Acuity Brands technical support (**Send Report**), and information on your application. User guides and other documentation for nLight support can be found at: https://nlight.acuitybrands.com/resources/user-guides

For new users we strongly recommend to view the **Quick Start Guide** and startup video to become familiar with the process and the app.

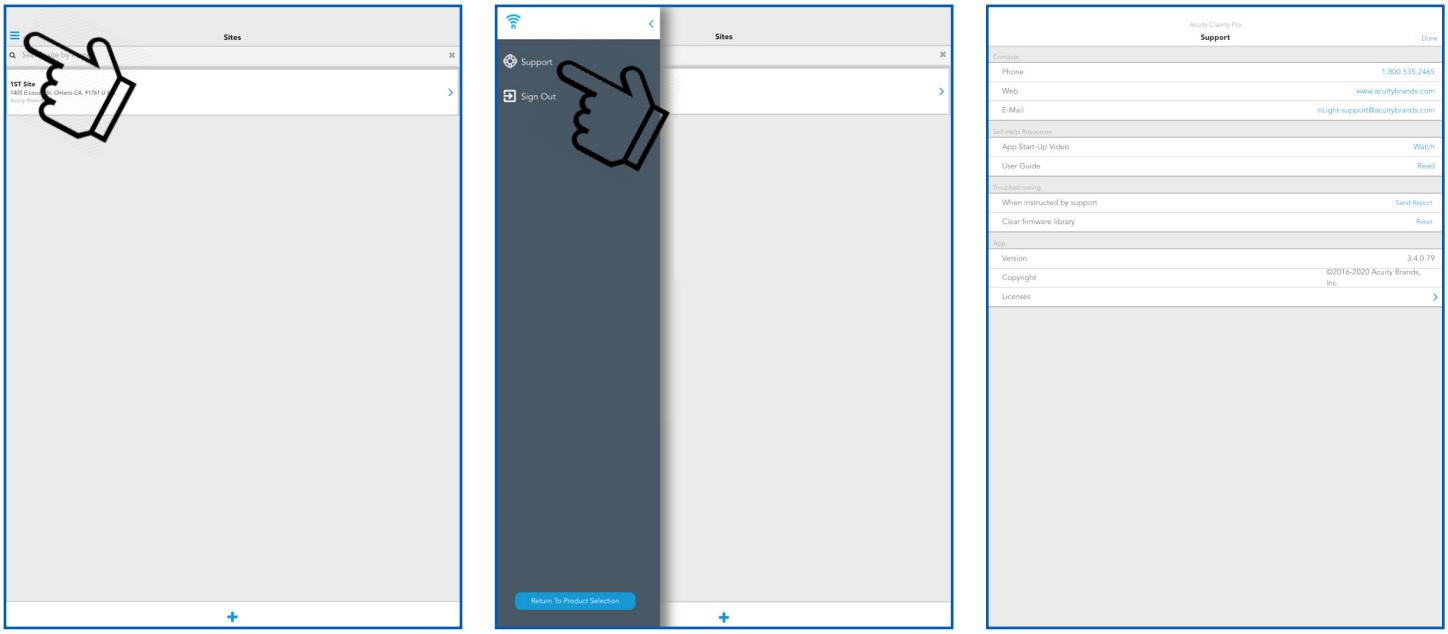


Figure 03: Support Page

Saving and Retrieving Site Information

Saving and retrieving previously saved sites in CL**AIR**ITY **+** is very easy. All the data you enter is saved in cloud-based servers for your future use. If you're not familiar with the cloud, that's OK – we take care of the technical components of the site behind the scenes using our 5 tier security system. Just know that your data is very secure and is ready for your use when you need it. The best part of the cloud is the ability to share it with others using the link https://air.acuitynext.com/.

As you make changes and proceed through the screens, information is saved either on your mobile device or in the cloud. In the event that you do not have a wireless or cellular connection to the Internet while making changes, no problem. Those changes are held within the app and pushed to the cloud as soon as you have a connection.

Sites Screen

The **Sites** screen lists all of your sites that you have either created or been give access to. After the app retrieves your sites from the cloud, it will display a list of those available to you. To work on a site, simply tap it in the list. If you need access to a site that you're not seeing in your list, please contact Acuity or contact the individual who has access to the site.

NOTE

All programming changes must be made in the immediate proximity to the area you are programming

NOTE

Internet connectivity is no longer required after you select a site to work in, and data is downloaded from the cloud.

Create a New Site

NOTE

To create a new site, follow the steps below.

If you are adding equipment to an existing installation, you must add the equipment to the existing site if the design calls for the equipment to work together.

1. From the mobile app, navigate to the **Site** Screen (Figure 04) and click on the **+** at the bottom of the screen.
2. Enter the information about the site you're creating. The more information you enter, the easier the site will be to search for and find the site in CL**AIR**ITY **+** in the future. Site Name – the name of the site or project; It will typically be the name of the building in which you're working (e.g. – the White House). We recommend that you do not abbreviate to make it easier to find the site in the future. Organization / Company – The startup service provider should select the name of the customer (e.g. – The US Government).

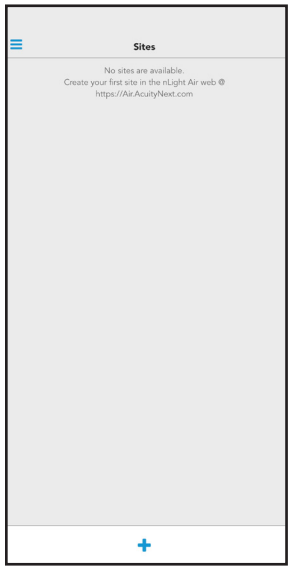


Figure 04: Sites Page - No Available

Search for an Existing Site

The Sites Screen will display all the sites to which the user can access. For some users who visit numerous sites, you can either search the sites you have created or been added to at the top of the **Sites** page using the search bar, or simply select the site you wish to access from the available items shown.

NOTE

The search is not case sensitive.

Edit an Existing Site Name or Address

Site details can be edited from the **Site Overview** screen (Figure 05) by tapping on the information that needs to change, making the change, and tapping **Done** when completed.

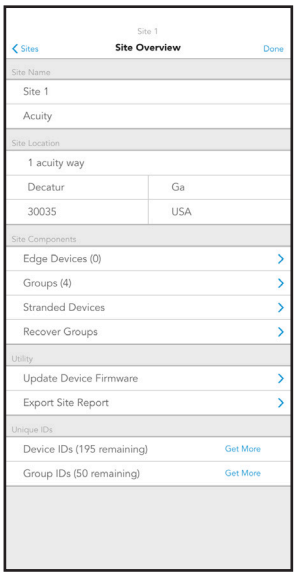


Figure 05: Site Overview

Create a New Group

Typically a group is created for each room. However, a group can not contain more than 127 devices.

To create a new group, follow these steps:

1. Tap on the **+** icon on the **Groups** screen (Figure 06).
2. Enter a name for the group. The group name is typically going to be the name of the room.
3. Tap the **Create** button.
4. You will then be taken to the **Group Overview** screen for the group that you created.
5. If you wish to edit a different group, simply select the **Group** icon in the top left to navigate back to the Groups screen.

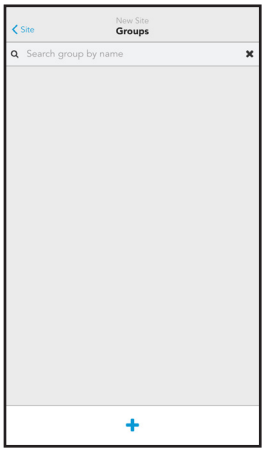


Figure 06: Groups

Edit an Existing Group

The **Groups** screen shows all of the groups within a site.

To edit an existing group, select it from the list of available groups (Figure 07).

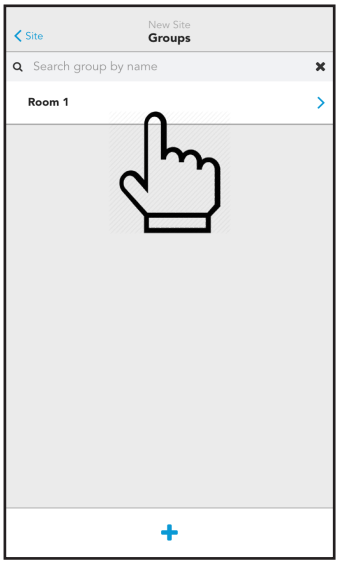


Figure 07: Groups Page

Modify the group details and tap **Done** when completed (Figure 08).

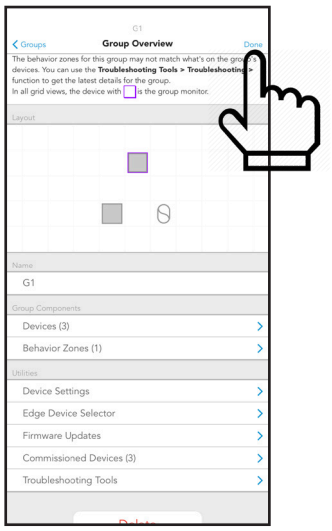


Figure 08: Groups Overview

Search for an Existing Group

The Group Screen will display all the existing groups in the site. For large sites with many groups, we have made it easy to search for the group you need. Groups can be sorted by name, signal strength, creation date, or last modified date. You can also filter to show only groups in BLE range or connected to a nLight Eclypse (EDGE Connected). To access the group search feature:

1. Navigate to the **Groups** Screen.
2. Enter the name of the group in the search bar at the top of the screen or tap the filter icon next to the search bar to access filtering or sorting options.
3. The list of groups that match your search criteria will update automatically.
4. Select the group you need to access from the list of groups.

NOTE

The search is not case sensitive.

Group Overview

The **Group Overview** screen (Figure 09) is used as a main landing point in the CL**AIR**ITY **+** app. It is the screen that allows for initial device identification and the assignment of behaviors.

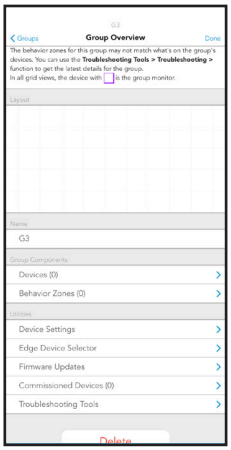


Figure 09: Group Overview

Discovering New nLight AIR Devices & Adding Devices to a Group

To discover new nLight AIR devices, following the steps below:

1. From the **Group Overview** screen, tap the **Devices** link (Figure 10).
2. The **Device Layout** screen will open. Tap the **+** icon on the bottom left of the grid (Figure 11).
3. The **Identify Devices** screen (Figure 12) will provide a list of nLight AIR devices, sorted by signal strength. If you click the **Refresh** button, the devices will re-sort based on the signal strength. If you do not see any devices in the list, ensure your mobile device's bluetooth is turned on, make sure you're in range of the devices (within about 60ft), and make sure that the device type is included in the filter at the top. Some devices, such as switches and battery powered sensors, require a button push in order to wake them up and turn the bluetooth radio on.
   Note: the list of devices has two views - those that are available and those that have already been assigned to a group.

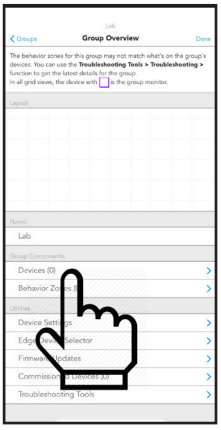


Figure 10: Groups Overview

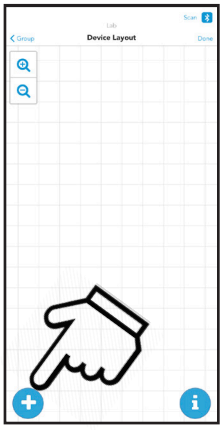


Figure 11: Device Layout

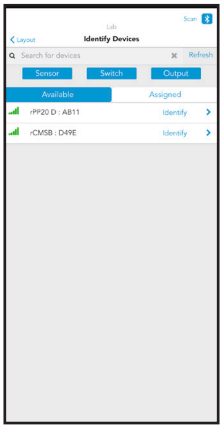


Figure 12: Identify and Select Devices

Discovering New nLight AIR Devices & Adding Devices to a Group - cont'd

4. To identify a fixture, tap the **Identify** button. Then look at the fixtures.
   - If you do not see one flashing on and off in the area, it is very possible that you are flashing a fixture in an adjacent room. So, please take care in this identifying process.
   - If you see a fixture flashing in the area you are working in, tap **Identify** again to stop the fixture from identifying, then click the arrow to the right to place the device on the grid.
5. To add the fixture to the grid, tap its relative position on the grid (Figure 13). Once the fixture has been added to the grid, it will not longer appear in the list of available devices. It will be added to the list of assigned devices. Once the fixture is added to the grid, you'll see the actual light level of the fixture change to a lower light output. Use this as a way to track how many more fixtures need to be added to the grid from the room you're in.
6. Continue this process until all fixtures in the area have been identified and added to the grid.

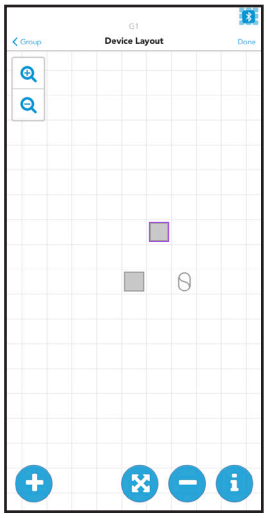


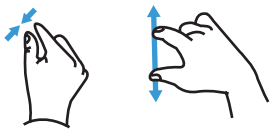
Figure 13: Device Layout - Grid

NOTE

A group may not contain more than 128 devices.

NOTE

The assigned tab has three distinct colors/symbols. A gray arrow indicates the device is assigned to the current group you are in. A blue arrow indicates the device is assigned to another group than the one you are currently in. A purple check indicates this device is a group monitor (and may or may not be in the current group you are in). All these devices are beaconing through their BLE radio.



NOTE

If you're working in a large area, you may find it necessary to move around the area to see all the devices. The list of devices will not automatically refresh. If you've moved within the area, we recommend tapping the refresh button. The list will update to show you those devices that have the strongest signal strength for your present location.

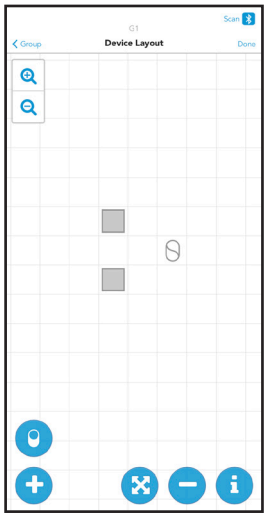


Figure 14: Device Layout - Wall Switch

NOTE

You can pan around the grid by dragging your finger across the grid. You may also zoom in and zoom out by using the +/- buttons or by pinching or spreading with your fingers on the screen.

7. Once you're ready to begin discovering wall switches, tap on the **+** button.
8. Choose the **Switch** option on the **Identify Devices** screen.
9. Press a button on the actual wall switch – the physical device on the wall. Wall switches will not remain in the list. They go to sleep after 1 minute of inactivity. Press any button on the switch to wake the device.
10. After the button is pressed, you'll see a wall switch on the device screen.
11. Press **Identify** and validate that the LED's on the front of the switch begin flashing.
12. Associate that device with its location on the grid by tapping on its relative position in the grid (Figure 14).
13. If you have stand-alone sensors in the space, tap on the **+** button.
14. Choose the sensor option on the **Identify Devices** screen.
15. For battery powered sensors, press the button next to the lens twice to wake it. They go to sleep after 1 minute of inactivity. Once the sensor is listed, press **Identify** and validate the LEDs on the sensor blink (**note** - motion will also cause the sensor to blink. So, stand motionless below the sensor during this step).
16. Associate that device with its position on the grid relative to the other devices.

Moving Devices on the Grid

1. To move a device on the grid, select the arrow button between the plus and minus buttons.
2. Select the device that needs to move by tapping it on the grid.
3. Select a new location for the device by tapping on the grid.

Removing Devices from the Grid

In the event a device needs to be removed from the group (whether it has been fully programmed or not), follow these steps:

1. Ensure you're physcally located in the group.
2. Navigate to the group in the app.
3. Open the **Group Overview** screen.
4. Select **Devices**.
5. From the grid view, select the **—** button at the bottom of the screen.
6. Tap on the device that needs to be removed.

NOTE

You must be located in the vicinity of the devices to perform this action. Removing a device may require changes to the Behavior Zones to ensure proper operation.

Device Information

Additional device information can be retrieved while on the grid screen. To do this, follow these steps:

1. Navigate to the grid screen.
2. Select the "i" icon in the lower right corner of the grid (Figure 15).
3. Tap on any device. This will show the device type, BLE ID, Device ID, Firmware versions, and label. Label default is BLE ID_GroupName. This label can be edited simply by tapping on the label, editing, and tapping the save button.
4. By tapping on any additional device, or the same device, you will flash the fixture once. You can repeatedly select the same device for an additional flash on each tap.

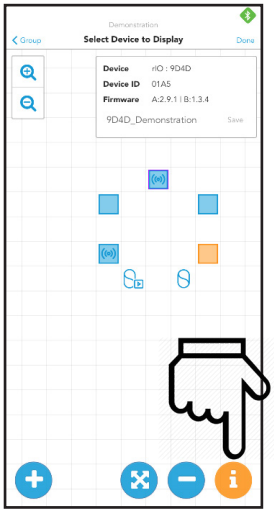


Figure 15: Moving Devices on the Grid

Creating Group Behavior Zones

1. Once the desired devices within a group have been added to the grid select **Done** in the top right corner of the page (Figure 16). This will take you to the **Behavior Zones** page where you will create or edit the behavior zones of the devices within your group. Optionally, you can navigate to behavior zones from the **Group Overview** screen, just below **Devices**.

2. On the **Behavior Zones** page your first option will be to select from behavior zone **Templates** where you can select **Description** to understand more about this template. If you wish to add one of these templates simply select the **+ Add** button (Figure 17). When a behavior zone template is added, a set of behavior zones will be created and listed at the top of the page.

3. The behavior zone identifies the number of outputs, sensors, and switches in the specific behavior as a function of the total number within the group. The specific settings that have been applied within a behavior zone are displayed as well. Once a behavior zone has been created, you can either delete or edit the behavior to further customize your behavior zones (Figure 18).

4. You also have the option of foregoing the behavior zone templates and creating your own behavior zone by selecting **Create a Behavior Zone** just below the Templates (Figure 17). Based upon the devices that have been added to your group, you will have the option to select from different behavior types (switch control, occupancy-common sensors, occupancy-individual sensors, photocell-common sensors, photocell-individual sensors, and External Input) (Figure 19).

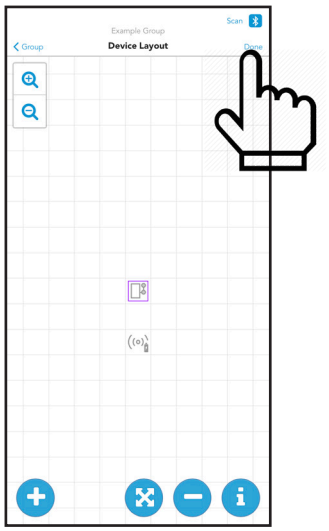


Figure 16: Device Layout Done

Figure 17: Add Behavior Zones

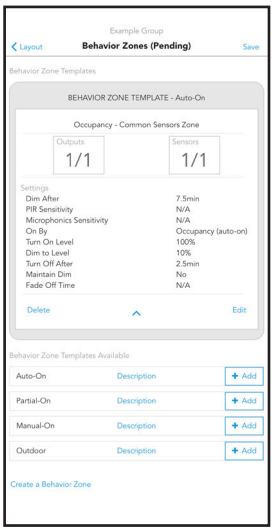


Figure 18: Behavior Zone Templates

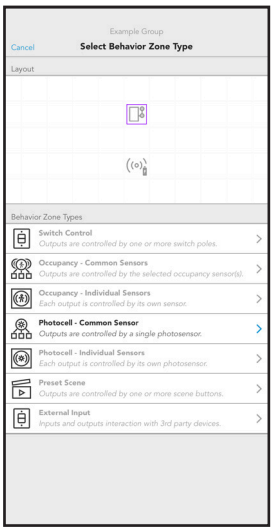


Figure 19: Behavior Zone Template

Creating Group Behavior Zones, cont'd

5. Select the behavior type that you would like to apply. Then tap the devices on the grid that you want to be part of this behavior zone (they will turn orange) (Figure 20). You can also click **Select All** or **Clear Selection** at the bottom of the page. After selecting the desired devices, you can either tap **Done** to create the Behavior Zone or tap the **Settings** tab to further define the settings.

6. If you have selected the **Settings** tab you can further customize your behavior set (Figure 21). Change the settings as required based upon your needs. Tap **Done** when complete with the behavior zone and you will return to the behavior zones screen with your newly applied behavior zone.

7. Configuration flags are added just above Behavior Zones to alert users of either a non-ideal Behavior Zone or to prevent saving altogether. An orange triangle (Figure 22) is a cautionary flag, but you can still proceed with saving. A red triangle (Figure 23) indicates an incorrect setting, and you cannot proceed with saving until the issue has been resolved.

8. Once you have resolved any issues, or chosen to move on with cautions if applicable, click the **Save** button in the upper right corner. This will network your devices together and send the behavior zone information to each device. In some cases, a battery powered sensor may return to a sleep state prior to this step. If this occurs, the app will instruct you to walk to each sensor and wake the device via motion. Alternatively, you can wake battery powered sensors via double tap of the button next to the lens. After waking all sensors, the save process will proceed. You have now commissioned these devices.

NOTE

When commissioning devices for the first time, some behaviors may take up to 2 minutes to respond correctly.

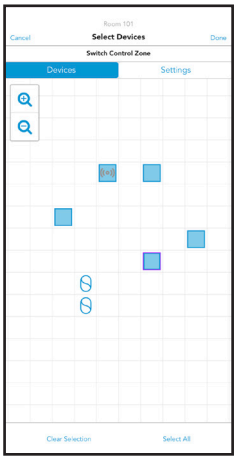


Figure 20: Select Devices from Grid

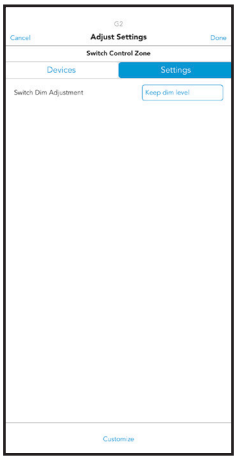


Figure 21: Settings Tab

Figure 22: Orange Triangle

Figure 23: Red Triangle

Behavior Zones Explained

Below is a summary of all behavior zones and how they can be configured.

1. On / Off by switch:
   - Can be applied to any group that has at least one fixture and one switch.
   - You may select if the light comes on to full bright or if it turns on to the prior dim level when the on button is pressed.
   - If combined with daylighting turning the lights on will make the fixtures go to their day lighting level. If the switch has raise and lower buttons, the user may raise the light level above the daylighting level.
   - If combined with occupancy the switch will override the occupancy behavior for 1 minute.

2. Occupancy:
   - Can be applied to any group with at least 1 sensor.
   - Configurable parameters include
     1. On by:
        - Occupancy (Auto on) - lights will turn on when at least 1 sensor in the zone sees motion. Lights will dim down after "X" minutes of no activity.
        - Switch (Manual On) - Lights must be turned on via a switch. Lights will dim down after "X" minutes of no activity.

2. Turn on to xx% when occupied.
3. Dim to % - The level the lights will dim to after "X" minutes of no activity.
4. After "X" minutes of no activity - The time delay between the sensors no longer sensing motion and the lights dimming to the dim to %.
5. Turn off time - The time delay between the dim to light level and the lights turning off. Total time between no motion and the lights turning off is the sum of the turn off time and the dim after time.
6. Maintain Dim for Open Office - If multiple zones within the same group are not all unoccupied, this setting forces this specific zone to remain at its dimmed state when unoccupied, until all zones within the group are unoccupied.
7. PIR Sensitivity - Options for sensitivity level of PIR.
8. Microphonics Sensitivity - Options for sensitivity level of Microphone.

- Immediately after sending programming values to the fixtures, the fixtures require a few minutes to synchronize before following the programmed time outs.

3. Photocell:
   - Can be applied to any group with at least 1 sensor.
   - Must be calibrated after programming has been sent to the fixtures. This can be done by navigating to the group overview screen, selecting device settings, and selecting photosensor calibration.
   - Users must select individual or common for photocell or occupancy behavior types. Individual sensors will control only the fixture it is associated with. It will result in an inconsistent lighting look on the ceiling, but it may be more consistent on the work surface. Common sensors will result in all the fixtures within a behavior zone responding to the one sensor, or multiple sensors, that the user selects. This option will result in a common look across the ceiling or lot.

4. Preset Scene Selector:
   - Only applies to groups with a scene switch in them.
   - Scenes allow users to customize their outputs by selecting different levels of light for each scene number available.
   - For each scene switch, users can add as many scenes as are available on the scene switch. If a scene switch has four numbers, four different scenes may be added to the behavior zone. More than 1 scene switch may be added per group, with up to 16 scenes available to be added per group.
   - You may select multiple scene buttons per each scene behavior zone. For instance, if one desires scenes 1 and 3 to have 50% output, select both numbers and then select the devices. Once created, a preset scene will set all output devices in a group to the saved static level through a single button press.
   - Set up instructions:
     1. Select **Create A(nother) Behavior Zone** (Figure 24) and select **Preset Scene** (Figure 25).
     2. Select a scene switch (2 or 4 square device on grid), choose the number you would like to edit on the switch and then tap **Done** (Figure 26).
     3. On the grid, select the devices you would like this scene to affect then navigate to the **Settings** tab (Figure 27).
     4. In the settings tab, drag the cursor to the desired light output. Users can also select to prohibit or allow manual change on the scene switch. If prohibited, scenes can only be edited through the CL**AIR**ITY **+** application (Figure 28).

NOTE

CLAIRITY + will gray out a condition if the setup of your system will not support it.

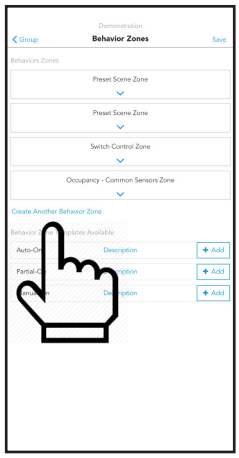


Figure 24: Create Behavior Zone

Figure 25: Preset Scene

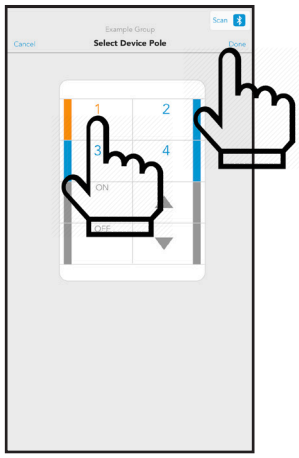


Figure 26: Select Scene Button

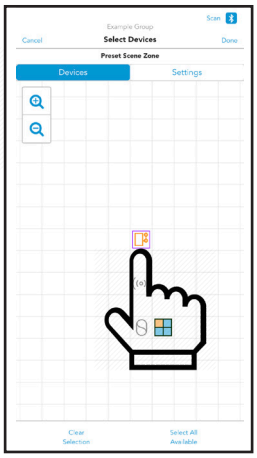


Figure 27: Select Device

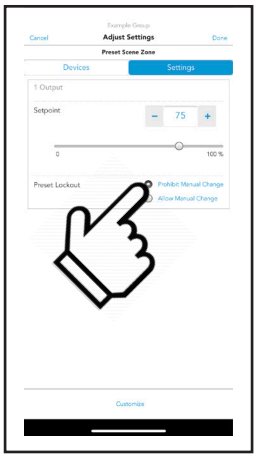


Figure 28: Adjust Settings

Creating Customized Settings

Customized settings allows a user to add additional devices to a zone with different settings. To create customized settings, follow these steps:

1. To customize a behavior zone, navigate to the behavior zone and select the **Settings** tab. Then select the **Customize** button located at the bottom of the page (Figure 29).
2. This will pull up a menu that contains either the switch or the sensor as well as the outputs. The **+** icon at the bottom allows you to add additional controllers or outputs with different settings (Figure 30).
3. Select **Output** or **Controller** as the device(s) for the customized setting (Figure 31).
4. Next, select the devices you wish to have a different setting applied (Figure 32).
5. Change the settings as needed and tap **List** in the upper left corner to return to the **Customized Settings** menu (Figure 33).
6. You have now created a new customized setting and will see the new details in the device list. Tap **Next** to complete this customized setting for the behavior zone (Figure 34).

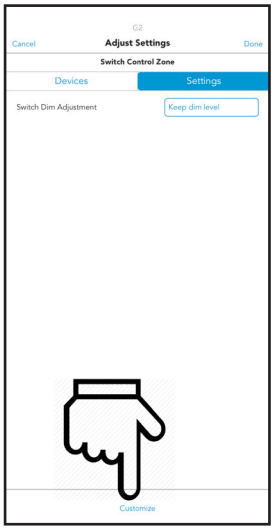


Figure 29: Choose Customize

NOTE

If a customized setting has been created while editing a behavior zone, you will need to edit that customized setting from the customized setting screen. Click Edit to navigate to the customized settings screen, then select the desired customized setting to enter the grid screen. When editing a behavior zone, if there is no customized setting, you will simply return to the grid screen.

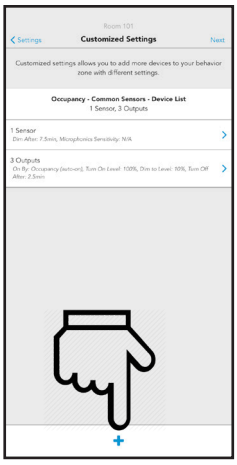


Figure 30:Customize

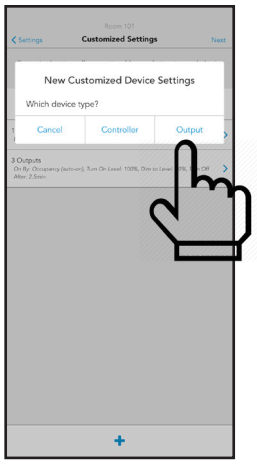


Figure 31: Select Output

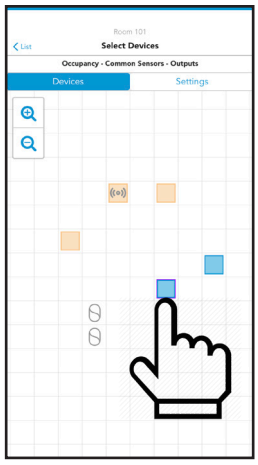


Figure 32: Select Next Devices

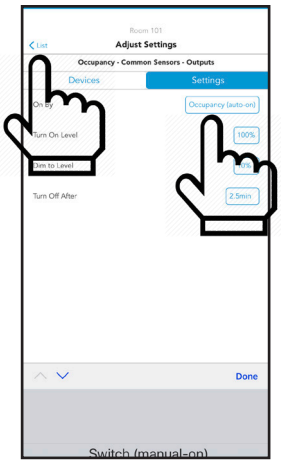


Figure 33: Select Settings

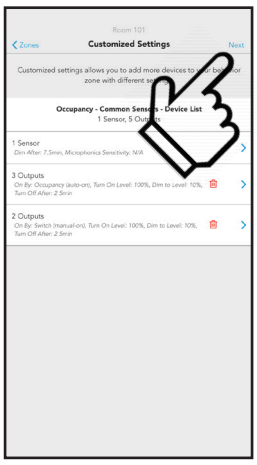


Figure 34: Select Next

Preset Scene Customization

When creating a preset scene, users have the option to "customize" and create different setpoints for different devices all within the same scene. Each device within a single scene can only adhere to one setpoint percentage.

Setting up customized scenes example:

1. Once a preset scene has been established with required devices, navigate to the settings tab and select the set point as you normally would.
2. At the bottom of the settings tab, select the **Customize** button (Figure 35).
3. This will take you to the customized settings tab within your scene. From here you can see the setpoints you have already created. To add a new setpoint, tap the "**+**" button on the bottom of the page (Figure 36).
4. A new customized device setting box will appear, select output. Now, select the devices you want for your new setpoint (Figure 37).
5. Navigate to the settings tab and adjust the setpoint as you would normally do when creating a preset scene and select the **Lists** button in the top left corner (Figure 37).
6. This will take you back to the customized settings screen where you will see the setpoint you have just added (Figure 38).
7. You can continue to customize your scene and edit different device setpoints until the desired settings are met.

NOTE

If a device has already been selected previously, it will appear in light orange and you will not be able to select it. You can make it available by returning to the Customized Settings list, selecting the zone it belongs to, and deselecting that device (it will turn blue). (Figure 39)

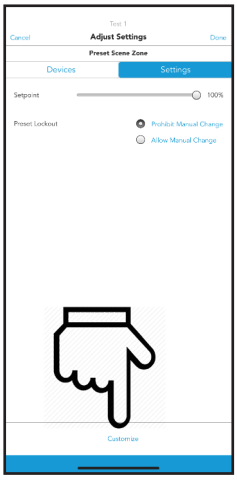


Figure 35: Adjust Settings

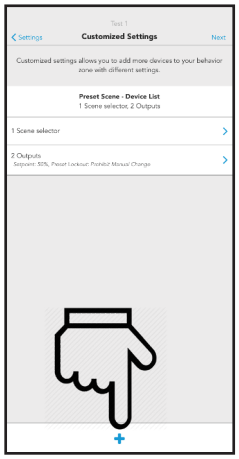


Figure 36: Customized Settings

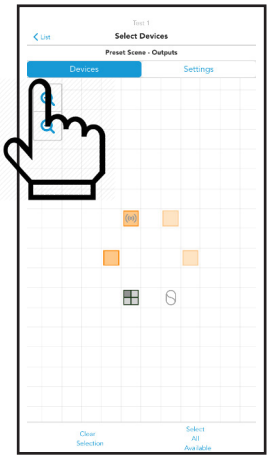


Figure 37: Select Devices

Figure 38: Customized Settings

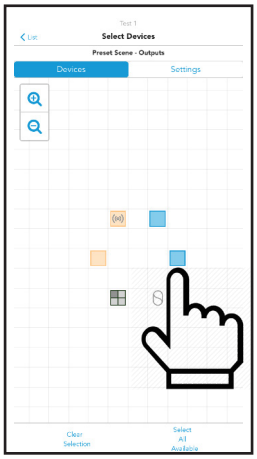


Figure 39: Deselect Devices

Commissioning an nLight AIR Adapter

To commission a new nLight AIR adapter, permanently mount the adapter. Do not commission the adapter before it is permanently mounted. Moving it can result in unstable RF connections to devices you've commissioned.

Once the adapter has been mounted and plugged into the ECLYPSE, allow 2 minutes before adding it to CL**AIR**ITY **+**. For the first 2 minutes, the Adapter is determining the clearest communication frequency to use. If you try to commission it too quickly after power on, CL**AIR**ITY **+** will provide you with a warning.

Commissioning an nLight AIR Adapter - cont'd

1. Navigate to the **Site Overview** screen (Figure 40).
2. Select **Edge Devices** (Figure 41).
3. Walk within about 30 feet of the Adapter you need to add.
4. Tap on the **+** to add a new Adapter.
5. Select the adapter from the list of available adapters.
6. Unless otherwise instructed by Technical Support, keep automatic mode enabled, and tap **Commission** (Figure 42).

If the project has more than one adapter, it is strongly recommended that you name the adapters. To do so, tap on it and rename it in CL**AIR**ITY **+**.

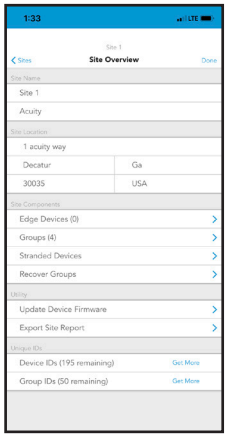


Figure 40: Site Overview

Figure 41: Available Edge Devices

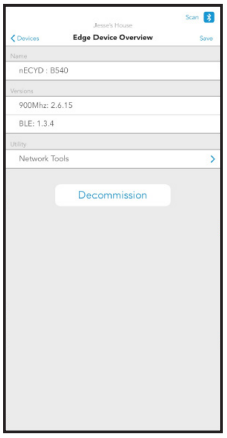


Figure 42: Edge Device Overview

Network Tools

The Edge Device Overview screen includes a Network Tools utility that includes two key functions: Network Troubleshooting and Connectivity Check. Both functions can be ran while within range of the Adapter (30 feet).

Network Troubleshooting triggers a query between CL**AIR**ITY **+** and the edge device (Adapter), updating the Adapter firmware version recorded in CL**AIR**ITY **+** if the firmware were updated from SensorView after initial discovery, listing any groups that are missing from the Adapter database, listing groups that may be missing from CL**AIR**ITY **+** that are present in the Adapter database, and giving a complete list of devices and groups that appear in both CL**AIR**ITY **+** and the Adapter database.

Network Troubleshooting should be run after updates are provided to devices from SensorView. It allows for synchronization between CL**AIR**ITY **+** and an Adapter, and synchronization is required for CL**AIR**ITY **+** to communicate effectively with the edge device, to create a database with device information, and to update information on connected devices.

Connectivity Check performs a test between the edge device and all non-battery, connected devices, listing devices and groups and flagging devices that have poor signal strength with the edge device.

Associate a Group with an nLight AIR Adapter

To associate an existing group with the nLight AIR Adapter, navigate to the Group Overview Screen. Walk to the physical space that correlates with the group. Tap on the **Edge Device Selector** option. Pick the appropriate Adapter from the list. Tap on the **Assign** button. CL**AIR**ITY **+** will make the appropriate RF Channel changes so the devices can communicate with the Adapter you've chosen.

CL**AIR**ITY **+** will also instruct the devices to attempt to communicate with the Adapter. The app will tell you once this process is complete. Once complete, the group will show as a networked group on the group screen with an icon next to the name. It will also be accessible in the Sensorview software.

CL**AIR**ITY **+** will show you any devices that are unable to communicate to the Adapter. You may retry. But, if the devices are unable to reach the adapter, please choose a different one on the project.

nLight AIR Adapter Recovery

If an adapter was force removed for any reason, the Recover Edge Devices tool will allow you to recover this device.

To recover edge devices within the CL**AIR**ITY **+** app, select "recovery tools" from the site overview screen, then select "recover edge devices" (Figure 43).

Navigate to the "unknown" tab and any unknown devices will be shown, allowing you to recover them to factory settings (Figure 44).

Figure 43: Site Recovery Tools

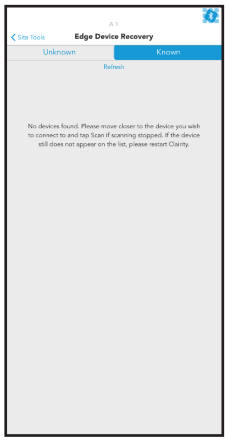


Figure 44: Edge Device Recovery

Move a Group from one nLight AIR Adapter to Another

To move a group from one nLight AIR Adapter to another, navigate to the Group Overview Screen. Walk to the physical space that correlates with the group. Tap on **Networked Edge Device** and tap on the **Unassign** button. Once complete, the group will no longer be associated with that Adapter.

Now follow the steps to Associate a Group with the nLight AIR Adapter.

Calibrating the Daylighting in an Area

To calibrate daylighting, follow the steps below:

1. Navigate to the **Group**.
2. From **Device Settings**, select **Photosensor Calibration** (Figure 45).
3. Manually adjust the set-point or choose to auto-calibrate the photosensor.

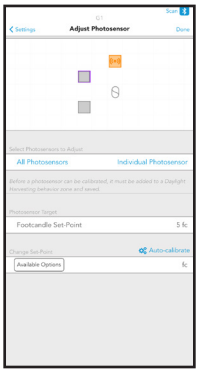


Figure 45: Photocell Calibration

Disable a Sensor

To optimize occupancy performance, sometimes it is necessary to disable sensors in fixtures. It may be necessary to do this to the fixture close to a doorway so it does not detect hallway traffic or in cases where sensors are very close to HVAC ducts.

To enable or disable particular sensors, simply select the sensors that you want applied (or not applied) to a specific behavior zone within the behavior zone workflow.

Set Dual Zone Offset

Offset is a sensor setting that commonly allows users to dim a second row of fixtures differently than the row closest to the windows in cases when only one sensor is being used. This feature is not needed in cases when each fixture has a sensor embedded.

To enable this feature, you must create a customized setting within a daylight harvesting zone. Create a custom behavior zone, choose photocell-common sensor, and select the first row of fixtures and the sensor. Go to the settings tab and select **Customize**.

Select **+** to add an output, and then select the devices that should dim less than the others by selecting them on the grid. Note, you may select more than one device at a time. Tap on the **Offset % Value** to make an adjustment. Note, a value less than 100% will cause the fixtures selected to dim less than those not selected. Finish by going back via **List** in the upper left corner, and then selecting **Next** in the upper right corner.

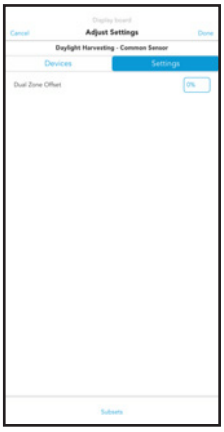


Figure 46: Offset

Microphonics Sensitivity

To optimize occupancy performance, you have the ability to adjust the microphonics sensitivity (for devices that have this capability).

To adjust microphonics sensitivity, select **Occupancy** under **Create a Behavior Zone**. Navigate to the **Settings** tab once you have selected the desired devices, tap **Microphonic Sensitivity** and select the level you would like the fixtures to respond to.

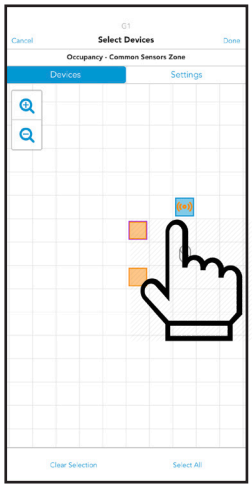


Figure 47: Select Sensor

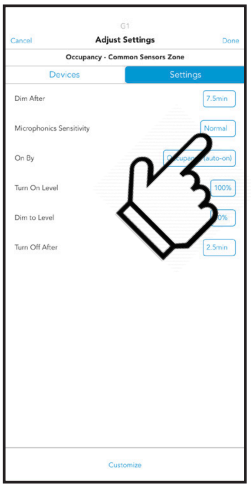


Figure 48: Microphonics Sensitivity

PIR Sensitivity

Groups with occupancy sensors can set and adjust PIR sensitivity. nLight AIR devices are intially programmed for high sensitivity, allowing you to decrease in situations where there are an increased number of false trips. To adjust sensitivity, follow the steps below:

1. Create an occupancy behavior zone.
2. Select the devices on the grid you want to adjust and navigate to the **Settings** tab.
3. Select **Low**, **Medium**, or **High** sensitivity (Figure 49).

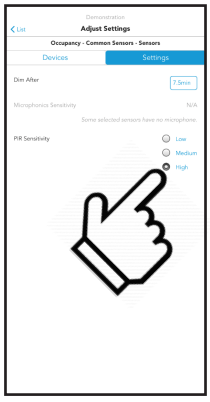


Figure 49: PIR Sensitivity

Set High/Low End Trim for Power Packs, rLSXRs, rSBORs, and rSDGRs

To adjust the maximum or minimum light level an output device can achieve, you can adjust the **High/Low End Trim**.

To do so, navigate to the **Group Overview** screen and choose the **Devices Settings** option (Figure 51). For 0-10V devices (such as the rPP20 Power Pack, rLSXR, rSDGR, and rSBOR), tap the **Low Voltage High/Low End Trim** option (Figure 50).

Tap on the devices you wish to change, use the sliders to make the adjustment, and tap **Save**.

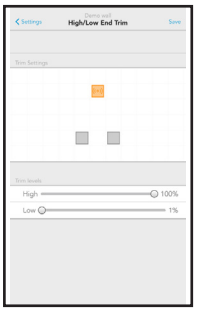


Figure 50: Hi/Low Trim Settings

Set High/Low End Trim for rES7, rIO, rMSOD and rSBG Based Fixtures

To adjust the maximum or minimum light level an output device can achieve, you can adjust the **High/Low End Trim**.

To do so, navigate to the **Group Overview** screen and choose the **Devices Settings** option. For rES7, rIO, rMSOD and rSBG Based fixtures, tap the **Digital High/Low End Trim** option.

Tap on the devices you wish to change, use the sliders to make the adjustment, and tap **Save**.

Group Firmware Updates

Group Updates - The CL**AIR**ITY **+** mobile app is able to update the firmware in the nLight AIR devices. This should only be done when instructed by Acuity Tech Support or upon receiving a notification from the mobile app.

To do so, ensure you're physically located in range of the group to be updated. Navigate to the appropriate group in the CL**AIR**ITY **+** mobile app. Near the bottom of the group overview screen (Figure 51), tap **Firmware Updates**. The **Firmware** screen (Figure 52) will show the latest version of firmware available and a summary of the firmware versions of the devices in the group. To update all devices in a group, tap **Install**.

Devices that are assigned to a group may also be updated individually. This is done by selecting the **Individual** tab (Figure 53) and clicking **Update** beside the device that needs an update.

NOTE

This process may take 2 - 5 minutes. You may leave the area when the progress bar reaches 100%. CLAIRITY + will tell you when you can move on to new areas.

NOTE

Wall switches and battery powered sensors can only be updated via the Individual tab.

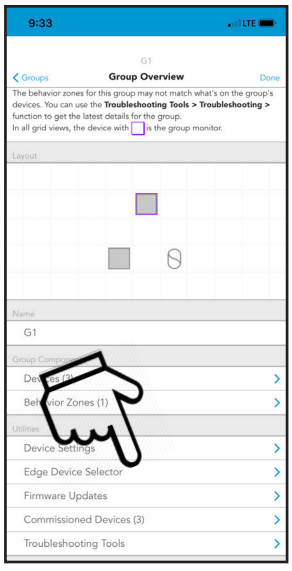


Figure 51: Group Overview

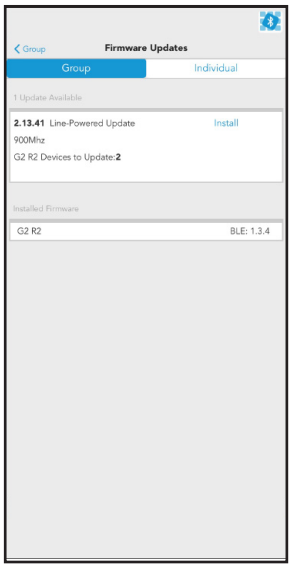


Figure 52: Group Firmware Update

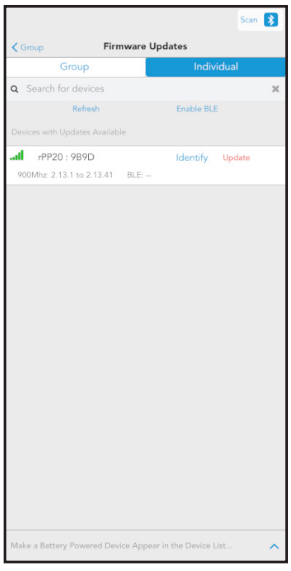


Figure 53: Individual Firmware Update

Individual Device Firmware Updates

To update an individual device before it is commissioned, navigate to the **Site Overview** page (Figure 54) and tap on **Update Device Firmware**. Once a device has been commissioned, it will no longer appear in this list and will only be updateable in the Group Firmware Updates screen.

From the list of devices, identify the device you want to update by using the **Identify** link (Figure 55). Tap **Update** to start the firmware update process.

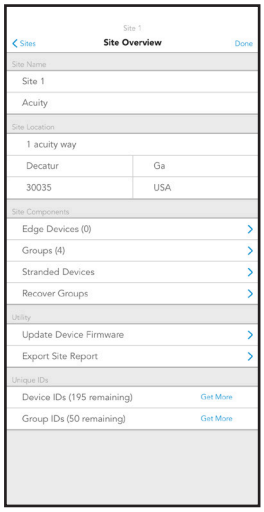


Figure 54: Site Overview

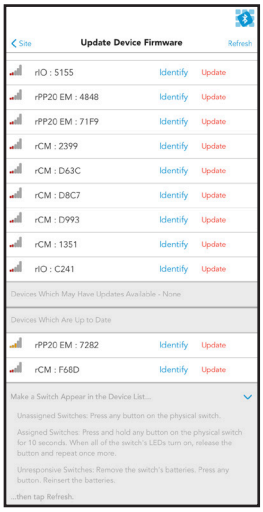


Figure 55: Update Firmware

NOTE

You must remain within 60 feet of the device you're updating for the duration of the update, which may be 3-4 minutes.

Site Access

For any site you create, you will have access to that site upon subsequent logins. However, you will not be able to see sites you did not create until access is granted to you. Please contact the original site creator to request access or reach out to Acuity. If you're not sure who created the site for the equipment you need to program, please reach out to Acuity Technical Support.

Sharing Sites

Sites may be shared with colleagues or customers. To do so, follow these steps (as detailed in Figure 56):

1. In your browser, go to air.acuitynext.com.
2. Sites that can be shared are listed under the Site Share tab.
3. Click on a listed site or search for the site you wish to share.
4. Enter the CL**AIR**ITY **+** user ID for another user into the Users search field.
5. Click Add User to grant the user access to the site.

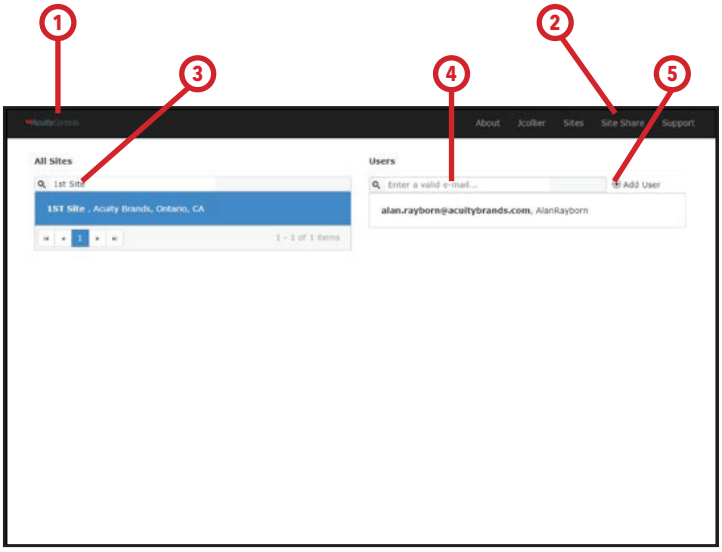


Figure 56: nLight AIR Website

NOTE

You'll be unable to share a site with someone who has not gone through the process of creating a CLAIRITY + account.

Communication Architecture

The communication between the app and the devices behaves differently before and after the initial grouping process.

Prior to devices being added to a group:

- The app communicates directly to each device via Bluetooth.

After devices have been added to a group:

- The app communicates with only one device (called the group monitor) within the group. That device then communicates to all the others on a different frequency.
- While the Bluetooth communication distance is approximately 100ft, it is possible the group monitor is out of range of the Bluetooth communication based on where you are standing within the area (especially for very large areas). If the CL**AIR**ITY **+** app fails to connect to the Group Monitor, the application will display a grid representation of the group and indicate which device to move toward to facilitate communications.

Troubleshooting Tools

Troubleshooting tools provide a few ways to check the health of your system or connect with previously commissioned groups. In the **Group Overview** screen, navigate to **Troubleshooting Tools**. From here, you are presented with several options: **Troubleshooting, Connectivity Check, Health Check, Repeater Diagnostic Tool,** and **Group Monitor Tool.**

Troubleshooting provides a few different checks for the group. First, it runs a connectivity check for all devices, verifying the devices can be reached by the group monitor. Those will be shown in green, with devices not found in red and devices not checked unchanged (in blue)(Figure 57). In addition to this check, this task will also download the latest device settings (including behaviors) applied to each device. Further information can be seen by selecting **Details**, tapping the **i** button and then selecting a device (Figure 58). When changes are made in SensorView, Troubleshooting will pull those changes across into CL**AIR**ITY **+**.

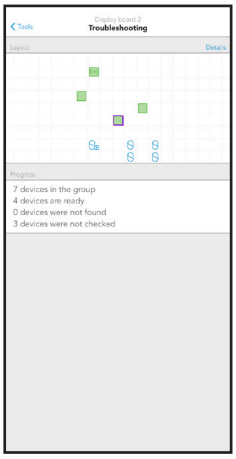


Figure 57: Troubleshooting

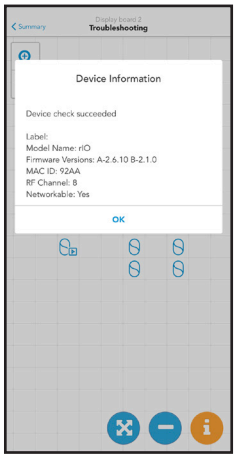


Figure 58: Troubleshooting Results

Connectivity Check will verify all output and sensor devices within the group are able to be reached by the group monitor.

Health Check prepares a group-specific report for that can be sent through the "Send Report" button found under the Support screen.

Repeater Diagnostics Tool will yield information on devices that could act as repeaters. This menu will show items such as hop layer, daughter count, and repeater status per device when the information button is pressed (Figure 59).

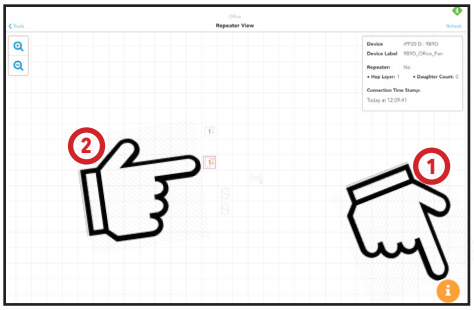


Figure 59: Repeater Diagnostics

Group Monitor Tool allows a user to select a new group monitor. This is done by selecting the "i" button selecting a non-battery powered device, and selecting Make Group Monitor (Figure 60).

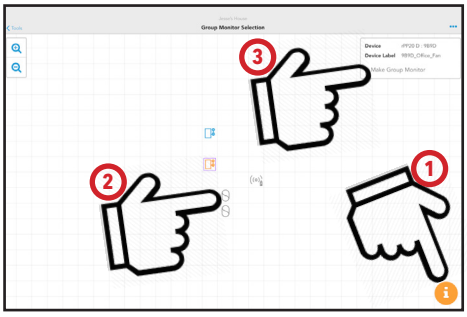


Figure 60: Group Monitor

Who to Call if You Have Questions

For support with your nLight AIR controls system and the CL**AIR**ITY **+** mobile app, please contact Acuity Technical Support at **1-800-535-2465.**

Updating CLAIRITY +

In the event that a new version of CL**AIR**ITY **+** is developed, you'll receive a notification through the app store that a new version has been made available. We recommend reading through the release notes associated with the new version so you can learn of the new features and capabilities of the new version prior to downloading it.

Multiple Users on One Site

More than one service provider may use the CL**AIR**ITY **+** app at one time. This is most common in the case of large sites with relatively short construction cycles. Each user can run through the startup process (create groups, create zones, set behaviors). We have a few recommendations for how to maximize their efficiency.

- Any user who has access to the site can grant access to others.
- We suggest each resource work in a different portion of the building. The distance between resources minimizes the likelihood that devices will be flashed in someone else's area. Resources cannot perform startup activities within the same group.
- In the event that simultaneous users are in a building that has poor cellular coverage, we recommend regular communication with your colleagues to ensure each knows who is starting up which portion of the building, as changes they make on their mobile device will not show on your mobile device until those changes can be pushed to the cloud through a cellular or wireless connection.

Reprogramming an Area

If changes need to be made to a given area, navigate to the group that corresponds with that area. The same process is followed for button reprogramming, occupancy sensor adjustments, and photosensor recalibration.

- On the Group Overview screen, tap on **Behavior Zones**
- Adjust the behavior zones accordingly. The behavior zones screen allows for the adjustment of occupancy parameters and switch settings.
- Tap **Save** and the programming will be pushed to the nLight AIR devices.
- For other device settings, such as photosensor calibration, navigate to the **Device Settings** screen from **Group Overview**, select the setting to adjust, and follow the instructions.

Whole Group Decommissioning

Whole group decommissioning is a process that will destroy all programming, zoning, and grouping. Essentially the fixtures will return to their out of box default state. Whole group decommissioning should NOT be used to modify zoning or programming parameters.

Whole group decommissioning should rarely be used. However, there are some circumstances where it makes sense. These include renovation of a previously commissioned nLight AIR space and product demonstrations.

To decommission a group:

1. Navigate to the **Group Overview** screen.
2. Click on the **Commissioned Devices** link (Figure 61). The commissioned devices screen will load.
3. To proceed with decommissioning, tap the **Decommission All** link (Figure 62).

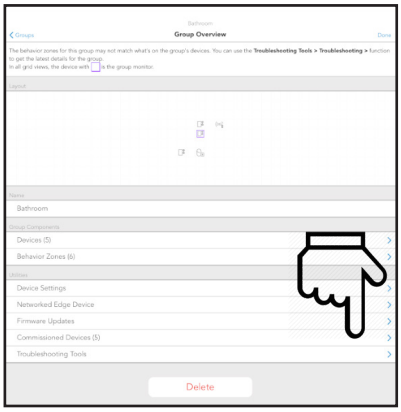


Figure 61: Group Overview

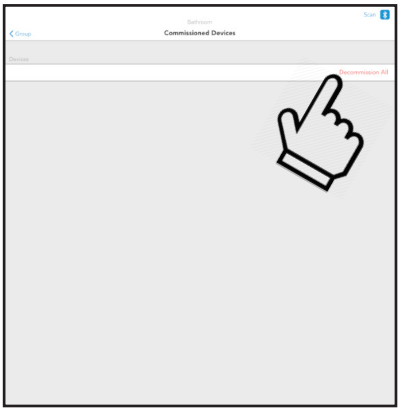


Figure 62: Commissioned Devices

NOTE

You must be located in the vicinity of the devices to perform this action.

Physically Removing Equipment

In the event that equipment needs to be physically removed from an area, you must first follow the **Removing Devices from the Grid** process described earlier in this document. Failing to do so will result in the inability to reprogram the device that has been removed.

Definition of Terms

Account	One or more sites that are all affiliated with one end user.
Area	A descriptor for a physical geographical area, within a customer site, that has some common use or purpose
Behavior Zone	A collection of devices expected to work together, defined by a specific behavior type. This is also referred to as the sequence of operation.
Commission	The act of finalizing device programming or pairing a device to a site.
Daylighting	A lighting control strategy that accounts for the presence of natural light and changes the artificial light to achieve a desired light level
Device	A generic term used to describe the individual units that comprise a system.
Fixture	A piece of equipment that outputs light
Group	All the devices within one area
Identify	A process by which a device provides some visual feedback (e.g. - the flashing of a fixture) so it's location can be determined.
Mobile Device	A personal handheld communication device that provides connectivity to wifi, cellular, or bluetooth
Occupancy Sensor	A control device that detects motion
Photosensor	A device that detects the presence of light.
Repeater	A device that forwards status and/or setting information to other devices that are out of range of initial broadcasting range of a transmitting device (such as the nLight AIR Adapter).
Site	An installation of lighting control equipment for one customer at one location
Startup	The act of troubleshooting and programming a new installation of equipment
Switch	A piece of equipment that, is typically mounted on a wall, that a user may interact with to control lights in their vicinity
Template	A pre-defined collection of behavior zones that create the described operation.

SensorView User Guide

Table of Contents

Table of Contents - cont'd

SensorView Overview

SensorView is an intuitive and easy-to-use, web-based software that gives authorized users the ability to remotely configure and monitor nLight® Wired and nLight® AIR network luminaires and controlled devices. It provides a simple and quick setup tool for creating custom configuration profiles that can either be scheduled or run on demand. SensorView also can assist with system commissioning by indicating and reporting on sensor and controller settings in addition to displaying live device status.

SensorView is installed on a single host workstation or server (provided by others) that resides on the same Ethernet LAN (or WAN) as one or more nLight ECLYPSE™ or nLight Gateway devices. SensorView can also be configured to communicate directly with a single group of devices. The system architecture is shown in Figure 01.

This document 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.

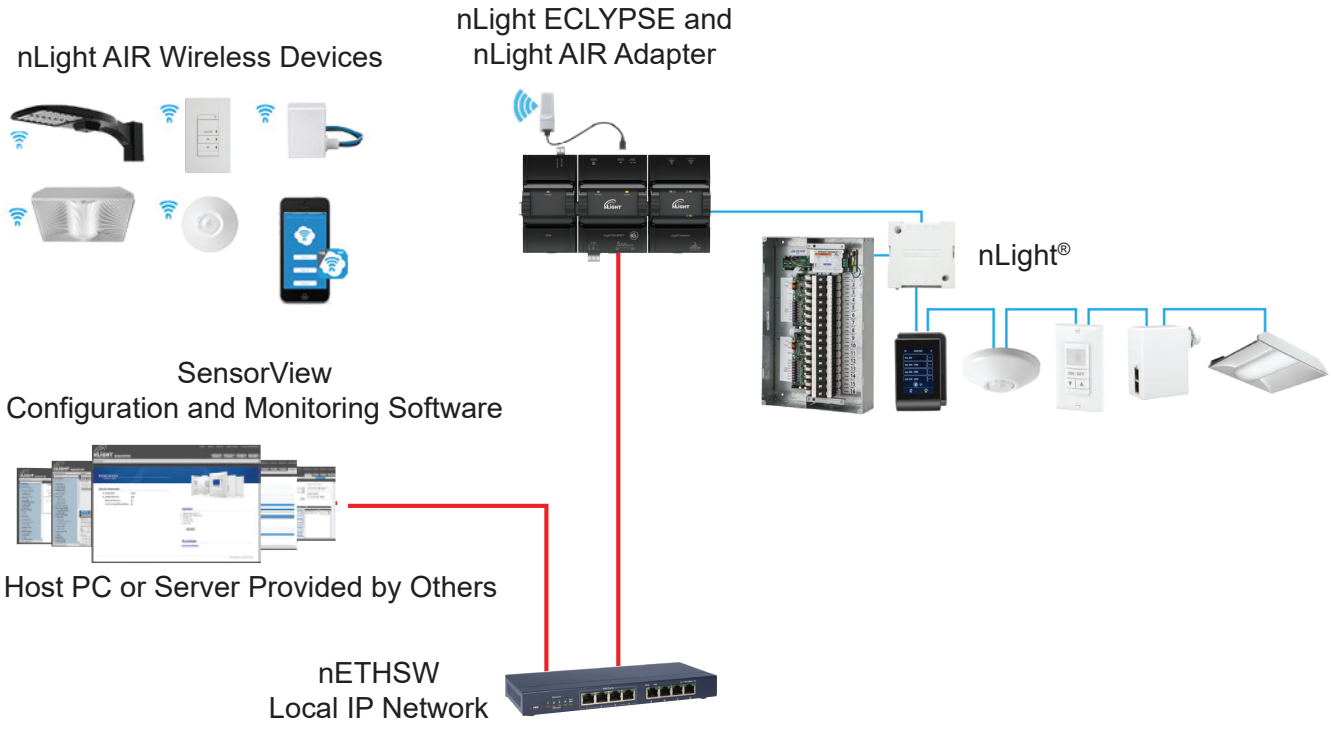


Figure 01 - System Architecture

SensorView Installation

To ensure proper intallation of the SensorView software, follow these steps:

1. **SensorView System Requirements:** Depending on the intended usage of SensorView, there are two sets of computer hardware/software requirements:

   - **Single-user / Commissioning Installation:** Recommend Windows 8.1 or Newer
   - **Multi-user Installation:** Recommend Windows Server 2012 or Newer
   - **Hardware Minimum Operating Specs:**
     * **Ram:** 8GB
     * **Hard Drive:** 20GB
     * **Browser:** Firefox, Chrome, IE 11+
   - **Version of Windows supported (both 32 and 64 bit versions supported):**
     * **Client Versions:** 8.1 or 10
     * **Server Versions:** 2012 (R2), 2016

2. **Pre-installation:** The following Windows software components are required prior to SensorView installation:

   - **.NET Framework:** Available for download (free) from Windows Updates web page
   - **IIS (Internet Information Services):** IIS 7.0 Windows

   NOTE

   If .NET/IIS are not installed prior to running the SensorView installer, user will be automatically prompted to install these items during SensorView installation.

3. **SensorView Installation:** The SensorView application installer is downloaded from the Acuity Brands website:

   - **http://www.acuitybrands.com/-/media/Software%20Downloads/nLight/SensorViewInstallerv612%20zip.zip?la=en**

   NOTE

   Internet access is required during installation to download latest available version of the SensorView software.

4. **Connection to Gateway:** The Gateway uses its port labeled **LAN** to communicate with the computer running the SensorView software.

   - Please reference the Gateway Setup section under the Admin section for details on methods to connect to a system Gateway.

If assistance is required, please contact our technical support team at 800-535-2465 or nLight-Support@AcuityBrands.com.

Login and User Management

Once installed, SensorView can be accessed several ways: from the Start menu, via a desktop shortcut, or by typing **http://<Host Computer Name>/SensorView** into a web browser. Users must enter a valid User Name and Password to login to the SensorView (Figure 02). The default User Name for the application is "**administrator**" with the Password "**admin**." After logging into the application using the default credentials, users can add new users or change the default user credentials through the **User** tab (Figure 03).

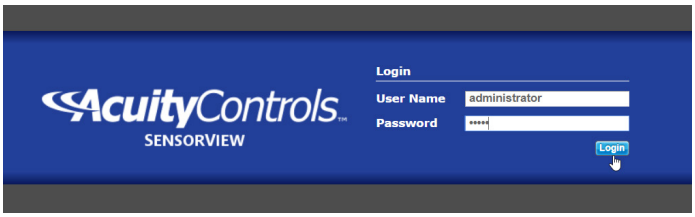


Figure 02: SensorView Login

Figure 03: Users Tab Location

SensorView supports three different User Types, as noted in the following table:

User Type	Description
Administrator	Administrator can access all the features in the application. The administrator user **only** features are listed below. • Add/Edit/Delete users. • Update the SensorView settings • Update the devices' Firmware. • View log details • View Reports • Configure and view the plugins • Export diagnostic archive
Basic	The Basic user privilege allows user to view and update all the device related settings and status except the features that can be only accessed by administrator.
Read-Only	The Read-Only user can only view the device settings and status.

Login and User Management - cont'd

Clicking on the **User** tab will bring you to the **User Accounts** screen. From here, you can follow these steps to add or edit users:

1. Click on the drop-down that says **administrator** and choose the **Add a user** option (Figure 04).

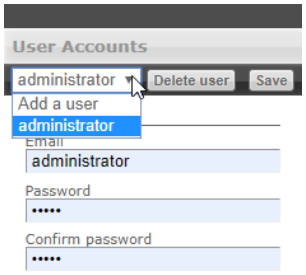


Figure 04: Add a User

2. Fill in the fields under the **User details** section with the relevant information (Figure 05).

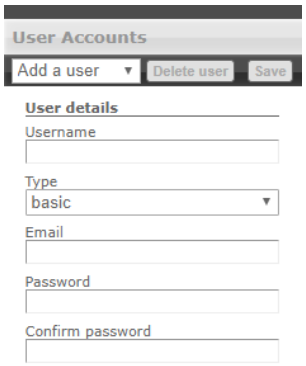


Figure 05: User Details

3. Choose the desired User **Type** from the drop down menu (Figure 06).

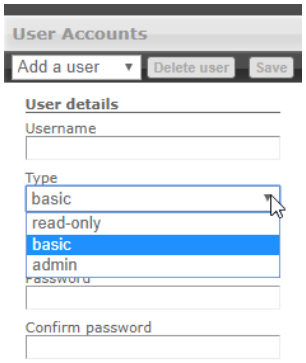


Figure 06: User Type

4. Select the devices from the device tree that a user should have visibility of. Devices must be selected for a user to be created.

5. Click the **Save** button to save the new user data (Figure 07).

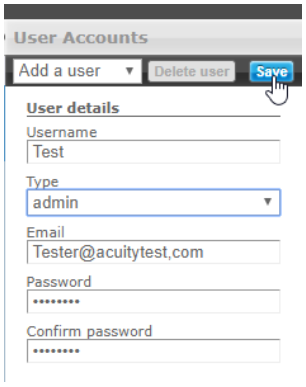


Figure 07: Save New User

Admin

The **Admin Dashboard** is accessed by pressing the **Admin** button on the top left of the SensorView window (Figure 08). This option allows the SensorView administrator the ability to update and configure the following settings, each of which will be explored further in this section:

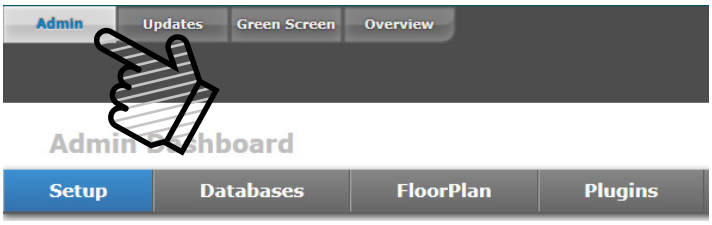


Figure 08: Accessing the Admin Dashboard

Setup (Figure 09) gives access to the basic settings of SensorView, including Registration (required to receive firmware updates), Location, Gateway Password, Gateways, Mail Server, and Custom Greeting.

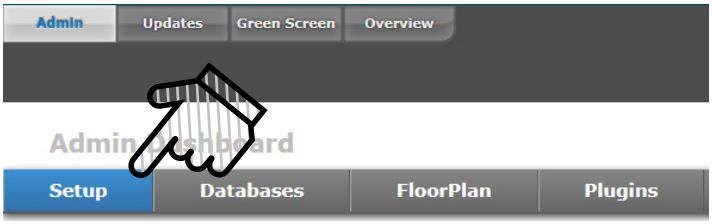


Figure 09: Admin Dashboard - Setup

Databases (Figure10) allows you to create and load full system backups, as well as the option to Import/Export the same.

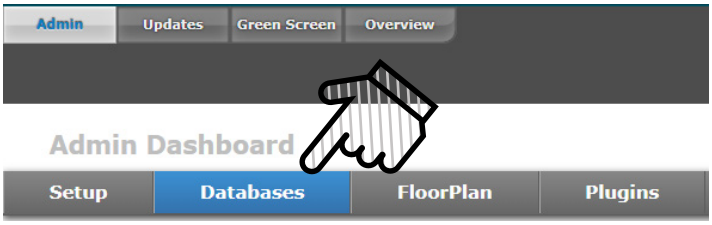


Figure 10: Admin Dashboard - Databases

FloorPlan (Figure 11) is for importing floor pan packages, and for exporting edited floor plans.

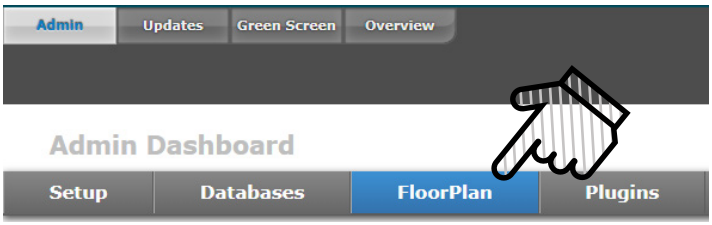


Figure 11: Admin Dashboard - Floorplan

The **Plugins** (Figure 12) option allows you to start services for the nLight GreenScreen Monitor, nLight Virtual Wallpod Server, and the nLight Plugin Host Service.

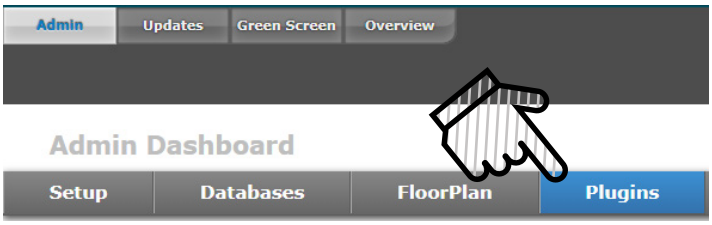


Figure 12: Admin Dashboard - Plugins

Located to the far right of the screen on the Admin Dashboard bar, **Reports** (Figure 13) allows you to generate various reports about SensorView and the devices on the connected network.

Figure 13: Admin Dashboard -Reports

Administrators can update the following settings in this section:

Registration

Registration is where you input your contact information and details about your site (Figure 14). SensorView must be registered with Acuity Brands to get software and firmware updates. The information captured in this section may appear on your diagnostic logs and reports that help the support team identify details about your site to help diagnose your system. An internet connection is required to save this setting.

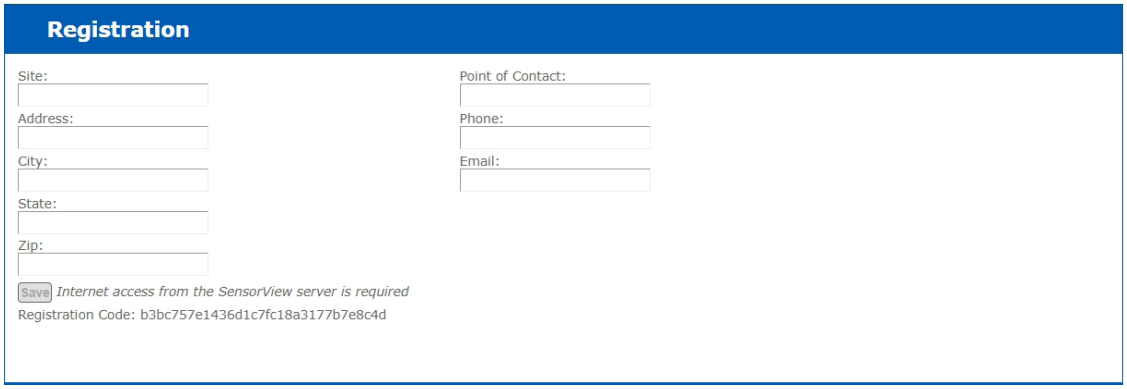


Figure 14: Setup - Registration

Location

The location of each gateway connected to SensorView can be updated in the **Location** section (Figure 15). Users can edit the location in one of two ways, as follows. If the **Edit Coordinates** box is checked, users may input the location via the latitude and longitude boxes on the right. If the **Edit Coordinates** box is unchecked, then the location may be edited through the dropdown menus. The **Save** button present in the bottom right of the section allows the user to save the updated location.

The location data helps SensorView maintain the date and time according to its time zone.

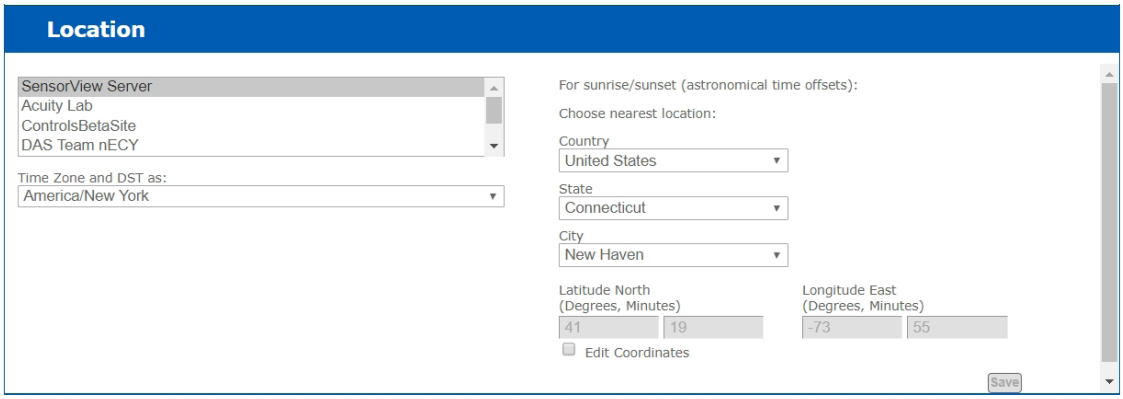


Figure 15: Setup - Location

Gateway Password

This feature enables authorized users to change the current system controller's password (Figure 16). It prevents unauthorized users from using a different SensorView instance to modify the system and restricts direct configuration access to system controllers. The **Save** button writes the updated password to the system controller. The **Gateway Password** will be blank for new installations and should be updated to match the SensorView Password assigned to all corresponding nLight ECLYPSE controllers. The Gateway Password can be updated on an nLight ECLYPSE controller by logging into the controller's web page (https://[ip address of controller]/login.html), accessing the nLight Explorer Tab, Selecting Settings, and Selecting the Reset button beside SensorView Password. Only alphanumeric characters are accepted.

Figure 16: Setup - Gateway Password

Gateways

All the gateways present in network where SensorView is connected will be automatically discovered and included in the Gateways section (Figure 17). Administrators can enter system controller IP addresses to discover the controllers. Once discovered, controllers will be reflected in the Devices section. Controllers can be excluded from the Devices section by unchecking the **Include** box of the respective controller. A controller can be deleted from SensorView by clicking on the **Delete** button.

Figure 17: Setup - Gateways

Mail Server

This section is used to update the Mail Server settings, which adjusts where notifications are sent (Figure 18).

Figure 18: Setup - Mail Server

Custom Greeting

This section is used to update the custom greeting, which appears at the login screen (Figure 19). The greetings will show on the Login screen, as either a header or footer greeting, or both (Figure 20).

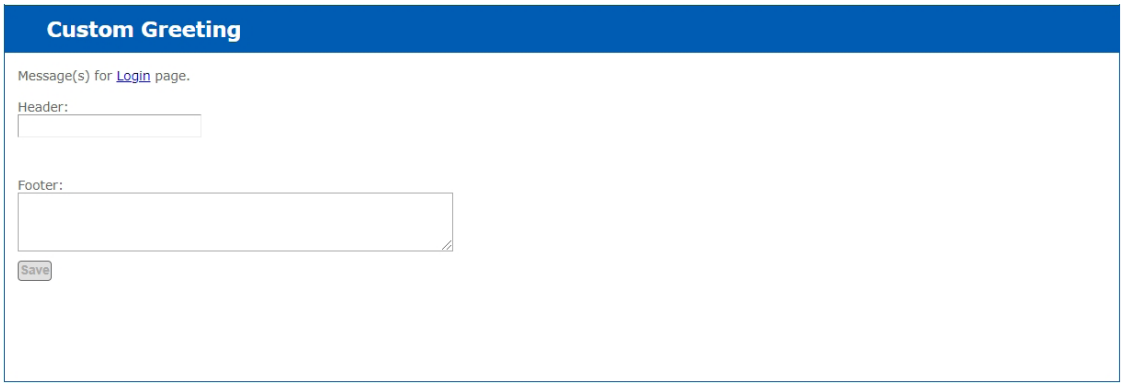


Figure 19: Setup - Custom Greeting

Figure 20: Setup - Greeting Locations

Admin Dashboard - Databases

The device network information and all other related details will be stored in the **Databases** section. The database will be backed up automatically and saved daily. The backed-up database's name contains the date and time so that the backup can be easily distinguished. Users can perform the following options on the database, as called out in Figure 21.

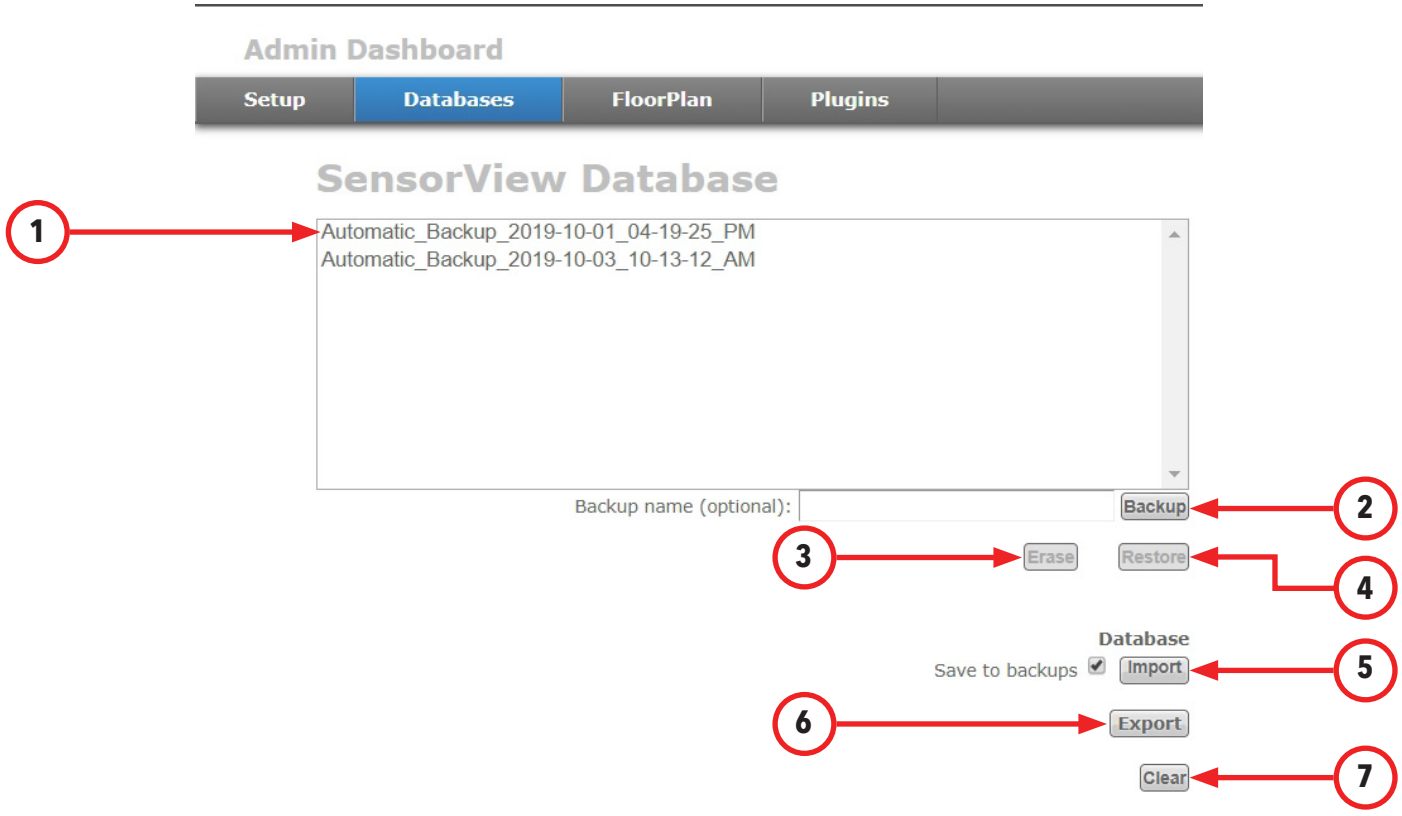


Figure 21: Databases Section

1. **Backup List:** All the backed-up databases will be displayed on this list. By selecting a database from the list user can perform Backup, Erase, Restore or Export the database as mentioned in below sections.

2. **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 back up a database from the list, select the desired database, enter a name in the **Backup name (optional)** field, and click **Backup**.

3. **Erase:** A backed-up database from the list can be deleted by using **Erase**. Select the database and click on **Erase** button to delete it.

4. **Restore:** A backed-up database can be restored to SensorView using this option. SensorView will load all data from the selected database and user can perform the changes on it.

5. **Import:** SensorView allows the import of SensorView databases. The SensorView database can be identified by the extension ***. svdb**. The database can be imported as well as keep a copy of it in the backup. The imported data will be displayed to the user and user can analyze the data. Importing a database will overwrite any previous databases information, including the login credentials for non-administrator users. Administrator user login credentials (administrator/SomePassword) will remain the same.

6. **Export:** The backed-up databases can be exported and shared with other users. The exported file will be with the extension of ***. svdb**. The file will be present in the download location of the browser.

7. **Clear:** The data of the current SensorView database can be cleared using this option. The data will be cleared and database will be filled with newer data from the networked devices.

Admin Dashboard - FloorPlan

The SensorView nFloorPlan tool provides a simple and intuitive way to navigate and monitor an nLight Wired and/or nLight AIR lighting control system instead of traditional tree view display. To display the floor plan, the administrators must load the floor map packages. This section allows user to import or export the map packages.

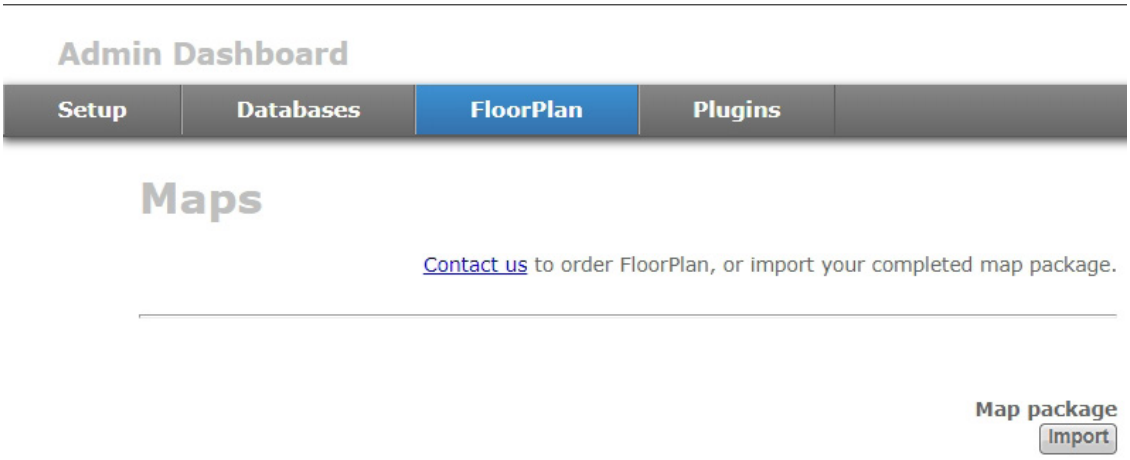


Figure 22: FloorPlan

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 clicking the **Import** button (Figure 22), then browsing to and selecting the file.

Plugins

Under the Plugins tab is the **Services** section, where each plugin is listed along with its current status, either Running or Stopped. Plugins can be stopped or started via the buttons to the right of the Status (Figure 23).

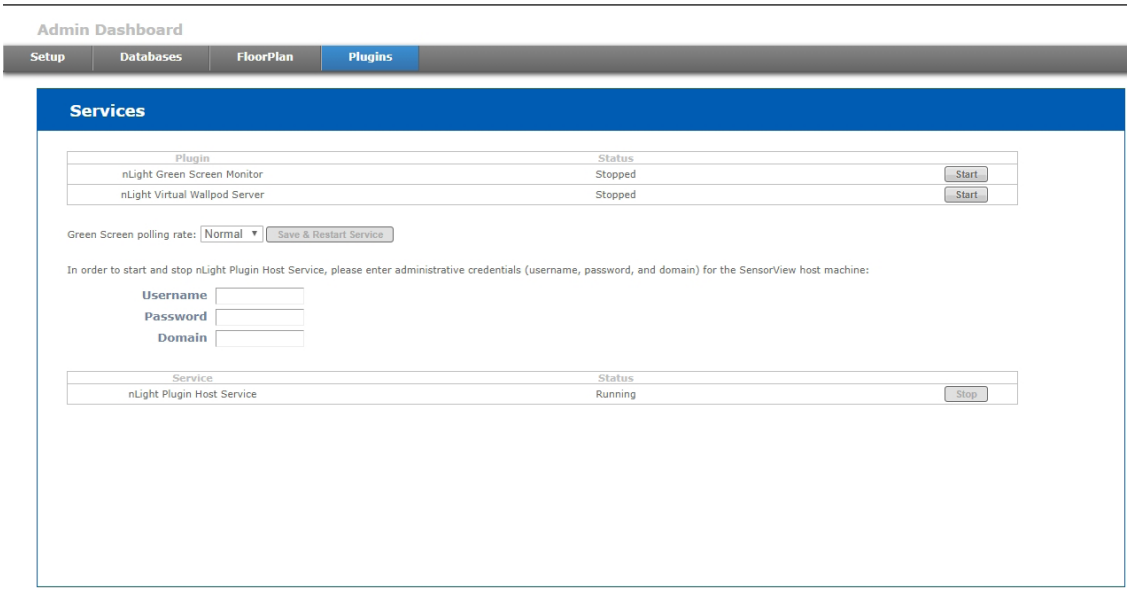


Figure 23: Plugins

GreenScreen polling rate controls the rate at which this plugin is being polled. Increasing the rate may allow for GreenScreen reporting points to increase, but will result in additional network traffic. To change the polling rate, select a new rate, and click Save & Restart Service.

The **nLight Plugin Host Service** status (either running or stopped) is indicated in the last table of the section. 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.

Admin Dashboard - Reports

Located to the far right of the Admin Dashboard bar (Figure24), **Reports** is linked directly to the current active SensorView database, authorized administrators can view detailed reports on the following:

Figure 24: Reports

- **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, Group, and parent Bridge.
- **Profile, Scene, & Presets Report:** Creates a printable report describing the configuration of all profiles, scenes, and presets currently in the system.
- **Device Settings Report:** Creates a printable report describing the default settings for all nLight devices in the system.
- **Global/Local Channels 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 gateways in the system. This is generally used for diagnostic purposes only

Updates

This feature enables user to update SensorView and network devices' firmware to the most recent versions. When this screen is accessed, SensorView's firmware cache will be updated for all available devices, and the information will be displayed as shown below (Figure 25).

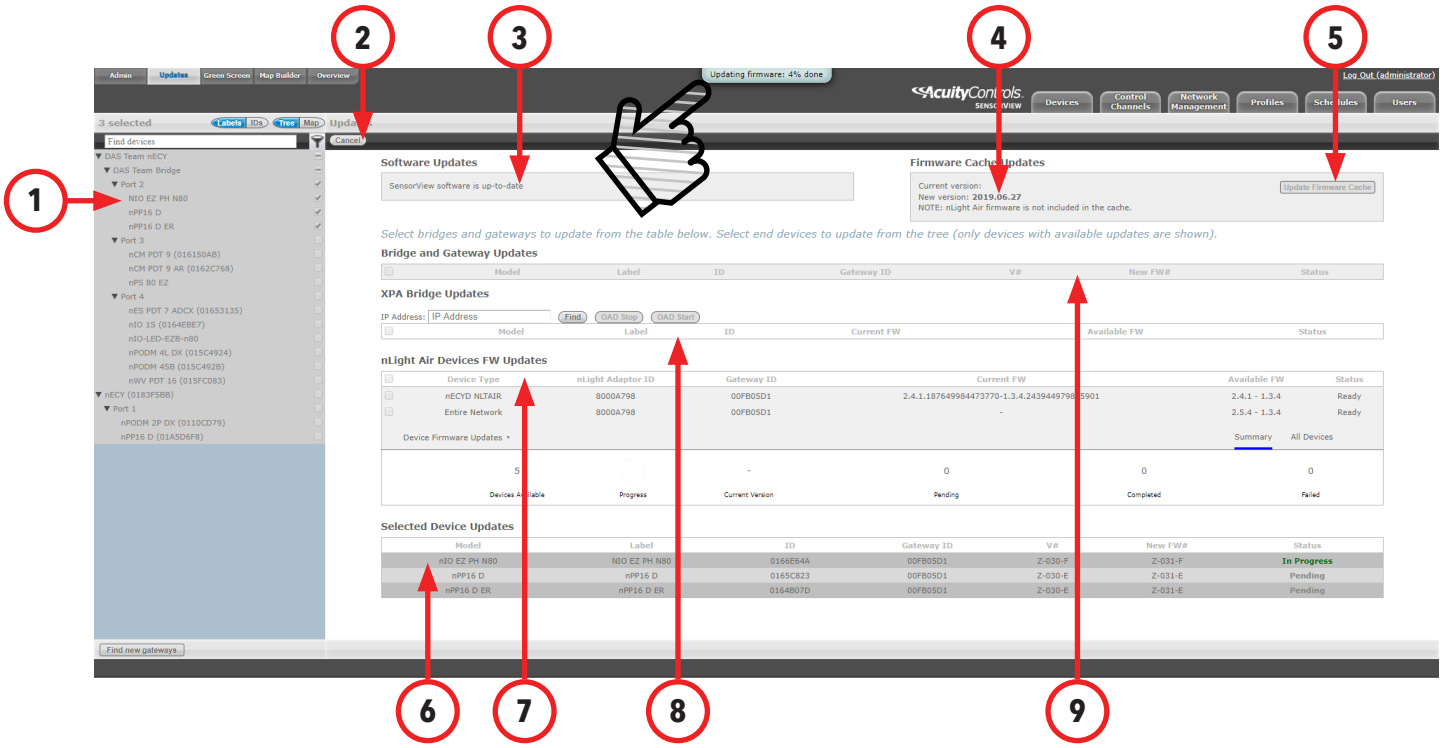


Figure 25: Updates

1. **Device Tree:** Devices with available updates will be displayed. As devices are selected, they will appear in the section indicated by callout 6. The devices will be updated to latest firmware upon click on **Update Firmware** button click after selecting it. The Gateway, Bridge and XPA device will be displayed in the grid directly.

2. **Update Firmware Button:** Clicking the **Update Firmware** button writes the latest firmware to all selected devices. As the devices update, the status of the update will be captured through a bubble at the top of the screen as pointed out in Figure 25. The status of the write will be displayed on the **Status** column of the grid. The grid also contains the details of the device with current firmware version.

3. **Software Updates:** If a newer version of SensorView is available, it will be displayed in this section. Users can run the installer and follow the installation setups described in the Installation section to continue with updates.

4. **Channel Information:** If updates are available for SensorView, this section will identify the channel from which the updates can be downloaded.

5. **Update Firmware Cache:** This feature enables user to download and update the local firmware cache of the devices.

6. **Selected Device Updates:** When devices are selected for a firmware update, they will appear in this section. Old and new firmware, update status, and completion status will be displayed in this section.

7. **nLight AIR Devices FW Updates:** If nLight AIR devices are present, a screen for updating each nLight AIR Adapter (nECYD NLTAIR) will be available along with options to update the entire nLight AIR network.

8. **XPA Bridge Updates:** XPoint Wireless devices will appear in this section. Devices are labeled using their IP address. Over the Air Discovery (OAD) options are available for any selected XPoint Wireless bridges.

9. **Bridge and Gateway Updates:** Bridge and system controller firmware can be updated by selecting devices from this section.

Figure 26: GreenScreen

This section will detail how to setup SensorView to use the GreenScreen plug-in (Figure 26). 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.
- GreenScreen is compatible with PostgreSQL versions 9.0 or higher.

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. The most recent versions can be downloaded at: http://www.enterprisedb.com/products/pgdownload.do#windows for the relevant windows version, x86-64 (64 bit) or x86-32 (32-bit).

Super-User Creation Screen

The screen below (Figure 27) configures the default super-user account for PostgreSQL, **take note of these credentials** as those will be the default login account and password for all access to the Postgre SQL database.

NOTE

Passwords may only use alpha-numeric characters (numbers, lowercase and uppercase letters) with no special characters.

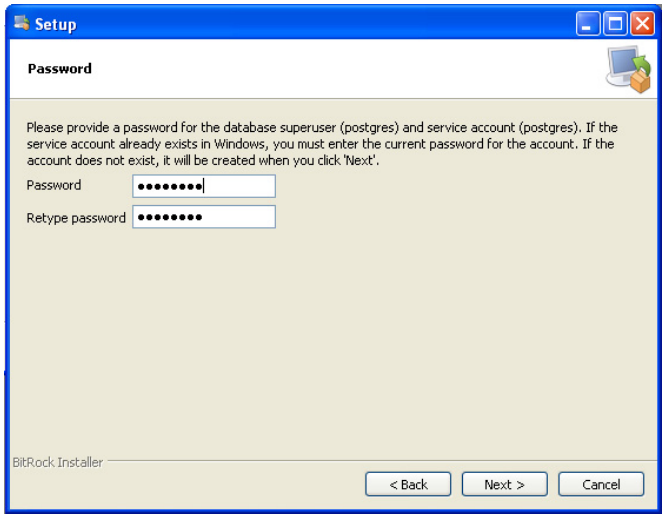


Figure 27: GreenScreen Password

Port Configuration Screen

The screen below (Figure 28) allows for configuration of the port that PostgreSQL will use for connections. Use whatever value is required by the system administrator.

NOTE

SensorView and GreenScreen can be configured to use any port value.

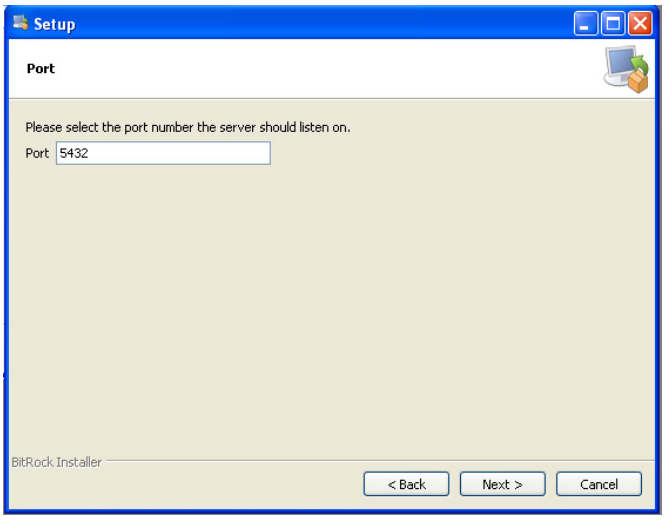


Figure 28: GreenScreen Port Configuration

Advanced Options

The screen below (Figure 29) 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.

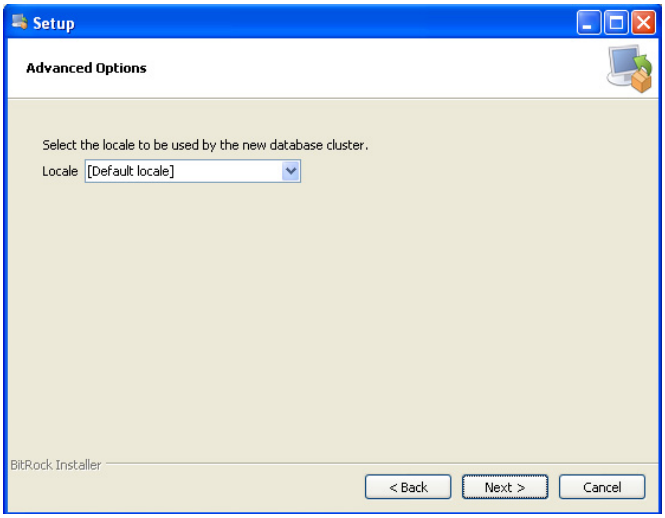


Figure 29: GreenScreen Advanced Options

GreenScreen - Configuring PostgreSQL to Allow 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 additional documentation on how to configure **pg_hba.conf**, as well as any questions, refer to:

Version of PostgreSQL	URL
9.0	http://www.postgresql.org/docs/9.0/static/auth-pg-hba-conf.html

For all database versions, adding the following line to the bottom of the file to allow ALL remote connections to the database:

host all 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.

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 -> System and Security -> Administrative Tools -> Services**. In the services window select the following service:

Version of PostgreSQL	Service Name
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 (Figure 30).

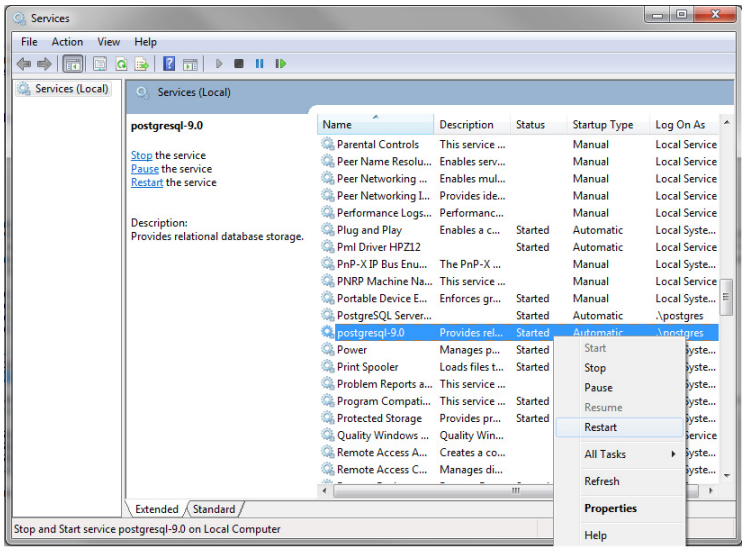


Figure 30: GreenScreen Restart Services

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.

GreenScreen - 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.

Installing a PostgreSQL Driver

For SensorView to connect and control the PostgreSQL database a driver must be installed on the machine running SensorView. Install the following driver:

https://ftp.postgresql.org/pub/odbc/versions/msi/psqlodbc_09_03_0400.zip

After downloading, open the zip file and run psqlodbc.msi and install the driver.

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 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 7 32bit/Windows 10 32bit 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 section. Select **Finish** and a form will appear with additional fields to fill out (Figure 31). 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 and password for the database user (refer to **Super User Creation**)
Password	
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

Pressing the Test button will fail with "database not found" until Configuring the Administrator Email has been completed.

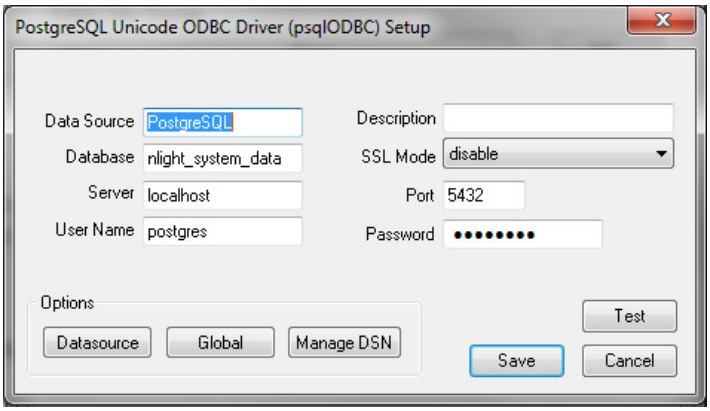


Figure 31: GreenScreen ODBC Driver Setup

GreenScreen - 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 **Plugins**.

Configure Administrator Email (Optional)

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 if the host Windows service fails.

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 (Figure 32). 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.

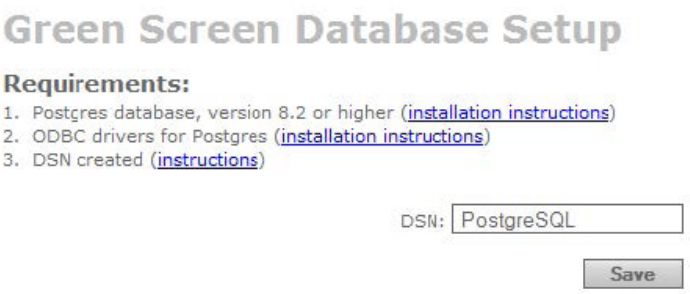


Figure 32: GreenScreen ODBC Database Setup

Starting GreenScreen

In order to start GreenScreen, the plug-ins component must have previously been installed (**Setting Up GreenScreen**); if this has not been done then there will be no **Plugins** tab. Proceed to the Admin screen in SensorView and select **Plugins** (Figure 33). 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 Plugin Host Service**. Once this is running GreenScreen can be started and stopped in the top window.

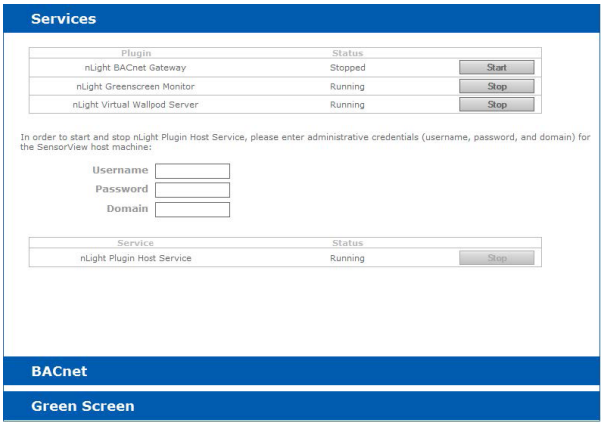


Figure 33: GreenScreen Start Plugins

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 (Figure 34).

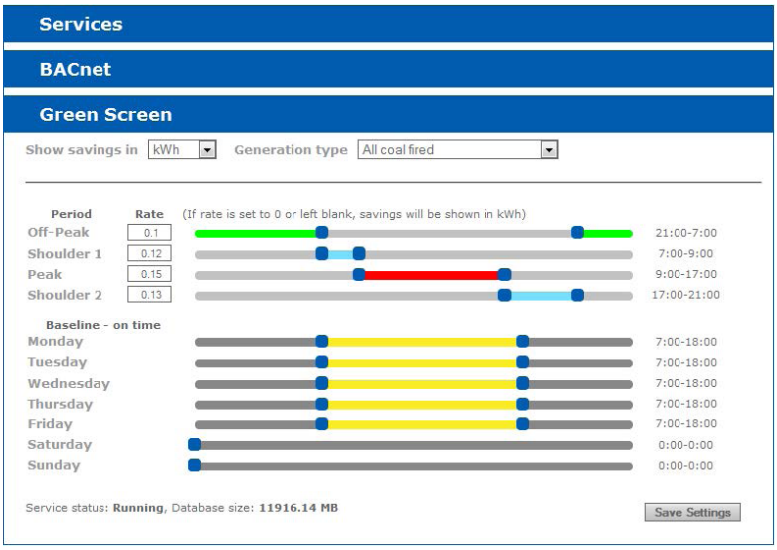


Figure 34: GreenScreen Configuration

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.

Overview

The **Overview** screen will be the default selection after the successful login of the user (Figure 35). The Overview screen will show the summary of the system.

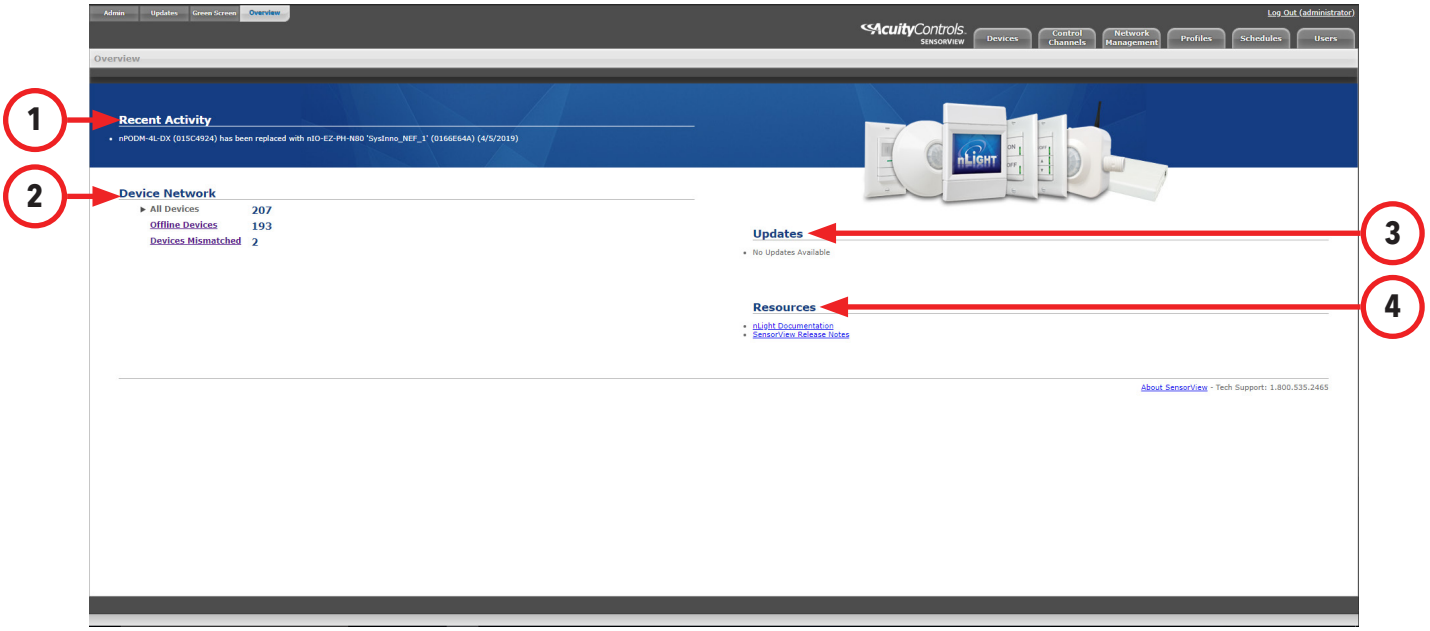


Figure 35: Overview Screen

The summary includes the details noted below:

1. **Recent Activity:** Recent activities that have occurred in the networked devices, such as Firmware updates, will be displayed in this section. The information will be very high level.

2. **Device Network:** The available gateways and associated device's count will be displayed in this section, including **All Devices**, **Offline Devices**, and **Devices Mismatched** (ones whose settings differ from SensorView's records).

3. **Updates:** All available updates for connected devices will appear here. Users can navigate to the update screen from this section.

4. **Resources:** Documentation for the current SensorView version and for the devices on the nLight network can be accessed here.

Devices

On the SensorView **Devices** 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 groups, each of which contain sensors, switches, relays, dimmers, or other devices.

Device Tree Overview

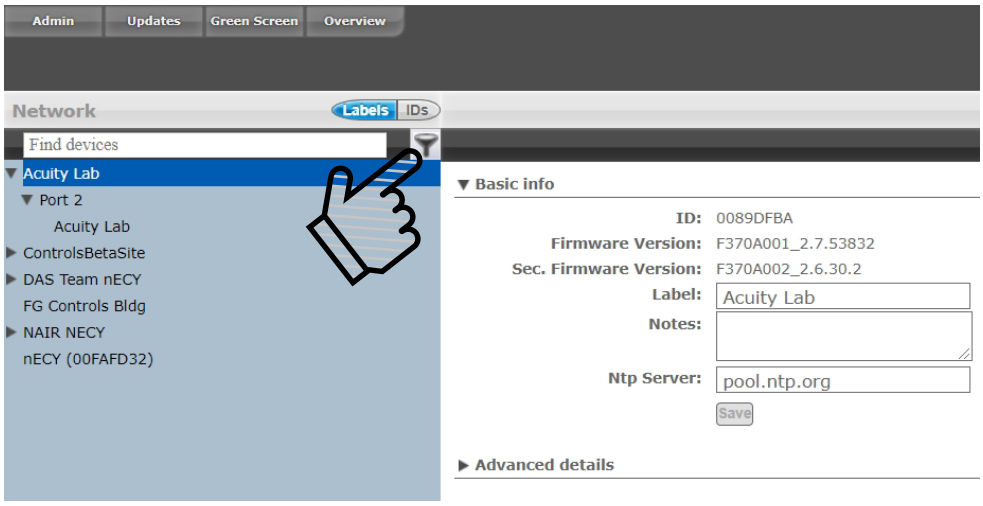


Figure 36: Device Tree

The **Device Tree Menu**, available from the filter icon to the right of the search textbox, contains selection features that aid in the location/selection of devices (Figure 36). Three primary types of search features exist: **Features**, **Profiles**, and **Device States** (Figure 37).

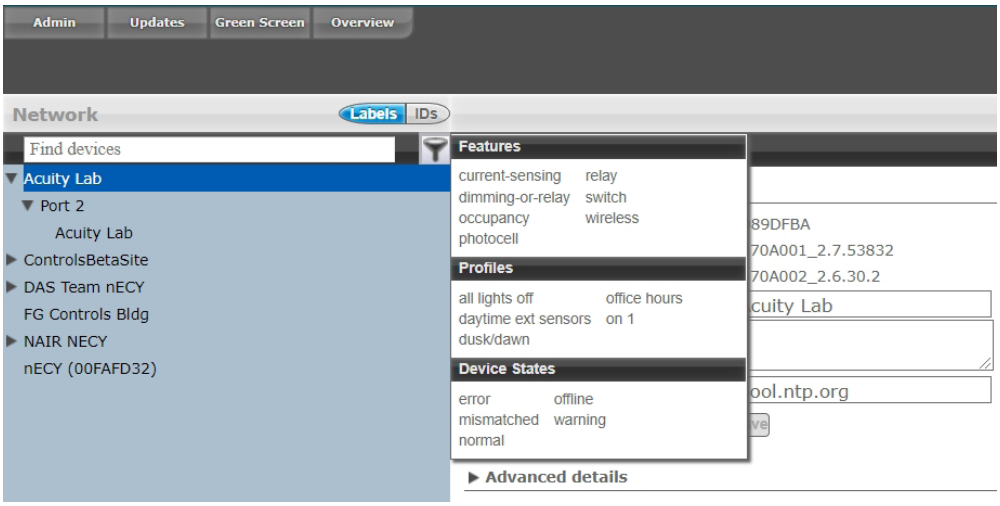


Figure 37: Device Tree Menu

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.

Find New Gateways (Figure 38) searches the local subnet for gateways that may not be reflected in the device tree.

Figure 38: Find New Gateways

Devices - Tree Layout

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

Figure 39: Tree Layout 01

Figure 40: Tree Layout 02

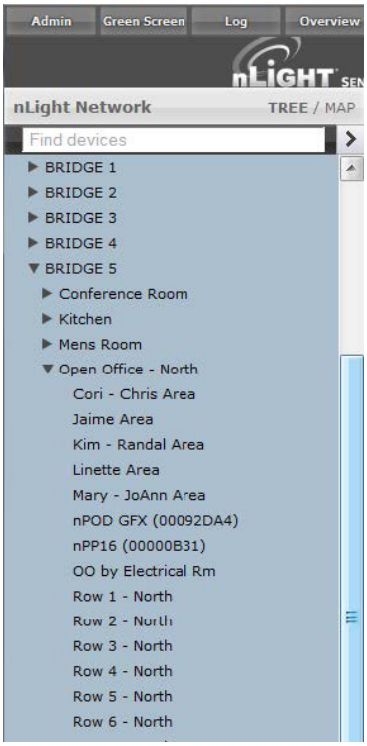


Figure 41: Tree Layout 03

- Bridges are not nested within their parents (Figure 39).
- Groups off a bridge are displayed in ascending alphabetical order (Figure 40).
- Devices in a group are displayed in alphabetical order, not wiring order (Figure 41).

Search/Filter/Locate Device

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** (Figure 42). 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 **Prebuilt Filters.**

1. **Device Search:** Allows a user to immediately begin typing to search for the device (over device ID, model, or custom label).

2. **Prebuilt Filters:** Allows for a user to search for a device based on:
   - **Features:** Current-sensing, dimming-or-relay, occupancy, photocell, relay, switch, wireless
   - **Profiles:** Select by Profile name
   - **Device States:** Error, normal, offline, warning

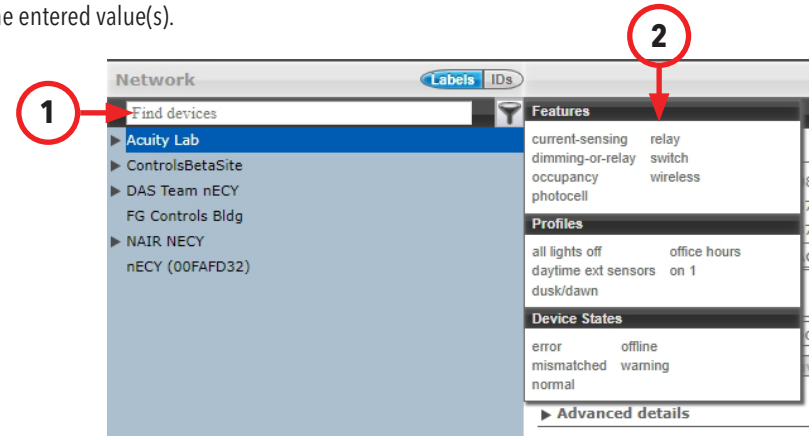


Figure 42: Search Devices

Note that any device matched and displayed will automatically cause the parent group, 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.

Devices - View Device Properties and 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**. Figure 43 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 **Group** called "Port 6", which has been selected from the device tree menu.

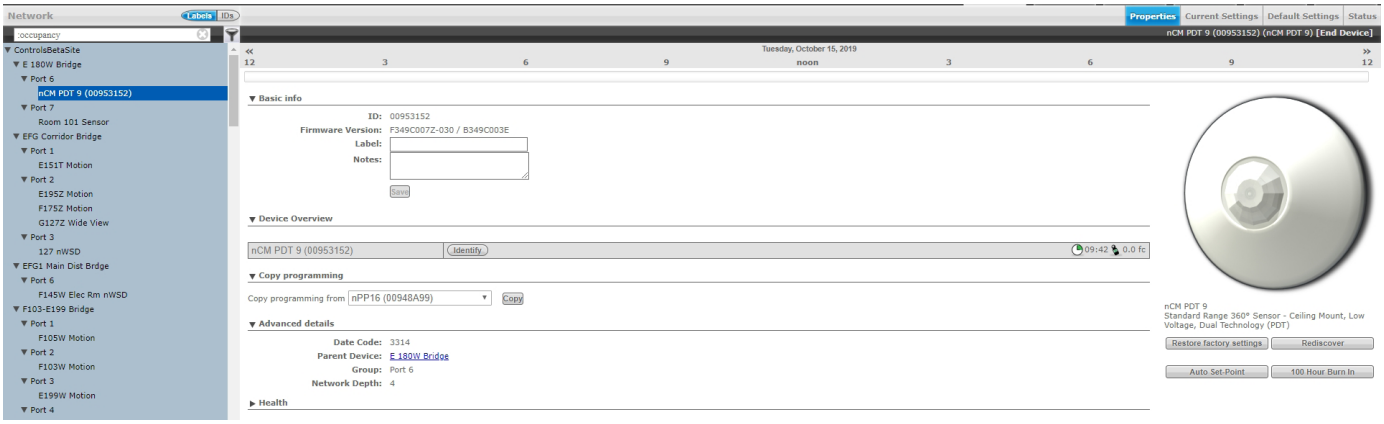


Figure 43: Device Properties

There are 5 possible states that an nLight device can be in. These different states generally indicate some sort of operational problem with a device.

- **Offline:** The device is no longer online, check that the device is properly connected
- **Bootstrap:** The device failed a firmware update and is in bootloader mode. 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, go to the device and select **Rediscover** or use **Network Management -> 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 device settings do not match what is expected. Synchronize the device (either using SensorView or the device's settings) to resolve. Choosing to synchronize from a device will update SensorView's record of device settings. Choosing to update from SensorView will update a device's settings to match SensorView's record.

NOTE

Device State is not the same as Device Status. Individual device types can have various status conditions, depending on their functions.

Under the product image of your selected device (Figure 44) are a number of options. Note that some options pertain only to certain types of devices and do not appear otherwise::

Restore Factory Settings

- Resets the device to its default factory settings.

Rediscover

- Reprompt Sensorview to poll the selected device.

100 Hour Burn In

- Overrides relay on and/or dimming output to full bright (typically used for lamp seasoning)

Download Screen Saver

- Download the current background screen image from the selected device.

Upload Screen Saver

- Upload a screen image to the selected device. Supported file formats: JPG, PNG, GIF, BMP, TIF Optimal resolution: 320x240 16bit color

Figure 44: Device Options

Devices - View Device Properties - cont'd

Other information found on the **Properties** tab includes the following. 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 firmware update.
- **Label:** A label can be customized to describe and represent the device. Labels are automatically generated for nLight AIR devices using the Clairity PRO(tm) mobile application. nLight Wired devices will have a blank label field until updated by the user. Information in this field is utilized for BACnet labeling. I.e., an output device will generate a BACnet object with the formatting [Label]_[BACnet Property Type]_[Device ID].
- **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 group; 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.

Device Overview

- A brief overview of the selected device, its unique ID, and its general status.
- **Identify:** Causes the device LED to flash, helping to identify the physical device in the space.

Copy Programming

- Copy programming to the selected device from another existing device.

Advanced Details

- **Date Code:** Indicates the internal lot number for the device.
- **Parent Device:** The name of the device above the selected group in the network hierarchy.
- **Group:** The name of the group in which the selected device resides.
- **Network Depth:** The number of steps below a gateway in the network hierarchy.

Health

- This section provides diagnostics read-outs for nLight Engineers and Field Techs.

Current Settings

The **Current Settings** option (Figure 45) allows the administrators to see the current settings for the selected device, and make changes there via drop down menus. Once changes are made, use the **Apply Settings** button to push the changes to the device, or **Revert to Defaults** to set the device back to the defaults set in the **Default Settings** option.

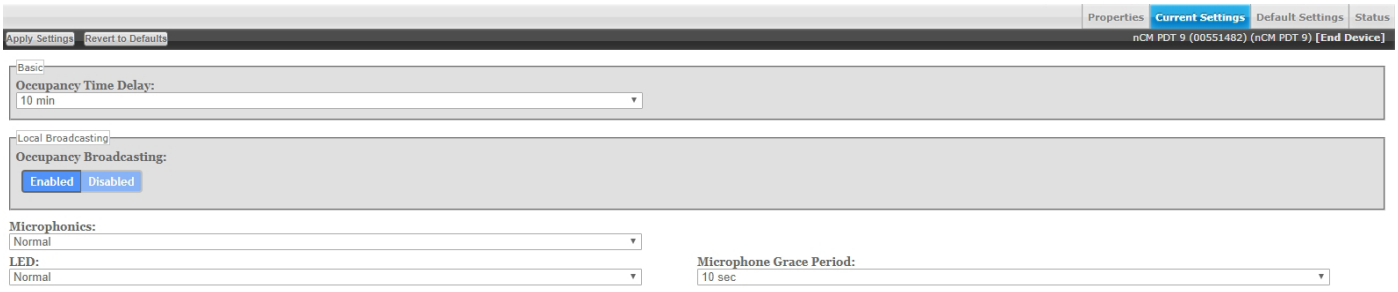


Figure 45: Device Current Settings

Devices - Default Settings

The **Default Settings** option (Figure 46) allows the administrators to change and apply the default settings for a device. Once changes are made, use the **Save Defaults** button to save the changes to the "Default" settings collection, or use the **Save Defaults and Apply Now** button to save the settings, update settings that appear under Current Settings, and affect active settings on the device.

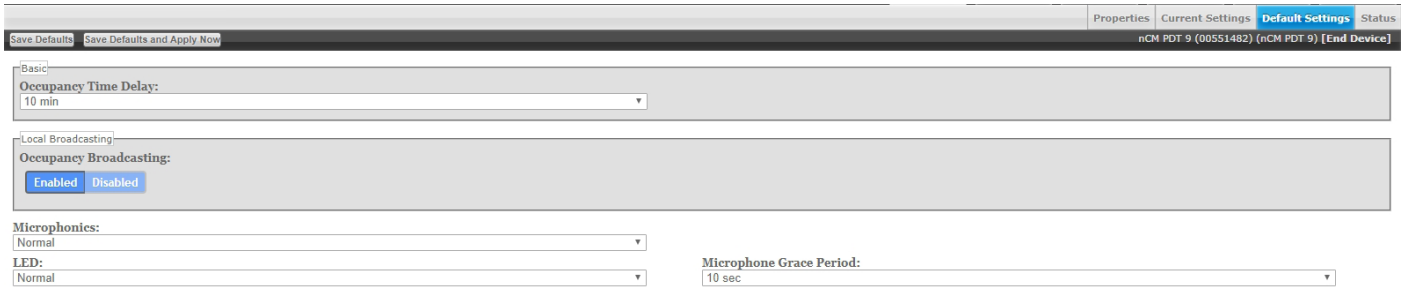


Figure 46: Device Default Settings

For detailed information on what settings affect, hover over a setting, and a description of that setting will appear in the lower left corner of the screen.

Wallpods

The **Wallpods** page is where users adjust what switch options appear on an nPOD GFX and nPOD TOUCH (Figure 47). Users can define how a switch will appear (as dimming capable or only on/off), and they can optional choose for the switch to appear under the Shades/Blind screen (applies to an nPOD TOUCH).

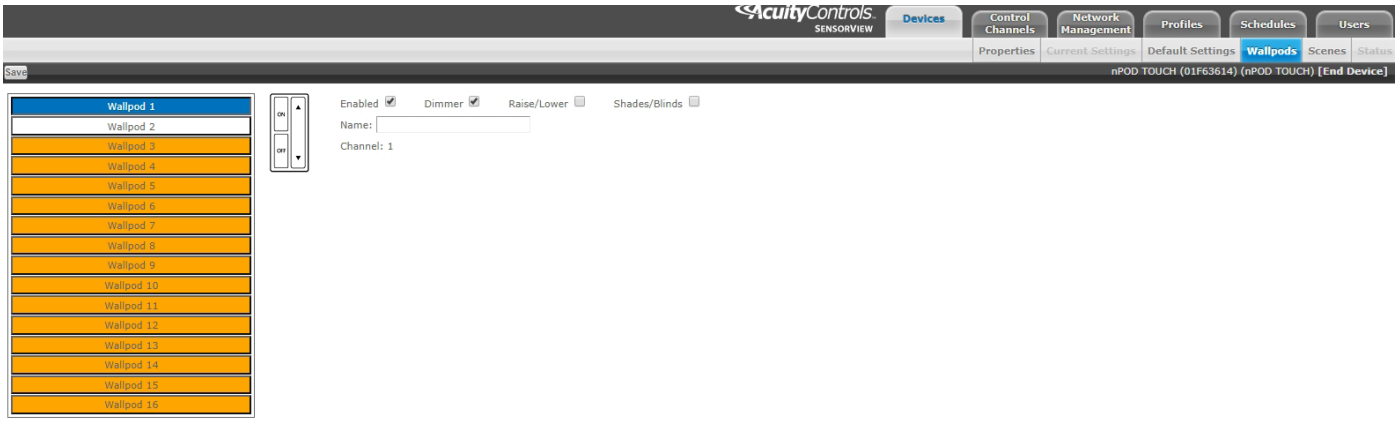


Figure 47:Wallpods

Scenes

The **Scenes** page is where users adjust what scene options affect an nPOD GFX or nPOD TOUCH (Figure 48).

Figure 48: Events

Devices - Status

The **Status** page (Figure 49) 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. 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.**

Figure 49: Device Status

Events

When selecting a system controller (nLight ECLYPSE or Gateway), the **Events** button will be visible (Figure 50). Selecting the Events button will display all gateway captured records over a user-selected time period (24 hours, 7 days, 30 days, or all records). The resulting list of events can be sorted by errors, warnings, or "other." Lastly, the cause for the event can be filtered as well.

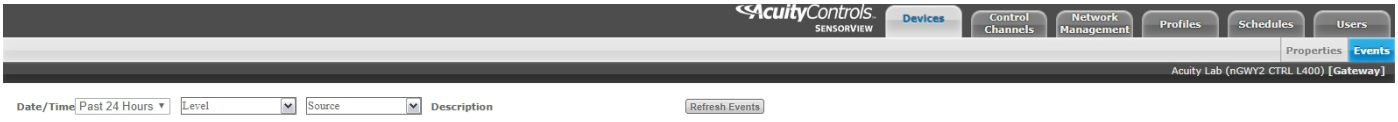


Figure 50: Events

AIR Site Survey

The **AIR Site Survey** screen (Figure 51) is visible only by selecting an nLight AIR Adapter (**nECYD NLTAIR G2**). This screen is used to view if a device is serving as a Repeater, device Daughter Count, and device Hop Layer.

Repeater status will reflect a "Yes" or "No" depending on if the device is presently serving as a repeater. **Daughter Count** indicates the number of devices that connect downstream of the device, bridged to the nECY and nECYD using Autonomous Bridging Technology. **Hop Layer** indicates what layer of the wireless network a device is on. A device within the initial broadcast range of an nECYD will be on hop layer 1, whereas if the device must connect to the nECYD through a single repeater-capable device, the device will appear on hop layer 2 or greater. A device on the third hop layer would only be able to connect to an nECY and nECYD through repeated messages by two devices in series.

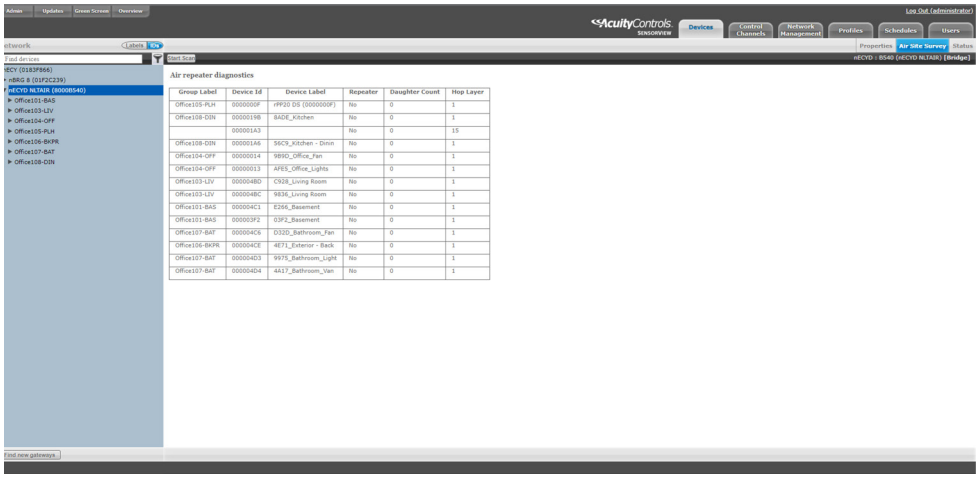


Figure 51: AIR Site Survey

Preset Scenes

Preset scenes, both global and local, are used to set output devices to a static light level when triggered. Most scene-capable devices are able to trigger a preset scene. When triggered, a preset scene is sent to tracking devices as a broadcast, which results in very fast response by end devices.

A local preset scene that is triggered by an nLight Wired device is used to adjust the light level of all or some directly connected output devices. Devices must be on the same daisy-chain or connected to the same nBRG 8 port to be affected by a preset scene local that is triggered by a Wired device.

A local preset scene that is triggered by an nLight AIR device is used to adjust the light level of all AIR devices in the same group. Devices must be in the same group to be affected by a local preset scene that is triggered by an AIR device.

A global preset scene that is triggered by an nLight Wired device is used to adjust the light level of output devices on the same nBRG 8 port as the broadcasting device or on a separate nBRG 8 port. Broadcasting and tracking devices must be configured under the same global channel prior to a global preset scene being available.

Global preset scenes for AIR devices are not supported at this time.

Control Channels

nLight devices exchange control information via the use of Local and Global channels, accessed via the **Control Channels** tab (Figure 52). Communication performed within a group (single nBRG port) is dictated via **Local Channels**; while **Global Channels** allow a device to receive input from any other device on the 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 Group and allow for switches to control individual fixtures or switch legs within a Group, rather than all of them. Global Channels are more commonly used to provide control over multiple spaces via a single input device.

Channels, both Global and Local, can be used to fine tune the control that one devices has over others, for Occupancy, Switching, and Daylighting.

Figure 52: Control Channels

Local Channels

The **Local Channels** option (Figure 53) allows a user to specify the channeling for all devices in the selected group. 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 left indicates broadcasting devices assigned to channels, and the column on the right indicates teacking devices assigned to channels.

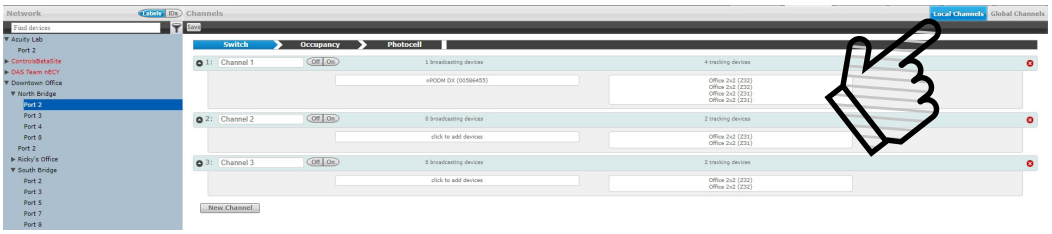


Figure 53: Control Channels - Local Channels

To configure a local channel (Figure 54):

1. Select a group from the **Device Tree**.
2. Add channels via the **New Channel** button.
3. Turn existing channels **Off** or **On**.
4. Add devices to the broadcasting devices.
5. Add devices to the tracking.
6. Once a field is selected, the device tree will indicate a list of devices that could be added to that field, via checkbox.
7. When all changes have been made, click **Save**.

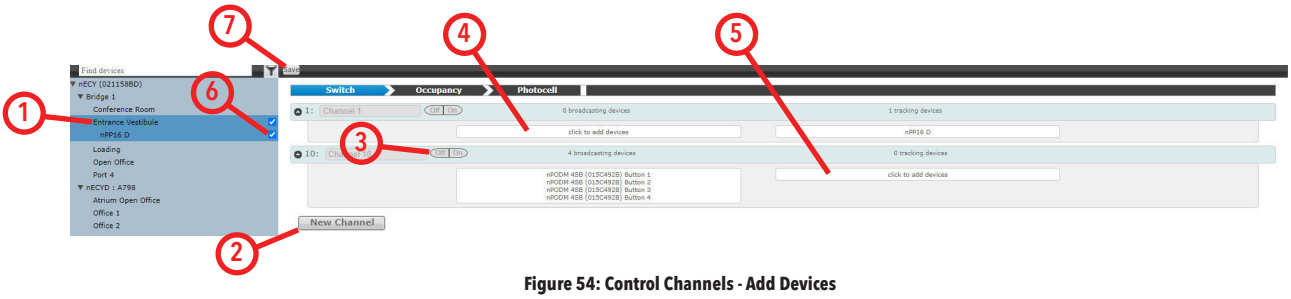


Figure 54: Control Channels - Add Devices

Control Channels - Global Channels

With traditional wired nLight systems, devices within a group communicate occupancy, photocell and switch events over local channels.
With **Global Channels**, communication of this information is possible between spaces as well. This provides enhanced design flexibility for applications requiring master control.

General Information:

- Switch, occupancy, and photocell (inhibit and automatic dimming) global channels are available for spaces connected to a single nLight ECLYPSE.
- Switch, occupancy, and inhibit photocell global channels are available between nLight ECLYPSE controllers.
- Automatic dimming via photocell for daylight harvesting is not available for devices connected to separate nLight ECLYPSE controllers. If daylight harvesting is required, both the broadcasting photocell and receiving output devices must be connected to the same nLight ECLYPSE.
- Global channels can only be configured through SensorView and cannot be configured using an nCOMKIT nor nConfig.
- Communication between Wired and AIR devices is available using global channels.
- A maximum of 128 global channels are available per nLight ECLYPSE. Global channels that span multiple ECLYPSE controllers will consume one channel on each nLight ECLYPSE whose device(s) are broadcasting or tracking on the channel.

To configure a global channel (Figure 55):

1. Under the Channels tab, select the **Global Channels** option. Any Global Channels that have been previously assigned will be displayed.
2. Select Switch, Occupancy, or Photocell to display all global channels in the respective category.
3. New channels can be added by clicking the **New Channel** button while viewing a relevant category.
4. Add devices to either the broadcasting or tracking fields by selecting the tracker or broadcaster box and selecting devices respectively from the device tree. The device tree will filter to show devices that can be added to the box selected. If the device you want to add to a box is not shown, verify you have selected the appropriate box and the appropriate device category.
5. Once a field is selected, the device tree will indicate a list of devices that could be added to that field, via checkbox. Devices can be added to more than one channel if desired.
6. To delete a channel, click the red circled X at the far right of the channel.
7. When all changes have been made, click **Save**.
8. Once saved, channels can be tested by clicking the **Off** and **On** buttons.

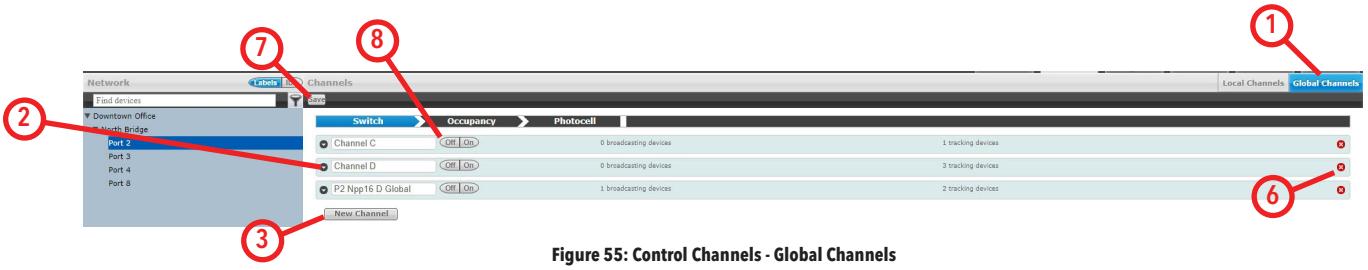


Figure 55: Control Channels - Global Channels

Network Management

The **Network Management** tab is where default settings can be modified for many devices at once.

Settings

From the **Settings** option (Figure 56), start by selecting devices from the **Device Tree**.

Figure 56: Network Management - Settings

Users may select multiple devices at once. When operating in this tab, all line items displayed in the tree will be given a checkbox which will allow for selection (Figure 57). 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. Selecting a device within a group only selects/deselects that device. Selecting a group, bridge, or gateway selects/deselects children; this allows for a user to quickly select all devices in a group, bridge, or gateway (Figure 58). The user may also deselect individual devices from a group, bridge, or gateway (Figure 59).

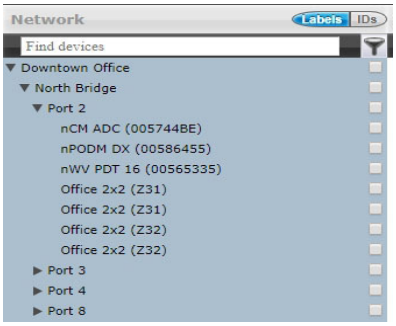


Figure 57: Network Management - MultiSelect

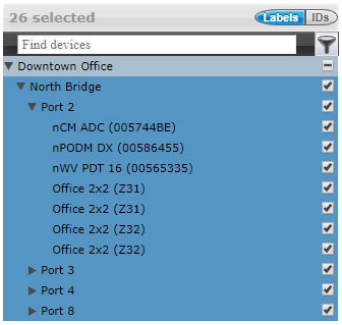


Figure 58: Network Management - Select All Devices

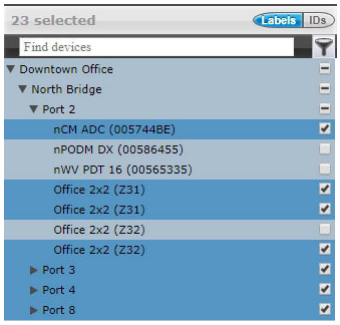


Figure 59: Network Management - Deselect Devices

With a device or devices selected, the user may now click the drop-down list next 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) for those settings before choosing **Save** (see below). Settings on multiple devices can be adjusted from this screen by selecting devices from the tree, and when updates are made, only the devices selected are affected. Settings that can be adjusted include settings such as Basic (PIR sensitivity, override, occupancy time delay), Dimming (follow photocell mode, occupied bright level, unoccupied dim level), Broadcasting, Tracking, ADR, and Global Broadcasting and Tracking. The other choices beneath the **Settings** option include:

Save

- **Defaults and Apply Now:** This saves your settings as a default and immediately applies them to the selected devices, as applicable.
- **Defaults Only:** Saves the settings as defaults but does not push them immediately to the devices selected.

Revert

- **To Custom Defaults:** Reverts the settings of the selected devices to the user defined custom values.
- **To Factory Settings:** Reverts the settings of the selected devices to factory default settings.

Synchronize

- The synchronize button allows users the ability to synchronize settings on multiple devices with SensorView or to synchronize SensorView settings to match the devices.

Rediscover Devices

- Rediscover devices causes SensorView to search for devices per what has been selected in the device tree.

Network Management - Group Copy

The **Group Copy** option (Figure 59) allows the user to copy settings, scenes, profiles, and loads to devices from a source group over to the destination group. Drag devices in the destination group to change the mapping. When devices are mapped appropriately, click **Copy.**

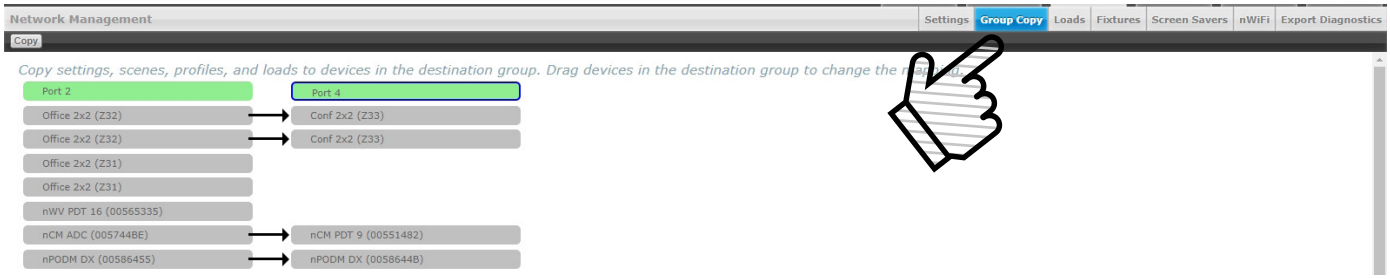


Figure 59: Network Management - Group Copy

Loads

Output capable devices have a field for **Load**, which represents the power of the fixture(s) they are controlling. The **Loads** option (Figure 60) allows a user to select devices to modify and write a value to the Load field on those devices. Click **Save** to apply the changes made. Click **Set Baselines** to make the new setting the baseline for that device (this will cause the relay to toggle on and off). Lastly, check the box to **Update Green Screen Historical Data** to ensure that changes made are recorded in the Green Screen reports.

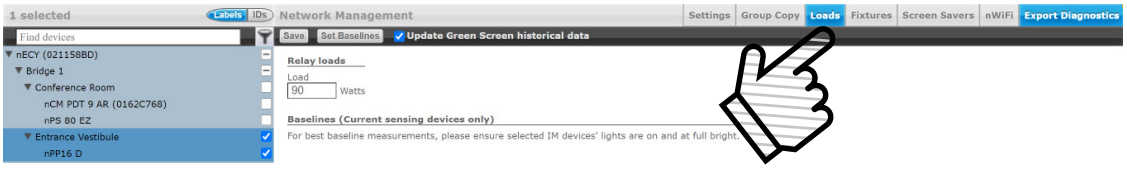


Figure 60: Network Management - Loads

Fixtures

The **Fixtures** option (Figure 61) allows for a user to adjust the icon that appears for the device when under Map view. Users can select from fixture manufacturer types Lithonia, Peerless, and Holophane. A selection of fixture-specific icons appear under each of the manufacturers. **Select A Manufacturer** via drop down, then **Select A Fixture** from the following list. When you are done, click **Save Fixtures**.

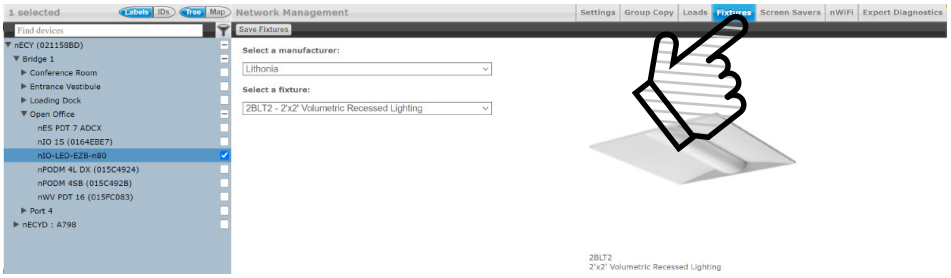


Figure 61: Network Management - Fixtures

Screen Savers

Screen Savers for nPOD GFX and nPOD TOUCH devices can be uploaded from this screen. Upload a screen image to the selected device using the **Upload Screen Saver** button. Optimal resolution is suggested to be 320 x 240 16bit color. Accepted file formats include JPG, PNG, GIF, BMP, and TIF.

Export Diagnostics

The **Export Diagnostics** screen is used to create a zip file with system-pertinent information required for both history and troubleshooting purposes. The file includes information on gateway health and diagnostic information, error logs, a SensorView database export, and a SensorView Map Builder export. Clear Health is used to reset all counters for selected devices to 0. Only devices that are selected using the tree view are affected. In the Description field, users can enter notes or text, and all entered information will appear in their Diagnostic Export as a .txt file. An option to **Include Health Statistics** of devices is found below **Description**. This option is enabled by default, and when left enabled, the created diagnostic file will include a .xlsv with information relating to devices and their corresponding health statistic counts.

Profiles

The **Profiles** tab (Figure 62) 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. The tab has three configuration panels: **Profiles**, **Settings**, and **Scheduler**. Profiles exist in both local and global forms. Global Profiles are created and edited via the Profiles tab. Local profiles are created and edited via the Devices tab by modifying settings on broadcasting devices, such as scene switches.

Figure 62: Profiles Tab

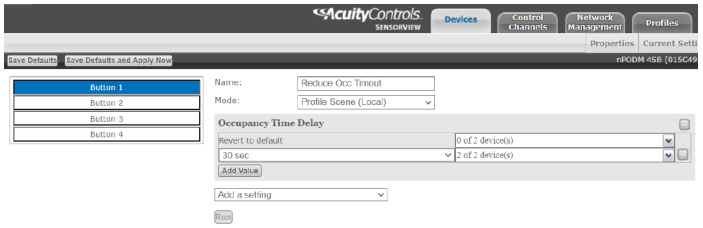


Figure 63: Local Profiles

Global Profiles are stored in the database and the Gateway, which administers profiles according to priorities. The profiles can also be activated on demand via SensorView, an nGWY2 GFX, or via a scene switch that is connected to a network of nLight devices. When activated, global profiles execute in unicast, writing to all applicable devices.

Local profiles are stored in broadcasting devices (Figure 63). The profiles are activated by triggering the broadcasting device, and when activated, local profiles execute in unicast, writing to all selected devices on the same nBRG 8 port or daisy-chain.

To configure a global profile:

1. Click **New** under the **Profiles** panel (Figure 64) to start creating a new profile, or click the name of a profile in the list to edit an existing profile.

2. In the **Settings** panel to the right of the Profiles panel, users will be prompted to select the devices affected by this profile and to create a name for the profile (Figure 65). When you are finished making changes to the profile, click the **Save** or **Save As Copy** button.
3. Add or remove devices using the checkboxes in the **Device Tree** on the left (Figure 66). Checked devices can participate in the profile and receive applicable settings while the profile runs.

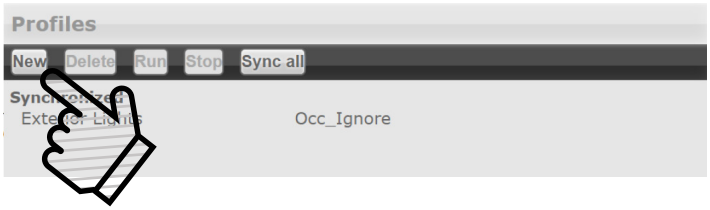


Figure 64: New Profiles

Figure 65: Name Profile

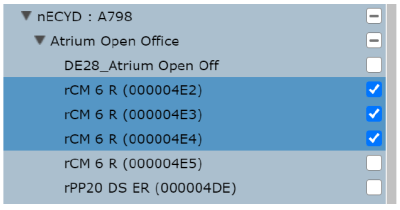


Figure 66: Select Devices

4. Select the desired settings for the selected devices via the **Add a Setting** drop down menu (Figure 67). Multiple settings can be added to the profile and will affect the applicable selected devices.

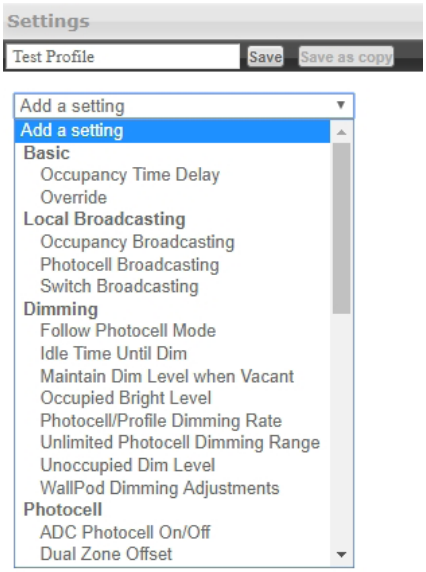


Figure 67: Select Settings

5. Create a new schedule on the **Scheduler** panel, or select an existing schedule from the drop down menu (Figure 68). The Scheduler allows the following options:

   - 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

   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

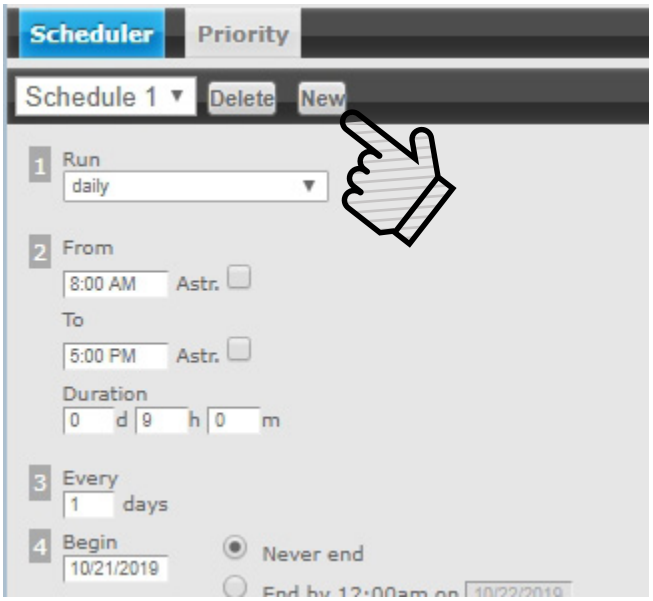


Figure 68: Create Schedule

6. Users can change the priority status of profiles on the **Priority** tab (Figure 69), which allows devices in multiple profiles to react based on the priority of said profiles. Select the priority of the profile to change, then use the arrows to move to the appropriate position, or down into the disabled area

Figure 69: Set Profile Priorities

Schedules

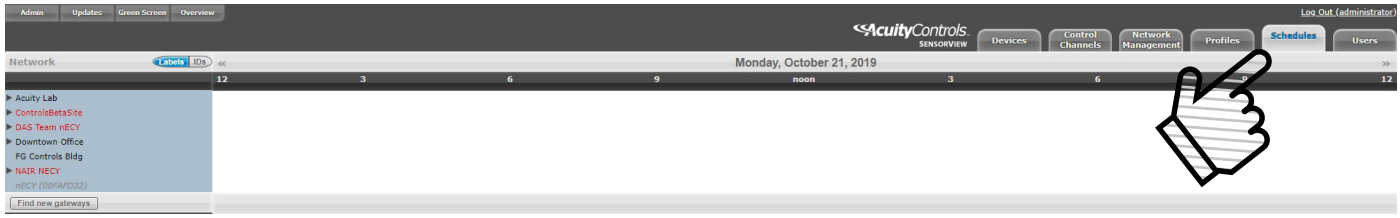


Figure 70: S hedules

The **Schedules** tab (Figure 70) 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.

If two profiles are scheduled at the same time, the one with the higher priority (per the **Profiles** tab section) takes precedence.

Users - Virtual Wallpod

With the Virtual Wallpod applications, users can control their lighting from their desktop or iOS mobile device.

SensorView is a required component of the Virtual WallPod application. Use of Virtual WallPods requires SensorView to be online and accessible, and it is only supported for legacy implementations of nLight. Implementations of nLight that leverage AIR to Wired global channels or AIR to AIR global channels should use the ENVYSION application (accessible through an nLight ECLYPSE) for desktop control and mobile application control of a space.

For more information on ENVYSION control capabilities, please see the ENVYSION specification sheet.

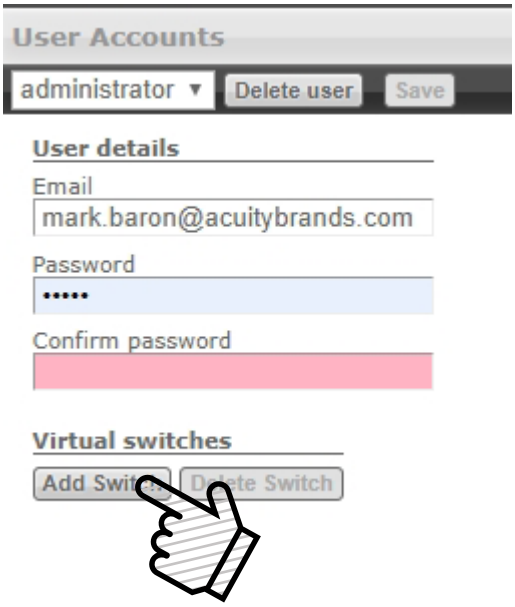


Figure 71: Virtual Switches

Before configuring your Virtual Switches, first, be sure that the **nLight Virtual Wallpod Server** is running. This can be found under the **Admin** tab, beneath the **Plugins** sub tab (Figure 72).

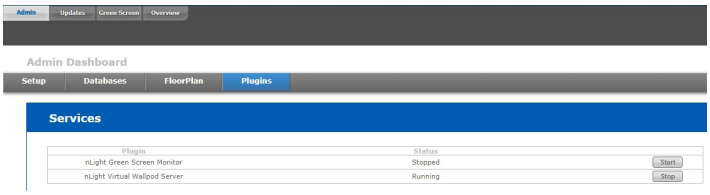


Figure 72: Virtual Wallpod Server

Now that the nLight Virtual WallPod Server is running, go to the **User** tab. Select a user by clicking on the drop down arrow beneath the words U**ser Accounts**. Click the **Add Switch** button beneath the **Virtual Switches** option beneath the selected user.

Next, configure the Virtual Wallpod (Figure 73). The following options may be configured:

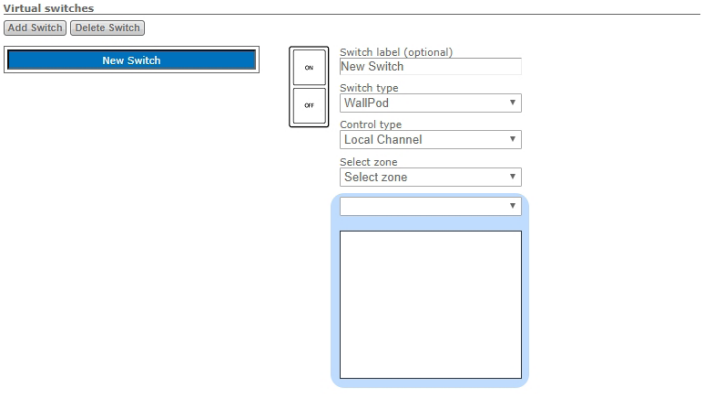


Figure 73: Configure Virtual Wallpod

Switch Label (optional)

- Create a label for the Virtual Switch.

Switch Type

- **Wallpod**
- **Dimming Wallpod**
- **Global Preset**
- **Button Press**

Control Type

- **Individual Device**
- **Local Channel**
- **Global Channel**

Select Zone

- Select the zone to be controlled by the Virtual Wallpod

Select Channel

- Select the channel within the zone to be controlled, and then select the devices listed there.

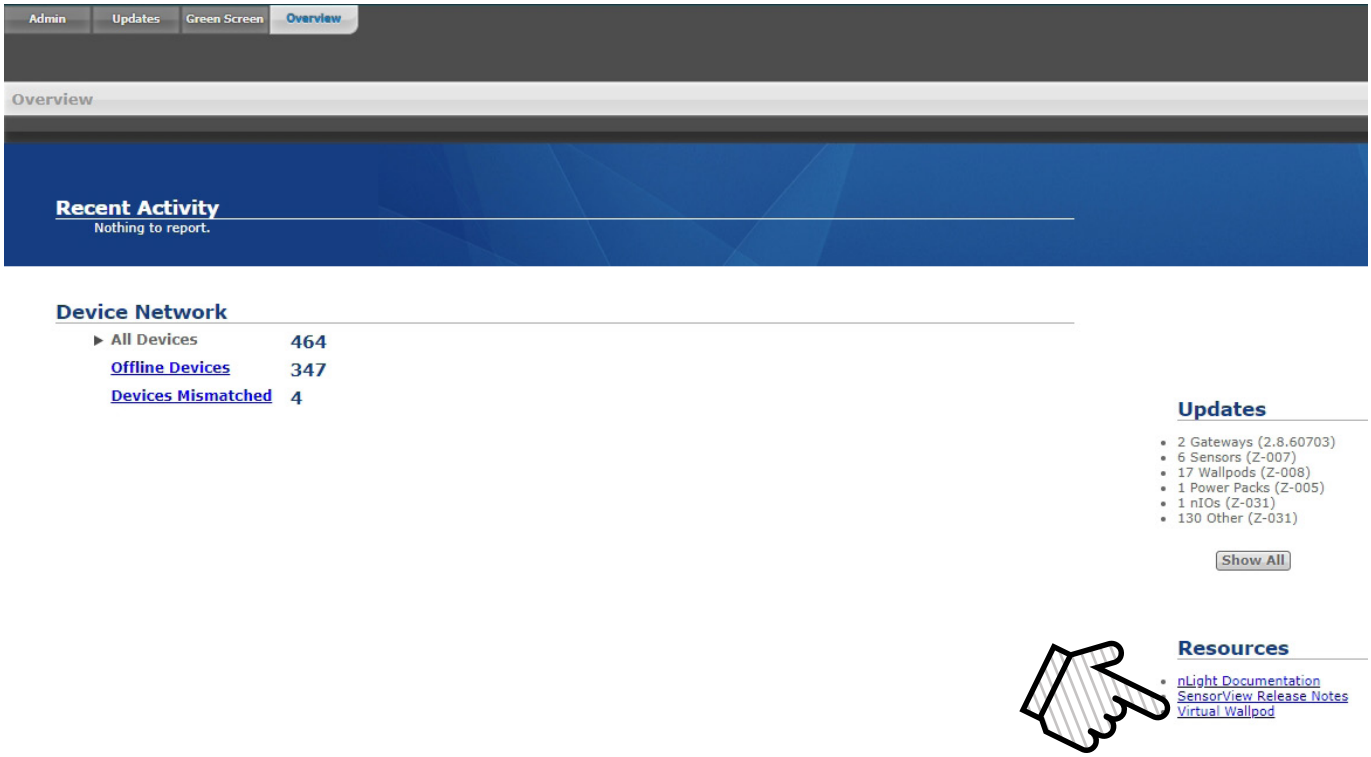


Figure 74: Virtual Wallpod Application

Download the **Virtual WallPod** application from the Overview page of SensorView (Figure 74). Click the **Overview** tab at the top right portion of the screen, then Virtual WallPod under the **Downloads** section (bottom right) to download. 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** and follow the installation steps to completion. Find and launch the device from your system's applications menu (Figure 75).

NOTE

The download link will only be shown if the Virtual WallPod Plugin has been enabled.

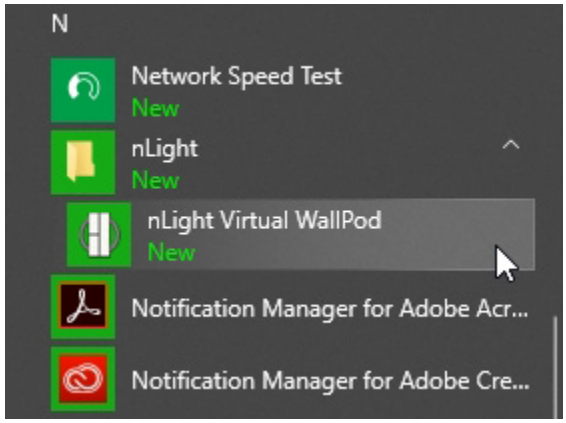


Figure 75: Launch Virtual Wallpod Application

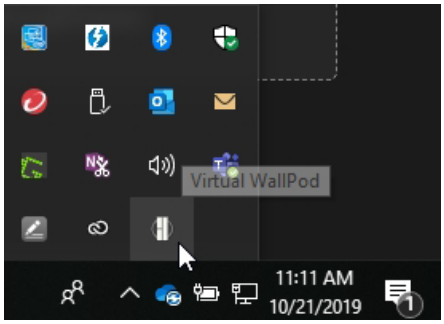


Figure 76:Virtual Wallpod Task Icon

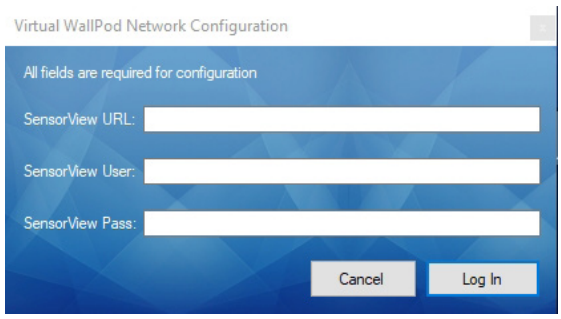


Figure 77: Network Configuration

Once the icon for the **nLight Virtual WallPod** appears in the **Taskbar** (Figure 76), right-click it and enter the **Network Configuration** (Figure 77).

If the nLight Virtual WallPod app is installed to the SensorView host machine, the SensorView URL will be **http://localhost/sensorview**.
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** (Figure 78) 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.

Figure 78: Virtual Wallpod Running

Virtual WallPod iOS App

This section details how to install and setup the **Virtual WallPod** software for iOS devices (Figure 79).

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.

Figure 79: Virtual Wallpodon iOS

Once the app is launched, the **Virtual Wallpod** Login screen will load (Figure 80). Click the Information icon in the upper right to access the configuration screen.

From there, enter the server URL , and enable the desired options from the following list:

- **Save Username**
- **Save Password**
- **Auto Logon**
- **Use Wi-Fi Connection**

Click **Done**, then login with the user credentials for the nLight Virtual WallPod you wish to control. Select a switch from the devices list. Installation is now complete.

Figure 80: Virtual Wallpodon iOS Login

CLAIRITY Link Transporter

The CL**AIR**ITY Link transporter encrypts information exchange between authenticated users and the CL**AIR**ITY Link portal. This software is available for optional installation when installing SensorView versions 15.2 and later. Using this software, factory authorized representatives are able to access a site with an active connectivity plan remotely using the CL**AIR**ITY Link portal.

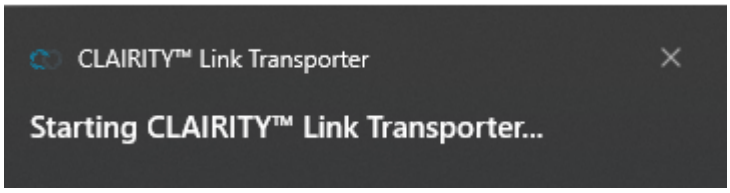
CLAIRITY™ Link Transporter

App

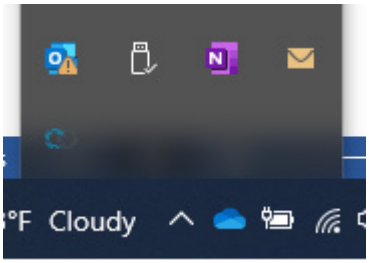
Running the CLAIRITY Link Transporter

The below are steps to run the CL**AIR**ITY Link transporter. An active Internet connection is needed for the transporter to authenticate with the CL**AIR**ITY Link cloud.

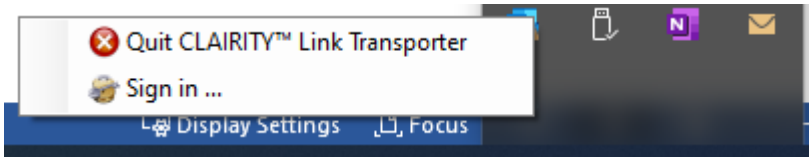
1. Run the CL**AIR**ITY Link transporter application. You will see a message like the below when the application starts.



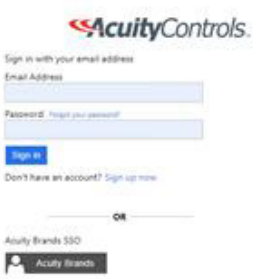
2. Open the system tray (collapsed list of programs on the right-hand side of the taskbar).



3. Right click on the CL**AIR**ITY Link icon and select "Sign In…"



4. If users have an existing CL**AIR**ITY Pro, CL**AIR**ITY, or SensorSwitch VLP account, their login can be used to sign into the CL**AIR**ITY Link transporter. Otherwise, new users will need to click "Sign up now".



5. Multi-factor authentication is required to log in after a valid username and password are provided. Users will be sent a verification code to their email address, and once the verification code is confirmed, the page will update and display the below confirmation message.

Authentication complete. You can return to the application. Feel free to close this browser tab.

6. With the CL**AIR**ITY Link transporter successfully running, authorized users can log into the CL**AIR**ITY Link portal using their portal credentials and interact with the CL**AIR**ITY Link routers and their downstream devices.

Sensorview Terms

The following is a glossary of terms, sorted alphabetically, used in Sensorview.

100 Hour Burn In	Overrides relay on and/or dimming output to full bright for one hundred hours.
Active Screen Brightness	Specifies the brightness of the backlight when device is in use.
ADC Photocell On/Off	Turn the lights on or off if dimming is insufficient to meet photocell Set-Point requirements.
Auto Set-Point	Photocell calibration procedure for detecting optimum lighting control level.
Automated Demand Response	Enable/Disable load shedding.
Automated Demand Response Low Level	Dim Level to use as upper limit when in load shedding mode.
Automated Demand Response Max Level	Dim Level to use as upper limit when in load shedding mode.
Automated Demand Response Medium Level	Dim Level to use as upper limit when in load shedding mode.
BLE Output Power	The BLE radio output power in dBm
Blink Warning	Enables a blink warning for the output to toggle five minutes before it turns off.
Button Action	Defines what action a button press performs.
Button Enabled	Specifies whether or not the button is currently disabled / inactive.
Cloud Detection	When enabled extends transition time from daylight harvesting to reduce on/off transitions when ambient light level is rapidly changing.
Color Number	Sets the active color for the color cell.
Color Number Switch Tracking	If enabled, the luminaire will ignore Color Number commands.
Color Temperature Global Switch Tracking	Indicates whether color temperature will track global switch channels.
Color Temperature Percent	The color temperature of a tunable white fixture as it relates to wall switch dim level percentage.
Color Temperature Switch Tracking	Indicates whether a device's color temperature output will react to manual switching and/or dimmer events.
Contrast Level	Sets the grayscale Contrast Level for the luminaire.
Custom Color 100%	Sets a user-defined color for Custom Color 100.
Custom Color 93%	Sets a user-defined color for Custom Color 93.
Custom Color 94%	Sets a user-defined color for Custom Color 94.
Custom Color 95%	Sets a user-defined color for Custom Color 95.
Custom Color 96%	Sets a user-defined color for Custom Color 96.
Custom Color 97%	Sets a user-defined color for Custom Color 97.
Custom Color 98%	Sets a user-defined color for Custom Color 98.
Custom Color 99%	Sets a user-defined color for Custom Color 99.
Deadband External Photocell	Adjustment factor for measured artificial light contribution
Dim When Held	Light levels will dim when pressed and held.
Dimming Always On	Maintain dimming level at minimum value when in the "off" state.
Dimming Curve	Specifies dimming curve used in the driver (linear/log).
Dimming Level	The dimming level output when the associated preset is activated.
Driver Group	Group dimming outputs together
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).
DZ Photocell Mode	Indicates a Dual Zone photocell sensor's method of operation.
Fade Off Time	The time after receiving an "off command" for lights to dim down before turning off.

Sensorview Terms - cont'd

Fade On Time	The time after receiving an "on command" for devices to reach full bright.
Follow Photocell Mode	Instructs a device to track the dimming output maintained by an ADC device.
Global Occupancy Broadcasting	Enable/Disable global occupancy broadcasting.
Global Occupancy Tracking	Enable/Disable global occupancy tracking.
Global Photocell Broadcasting	Enable/Disable global photocell broadcasting.
Global Photocell Tracking	Enable/Disable global photocell tracking.
Global Switch Broadcasting	Enable/Disable global switch broadcasting.
Global Switch Tracking	Enable/Disable global switch tracking.
High End Input Trim (100%)	Max photocell voltage. Follow photocell level will be 100% at high trim.
High End Trim (100%)	Maximum dimming voltage. Output reports 100% at high trim; corresponding lumens depend on ballast/driver.
Idle Screen Brightness	Backlight brightness is reduced to this level after backlight timeout setting.
Idle Time Until Dim	Time after last detected occupancy that lights reduce to Unoccupied Dim Level for local channels. Time after occupancy time delay expires lights remain at Unoccupied Dim Level for global channels.
Invert Relay Logic	Reverses open/closed state for relays.
Lamp Type	Specifies the dimming curve for PCD.
LED	Controls whether or not a device will illuminate its LED.
LED 1% Follow Photocell Level	Foot-candle level in shaft in which the LEDs will be full dim (1%).
LED 100% Follow Photocell Level	Foot-candle level in shaft in which the LEDs will be full bright (100%).
LED 50% Follow Photocell Level	Foot-candle level in shaft in which the LEDs will be at 50%.
LED Inhibit Offset	Offset (deadband) above "LED 1% Follow Photocell Level" before "Photocell Transition Off" timer begins.
Line Voltage	Specifies the main's voltage the current monitoring device is operating on; used to properly calculate power level.
Load Fault Protection	Enable/Disable load fault protection.
Local Occupancy Only	Instructs a device with a relay and/or dimming output to react to only its internal occupancy information.
Local Photocell Only	Instructs a device with a relay and/or dimming output to react to only its internal photocell information.
Local Switch Only	Instructs a device with a relay and/or dimming output to react to only its internal switch information..
Louver inhibit	Foot-candle level in shaft in which the Louver Transitions from Full Open to Full Close (Evening) or Full Close to Full Open (Morning).
Louver Photocell Delay Time	The amount of time between pulses that are sent to the motor in response to daylight harvesting.
Louver Photocell Pulse Time	The length of the pulses that are sent to the motor in response to daylight harvesting.
Louver Stroke Time	Time it takes the louver to go from fully open to fully closed (or vice versa).
Louver Switch Delay Time	Time between pulses due to switch commands.
Louver Switch Pulse Time	Time the relay closes due to switch commands.
Low End Input Trim (1%)	Min photocell voltage. Follow photocell level will be 1% at low trim.
Low End Trim (1%)	Min dimming voltage. Dim level reports 1% at low trim; lumen output depends on ballast/driver. Not recommended to be below factory defaults.
Lumen Compensation	Specifies lumen compensation mode.
Maintain Dim Level when Vacant	Prevents lights from turning fully off once in unoccupied state.

Sensorview Terms - cont'd

Maintain Dim Level (Local Occ)	Lights will go to their Unoccupied Dim Level when occupancy is detected on an otherwise untracked local channel but no occupancy is detected on a directly tracked local channel.
Maintain Dim Level (Global Occ)	Lights will go to their Unoccupied Dim Level when occupancy is detected on an otherwise untracked global channel but no occupancy is detected on a directly tracked global channel.
Microphone Grace Period	The time period after lights are automatically turned off that they can be reactivated by audio.
Microphonics	Specifies sensitivity of microphone used to enhance occupancy detection.
Middle Input Trim (50%)	Mid photocell voltage. Follow photocell level will be 50% at middle trim.
MLO (High)	Dim level for the MLO high state.
MLO (Low)	Dim level for the MLO low state.
MLO Mode	When enabled allows a single pole switch to control two individual switch channels.
MLO Secondary Broadcast Channel	The channel on which a device with a manual switch will transmit its secondary MLO switch press.
MLV Mode Enabled	Optimizes control for magnetic low voltage devices, preventing flickering.
Momentary Relay Mode	Toggles relay momentarily for 1s when a tracked input causes an state change..
nClass	Operational modes for classroom configurations.
Night Light Brightness	The percent of full brightness of the units night light LED.
nIO Input	Specifies how the device should interpret incoming data on the input wires and the action it should take.
nIO RLX Input	Determines if actions on the input wire affect dimming, on/off, or both.
Occupancy Broadcast Channel	The local 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 Expiration of Manual Off	Reverts override off commands to normal mode after Occupancy Time Delay expires.
Occupancy PIR Sensitivity	Threshold at which motion is considered detected for Occupancy.
Occupancy Time Delay	The length of time an occupancy sensor will keep the lights on after it last detects occupancy.
Occupancy Tracking	Indicates whether a device's relay and/or dimming output will react to occupancy information.
Occupancy Tracking Channels	The local channels on which a relay and/or dimming output receives occupancy information.
Occupied Bright Level	The percentage of the controllable dimming range up to which lights will rise when occupancy is detected or the luminaire is overridden on.
Override	Indicates whether a device's relay is forced on/off and/or dimming output is forced to maximum/minimum.
Override Input State	Specifies the state to which the relay will remain when panel Override input is made and held.
Pattern Number 3 Cell	Sets a predefined grayscale pattern.
Pattern Number 5 Cell	Sets a predefined grayscale pattern.
Pattern Number 9 Cell	Sets a predefined grayscale pattern.
Phase Dimming Frequency	Specifies frequency of the power feed the phase dimmer is operating on.
Photocell Broadcast Channel	The local 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 percentage up to which an automatic dimming photocell will control.
Photocell Dimming Range (Low)	The minimum output percentage down to which an automatic dimming photocell will control.
Photocell Mode	Enable photocell either to turn lights on and off, or only prevent lights from turning on.
Photocell Tracking	Indicates whether a device's relay and/or dimming output will react to photocell information.
Photocell Tracking Channels	The local channels on which a relay and/or dimming output receives photocell information.
Photocell Transition Off	The time period for which a photocell must measure a light level above the set-point before it will turn the lights off.

Sensorview Terms - cont'd

Photocell Transition On	The time period for which a photocell must measure a light level below the set-point before it will initiate the lights on.
Photocell/Profile Dimming Rate	The speed at which dimming level changes when triggered via profile scenes (global or local) or automatic photocell dimming.
PIN Protection	Specifies whether a pin is required to modify light levels and program device.
Predictive Exit Time	Time period after manually switching lights off for the occupant to leave the space.
Predictive Grace Period	The time period after the Predictive Exit Time that the sensor rescans the room for remaining occupants (Predictive Off mode only)
Profile Override	Allow button-initiated profiles to run concurrently, as long as the profiles target different devices.
Push-Button Operation	Overrides a device and enables its push-button to toggle the device's internal relay(s) or dim level.
Reduced Turn-on	Reduces the initial PIR detection strength required to trigger occupancy.
Relay Always On	Forces relay to stay closed even in off state.
Relay End State	Specifies the state which the relay will go to when the panel loses power.
Relay Line Voltage Phase	Indicates relay load's phase relative to relay panel power supply. Helps reduce relay wear related to high switching voltages
Relay Throw Delay	Specifies the delay between relays when throwing multiple relays at the same time.
Rubik Factory Test Mode	Factory test commands.
Scene Expiration Blink	Blink warning will toggle all outputs prior to the expiration of the scene timer.
Scene Expiration Time	The length of time a selected profile scene (global or local) will run before reverting affected devices to defaults.
Screen Backlight Timeout	Specifies how long the backlight should remain at full brightness when in use.
Screen Backlight Timeout	Specifies how long the backlight should remain at full brightness when in use.
Screen Order for GFX Scenes/WallPods	Specifies order of the Scenes and WallPods screens.
Screen Saver Mode	Controls displayed screen saver.
Screen Saver Timeout	Sets idle time before screen saver is displayed.
Screen Saver Timeout	Sets idle time before screen saver is displayed.
Semi-Auto Grace Period	The time period after lights are automatically turned off that they can be reactivated with occupancy.
Sensor LED	Controls whether or not the sensor will illuminate its LED.
Set-Point Ones Digit	The target light level that is to be maintained by the device (foot-candles).
Set-Point Tens Digit	The target light level that is to be maintained by the device (foot-candles).
Setup Screen Timeout	Sets idle time before device exits setup mode.
Setup Screen Timeout	Sets idle time before device exits setup mode.
Special Operating Modes	Unique behaviors for relays and/or dimming outputs.
Special Switch Tracking Mode	Allows a device to ignore specific switch commands.
Speed Percent	Sets the speed at which grayscale patterns will transition.
Speed Switch Tracking	If enabled, the luminaire will ignore Speed Percent commands.
Start-to-High	Lights go to full bright for 20 minutes upon initial power up.
Sunlight Discount Factor	Adjust the photocell's ability to influence light level. Decreasing the discount in a period of high daylight will lower the light level.
Sweep Exit Time	The time period before a sweep is executed (affects all buttons operating in sweep mode).
Sweep Grace Period	The remaining time delay a sensor reverts to after a sweep is executed.
Switch Broadcast Channel	The local channel on which a device with a manual switch and/or dimmer transmits.

Sensorview Terms - cont'd

Switch Broadcasting	Indicates whether a device will transmit its manual switching and/or dimmer events to the rest of its zone.
Switch Tracking	Indicates whether a device's relay and/or dimming output will react to manual switching and/or dimmer events.
Switch Tracking Channels	The local channels on which a relay and/or dimming output receives manual switching or dimming events.
Temperature Fault Protection	Enable/Disable temperature fault protection.
Timed Expiration of Manual Off	Reverts override off commands to normal mode after Timed Override Delay expires.
Timed Override Delay	The length of time an Override On or Off state initiated by a Special Operating Mode will remain in effect.
Unlimited Photocell Dimming Range	Allows the offset zone on a DZ device, or follow photocell device, to go full bright or full dim.
Unoccupied Dim Level	Level to which lights dim once the Idle Time Until Dim expires. Also, low trim level for dimming switches and photocells.
Visibility (Graphic Preset)	Specifies whether or not a configured Preset button will be displayed.
Visibility (Graphic Scene)	Specifies whether or not a configured Scene button will be displayed on the main page.
Visibility (Graphic WallPod)	Specifies whether or not a configured WallPod button will be displayed on the main page.
WallPod Dimming Adjustments	Defines whether user dimming adjustments are maintained after lights are cycled or whether they revert to preset levels.

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
	**Temperature**	Current temperature at the processor of the device
	**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

Status Icons - cont'd

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
	**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
	**Compensated Output Level**	Compensated Output Level: 0
		Pole State reason: Manual Switch Override Off
		
	**Relay State (per pole)**	Closed

Status Icons - cont'd

Occupancy, Relay & Dimming Status - cont'd

Icon	Value	Description
	**Relay State (per pole)**	Open

Photocell Status

Icon	Value	Description
	**Wireless Signal Strength: (1- 5)**	Indicates wireless signal strength (higher is better)
	**Wireless PAN ID**	Wireless panel identification number
	**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
	**Bridge Port Information**	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
		
		
		
		
		
		
		
		Number of downstream wireless Bridges and Transceivers

Photocell Status - cont'd

Icon	Value	Description
 	**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
		Number of downstream wireless Bridges & Transceivers

System Backbone IT Information

Overview

nLight® 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.
- Connection to a Network Time Protocol (NTP) server.
- System integration with a Building Management System (BMS) via BACnet/IP protocol.
- Remote support and diagnostics.

A simplified system riser diagram for a typical nLight installation 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. 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.

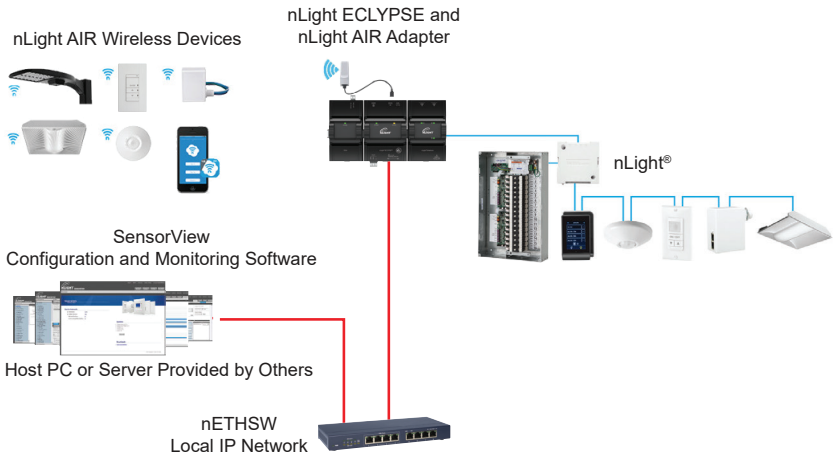


Figure 01: nLight Platform

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 machine requirements.
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.

NOTE

- **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.**

System Backbone IT Information

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.

Protocol	Port	nLight Devices	Usage	Security	Internet Required
UDP	7	• SensorView • nECY	Device identification on local subnet	None, does not contain sensitive data.	No
UDP	67	• Sensorview • nECY	DHCP (outbound)	None, does not contain sensitive data.	No
UDP	68	• SensorView • nECY	DHCP (inbound)	None, does not contain sensitive data.	No
TCP	80	• SensorView	SensorView device configuration data (inbound/outbound), firmware update downloads for nLight Wired	None, does not contain sensitive data. Configuration is read only.	Yes
UDP	123	• SensorView • nECY • CLAIRITY Link Router	NTP time synchronization (outbound)	None, does not contain sensitive data.	No
TCP	443	• SensorView • nECY • CLAIRITY Link Router	Firmware updates for nLight AIR devices Remote access through CLAIRITY Link portal Atrius services for real time location services	TLS	Yes
TCP	5551	• SensorView • nECY	System configuration (inbound/outbound)	AES-128 for nECY	No
UDP	5551	• SensorView • nECY	nLight Protocol over IP	None, should be protected by LAN routing/ firewall.	No
UDP	5555	• SensorView • nECY	Device identification on local subnet	None, does not contain sensitive data.	No
UDP	5556	• SensorView • nECY	nLight Protocol over IP	None, should be protected by LAN routing/ firewall.	No
UDP	9090	• Sensorview	Used for inter-process communication between SensorView and the plugin host service for GreenScreen	None, does not contain sensitive data. Configuration is read only.	No
UDP	47808	• nECY	BACnet over IP protocol	None, BACnet standard, should be protected by LAN routing/firewall.	No

Table 1-1: Required Network Ports and Usage

NOTE

- **SensorView's installer utilizes information from the following URL across port 80: http://nlight.sensorswitch.com/SSIReg/WebService.asmx**
- **SensorView installer downloads and firmware updates for nLight devices are made by accessing the following URL across port 443: https://fota.acuitynext.io/**
- **Remote access through CLAIRITY Link using an Ethernet connection requires access to the following host name across port 443: clairitylink.acuitynext.com. Access to 2.android.pool.ntp.org across port 123 is also required, unless the router and network are configured for another NTP provider. NTP service is required for time synchronization and communication with the CLAIRITY Link portal. For remote access, cellular connectivity is supported in lieu of the above network configurations. See the CLAIRITY Link specification sheet for information on cellular connectivity.**
- **Atrius Services and CLAIRITY Link require access to the following fully qualified domain names (FQDN) over port 443: atrius01iothuzznqzhqcx.azure-devices.net and atrioth01sauzznqzhqcx.blob.core.windows.net**
- **Internet access is not required for regular system functionality. nLight system controllers and end devices do not rely on an Internet connection for continued operation. Internet connectivity is primarily needed during initial setup and when firmware updates are applied.**
- **Device firmware updates are not pushed to devices. Updates must be applied by a user.**

System Backbone IT Information

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).

Application Use	Network Consumption per LAN Component (nECY, XPA BRG, nADR)
SensorView Configuration	< 0.2kbps (when SensorView is actively in use)
SensorView Plugins	< 0.2kbps (Assuming GreenScreen and Virtual WallPod are active simultaneously)

Table 1-2: Approximate Bandwidth Consumption

Remote Connectivity to nLight Systems Through CLAIRITY Link

CLAIRITY™ Link allows trusted experts to remotely update schedules, program devices, monitor for outages, and support networked nLight sites via secure cellular and Ethernet connections. Remote access reduces the need for in-person technician visits, reduces response time, and allows comprehensive access to maintain lighting operations. The solution provides several features to protect in-transit data and data at rest, such as:

1. TLS 1.2 protection of in-transit data and secure connectivity through a web application firewall.
2. Multi-factor authentication, role-based access control, account-specific access control, AES-256 encrypted data at rest, and passwords that meet NSA guidelines.
3. TLS 1.2 protection of in-transit data, secure connection string authentication to verify connecting devices.
4. Integrated firewall between outbound Internet and modem's LAN connection, whitelisted URLs, and signed and encrypted firmware. Communication between the router and the CLAIRITY Link portal only begins through outbound communication initiated by the router.
5. Router will only forward information from nLight ECLYPSE™ controllers and their connected devices to the cloud. All other messages are ignored.

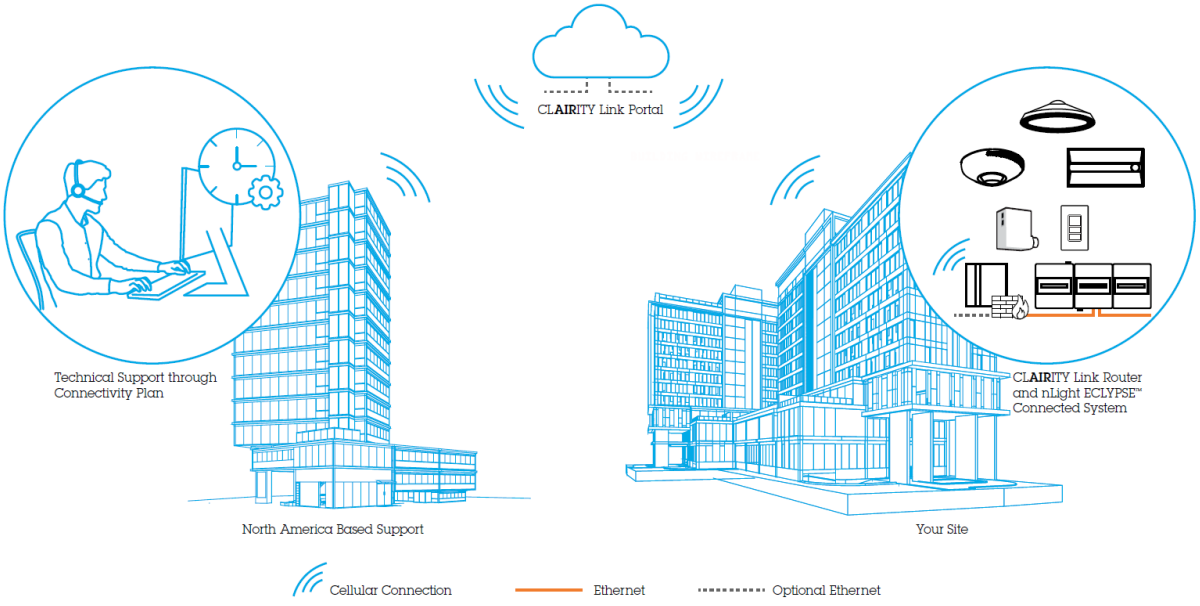


Figure 02: Security Details

nLight® ECLYPSE™

User Guide

Document Revision History

- Version 1.0 - September 2017
  - Release to Market
- Version 1.1 – July 2019
  - Added SSO, Open ADR, nLight Air PTI
- Version 1.2 – Dec 2019
  - Updated images and screenshots
  - Updated the Wireless Configuration section for security updates

Copyright

Table of Contents

CHAPTER 5

CHAPTER 6

CHAPTER 7

CHAPTER 1
Introduction

Overview

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

About the nLight ECLYPSE Controller

The nLight ECLYPSE 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 networks. For this document, the nLight ECLYPSE will also be referred to as just ECLYPSE.

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

About the IP Protocol Suite

Acuity Controls' nLight ECLYPSE 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 multilayered protocol suite that reliably transmits data over the public Internet and privately firewalled-off intranets. As integral part of our interconnected world, this protocol is used by applications such as the World Wide Web, email, File Transfer Protocol (FTP), datashares, and so on.

ECLYPSE 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. Acuity Controls' controllers support both BACnet/IP and BACnet Master-Slave/Token-Passing (MS/TP) communications 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 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 on Acuity Brands website

nLight ECLYPSE Introduction

The nLight ECLYPSE 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 nLight ECLYPSE consists of an automation and connectivity server, power supply, and an nLight Interface module.

This programmable 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 configuration 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

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.

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
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.

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 IP devices:

- 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 (attached per TIA/EIA-568-A,), using Cat 5e data cable. The maximum cable length between devices is 328 ft. (100 m) at 100 MB/s data rate.
  - The electrical signal requirements for data packet transport.
  - 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 *About Routers, Switches, and Hubs*.
- 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 nLight ECLYPSE 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 host computer.
- 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 so on.

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.

DHCP Versus Manual Network Settings

The following methods can be used to set the network settings:

- Manually set network settings allow precise control over the network's configuration. This option may require an in-depth understanding of arcane networking details – much of which is covered in this guide. See *Networking Basics*.
- Use the router's DHCP setting to automatically connect devices to the network by negotiating the appropriate settings with the device. This option may not be applicable to all networks; for example, the network administrator does not want to use DHCP and has supplied information to manually configure the device's IP interface.

No matter which option is chosen, it will be necessary to coordinate with Information Technology (IT) department personnel the use of shared network resources.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a router feature that dynamically allocates configuration parameters to connected devices such as IP, DNS, and default gateway addresses. Enabling DHCP on a router normally eliminates the need to manually configure network settings on connected devices. The implementation of DHCP on most routers allows a device to be assigned a fixed IP address by associating a specific IP address to a device's MAC address.

Devices that use ECLYPSE's internal router with the DHCP option (Hotspot/AP mode) cannot be assigned fixed IP addresses according to the device's MAC address.

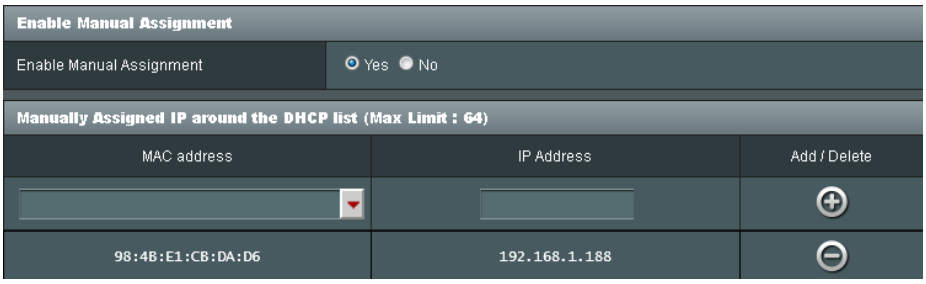


Figure 1: Typical Router Configuration to Assign a Device's MAC Address to a Fixed IP Address

If your router supports DHCP and you have access to the router's configuration interface, this is the most straight-forward way to configure your network. Ensure that all devices that require a fixed IP address use a manually assigned IP address.

Fixed IP Address or Hostname Management

Why Should ECLYPSE IP controllers use a fixed IP address or use hostname Management? To program or to access an IP controller, you must be able to connect to it. Like a postal address, a fixed IP address that is always assigned to the same device allows you to consistently connect to and work with the same device.

An alternative to using a fixed IP address is to use the controller's Hostname Management which allows a controller to be identified by a nickname such as ***Office_205*** instead of the controller's IP address. The hostname can be used in a Web browser.

Networking Basics

When manually configuring the TCP/IP interface on an ECLYPSE IP controller (the DHCP option is not used), an IP address, subnetwork mask, and a default gateway are required in the Network Settings.

IP Addressing

The most widely used internet addressing scheme is IPv4. It codes an IP address in 32 bits.

An IPv4 address is made up of two parts defined by a subnetwork mask; the network portion (which identifies a specific network or subnetwork) and the host portion (which identifies a specific device).

About the Subnetwork Mask

Devices on the same sub-network can address IP packets to each other directly without routing. The range of IP addresses available in a sub-network is defined by the subnetwork mask. This is also called the subnetwork mask's 'address space'. The subnetwork mask is coded in 32 bits as follows.

An IP packet addressed to a device on another network portion will have to be routed through the router's WAN port as such an address is not local. BACnet/IP broadcast discovery messages such as "Who-Is" do not pass through network routers that separate subnetworks. This means that BACnet/IP controllers on different subnetworks will not normally communicate with each other.

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. See BBMD Settings.

Network Class			CIDR	Subnetwork Mask	Block Size	Number of Subnetworks according to the Network Type			Number of Hosts according to the Network Type		
						Class A	Class B	Class C	Class A	Class B	Class C
←Class A Network→			/8	255.0.0.0	256	1			16777214		
			/9	255.128.0.0	128	2			8388606		
			/10	255.192.0.0	64	4			4194302		
			/11	255.224.0.0	32	8			2097150		
			/12	255.240.0.0	16	16			1048574		
			/13	255.248.0.0	8	32			525286		
			/14	255.252.0.0	4	64			262142		
			/15	255.254.0.0	2	128			131070		
	←Class B Network→		/16	255.255.0.0	256	256	1		65534	65534	
			/17	255.255.128.0	128	512	2		32766	32766	
			/18	255.255.192.0	64	1024	4		16382	16382	
			/19	255.255.224.0	32	2048	8		8190	8190	
			/20	255.255.240.0	16	4096	16		4094	4094	
			/21	255.255.248.0	8	8192	32		2046	2046	
			/22	255.255.252.0	4	16384	64		1022	1022	
			/23	255.255.254.0	2	32768	128		510	510	
		←Class C Network→	/24	255.255.255.0	256	65536	256	1	254	254	254
			/25	255.255.255.128	128	131072	512	2	126	126	126
			/26	255.255.255.192	64	262144	1024	4	62	62	62
			/27	255.255.255.224	32	524288	2048	8	30	30	30
			/28	255.255.255.240	16	1048576	4096	16	14	14	14
			/29	255.255.255.248	8	2097152	8192	32	6	6	6
			/30	255.255.255.252	4	4194304	16384	64	2	2	2

CIDR Addressing

Another way to express the subnetwork mask is through CIDR addressing (Classless Inter-Domain Routing) which is written as a slash and a number which represents the number of true bits set in the subnetwork mask. For example, the subnetwork mask 255.128.0.0 is 11111111 10000000 00000000 00000000 in binary or /9.

An IP address can be expressed with its CIDR subnetwork mask in the form of 192.168.0.0/24 for example.

Private IPv4 Address Ranges

Each IP address class has a private address range. Private IPv4 addresses cannot be routed over the Internet.

nLight ECLYPSE IP controllers will normally be assigned to a private IP address and are connected to the LAN ports of a router, thereby keeping them behind a firewall from the internet while allowing them to freely communicate to each other and to other trusted devices.

The following IPv4 address ranges are reserved for private networks.

Network Class	IP Address Range	Number of Addresses	Largest CIDR Block (subnetwork mask)
A	10.0.0.0 - 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)
B	172.16.0.0 - 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)
C	192.168.0.0 - 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)

Reserved Host Addresses

The first and the last IP addresses are reserved for special use on all subnetwork IP address ranges:

The first IP Address is the Network ID. Networks with different network IDs are considered to be distinct. By default, no direct communication can take place between two networks that have different Network IDs. This prevents computers on one network from being accessed by computers on another network. When one department or organization is on one network, it is segregated from computers on other networks.

Last IP Address is the Broadcast Address: this is used for a specific type of network traffic that is destined to every host in the subnetwork range of IP addresses. For example, the device's DHCP client uses the broadcast address to find the network's DHCP server.

For Example, with a typical class C private network:

Subnetwork Mask = 255.255.255.0

Network ID = 192.168.1.0

Gateway = 192.168.1.1

Broadcast Address = 192.168.1.255

Usable IP Addresses = 192.168.1.2 - 192.168.1.254

Default Gateway

Two hosts on the same subnetwork can directly communicate with each other. When a host wants to communicate to an IP address that is not in the subnetwork address range, the host sends the packet to the default gateway. The default gateway is usually the router's IP address and is usually set in the routers administration interface. For more information about IP routing, see *About Routers, Switches, and Hubs*.

Certain ECLYPSE controller services use the default gateway. See *ECLYPSE Services that Require Internet Connectivity*.

Domain Name System (DNS)

When you want to connect to another computer or service on the Internet (to a Website for example), rarely would you want to use the IP address to make the connection as it would be a pain to remember the numeric IP address for each and every site you want to visit. The Domain Name System (DNS) was created to allow internet users to take advantage of a meaningful Uniform Resource Locator (URL) such as https://www.acuitybrands.com/ to connect to an IP address without having to know the server's or computer's numerical IP address. The DNS does this by looking up the URL and providing the numeric IP address to the requesting computer. Should the IP address of a computer/server be changed, the DNS server can be updated with its new IP address, thereby ensuring that other networked computers can still find this computer/server through its URL.

Set the DNS IP address of the Domain Name System (DNS) servers in routers and in IP controllers that have manually-configured IP parameters. Between one and three DNS IP address is usually provided by the Internet Service Provider (ISP). The second and third DNS addresses are for failover should the first DNS become unavailable.

If you do not know the address of your DNS server(s), try the following publicly-available DNS server addresses: primary = 8.8.8.8 and secondary = 4.4.4.4

Some ECLYPSE controller services use DNS to resolve Web addresses thereby allowing the service to operate. See *ECLYPSE Services that Require Internet Connectivity*.

About Routers, Switches, and Hubs

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

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.
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.

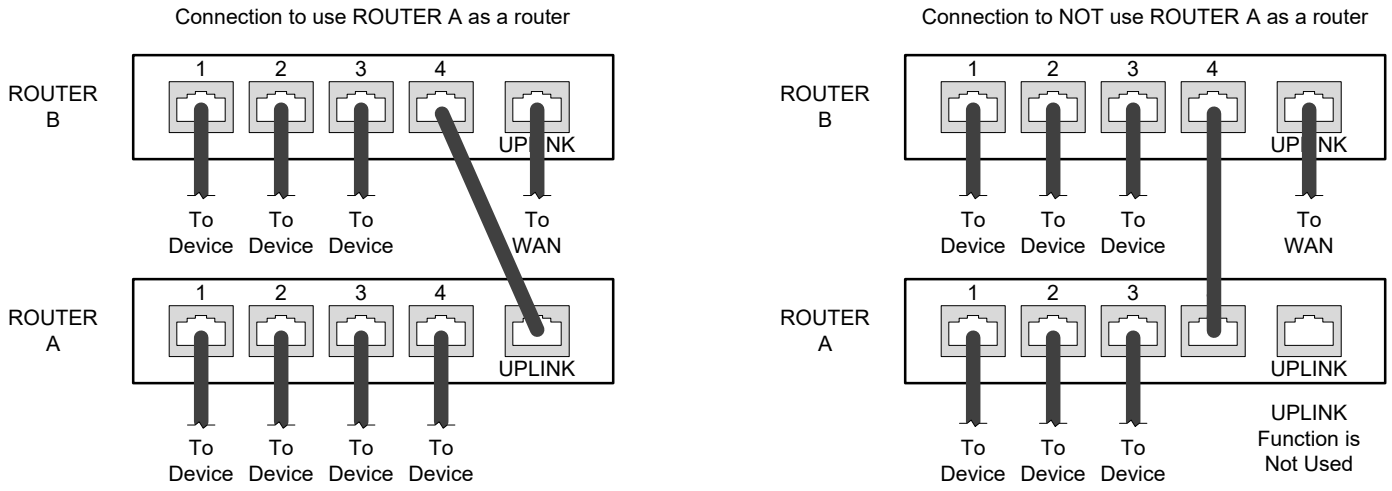


Figure 2: The Way a Router is Connected Changes its Function

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 ECLYPSE controllers is explained in chapter *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.

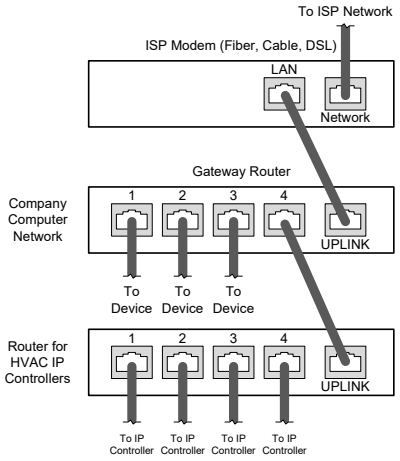


Figure 3: Network Segment for HVAC IP Controllers

For certain wireless topologies, a wireless router can be used to connect to the controller. In this scenario, a wireless operator interface (laptop or tablet) can be used for commissioning as shown in the figure below.

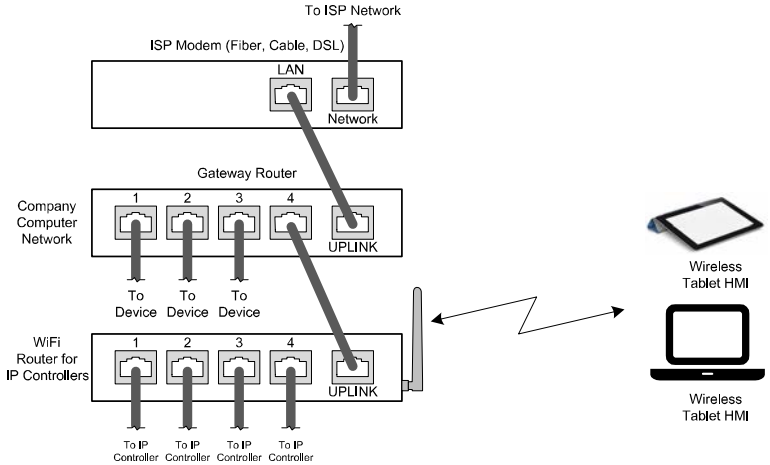


Figure 4: Network Segment for HVAC IP Controllers with a Wireless Access Point

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

CHAPTER 4
IP Network Protocols and Port Numbers

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

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 controllers is explained in *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.

IP Network Port Numbers and Protocols

This section lists the 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	
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)	**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*.
HTTPS	443 (TCP)	**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*.
Radius Server	1812 (UDP)	Authentication Port: This is the port on which authentication requests are made.	

Service	Default Port Number (Protocol)	Description	Where can this port number be changed?
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*.
BACnet/IP	47808 (UDP)	The BACnet over IP protocol.	See *BACnet Settings*.
MQTT	8883 (TCP)	Secure MQ Telemetry Transport. This is an internal port that facilitates communication with the nLight Gateway.	
zeroconf	5353 (UDP)	This is an internal port used to access a device through the hostname.	
Unknown	5551 (TCP)	System configuration (inbound/outbound)	
Echo	7 (UDP)	Device identification on local subnet	
Rplay	5555 (UDP)	Device identification on local subnet	
Freeciv	5556 (UDP)	nLight Protocol over IP	
Unknown	33312 (UDP)		
Unknown	39631 (UDP)		

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 Network

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.

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 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.

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) ECLYPSE IP devices have two RJ-45 female RJ-45 connectors that provide IP packet switching to support follow-on devices.
Daisy-chain limit, ECLYPSE Controllers	Up to 20 devices can be daisy-chained per network switch port.
Daisy-chain limit, VAV Controllers	Up to 50 devices can be daisy-chained per network switch port.
EOL terminations	Not applicable
Shield grounding	Not applicable

Table 1: Wired Network Cable Physical Specifications and Requirements

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

Table 2: Recommended Cable Types to use for the Cat 5e Cable Subnetwork Bus

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.

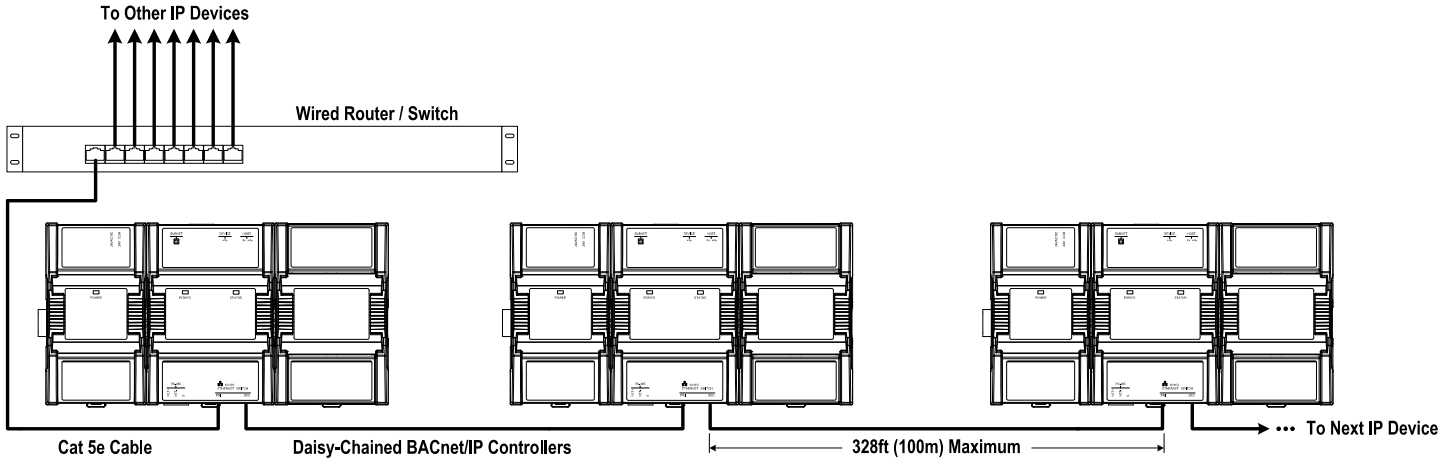


Figure 5: Wired Network Connection - Daisy-Chained

Spanning Tree Protocol (STP)

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, non-PoE 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.

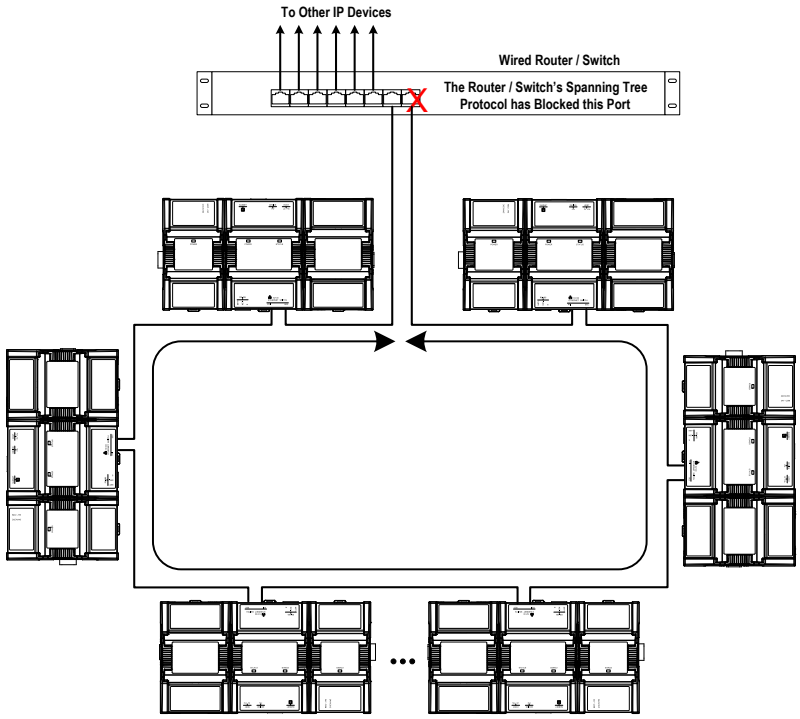


Figure 6: Wired Network Connection: Spanning Tree Protocol – Normal Operation

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.

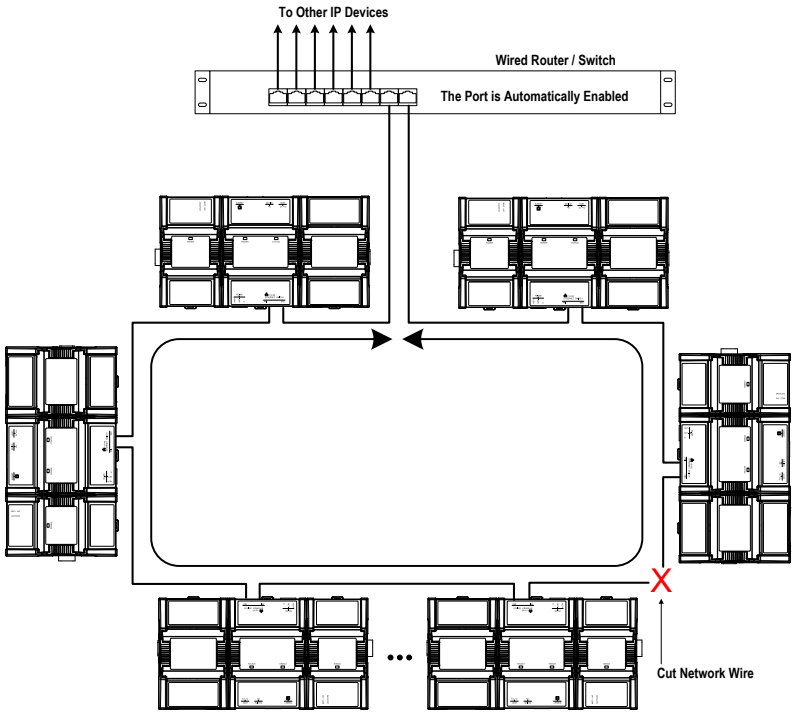


Figure 7: Wired Network Connection: Spanning Tree Protocol – Failover Operation

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 Controller

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

Wireless Network Connection

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

Figure 8: Wi-Fi Adapter

It adds wireless IP connectivity to controllers and it can be used in many wireless topologies and applications.

To wirelessly connect to a controller for the first time, see *First Time Connection to an ECLYPSE Controller*.

To configure a Wi-Fi adapter, see *Network Settings*. See also chapter *Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks*.

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 that is in close proximity to the ECLYPSE Wi-Fi adapter can cause interference, even if its operating frequency is 1.9 GHz for example.

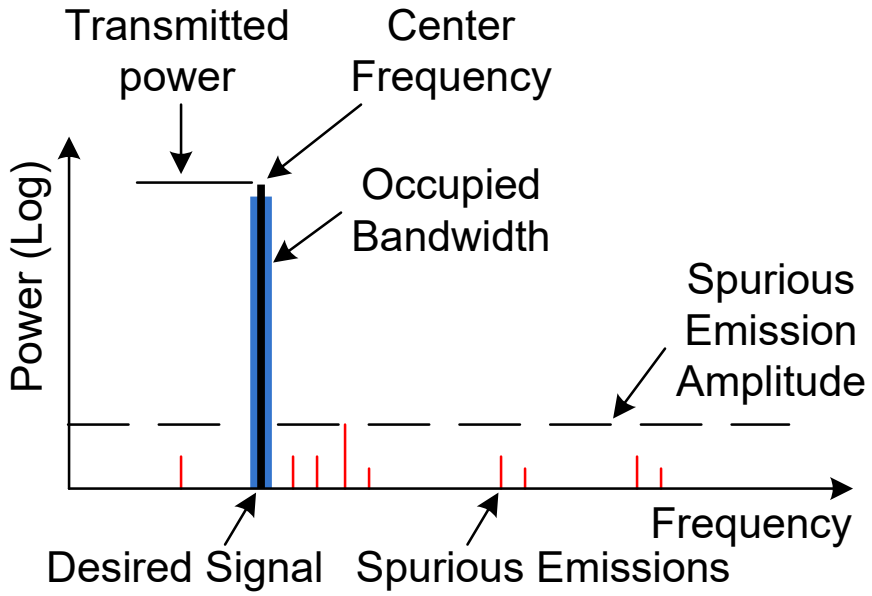


Figure 9: Typical Radio Transmitter Spurious Emissions

Distance Between the Wi-Fi Adapter and Sources of Interference

Unrelated transmitters should be more than 6.5 feet (2 m) away from the 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 mid-point 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 802.11g, 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.

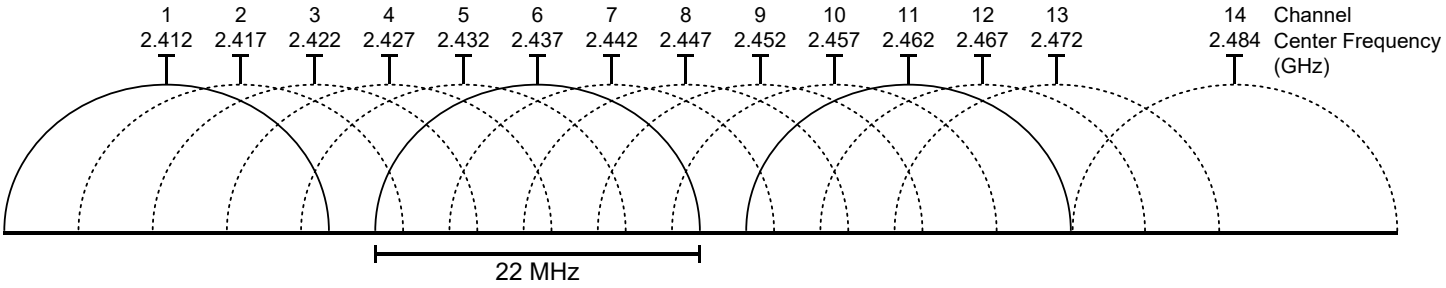


Figure 10: 2.4 GHz Band 802.11g Radio Spectrum Showing Inter-Channel Overlap

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-channel overlap 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

Range is dependent upon many environmental variables that are present in buildings. In normal conditions, a radio signal is transmitted at a maximum range between Wi-Fi Adapters of 50 feet (15 m) at 2.4 GHz (IEEE 802.11b/g/n).

In certain cases where there are obstructions, the range could be less.

Because radio signals and transmission range can vary according to building and office setup, you can troubleshoot Wi-Fi network performance issues by running a Wi-Fi surveying or Wi-Fi stumbling tool on a laptop computer. This software shows the currently operating Wi-Fi networks operating within range, their signal strength, and their channel number so as to make the best configuration choices.

Radio Signal Transmission Obstructions

Radio signals are electromagnetic waves; hence the further they travel, the weaker the signal becomes thereby limiting effective range of operation. Coverage is further decreased by specific materials found in the direction of the transmission. For example, while radio waves can penetrate a wall, they are dampened more than if the waves were on a direct line-of-sight (LoS) path.

The following table shows the different types of building materials and range reduction:

Wall Material	Range Reduction vs. LoS
Wood, drywall, glass (uncoated, without metal)	0 – 10%
Brick, particle board	5 – 35%
Metal, steel-reinforced concrete, mirrors. See *Where to Locate Wireless Adapters*	10 – 90%

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.

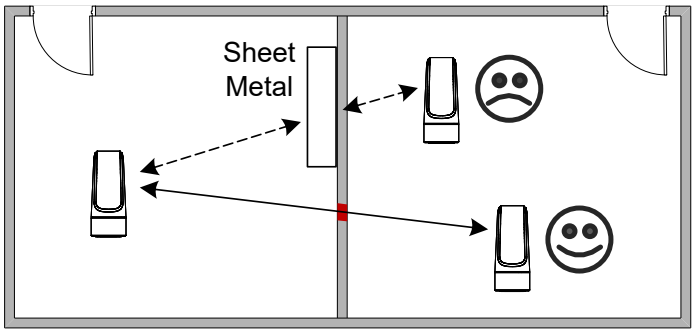


Figure 11: Screening of Radio Waves

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)).

For more examples on how to position the wireless adapter, see *ECLYPSE Wi-Fi Adapter Mounting Tips*.

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 below). Therefore, it is preferable that the transmission be arranged so that it travels straight and perpendicularly through the obstruction.

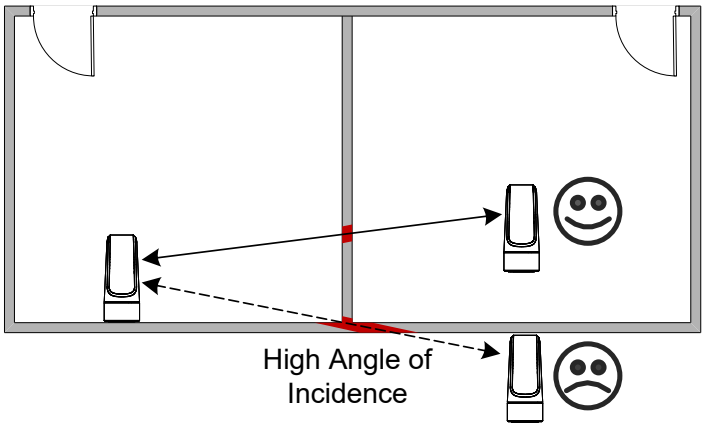


Figure 12: Angle of Radio Waves

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

ECLYPSE Wi-Fi Adapter Mounting Tips

This section provides information and examples on how to properly position the Wi-Fi Adapter to ensure reliable wireless communication. The most common guidelines to remember when installing the Wi-Fi Adapter is to keep it at least 1” (2.5 cm) away from metal, and never install the 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 Wi-Fi Adapter on a metal relay panel or utility box with a controller inside the panel/box. To maximize wireless range, the Wi-Fi Adapter must be installed on the top or side of the panel.

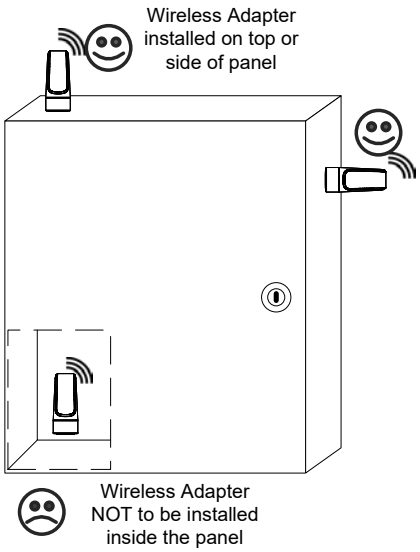


Figure 13: Wi-Fi Adapter Position with Metal Relay Panel/Utility Box

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.

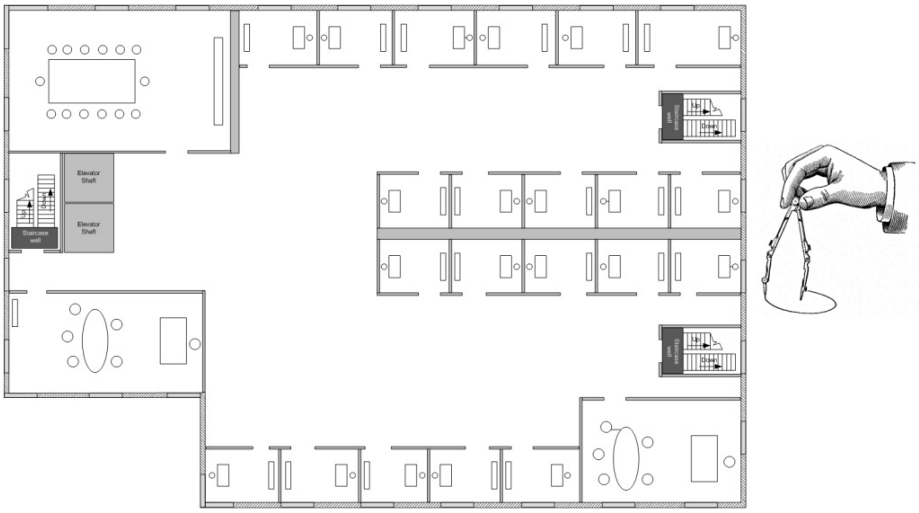


Figure 14: Copy of floor plan and a compass

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

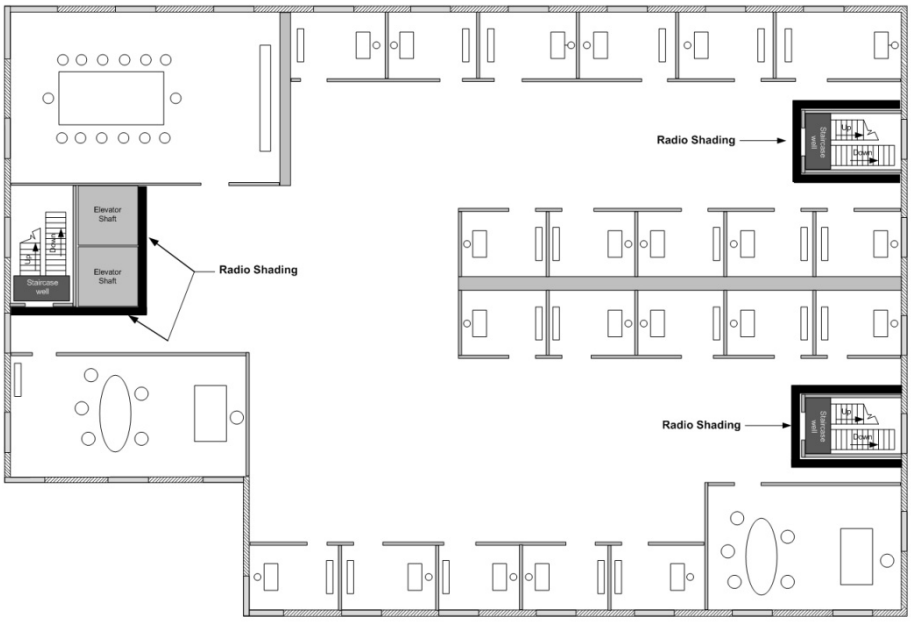


Figure 15: Mark relevant radio shadings

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

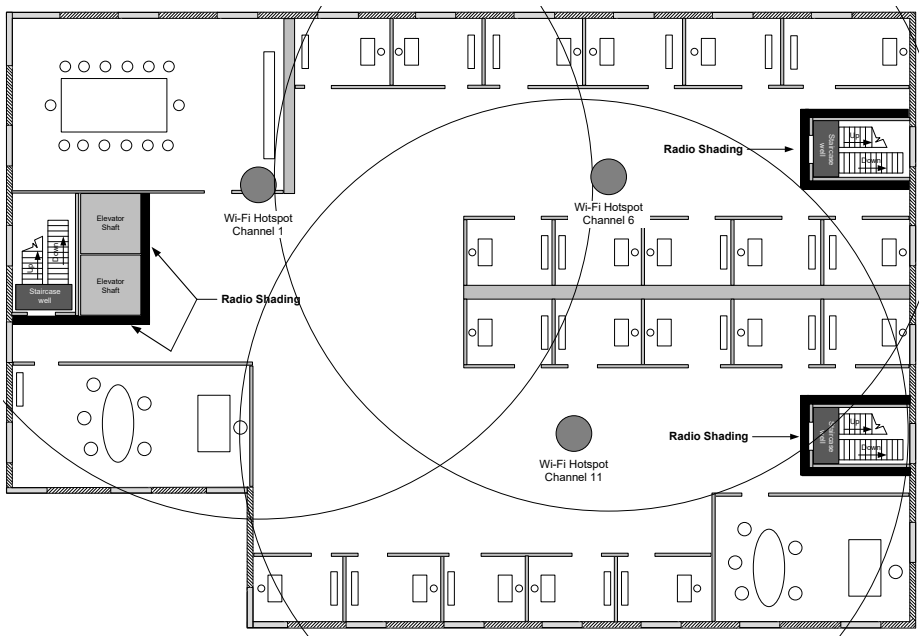


Figure 16: Radio Wi-Fi Adapter Location

Make sure that the 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 conditions should 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 Wi-Fi Adapter positions. Unfavorable conditions can be improved by changing the antenna position or by adding a router closer to the controller(s).

ECLYPSE Wi-Fi Adapter Connection Modes

The 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 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.	16
Access Point	This sets the mode of the 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 network 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 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.

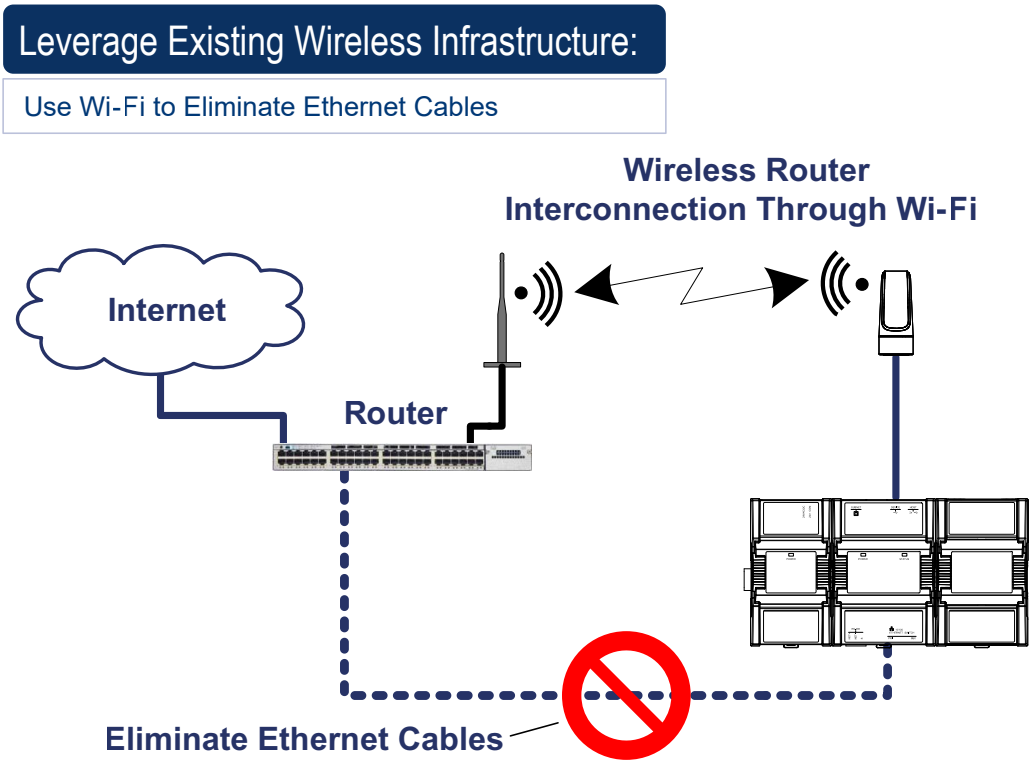


Figure 17: Leveraging Existing Wireless Infrastructure by Eliminating Ethernet Cables

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 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 Wi-Fi adapter can also be temporarily added to a controller for wireless commissioning purposes. A variety of software applications are available for system monitoring and override, commissioning, configuration and programming. To configure the Wi-Fi access point connection mode, see *Setting up a Wi-Fi Access Point Wireless Network*.

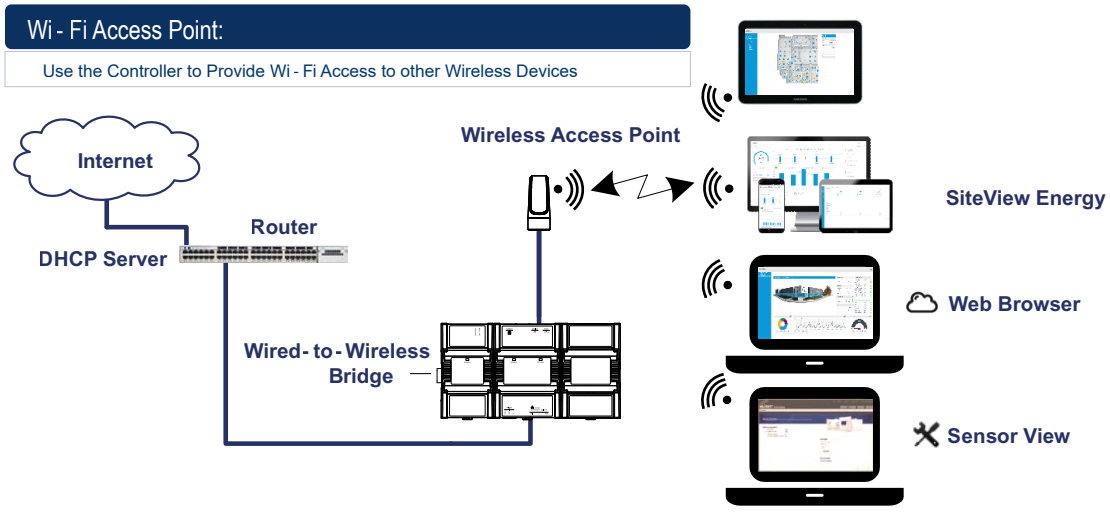


Figure 18: Using an ECLYPSE Controller to Create an Access Point

A second 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 Access Point Wireless Network*.

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

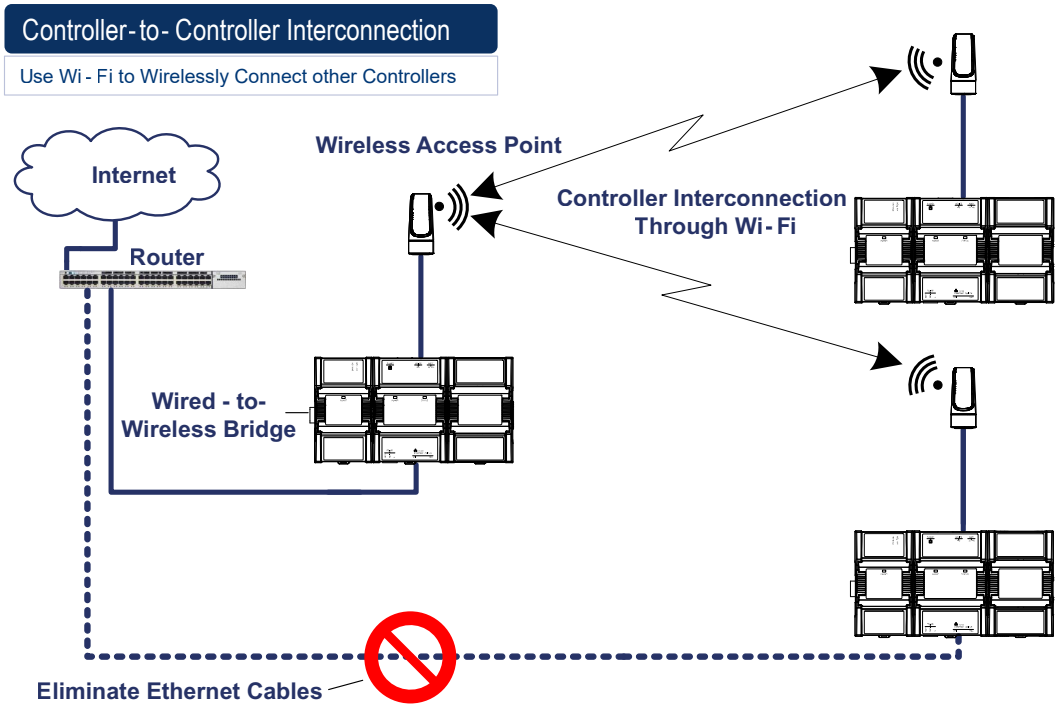


Figure 19: Using an ECLYPSE Controller as a Wireless Bridge

Wi-Fi Hotspot

Should the wired network not use a DHCP server (uses fixed IP addresses); an 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 a Wi-Fi adapter is connected to an ECLYPSE controller. The Wi-Fi adapter can also be temporarily added to an ECLYPSE controller for wireless commissioning purposes. A variety of software applications are available for system monitoring and override, commissioning, configuration and programming. To configure the Wi-Fi hotspot connection mode, see *Setting up a Wi-Fi Hotspot Wireless Network*.

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.

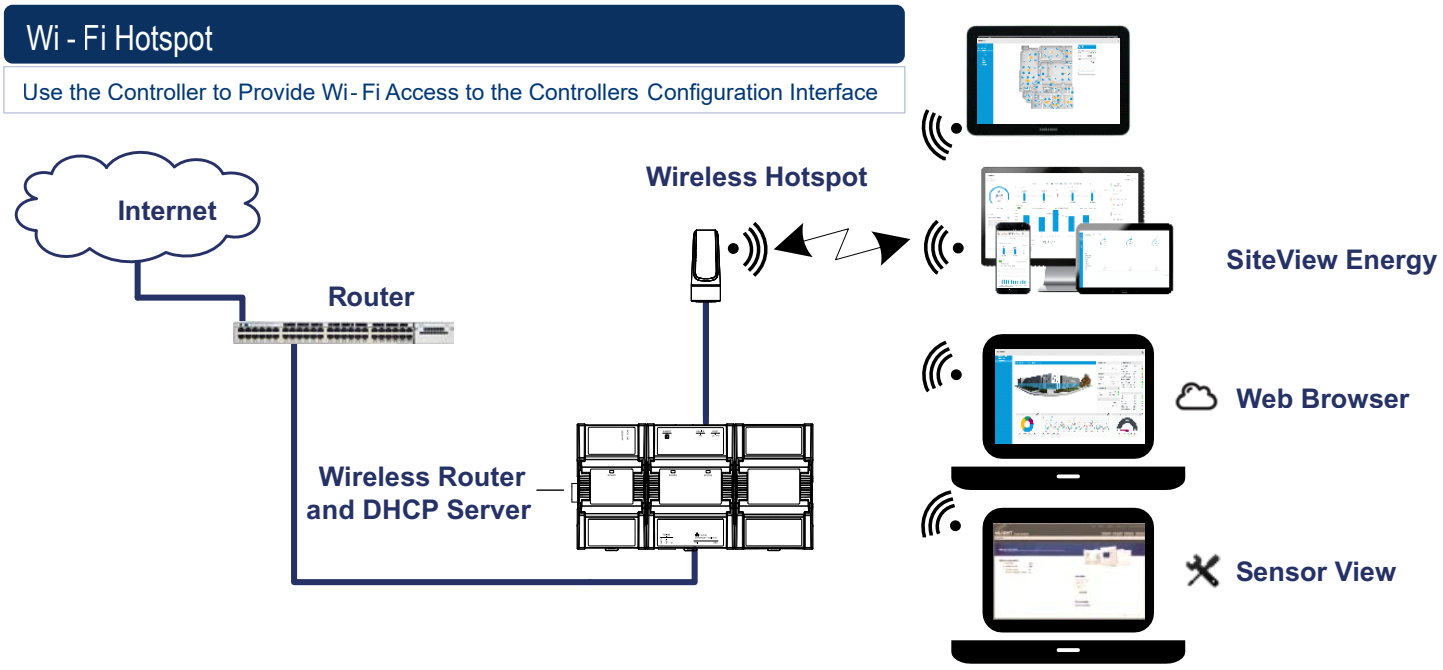


Figure 20: Using an ECLYPSE Controller to Create a Hotspot

Wireless Bridge

A second 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.

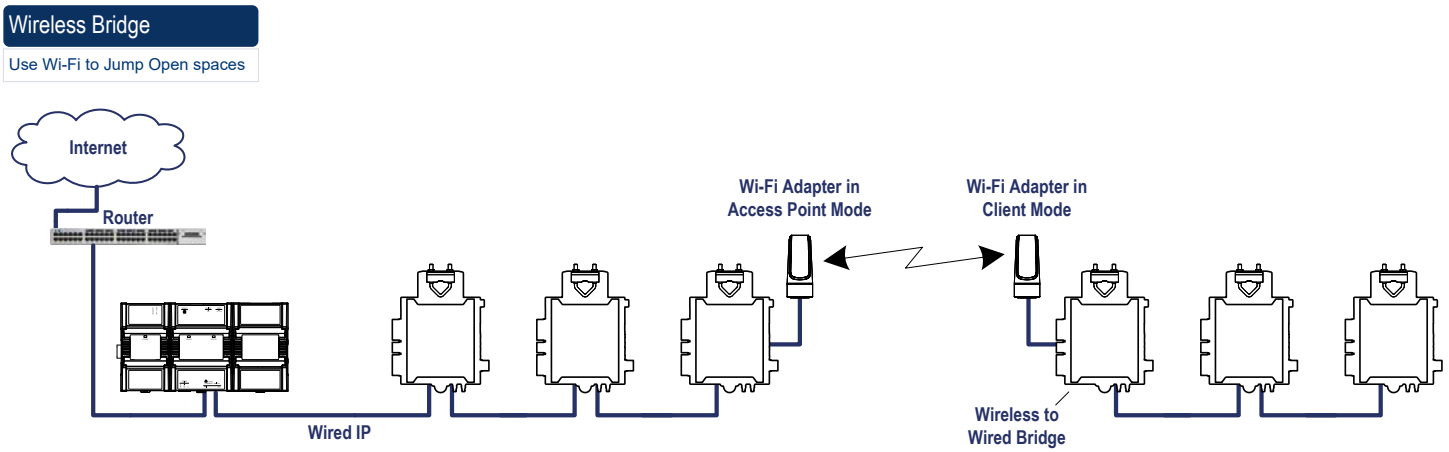


Figure 21: Using an ECLYPSE Controller as a Wireless Bridge

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:

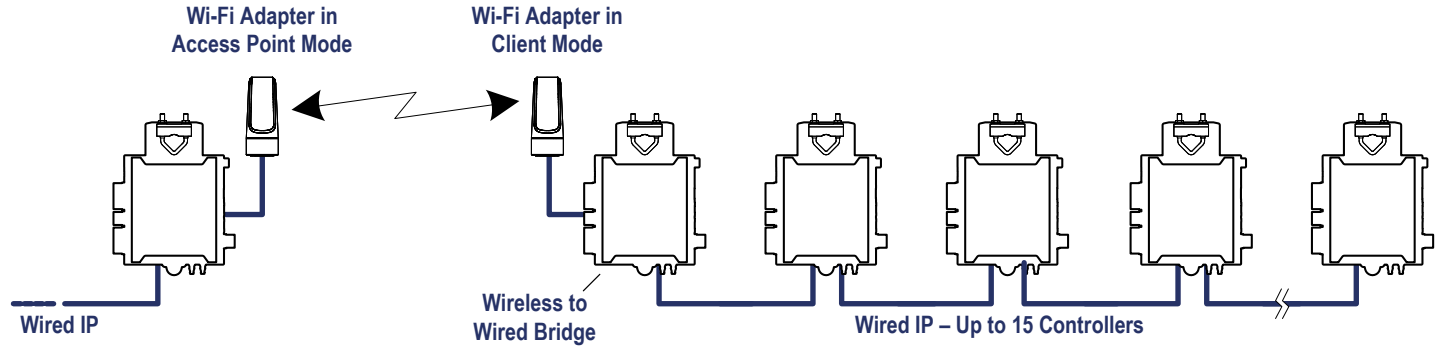


Figure 22: Using an ECLYPSE Controller as a Wireless Bridge

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

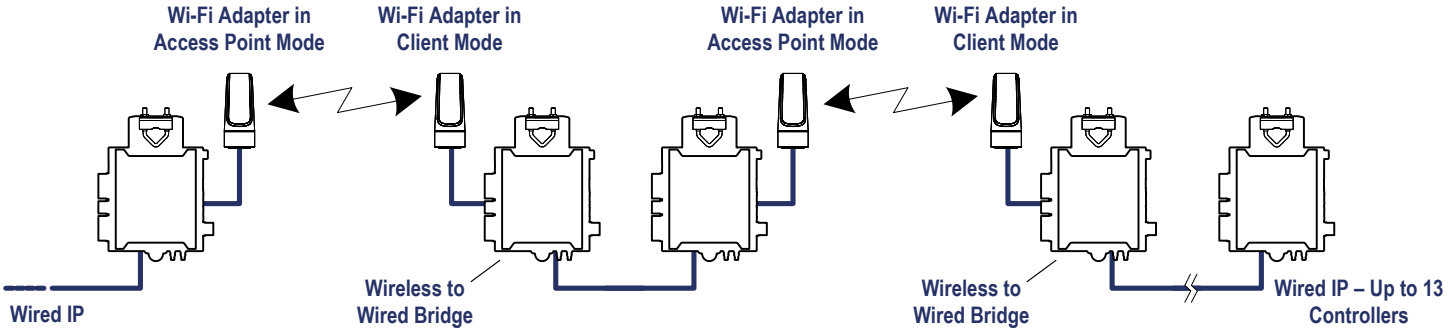


Figure 23: Using an ECLYPSE Controller as a Wireless Bridge

- 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.

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 Connected VAV controller that has its wireless settings configured as an Access Point. The other ECLYPSE Connected VAV controllers are configured as Wi-Fi Clients and are wirelessly connected to the same Access Point.

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

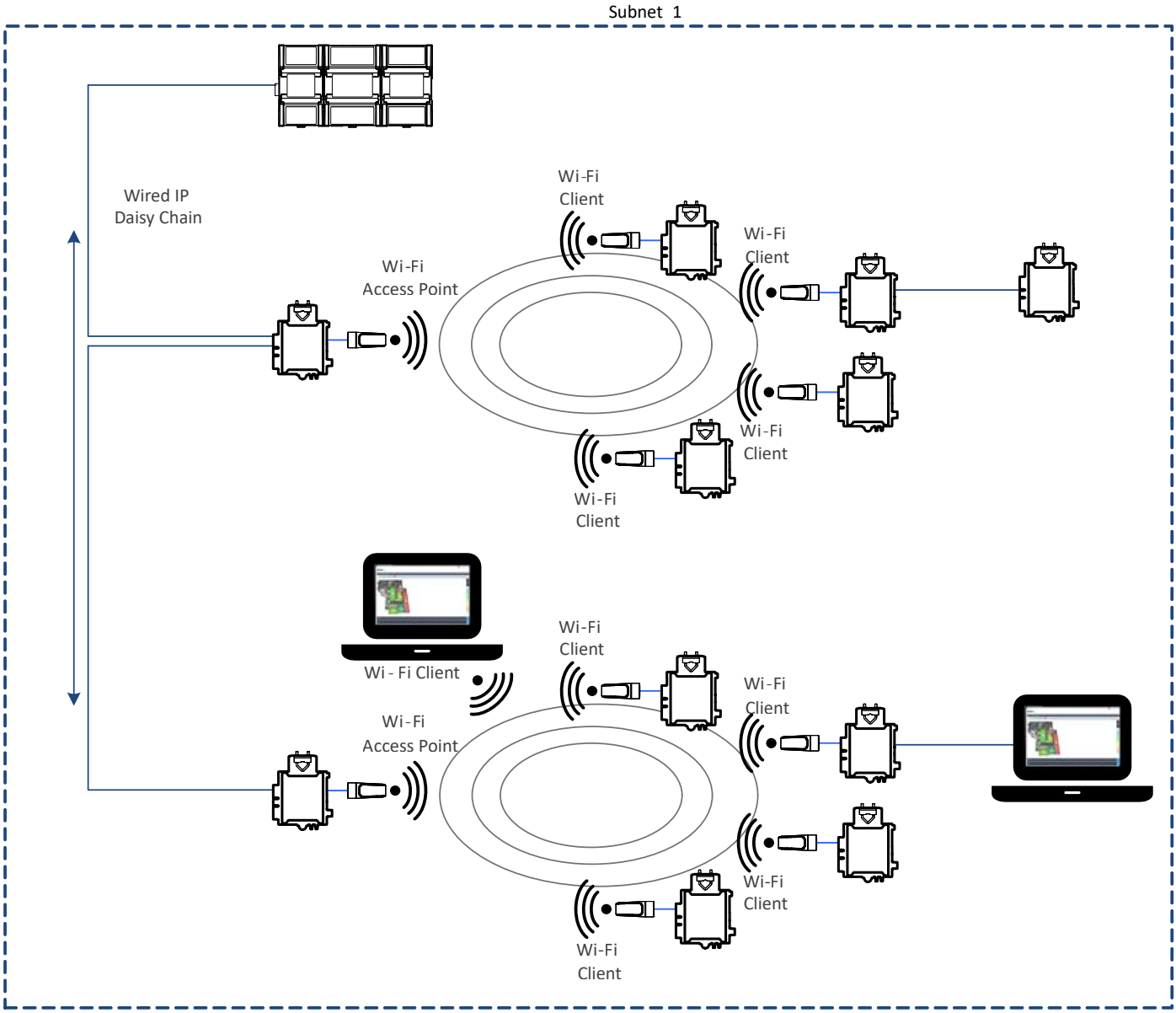


Figure 24: Client to Access Point Configuration

Client to Hotspot Configuration

Laptop 1 is connected as a Wi-Fi client to an ECLYPSE Controller that has its wireless settings configured as a Hotspot (Subnetwork 2). The ECLYPSE Connected VAV 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 Connected VAV 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 ECLYPSE 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 on its same subnet. 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 Connected VAV 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).

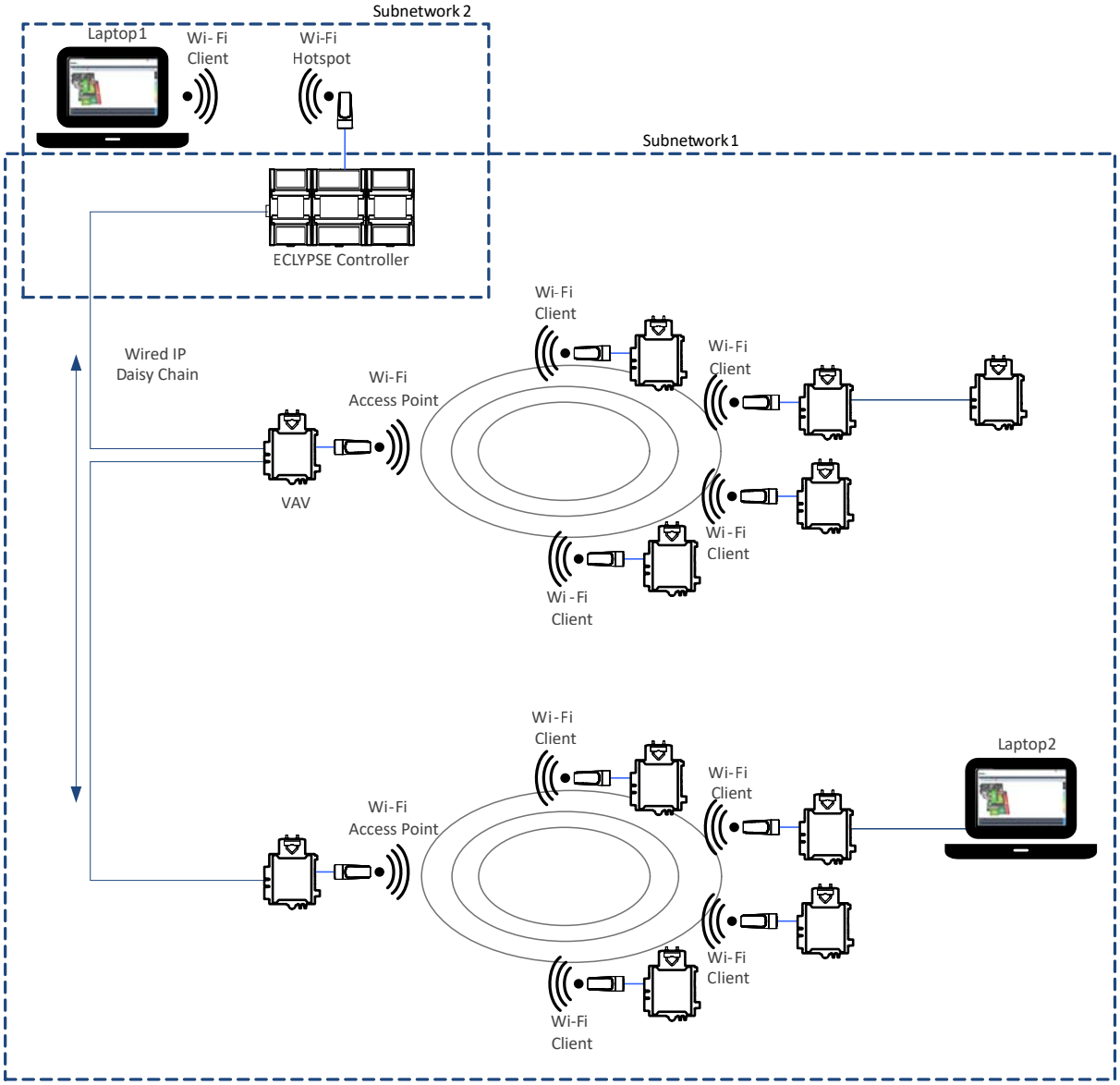


Figure 25: Client to Hotspot Configuration

CHAPTER 6
First Time Connection to an ECLYPSE Controller

This chapter describes how to get started with an ECLYPSE controller. This includes connecting to the factory-default IP address to gain access to the controller's configuration interfaces.

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.

The ECLYPSE Controller configuration can be made through the controller's configuration Web interface that is accessed either through a direct ethernet connection to a PC, or via Wi-Fi connection. This Web interface is used to set all the controller's configuration parameters including the controller's IP address according to your network planning. See *ECLYPSE Web Interface*.

There are two networking methods to connect to a controller:

- Wired (Ethernet connection) with a PC.
- Wireless (when the Wi-Fi Adapter is connected to the controller) 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.

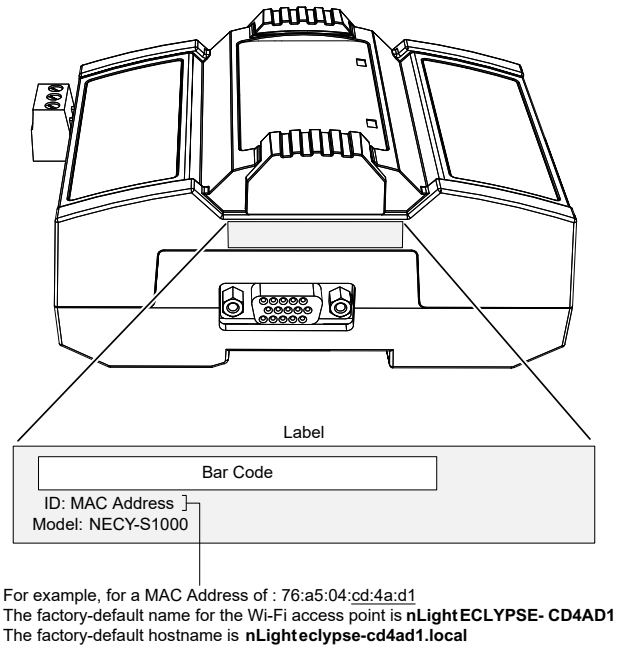


Figure 26: Finding the Controller's MAC Address

Ethernet Network Connection

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 ECLYPSE Controllers*.

See also Connecting IP Devices to an IP Network for network wiring considerations.

Network Connections for ECLYPSE 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.

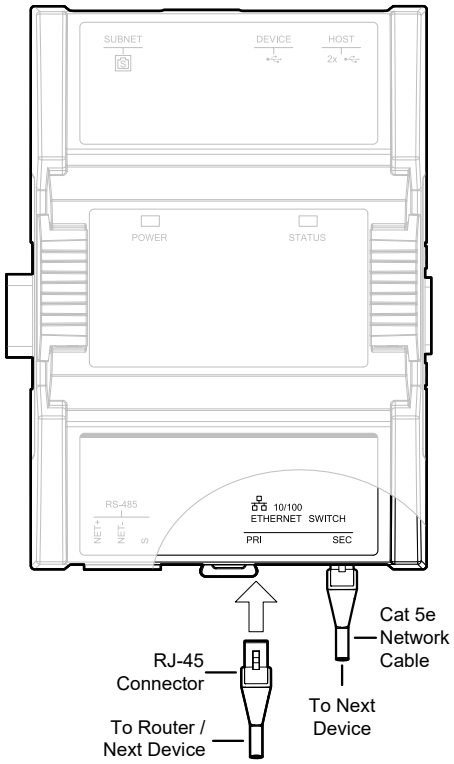


Figure 27: nLight ECLYPSE Wired Network Connection: Cat 5e Cables with RJ-45 Connectors are used

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 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 **ECLYPSE-XXYYZZ** where **XXYYZZ** are the last 6 hexadecimal characters of the controller'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.

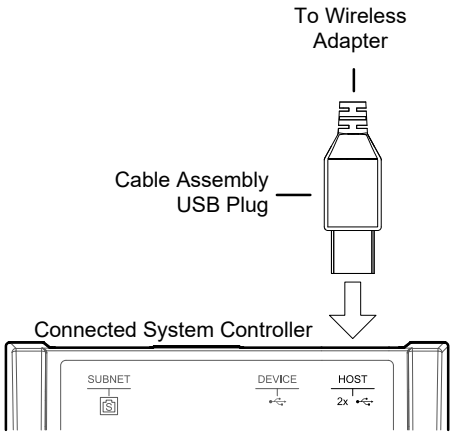


Figure 28: Connecting the Wireless Adapter to the Controller's USB HOST Port

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

Default Credentials

If this is a first-time connection to an ECLYPSE controller, or if the controller has been reset to factory default settings, you must use the default username and password.

- **Default username:**admin
- **Default password:** admin

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. The hostname can be used in a Web browser's address bar. 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. Log in 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. Log in 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*.

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).

4. Open your Web browser.
5. In the Web browser's address bar enter the controller's IP address and click go.
6. Log in 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 ECLYPSE 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 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. See *User Management*, *Securing an ECLYPSE Controller*, *Supported RADIUS Server Architectures*.

Next Steps

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

CHAPTER 7
Supported RADIUS Server Architectures

A RADIUS server is used to centralize user credentials (controller login username / password) across all devices. This chapter describes the supported RADIUS server architectures and how to configure a RADIUS server in an ECLYPSE controller.

Overview

When network connectivity allows, a user can connect directly to an ECLYPSE controller. No matter the connection method, a user has to authenticate themselves with their user credential (controller login username / password combination).

When a user connects to an ECLYPSE controller, the ECLYPSE controller connects to the remote RADIUS server to authenticate the user's credential. A RADIUS server uses a challenge/response mechanism to authenticate a user's login credentials. An unrecognized username or a valid username with an invalid password receive an 'access denied' response. A remote RADIUS server can be another ECLYPSE controller, or a Microsoft Windows Domain Active Directory Server.

Authentication Fallback

Should the connection to the remote RADIUS server be temporarily lost, ECLYPSE controllers have a fall back authentication mode: users that have already authenticated themselves with the remote RADIUS server and then the connection to the RADIUS server is lost, these users will still be able to log in to the controller as their successfully authenticated credentials are locally cached.

The user profile cache is updated when the user authenticates themselves while there is a working RADIUS server connection. For this reason, at a minimum, admin users should log in to each ECLYPSE controller at least once, so their login can be cached on that controller. Otherwise, if there is a RADIUS server connectivity issue and a user who has never before connected to the ECLYPSE controller will be locked out from the controller. It is particularly important for admin user credentials to be cached on each controller as an admin user can change the controller's network connection parameters that may be at cause for the loss of connectivity to the RADIUS server.

RADIUS Server and Enabling FIPS 140-2 Mode

On a project where the controllers have FIPS 140-2 mode enabled, a third-party Radius server cannot be used. If the use of a Radius based authentication is required, an ECLYPSE controller must act as the Radius server. In addition, third party Radius clients will not be able to connect to the ECLYPSE Radius server. For more information, see *FIPS 140-2 Mode*.

RADIUS Server Architectures

Local Credential Authentication

Each device has its own credential database in the local credential authentication architecture. This approach is labor-intensive as multiple credential database instances must be maintained.

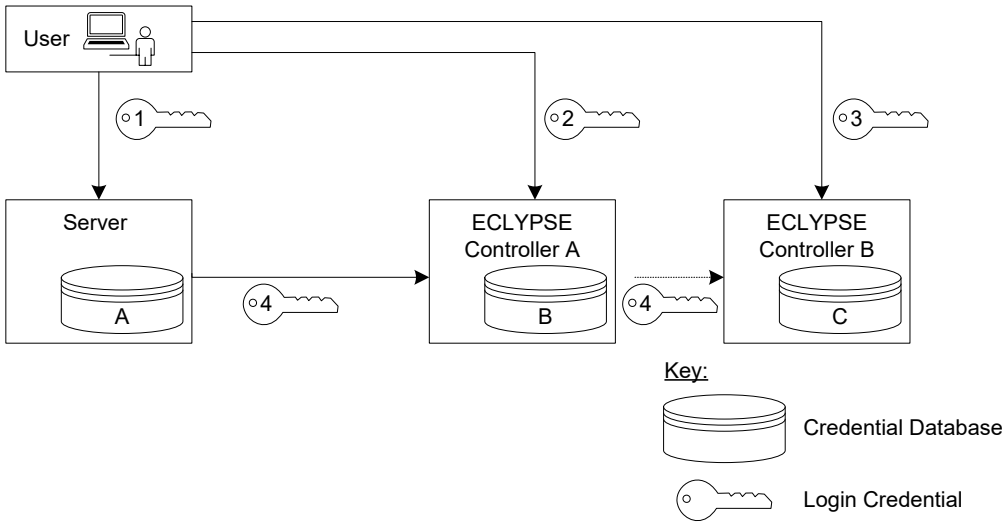


Figure 29: Local Credential Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by a user to connect to the Server station. This credential is managed by the Server.
Login Credential 2	This is the login credential used by a user to connect to ECLYPSE controller A. This credential is managed in controller's A *User Management* credential database.
Login Credential 3	This is the login credential used by a user to connect to ECLYPSE controller B. This credential is managed in controller's B *User Management* credential database.
Login Credential 4	This is the login credential used by the Server's Rest Service to connect to ECLYPSE controller A and B. This credential is managed in this controller's A and B *User Management* credential databases.
Credential Database A	This is the Server's user credential database.
Credential Database B and C	This is the ECLYPSE controller A's credential database and ECLYPSE controller B's credential database. If the User can to connect to either of these controllers through the Server, the controller's credential database must have the credentials for the Server's RestService. Each credential database must also have the credentials for each user that will log in to ECLYPSE controller A (for example, administrators, direct connection by users, ENVYSION users, etc.). See *User Management*.

ECLYPSE-Based Centralized Credential Authentication

The credential database is centralized in an ECLYPSE controller that is configured as a RADIUS server, to authenticate login requests made directly to it, and by other subscribed ECLYPSE controllers.

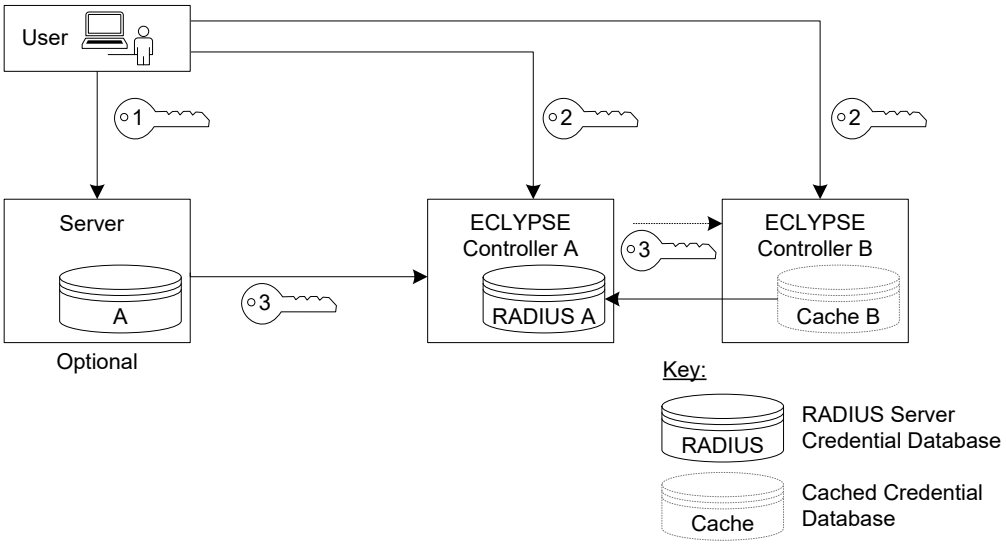


Figure 30: ECLYPSE-Based Centralized Credential Authentication

This authentication method has the following components.

Component	Description
Login Credential 1	This is the login credential used by a user to connect to the Server. This credential is managed by the Server.
Login Credential 2	This is the login credential used by a user to connect to ECLYPSE controller A. This credential is managed in controller's A *User Management* credential database.
Login Credential 3	This is the login credential used by the Server's Rest Service to connect to any ECLYPSE controller. This credential is managed in this ECLYPSE controller A's *User Management* RADIUS server credential database.
Credential Database A	This is the Server's user credential database. This credential database is independent of all other credential databases.
RADIUS Server A Credential Database	This is the ECLYPSE controller A's RADIUS Server credential database. This credential database must also have the credentials for each user that will log in to any ECLYPSE controller (for example, administrators, direct connection users, ENVYSION users, etc.). See *User Management*.
Credential Database Cache B	This is the ECLYPSE controller B's cached credential database. If the connection to ECLYPSE controller A's RADIUS Server is lost, users that have previously authenticated themselves with the ECLYPSE controller A's RADIUS Server credential database on a given controller will still be able to log in to those controllers as their credentials are locally cached.

CHAPTER 8
ECLYPSE Web Interface

This chapter describes the ECLYPSE controller's Web interface.

Overview

The ECLYPSE controller has a web-based interface that allows you to view system status, configure the controller, update the controller's firmware, and access 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*.

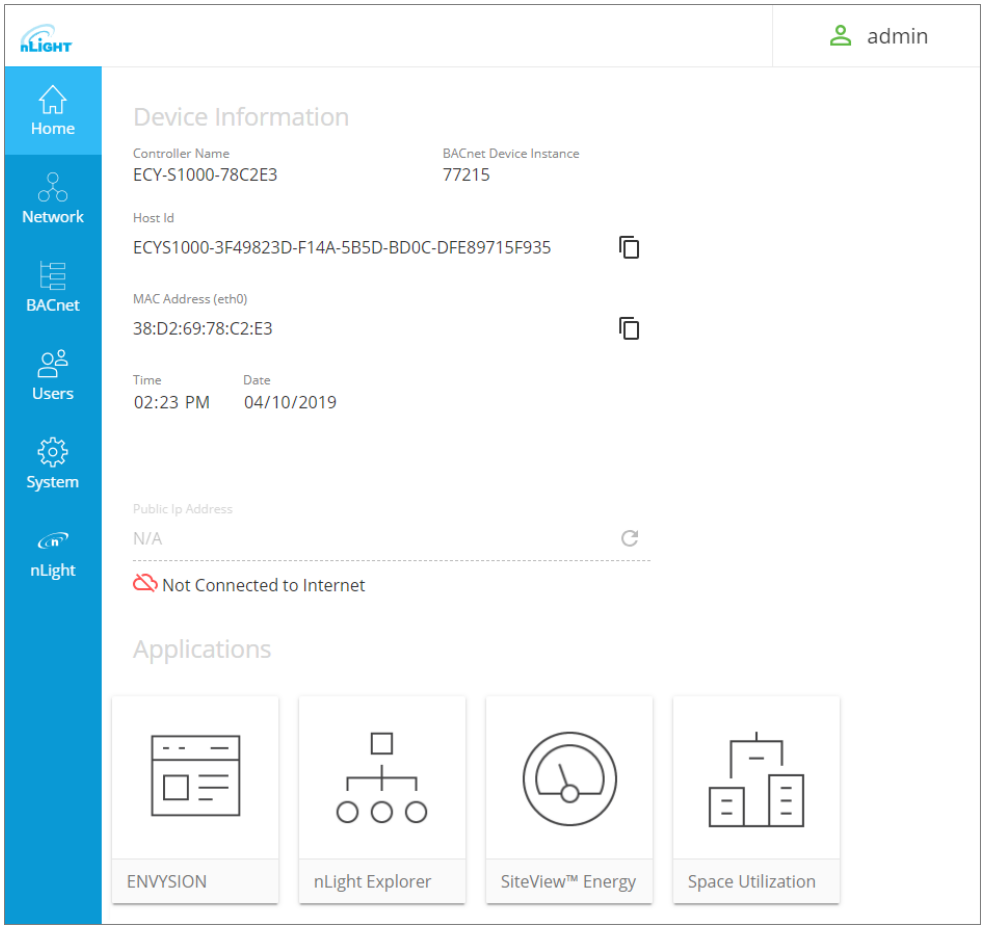


Figure 31: Example of an ECLYPSE Controller's Web Interface Welcome Home Page (options may vary)

Web Interface Main 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, users, controller's firmware, and much more.

The menus may vary according to the associated device licenses and the user's access level. These configuration parameters are password protected.

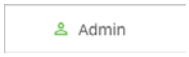
Home Page

The web interface home page consists of the following items:

Item	Description
Device Information	Basic information on the device such as controller name, device instance, host ID, MAC address, time, and date
	Copy icon that allows you to copy the Host Id and/or the MAC address of the device to that you can quickly paste elsewhere as needed
Public IP Address	IP address to access your ECLYPSE controller from a public network (e.g. Internet)
Connected/Not Connected to Internet	ECLYPSE controller Internet connection status
Applications	Access different applications associated to your projects and controller license such as the following: – **ENVYSION**: Embedded graphic design and visualization interface. Host system-based graphics for lighting control systems and more, directly from the controller. See the ENVYSION User Guide. – **Space Utilization:** The Space Utilization edge application allows building owners and property managers to analyze where occupants spend their time throughout the day, to make data-driven decisions for renovation, space planning and other expansions. – **SiteView™ Energy:** The energy metering edge application gives building owners real-time, actionable data about their facility's energy consumption, making it easier to identify usage trends and savings. – **nLight Explorer:** An edge application that gives a general system overview and system health of connected nLight devices.

User Profile and Login Credentials

It is important to create new user accounts with strong passwords to protect the controller from unauthorized access.

The profile box 

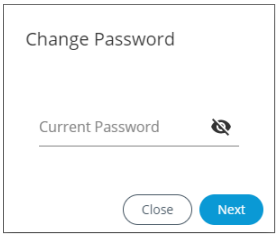
is used to change your password and logout from your ECLYPSE controller.

On your first login to an ECLYPSE controller, you will be prompted to change the factory default password. We recommend you choose a strong password for the 'admin' account as it gives full control over the controller.

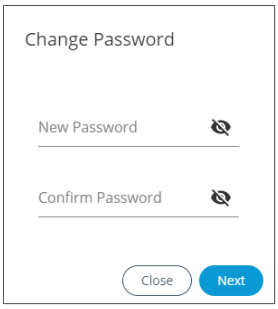
See *User Management*, *Securing an ECLYPSE Controller*, and *Supported RADIUS Server Architectures*.

To Change Your Password

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

Click the show password icon to see the password you are entering.

Network Settings

The **Network** menu is used to configure the ECLYPSE controller's network interface and setup 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 *Network Connections for ECLYPSE Controllers*. 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.

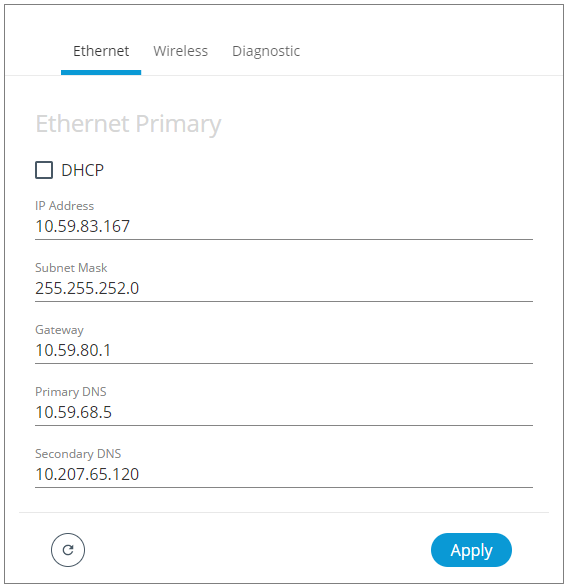


Figure 32: Primary Ethernet Configuration in ECLYPSE Web Interface

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	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	Subnet mask provided by the network's DHCP server	Set the connected network's subnetwork mask. See *About the Subnetwork Mask*.
Gateway	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	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 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.

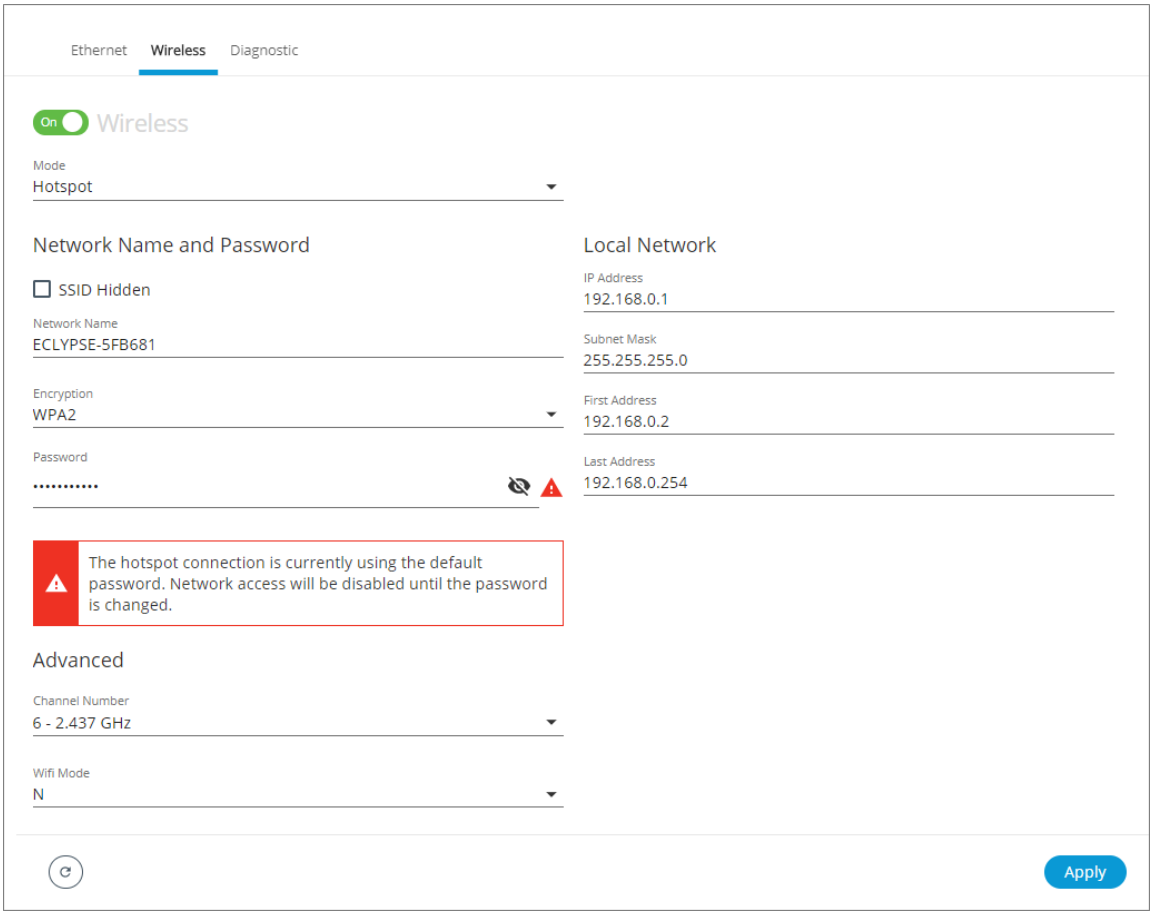


Figure 33: The Wi-Fi network operating modes: Hotspot, Access-Point, or Client.

The Wireless connection parameters can be set as follows.

Item	Description
On / Off 	Enable/disable 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 hotspot 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 configure 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 *ECLYPSE Wi-Fi Adapter Connection Modes*.
SSID Hidden	Hide or show the Service Set IDentification (SSID)
Network Name	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 the list of 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. – **WPA2E**: Use this option if you are connecting to an enterprise network that has a working RADIUS authentication server. This RADIUS server provides user authentication.
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.  If using a Hotsopt connection, network access will be disabled until the default password is changed. If using an Access Point connection, the default password must be changed before you can save and apply your changes to this page.
	Click to show or hide the password.
IP Address	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	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 hotspot is to use. The wireless mode can also be set. See below.
Channel Number	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-Fi Mode	Sets the wireless mode (wireless G or wireless N). Wireless N mode is backwards compatible with wireless G and B. Wireless G mode is backwards compatible with wireless B.
	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.

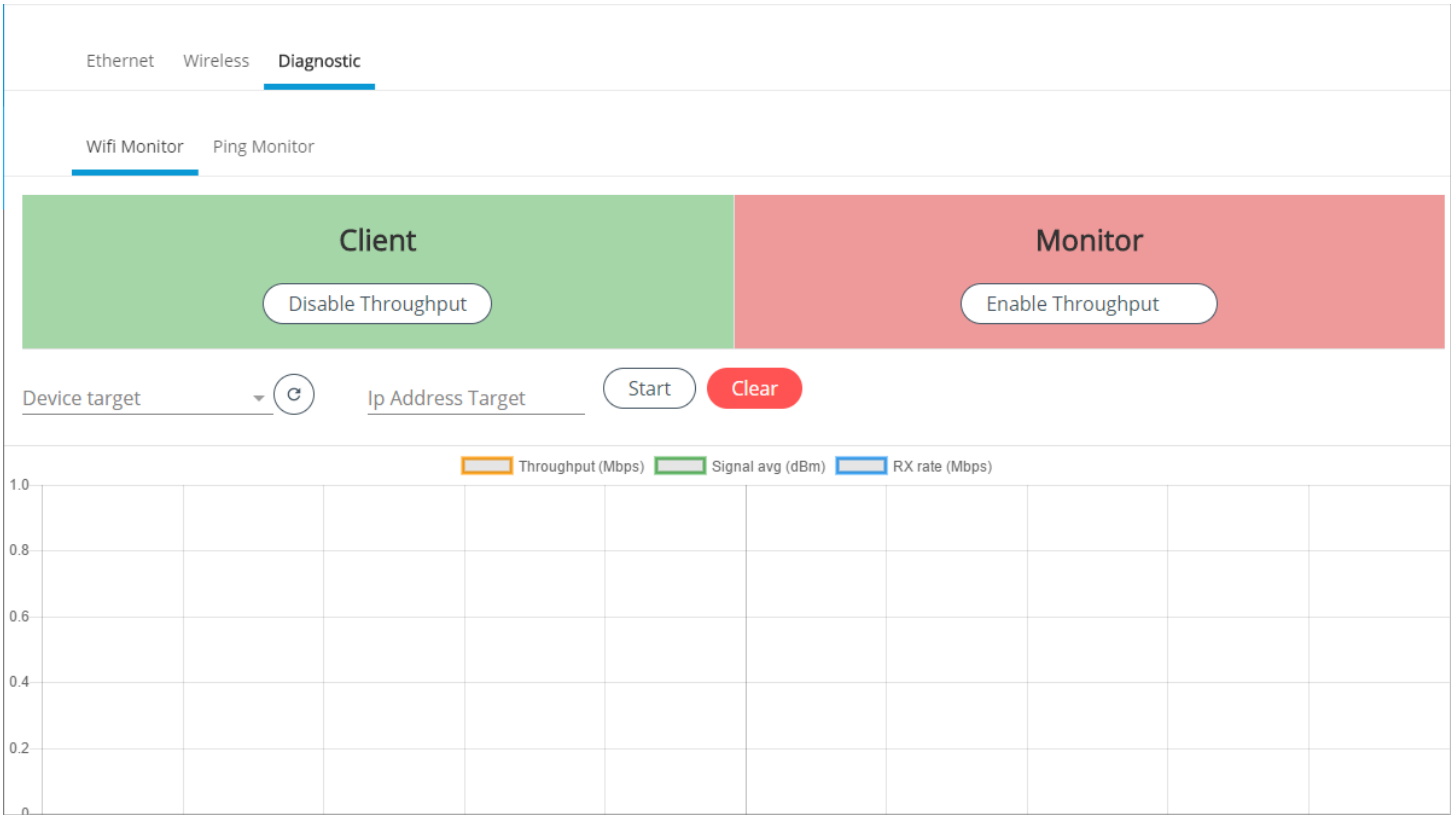


Figure 34: Network Diagnostics – Wi-Fi Monitor

Item	Description
Disable Throughput	Disables the Wi-Fi Monitoring throughput client service. For Wi-Fi monitor to work, this must be started.
Enable Throughput	Activates the Wi-Fi Monitoring throughput client service. For Wi-Fi monitor to work, this must be started.
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)	Transmit datarate to the target
Signal avg (dBm)	Current average received 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)	Receiving data rate from the target

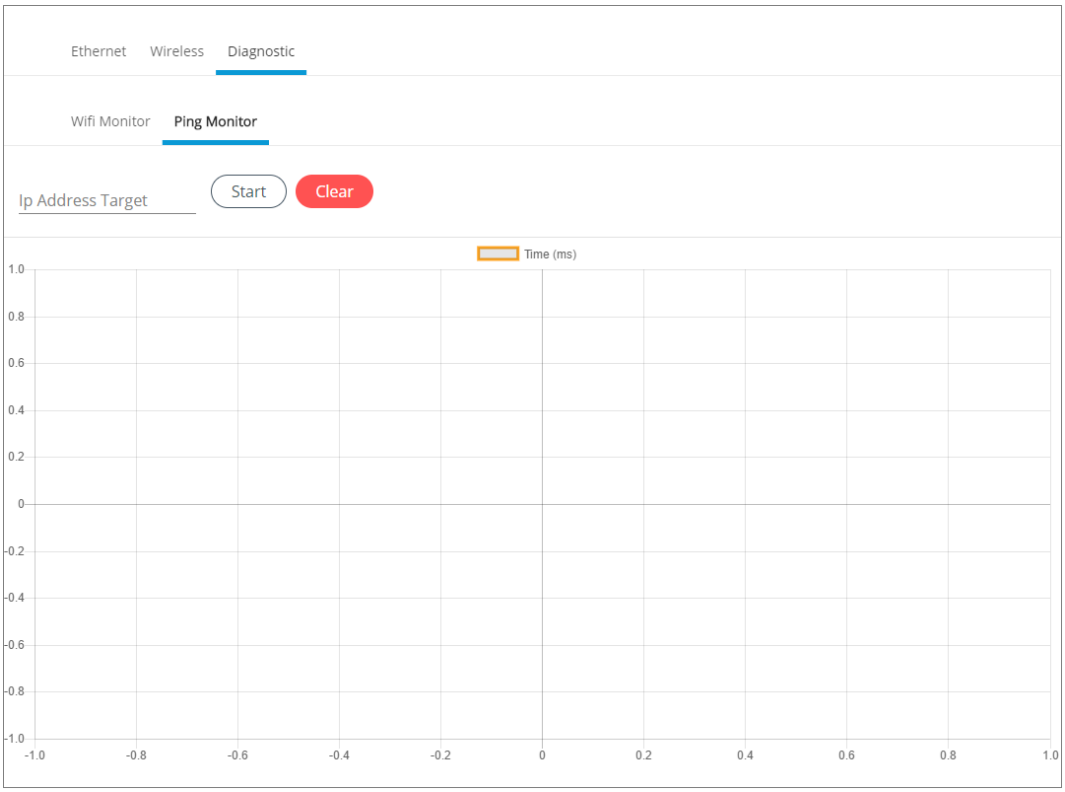


Figure 35: Network Diagnostics – Ping Monitor

Item	Description
Ip Address Target	Enter the corresponding controller's IP address for its Wi-Fi interface in **Ip Address Target**.
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.

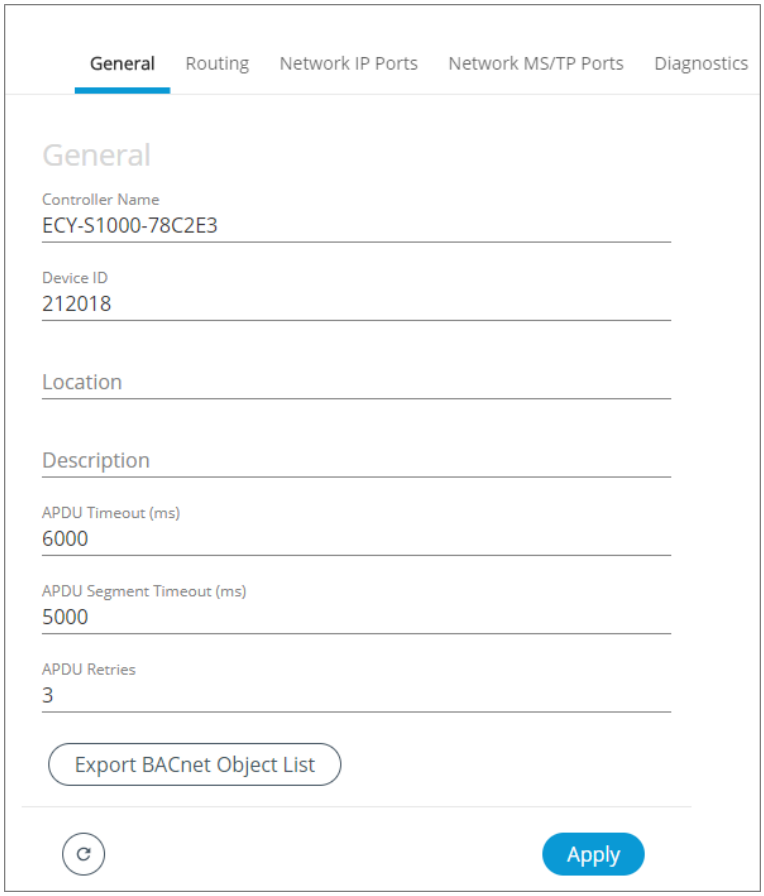


Figure 36: General BACnet Settings

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.
Location	Current controller's physical location. This is exposed on the BACnet network as a device object property.
Description	Description of the controller's function. This is exposed on the BACnet network as a device object property.
APDU Timeout (ms)	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.
APDU Segment Timeout (ms)	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	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.
Export BACnet Object List	Export all controller BACnet variables to a file (.csv).
	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 ECLYPSE Controller's RS-485 port and BACnet/IP controllers connected to the ECLYPSE Controller's Ethernet Switch ports. For example, routing must be enabled for a Server to discover the BACnet MS/TP controllers connected to the ECLYPSE Controller's RS-485 port.

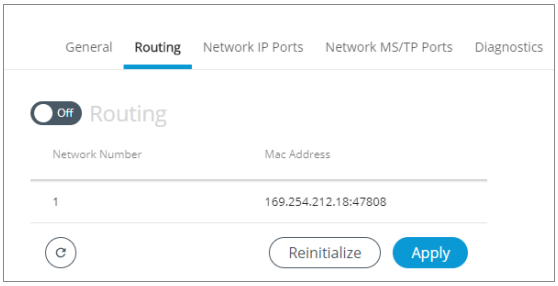


Figure 37: BACnet Routing Configuration

Item	Description
On / Off 	Enables/disable the routing of BACnet packets between BACnet MS/TP controllers connected to the ECLYPSE Controller's RS-485 port and BACnet/IP controllers connected to the ECLYPSE Controller's Ethernet Switch ports.
Network Number	Network number that 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	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-board port) as well as the BACnet Broadcast Management Device (BBMD) and Foreign Device for intranetwork connectivity.

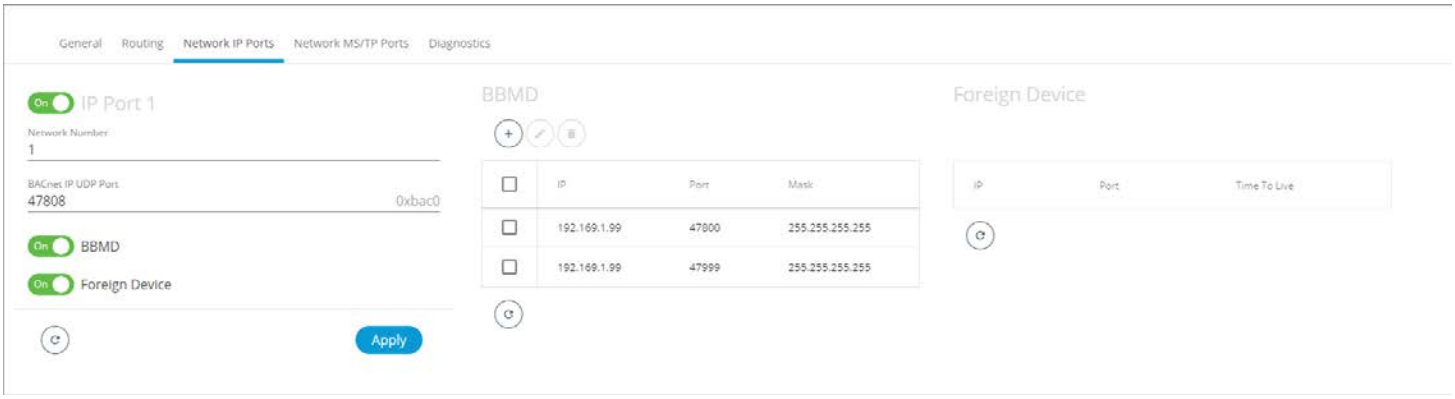


Figure 38: BACnet IP Configuration - Network IP Ports

On-Board Port

Item	Description
On / Off 	Enables/disables the routing of BACnet packets between BACnet MS/TP controllers connected to the ECLYPSE Controller's RS-485 port and BACnet/IP controllers connected to the ECLYPSE Controller's Ethernet Switch ports.
Network Number	Network number that 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	Standard BACnet/IP port number (UDP 47808) used by BACnet devices to communicate.
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. To add a BBMD:

1. Click  .

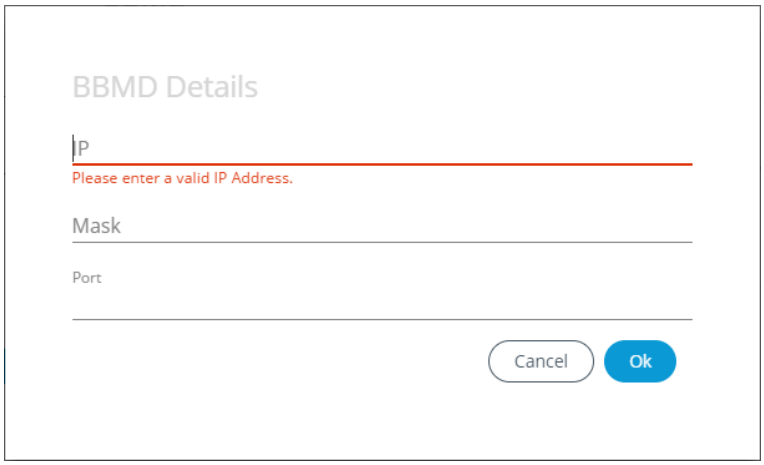


Figure 39: Adding a BBMD

2. In the **IP** field, enter IP address of the BBMD located on the other subnetwork.
3. In the **Mask** field, enter the subnetwork mask 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**.

You can also edit or delete a BBMD selected from the list using the Edit icon  or Delete icon  provided.

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	IP address of a controller (foreign device) located on another subnetwork
Port	Delay after which the foreign device is forgotten
Time to Live	Time-to-live value that serves as a timestamp attached to the data. Once the timespan has elapsed, data is discarded.
	Click to refresh the information in the list.

Network MS/TP Ports

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. The following network configuration parameters are for an RS-485 port that is used to communicate with BACnet MS/TP controllers.

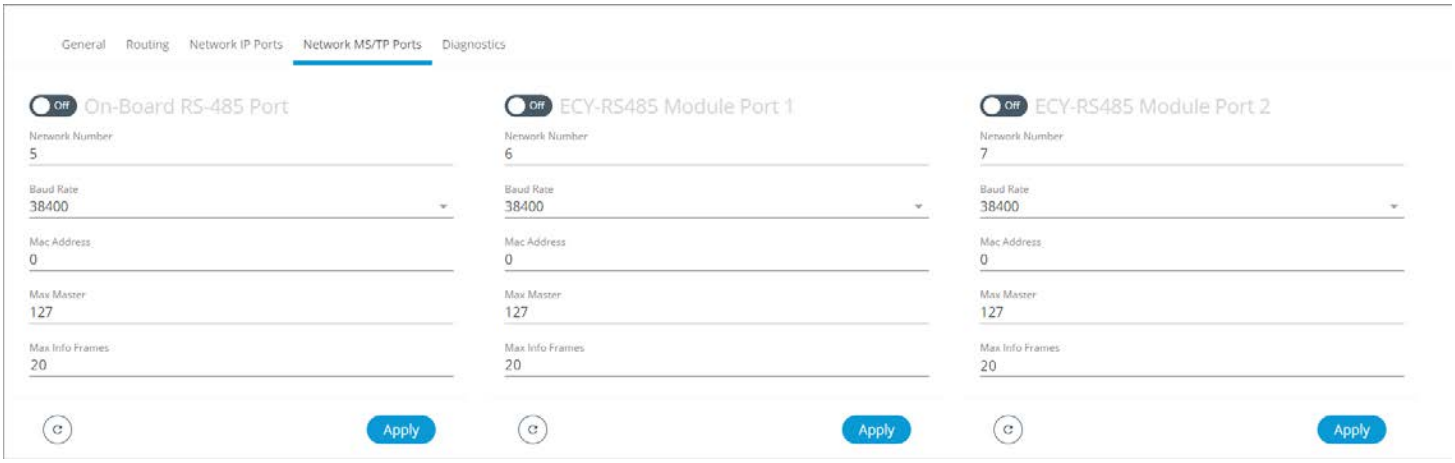


Figure 40: Network MS/TP Ports

Item	Description
On / Off 	Enables/disables the controller's BACnet MS/TP connection. If the controller has been configured to use Modbus RTU, this option cannot be enabled.
Network Number	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	Recommended baud rate setting is 38 400. See *Baud Rate*.
Mac Address	The ECLYPSE 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 ECLYPSE 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.

Diagnostics

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.

The following Diagnostics tab provides information on live values passing through the RS-485 ports. By default, the live values are displayed. You can stop and restart the streaming of the live values using the Stop Live Values/Start Live Values button.

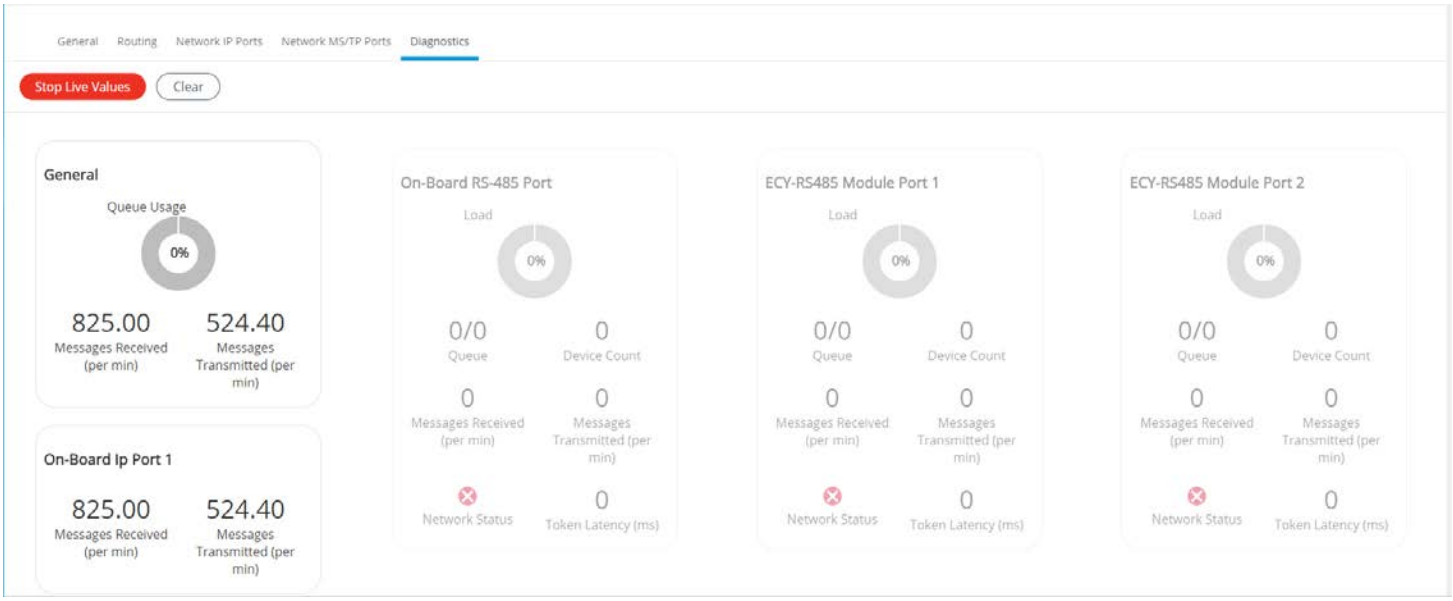


Figure 41: BACnet Diagnostics

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 managed in *Server* or *Client* mode. You can also set the Welcome page a user will land on when they connect to the controller.

An ECLYPSE controller can manage users through several mechanisms. It can either be in *Server* mode that provides a user database to other ECLYPSE controllers and itself, or in Client mode for access to a remote user database.

You can provide appropriate privileges to users depending on the clearance level desired for each role. You can also modify user properties and customize the user experience by assigning a Welcome page to each user.

Server/Client User Configuration

When you configure an ECLYPSE controller in server mode, you can add new users, select their roles, and choose their custom Welcome page. This page will be the default page displayed after a user logs in to an ECLYPSE controller.

If you configure an ECLYPSE controller in client mode, you can only choose the Welcome page displayed to a user. Any other information will be retrieved from the remote server. The Welcome page chosen in client mode has priority over the one configured in the server.

Adding a User in Server Mode

Adding a user creates a user profile that allows a person to log in to the controller with a username / password combination and to have access to certain controller software interfaces. These users will have login access to the controller. It is important to create new user accounts with strong passwords to protect the controller from unauthorized access. See also *Password Policy* and/or *Securing an ECLYPSE Controller*.

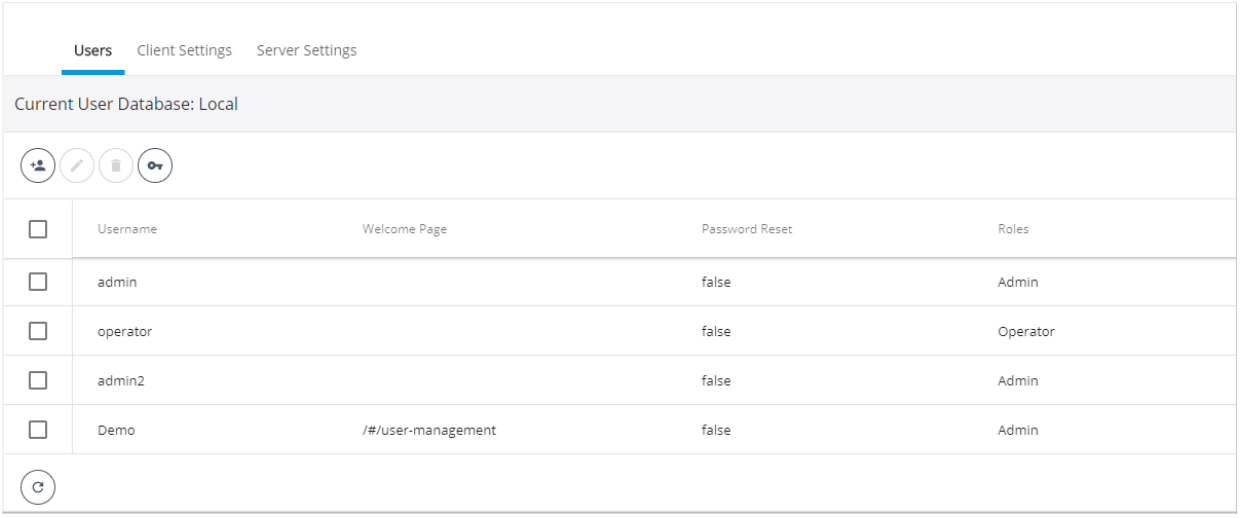


Figure 42: Adding Users in Server Mode

1. Click the Add User icon  to add a new user or select a user and click edit  to edit an existing user. The **User Details** window is displayed.

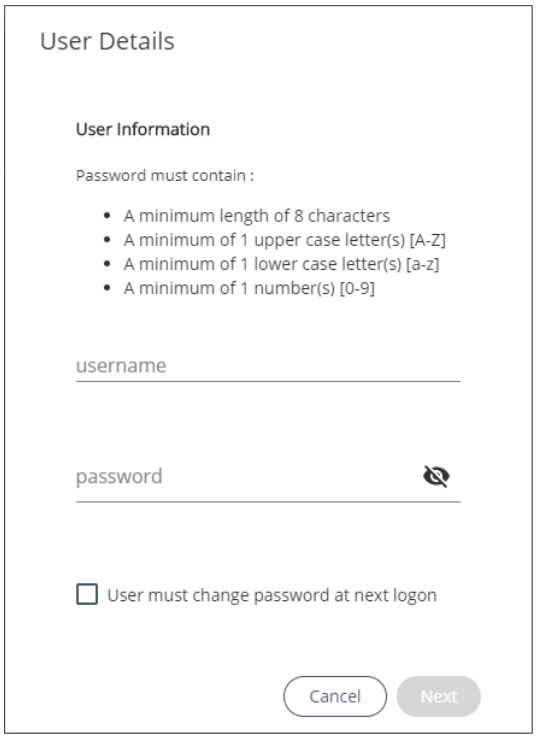


Figure 43: Adding a User

2. Enter the information as shown below:

Item	Description
Username	User's login credential
Password	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.

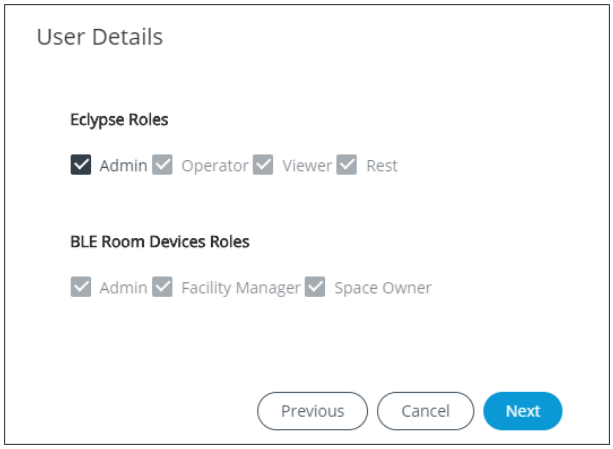


Figure 44: User Details - Roles

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

ECLYPSE Roles	Description
Admin	Allows user access to the ENVYSION studio and viewer. The user can also view and modify all configuration interface parameters. When this option is chosen, the user also receives Admin access for BLE Room Device Roles.
Operator	Allows user access to the ENVYSION interface in viewing mode as well as gives partial access to the 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 ECLYPSE Web Configuration Interface.
Rest	Allows a user to program the controller with a RESTful API enabled programming tool. This user does not have access to the ECLYPSE Web Configuration Interface or ENVYSION.

Table 3: ECLYPSE Roles

BLE Room Device Roles are not available on the nLight ECLYPSE and can be ignored.

5. Click **Next**. The **Welcome Page** screen is displayed allowing you to define the user's landing page that will be displayed when they login to the controller.

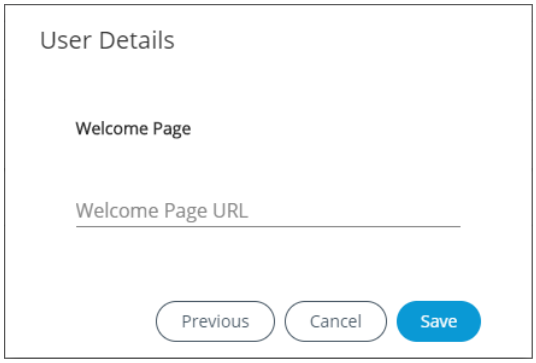


Figure 45: User Details - Welcome Page

6. Enter the URL of the web page you want to define as the landing page. The URL is the one 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 if the address for the user default web page is **HOSTNAME/eclypse/envysion/index.html** OR **192.168.0.10/#/bacnet.html**, remove the hostname or IP Address so that the URL becomes **/eclypse/envysion/index.html**, or **/#/bacnet**.

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

The edit icon is used to 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.

Defining a User Welcome Page in Client Mode

In Client mode, you can only add a Welcome page to your user considering that the rest of the data is stored on the Server, essentially the credentials and roles (see *Adding a User in Server Mode*). This user's Welcome page however will have priority over the page defined in the Server mode.

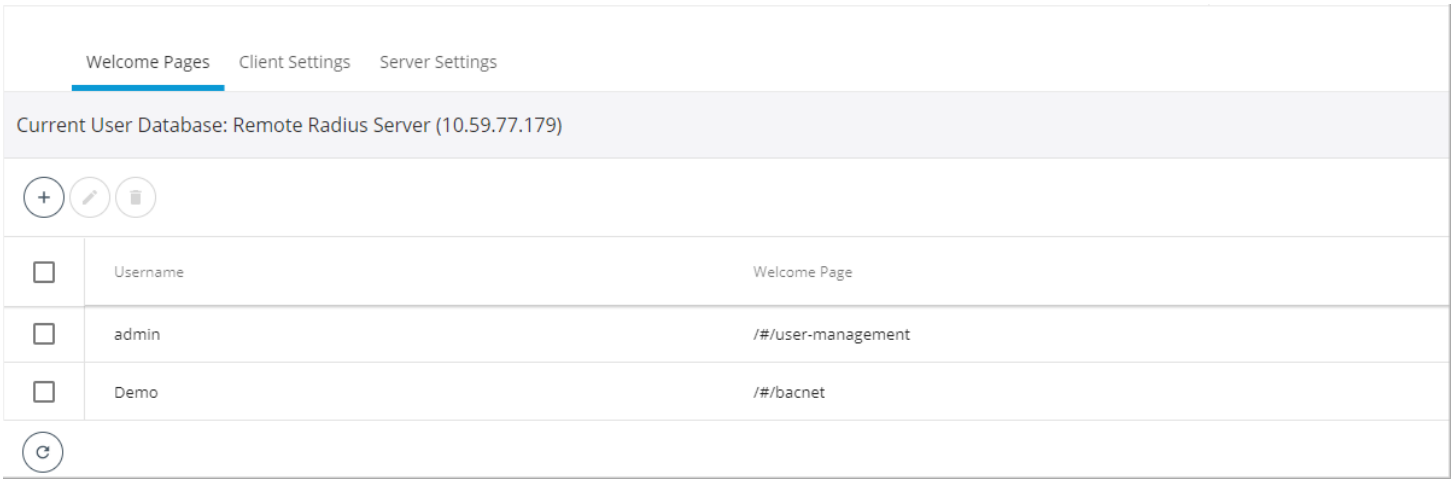


Figure 46: Adding a User in Client Mode

1. Click  to add a user and Welcome page. The **User Details** window is displayed.

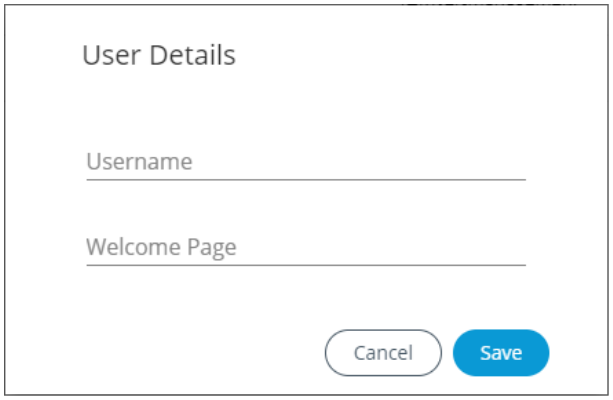


Figure 47: User Details

2. In **Username**, enter the name of the user.
3. In **Welcome Page**, enter the URL of the web page you want to define as the landing page. The URL is the one 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 if the address for the user default web page is **HOSTNAME/eclypse/envysion/index.html** OR **192.168.0.10/#/bacnet**, remove the hostname or IP Address so that the URL becomes **/eclypse/envysion/index.html** or **/#/bacnet**.
4. Click **Save**.

To edit an existing user, select the user from the list and click the edit icon  and to remove, click the delete icon  .

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) it makes the password harder to guess and makes a brute force attack less effective.

Click the key icon to display the **Password Policy** options:

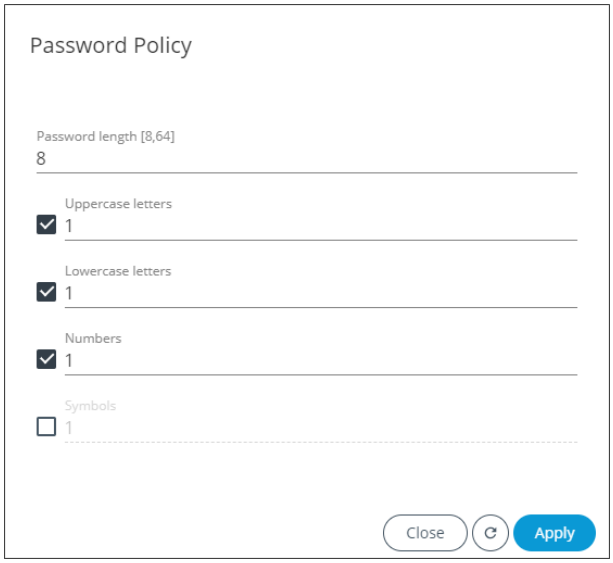


Figure 48: Password Policy Options

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

Radius Server/Client Settings

You can use the network's RADIUS Server for user authentication management.

RADIUS Server Settings

When **Radius Server** is selected in the **Server Settings** tab, this controller can be used as a RADIUS server by other controllers on the network. In this scenario, the other controllers must be configured to use the *Client* **RADIUS Server** mode with this controller's IP address. This centralizes access management on this controller thereby saving time by eliminating the need to add users to each controller individually. Set the port numbers and shared key that other controllers will use to connect to this controller. See *Supported RADIUS Server Architectures*.

The port values of 1812 for authentication and 1813 for accounting are standard RADIUS port numbers. However, other port numbers may be used. No matter which port numbers are used, make sure that the port numbers are unused by other services on this controller and that both the RADIUS server and the RADIUS clients use the same port number values. See also *IP Network Port Numbers and Protocols*.

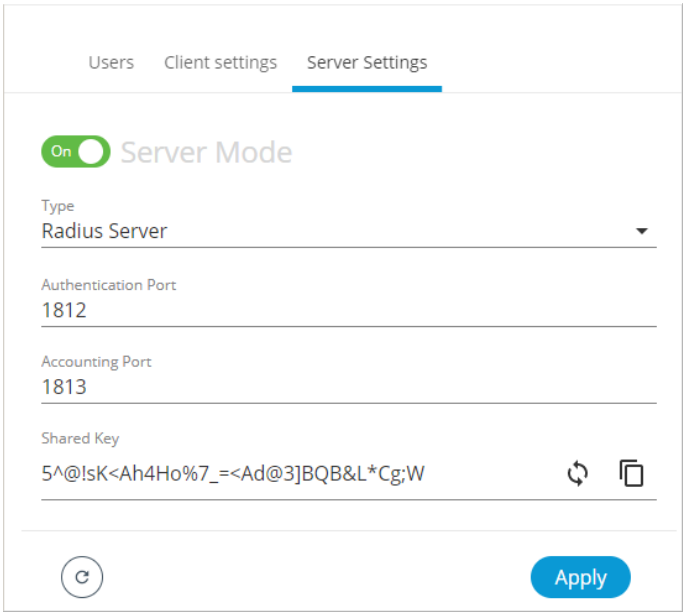


Figure 49: Radius Server Settings

To setup the RADIUS server settings, complete the parameters as described in the following table:

Item	Description
Authentication Port	RADIUS server authentication port number
Accounting Port	RADIUS server accounting port number
Shared Key	Encryption key that devices use to encrypt and decrypt user authentication credentials that are sent between devices. The shared key should be a long string made up of 16 to 132 random alphanumeric characters and symbols that would be difficult to guess. This same key must be copied to any RADIUS client.
	Click to copy the shared key to the clipboard.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

RADIUS Client Settings

When **Radius Server** is selected in the **Client Settings** tab the following configuration parameters shown in the table below are available. This centralizes access management on the RADIUS server thereby saving time by eliminating the need to add users to each controller individually. The client RADIUS server can be another ECLYPSE controller or a Microsoft Windows Domain Active Directory Server. See *Supported RADIUS Server Architectures*.

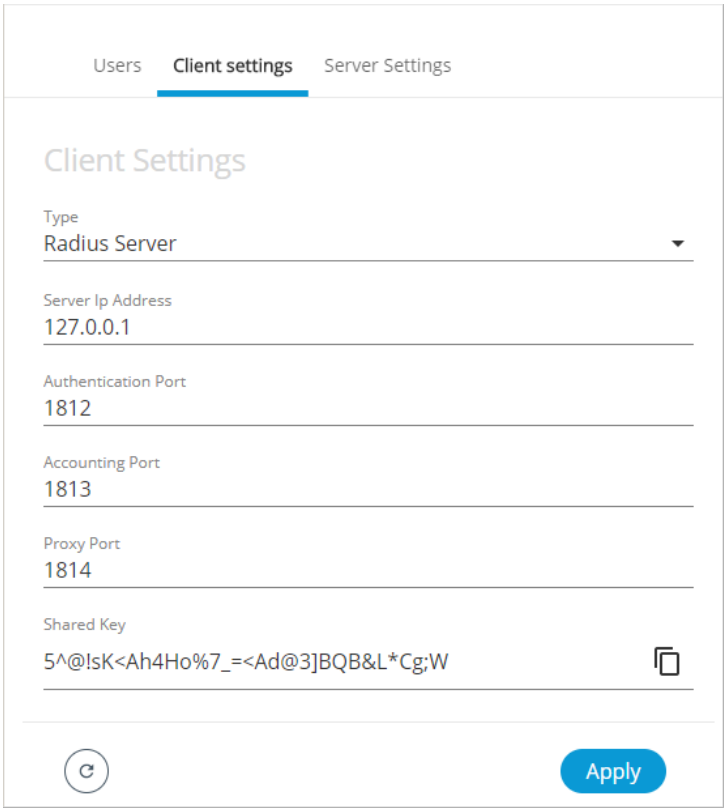


Figure 50: Radius Client Settings

To setup the RADIUS client settings, complete the parameters as described in the following table:

Item	Description
Server IP Address	IP address of the RADIUS server. This can be the IP address of an ECLYPSE controller that is set as the Server Radius or a suitably-configured RADIUS server on a Microsoft Windows Domain Active Directory Server.
Authentication Port	Port on which authentication requests are made
Accounting Port	Port on which accounting request are made. This is only used to receive accounting requests from other RADIUS servers.
Proxy Port	Internal port used to proxy requests between a server mode and client mode
Shared Key	Encryption key that devices use to encrypt and decrypt user authentication credentials that are sent between devices. The shared key should be a long string made up of 16 to 132 random alphanumeric characters and symbols that would be difficult to guess.
	Click to copy the shared key to the clipboard.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

Should the connection to the RADIUS server be temporarily lost, ECLYPSE controllers have a fall back authentication mode: Users that have already authenticated themselves with the RADIUS server and then the connection to the RADIUS server is lost, these users will still be able to log in to the controller as their successfully authenticated credentials are locally cached.

The user profile cache is updated when the user authenticates themselves while there is a working RADIUS server connection. For this reason, at a minimum, admin users should log in to each ECLYPSE controller at least once, so their login can be cached on that controller. Otherwise, if there is a RADIUS server connectivity issue, and a user who has never connected to the ECLYPSE controller before will be locked out from the controller. It is particularly important for admin user credentials to be cached on each controller as an admin user can change the controller's network connection parameters that may be at cause for the loss of connectivity to the RADIUS server.

The port values of 1812 for authentication and 1813 for accounting are RADIUS standard port numbers. However, other port numbers may be used. No matter which port numbers are used, make sure that the port numbers are unused by other services on this controller and that both the RADIUS server and the RADIUS clients use the same port number values. See also *IP Network Port Numbers and Protocols*.

Single Sign On (SSO) Settings

The **Single Sign On (SSO)** service allows a user to use one set of login credentials (e.g.username and password) to access multiple ECLYPSE controllers that are on the same network. This provides a secure centralized login method to authenticate users.

The basic functionality behind an SSO service with ECLYPSE controllers is the Client-Server architecture where one controller is defined as the Server dedicated to authentication/authorization purposes to access the Client controllers.

The SSO authenticates the user for all the controllers the user has been given rights to and eliminates further login prompts when the user accesses other controllers within the same session.

The session ends if you close the web browser or you log out. It is recommended that you close your web browser after logging out.

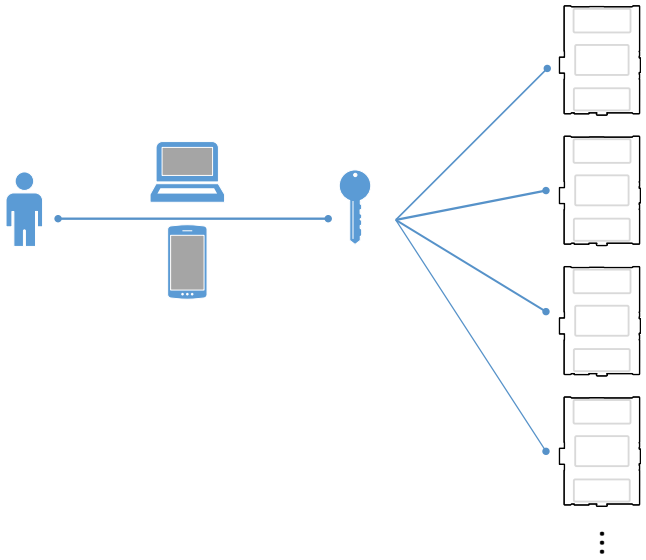


Figure 51: SSO Architecture

With the SSO service, you will be automatically redirected to the SSO server login page when you navigate to a SSO client web page. Once you are authenticated by the server, you will be redirected to the web page you requested on the client. If you requested the default page, you will be redirected to your Welcome page instead.

Figure 52: SSO Authentication Sequence

The SSO requires HTTPS to function properly. HTTP cannot be enabled and will automatically be disabled when SSO is activated.

See also *Setting Up the SSO Functionality*.

SSO Server Settings

The **Server Settings** tab allows you to select the type of server mode for the Server controller. The available modes are **Single Sign On** or **Radius Server**.

When **Type** is set to **Single Sign On (SSO)**, the controller will be defined as the SSO Server dedicated to authentication purposes. Therefore, a single login to the server will authenticate user access to multiple ECLYPSE controllers that are on the same network.

An SSO server must be configured with a static IP address. If the SSO server IP address changes, you will have to reconfigure all SSO clients with the new IP address. See *Ethernet*.

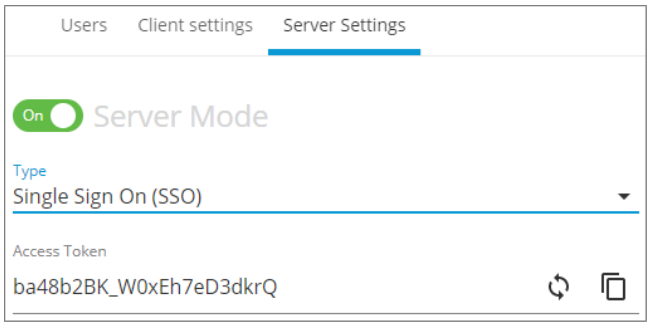


Figure 53: SSO Server Settings

Item	Description
Server Mode (On/Off) 	Enable or disable the functionality of the server. When set to OFF, the controller is no longer in server mode.
Type	Server type
Access Token	Identifier used by the server that is handling the protected resource to lookup the associated authorization information. The access token is usually a long string made up of 16 to 132 random alphanumeric characters and symbols that would be difficult to guess. When the SSO service is selected, the access token ID is displayed by default. If required, you can generate a new code using the generate icon or manually enter an access token.
	Click to copy the access token to the clipboard.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes

See also *Setting Up the SSO Functionality*.

SSO Client Settings

The **Client Settings** tab allows you to select the type of client mode for the Client controller(s). When **Type** is set to **Single Sign On (SSO)**, the controller will use the SSO server for authentication.

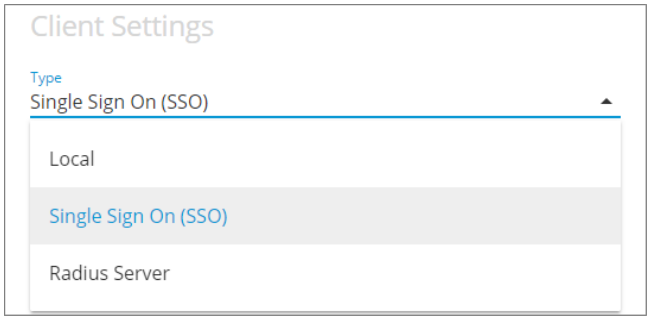


Figure 54: Client Settings - Type

When **Type** is set to **Local**, credentials are added to and managed by this controller.

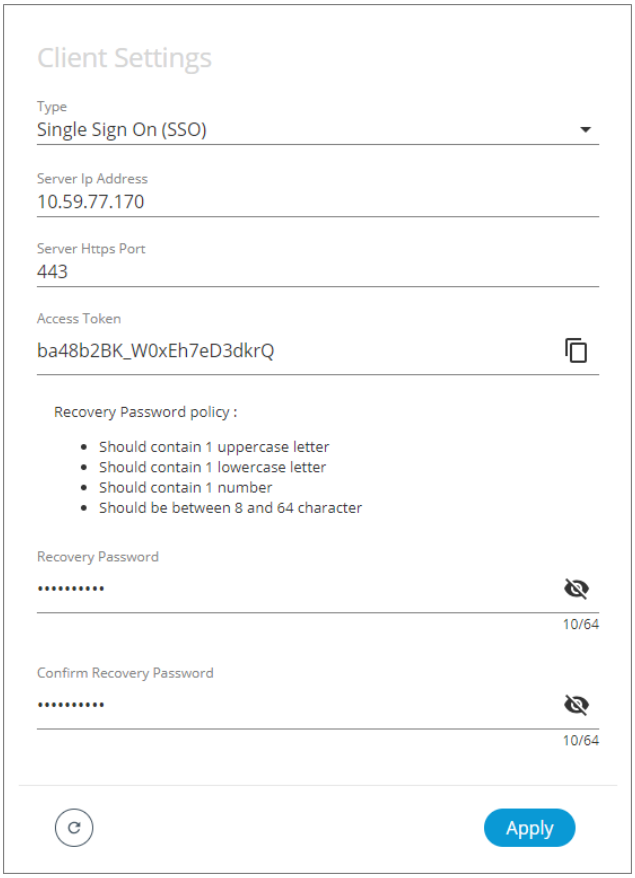


Figure 55: Client Settings - SSO

Item	Description
Type	Server type
Server IP Address	Server IP address of the SSO server. This is the IP address of the ECLYPSE controller that was configured as the server. **Note:** An SSO server must be configured with a static IP address. If the SSO server IP address changes, you will have to reconfigure all SSO clients with the new IP address. See *Ethernet*.
Server Https Port	Server HTTPS port of the SSO server. By default, this port is set to 443.
Access Token	Server access token of the SSO server. If the server access token changes, this parameter should be updated by the user accordingly. In the **Access Token** field, enter the access token belonging to the Server. To do so, go to **Server Settings**, copy the access token using the copy icon and paste (CTRL+V) into the **Access Token** field in **Client Settings**.
Recovery Password / Confirm Recovery Password	Define a recovery password to access the controller in recovery mode if ever the server is unavailable. See *Single Sign On (SSO) Troubleshooting*. Click the show password icon to see the password you are entering. In order for the recovery to work, we highly recommend you do not forget your recovery password. If so, a factory reset will be required.
	Click to copy the access token to the clipboard.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes.

Setting Up the SSO Functionality

This section explains how to setup the SSO functionality by setting up the SSO Server first, followed by the SSO Client. For more information, see *Single Sign On (SSO) Settings*.

An SSO server must be configured with a static IP address. If the SSO server IP address changes, you will have to reconfigure all SSO clients with the new IP address. See *Ethernet*.

SSO functionality is only available in HTTPS mode. See *Web Server Access* for more information on enabling HTTPS.

Setting up the SSO Server

1. Open a web browser.
2. Enter the IP address of the controller that will become the Server (e.g., 192.168.0.10). The ECLYPSE login page is displayed.
3. Enter your credentials to log in. The ECLYPSE home page is displayed.
4. In the **Users** menu, select the **Server Settings** tab and make sure the **Server Mode** is set to **On**.

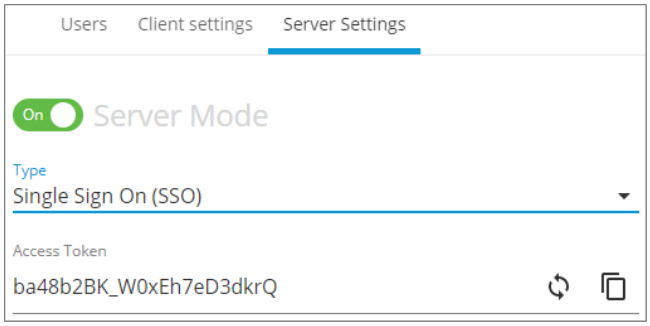


Figure 56: SSO Server Settings

5. In **Type**, select **Single Sign On (SSO)**.
6. In **Access Token**, an access token is displayed by default. If required, you can generate a new access token or manually enter a custom access token. This exact access token will be needed to setup the Client server (see next procedure *Setting Up the SSO Client*).
7. Click Apply.

Setting Up the SSO Client

1. Open a web browser or a new tab in the current Web browser.
2. Enter the IP address of the controller that will become the Client (e.g., 192.168.0.22). The ECLYPSE login page is displayed.
3. Enter your credentials to log in. The ECLYPSE home page is displayed.
4. In the **Users** menu, select the **Server Settings** tab and make sure the **Server Mode** is set to **Off**. If not, set the **Server Mode** to **Off** and click **Apply** before proceeding.

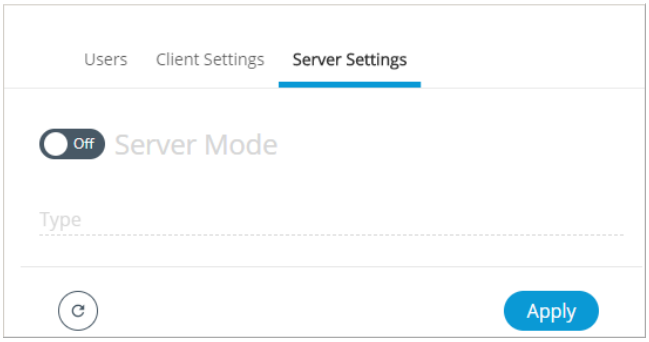


Figure 57: SSO Server Settings - Server Mode Off

5. Select the **Client Settings** tab to setup the SSO client.
6. In **Type**, select **Single Sign On**. Additional fields are displayed.

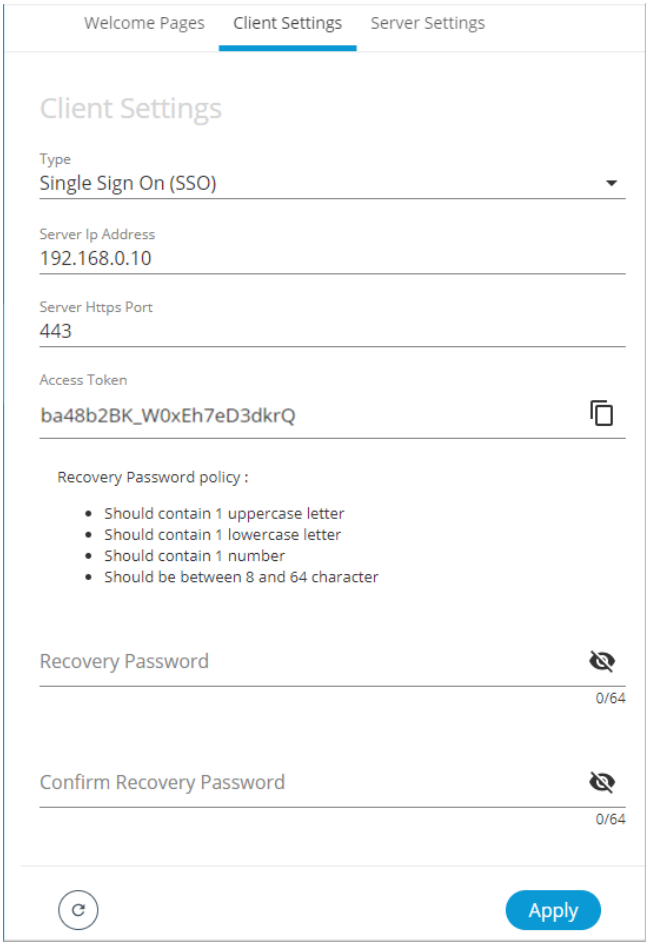


Figure 58: SSO Client Settings

7. In **Server IP Address**, enter the server IP address of the controller that is configured as the Server (e.g., 192.168.0.10).
8. In **Server Https Port**, verify that the port number matches the HTTPS port number of the SSO server in **System > Web Server** (e.g., 443).
9. In **Access Token**, you must enter the access token from the SSO Server. Copy the access token from the **Server Settings** (see above procedure *Setting up the SSO Server*) and paste in this field.

10. In **Recovery Password**, enter a recovery password that you will use in a case where the server is no longer available.
11. In **Confirm Recovery Password**, enter the password again.
12. Click **Apply** to apply and save the configuration.
13. When setting up a new SSO connection, a message is displayed to notify you that a new certificate has been detected. To validate the authenticity of the server, click **Continue**.

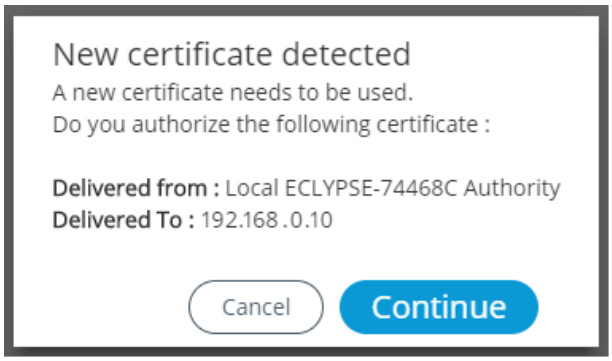
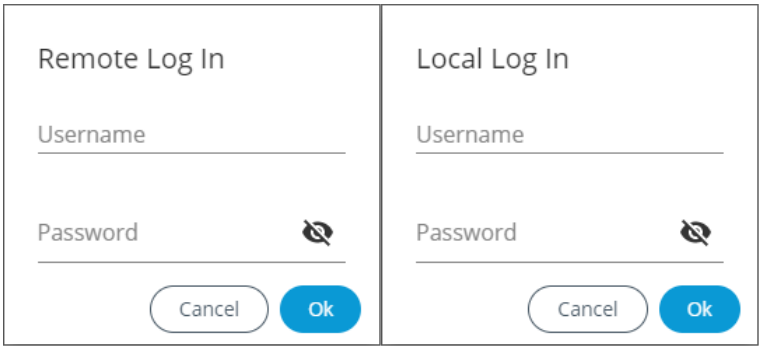


Figure 59: SSO New Certificate Detected

14. A new page is displayed confirming that the server settings are being applied. After approximately 1 minute, you can refresh your browser manually using the F5 key or close and reopen your browser.

To switch from the SSO Mode to Radius or Local Mode, you will be asked to log in to the remote or local server. These credentials are the ones associated to the server you wish to switch to.

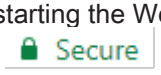


Certificate Authentication with SSO

To avoid getting certificate authentication messages:
Also see *Saving a Certificate*.

1. Go to the System menu and select the Web Server tab.
2. Click **Export Authority Public Key**. A certificate is downloaded (.crt file) and can be found in the **Downloads** folder.
3. Go to your browser settings. For the purpose of this procedure, Google Chrome web browser is used.
4. Scroll down to the bottom of the Chrome **Settings** page and select **Advanced**.
5. Select **Manage certificates**. The **Certificates** window is displayed.
6. Select the **Trusted Root Certification Authorities** tab.
7. Click **Import**.
8. Click **Next**.
9. Browse to the **Downloads** folder and select the certificate file (.crt) that was previously downloaded.
10. Click **Next** throughout the next windows and then click **Finish**.

11. A warning message is displayed. Click **Yes** to continue and apply the certificate.
12. Close all Google Chrome windows for the changes to be applied.

When restarting the Web browser, you will no longer get a message stating that your connection is NOT secure, but rather a Secure  green padlock icon will appear in the URL bar to indicate a secure connection.

System Settings

This is where you configure the controller's date and time, Web interface, port numbers, secure web interface, and the license. A secure web interface requires a SSL certificate.

Device Information

This shows detailed information about the controller such as the firmware version, MAC address for each network interface, extension modules versions, and Wi-Fi information.

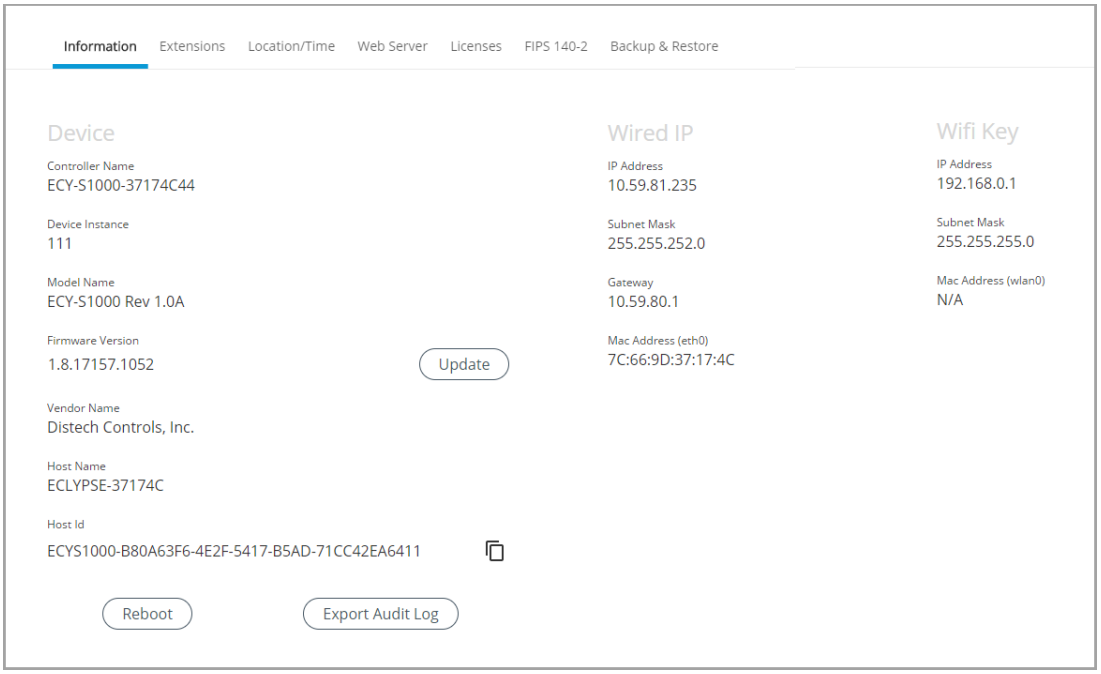


Figure 60: General Device Information

Item	Description
Update	The controller's firmware can be updated through the Firmware Update file upload interface. See *Updating the Firmware*. Also see Extensions.
Reboot	Click to reboot the controller. **Note:** Rebooting the controller will interrupt the operation of any connected equipment and the controller will be offline from the network for the duration of the reboot.
Export Audit Log	Export an audit log in .csv format showing auditable events such as account logins, event ID and description, event type, etc. See *Export Audit Log* for more information.

The **Wired IP** (wired Ethernet connection) and **Wifi Key** (wireless connection) sections provide information such as the IP address, subnet mask, gateway and Mac address

The Mac Address is the same for both Primary (PRI) Wired Ethernet connection (ETH0) and the Secondary (SEC) Wired Ethernet connection.

Updating the Firmware

The controller's firmware can be updated through the Firmware Update file upload interface for an ECLYPSE series controller.

1. In System settings under the **Information** tab, click **Update** located next to the firmware version. The Firmware Update window is displayed:

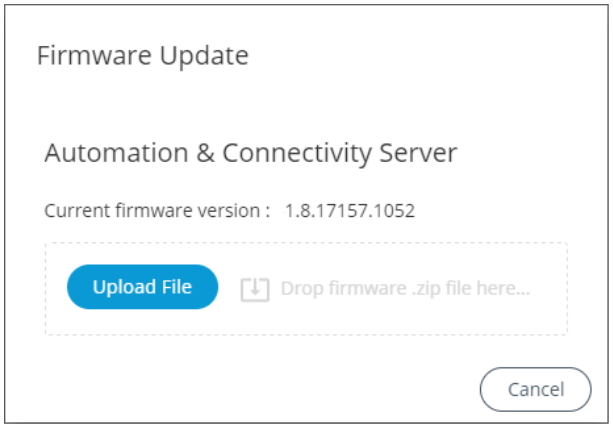


Figure 61: The Firmware Update File Upload Interface

2. Upload the firmware file using one of the following firmware upload methods:
   - Click Upload File to find the firmware file on your PC.
   - In Windows Explorer, find the firmware file on your PC and drag and drop it in the dotted area.

The file upload starts followed by the firmware upgrade. Once the upgrade is complete, the controller will reboot. If you click Cancel, not only will the upload processed be canceled, but also the upgrade.

Do not remove power from the controller or interrupt the network connection to the controller during the firmware upgrade process. Failing to do so may render the controller unusable.

See also Extensions to update the ECLYPSE Controller's I/O extension modules.

Export Audit Log

Auditable events are authentication and authorization failures and all operations done in the users' configuration. The **Export Audit Log** is used to export a .csv file that details the auditable events that are audited by the device, and/or web application (account logins, event ID and description, event type, etc).

The following device auditable events are logged:

Event Types	Description
Authentication In	When a user logs in. Only unauthorized logins will be logged
For the following event types, logging is done only on operations done in the users' configuration:	
Rest_Post	When a user sends a write/update action on the Rest API
Rest_Put	When a user sends an update action on the Rest API
Rest_Delete	When a user sends a delete action on the Rest API
Rest_Get	When a user sends a read action on the Rest API
Web_Interface	When a user performs an action on the Web interface.

The .csv file displays the event details in the following information columns:

Column Heading	Description
eventID	Sequential event number
timestamp	Time of occurrence of a particular event (date and time of day) in GMT
user	User ID or username
ipAddress	IP address of the client making the request
type	Event type as described in the previous table
description	Event type description
result	Result status for any of the event types: success, error, or unauthorized
event	Action performed by the user. For an authentication event, the event column will indicate a Web or Rest API authentication. Other events shown in this column relate to User Management events such as editing, adding, or updating data such as passwords and users, and also unauthorized access attempts.

	A	B	C	D	E	F	G	H	I
1	eventID	timestamp	user	ipAddress	type	description	result	event	
2	1	5/16/2017 17:45	admin	10.59.76.27	REST_POST	User send a write/update action on the Rest API	SUCCESS	User management - User radius global configuration	
3	2	5/23/2017 13:42	admin	10.59.76.27	AUTHENTICATION_IN	User logged in	UNAUTHORIZED	Authentication - Web	
4									
5									
6									
7									
8									
9									
10									

auditLogs (2)

Figure 62: Example of an exported .csv file of auditable events

Location and Time

The Location/Time tab is used to configure the system date and time as well as the weather and current location.

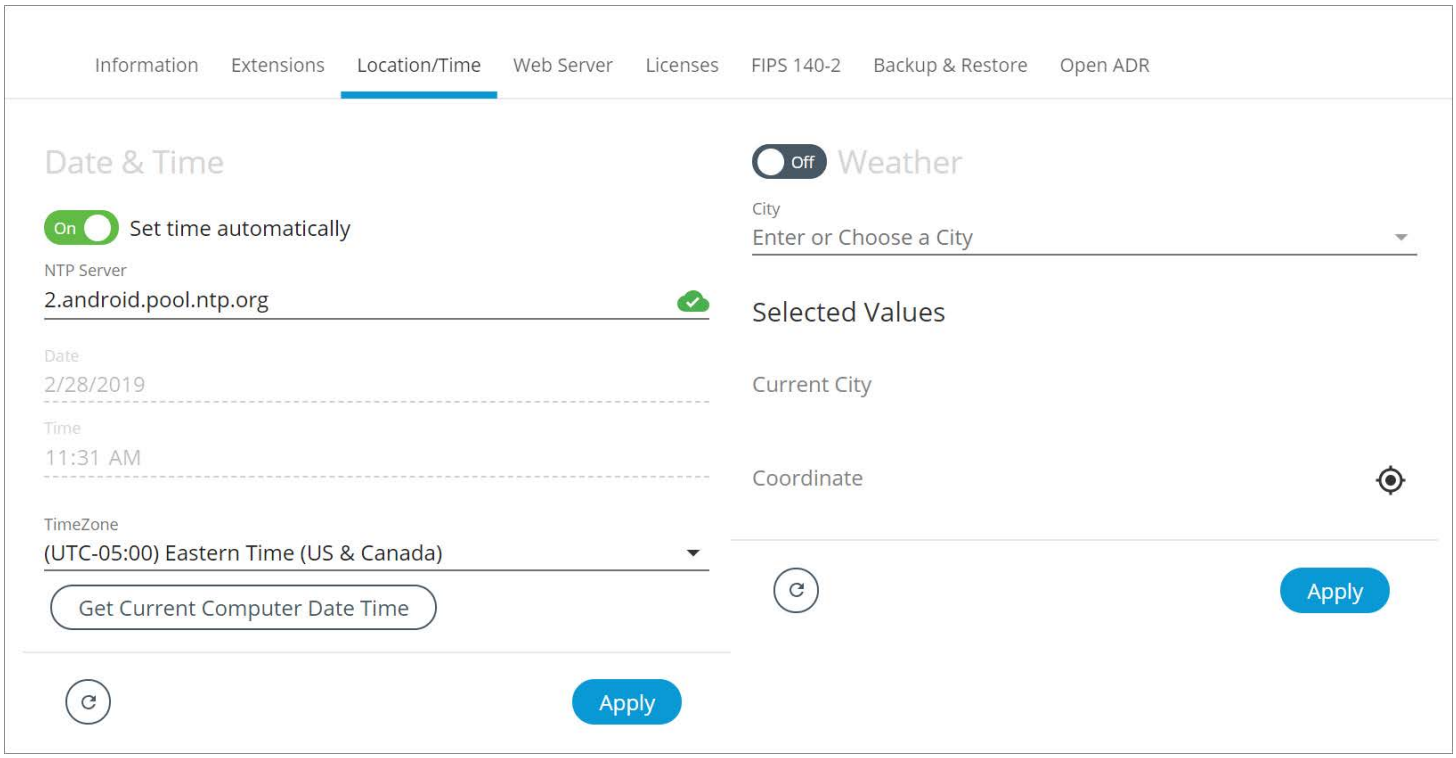


Figure 63: System Settings – Location, Date, and Time

Item	Description
Set Time Automatically 	Toggle On or Off to automatically set the time based on the NTP Server
NTP Server	Input the desired NTP Server that will be used to automatically fetch time and date information. A successful connection will display the  icon and an unsuccessful connection will display the  icon.
Date	Set the controller's date.
Time and Time Zone	Set the controller clock's time and the time zone the controller is located in.
Get Current Computer Date Time	Click to get the current time a date from an Internet time clock server. Internet connectivity is required for this feature to work.
Weather On/Off 	Weather service is not available for nLight ECLYPSE controllers.
City	Set the city location from which the system will use weather data.
Current City	Displays the currently selected city
Coordinate	Displays the latitude and longitude coordinates of the currently selected city. Click the coordinate icon  to display to open the location in Google maps.
	Click to refresh the information in the list.
Apply	Click **Apply** to apply and save the changes.

Web Server Access

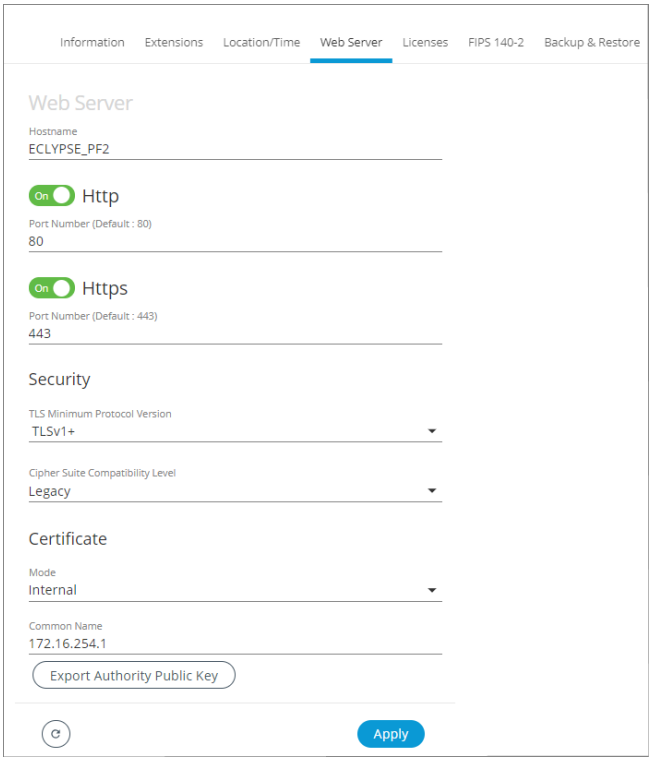


Figure 64: System Settings – Web Server Access

Item		Description
Hostname		Give this controller a label or nickname to identify it on the network. The hostname can be used in place of an IP address to identify this controller on the network. This hostname can be used in a Web browser's address. A hostname may contain only the ASCII letters 'a' through 'z' (case-insensitive), the digits '0' through '9', and the hyphen ('-'). A hostname cannot start with a hyphen and must not end with a hyphen. No other symbols, punctuation characters, or white space are permitted.
HTTP		Set this to enable the standard Webserver on this controller. When Single Sign On (SSO) is enabled, HTTP is not available. See also *FIPS 140-2 Mode*.
HTTPS		Set this to enable the secure Webserver on this controller. Connections to this sever are encrypted which helps to prevent eavesdropping thereby keeping passwords secure.
Security		**TLS minimum Protocol Version:** – Select the appropriate Transport Layer Protocol (TLSv1+, TLSv1.1+, or TLSv1.2) minimum version to be used for server authentication and secure encryption and decryption of data over the Internet. **Cipher Suite Compatibility Level:** – Legacy: This is the default value and is used only if you need to support outdated client and browser versions (e.g., Internet Explorer 6, Client in Java 6). Recommended: This level provides a higher level of security but is only compatible with latest client and browser versions (e.g., Firefox 27+, Chrome 30+, Client in Java 8).
Certificate Mode		Select the type of certificate (Internal or Custom) to be used by the ECLYPSE controller. – **Internal**: Use a self-signed certificate that has been created automatically by the ECLYPSE controller. – **Custom**: Use a custom certificate. In this case, the user must import the custom certificate into the ECLYPSE controller.
Internal Certificate	Common Name	For HTTPS connections, a certificate must have the controller's current URL or IP address encoded into it to show to the connecting device that the connection corresponds to the certificate. Set the controller's current IP address, hostname, or DNS name.
	Export Authority Public Key	For HTTPS connections, click to export the public key from the local authority that generates the internal certificate to a file on your PC. You must import this certificate into all PCs that are going to connect to this controller as a trusted certificate. See *Saving a Certificate*.
Custom Certificate	Status	Displays the certificate status: – **File not found**: No certificate has been imported. – **Present**: A certificate has been imported.
	Import Custom Certificate	Upload a custom certificate. You can also drag and drop a certificate file in the dotted area.
	Password	The password for the imported certificate.
		Click to refresh the information in the list.
Apply		Click **Apply** to apply and save the changes.

Saving a Certificate

When the HTTPS Certification has been configured, you can save the certificate on your PC. This certificate must be distributed to all PCs that will connect to this controller. It is this certificate that allows a trusted connection to be made between the two devices.

1. Enable Certificate Mode to **Internal**, and set this controller's IP address or DNS name in the **Common Name parameter**.
2. Click **Export Authority Public Key** to save the certificate on your PC.
3. Save the file on your PC.
4. Distribute this file to all PCs that will connect to this controller.
5. Install the certificate on the PC by double-clicking it in Microsoft Windows Explorer.
6. Click **Open**.

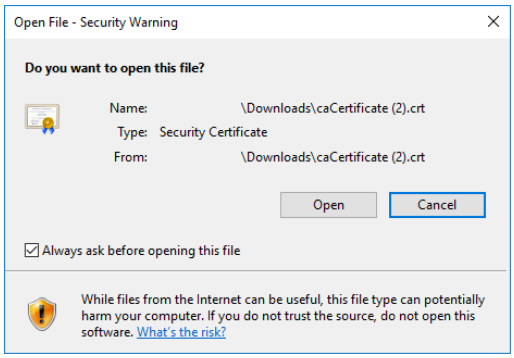


Figure 65: Certificate Security Warning

7. Install the certificate in the Trusted Root Certification Authorities store. Click **Install Certificate**.

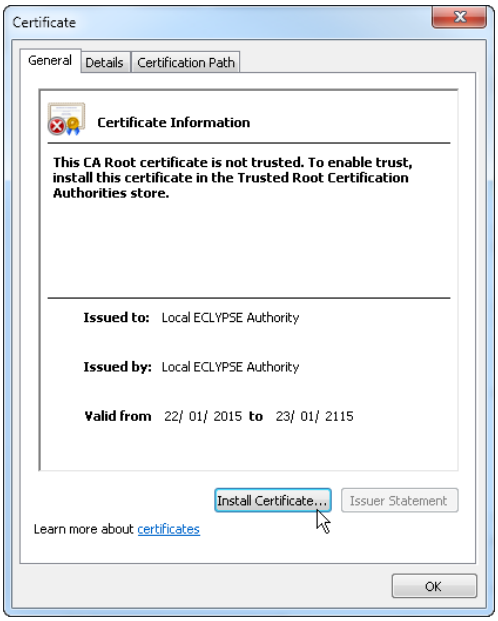


Figure 66: Installing the Certificate on the PC

8. Select **Place all certificates in the following store**. Click **Browse**.

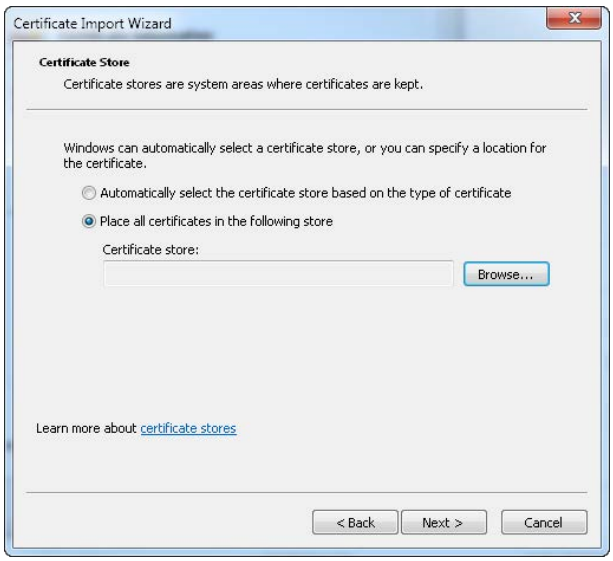


Figure 67: Selecting the Store

9. Select **Trusted Root Certificate Authorities** and click **OK**.

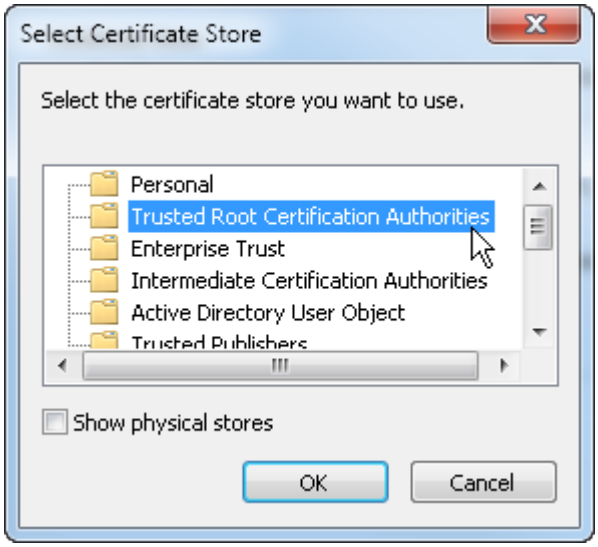


Figure 68: Selecting the Trusted Root Certification Authorities Store

10. Click **Next**. Click **Finish**.
11. Accept the warning. Click **Yes**.

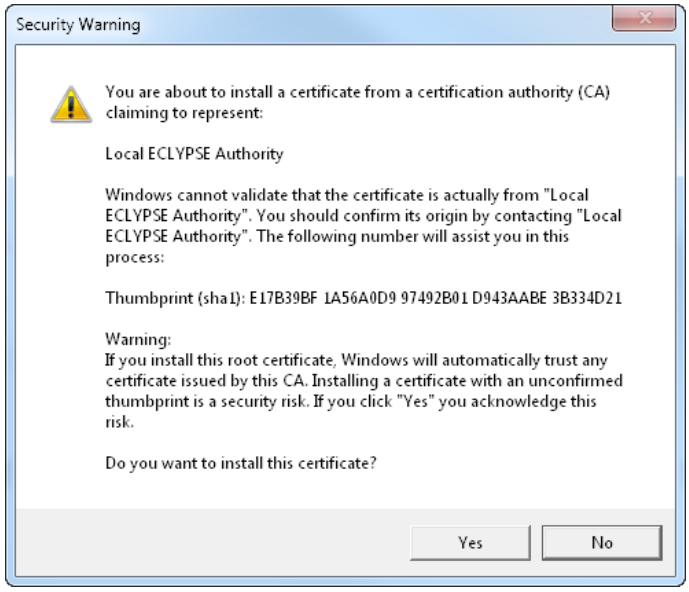


Figure 69: Accept the Warning

Removing a Certificate

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.

Security certificates are managed on a PC through the Certificate Manager. To delete an ECLYPSE controller's HTTPS security certificate from a PC, proceed as follows.

1. On the PC, open the Certificate Manager: click **Start** and type **certmgr.msc** into the search box and press **Enter**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
2. In the Certificate Manager, navigate to **Certificates - Current User\Trusted Root Certification Authorities\Certificates**. When you open this folder, certificates are displayed along with related details in the right pane.
3. Certificates for ECLYPSE controllers are named in the following ways:
   - Local ECLYPSE Authority
   - Local **ECLYPSE-XXXXXX Authority** where **XXXXXX** is the controller's MAC address. See *Controller Identification*.

     Backup the certificate in case it will be needed: right-click the certificate and select **All Tasks\Export**.
4. Delete the certificate: right-click the certificate and select **Delete**.

When you connect to the controller, your browser will ask you to accept the new HTTPS security certificate.

Licenses

You can import licenses from your PC or a Web server, as well as export an existing license.

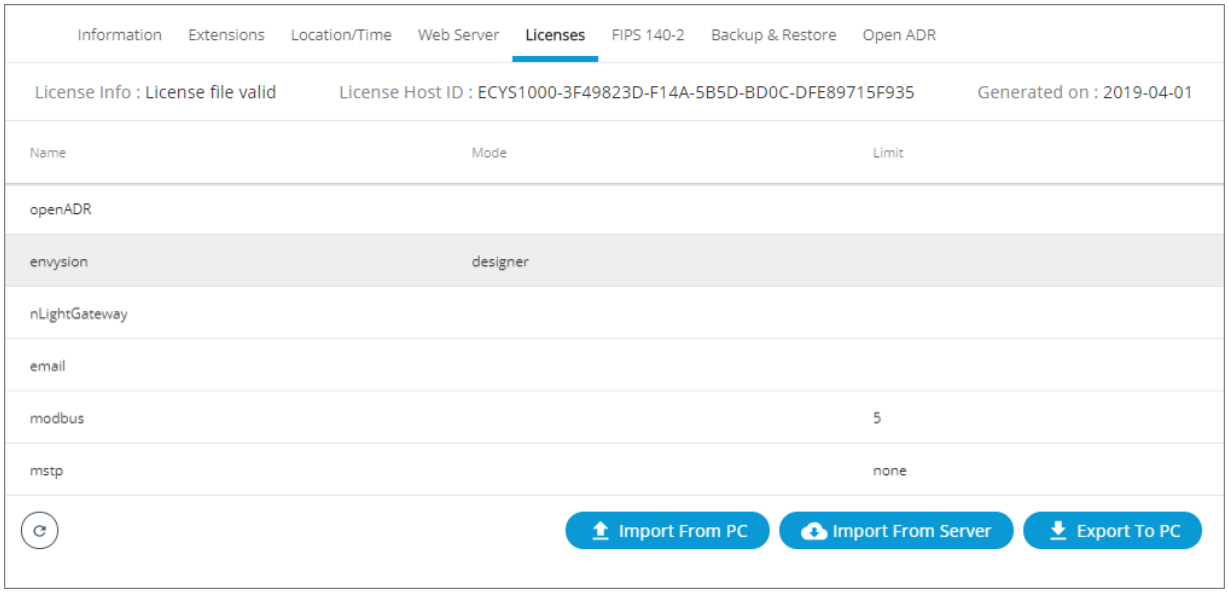


Figure 70: System Settings – Licenses

Item	Description
License Info	Basic license information
License Host ID	License host ID
Generated on	License generation date
Name	The name of the licensed feature
Mode	The feature's operating mode
Limit	The quantity limited by the license. 'None' indicates that there is no limitation.
Import From PC	Imports a license file from your PC. 1. Click **Import from PC**. 2. Click **Upload File** to select a file from your PC or drag and drop the file in the dotted area.
Import From Server	Imports a license file directly from a Web server. Internet connectivity on the computer is required. Once connected to the Web server the license is imported and a message is displayed to confirm the successful file import.
Export To PC	Saves the controller's license file to your PC. Select **Export to PC** to download a .zip file of the license.
	Click to refresh the information in the list.

FIPS 140-2 Mode

The FIPS 140-2 system setting enables FIPS 140-2 mode and resets configuration settings.

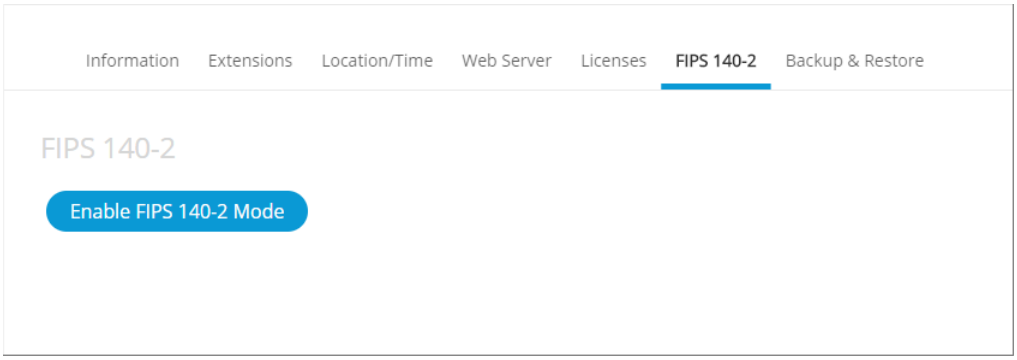


Figure 71: System Settings – FIPS 140-2 Mode

Federal Information Processing Standards 140-2 (FIPS) is a standard developed by the US Federal government, defining specific encryption methods used to ensure computer security. The ECLYPSE controller web interface has an option to enable FIPS 140-2 mode within **System** settings.

When FIPS 140-2 mode is enabled on an ECLYPSE controller, several controller settings will be reset as part of the FIPS 140-2 compliance requirements. Therefore, it is strongly recommended to enable FIPS 140-2 mode, if required, before configuring the controllers on the project.

When FIPS 140-2 mode is enabled, a notification is displayed to indicate that the controller is rebooting. You must manually refresh your browser once the reboot is finished.

The following controller settings will be reset when FIPS 140-2 mode is enabled:

- Network settings
- Web settings
- Hostname
- BACnet ports
- Weather Information
- Users reset
- HTTPS Certificates will be lost
- Default username and password

In addition, enabling FIPS 140-2 mode will have the following impact on the controller to respect compliance:

- FIPS 140-2 mode can't be disabled without a factory reset: to disable FIPS 140-2 mode on an ECLYPSE controller, a factory reset must be performed.
- Wi-Fi is disabled: Enabling FIPS 140-2 mode will disable Wi-Fi. The controller can then be connected to a network only via its Ethernet port, using an Ethernet cable.
- Password requirements: When FIPS 140-2 mode is enabled, a stronger user password is required. The password must be at least 14 characters long. As soon as FIPS 140-2 is enabled, the controller resets to a default username and password, and the user will then be prompted to reset both.
  - **Default username**: admin
  - **Default password**: adminadminadmin
- Radius server: On a project where the controllers have FIPS 140-2 mode enabled, a third-party Radius server cannot be used. If the use of a Radius based authentication is required, an ECLYPSE controller must act as the Radius server. In addition, third party Radius clients will not be able to connect to the ECLYPSE Radius server.
- When GSA mode is active, the main ECLYPSE Configuration Portal login page can display a warning banner at the top of the screen by setting the display banner option to ON.

  The banner states the following message: "*This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY.*". This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution."

GSA IT Security Mode

In the FIPS 140-2 menu, you can enable or disable the General Services Administration (GSA) IT Security mode. It is mandatory to enable this option for all U.S. General Services Administration Federal Government buildings.

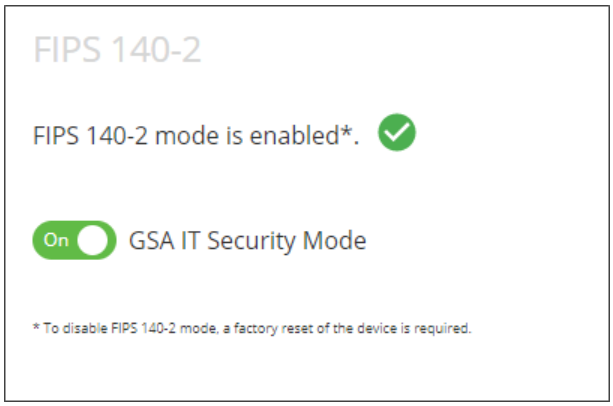


Figure 72: GSA IT Security Mode

Enabling this option will authorize only TLS1.2 encrypted communication and display a warning banner when connecting to the Web server. A confirmation message is displayed to ensure that you really want to enable/disable the GSA IT Security Mode.

When enabling or disabling the GSA IT Security mode, the Web server will be restarted.

Backup and Restore

The **Backup and Restore** tab allows you to fully backup and restore the ECLYPSE controller such as the settings, extensions firmware, ENVYSION project, etc. The backup file is created on an ECLYPSE controller and can then be downloaded to the PC using the download option. The backup file can also be created on a USB key and then restored in a controller.

The backup file for an ECLYPSE controller can only be created on a FAT32-formatted USB flash drive.

The **Backup and Restore** window, shown below, is used to create a backup as well as import and restore a backup. When a backup is created, the file appears in the list as shown in the following figure.

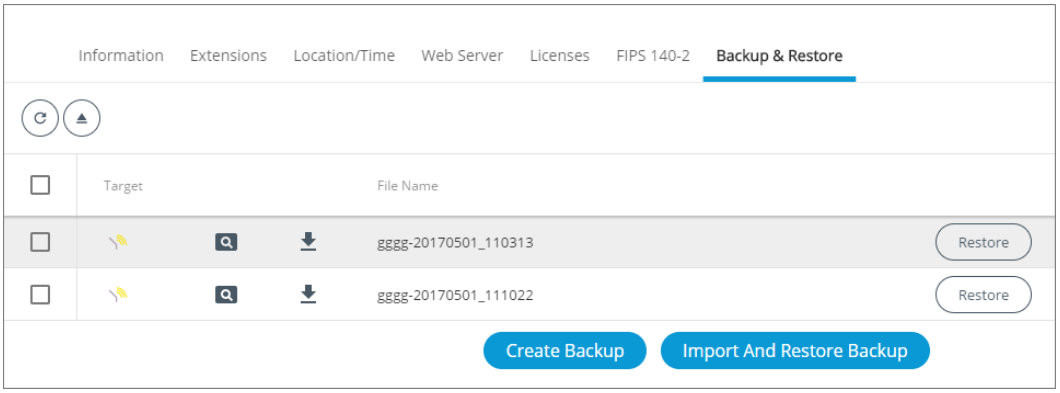


Figure 73: System Settings - Backup and Restore

Item	Description
	Click to refresh the information in the list.
	Click to eject the USB key. This is highly recommended in order to avoid data corruption.
Checkbox	Select the checkbox next to the file or files you wish to delete. Select the main selection checkbox at the top left corner of the list to select all or deselect all items in the list.
Target	- Indicates that the backup is in the ECLYPSE controller - Indicates that the backup is in the USB key
	Click to display a preview of the backup file information (name, status, model, firmware version, selected features, etc.). Directly from this preview window, you can choose to restore the file.
	Click to download the backup file (.ecybackup file) on your PC.
Filename	Name of the backup file.
Restore	Restore the selected backup file that is currently on your PC
Create Backup	Start the backup. See *Creating a Backup*.
Import and Restore Backup	Import on device and then restore the backup

Creating a Backup

The backup functionality guides you through a series of well-defined steps to easily create the data backup.

1. In the Backup & Restore main screen, click **Create Backup**. The options to create a new backup are displayed.

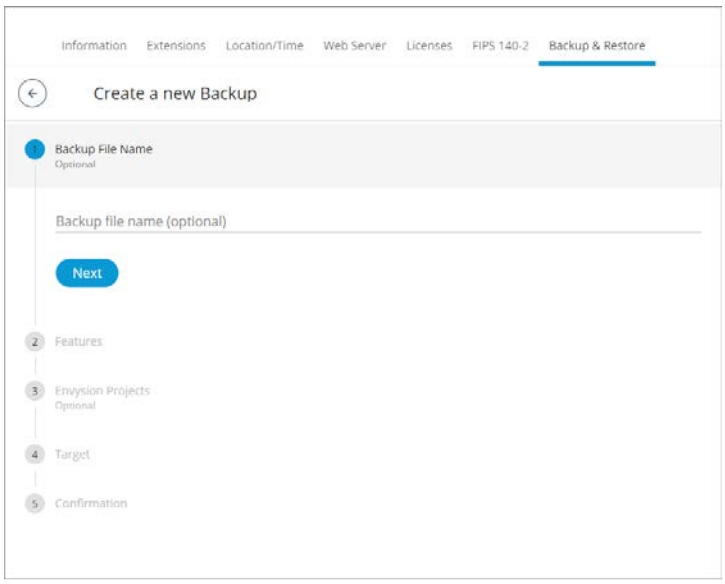


Figure 74: Creating a New Backup

2. In the **Backup File Name** section, enter the backup file name, and click **Next**.
3. In the **Features** section, select the data you wish to backup and click **Next**.

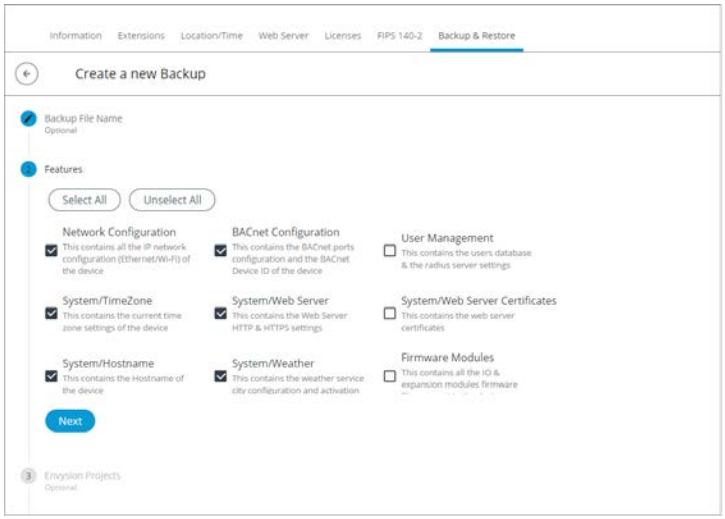


Figure 75: Backup Features

4. Select the ENVYSION projects you wish to backup and click **Next**.
5. In the **Target** section, select to store the backup in the **Device** or on a **USB key** and click **Next**.

If no USB key is plugged in, the **USB key** option is grayed out. At this point you can insert a USB key but remember to refresh in order to make the option available.

In the **Confirmation** section, an overview of the data you selected to backup is displayed. Click **Finish** to create the backup.

Keep in mind that space may be limited on your ECLYPSE controller therefore plan to remove the backup from the controller shortly after.

Importing and Restoring a Backup

The restore functionality guides you through a series of well-defined steps to easily import and restore a backup.

1. In the **Backup & Restore** main screen, click **Import and Restore Backup**. The restore options are displayed.

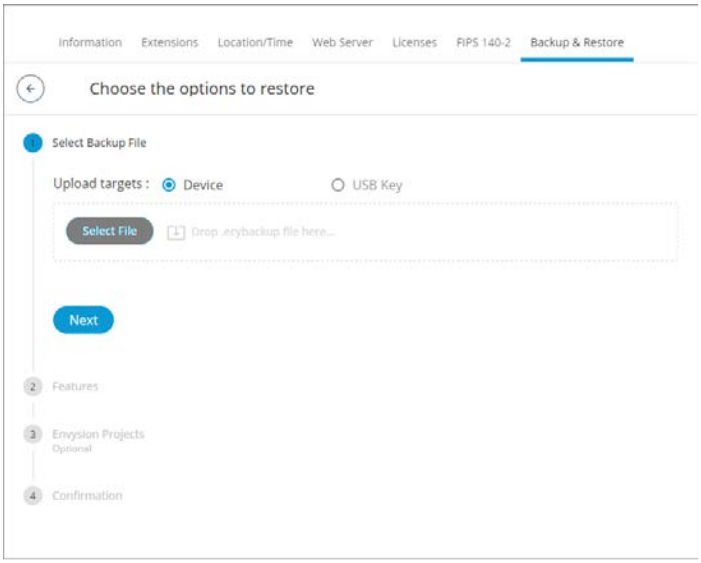


Figure 76: Restoring a Backup

2. In the **Select Backup File** section, select to upload from the **Device** or **USB Key**.
3. Click **Select File** to select the backup file (.ecybackup) you wish to restore or drag and drop the backup file in the dotted area.
4. Click **Next**.
5. In the **Features** section, select the data you wish to backup and click **Next**.

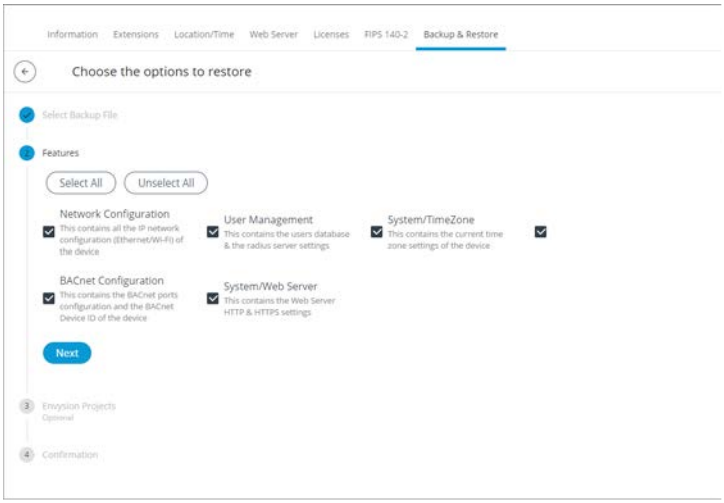


Figure 77: Restore Backup Features

6. Select the ENVYSION projects you wish to restore and click **Next**.
7. In the **Confirmation** section, an overview of the data you selected to restore is displayed and by default the **Remove backup file after restore** option is selected. When selected, the backup file will be removed after the device reboots.
8. Click **Finish** to restore the backup. A status page is displayed to indicate that the data is being restored.

Do not power off the device or close the browser window. You will automatically be redirected to the login page once the device is ready

Restoring a Selected File

In the **Backup & Restore** main screen, a **Restore** button is available next to each backup file. This allows you to restore a selected backup file on your PC.

1. In the **Backup & Restore** main screen, select the backup file(s) you wish to restore from the list.

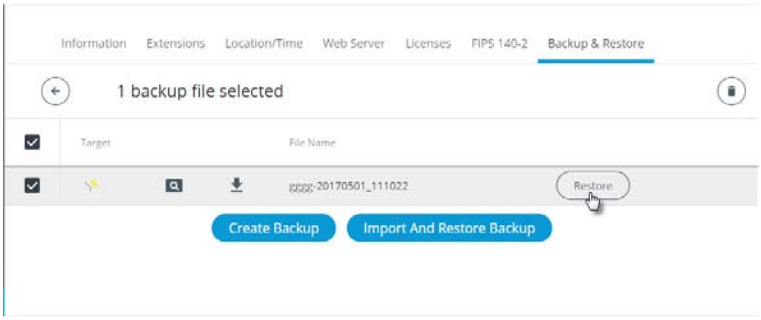


Figure 78: Restoring a Selected Backup File

2. Click **Restore**. The restore options are displayed.

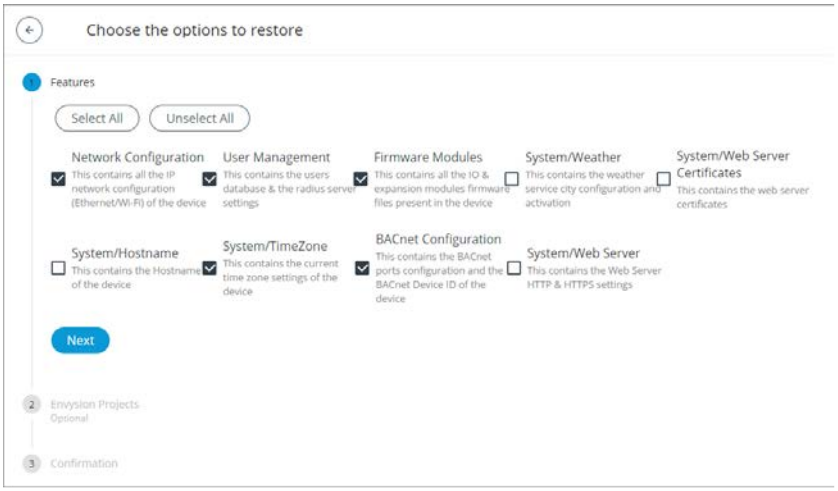


Figure 79: Restore Selected Backup File Features

3. Select the features you want to restore. By default, all features are selected. To unselect some of the features, simply click the checkbox or use the **Select All** or **Unselect All** options.
4. Click **Next**.
5. Select the ENVYSION projects to restore and click **Next**.

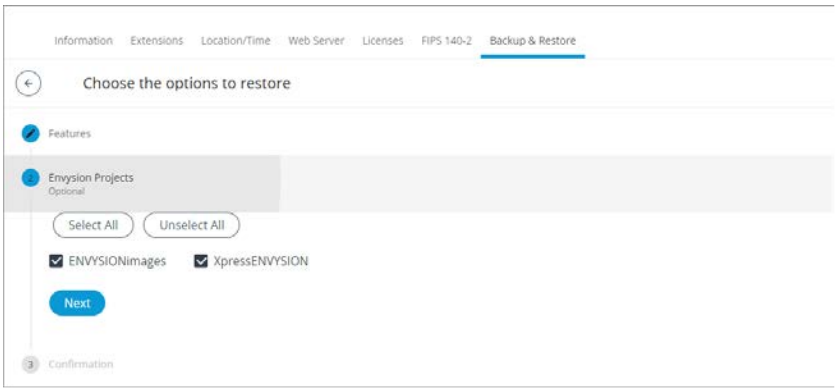


Figure 80: Restoring ENVYSION Projects

6. In the Confirmation section, review the selected features you selected and select **Remove backup file after restore** to remove the backup file from the device after reboot.
7. Click **Finish**. The restore process may take a few minutes.

You cannot restore a “non-FIPS 140-2” to a FIPS 140-2 device because the file is not encrypted and therefore not compatible with the FIPS 140-2 mode.

You also cannot restore a backup which was created in a more recent firmware version than the one you are restoring to.

Open ADR Virtual End Node (VEN)

The nLight ECLYPSE is available with a software module that embeds Open Automated Demand Response (OpenADR) 2.0a Virtual End Node (VEN) capability directly into the controller, eliminating the requirement for a separate system component that acts as a VEN. Ordering the nECY with the “ADR” option enables this software module and provides the nECY with the ability to control nLight Wired and Air devices to reduced light levels during Demand Response (DR) events.

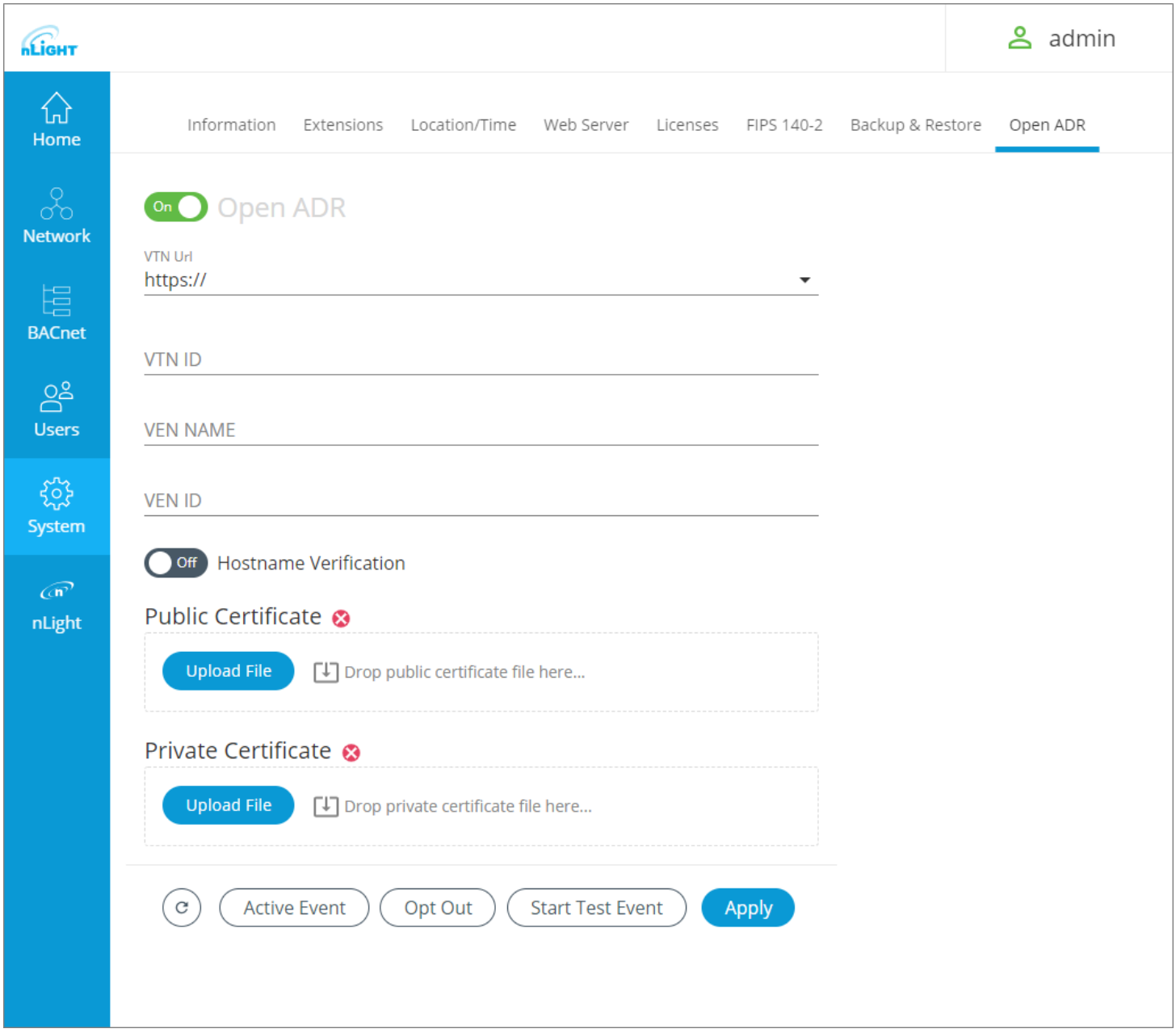


Figure 81: Open ADR configuration in the ECLYPSE web interface

Item	Description
Open ADR 	Toggle On or Off the Open ADR functionality
VTN Url	Enter the URL of the Virtual Top Node (VTN). You must also choose between http:// or https:// connection. If using https://, you will be required to upload a public and private certificate, as well as have the option of verifying the Hostname.
VTN ID	Enter the VTN ID code.
VEN NAME	Enter the Virtual End Node (VEN) name.
VEN ID	Enter VEN ID code.
	Click to refresh the information in the list.
Active Event	The Active Event button displays any active Open ADR events associated with the controller.
Opt Out	This will signal the VEN to not participate in an event.
Start Test Event	Click to start a test event. Test events demonstrate DR commissioning to the owner and/or commissioning agent. Each test event lasts one minute and can be assigned an Automated Demand Response severity level of **Normal**, **Low**, **Medium** and **Max**. Click the button again to stop the test event before the one minute is up.
Apply	Click **Apply** to apply and save the changes.

Sequence of Operations – Embedded OpenADR

The following is the communication path between OpenADR VTN server and nLight networked devices:

1. The nECY receives a DR event signal from the OpenADR VTN server.
2. The nECY invokes the appropriate “Automated DR Level” setting in nLight devices connected to it which corresponds to the severity of the event indicated in the DR signal.
3. Each nLight device is capped at its individual Automated DR Level setting; distributed control algorithms within each device are capable of controlling light levels below the Automated DR Level setting (e.g., in response to daylight, occupancy, or manual wall controls) but they cannot exceed this maximum output level.
4. At the end of the event, the Automated DR Level is released by the nECY allowing networked devices to output light levels up to their normal High Trim setting.

The Automated DR Levels can be configured for specific luminaires, devices or zones using SensorView software interface.

- Networked control devices supporting ECLYPSE Embedded OpenADR have ADR settings enabled out-of-box with the following default settings (can be changed during system startup):
  - Automated Demand Response: Enabled
  - Automated Demand Response Low Level: 90% max light output
  - Automated Demand Response Medium Level: 80% max light output
  - Automated Demand Response Max Level: 70% max light output
- Automated DR Level settings are individually configurable for specific luminaires, devices, or zones.
  - Light outputs of 100% to 1% (in 1% increments) and “Off” can be configured for each severity level of Automated DR.
  - Luminaires can be enabled or disabled to respond to ADR events invoked by the nECY.
- The nECY can issue a Test Event to demonstrate DR commissioning to the owner and/or commissioning agent.

Figure 82: Device "Default Settings" Configuration for Embedded AutoDR Response in SensorView

The Automated DR Levels can be configured for specific luminaires, devices or zones using the SensorView software interface.

Application Requirements

The utility VTN server must support OpenADR 2.0a VEN clients.

The nECY must have an outbound https connection to the OpenADR VTN IP address (TCP 443).

nLight ECLYPSE BACnet Points

BACnet points for all nLight devices are automatically generated in the ECLYPSE controller once the network scan is launched.

To optimize the automatic BACnet point generation, there is a filter function in the ECLYPSE web interface that will filter certain types of nLight resources to be skipped in the BACnet resources creation process.

As an option, you can also customize the active and inactive text that is associated with certain objects directly from the web interface.

To benefit from this feature, once the SensorView configuration is done and before configuring the ECLYPSE BACnet resources, go on the ECLYPSE web interface and click on the nLight Icon from the navigation pane.

BACnet Object Mapping

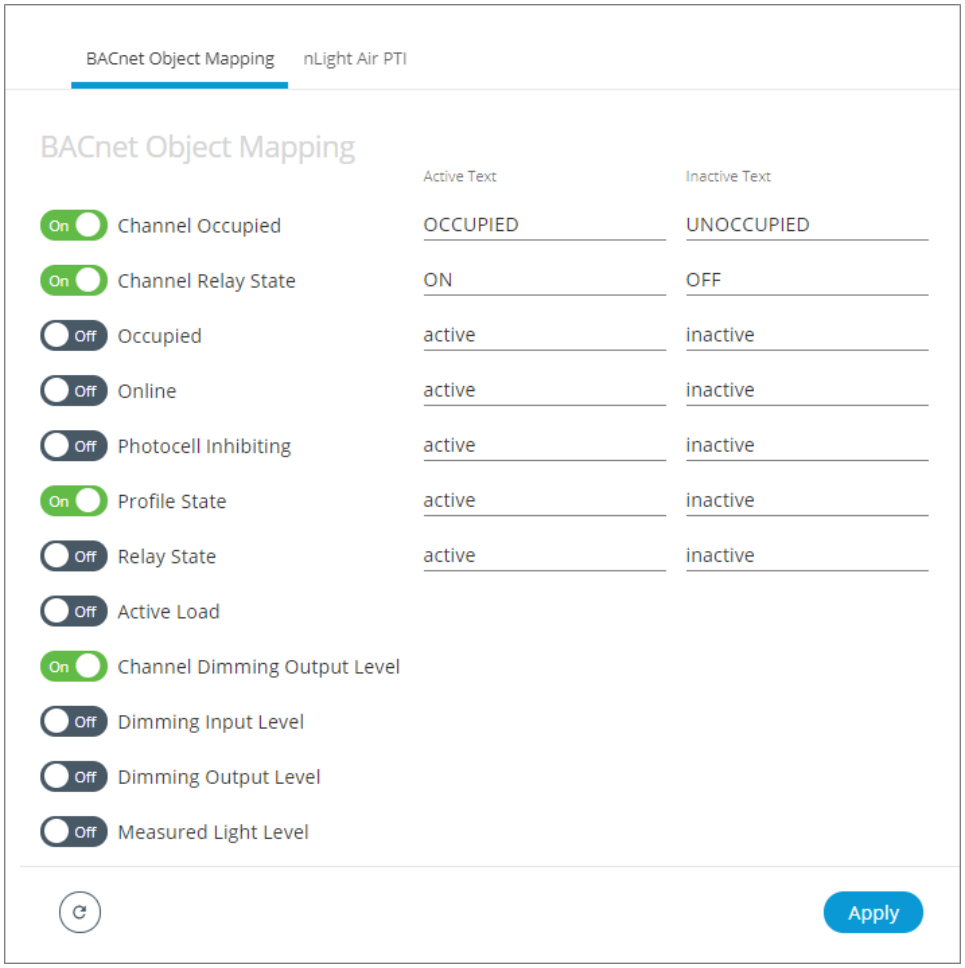


Figure 83: BACnet Object Mapping

Once the BACnet Object Mapping page is open, toggle to the ON position all of the resources you want included the nLight devices scan. The unwanted device points will be automatically filtered and will not appear in the devices points under the nLight BACnet Data tree in ENVYSION.

nLight Air PTI

The nLight Air Packet Trace Interface (PTI) will log information from nLight Air devices that are connected to the controller. The duration of the PTI can be adjusted using the + and – icons. Click the **Start** button to begin logging. After the PTI is finished running, it creates a log file that can be downloaded using the **Download Logs** button.

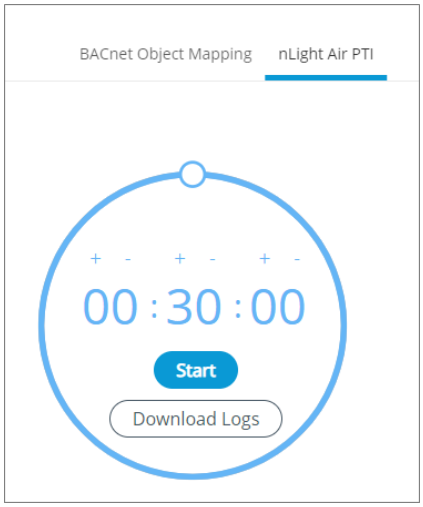


Figure 84: nLight Air PTI

CHAPTER 9
Configuring the ECLYPSE Wi-Fi Adapter Wireless Networks

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

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.

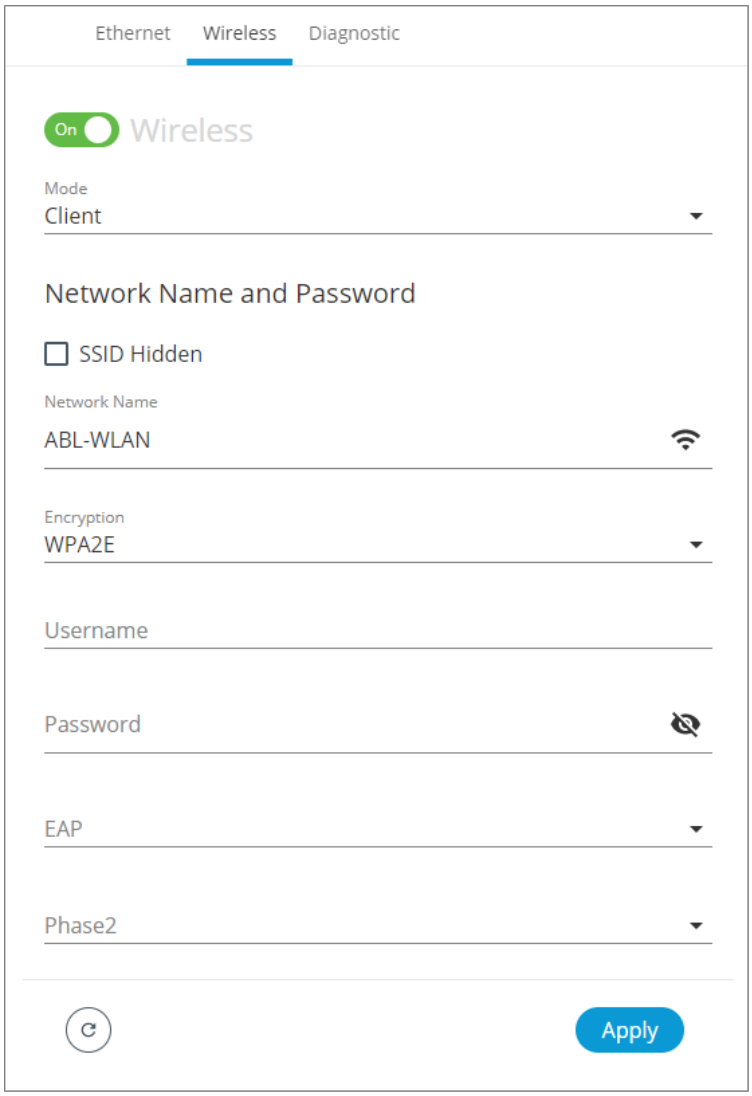


Figure 85: Client Wireless Network Settings

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

1. Set Wireless to **On**.
2. Set the **Mode** to **Client**.
3. Click the Find Network icon to search for available access points that are within range. The access points are listed on the right.

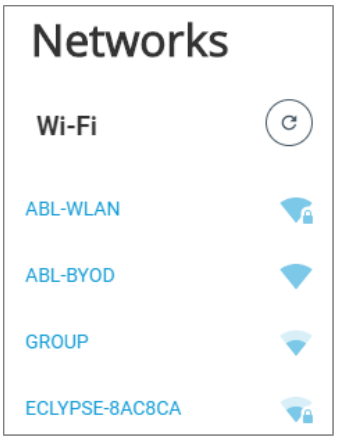


Figure 86: List of Available Access Points to Pair With

4. Select an access point to pair with from the Networks list. The **Encryption** mode is provided by the access point.
5. Enter the required **Username** and **Password**.
6. Choose the access point's **Extensible Authentication Protocol (EAP)** and **Phase2** type.
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.

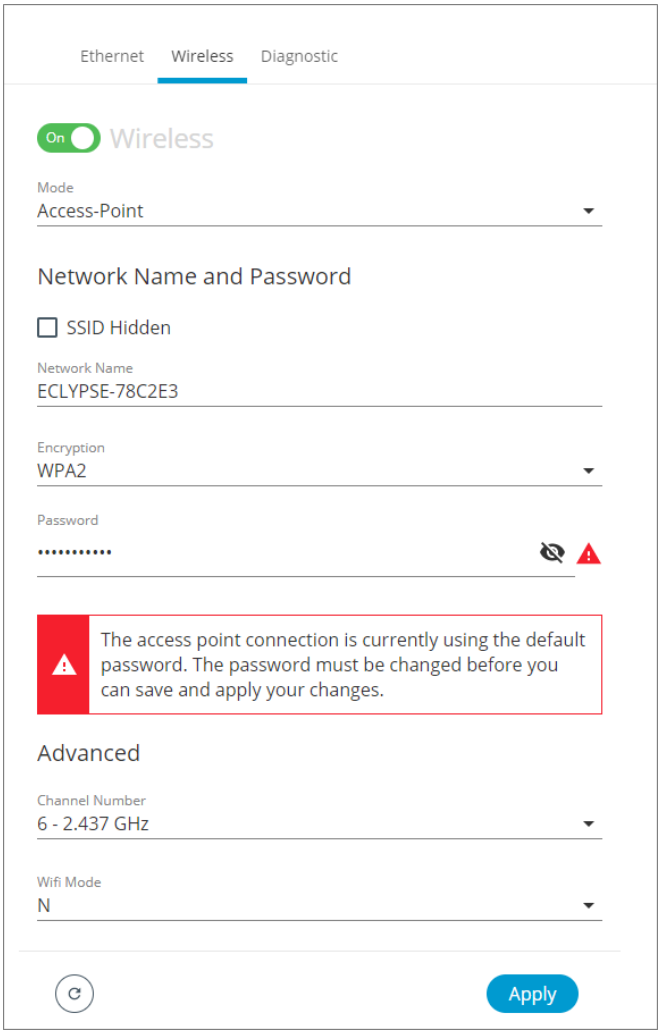


Figure 87: Access Point Wireless Network Settings

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

1. Under **Wireless Configuration**, set wireless to **On**.
2. Set the **Mode** to **Access-Point**.
3. Choose whether the **SSID** should be hidden or not.
4. Set the name for this access point by which wireless clients will identify it in **Network Name**.
5. 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.

6. 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. The default password must be changed before you can save and apply your changes to this page.
7. Under **Advanced**, set the **Channel Number** and **Wi-Fi Mode**. See *Wireless Configuration* for an explanation of these parameters.
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 forward 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)*.

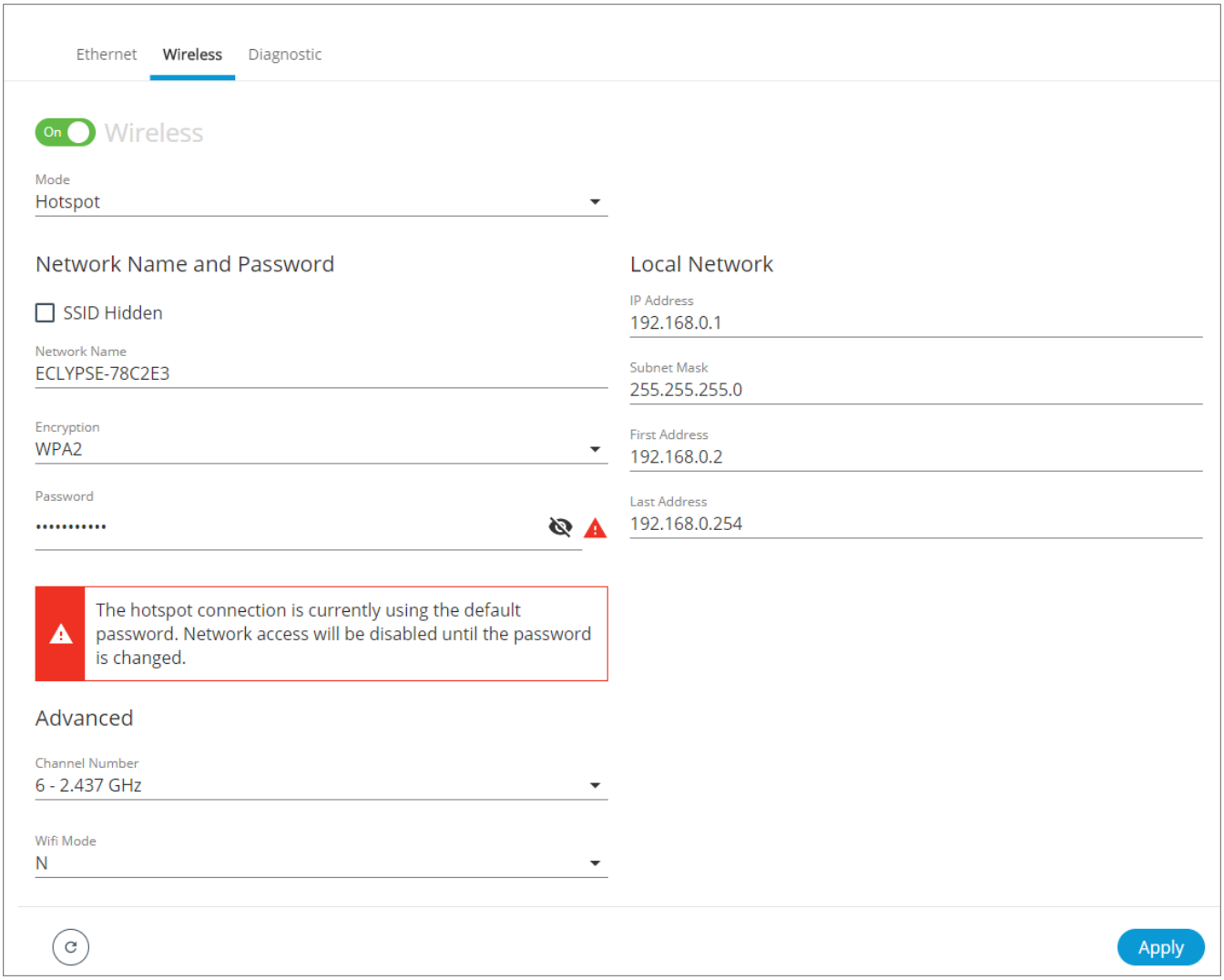


Figure 88: Hotspot Wireless Network Settings

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

1. Under **Wireless Configuration**, set wireless to **On**.

2. Set the **Mode** to **Hotspot**.
3. Choose whether the **SSID** should be hidden or not.
4. Set the name for this access point by which wireless clients will identify it in **Network Name**.
5. 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.
6. 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. Network access will be disabled until the default password is changed.
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 Number**, and **Wi-Fi Mode**. See *Wireless Configuration* for an explanation of these parameters.
11. Click **Apply**.

CHAPTER 10
Securing an ECLYPSE Controller

This section describes how to secure an ECLYPSE controller from unauthorized access and use.

Introduction

This chapter describes how to implement best security practices for 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 ECLYPSE 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. 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 a 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 log in using those credentials. 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. 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 to compromise the network, they would not be 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 trusted SSL certificate. Refer to *Web Server Access* for information on how to import a custom certificate.

Additional Measures

Update the Controller's Firmware to the Latest Release

Always keep the ECLYPSE controller's firmware up-to-date. The most recent firmware has the latest bug fixes, security updates, and stability enhancements.

External Factors

Install Controllers in a Secure Location

Ensure that the ECLYPSE controller is installed in a physically secure location, under lock and key. Through physical access, an attacker can take over the controller to do with it what they please.

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 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 eavesdropping on the communications channel to steal user credentials.

CHAPTER 11
BACnet MS/TP Communication Data Bus Fundamentals

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

BACnet MS/TP Data Transmission Essentials

Certain ECLYPSE controllers support BACnet MS/TP to BACnet/IP routing. See the Controller's datasheet for more information. To enable BACnet MS/TP to BACnet/IP routing, 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. When the ECLYPSE Controller is configured for BACnet MS/TP, values from the connected BACnet MS/TP controllers can be used in ENVYSION graphics hosted on the ECLYPSE Controller. Furthermore, the ECLYPSE Controller acts as a BACnet/IP to BACnet MS/TP bridge that allows BACnet objects to be shared among BACnet 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). An example of an interconnected BACnet MS/TP data bus is shown in *Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers*.

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 *Only a Daisy-Chained Data Bus Topology is Acceptable*). 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.

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+	

Table 4: Common Identification Labels for BACnet MS/TP Data Bus Polarity for other Manufacturers

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 *Baud Rate*.
- It is recommended that you connect no more than 50 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 between controllers.

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.

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.

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:

Manufacturer	Quantity of devices (example)	Equivalent full-load devices	Maximum devices supported by the manufacturer
⅛-load devices	8	1	128[1] Maximum 50 recommended
½-load devices	14	7	64 Maximum 50 recommended
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.

Table 5: Device Loading Example

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 an ECLYPSE Controller 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 failover protection.
- For example, set the baud rate of the ECLYPSE Controller (if equipped) and one other controller to 38 400 baud. If the ECLYPSE Controller becomes unavailable and there is a power cycle, the BACnet compatible 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.

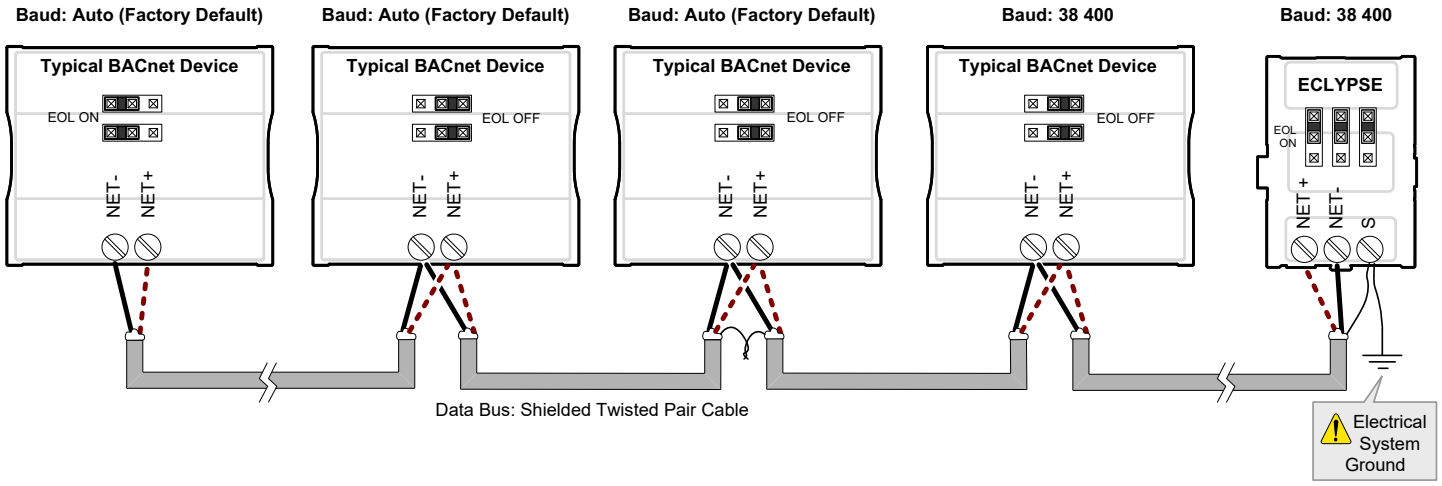


Figure 89: Setting the Baud rate on two Controllers on a BACnet MS/TP Data Bus Segment for Failover Protection

To set the baud rate for:

- ECLYPSE Controllers, see *Network MS/TP Ports*.

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. It is strongly recommended that the following data bus segment cable specifications be respected.

Parameter	Details
Media	Twisted pair, 24 AWG
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)

Table 6: BACnet MS/TP Data Bus Segment Physical Specifications and Cable Requirements

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.

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

Table 7: Recommended Cable Types for BACnet MS/TP Data Buses

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.

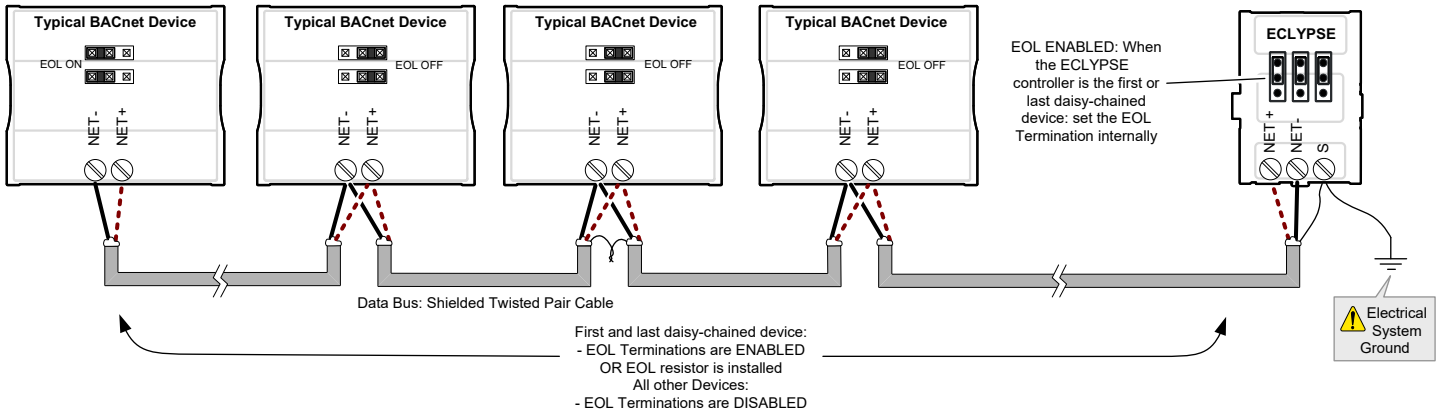


Figure 90: EOL Terminations Must be Enabled at Both the First and Last Device on the Data Bus

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 ECLYPSE Controller at the other end, you must set the built-in EOL termination in the controller so that proper biasing is provided to the BACnet MS/TP data bus.

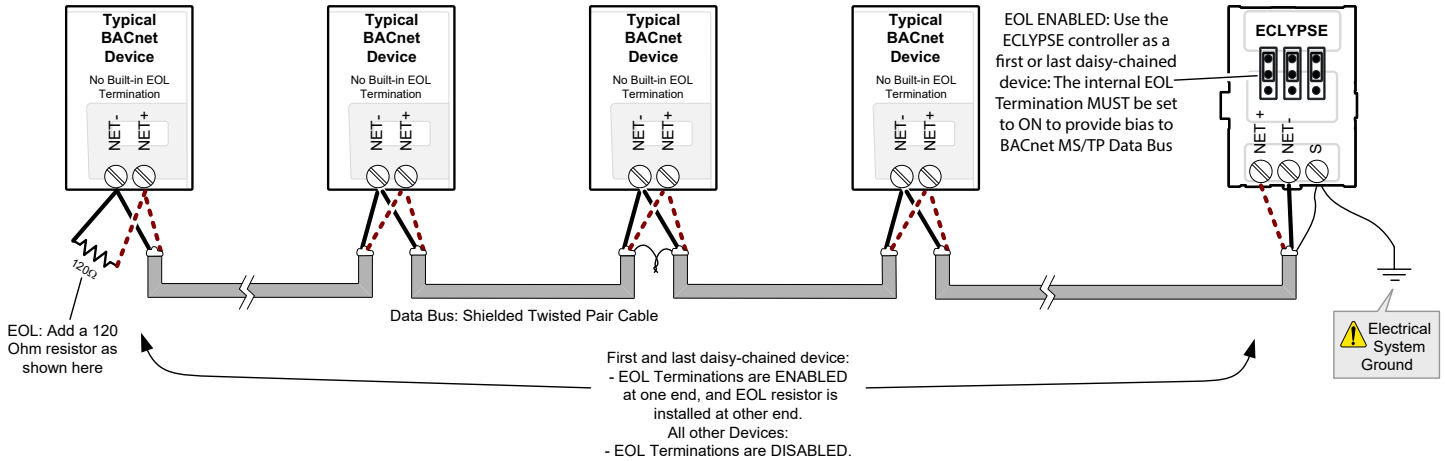


Figure 91: Typical EOL Terminations with BACnet MS/TP Thermostats with Biasing Provided by the Controller's Built-in EOL Termination set to ON

About Setting Built-in EOL Terminations

ECLYPSE 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 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 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 the previous figure.

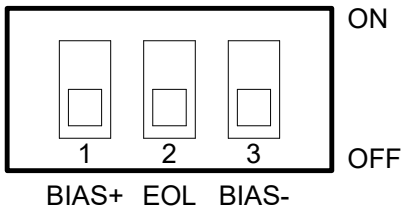


Figure 92: Typical Controller with Separate EOL Termination and Bias Configuration Settings

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.

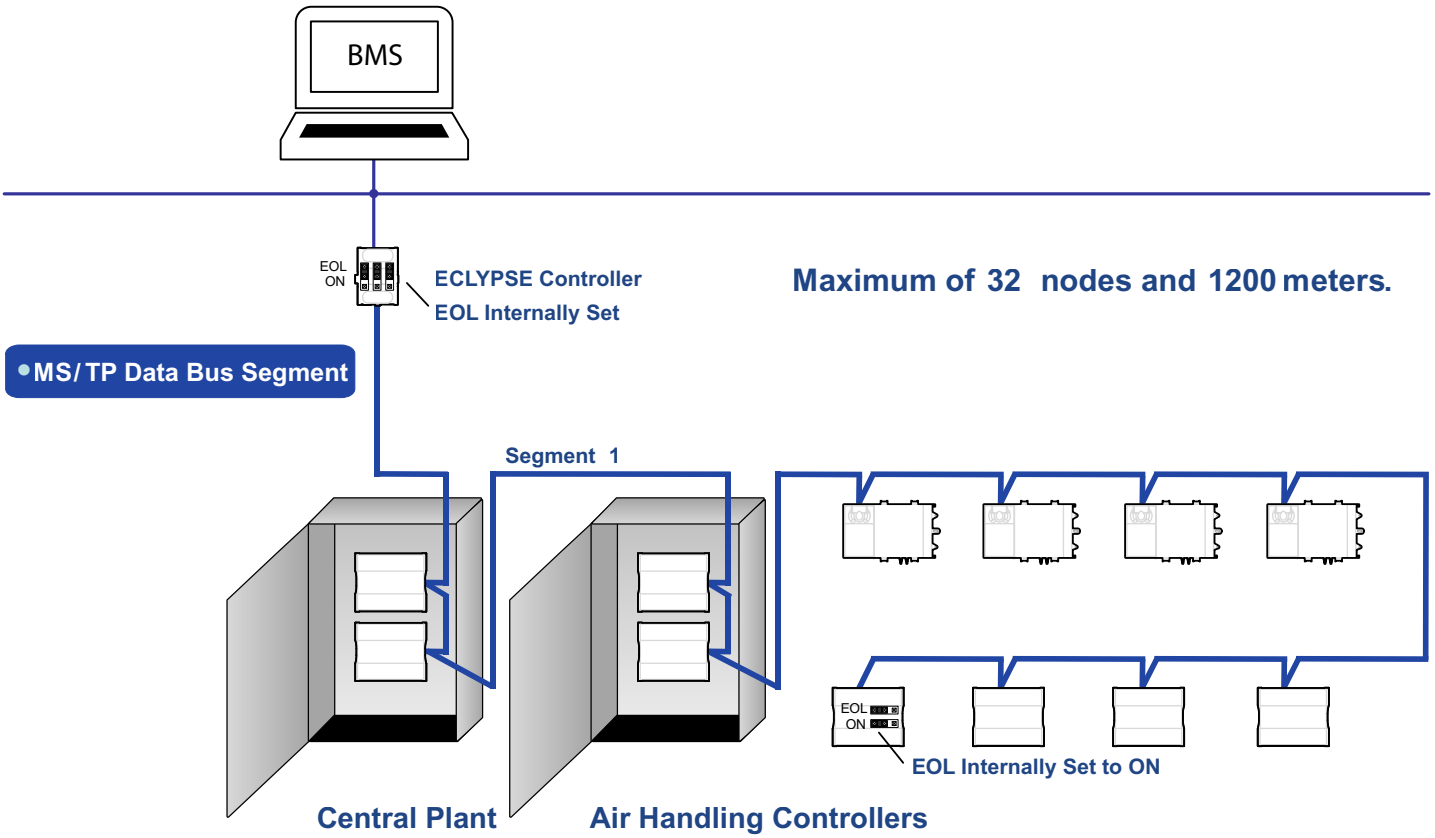


Figure 93: Typical BACnet MS/TP LAN Topology Showing How Devices are Daisy-Chained Together to Form One Data Bus Segment

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*).

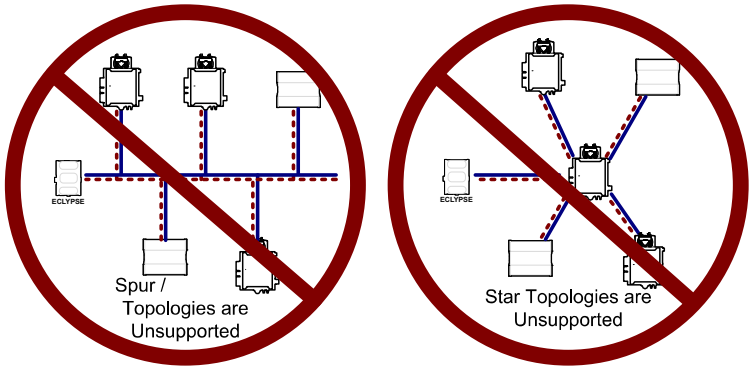


Figure 94: Unsupported BACnet MS/TP LAN Topologies

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 24V-Powered Controllers:

The data bus' cable shields must be twisted together and isolated with electrical tape at each device. Note that for 24V-Powered Controllers, the power supply transformer's secondary that is connected to the 24V COM terminal is usually 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.

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 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 **S** terminal.

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

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 ECLYPSE Controller, as shown in the figures below.

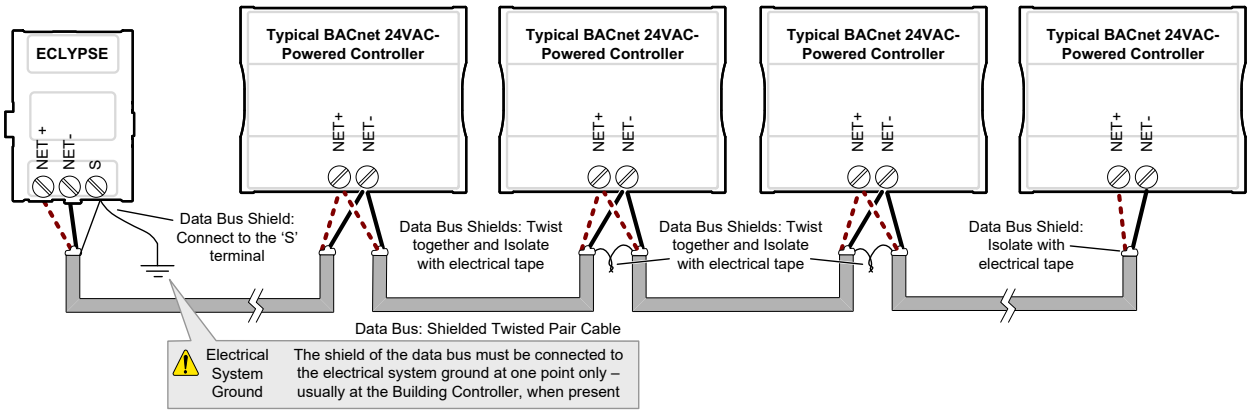


Figure 95: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECLYPSE Controller located at the End of the Data Bus

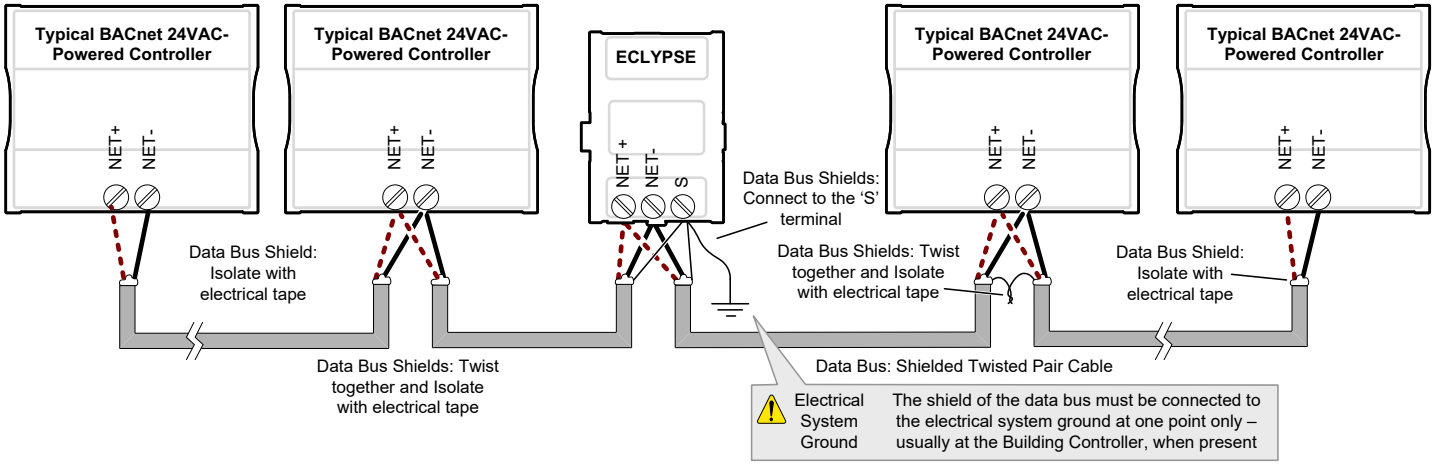


Figure 96: Typical Cable-Shield Grounding Requirements for a BACnet MS/TP Data Bus Segment with an ECLYPSE Controller located in the Middle of the Data Bus

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 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.

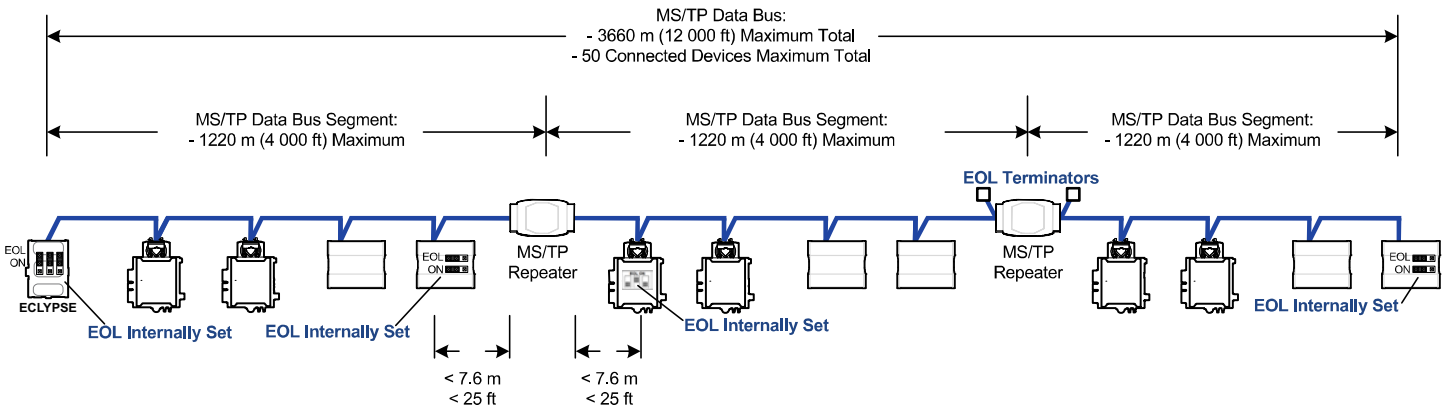


Figure 97: Using a Repeater to Extend the Range of the LAN

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

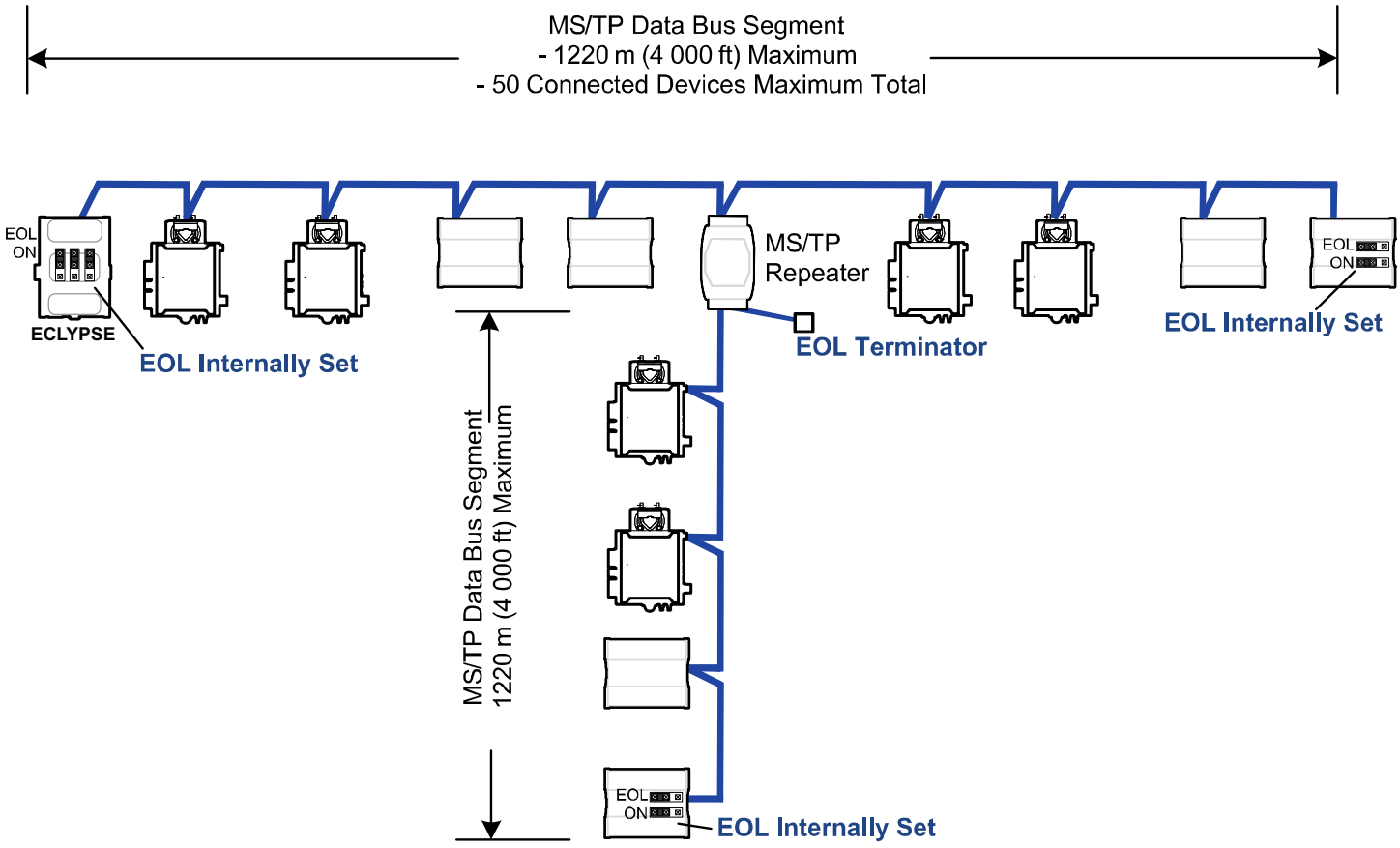


Figure 98: Adding a Spur by Using a Repeater

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*.

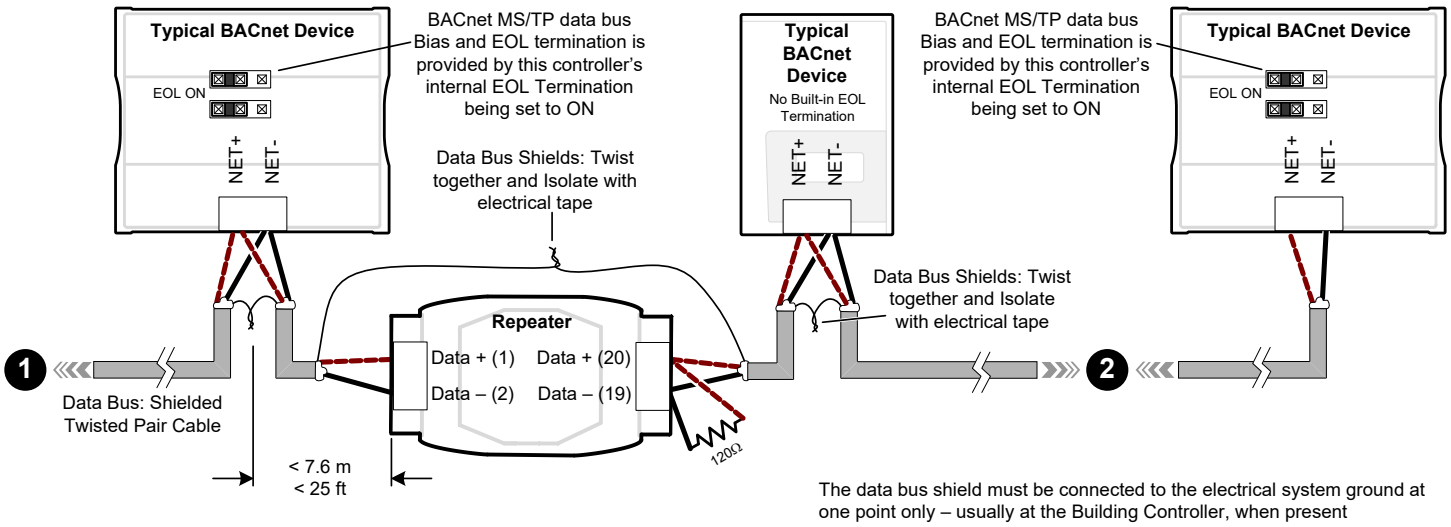


Figure 99: Repeater Connections when it is the First or Last Device on its Respective Data Bus Segment

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 the above figure, 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 the above figure, 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 the above figure. 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 *About the MAC Address*). The MAC Address is also used to share data bus bandwidth between devices through token passing between Master devices.
- 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 entire network).
- 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 *Adopting a Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers*.

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 ECLYPSE Controller's MS/TP port be always set to 0.

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

MAC Address Value / Range	Usage	Devices
0	Data Bus Master (ECLYPSE Controller)	This address is invalid for other BACnet devices
1	Temporary commissioning connection	This address is invalid for other BACnet devices
2	Reserved	Other
3-127	Master Range	Master devices: All master devices 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

Table 8: Recommended BACnet MS/TP Bus MAC Address Values / Ranges for BACnet MS/TP Data Bus Devices

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.

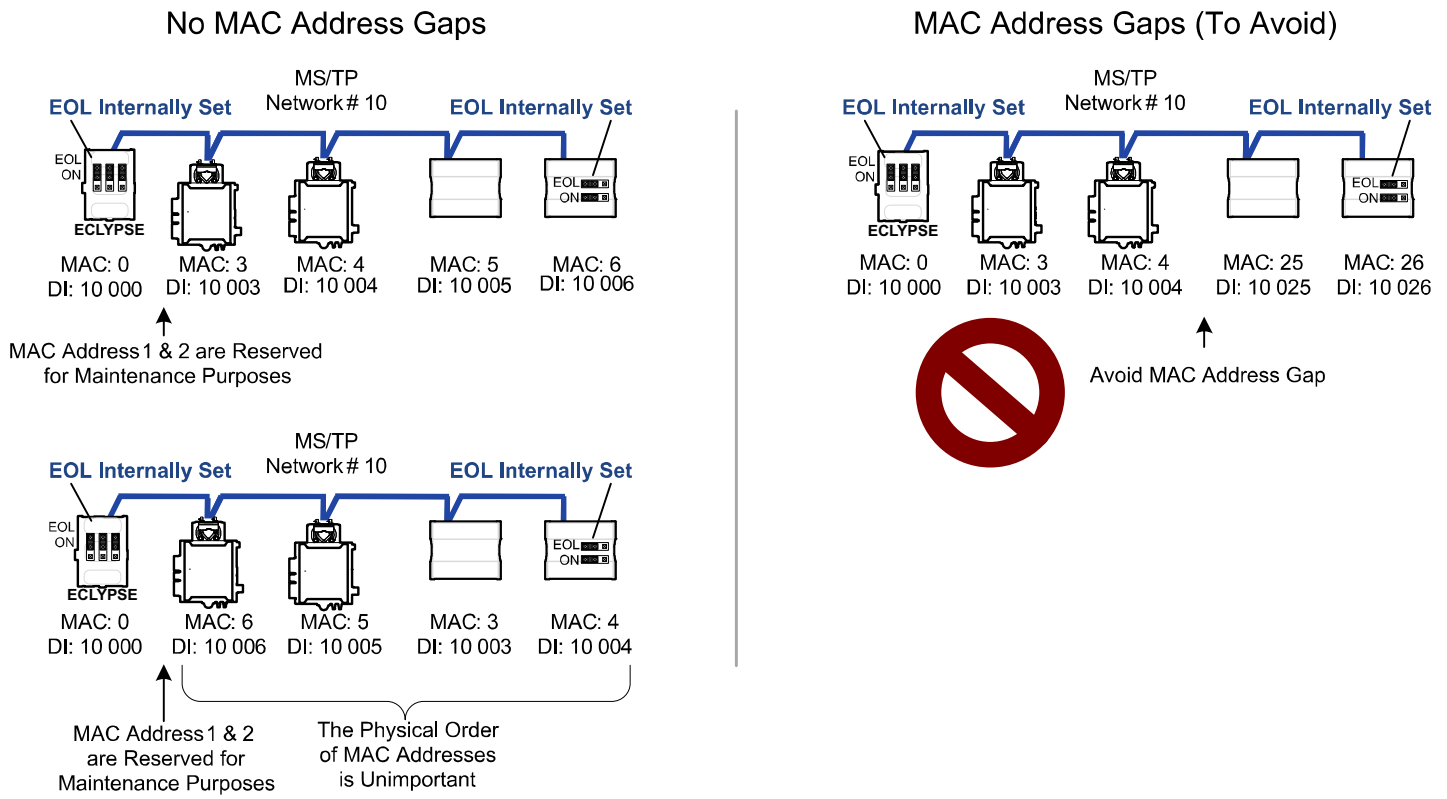


Figure 100: Setting the Max Master on the ECLYPSE Controller to the Highest MAC Address Used on the BACnet MS/TP Data Bus

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 (ECLYPSE 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 ECLYPSE 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 Master requests.

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 ECLYPSE 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 ECLYPSE Controller and separately with the Supervisor for each connected BACnet MS/TP device.

For the ECLYPSE 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 *specific* 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, a BACnet controller), use a Supervisor to do so.

Default Device Instance Number Numbering System for nLight ECLYPSE Controllers

By default, nLight ECLYPSE controllers 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 the nLight ECLYPSE controller's unique BACnet Manufacturer ID.

This Numbering system is sufficient for a BACnet network that has only one nLight ECLYPSE Controller. For larger BACnet networks that have more than one 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.

Description	Range	Example
BACnet/IP Network Number	0 to 65 534	1
ECLYPSE 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: ECLYPSE Controller BACnet/IP Device Instance Number/1000 + 0,1,2,3,4 (for each LAN)	10 to 4190	10 20 30
BACnet MS/TP Device Instance Number =	10 000 to 4 190 256	10 006 where MAC = 6

Table 9: Recommended Numbering Scheme for MAC Addresses, Instance Numbers, and Network Numbers

An example of this numbering system is shown below.

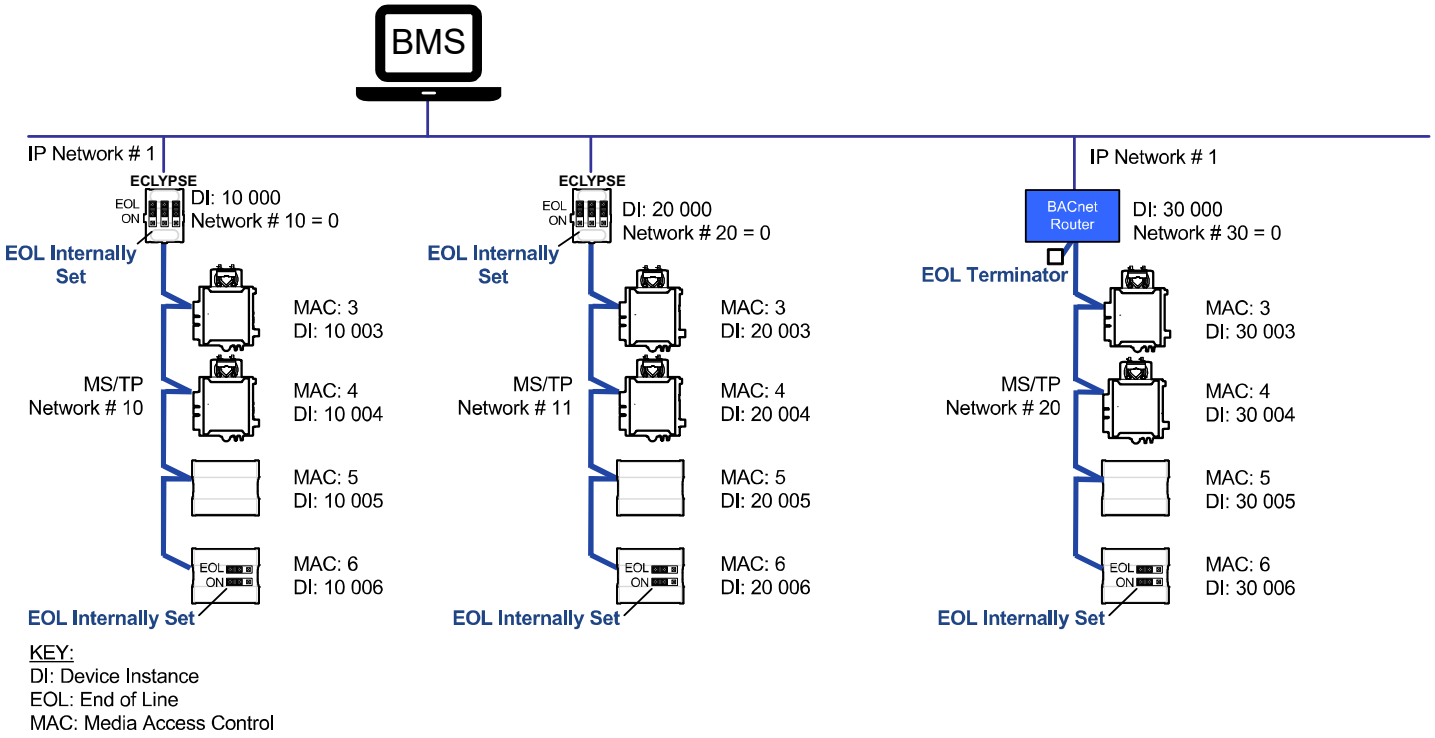


Figure 101: BACnet MS/TP Numbering System for MAC Addresses, Device Instance Numbers, and Network Numbers

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

Setting the Controller's MAC Address

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

Inter-Building BACnet Connection

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

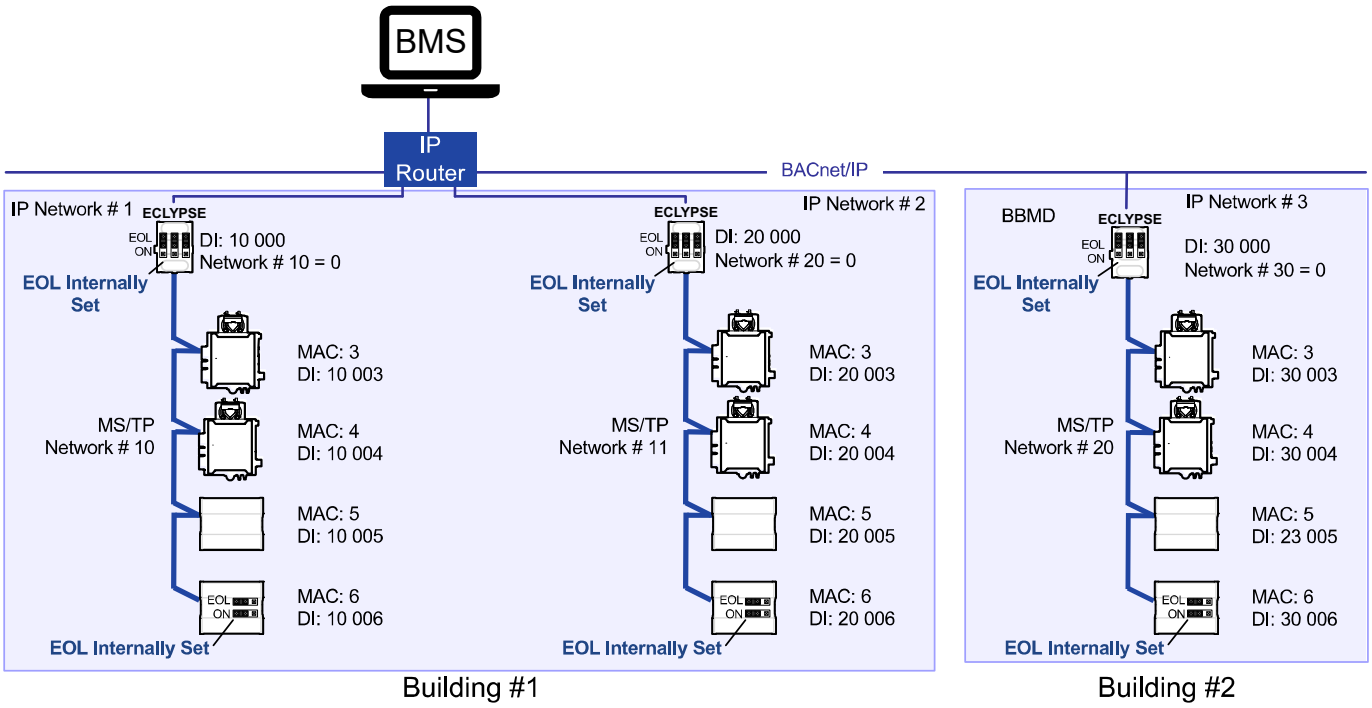


Figure 102: Typical Inter-Building Connection Using BACnet/IP or FOX

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 ECLYPSE Controllers communicate to each other over a standard IP connection that is separated by an IP router, both controllers 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.

The PS120 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 Controller's S terminal to provide a signal 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 the table below).

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

Table 10: Resistance of Common Copper Wire Sizes

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 the figure below), the voltage developed across it will be 6.4 volts. This effect is called ground lift.

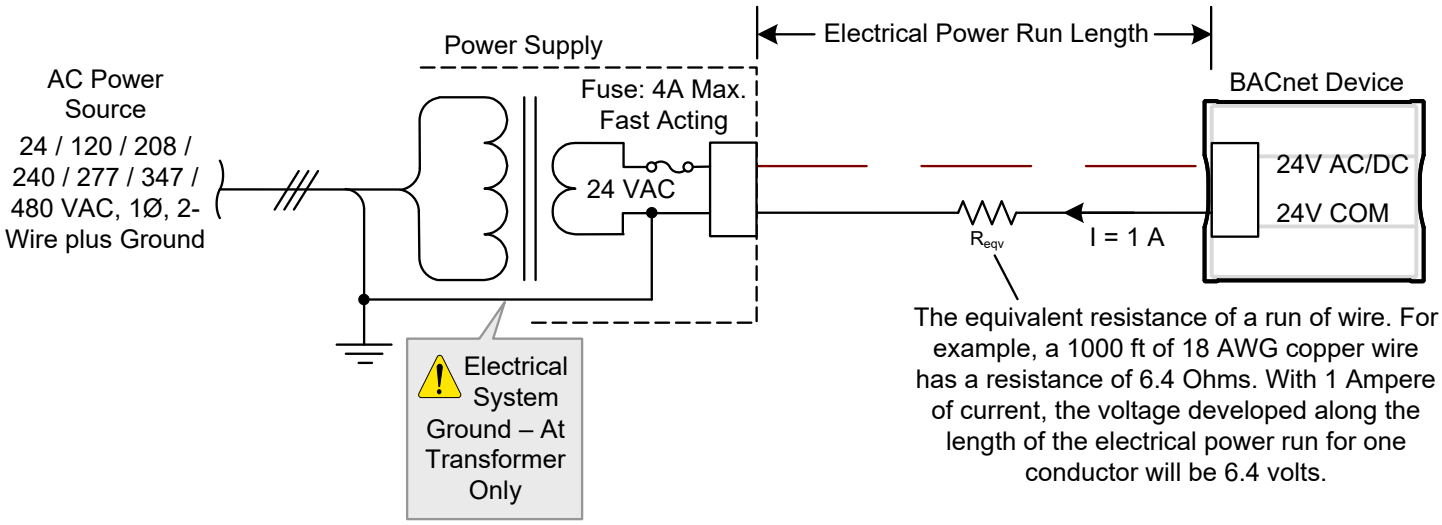


Figure 103: Ground Lift from a Long Power Run with a 24VAC Device

Because the 24V COM terminal on BACnet MS/TP 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 even voltage 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 RMS AC 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 communicating sensors). Refer to the respective module's datasheet for related power consumption information.

Transformer Selection and Determining the Maximum Power Run Length

To conform to Class 2 installation requirements, only use transformers of 100VA or less to power the device(s).

It is recommended to wire only one controller per 24VAC transformer.

For VAV devices, if only one 24VAC transformer is available, determine the maximum number of daisy-chained VAVs that can be supplied on a single power cable supplied by a 100 VA transformer based on the controller's expected power consumption including external loads, the cable's wire gauge, and the total cable length, using the following table. Any installation condition that is outside of the parameters of the following table should be avoided.

Daisy-chaining controllers is not permitted when a VAV controller's expected power consumption including external loads is over 15VA. In this case the controller must be connected to the 24VAC transformer in a star topology. The transformer must be installed in close proximity to the controller.

AWG	Power Run Total Cable Length	Maximum Number of Devices @ 7 VA per device	Maximum Number of Devices @ 10 VA per device	Maximum Number of Devices @ 15 VA per device
14[1]	75 m (250 ft.)	4	2	1
14	60 m (200 ft.)	5	3	2
14	45 m (150 ft.)	5	4	3
14	30 m (100 ft.)	5	5	4
16	60 m (200 ft.)	3	0	1
16	45 m (150 ft.)	5	3	2
16	30 m (100 ft.)	5	4	3
18	45 m (150 ft.)	3	2	1
18	30 m (100 ft.)	5	3	2

Table 11: Maximum Number of 24VAC VAV Devices on a Power Run with a 100 VA Transformer (Daisy-Chained)

1. Device terminals are not capable of accepting two 14 AWG wires (when daisy-chaining devices). Use a wire nut with a pig tail to make such a connection.

For non-VAV devices, determine the appropriate size transformer for the job as follows:

- ☐ Add up the power requirements of all devices plus all external loads (see *About External Loads*). Multiply the total power needed by a multiplier of 1.3, as a security 164margin. For example, to power five devices (15 VA each), the total load is 75 VA multiplied by 1.3 is 98 VA. Choose a size of transformer just over this amount: For example, a 100 VA model.
- ☐ When the total load of a number of devices requires a transformer with a rating greater than 100 VA, use two or more transformers. Ensure that the load to be connected to each transformer follows the guideline of Step 1 above.

24VAC Power Supply Connection

Use an external fuse on the 24VAC side (secondary side) of the transformer, as shown in the figure below, 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 *Common Identification Labels for BACnet MS/TP Data Bus Polarity for other Manufacturers*).

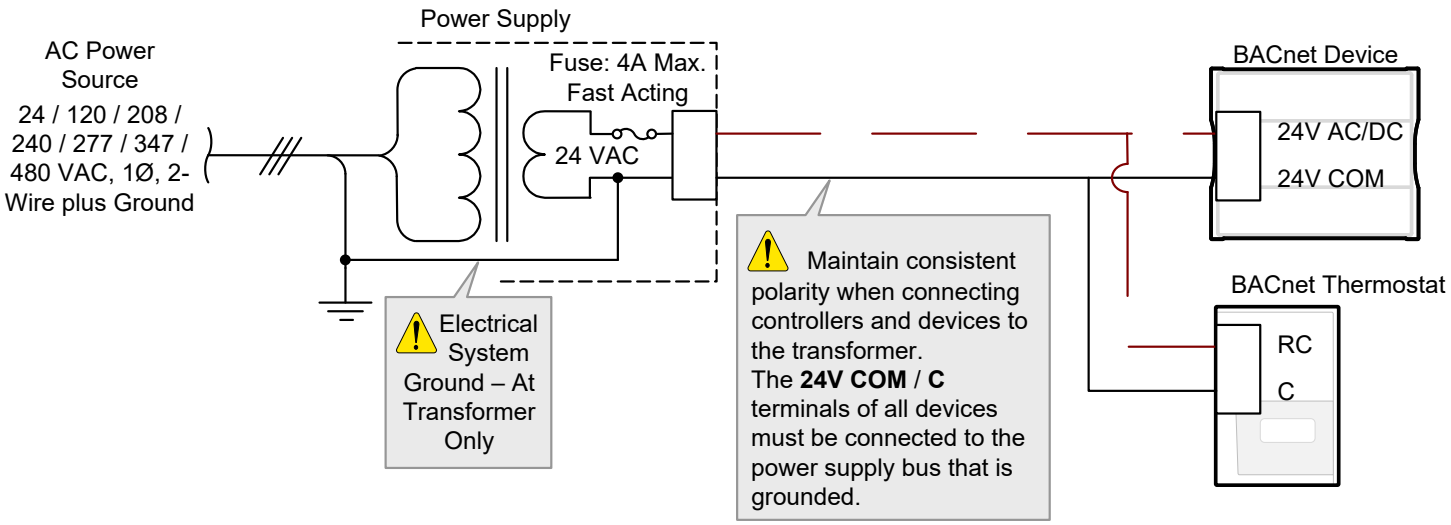


Figure 104: The 24V COM / C Terminal of all Devices must be Connected to the Grounded Power Supply Bus

CHAPTER 12
Modbus TCP Configuration

This chapter describes the Modbus TCP Configuration.

Controller Modbus Support

Certain ECLYPSE controller models support communication with Modbus devices. Refer to the controller's datasheet for more information.

Modbus TCP Device Connection

Modbus TCP devices are connected to the same subnet that the controller is connected to:

- Connect the Modbus TCP device to the same network switch/router to which the controller is connected.
- Connect the Modbus TCP device to either one of the controller's Ethernet ports.

Device Addressing

Device addressing allows the coordinated transfer of messages between the master (the ECLYPSE Controller) and the slave Modbus TCP device. For this, each Modbus TCP device is identified by its address.

About Device Addressing

Each slave device must have its own unique address number in the range from 1 to 254.
Refer to the device's hardware installation guide for information about how to set its address number.

CHAPTER 13
Modbus RTU Communication Data Bus Fundamentals

This chapter describes the Modbus RTU Communications Data Bus operating principles.

Controller Modbus Support

Certain ECLYPSE controller models support communication with Modbus devices. Refer to the controller's datasheet for more information.

For controllers that support either BACnet MS/TP or Modbus RTU network options, this option is selected in the controller's web interface. Modbus RTU communications are made by connecting directly to the RS-485 port.

Modbus RTU Data Transmission Essentials

When the ECLYPSE Controller is configured for Modbus RTU, it acts as the Modbus master that initiates requests to any slave device connected to this data bus. All slave devices must support Modbus RTU communications protocol. The ECLYPSE Controller does not work with Modbus ASCII devices.

The Modbus RTU data bus protocol uses the EIA-485 (RS-485) 3-wire physical layer standard for data transmission. EIA-485 is a standard that defines the electrical characteristics of the ECLYPSE Wi-Fi Adapters 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 Modbus RTU.

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.

Modbus RTU Data Bus is Polatiry Sensitive

The polarity of all devices that are connected to the Modbus RTU 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 Modbus RTU data bus polarity.

Controller	Typical Data Bus Connection Terminals		
	Inverting	Non-inverting	Reference
Common identification labels for Modbus RTU data bus polarity	D0	D1	SC, C, or C
	A or A'	B or B'	Common
	Data –	Data +	Data 0V

Table 12: Common Identification Labels for Modbus RTU Data Bus Polarity

When interfacing with Modbus RTU devices, refer to the documentation provided with the device to correctly wire the device.

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. It is strongly recommended that the following data bus segment cable specifications be respected.

Parameter	Details
Media	Twisted pair, 24 AWG
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)

Table 13: Modbus RTU Data Bus Segment Physical Specifications and Cable Requirements

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.

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

Table 14: Recommended Cable Types for Modbus RTU Data Buses

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. Meaning, they can electrically transmit 1, 0, and an idle state. When the transmitter is in the idle state, it is effectively offline 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. If a Modbus RTU device 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.

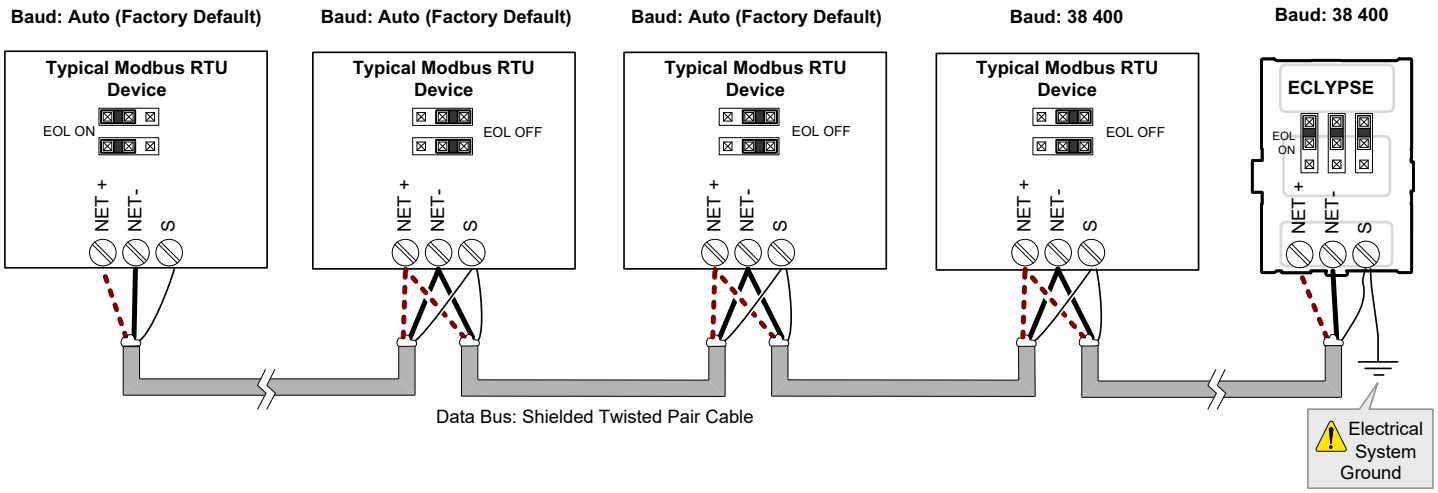


Figure 105: EOL Terminations Must be Enabled at Both the First and Last Device on the Data Bus

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 Modbus RTU Data Bus biasing) capabilities to be used at the end of a Modbus RTU data bus. Instead, use the *BACnet/IP to MS/TP Router* for this application.

About Setting Built-in EOL Terminations

ECLYPSE 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 ECLYPSE controller is located in the middle of the data bus and either one or both Modbus RTU devices at the data bus ends do not have biasing or EOL terminations. In this situation, set the bias on the ECLYPSE controller and set the EOL termination on the Modbus RTU devices at the end of the data bus. If a Modbus RTU device 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.

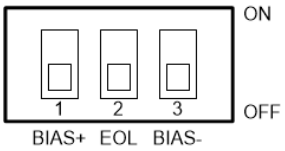


Figure 106: Typical ECLYPSE Controller with Separate EOL Termination and Bias Configuration Settings

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

Only a Daisy-Chained Data Bus Topology is Acceptable

Use a daisy-chained Modbus RTU data bus topology only. No other data bus topology is allowed.

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.

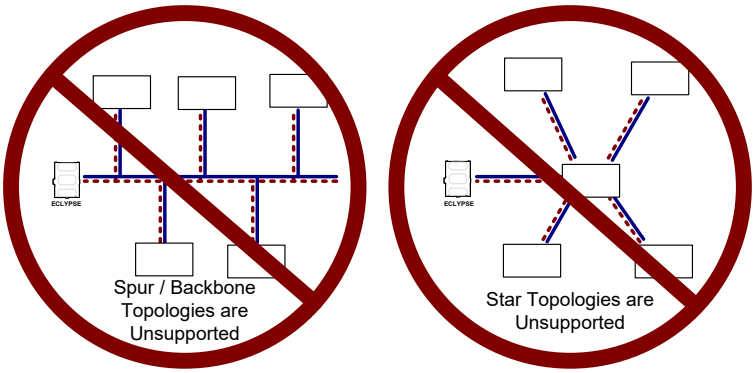


Figure 107: Unsupported Modbus RTU Data Bus Topologies

Data Bus Shield Grounding Requirements

The EIA-485 data bus standard requires that the data bus must be shielded against interference. A Modbus RTU data bus must also be properly grounded.

The data bus' cable shields must be twisted together and connected to the S or shield terminal at each ECLYPSE 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 Controllers, the data bus' cable shield provides the ground reference for the data bus. If the controller is at the end of the BACnet 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 shielding effectiveness.

Modbus RTU 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 ECLYPSE Controller, as shown below.

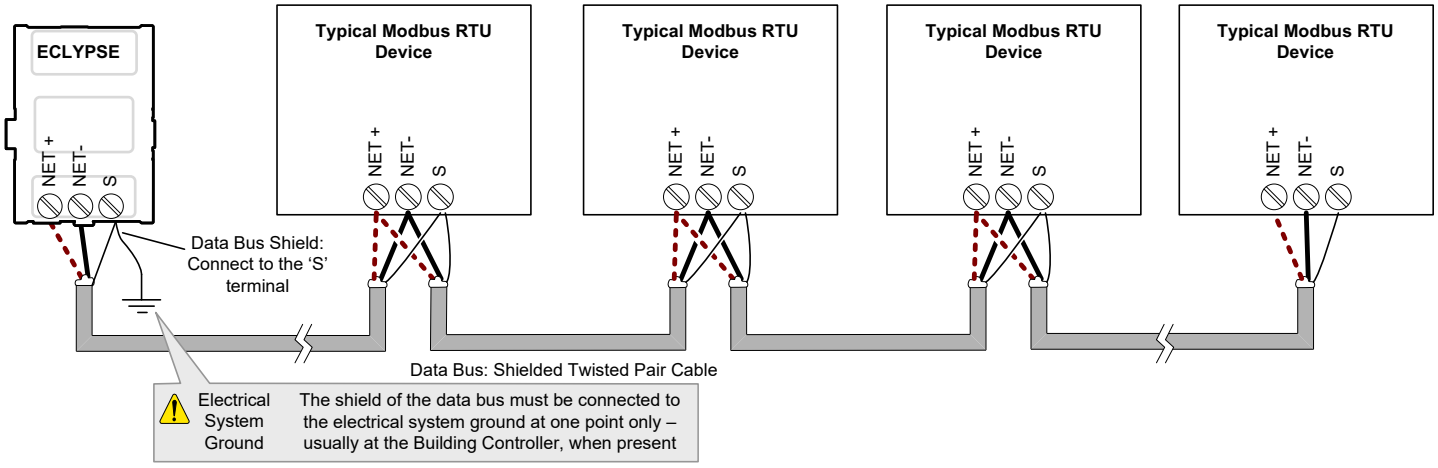


Figure 108: Typical Cable-Shield Grounding Requirements for a Modbus RTU Data Bus Segment with an ECLYPSE Controller located at the End of the Data Bus

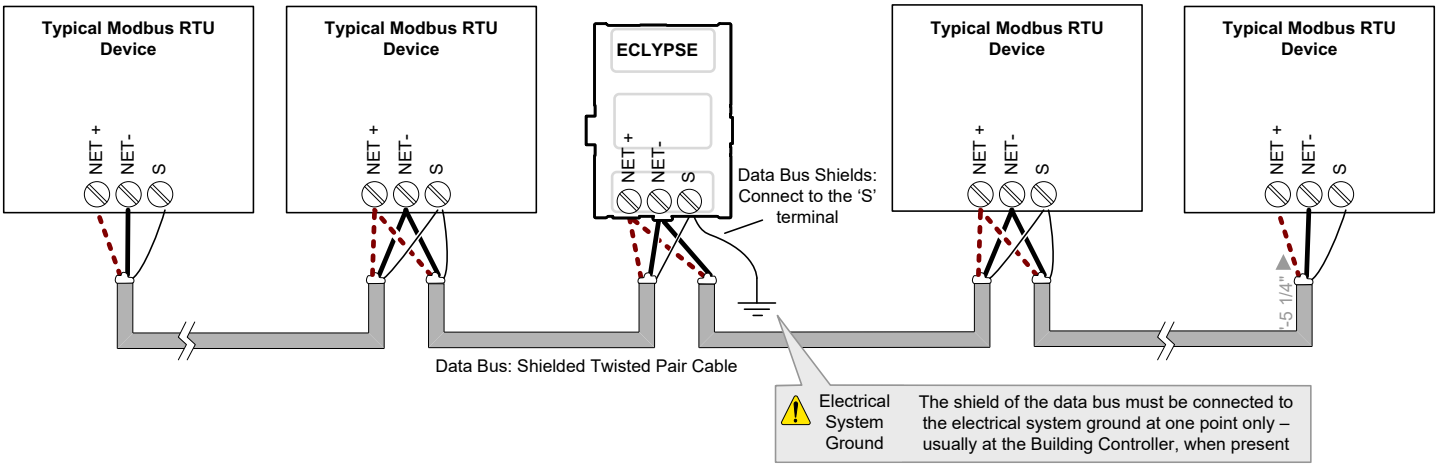


Figure 109: Typical Cable-Shield Grounding Requirements for a Modbus RTU Data Bus Segment with an ECLYPSE Controller located in the Middle of the Data Bus

Device Addressing

Device addressing allows the coordinated transfer of messages between the master (the ECLYPSE Controller) and the slave Modbus RTU device. For this, each device connected to the Modbus RTU data bus is identified by its address.

About the Device Address

Each slave device must have its own unique address number in the range from 1 to 247.

Refer to the device's hardware installation guide for information about how to set its address number.

CHAPTER 14
Resetting or Rebooting the Controller

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

Resetting or Rebooting the Controller

The reset button is located between the RS-458 and Ethernet connectors on an nLight ECLYPSE controller. 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. *Removing a Certificate*.

CHAPTER 15
ECLYPSE Controller Troubleshooting

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

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*.
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 24V COM 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 each controller. If it is set to 0 (all off), 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. 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 the LED Fault Conditions provided by the manufacturer of your BACnet controller. This range is for slave devices that cannot initiate communication.
	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 the LED Fault Conditions provided by the manufacturer of your BACnet controller.
Controller communicates well over a short network BACnet MS/TP network, but does not communicate on large network	Network length	See *Data Bus Physical Specifications and Cable Requirements*.
	Wire type	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.

Symptom	Possible Cause	Solution
	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. See *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	Check the configuration of the output with an HVAC programming tool. For example, is it enabled?
	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 15: Troubleshooting Controller Symptoms

Action	Recommendation
Properly terminate the BACnet MS/TP data bus	EOL terminations must be enabled / installed at either end of the data bus only. See *When to Use EOL Terminations*.
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.
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 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*.

Table 16: Verify that the Following Recommendations have been Carried Out Before Calling Technical Support

CHAPTER 16
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.

Symptom	Possible Cause	Solution
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 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 Wi-Fi Adapter	Exchange the wireless dongle with another 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*.
No communications even though the 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.

Table 17: Troubleshooting Wi-Fi Network Symptoms

CHAPTER 17
Single Sign On (SSO) Troubleshooting

You can use this Troubleshooting Guide to help detect and correct issues with the SSO functionality. Even though the following table provides a work around to the issues, in general, we highly recommend that you always find the solution to any problem you may encounter.

Symptom	Possible Cause	Work Arounds	Solution
Recovery password is requested in the Web browser.	SSO Server is down or a networking or connection issue has occured.	Enter your recovery password.	Verify the server status and server connections. Verify the network connectivity. Reconfigure the SSO parameters. See Setting Up the SSO Functionality