PHILIPS
dynalite

System Builder

Ethernet Gateways

PDEB, PDEG, PDDEG-S

Ethernet Gateways

Commissioning Guide

Revision 18

About this document

This document describes the Ethernet Gateways (EG) commissioning process. A working knowledge of IP addressing, System Builder (SB), Connected Lighting and Dynalite commissioning processes is required to effectively use this document.

Target audience

Commissioning engineers

Prerequisites

Before commissioning the product, you should have completed System Builder training course.

Disclaimer

These instructions have been prepared by Philips Dynalite and provide information on products for use by registered partners or owners. Some information may become superseded through changes to the law and as a result of evolving technology and industry practices. Any reference to non- Philips products or web links does not constitute an endorsement of those products or service.

The approach in this guide will be generic in nature. However, depending on the geographic location of the building, there will be national, regional, and local electrical and occupancy regulations that will need to be considered in the planning and implementation and installation of the system.

Copyright

© 2022 Signify Holding. All rights reserved. Specifications are subject to change without notice. No representation or warranty as to the accuracy or completeness of the information included herein is given and any liability for any action in reliance thereon is disclaimed. Philips and the Philips Shield Emblem are registered trademarks of Koninklijke Philips N.V. All other trademarks are owned by Signify Holding or their respective owners.

Icon Legend

- Danger
- Warning
- Important
- Note
- Tip

Contents

PDEB, PDEG, PDDEG-S

1 Product Overview 5
1.1 Introduction 5
1.2 Features 6
2 Commissioning 8
2.1 Connecting System Builder 10
2.1.1 Adding an IPv4 port 13
2.1.2 Connection status 14
2.1.3 Creating a Site CA Certificate 15
2.1.4 System Hardening 16
2.2 Wireless Commissioning 17
2.2.1 Adding an EG 17
2.2.2 Adding an IP Address 19
2.2.3 Configuring the wireless router 21
2.2.4 Connect wirelessly 22
2.3 Ethernet Access Point 23
2.3.1 Wi-Fi access 24
2.3.2 Uploading files 25
2.3.3 CGI access 27
2.3.4 HTTPS Secure Access 31
2.4 Ethernet Bridge 36
2.4.1 Address Offsets 36
2.4.2 Ethernet to RS-485 37
2.4.3 Ethernet to Ethernet 42
2.4.4 Secure Ethernet to RS-485 45
2.4.5 Secure Ethernet to Ethernet 48
2.4.6 Connecting to the Ethernet Trunk 51
2.4.7 Connecting to a Serial Spur 53
2.5 Adding devices to a spur 55
2.6 Setting time zone and realtime clock 56
2.7 Area Cascading 57
2.8 Day Rhythm lighting 59
3 Integration 64
3.1 Hue Integration 64
3.1.1 Configuring Hue lamps 65
3.1.2 Adding Hue bridges 65
3.1.3 Mapping Hue configuration 66
3.2 Text over IP 69
3.2.1 SendPF text commands 70
3.2.2 SendP text commands 71
3.2.3 Receive text commands 72
3.2.4 Receive binary commands 73
3.2.5 Cool Automation integration 74
3.3 DyNet Text 79
3.3.1 Syntax 79
3.3.2 Telnet access 80
3.3.3 Commands 81
3.3.4 Responses 85
3.4 Integration alternatives 87
4 BACnet Gateway 88
4.1 Overview 88
4.2 Integration Design 89
4.3 Connecting to BACnet 89
4.4 BACnet Configuration Wizard 90
4.5 Licensing 93
4.6 Test Functionality 94
5 Philips Web Interface 95
5.1 Ethernet Gateway Overview 95
5.2 Scheduler 96
5.2.1 All Schedules 96
5.2.2 Public Holidays 96
5.2.3 Special Events 97
5.3 Schedule Editor 97
5.3.1 Edit Schedule 97
5.3.2 Add Actions 101
5.4 Controls 102
5.4.1 Area Management 102
5.5 Status 104
5.5.1 Status Overview 104
5.5.2 Devices 105
5.5.3 Date & Time 105
5.6 Languages 107
5.7 Log files 109
6 System Manager Schedules 110
6.1 Schedule Deployment 110
6.2 Schedule limitations 111
7 Property Editors 113
7.1 Device Properties 113
7.2 Connection Settings 118
7.3 Create Device 119
7.4 Schedules 120
7.5 Bridge Address Ranges 125
7.6 Port Editor 126
7.7 Routing 129
7.8 Hue Bridges 129
7.9 Metrics 129
7.10 Users 130
7.11 Switches 132
7.12 Tasks 137
7.13 Device Discovery 138
7.14 Product Details 140
8 Appendix A: Firmware Upgrade 141
9 Appendix B: Replacing a 100BT 143
10 Appendix C: Signify Certificate Installation 150

1 Product Overview

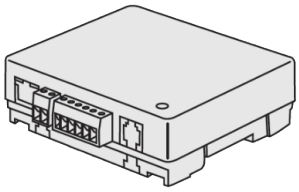
1.1 Introduction

The PDEB, PDEG and PDDEG-S are hardware Ethernet Gateways (EGs) designed to link network segments together, using the internet or local area network (LAN). They provide a multipurpose Ethernet connection for connected lighting control systems, enabling bridging functionality between an Ethernet trunk and a DyNet RS-485 spur or between an Ethernet trunk and an Ethernet Spur (PoE or wireless subnet). The PDDEG-S also provides a secure connection to the cloud and to other Ethernet enabled devices.

The flexible functionality of each Ethernet Gateway (EG) extends the control system over existing Ethernet networks for communication with third party systems or where segments of the control system are separated by great distances. It enables remote control of sites and offers monitor and manage capabilities similar to System Manager. The bridge supports IPv4 and IPv6 protocols, with Static or DHCP assigned IP addressing. inbuilt routing, message filters, and links multiple EG's together in a system.

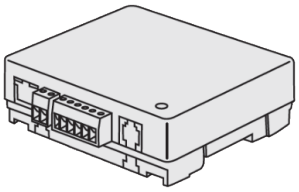
An inbuilt webserver offers a simple end-user interface for different browser-based control scenarios, where the full System Manager suite is not required. The interface incorporates a timeclock, schedule editor and a task engine that can process conditional and sequential logic and arithmetic functions.

Wi-Fi access to an EG facilitates personal control from mobile applications or for wireless commissioning.



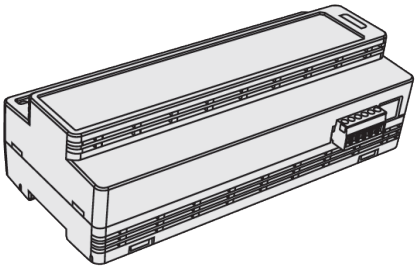
PDEB

Philips Dynalite Ethernet Bridge



PDEG

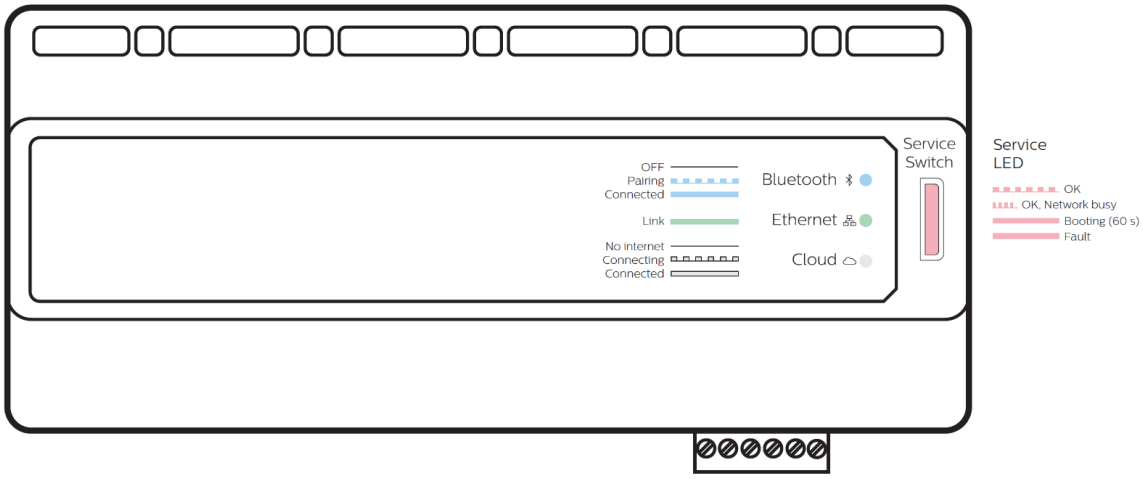
Philips Dynalite Ethernet Gateway



PDDEG-S

Philips Dynalite DIN-rail Ethernet Gateway – Supervisor

PDDEG-S Indicator LEDs



LED Indications

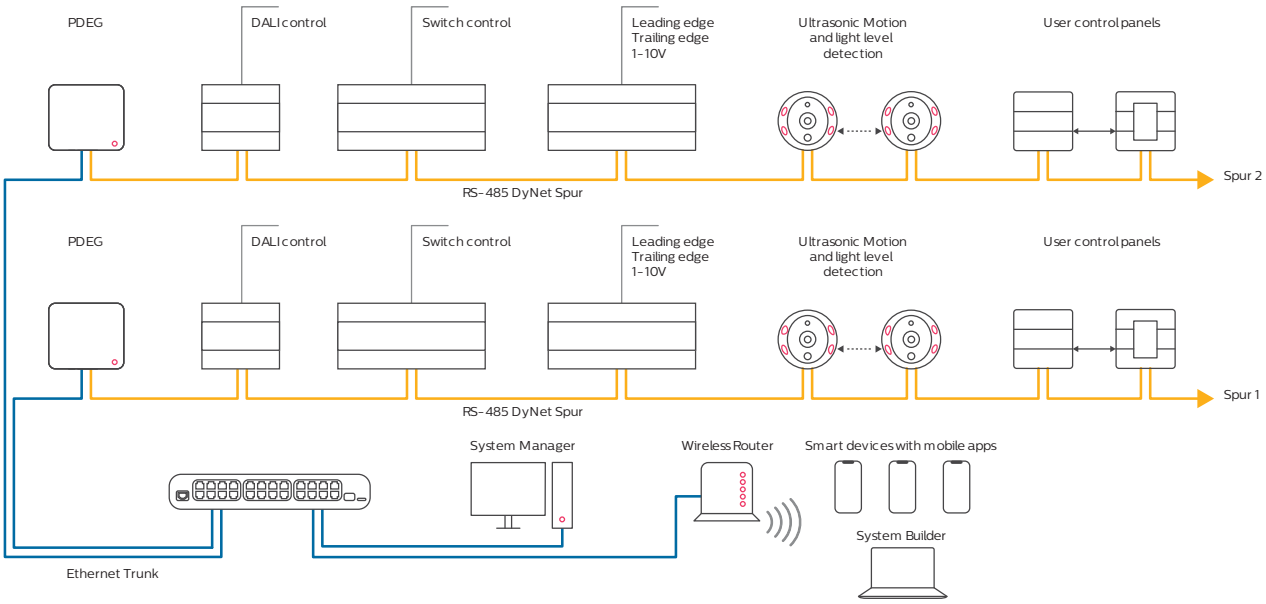
1.2 Features

Feature	PDEB	PDEG	PDDEG-S
Routing Address offset and message filtering.	●	●	●
Translation Between DyNet1 and DyNet2	●	●	●
Network checker Network/device status monitor and traffic log, system metrics.	●	●	●
Area Cascading controller Occupancy control for multiple dependent areas.	●	●	●
IP Addressing UDP, TCP IP (IPv4/IPv6)	●	●	●
Protocols DyNet text, Text over IP	●	●	●
Ethernet field network DyNet, DyNet2	●	●	●
Modbus power meters Modbus over RS-485 Modbus over IP (only available on PDDEG-S)	●	●	●
Hue Integration	●	●	
Scheduler Real-time clock and backup battery.		●	●
Mobile device Mobile apps: EnvisionTouch, DynamicTouch, Philips Dynalite Control		●	●
Web apps and APIs Webserver, CGI, RESTful APIs		● (http/https)	● (https)
External Authentication OAuth, LDAP			●
Secure connections TLS TCP connections between System Manager, Gateway, and Ethernet devices.			●
Cloud services Interact Cloud, Azure Cloud, Google Home, Amazon, Apple, 3rd party cloud.			●
BACnet integration BACnet.			●

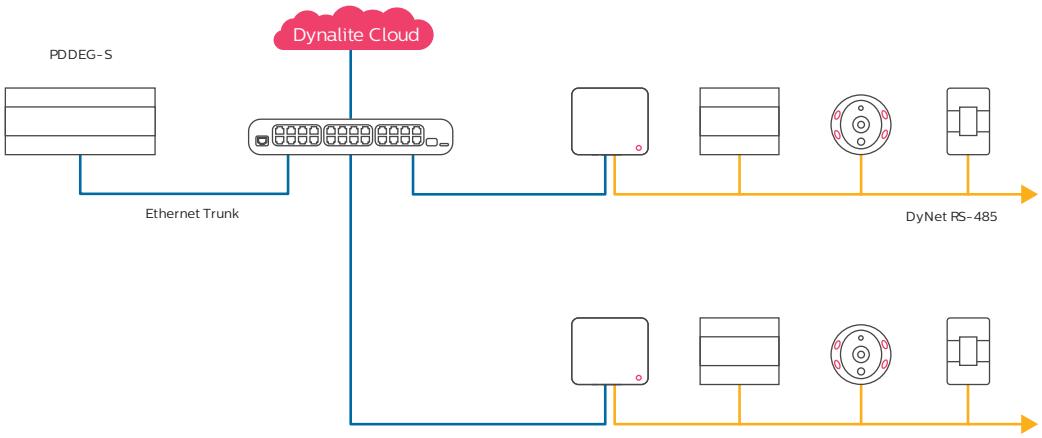
2 Commissioning

The EG acts as a bridge between RS-485 and Ethernet networks or between multiple Ethernet socket connections. This allows a trunk and spur system to be easily scaled up by adding an EG for each required spur. Note: A PDDEG-S must be used for secure Ethernet connections.

In addition, the PDDEG-S can function as a building connectivity bridge to connect the on-premises system to the cloud or to a multisite system.



Hybrid Ethernet and RS-485 control system



Control system with PDDEG-S gateway

The Dynalite cloud facility is currently under development.

Ethernet gateways have several standard applications that can be easily configured by selecting one of the options in the Bridge Configuration Wizard:

1. **Ethernet Access Point** - standard routing for Ethernet connections to the gateway.
2. **Ethernet to RS-485 Translation Gateway** - routing and translation between Ethernet trunk and DyNet RS-485 spur devices.
3. **Ethernet to Ethernet Translation Gateway** - routing and translation between an Ethernet trunk and other Ethernet devices. Can be used to configure secure Ethernet communication between PDDEG-S and spur Ethernet devices such as the DDBC320-DALI.
4. **Ethernet to IPv6 Multicast Gateway** - routing and translation between Ethernet trunk and IPv6 multi-cast spur connection to PoE Luminaires or Wireless Gateway (PDZG-E) devices. This option is also used to configure a hybrid system (DyNet, PoE, Wireless) by selecting 'Enable RS-485 Spur' in Step 2.
5. **Hotel Floor Ethernet Gateway** - routing and translation between Ethernet trunk and GRMS devices.
6. **Hotel Room Ethernet Gateway** – routing and translation between Ethernet spur and RS-485 devices (for GRMS devices only).

WebSocket/Cloud Connection/BACnet integration is now included in options 1, 2 & 4.

For more information on option 4, please refer to the POE Wired or Wireless Commissioning Guides.

For more information on options 5 & 6, please refer to the STR Commissioning Guide.

All gateways confgurations are limited to 50 Ports, 100 Routing Records and 200 Filters. These limits are quickly exceeded when using common areas between gateways. Do not use common areas unless there is a genuine need.

For security purposes, the PDDEG-S cannot be factory reset from System Builder. Use the following procedure to factory reset the PDDEG-S.

Factory reset a PDDEG-S:

1. Disconnect the power from the PDDEG-S.
2. Remove the front cover.
3. Move the jumper wire to link positions 1-2.
4. Power on the PDDEG-S and wait ~30 seconds for it to reboot.
5. Power off the PDDEG-S.
6. Move the jumper wire to link positions 2-3.
7. Replace the front cover.
8. Power on the PDDEG-S and wait ~30 seconds for it to reboot.

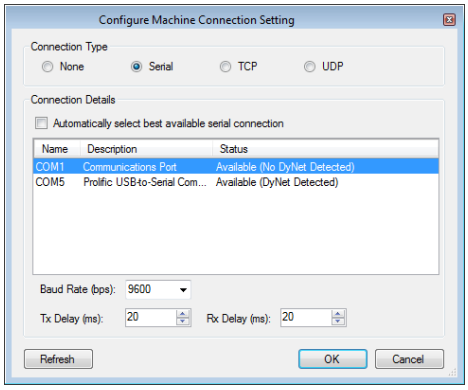
2.1 Connecting System Builder

Before you start commissioning you must first connect System Builder (SB) to the system. Use a USB PC node adapter to connect over RS-485 or an EG to connect over Ethernet or Wi-Fi.

To establish a successful connection, select the Job name (to connect to the trunk) or a Gateway/Bridge (to connect to a spur) in the tree and click Connection Settings then select the Connection Type:

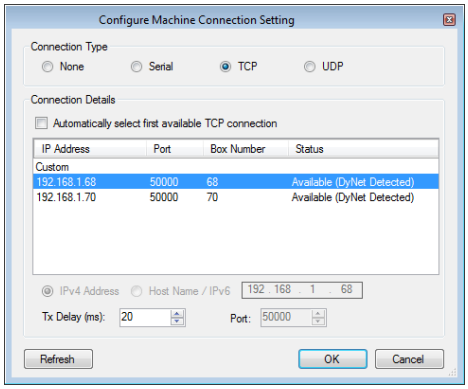
Serial RS-485 connections

The Connection Details section lists the available USB COM ports and shows the port status.



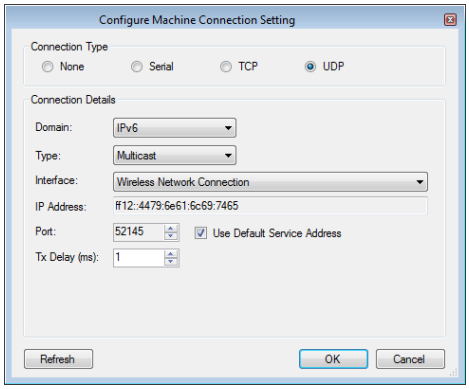
TCP Ethernet connections

The Connection Details section lists the available EGs configured with TCP IP addresses, port numbers and Box numbers and shows the port status. The default port number is 50000.



UDP Ethernet connections

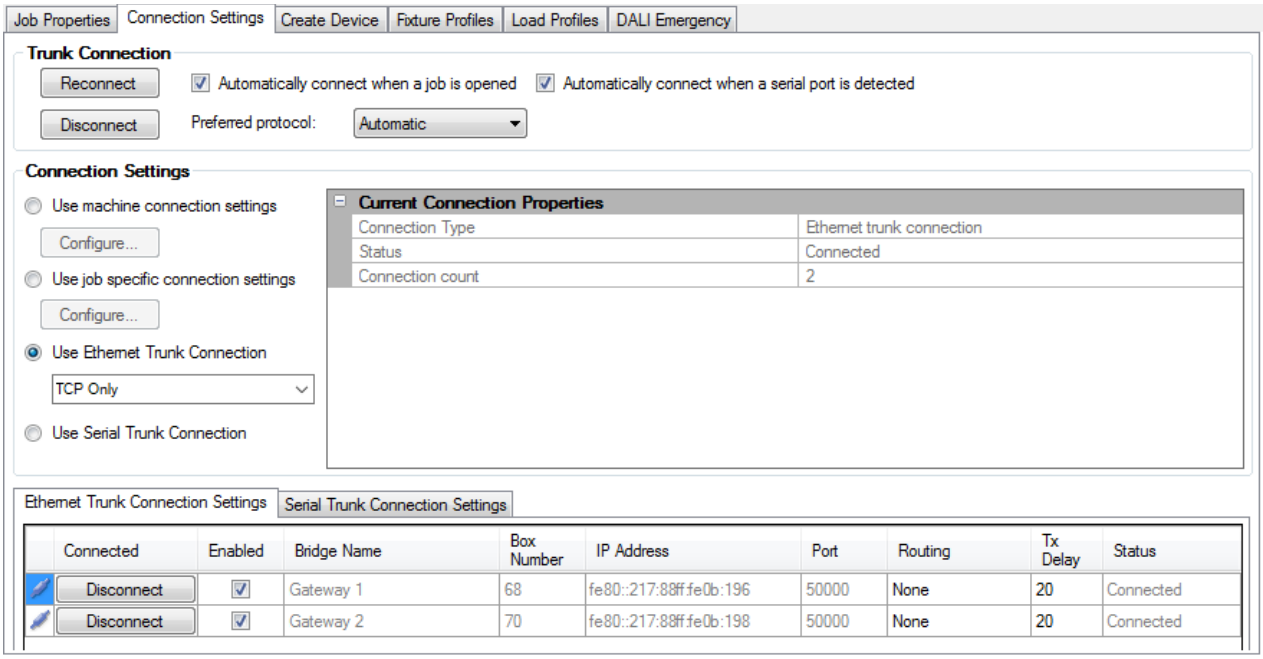
The Connection Details section allows you to select the Domain, Type, Interface, IP address and Port number. The default is IPv6 multicast service address: ff12:4479:6e61:6c69:7465 Port 52145.



Note: for security purposes, the UDP Multicast default service address is being replaced. To connect to Ethernet devices, click the Insert Devices from Network icon and select Discover Network > Discover Devices over Ethernet (This will find Ethernet devices even when SB is disconnected).

Ethernet Trunk connection

The Ethernet Trunk Connection Settings page lists the available EGs configured with TCP IP addresses, port numbers and box numbers and shows the port status. The default port number is 50000. This connection is only available after EG commissioning is complete.

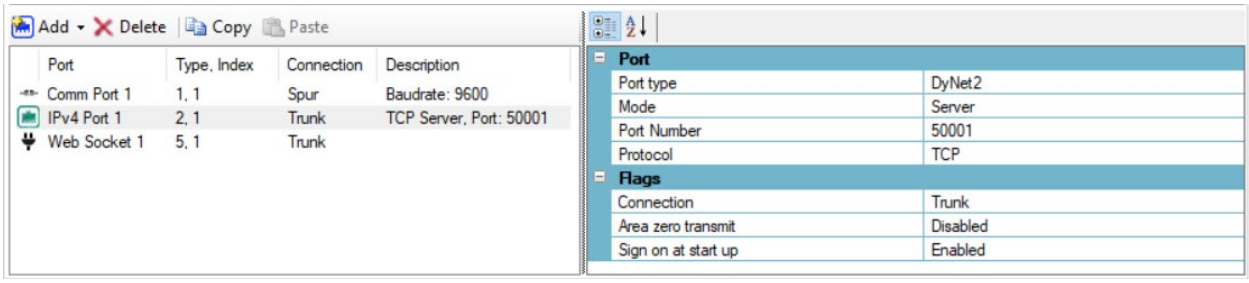


2.1.1 Adding an IPv4 port

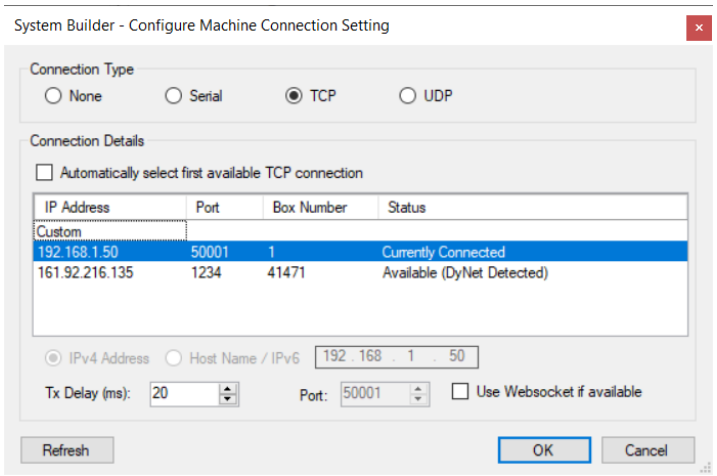
If you want to create a TCP connection to the EG instead of using a serial connection or UDP IPv6 multicast connection, you can add a TCP IPv4 port and make the gateway a server.

Add an IPv4 port:

1. Plug in a PC Node to the USB port on your PC and then to the RS-485 port on the device.
2. Connect SB to the device via the RS-485 network serial port.
3. Click, the Port Editor tab.
4. Set Static IP to True.
5. Enter an IP address (for example, 192.168.1.50).
6. Click Add and select IPv4 port.
7. Configure the IPv4 Port with the following settings.



8. Press F12 or click Save to Device.
9. Click Send Device Reset.
10. After the device reboots, reconnect SB with a TCP connection. For example,

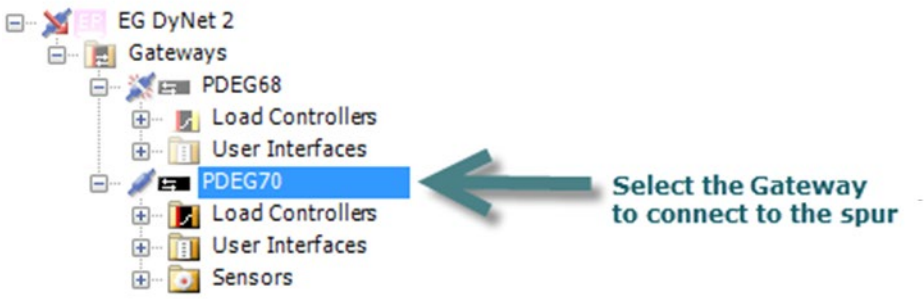


2.1.2 Connection status

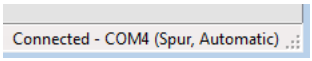
You can connect your PC to any device in a single spur network; however, for multiple spur networks System Builder (SB) needs to know if it is physically connected to the trunk or to the spur to ensure that it can correctly address devices. In multi-spur networks the following icons in the tree show which part of the network SB is connected to:

- SB is currently connected to this trunk or spur
- SB is connected at a level above this spur
- SB is connected at a level below this trunk
- SB is NOT currently connected to this trunk or spur

Spur example:

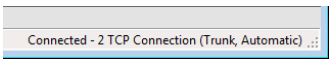


SB shows the connection status in the lower right corner



Trunk example:

SB shows the connection status in the lower right corner



SB can connect to a Trunk or Spur in the system without physically changing how the PC is plugged in. Check that the physical connection matches the view in the tree. Errors in address translation may occur in your system if you change configuration or add devices whilst being connected to a different level/bridge than intended.

2.1.3 Creating a Site CA Certificate

The Site CA certificate (Site Private Key) is created in SB and is then used to sign and upload a Device Site Certificate to the PDDEG-S gateways and to Ethernet devices: When SB has a Site CA certificate, it shows a green lock icon at job level in the System and Building views.

SB shows a green lock icon next to an PDDEG-S or Ethernet device when a Device Site Certificate has been uploaded. This enables SB/SM and Ethernet devices to securely connect to the PDDEG-S gateways via a secure TLS TCP connection.

If the lock icon on an EG shows a warning icon, then check the tooltip as it will indicate either:

- Device site certificate configured but Site CA used to sign the device site certificate is not found on this machine. System Builder will be unable to securely connect to this device. Ensure correct Site CA certificate is imported into this machine with the Tools menu, **Set Site CA Certificate** option.
- Device site certificate configured but doesn't match Site CA configured in job. System Builder will be unable to securely connect to this device. An updated device site certificate should be signed and uploaded to the device.

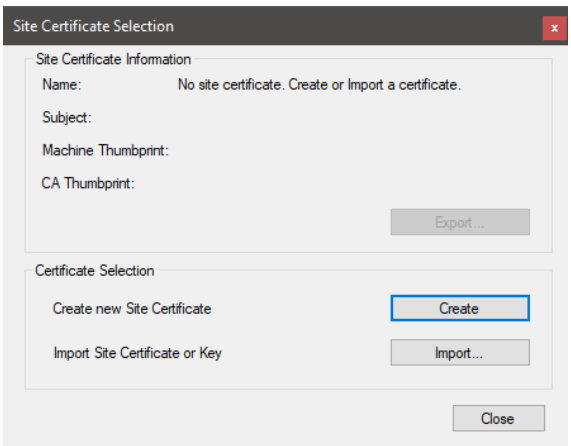
The Site CA certificate is stored in your machine not in the job file. To allow another machine to commission the same site you must securely send the job file, the Site CA Certificate, and the password.

Having a lock icon in SB, a gateway, or a device simply means you have created and uploaded a certificate. You still need to configure the secure connections (with the bridge configuration wizard) and save to device before you can connect securely.

For more information, refer to topics 2.4.4 Secure Ethernet to RS-485 2.4.5 Secure Ethernet to Ethernet.

Create/Import Site CA Certificate:

1. From the Tools menu, select **Set Site CA Certificate** to open the Site Certificate Selection window.
2. If starting a new job, click the Create button to create a new Site Certificate.
   a. After creating a new Site Certificate, you will be prompted to Export the Site Certificate and save it in a secure location.
   b. For additional security when exporting the Site Certificate, you must enter a password. This password will be required by anyone importing the site certificate into another machine.
3. If someone has already started commissioning any of the devices and already created a Site Certificate, then they will need to export the certificate from their machine. You can then import the Site Certificate and enter the password into any machines used to commission or connect to secure Ethernet devices.



2.1.4 System Hardening

The proprietary DyNet communication over IP networks may or may not contain any additional security measures. Therefore, it is recommended that physical access to the system is restricted to authorized persons only and is segregated from other Ethernet based networks.

To mitigate the risk of unauthorized access to a system, it is important that during commissioning, site specific information is stored securely and only shared with relevant project stakeholders.

System hardening must be performed on every system before handover to the customer. Ensure that you secure all system connections and interfaces as much as possible. To complete commissioning, the commissioning engineer must disable all connectivity except that required and remove default credentials.

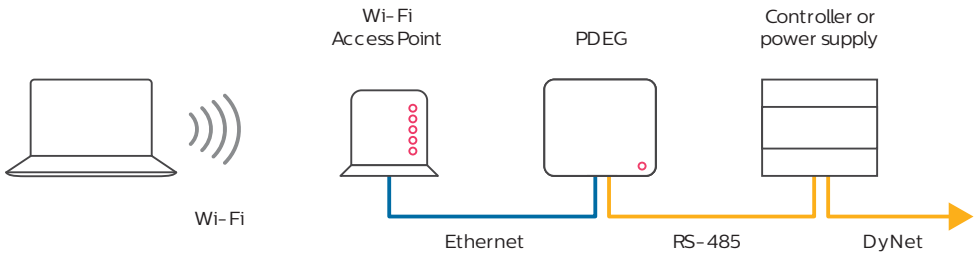
System Hardening checklist:

- ☐ 1. Backup databases.
- ☐ 2. Install gateways and controllers in a secure enclosure/distribution board/room.
- ☐ 3. Make the data cabling physically inaccessible except to authorized persons, as much as possible.
- ☐ 4. Use a VLAN or separate cables to segregate the control network from corporate IP networks.
- ☐ 5. Use a secure connection or VPN where possible for connections to Integrated systems.
- ☐ 6. Delete unnecessary System Manager user accounts and carefully manage necessary accounts.
- ☐ 7. Delete unnecessary Ethernet gateways user accounts.
- ☐ 8. Enable CGI (only) user authentication on interfaces.
- ☐ 9. Implement LDAP + StartTLS for user authentication on relevant devices, where possible.
- ☐ 10. Remove unnecessary user permissions.
- ☐ 11. Implement complex user passwords in interfaces (8-12 Characters).
- ☐ 12. Implement complex user passwords in gateways (> 20 character fully random, that is not shared by any other gateway).
- ☐ 13. Disable UDP default multicast port.
- ☐ 14. Disable UDP default unicast port.
- ☐ 15. Disable WebSocket if not used.
- ☐ 16. Remove unnecessary protocols and disable unnecessary features such as FTP and Telnet.
- ☐ 17. Disable unnecessary ports.
- ☐ 18. Install security certificates in gateways to establish TLS TCP connections, where possible.
- ☐ 19. Install security certificates on the server/client machines to use HTTPS connections where possible.
- ☐ 20. Install 802.1X certificates to enable 802.1X (https://en.wikipedia.org/wiki/IEEE_802.1X)

For more information, refer to the Dynalite System Hardening Guide.

2.2 Wireless Commissioning

A wireless connection from EG to System Builder (SB) makes it possible to commission a system from anywhere within Wi-Fi range. The EG does not need to be part of the job file when commissioning wirelessly. However, the EG does require some initial configuration to support Wi-Fi connections.

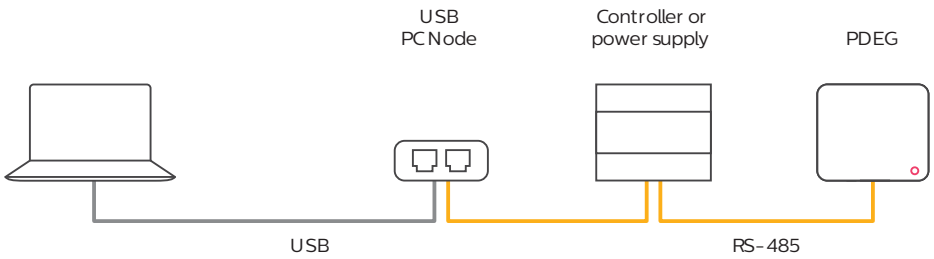


2.2.1 Adding an EG

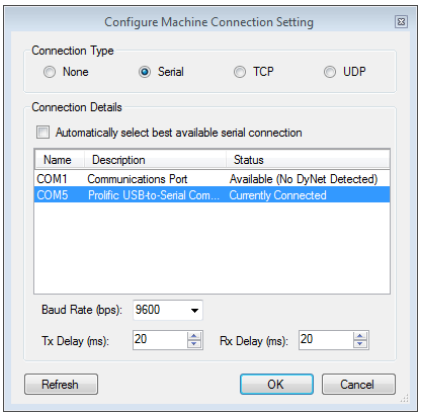
The following topic describes how to setup an EG and wireless router to support wireless commissioning.

Add an EG to the job over RS-485:

1. Plug the EG into a DyNet port on a spur to provide power and communications via the RS-485 network.
2. Plug the commissioning PC into a USB PC node, then plug the USB PC node into a DyNet port on the same spur.

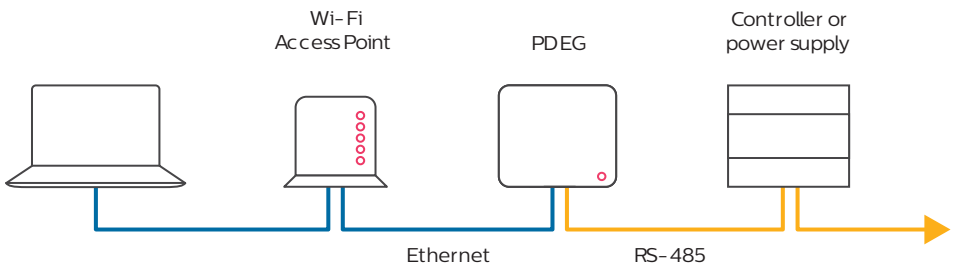


3. Launch SB and connect using a serial connection.
4. Click Insert Devices from Network.
5. Press the Service switch on top of the EG (to sign-on the device) or search by device code for EG (0xDC). The EG now appears in the Discovered Devices list.
6. Select Add and Load Devices. The EG appears in the Job.
7. Close the Insert Devices from Network dialogue box.



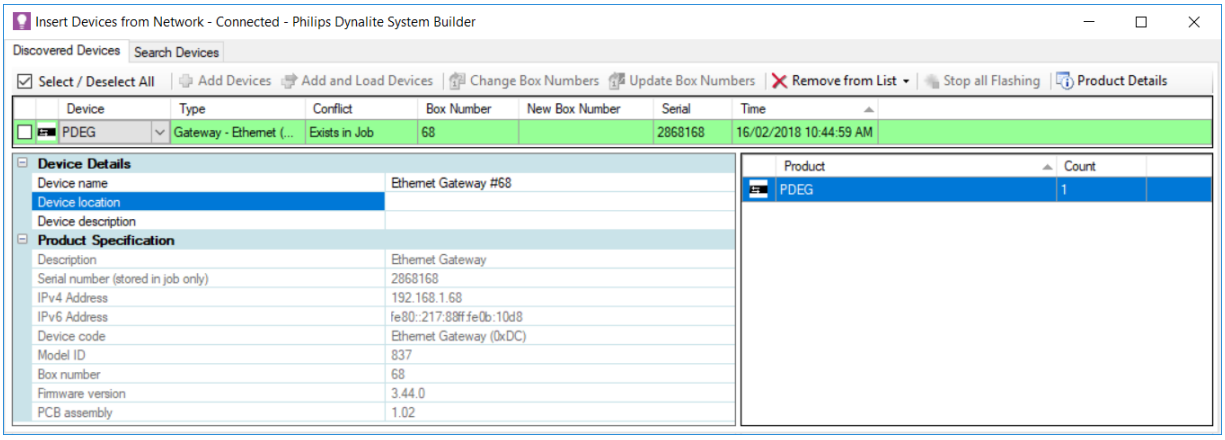
Add an EG to the job over Ethernet:

1. Connect power to the EG either via the DyNet port or via the terminal strip.
2. Plug the commissioning PC into the EG Ethernet socket, either directly or via a router (check that you have selected the correct Interface adapter for your PC).



3. Launch SB and click Insert Devices from Network
4. Select Discover Network > Discover Devices over Ethernet (This will find Ethernet devices even when SB is disconnected) or press the device service switch (to sign-on the device) or search by device code for EG (0xDC) or PDDEG-S (0xBE).

   The EG now appears in the Discovered Devices list.
5. Select Add and Load Devices. The EG appears in the Job.
6. Close the Insert Devices from Network dialogue box.



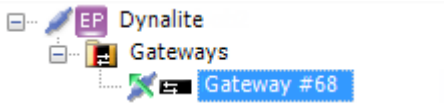
For security purposes, the UDP Multicast default service address is being replaced. To connect to Ethernet devices, click the Insert Devices from Network icon and select Discover Network > Discover Devices over Ethernet (This will find Ethernet devices even when SB is disconnected).

2.2.2 Adding an IP Address

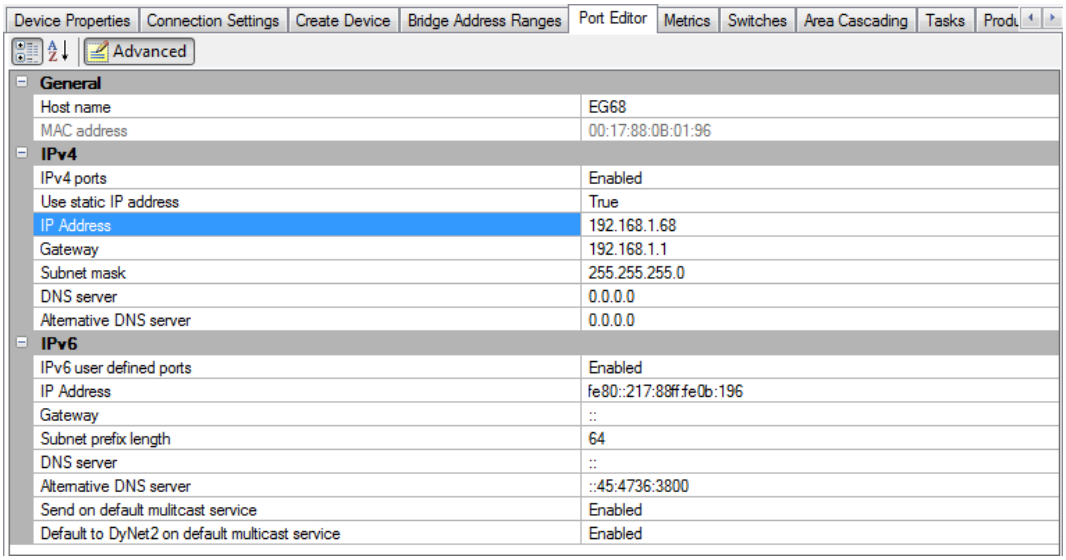
To create a TCP IPv4 connection, EG must be configured with a valid IP address. The IP address should be set to an appropriate subnet address and can be either static or dynamically assigned by the router using DHCP. This specifies the destination address for DyNet commands received by the EG.

For example, where the subnet mask is 255.255.255.0 (the default mask for Class C IP addresses) and the routers local IP address is 192.168.1.1, the EG address should be set in the range 192.168.1.2 to 192.168.1.255.

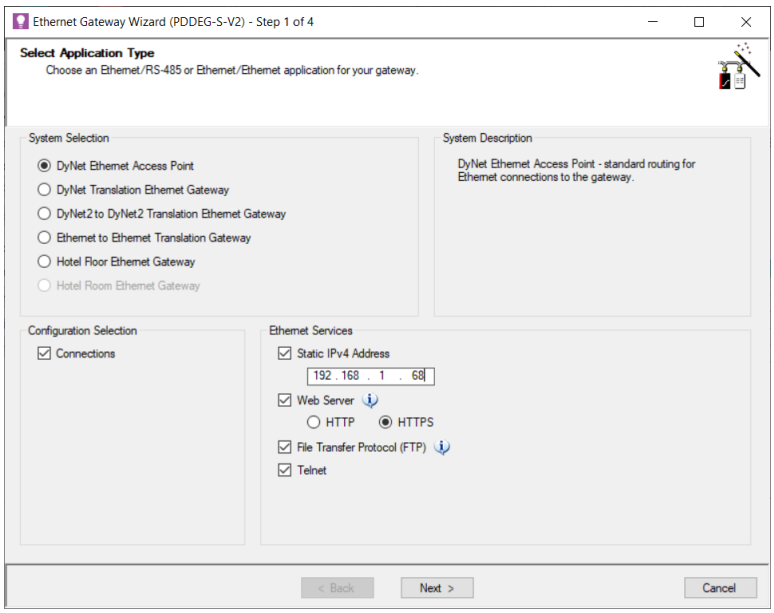
Configure IP address and Ethernet access point:



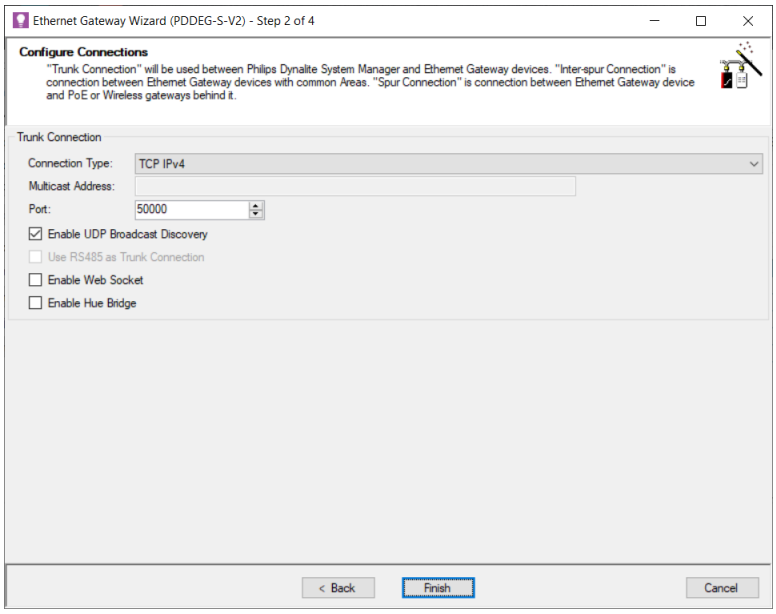
1. Select the EG from the Device tree.
2. In the Port Editor page enter a Host name.
3. Under IPv4 properties, set Static IP to True (or False if using DHCP).
4. When using a Static IP address, enter an IP address for the EG.
5. In the Gateway property, enter the IP address of the router.
6. In the Subnet mask property, enter the subnet mask of the router if different to the default value.



7. Right-click the EG in the Device tree and select Bridge Configuration Wizard... or press Alt+W.
8. Select DyNet Ethernet Access Point and click the Next button.



9. In Connection Type, select TCPv4 and in Port, select 50000. Click the Finish button. The Port Editor and Router properties are set by the wizard.



The **Enable UDP Broadcast Discovery** checkbox, enables the UDP IPv4 discovery port (Port 9998) used by DynamicTouch to discover the EG. It also allows the EG to appear in the list of bridges found in the Connection Settings page under Ethernet Trunk Connection Settings.

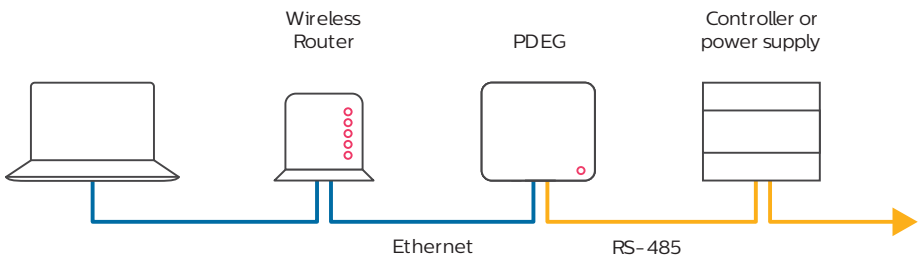
10. Click Save to Device.
11. Unplug the USB PC node.

2.2.3 Configuring the wireless router

The process of setting up a wireless router varies between brands, but the basic procedure should be similar.

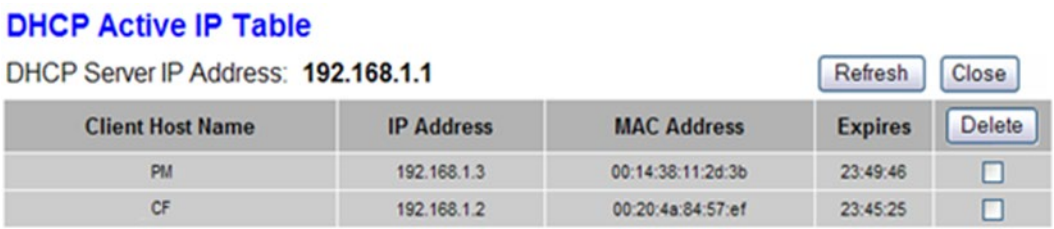
Configure wireless router:

1. Plug the EG into a DyNet port with a DyNet cable.
2. Plug the EG into the router with an Ethernet cable.
3. Plug your PC into the router with an Ethernet cable.



4. Enter the default IP address of your router (http://192.168.0.1 or http://192.168.1.1) into your browser to open the router configuration pages.

5. Log into the router with the administrator ID (admin) and password (password) and then navigate through the menu to find the list of connected devices or DHCP clients on the wireless router. Refer to manufacturer's documentation.



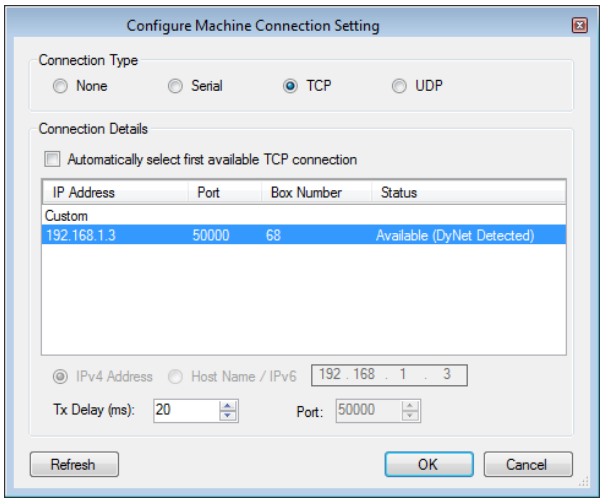
6. Identify the EG in the table. The client host name is the Host name as configured in the SB Port Editor if using DHCP (not displayed for static IP addresses).
7. Configure the wireless network properties of the router, including a unique SSID and security settings. Ensure all router default passwords are changed to prevent unauthorized access.
8. Check that the router is configured to allow IPv6 multicast addresses.
9. Unplug the PC from the wireless router. Leave the EG plugged in.

2.2.4 Connect wirelessly

By bundling the EG, wireless router and associated power supplies together, they can be easily carried and plugged into an RS-485 spur to wirelessly commission each floor.

Connect SB to the network over Wi-Fi:

1. Click the Wi-Fi icon on your PC and select your wireless network.
2. Click the Connect button.



3. Launch SB and click the Connection Settings icon.
4. Click the Configure button
5. Select the TCP Connection Type. The connection details for your EG appear in the list.
6. Click the OK button to connect to the network via Wi-Fi.
7. Check that the SB Network log shows DyNet messages received from the network.

The EG shown is not part of the job. It is only used to connect SB. This EG is in addition to the bridge that connects the RS-485 spur to the IP trunk.

If connecting SB to the IP trunk or to an IP spur (in a PoE system) then the additional EG is not required.

2.3 Ethernet Access Point

When EG is configured as a permanent Ethernet access point, it allows any modern browser to communicate with the control system over the Wi-Fi/LAN/Internet. A browser is only able to communicate with one EG at a time, so control is limited to the logical areas set in each EG. However, if a common logical address range is set in each EG then these areas can all be controlled even if they span different EG's.

To setup the EG as Ethernet access point, you must first, run the Bridge Configuration Wizard to enable the DyNet Ethernet Access Point routing. Refer to Topic 2.2.2 Adding an IP Address.

Basic authentication is provided for Web-server, Telnet and FTP connections by adding usernames and passwords in System Builder.

Add EG users:

1. In SB, select the EG.
2. Click the Device Properties tab
3. Enable FTP, Telnet and/or Web Server applications and related properties.
4. Click the Users tab.
5. Click Add (maximum of five users).
6. Under User properties, enter the Name, Password and set the Enable property to True (usernames and passwords have a 40-character limit and are case sensitive).
7. Under Permissions Properties, set FTP, Telnet and/or Web server [authentication] to enabled.

If user-names and passwords are forgotten and you do not have the job file, they can be retrieved from the EG by loading from device. They can be backed up or replaced, but cannot be viewed in SB.

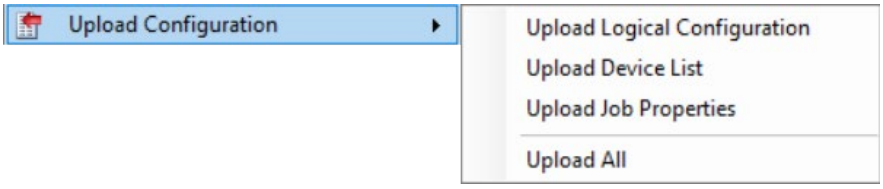
2.3.1 Wi-Fi access

For a completely customized interface, mobile apps accessing the connected lighting control system can be manually configured, or the interface can be auto-configured by reading the configuration data (project.xml file) stored in the EG. This saves configuration time and ensures control accuracy on mobile devices.

Once you have completed the logical configuration by entering your area, channel and preset names, you can upload your Project.xml file to the device.

Click Save To Device after making any configuration changes.

SB has an option to upload a project.xml file by right-clicking the EG and selecting Upload Configuration ▸ Upload Logical Configuration. As well as uploading the logical configuration. You can also upload other files by selecting:

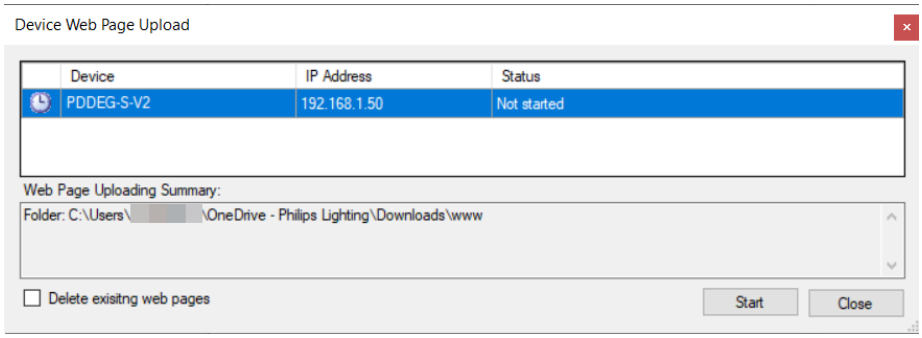


To control the system, connect the self-configuring mobile app to the network via Wi-Fi and enter the IP address of the EG. The controls in the app auto-configure based on the project.xml file in the EG. The EG supports up to 30 concurrent sessions for mobile apps

- The EG must have an IP address to upload the file. Refer to Wireless Commissioning about adding an IP address. Also, ensure that the EG is on the same subnet as your mobile device. Wireless routers/access points usually give out IP addresses within a certain range. For example: 192.168.10.1 to 192.168.10.100.
- To establish a secure connection when using an app, you may need install the certificate for the relevant operating system on your mobile devices. Refer to Appendix C: Signify Certificate Installation.

2.3.2 Uploading files

To upload a custom web interface, right-click and select Upload Custom Web Pages.
You may decide to delete the existing web pages via the checkbox in the Web Page Upload dialogue box.
Reset the device to apply the new configuration.



To upload other xml project files into the gateway, right-click and select Upload Configuration >

- Upload Logical Configuration (
- Upload Device List
- Upload Job Properties
- Upload All

Files on the PDEG must use 8.3 format file naming.

Files can be transferred from a project folder on PDDEG-S or on PDEG with firmware 3.53 or later, (PDEG doesn't support compressed files)

FTP cannot be used to update files on PDDEG-S, PDTS and PDEG (firmware 3.58 or later)

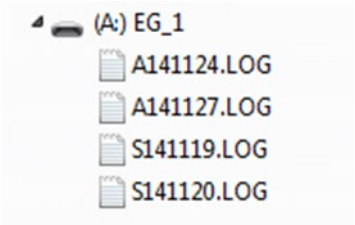
You can also save your Project.xml file by selecting File > Export > Logical Data.

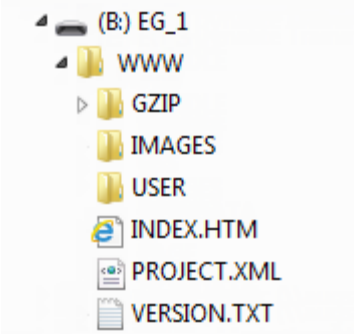
When transferring a custom web interface, custom settings, or updating the project.xml, be aware that the index.htm file (or another Starting Web page) must exist before proceeding. Do not use a compressed file format.

To upload files, SB must be connected to the device over Ethernet. Other settings can be modified when SB is connected to either Ethernet or RS-485.

There are two main directories on the device:

Directory A	Directory B
Rolling 28-day log files. Refer to topic: Log files.	/WWW
	/GZIP contains all pre-compressed user interface files for EG. N.B. any uncompressed files referenced from this folder will return browser errors.
	/IMAGES contains all images (JPG/GIF/PNG) used within the user interface files.
	/USER a folder containing user defined custom web pages, if any.
	/INDEX.HTM existing default homepage for the EG web interface.
	/PROJECT.XML project specific configuration file created on the EG. This file is not present within the installation files.
	/VERSION.TXT EG user interface build version.





2.3.3 CGI access

This section describes the Common Gateway Interface (CGI) available from the default or custom web pages. The web pages enable the user to send commands from the device to the network and request information from the network.

The default Philips web interface is preloaded directly under the B:www folder.

The CGI has been modelled on the Dynalite Text protocol and the Dynalite Tasking syntax. In these protocols many of the command parameters are optional, so if a parameter is not specified then the default value (or the value that was previously specified) for this parameter is used for subsequent CGI requests. Alternatively, you may explicitly specify a value for all parameters each time a command is executed.

Issues to consider:

- If your default page is no longer index.htm, then you must change the option in devices properties.
- The filename WebPage.cgi is reserved for retrieving webpage data.
- The filename SetDyNet.cgi is reserved for issuing DyNet commands.
- The filename GetDyNet.cgi is reserved for retrieving DyNet status.
- All files names are case sensitive on this device, following Unix and web standards.
- The **?** char is used to initialize a CGI string and the **&** char is used for delimiting.
  For example. 192.168.2.2/GetDyNet.cgi?a=3&p=2&l

DyNet commands and status requests

Following table lists the HTTP/CGI requests available from the device.

Function	CGI request	**Required** & Optional Parameters	Value Required	Value Range	Description
Recall preset (Set) Request current preset (Get)	**P** or **PRESET** Preset number Command	**A** C, J, F	Yes	0 to 65535	Also supports special presets: 0=Reset Preset 65520=Off 65532=Restored Saved 65533=Toggle 65534=Panic 65535=Don't care preset
Recall channel level (Set) Request current channel level (Get)	**L** or **LEVEL** Channel level Command/Parameter	**A** C, J, F	Yes	0 to 100	Channel level in percentage 255 is special don't know/don't care value.
Program/save preset (Set)	**PP** or **S** Preset number Command	**L, A** C, J	Yes	0 to 255	Saves the current channel levels to the specified preset
Start task (Set)	**STT** Task number Command	**-** DC, BN	Yes	0 to 255	If DC and BN are not provided, the device's DC and BN will be used.
Stop task (Set)	**SPT** Task number Command	**-** DC, BN	Yes	0 to 255	If DC and BN are not provided, the device's DC and BN will be used.
Pause task (Set)	**PT** Task number Command	**-** DC, BN	Yes	0 to 255	If DC and BN are not provided, the device's DC and BN will be used.
Enable event (Set)	**EEVT** Event number Command	**-** -	Yes	0 to 255	0: All Events Other values: particular event number
Disable event (Set)	**DEVT** Event number Command	**-** -	Yes	0 to 255	0: All Events Other values: particular event number

Function	CGI request	**Required** & Optional Parameters	Value Required	Value Range	Description
Trigger event (Set)	**TEVT** Event number Command	- -	Yes	1 to 255	0: All Events Other values: particular event number
Read task port value (Get)	**RPV** Task port number Command	- SBP	Yes	0 to 255	SBP is optional for task sub-port number
Write on task port (Set)	**WPV** Task port number Command	- SBP	Yes	0 to 255	SBP is optional for task sub-port number
Write on sub-task port (Set)	**SBP** Task sub-port number Parameter	**RPV or WPV**	Yes	0 to 255	
Value to write to Port (Set)	**V** Value to write Parameter	**WPV** SBP	Yes	0 to 255	Specifies the value to write to task port.
Nudge up (Set)	**NU** Increment factor Command	**A** C, J	Yes	0 to 100	Channel level in percentage
Nudge down (Set)	**ND** Decrement factor Command	**A** C, J	Yes	0 to 100	Channel level in percentage
Ramp level (Set)	**RL** or **RAMPLEVEL** Ramp level value Command	**A** C, J	Yes	0 to 100	Level in percentage
Stop fade (Set)	**SF** or **STOPFADE** Stop fading Command	**A** C, J	No		
Get temperature (Get)	**TPTR** or **TEMPERATURE** Temperature in +/- xx.yy format Command	**A** J	No	-64 to 64	Returned temperature shall be in +/- xx.yy format
Set temperature set-point (Set) Get temperature set-point (Get)	**TPSP** or **TEMPERATURESETPOINT** Temperature in +/- xx.yy format Command	**A** J	Yes, for Set No, for Get	-64 to 64	Returned temperature shall be in +/- xx.yy format
Get DALI ballast runtime status (Get)	**QBS** DALI ballast runtime status Command	**DC, BN, C** CN	No		Reply if CN not specified: **QBS**=x Reply if CN specified (for example CN=5): **QBS**=x;x;x;x;x x=0 : Lamp failure, ballast offline x=1 : Lamp Ok, ballast offline x=2 : Lamp failure, ballast online x=3 : Lamp Ok, ballast online C: 1 to 64 for DDBC120-DALI CN: 1 to 64 for DDBC120-DALI
Set the preset offset (Set)	**O** or **OFFSET** Preset offset Command	**A** J	Yes	0 to 127 or 0 to 65535	Set the preset offset for an area. The maximum value that can be set for a DyNet 1 message is 127. The maximum value that can be set for a DyNet 2 message is 65535.
Set reply time out (Set) Get reply time out (Get)	**REPLYTIMEOUT** Reply time out in milliseconds Command	- -	Yes, for Set No, for Get	200 to 20000	This is the amount of time that device will wait for a any request message (when GetDyNet.cgi is used) to get back with a reply. If there is no reply after this time, device will reply with an error back to the client.

Function	CGI request	**Required** & Optional Parameters	Value Required	Value Range	Description
Set task register X (Set) Get task register X (Get)	**X** X register value Command	- -	No	0 to 255	
Set task accumulator (Set) Get task accumulator (Get)	**ACC** ACC register value Command	- -	No	0 to 255	
Area (Set or Get)	**A** or **AREA** Area number Parameter	- -	Yes	Area: 0 to 65535 Channel: 1 to 255	If area is not specified, then request will be processed for last area received and saved by the Xport. Else channel level for requested area will be returned, without storing the requested area.
Join (Set or Get)	**J** or **JOIN** Join value Parameter	- -	Yes	0 to 255	
Channel number (Set or Get)	**C** or **CHANNEL** Channel number Parameter	- -	Yes	0 to 65535	
Number of physical channels (Get)	**CN** Number of physical channels Parameter	- -	Yes	0 to 65535	
Box number (Set or Get)	**BN** Box number value in physical address Parameter	- -	Yes	0 to 255	
Device Code (Set or Get)	**DC** Device Code value in physical address Parameter	- -	Yes	0 to 255	
Fade time (Set)	**F or FADE** Fade time in milliseconds Parameter	- -	Yes	0 to 5,242,710 ms	

DyNet commands and status request examples

To control DyNet Areas, DyNet logical commands use the http Set method with the SetDyNet.cgi file. DyNet logical status requests use the http Get method with the GetDyNet.cgi File.

Example 1: Recalling preset 2 in area 3.

http://192.168.10.10/SetDyNet.cgi?a=3&p=2

This sets area 3 to preset 2. Multiple parameters may be used in the one request; however, only one of them should be of the command type. The response from this HTTP request automatically redirects the browser back to the calling page as detailed below.

<html><body onload=history.back()></body></html>

Example 2: Request the current preset in area 3

http://192.168.10.10/GetDyNet.cgi?a=3&p or http://192.168.10.10/GetDyNet.cgi?a=3

The response from this HTTP request contains the state retrieved from the DyNet area.

A single numeric value is returned indicating the current preset or channel level. If the logical entity does not exist a single full stop character "." is returned. If the response shown below is returned from the request, then area 3 is in preset 4.

p=4

Example 3: Set the preset offset in area 2 to 6

http://192.168.10.10/SetDyNet.cgi?a=2&o=6

If the current preset is 4, the reply will be:

p=4 o=6

Example 4: Check the current setting for Reply Time Out and set it to a new value

Reading the current setting:

http://192.168.10.10/GetDyNet.cgi?replytimeout

returns:

replytimeout=200

Now setting it to a new value:

(this is typically for wireless devices that can have a very slow response times)

http://192.168.10.10/SetDyNet.cgi?replytimeout=2000

Example 5: Program Area 2, Channel 3 and Level 25% to Preset 10

http://192.168.10.10/SetDyNet.cgi?a=2&c=3,j=255&l=25&pp=10

Example 6: Fade Area 2, Channel 3 to 25% channel level with 5 seconds fade time

http://192.168.10.10/SetDyNet.cgi?a=2&c=3,j=255&l=25&f=5000

Example 7: Request the saved channel level in Area 2, Channel 3 for Preset 4

http://192.168.10.10/GetDyNet.cgi?a=2&c=3&j=255&p=4

Example 8: Request the current channel level in Area 3, channel 2 (returns 23%)

http://192.168.10.10/GetDyNet.cgi?a=3&c=2&j=255&l

or

http://192.168.10.10/GetDyNet.cgi?a=3&c=2&j=255

returns:

l=23

2.3.4 HTTPS Secure Access

HTTPS provides a secure connection between your browser and an Ethernet gateway.

HTTPS adds two things to HTTP: secrecy and trust. Secrecy is established with an SSL/TLS connection that encrypts the browser's data communications.

The most common solution for establishing trust, is based on certificates signed by third-party certificate authorities. Typically, a chain-of-trust is established for a server by preinstalling a signed web-server certificate, supplied by a certificate authority (CA) trusted by the client.

Configuring HTTPS

System Builder has the capability to manage certificates, sign certificates, send certificate signing requests and configure users with different access permissions.

There are three web server certificate options for establishing HTTPS access to the gateway:

- **System Builder certificate (recommended).**
  For most applications it is preferable to create and upload a System Builder signed certificate on the gateway and install the matching root certificate for each client's browser or app that will access the server.
- **Self-signed certificate**
  Request the gateway to generate a self-signed certificate. This allows a secure connection using HTTPS however, the browser will show a non-trusted warning.
- **Certificate Authority signed certificate**
  If you have a domain, you may select a Certificate Authority signed certificate. System Builder will instruct the EG to create a Certificate Signing Request (CSR) from the private key built in to the EG. The CSR can then be sent to a third-party CA. It is the responsibility of the CA to determine if you are trustworthy. They can respond to the certificate signing request by signing your server certificate and sending you the result. You then upload the signed certificate onto your EG. The signed certificate usually does not need to be installed for each client as third-party CA's are already known to most browsers, however there may be ongoing costs with this option.

You must have a user configured with Web server, CGI, Certificate read and write enabled. For more information on user permissions, refer to Property Editors – Users.

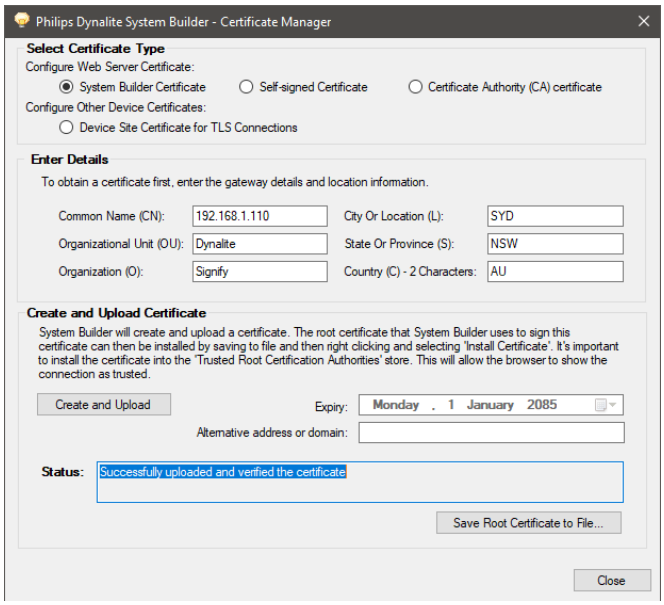
EG firmware version v3.44 and above supports secure connections via HTTPS. Web pages can be accessed via HTTPS however mobile apps currently only support HTTP.

The Device Site Certificate for TLS connections option is used to establish a TLS TCP connection between the PDDEG-S and GRMS-E devices or between PDDEG-S and DDBC320-DALI.

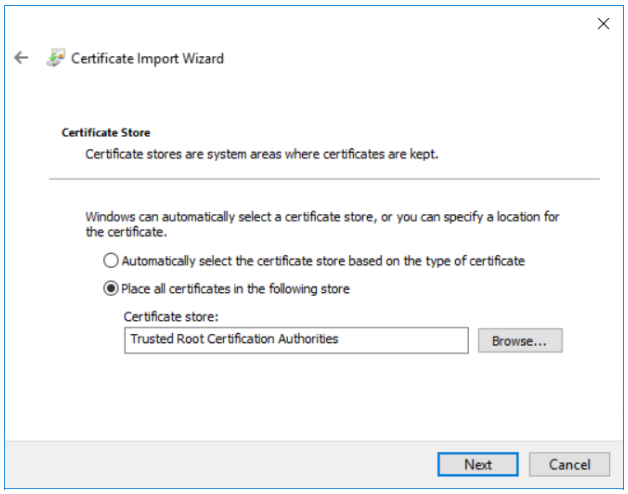
The 802.1X certificates option is used when clients only want devices they know about on the network. If the device does not present the correct credentials (certificate) then that ethernet port is disconnected and the device is not allowed to send traffic.

Create System Builder certificate:

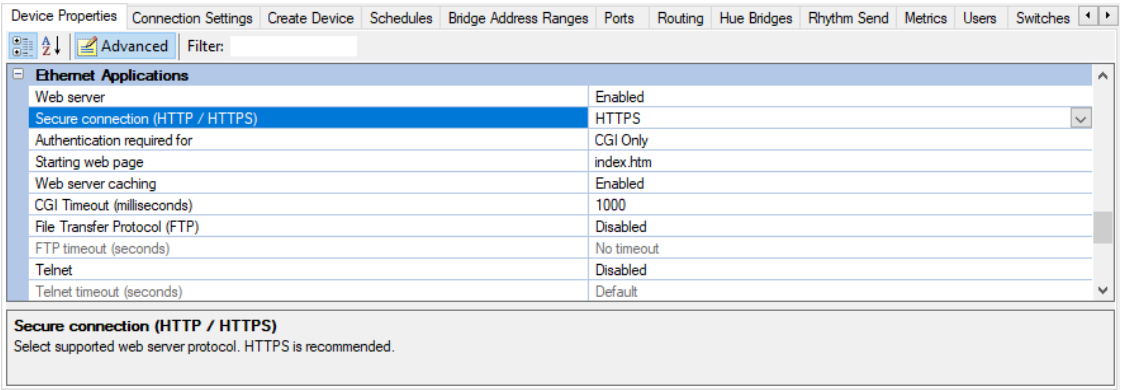
1. Connect SB to the EG over Ethernet.
2. Right-click the EG and select Manage Certificate.
3. Enter the gateway details and location information.
4. Select the Certificate type – System Builder certificate.
5. Click the Create and Upload button. After a minute or two, System Builder creates a signed certificate file on the gateway. Restart the gateway to apply the certificate.



6. Click the Save Root Certificate to File button to save the (.cer) file to your PC.
7. Right-click the security certificate (.cer) file on your PC and select Install Certificate. The Certificate Import Wizard opens.
8. In the wizard, click the Next button, select Place all certificates in the following store and select the Trusted Root Certification Authorities folder.

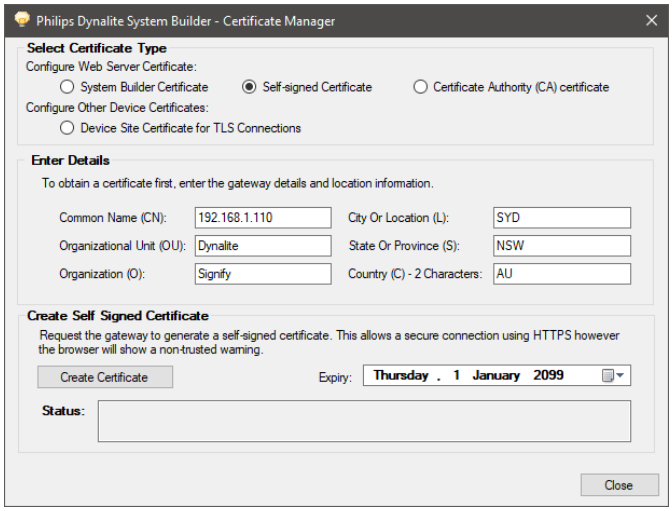


9. Click the Next button and Finish button to complete the import wizard. The wizard displays a security warning.
10. Click the Yes button to install the certificate. The wizard shows a message that the import was successful.
11. In Device Properties > Ethernet Applications > Secure connection (HTTP/HTTPS) select HTTPS from the dropdown list.
12. Click Save to device or press [F12] on the keyboard.



Create Self-signed certificate:

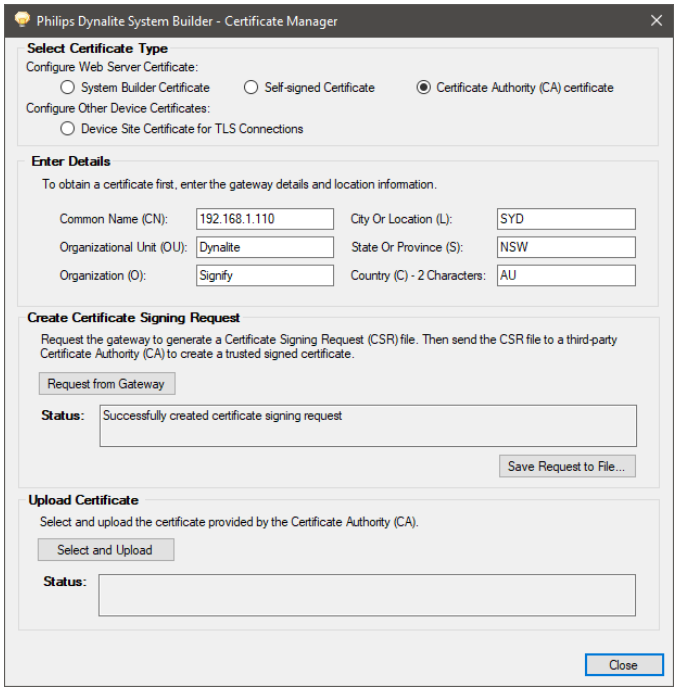
1. Connect SB to the EG over Ethernet.
2. Right-click the EG and select Manage Certificate.
3. Enter the gateway details and location information.
4. Select the Certificate type – Self-signed certificate.
5. For a self-signed certificate, click Create Certificate. After a minute or two, System Builder creates a self-signed certificate file on the gateway. Restart the gateway to apply the certificate.



6. In Device Properties > Ethernet Applications > Secure connection (HTTP/HTTPS) select HTTPS from the dropdown list.
7. Click Save to device or press [F12] on the keyboard.

Create Certificate Authority (CA) certificate:

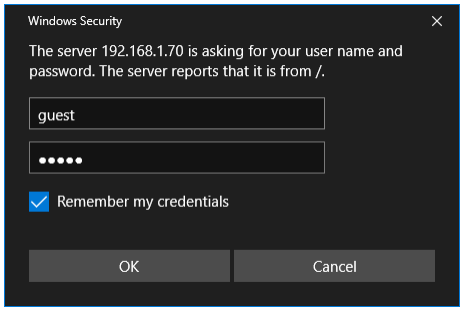
1. Connect SB to the EG over Ethernet.
2. Right-click the EG and select Manage Certificate.
3. Enter the gateway details and location information.
4. Select the Certificate type – Certificate Authority (CA) certificate.
5. Click the Request from Gateway button. After a minute or two, System Builder creates a certificate signing request file on the gateway.
6. Click the Save Request to File button to save the (.csr) file to your PC and send the CSR file to a CA for signing.



7. After the CA returns the signed certificate, click the Select and Upload button, select the certificate file (.pem) and click open. System Builder uploads the file to the gateway. Restart the gateway to apply the certificate.
8. In Device Properties > Ethernet Applications > Secure connection (HTTP/HTTPS) select HTTPS from the dropdown list.
9. Click Save to device or press [F12] on the keyboard.

Establishing a HTTPS connection

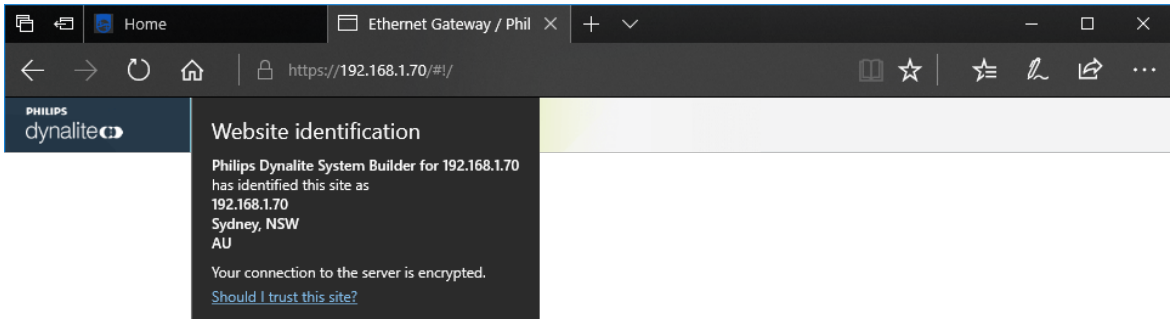
To confirm your signed certificate, open the Ethernet Gateway home page in your browser by entering https:// and the EGs IP address. When a browser connects to the gateway's webserver, it will prompt you to enter your username and password (as setup in System Builder - Users property editor)'



The browser will verify that your server certificate has been signed by a trusted CA.

The browser then establishes a secure connection with the EG webserver.

To see whether a website is safe to visit, you can check the site's security information by looking at the security status to the left of the web address bar. The browser will alert you if you cannot visit the site safely or privately by showing a red address bar with warnings when a server certificate is not trusted. For HTTPS connections, the web address will show a closed padlock icon.



2.4 Ethernet Bridge

2.4.1 Address Offsets

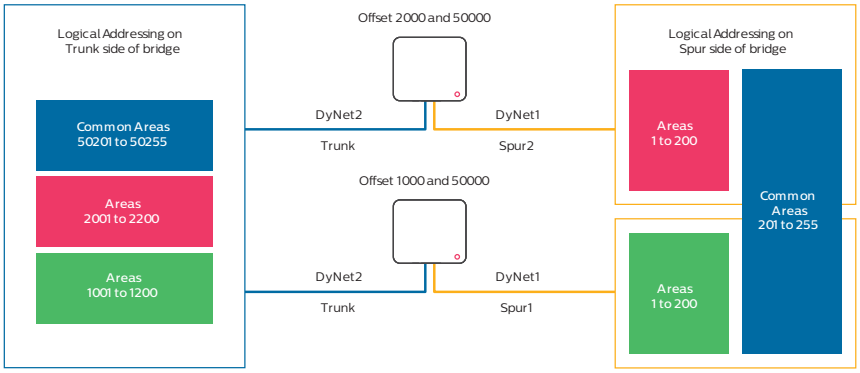
Each floor gateway is configured with a unique IP address and DyNet address offset for each spur (physical and logical address range, for example, 1000, 2000, 3000 etc.).

Logical address offsets in each EG enables reuse of area numbers (and use of common area numbers when required). The routing ensures that only system wide and inter-spur communications are sent over the trunk. Intra-spur communications remain within the spur.

A common logical range may also be added to other gateways (for example, areas 201 – 255) for logical messages to other floors. The Bridge Configuration Wizard will identify other gateways with common areas.

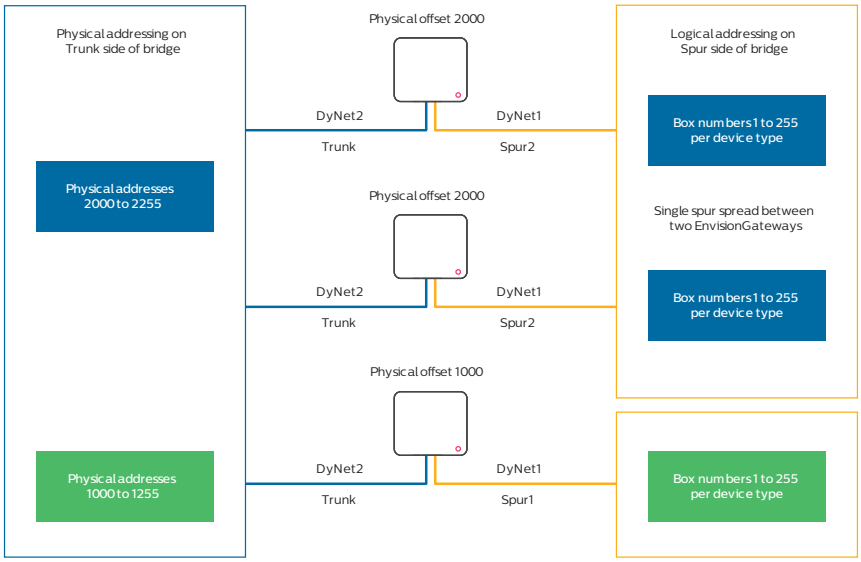
Common areas create a lot of additional routing between the gateways. Only use common areas if you have a genuine need to control areas on different floors from a user interface/sensor on another floor.

The diagram below shows different logical address range offsets on two spurs and a common logical address range shared by both spurs.



Logical Addressing

Physical address offsets in each EG enable it to maintain electrical isolation from the trunk while keeping intra-spur communication within the spur and allowing the reuse of device box numbers. The diagram below shows different physical address range offsets on two spurs and a common physical address range when using two EGs as a single spur.



Physical Addressing

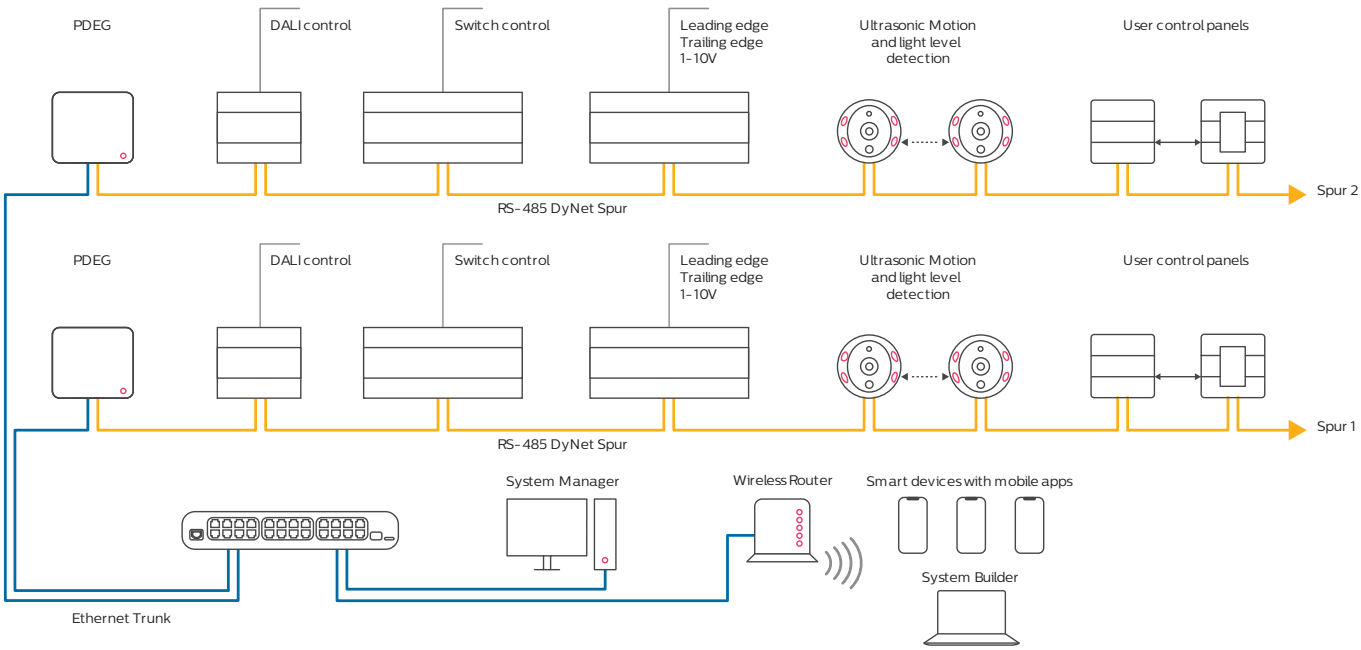
2.4.2 Ethernet to RS-485

The EG acts as a bridge between Ethernet and RS-485 to establish a trunk and spur topology for efficient data transport. EGs are usually added to the SB job first, to establish the Ethernet trunk, and then other devices are added under each EG to create the RS-485 spur subnetworks.

The EGs provides a way to isolate parts of the network by routing messages only for SM, common areas and devices on other spurs, over the trunk. In addition, EGs provide status polling, metric collection, area cascading, and scheduling features.

TCP connections can be secure or non-secure.

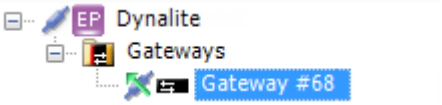
- Non-secure connections can use a PDEG or PDDEG-S.
- Secure connections must use a PDDEG-S.



To commission an EG as an Ethernet bridge, first plug the commissioning PC into a DyNet spur with an EG. Connect SB using a serial connection and add the EG to the job. Refer to Adding an EG over RS-485.

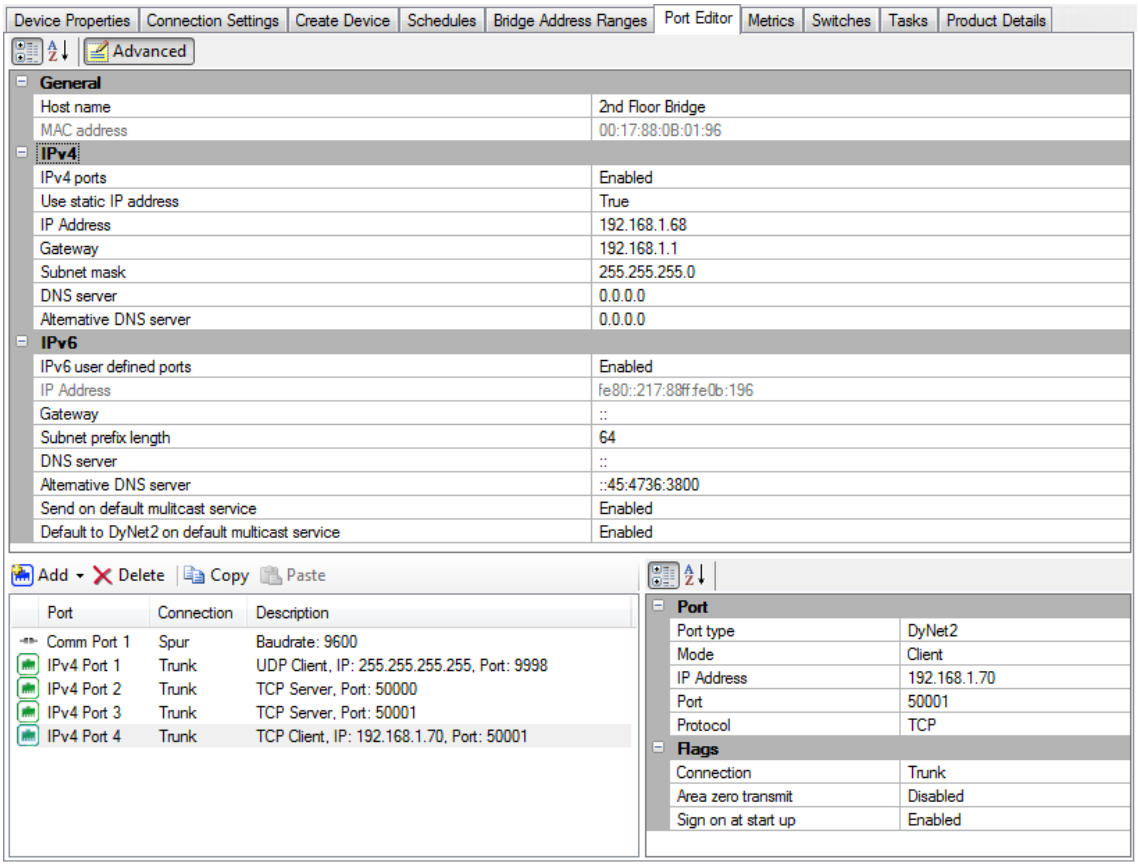
The EG can be precommissioned. However, ports and connection settings may require updating once installed in on-site.

Configure IPv4 addressing:



1. Select the EG from the Device tree.
2. In the Device Properties page under Device Identification, enter the Device name (this identifies the EG in SB).
3. In the Port Editor page enter a Host name (this identifies the EG on the LAN).
4. Under IPv4 properties, set Static IP to True.
5. Enter an IP address for the EG.
6. In the Gateway property, enter the IP address of the router.
7. In the Subnet mask property, enter the subnet mask of the router if different to the default value.
8. Repeat this procedure for every bridging EG in your system.

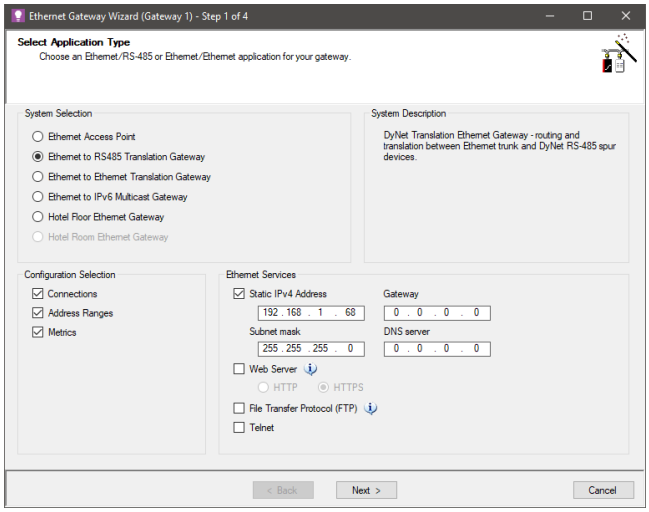
To create the required ports and routing rules for your EG, please run the Bridge Configuration Wizard.



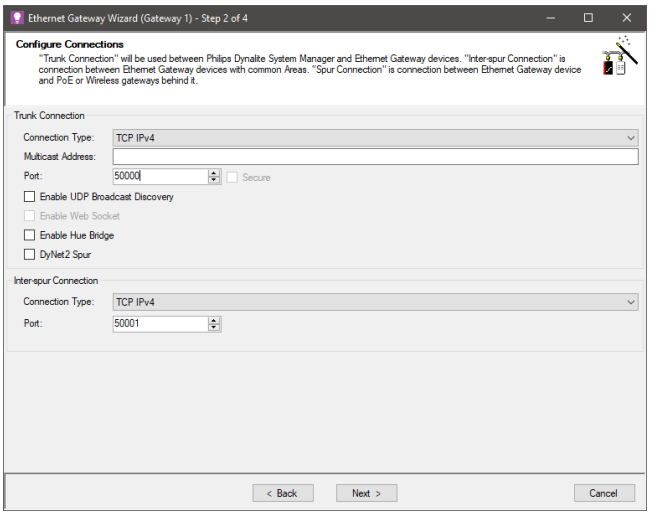
Configure Ethernet to RS-485 Translation Gateway:

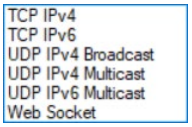
1. Connect SB to the network via a serial RS-485 connection.
2. Right-click the EG in the device tree and select Bridge Configuration Wizard... or press Alt+W.
3. Select **Ethernet to RS-485 Translation Gateway** and click the **Next** button.

For precommissioning, untick the Connections checkbox. Trunk and Inter-spur IP addresses can be added when connected on site.



4. Under Trunk Connection, set the Connection Type to TCPv4, port 50000.
5. Under Inter-spur Connection, set the Connection Type as TCPv4, port 50001 and click the **Next** button.





Trunk and Inter-spur connection options.

The **Enable UDP Broadcast Discovery** checkbox enables the UDP IPv4 discovery port (Port 9998) used by SB to find the bridges in the system (listed in the Connection Settings page under Ethernet Trunk Connection Settings). It also enables DynamicTouch access.

The **Enable WebSocket** option is an alternative way to connect to SB/SM.

The **Enable Hue Bridge** option creates the routing required for Philips Hue integration.

The **DyNet 2 Spur** option routes DyNet 2 messages from the trunk onto a DyNet2 RS-485 spur.

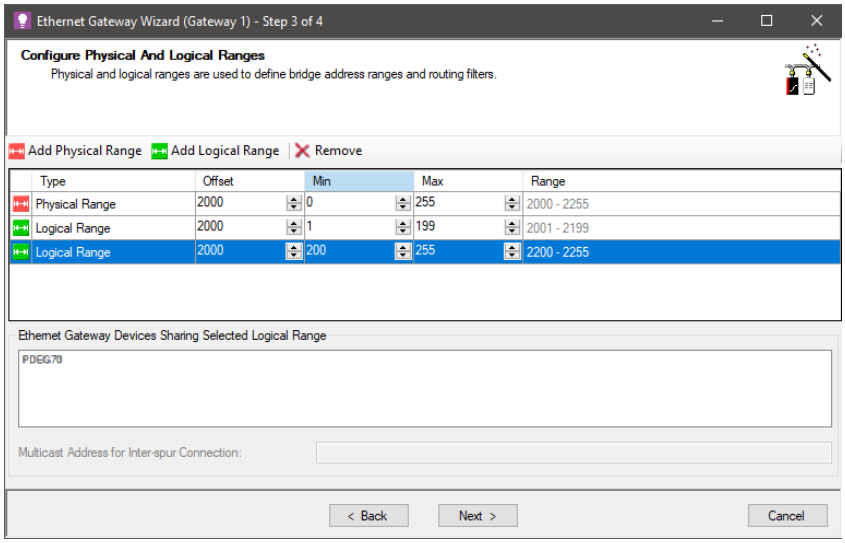
6. Click the Add Physical Range icon and enter Offset, Min and Max values.
7. Click the Add Logical Range icon and enter Offset, Min and Max values.
   Primary address Min value must be 1 or 0 (see Note).
8. Click the Add Logical Range icon again (optional) to enter address ranges that are common to multiple EGs. The range defined by the Min and Max values must not overlap with the other logical ranges.

   SB lists the EG devices that it finds in the job that share common address ranges. The address ranges must match exactly.

   Click the Next button.

Do not use common areas unless you have a genuine need to control areas on different floors from a user interface/sensor on another floor. When finishing the wizard, it will ask if you want to automatically create the additional routing between the gateways with common areas.

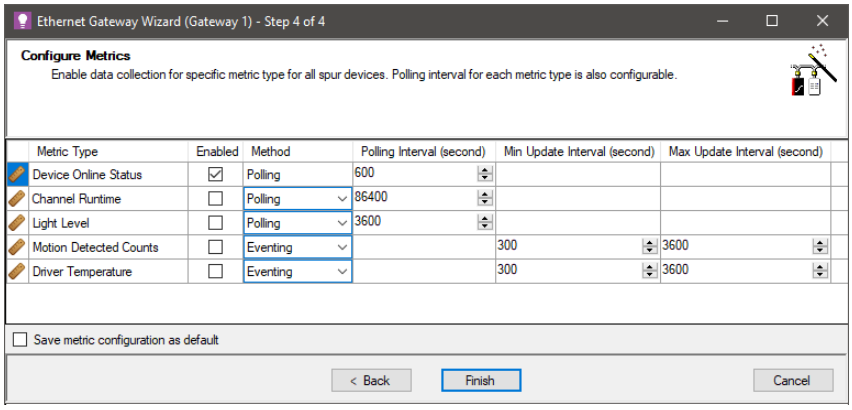
The primary logical range for the spur can also be changed to start from 0 if you want to allow for Area 0 (All Areas) messages to be sent from the trunk. You must enable the Area Zero Transmit property on the port record for the EG and spur devices may require further configuration to support this.



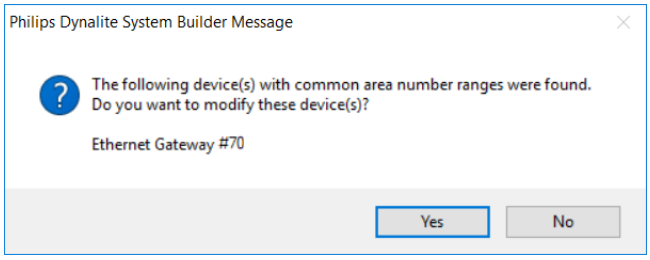
A common logical range enables the system to address areas that span multiple spurs. A common physical range enables devices to appear on a single spur when attached to different EGs.

9. You can select the checkbox and enter different polling periods, if applicable or click the next button to accept the default metrics for devices and channels on the spur.

Ensure only necessary metrics are selected to minimize network traffic.



10. Click the Finish button.
11. A popup message indicates the other EGs that must have their settings saved.
12. Click Yes.



13. Click Save to Device.
14. Repeat this procedure for every EG bridge in your system.
15. Click File Save to save the job to your PC.

For increased security, the Bridge Configuration Wizard will disable the IPv6 default multicast connection when saved to the gateway. This means SB must now connect to the gateway using the Ethernet Trunk Connection or serial connection.

2.4.3 Ethernet to Ethernet

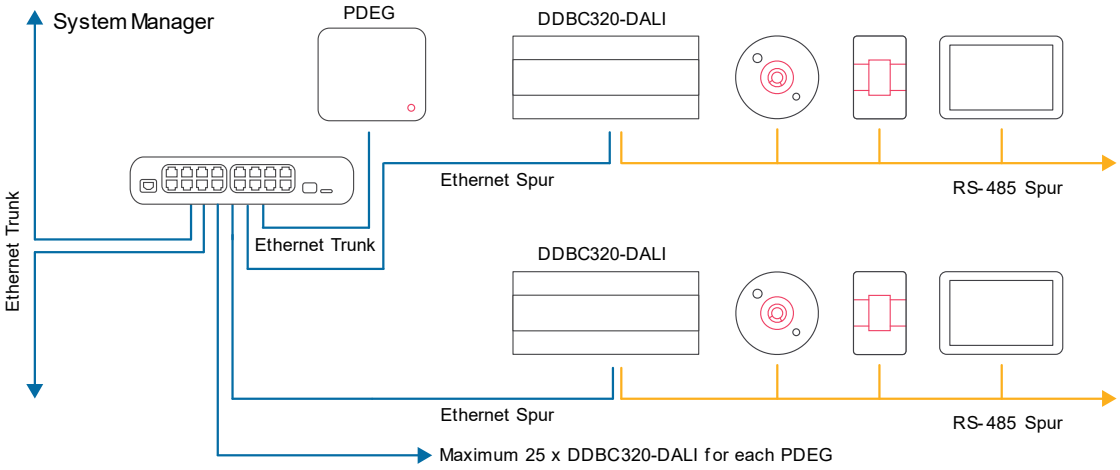
Configuring the PDEG or PDDEG-S as an 'Ethernet to Ethernet Translation Gateway' and connecting multiple DDBC320-DALI controllers together via their Ethernet ports provides a cost-effective scalable lighting control solution.

TCP connections can be secure or non-secure.

- Non-secure connections can use a PDEG or PDDEG-S.
- Secure connections must use a PDDEG-S.

When configured, SB and SM connect to the PDEG or PDDEG-S gateways via TCP connections. The PDEG or PDDEG-S gateways then connect to each DDBC320-DALI via separate TCP connections.

A maximum of 25 DDBC320-DALI controllers can be connected to each PDEG or PDDEG-S and up to three DDBC320-DALI can be configured with the same offset, to behave as a single spur.

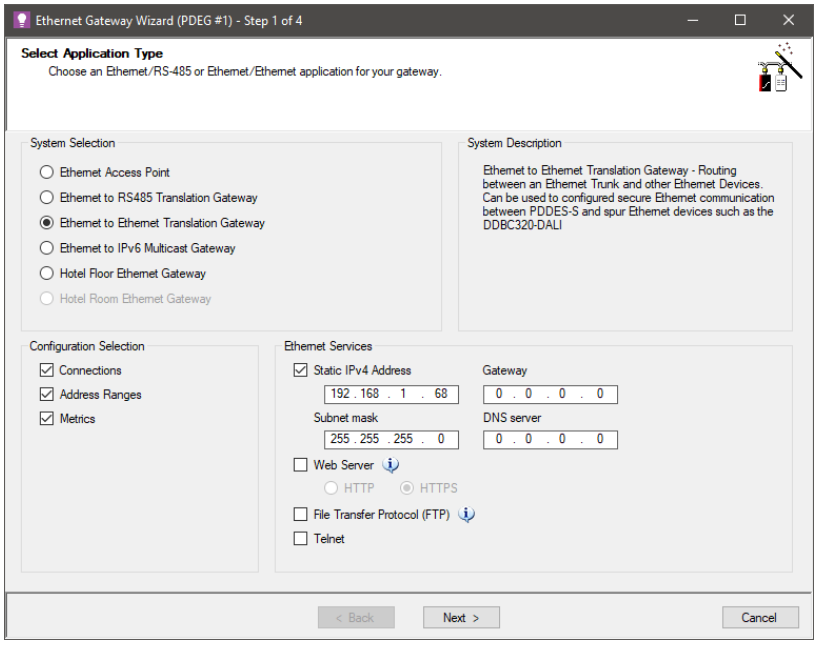


It is recommended that DyNet spur address range offsets are configured on the DDBC320-DALI rather than on the PDEG/PDDEG-S.

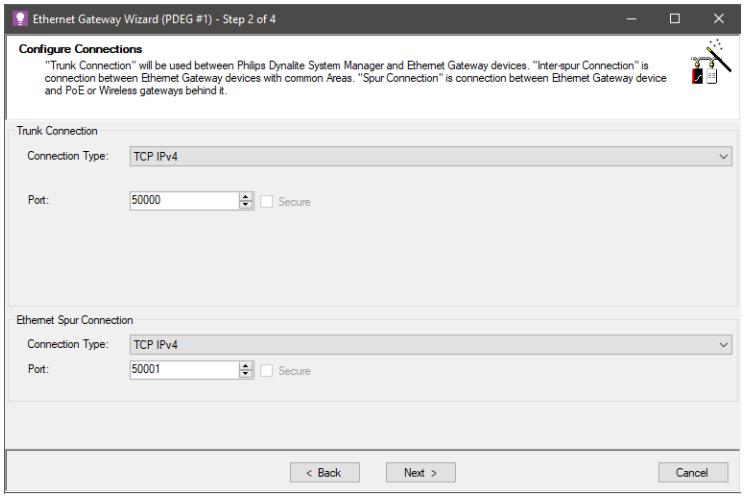
For more information on configuring DDBC320-DALI Ethernet connections, refer to the Signal Dimmers Commissioning Guide.

Configure Ethernet to Ethernet Translation Gateway:

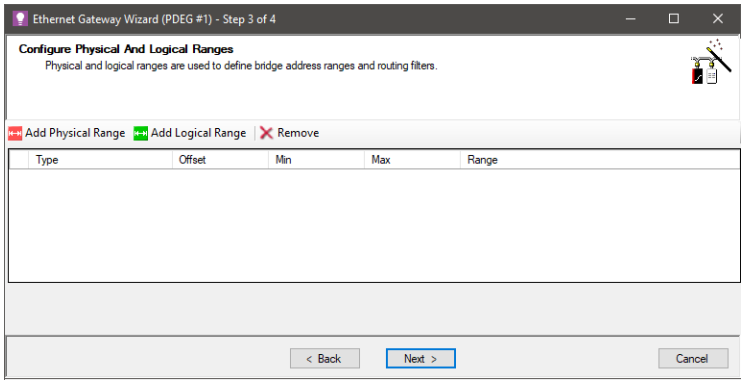
1. Right-click the EG in System View and select Bridge Configuration Wizard... (Alt+W).
1. Add a PDEG or PDDEG-S to the job.
2. Run the Bridge Configuration Wizard (Alt+W).
3. Under System Selection, select **Ethernet to Ethernet Translation Gateway**.
4. Select **Static IPv4 Address** and enter IP Address (and Gateway and Subnet mask if required).
5. Under Configuration Selection, ensure **Connections** is selected and click **Next**.



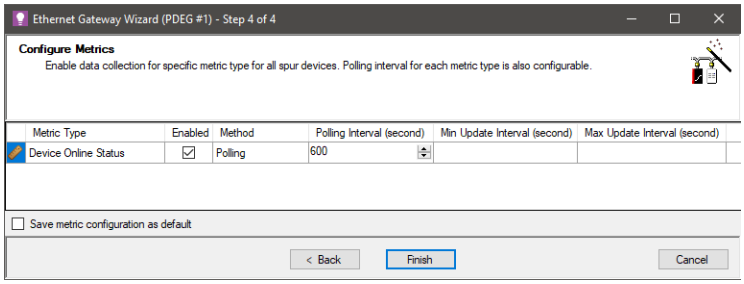
6. Under Trunk Connection, select TCP IPv4, port 50000.
7. Under Ethernet Spur Connection, select TCP IPv4, port 50001 and click **Next**.



8. Do not add any Physical and Logical Range and click **Next**.



9. Ensure Device Online Status metric checked and click **Finish**.



The wizard adds three new routing records:

- IPv4 TCP Port 51443 → IPv4 TCP Port 50443
- IPv4 TCP Port 50443 → IPv4 TCP Port 51443
- IPv4 TCP Port 50443 → IPv4 TCP Port 50443

This last routine record is required only when different DDBC320-DALI have common areas. When the network is busy, there may be performance issues as this routing record will result in all messages from every DDBC320-DALI being routed to all other DDBC320-DALI controllers. In this case it may be necessary to have separate secure ports (with different port numbers) for groups of DDBC320-DALI that have common areas.

2.4.4 Secure Ethernet to RS-485

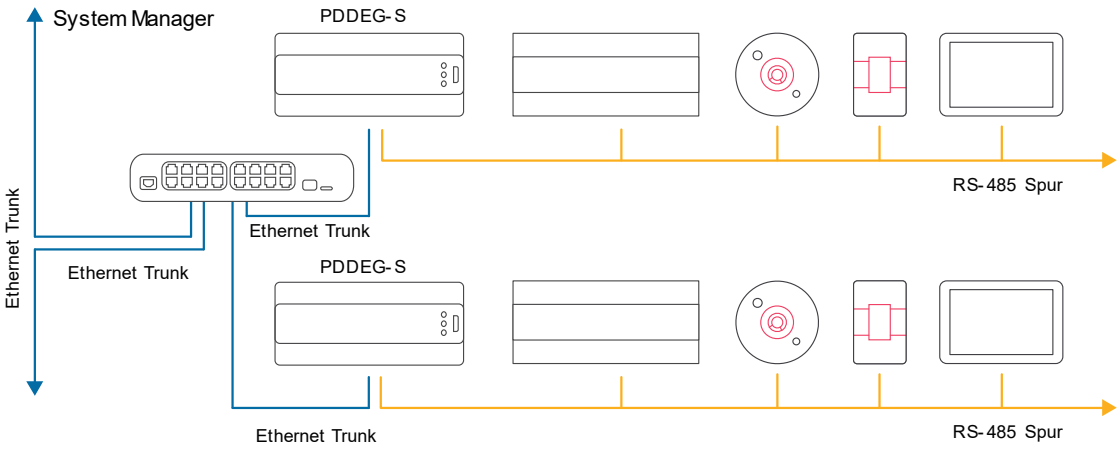
Firstly, you must create/import a Site CA Certificate in System Builder. Refer to topic 2.1.3 Creating a Site CA Certificate.

Creating secure Ethernet connections requires a PDDEG-S. To ensure end-to end security, each PDDEG-S and Ethernet device must be configured for secure connections in the job before importing the job into SM.

To enable SM to connect securely to the PDDEG-S gateways in the system, Open SB on the SM Server machine and import the Site CA certificate to that machine and save the job/database.

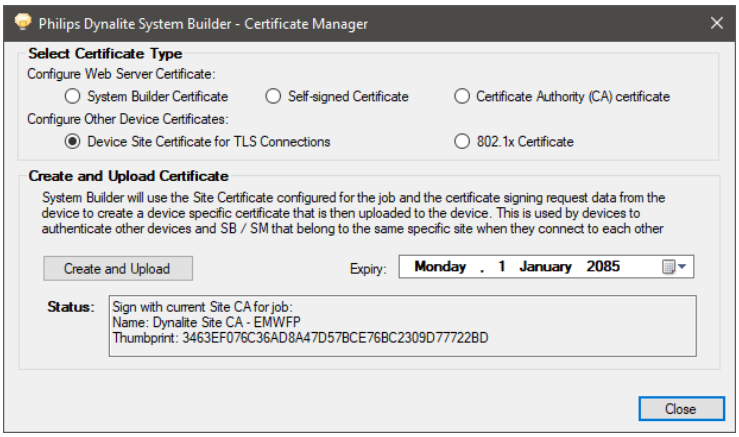
SB enables you to:

- Connect to the system via a secure trunk connection.
- Manage site certificates.
- Upload Device Site Certificates to devices.



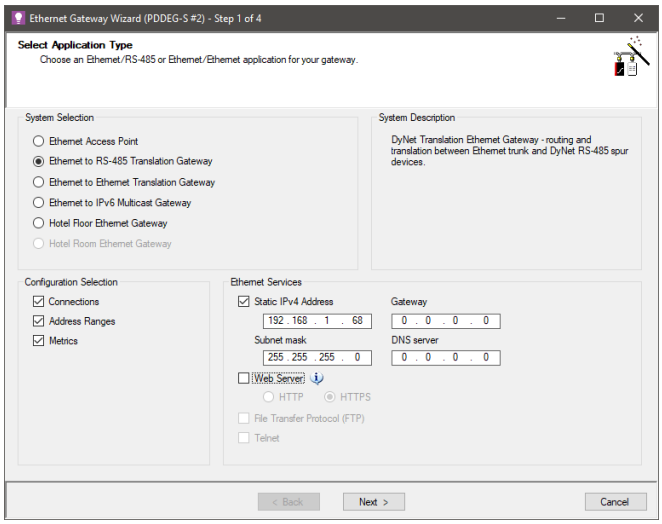
Create and upload certificate to the PDDEG-S:

1. Right-click the PDDEG-S in System View and select Manage Certificate.
2. Select Certificate type **Device Site Certificate for TLS Connections**.
3. Click the **Create and Upload** button. After a minute or two, System Builder creates and uploads a signed certificate file to the gateway.
4. Click the Close button.

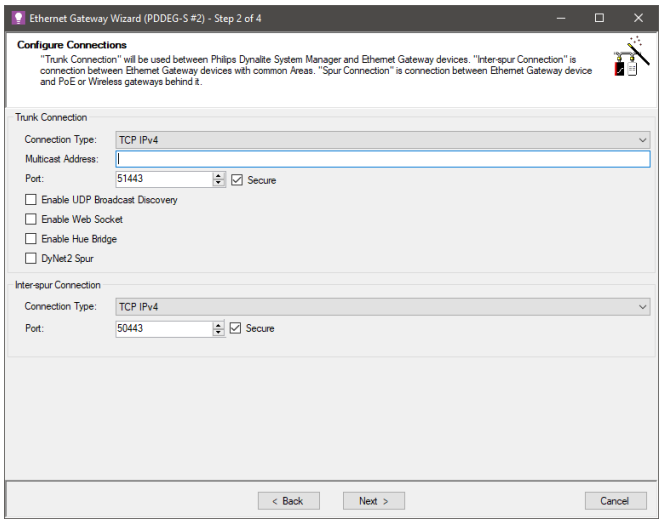


Configure secure Ethernet to RS-485 Translation Gateway:

1. Right-click the EG in System View and select Bridge Configuration Wizard... (Alt+W).
2. Select **Ethernet to RS-485 Translation Gateway**
3. Enter an IPv4 address (do not select Webserver)
4. Click the **Next** button.



5. Under Trunk Connection, select the TCP IPv4 and Secure checkbox.
6. Under Inter-spur Connection, select TCP IPv4, port 50443 and Secure checkbox and click the **Next** button.

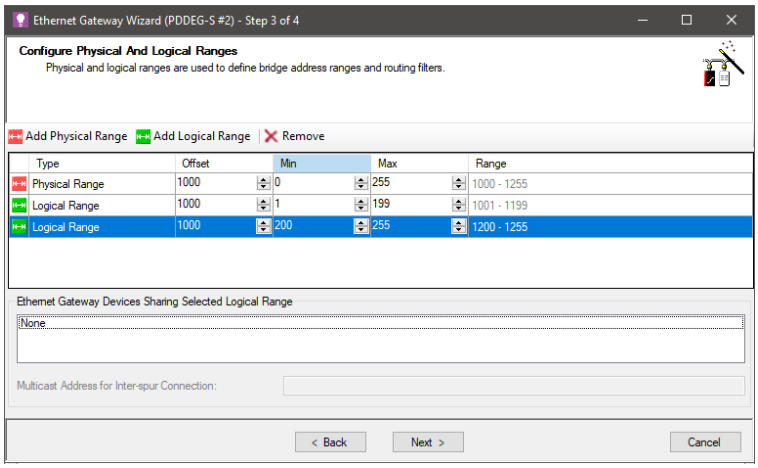


- The **Enable UDP Broadcast Discovery** checkbox enables the UDP IPv4 discovery port (Port 9998) used by SB to find the bridges in the system (listed in the Connection Settings page under Ethernet Trunk Connection Settings). It also enables DynamicTouch access.
- The **Enable WebSocket** option is an alternative way to connect to SB/SM.
- The **Enable Hue Bridge** option creates the routing required for Philips Hue integration.
- The **DyNet 2 Spur** option routes DyNet 2 messages from the trunk onto a DyNet2 RS-485 spur.

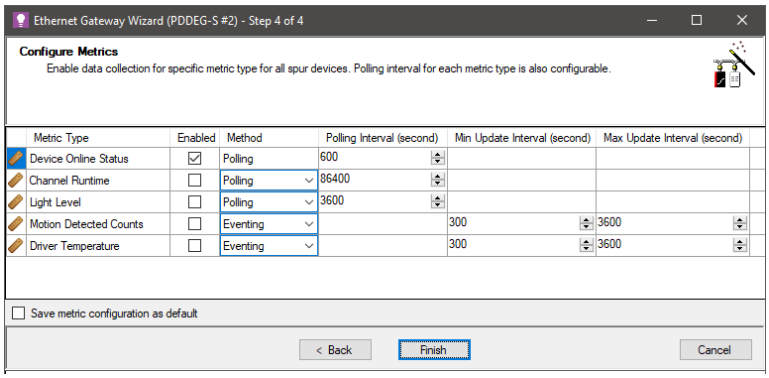
7. Click the Add Physical Range icon and enter Offset, Min and Max values.
8. Click the Add Logical Range icon and enter Offset, Min and Max values.
9. Click the Add Logical Range icon again (optional) to enter address ranges that are common to multiple EGs. The range defined by the Min and Max values must not overlap with the other logical ranges.

   SB lists the EG devices that it finds in the job that share common address ranges. The address ranges must match exactly. Click the **Next** button.

Do not use common areas unless you have a genuine need to control areas on different floors from a user interface/sensor on another floor. When finishing the wizard, it will ask if you want to automatically create the additional routing between the gateways with common areas.



10. Click the **Next** button to accept the default metrics on the spur.
    You can check/uncheck the checkbox or enter different polling periods, if applicable.
11. Click the **Finish** button and click the **Yes** button to the confirmation message.



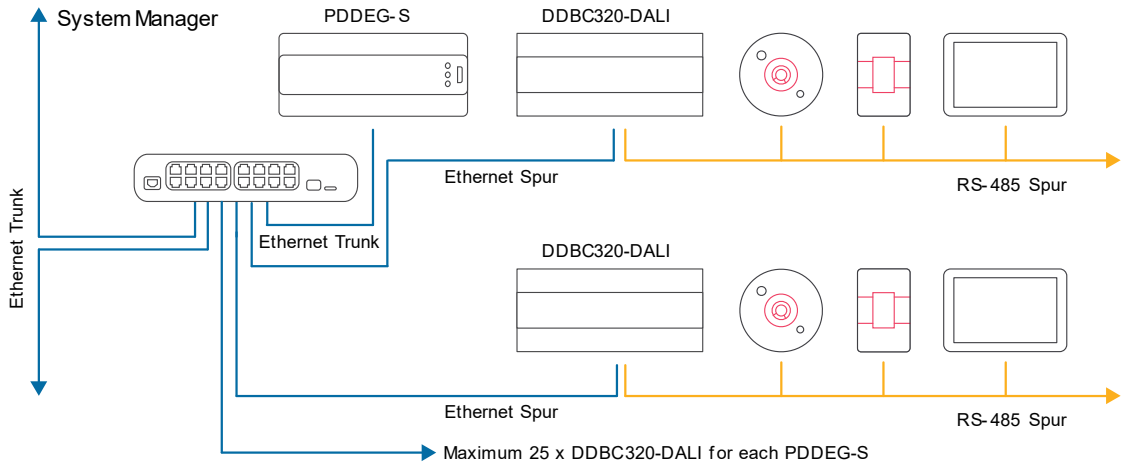
12. Record the box number and IP address of each gateway in your project notes. This is a useful reference.
13. Click Save to Device.
14. Click File Save to save the job to your PC.

2.4.5 Secure Ethernet to Ethernet

Configuring the PDDEG-S as a secure 'Ethernet to Ethernet Translation Gateway' and connecting multiple DDBC320-DALI controllers together via their Ethernet ports provides a cost-effective and secure scalable lighting control solution.

When configured, SB and SM connect to the PDDEG-S gateways via TLS TCP connections. The PDDEG-S gateways then connect to each DDBC320-DALI via separate TLS TCP connections.

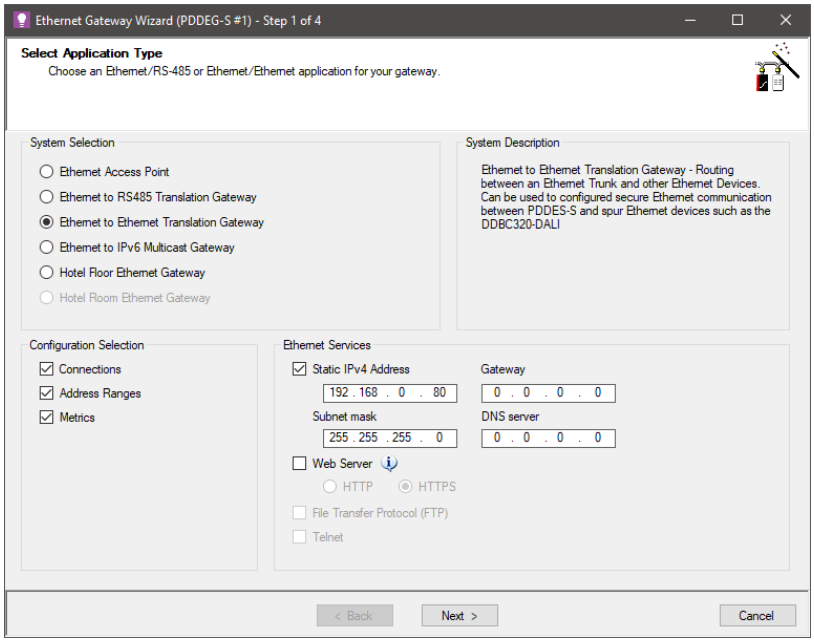
A maximum of 25 DDBC320-DALI controllers can be connected to each PDDEG-S and up to three DDBC320-DALI can be configured with the same offset, to behave as a single spur.



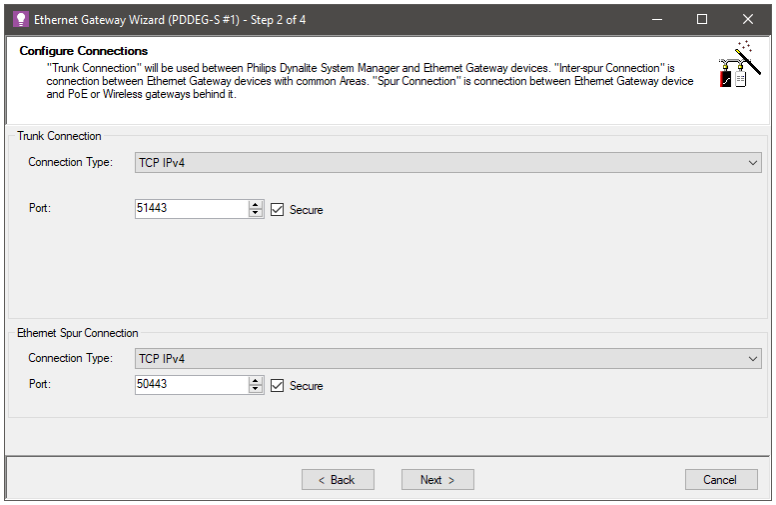
- It is recommended that DyNet spur address range offsets are configured on the DDBC320-DALI rather than on the PDDEG-S.
- For more information on configuring secure DDBC320-DALI Ethernet connections, refer to the Signal Dimmers Commissioning Guide.
- Also, a maximum of 25 DDRC-GRMS-E controllers can be securely connected to each PDDEG-S.

Configure secure Ethernet to Ethernet Translation Gateway:

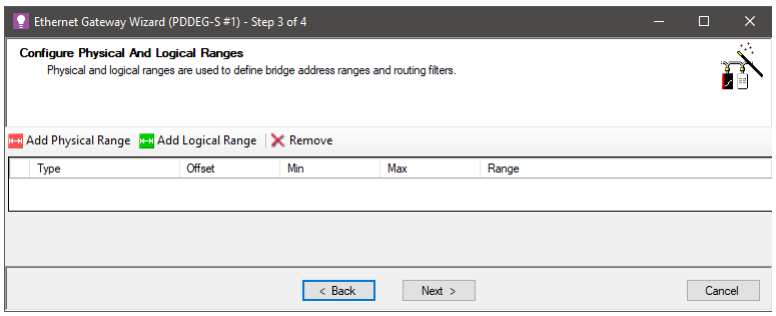
1. Right-click the EG in System View and select Bridge Configuration Wizard... (Alt+W).
2. Add a PDDEG-S to the job.
3. Run the Bridge Configuration Wizard (Alt+W).
4. Under System Selection, select **Ethernet to Ethernet Translation Gateway**.
5. Select **Static IPv4 Address** and enter IP Address (and Gateway and Subnet mask if required).
6. Under Configuration Selection, ensure **Connections** is selected and click **Next**.



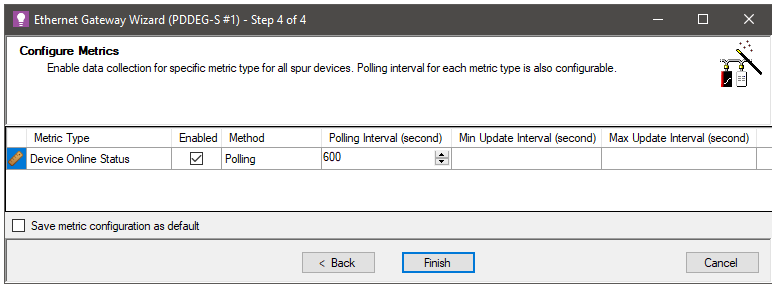
7. Under Trunk Connection, select TCP IPv4, port 51443 and the Secure checkbox.
8. Under Ethernet Spur Connection, select TCP IPv4, port 50443 and the Secure checkbox and click **Next**.



9. Do not add any Physical and Logical Range and click **Next**.



10. Ensure Device Online Status metric checked and click **Finish**.



The wizard adds three new routing records:

- IPv4 TCP Port 51443 → IPv4 TCP Port 50443
- IPv4 TCP Port 50443 → IPv4 TCP Port 51443
- IPv4 TCP Port 50443 → IPv4 TCP Port 50443

This last routine record is required only when different DDBC320-DALI have common areas. When the network is busy, there may be performance issues as this routing record will result in all messages from every DDBC320-DALI being routed to all other DDBC320-DALI controllers. In this case it may be necessary to have separate secure ports (with different port numbers) for groups of DDBC320-DALI that have common areas.

2.4.6 Connecting to the Ethernet Trunk

Once each EG has been configured as a DyNet translation bridge, it will carry DyNet2 messages over the Ethernet trunk. The bridge translates the DyNet1 messages on the spur to DyNet2 on the trunk.

When SB is connected to the trunk, all configured EGs are automatically connected and are marked with the connected upstream icon .

In a multispur network, SB can communicate using an Ethernet Trunk connection. This allows one commissioning engineer to commission the entire system from a single PC.

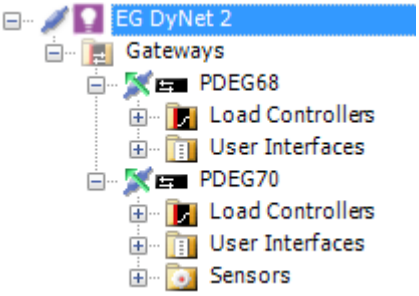
Before you can connect System Builder via a trunk connection, you must have previously run the Bridge Configuration wizard on each EG to configure the translation and then saved it to the device. The Bridge Configuration Wizard will disable the IPv6 default multicast connection when saved to the gateway. This means SB must now connect to the gateway using the Ethernet Trunk Connection or serial connection.

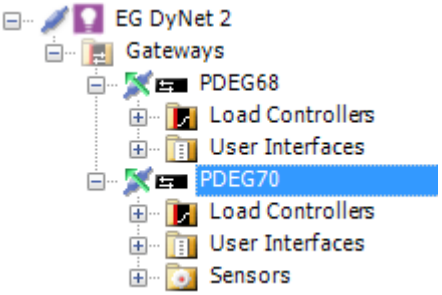
Secure connections require configuring the Ethernet trunk to 'Secure trunk connection' in the job for SB/SM to connect securely.

Connect SB to the trunk:

1. Plug your PC into the router router/switch/vlan with an Ethernet cable or connect over Wi-Fi.
2. Ping the IP address of each EG to check the connection (ensure your PC is on the same subnet as the EGs).
3. Launch SB. If you haven't already added the EGs to the current job, add them now by searching or sign-on.
4. Select the job name in the Device tree.
5. Click the Connection Settings tab.
6. Under Connection Settings, select Use Ethernet Trunk Connection.
7. From the dropdown list, select:
   - TCP only
   - WebSocket Connection (if available)
   - Secure trunk connection

   The EGs in your system are listed in the Ethernet Trunk Connection Settings table at the bottom of the page. The list contains an entry for each EG contained in the job. Its Bridge Name, Box Number, IP address, Port, Routing, Tx Delay and current status are displayed. From here, all connections can be enabled and disabled (see screenshot on next page)
8. At the top of the page, under Trunk Connection, click the Connect button. SB connects to each EG using the connection settings previously defined by the Bridge Configuration wizard.



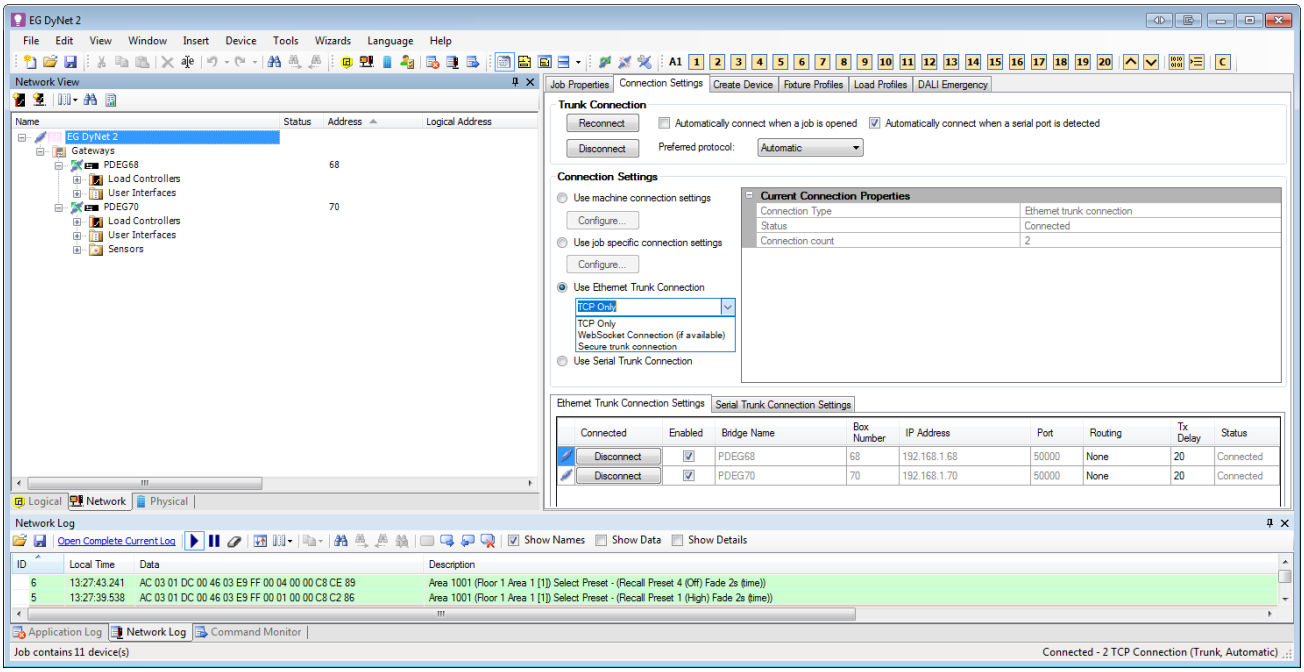


WebSocket and Secure Trunk connections are only valid when connecting to PDDEG-S (not PDEG)

SB can connect to the system from the context menu by right-clicking a selected EG or the top-level job name in System View or by opening the Connection Settings page.

Select an EG in the Device tree before adding other devices to the spur.

When searching for spur devices on the network while SB is connected to the trunk, ensure you enter the address offset in the search parameters. For example, if the trunk gateway is configured with an offset of 1000, enter a minimum of 1000 and a maximum of 1099 to find devices connected to this spur.

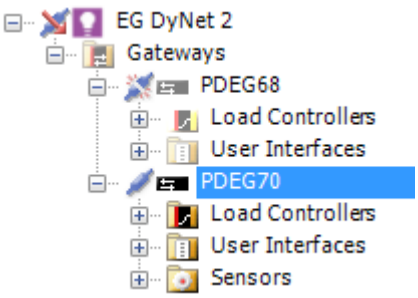


Ethernet Trunk Connection

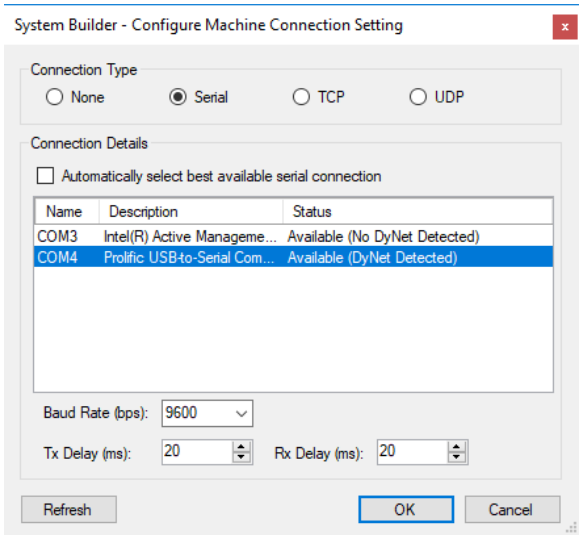
2.4.7 Connecting to a Serial Spur

In an RS-485 multispur network, SB can communicate with the network using a spur connection to a trunk gateway (EG or DDNG485). This allows multiple people to configure different parts of the system at the same time, considerably reducing the commissioning time.

Connect SB to the spur:

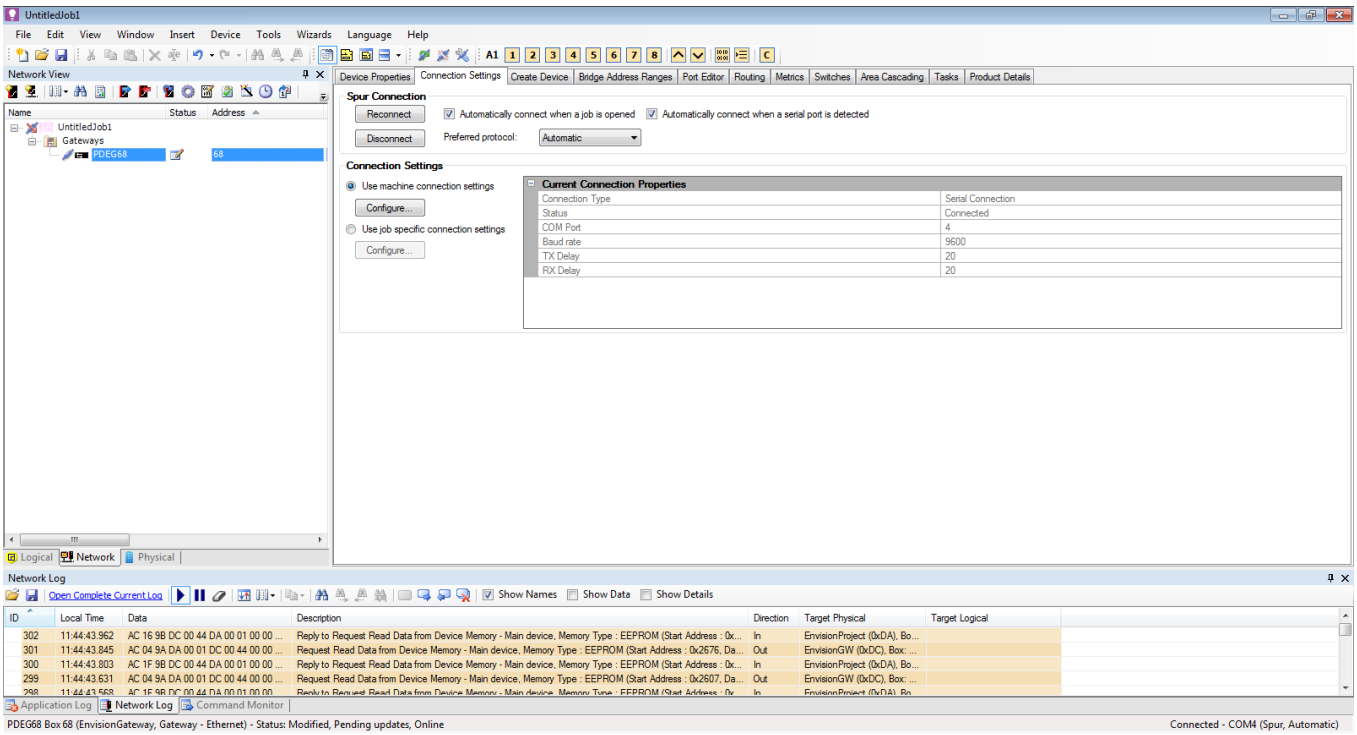


1. Plug a USB PC node into the commissioning PC and then into a DyNet port on the same spur as the EG.
2. Launch SB.
3. Select the EG you want to connect to, in the Device tree.
4. Click the Connection Settings tab.
5. Under Connection Settings, select your preference; Use machine connection settings or Use job specific connection settings.
6. Click the Configure button. SB displays a list of discovered connections.
7. Select Serial for the Connection Type and the connection from the Connection Details list and click the OK button.
8. If the Connection Type and Connection Details are set in SB, then at the top of the page, under Spur Connection, click the Connect button. SB connects to the selected EG.
9. Check that you have selected the correct EG in the Device tree before adding other devices to the spur.



You can perform wireless commissioning by connecting to the RS-485 spur using your bundled wireless router and EG (that is not part of the job), by plugging it into a DyNet port on a spur.

When searching for devices on the network while SB is connected to the spur, you do not need to enter an offset in the search parameters. For example, regardless of the offset configured in the EG, simply use the default minimum of 0 and a maximum of 99 (or 999 for a DyNet2 spur) to find devices connected to this spur.



Serial Spur Connection

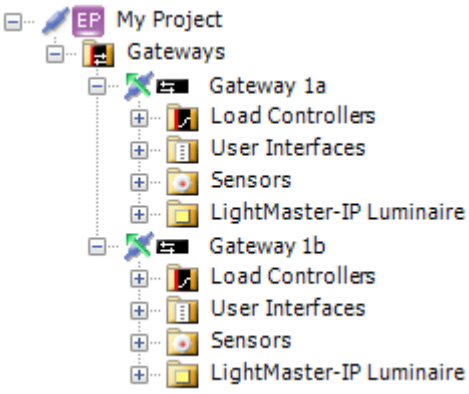
2.5 Adding devices to a spur

SB can insert new devices into a job on the trunk or on a spur. When devices are connected to a spur, they are displayed in the System View under a trunk gateway (EG or DDNG485).

There are two ways to add devices to a spur:

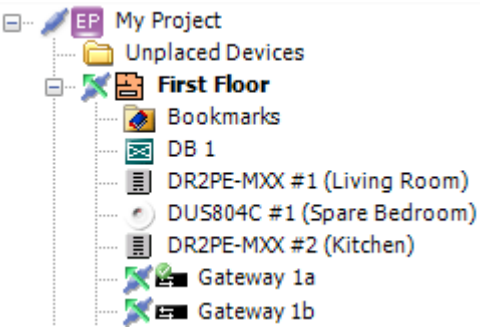
- From System View
- From Physical View

Add devices to a spur from System View:



1. Select the job name in the Device tree
2. Click or and insert an EG into the job.
3. Select the required EG.
4. Click or to insert devices into the job. The devices are added to the spur.

Add devices to a spur from Physical View.



1. Right-click a floor plan in Physical View and select Show Floor Plan.
2. Click and add EG to the Device Palette.
3. Click the icon in the Device Palette, then click on the floor plan (or drag the EG from the Device tree onto the floor plan).
4. in Physical View, right-click the EG and select Set Default Bridge Device.
5. Place other devices onto the floor plan from the Device Palette. The devices are added to the spur.

If there is only one trunk gateway on a floor plan then all devices placed onto the floor plan will be automatically added to this spur.

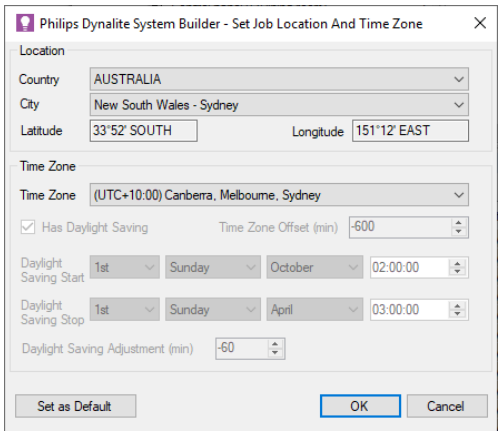
2.6 Setting time zone and realtime clock

The internal astronomical clock in the EG enables advanced scheduling of system actions and automated tasks based on time of day or sunrise/sunset. To modify the settings, refer to Device Properties > Realtime Clock.

When first connecting to the device, it is important for schedules and logs to be set to the correct time zone and local time.

- The time zone may be set for the whole job or for an individual device and must be saved to the device. When pre-commissioning devices, be aware that you may need to configure devices for the time zone of the site.
- Local time may be set for the whole job or for an individual device and is synchronized immediately without having to save to device. The local time must be set again if a device is factory reset.

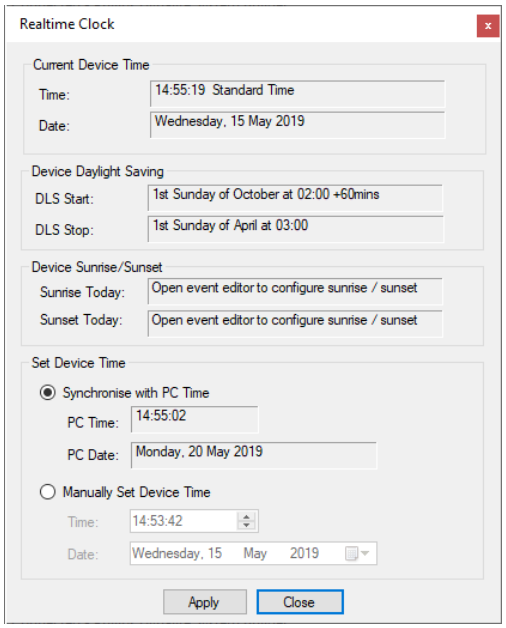
Set the time zone:



1. From the Tools menu select Set Location and Time Zone. or for an individual device, right-click the device and select Set Location and Time Zone.
2. Select the country from the dropdown list.
3. Select the city from the dropdown list.
4. Click the OK button.
5. Click Save to Device.

System Builder cannot set the time zone from coordinates. For all Linux devices (PDDEG-S, PDTS) or to set a custom latitude and longitude, you must first select a country and city in the site's time zone. Click OK and Save to Device. Then from the Country dropdown, select Custom and enter the site's latitude and longitude.

Set the local time:



1. From the Tools menu select Set Realtime Clock for all Devices or for an individual device, right-click the device and select Set Realtime Clock.
2. Under Set Device Time, select:
   a. Synchronize with PC Time. Click the Apply button to set the Realtime clock to your PC time.

   or

   b. Manually Set Device Time. Enter the time and date and click the Apply button.
3. Click the Apply button.
4. Click the Close button.

For more information, refer to 7.1 Device properties > Real-Time Clock

2.7 Area Cascading

The EG contains 100 Area Cascading objects that can be configured to create control dependencies between different areas. Area Cascading objects function as virtual devices in the system and are categorized as follows:

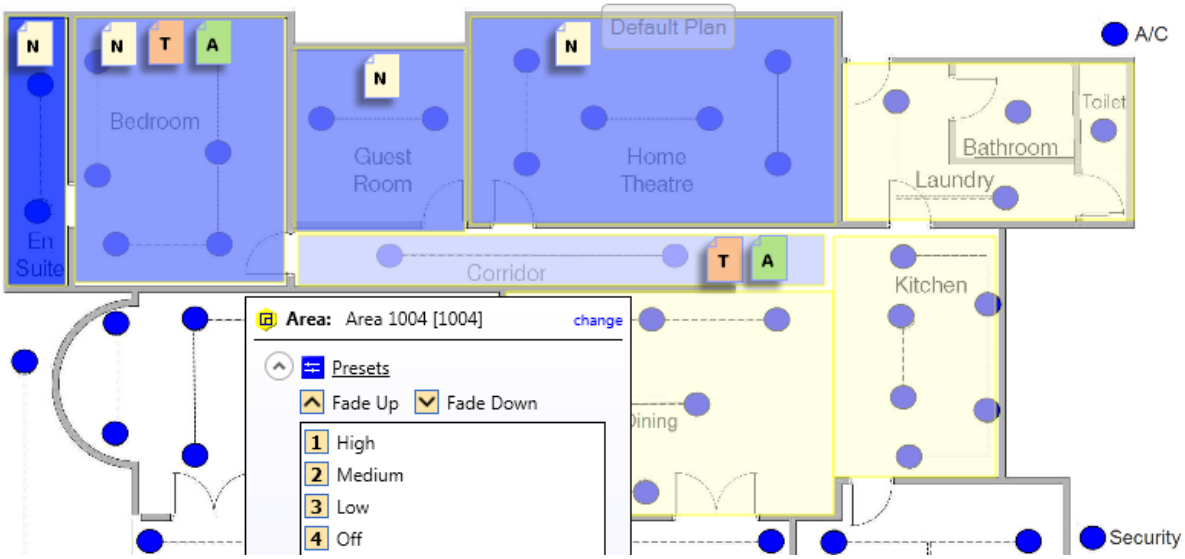
Parent area objects:

- Activator
- Timer

Child area object:

- Notifier

In the below diagram, the dependency hierarchy is indicated by the shading of the areas, darker shading for child areas and lighter shading for parent areas. The letters N, T and A indicate the Area Cascading objects required in each Area Cascading area.



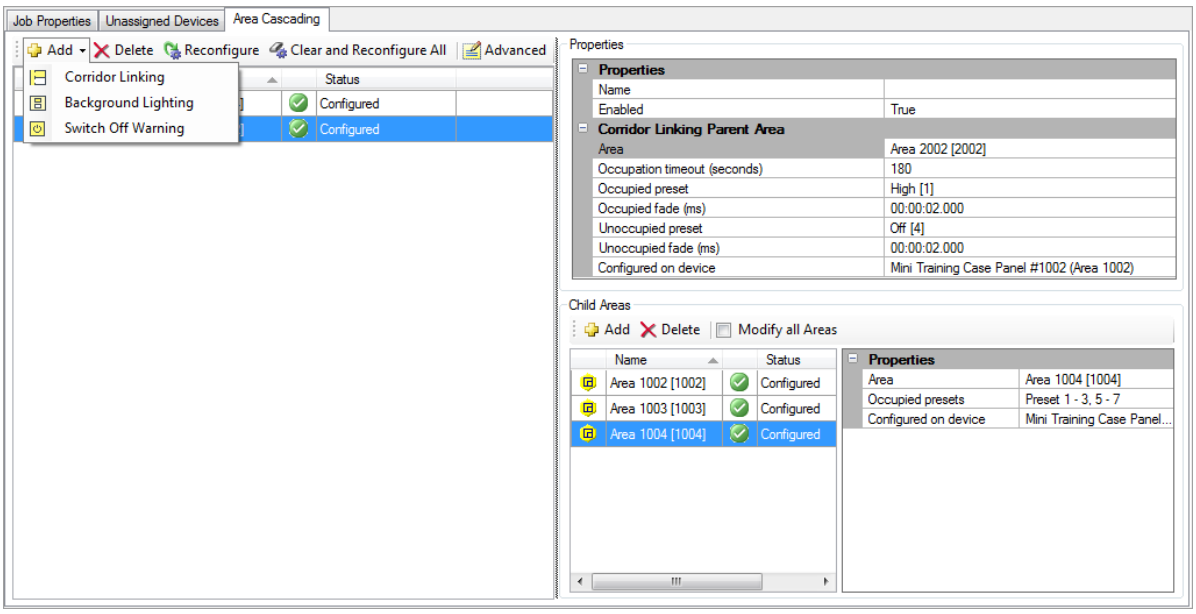
When a Notifier object is placed into an area, it reports the status of that child area as occupied or unoccupied to the Timer and Activator that are in the linked parent area. This enables any area to be controlled by any other area. The Area Cascading objects operate in occupied and unoccupied preset scenes as defined by the commissioning engineer.

Multiple dependencies can be created by cascading the areas from child to parent to grandparent to great grandparent etc. This enables late night egress pathways for a whole building to be created, where unoccupied areas will turn off after a timeout while keeping the areas to the exit lit in any occupied part of the building.

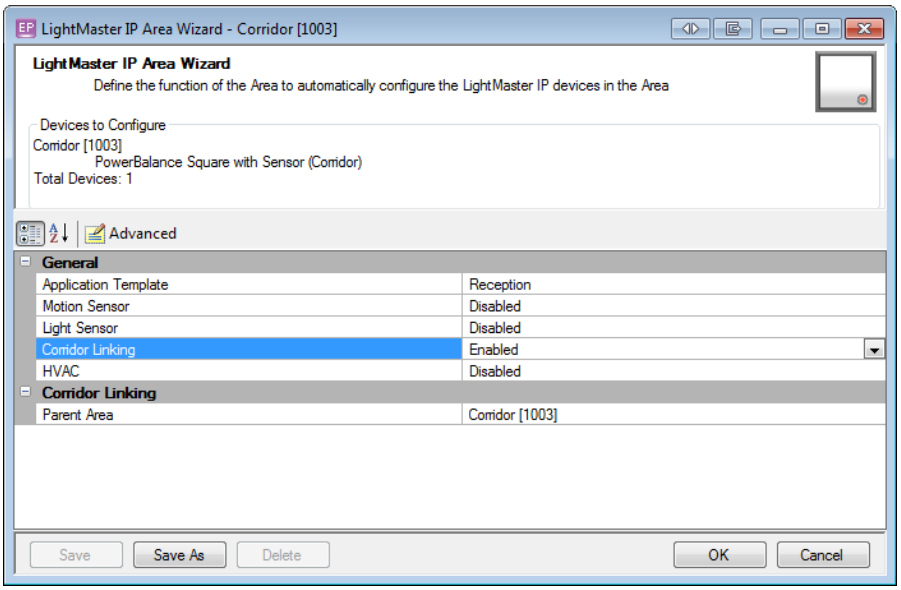
The Area Cascading editor allows you to create different functions for dependent areas:

- Corridor Linking Child Area
- Corridor Linking Parent Area
- Background Lighting Child Area
- Background Lighting Parent Area
- Switch Off Warning Area

Area Cascading is configured by selecting the job name in Areas View and clicking the Area Cascading tab, or on the floor plan by clicking the Highlight Area Cascading Areas icon and right-clicking areas on the floor plan. Refer to the Area Cascading Commissioning Guide for more information.

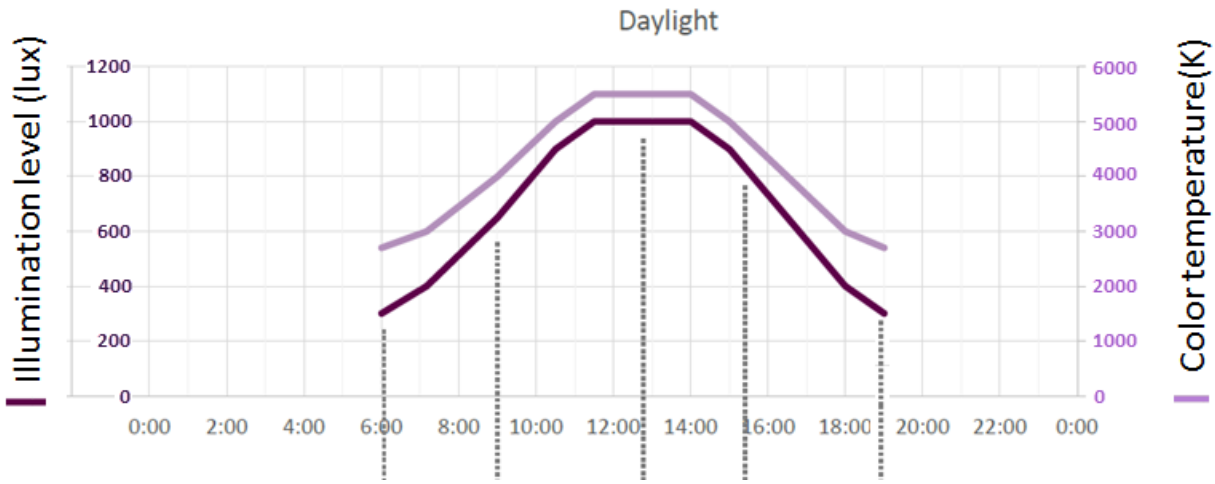


When using EG as an Ethernet area controller, Area Cascading - Corridor Linking can also be configured by right-clicking an area in Areas View and selecting LightMaster IP Area Wizard.
Refer to the Interact Office Commissioning Guide for more information.



2.8 Day Rhythm lighting

The Day Rhythm (bio-adaptive lighting) feature enables colour temperature and light intensity to be dynamically varied throughout the day to simulate the natural daylight cycle. The feature requires an Ethernet Gateway, a DALI 209-compatible controller connected to tunable-white luminaires and a DyNet sensor if performing daylight harvesting at the same time.



The following editors are used to configure Day Rhythm feature.

- **Rhythm Send editor (EG)**
  The Rhythm Send editor is used to configure the Day Rhythm lighting curves in the Ethernet Gateway. Up to five curves can be configured to simulate natural daylight colour temperature and intensity over the course of a day. Different curves can be used to cater for different seasons or for different wake times.
- **Rhythm Receive editor (Sensor & DALI Controller)**
  The Rhythm Receive editor is used to select the Day Rhythm curve messages received by DALI controllers and DyNet sensors.
- **Outputs editor (Areas View)**
  The Outputs editor (in the area where you want to implement day rhythm), is used to specify the initial Day Rhythm curve number and the Day Rhythm Active Presets for drivers that will follow a day rhythm curve.
- **Light Control – Closed Loop editor (Sensor)**
  The Light Control – Closed Loop editor, is used to specify the Day Rhythm curve number and to enable the Day Rhythm Active Presets for a sensor.

The default Day Rhythm curve for sensors and controller outputs it is dynamically changeable. You can schedule commands to change/enable and disable curves in a single area with the following commands:

- Target area to curve 1 - DyNet(0x1c,target area, 0x19,0x48,0,0,0xff)
- Target area to curve 2 - DyNet(0x1c,target area, 0x19,0x48,1,0,0xff)
- Target area to curve 3 - DyNet(0x1c,target area, 0x19,0x48,2,0,0xff)
- Target area to curve 4 - DyNet(0x1c,target area, 0x19,0x48,3,0,0xff)
- Target area to curve 5 - DyNet(0x1c,target area, 0x19,0x48,4,0,0xff)
- Target area disable curve - DyNet(0x1c,target area, 0x19,0x48,0xff,0,0xff)

When a Colour + Level Day Rhythm Curve is enabled, the EG sends a DyNet2 message once a minute containing both the colour temperature and the channel level to DALI controllers.

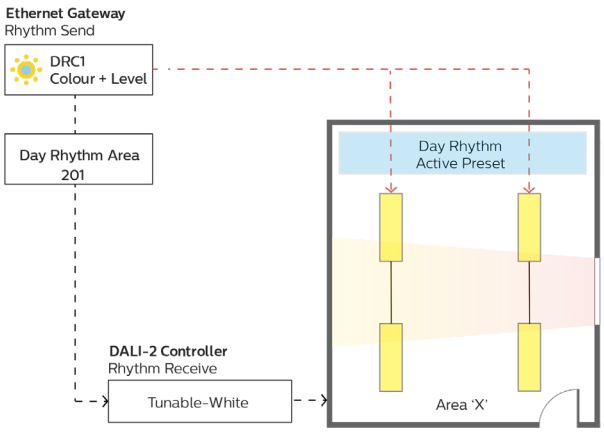
When a Colour + Lux Day Rhythm Curve is enabled, the EG sends a DyNet2 message once a minute containing the colour temperature to DALI controllers and a target lux level to sensors performing closed-loop light control (daylight harvesting).

- Colour temperature range is 2500 to 7000 Kelvins.
- Channel level range is 0 to 100%.
- Sensor lux range is 0 – 60000 lux.

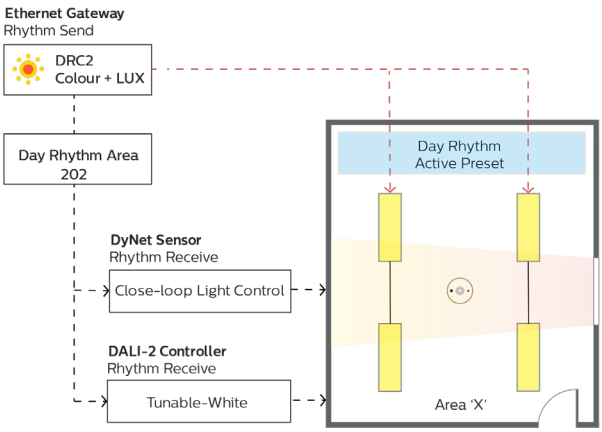
A Day Rhythm Area Number for each curve links logical messages from the EG to the DALI controllers and DyNet sensors, so they can listen for the Day Rhythm Curve broadcasts.

A DALI controller receives a Day Rhythm message and if the specified channels in Area 'X' are in a Day Rhythm Active Preset, the controller ramps their colour temperature and channel level according to the latest received values.

A sensor in Area 'X' receives a Day Rhythm message, and if the area is in a Day Rhythm Active Preset, the sensor detects the amount of daylight and regulates the light intensity of the specified channels to achieve the latest received target lux level.



Colour + Level bio-adaptive lighting



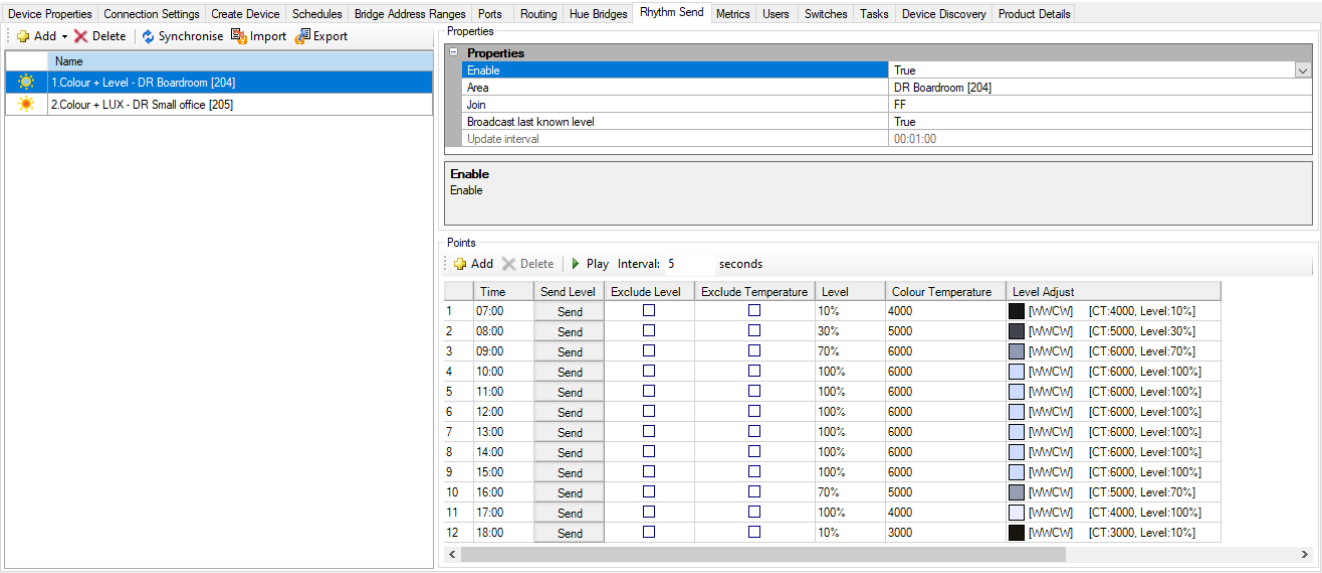
Colour + Lux bio-adaptive lighting

- You can configure Rhythm Receive on any number of sensors and DALI controllers as long as they are in areas within the logical area range of the EG.
- Sensors performing daylight harvesting in a single area must listen to the same Day Rhythm curve.
- DALI drivers and luminaires must be compatible with the configured colour temperature range.
- DALI sensors and the DUS804CS-UP do not currently support the Day Rhythm feature.

Configure an Ethernet gateway for Day Rhythm:

1. In System View, select an EG and click the Rhythm Send tab. Note that the EG can only broadcast Day Rhythm messages to logical areas within its translation area range.
2. Click Add and select Colour + Level or Colour + LUX. A Day Rhythm curve is added (1 to 5) (Ensure Enable is set to True).
3. Select a day rhythm area where the DALI controllers and sensors can listen for day rhythm messages. You must select a different day rhythm area for each curve.
4. Select Broadcast last known level, to keep broadcasting the curve levels between the last point of the day until the first point of the next day.
5. In the Points section, click Add, to create the Day Rhythm Curve points. You can add up to 24 points. When you add more points, the time will increment hourly based on the time of the first point or you can manually enter the time.
6. Edit the properties for each point on the curve:
   a. Time – time of day specified for the selected point.
   b. Exclude level – current channel levels will not be altered at the selected point.
   c. Exclude Temperature – current colour temperature will not be altered at the selected point.
   d. Level (Lux) – channel level (or Lux) target at the selected point.
   e. Colour temperature – colour temperature target at the selected point.
   (The Level Adjust property provides sliders to adjust both the channel level/lux level and colour temperature).
7. Click Save to device or press [F12] on the keyboard.

To run a test, enter the interval time and click Play.



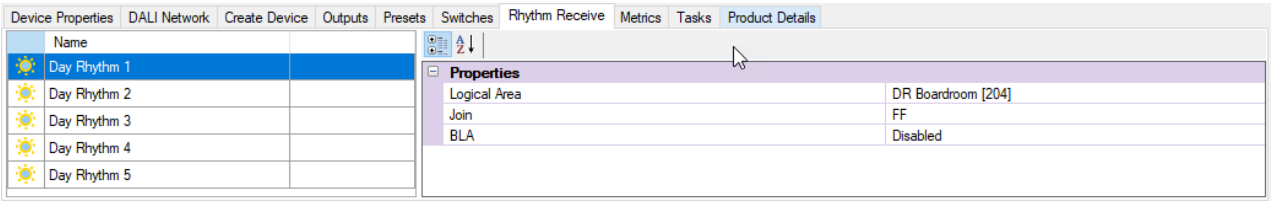
You can click the Synchronize button to detect and automatically create corresponding day rhythm curves with the matching day rhythm areas in the controllers (and sensors) under the gateway that support day rhythms.

In addition, you can select import or export to transfer Day Rhythm curves between projects.

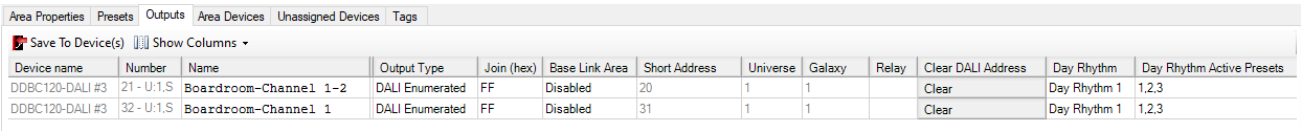
The Rhythm Receive Editor lets you select the same day-rhythm curves and areas configured in the EG so the controllers and sensors can receive the Day Rhythm messages from the EG.

Configure a DALI controller for Day Rhythm:

1. In System View, select a DALI Controller.
2. Click the Rhythm Receive tab.
3. Select a Day Rhythm curve and area corresponding to the curve and area configured in the EG (you can skip this step if you clicked the Synchronize button in the EG > Rhythm Send Editor).



4. In Areas View, select the area where the DALI drivers are assigned or click the Unassigned Devices tab to find the DALI controller and assign the drivers to the area where you intend to use Day Rhythm.
5. In Areas View, click the Outputs tab.
6. Right-click the heading row and select the following columns to be displayed:
   a. Day Rhythm
   b. Day Rhythm Active Presets
7. Click the Day Rhythm property for each driver channel and select a default curve (1 to 5).
8. Click the Day Rhythm Active Preset property for each channel and select the presets (1 to 16) where the Day Rhythm curve will be active.



9. Click Save to device or press [F12] on the keyboard.
10. Select one of the Day Rhythm active presets for the required area. The relevant controller lighting channels will start displaying the light intensity and colour temperature as defined by your curve.

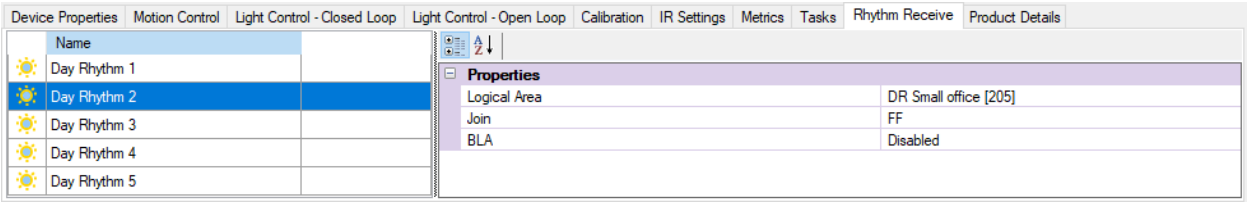
You can edit the properties in the DALI controller Outputs editor provided the channels are assigned to the intended areas. The Outputs editor lets you select the day rhythm active presets and the curve each channel responds to. For example, you could select Day Rhythm to only function on channels 1, 2 and 3 when those channels are in Preset 1 or Preset 2.

You can also copy and paste curve numbers and active presets to other channels.

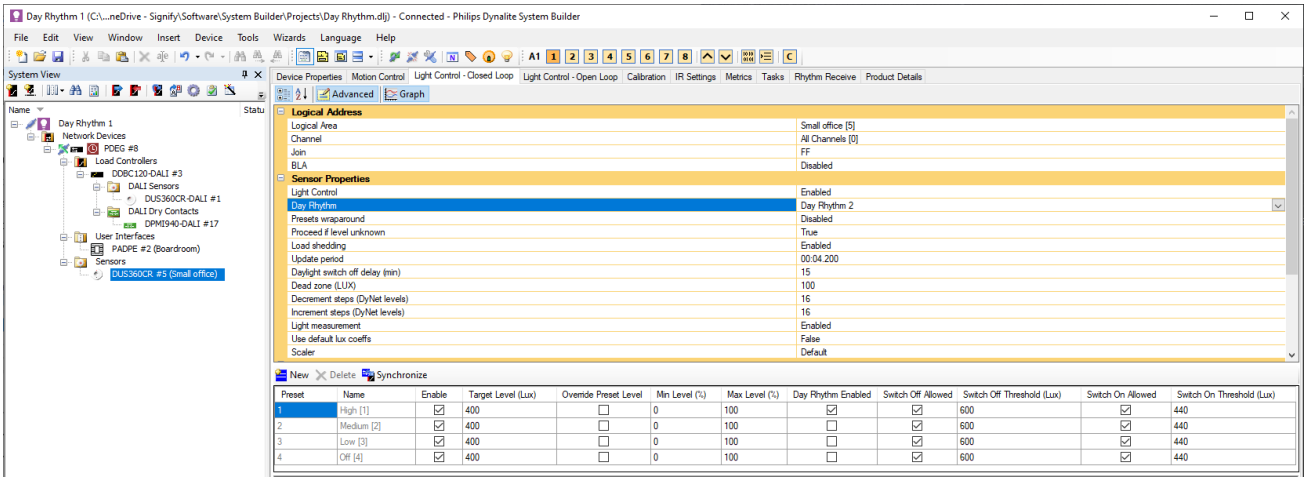
You must have configured an EG with a Colour + LUX Day Rhythm curve for the sensor to use for Day Rhythm.

Configure a Sensor for Day Rhythm:

1. In System View, select a DyNet sensor.
2. Click Device Properties tab.
3. Click Advanced to show more properties.
4. Select Device Logical Address > Logical Area and click the change button to select the area where the sensor is located or if you have a floor plan, you can drag the sensor from the device tree into the required area.
5. Click the Rhythm Receive tab.
6. Select a Day Rhythm curve and area corresponding to the Colour + LUX curve and area configured in the EG (you can skip this step if you clicked the Synchronize button in the EG > Rhythm Send Editor).



7. Click the Light Control – Closed Loop tab. (ensure Light Control is Enabled)
8. In Sensor Properties > Day Rhythm, select the default curve that the sensor will follow.
9. In the Presets section, click New to add a Preset that the sensor will use for Day Rhythm.
10. Click Advanced to show more columns.
11. Select the Day Rhythm Enabled checkbox.
12. Click Save to device or press [F12] on the keyboard.
13. Select one of the Day Rhythm active presets for the required area. The sensor will start regulating the lights and the relevant controller lighting channels will start displaying the target lux level and colour temperature as defined by your curve.



3 Integration

3.1 Hue Integration

The PDEG provides limited one-way integration with Philips Hue.

The Hue Editor allows you to configure a Dynalite system to send preset and channel level messages to a Hue system.

A Hue system is made up of several Hue lights that are connected to a Hue bridge with the wireless ZigBee protocol. The bridge connects to a Wireless Access point via Ethernet and the Hue app connects to the Wireless Access point over Wi-Fi or over the Internet. Configuration data for the Hue lights, rooms and scenes is stored in the Hue bridge.

When Hue integration, is enabled in the Hue Bridges editor, the PDEG reserves 64 areas as Hue areas, starting from the Start DyNet Area. Each Hue room corresponds to a DyNet area, and each Hue light corresponds to a DyNet logical channel. Additionally, The Start DyNet Area can control all the lights for a Hue bridge.

Terminology

Hue	DyNet
Room	Area
Scenes	Presets
All Hue rooms	Start DyNet Area
Lamp X	Logical Channel X

Considerations

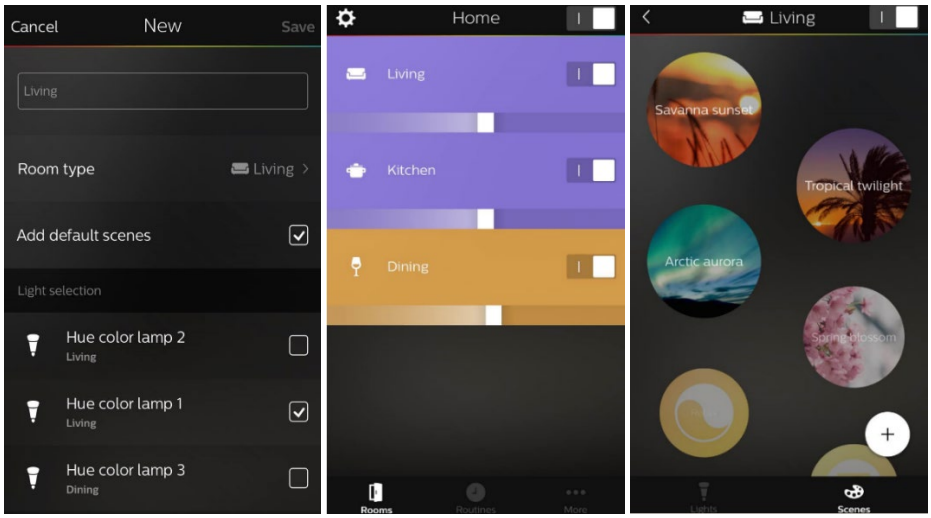
- The Hue System must be commissioned using the Hue App 2.x or later, before interfacing to the PDEG.
- The Hue 2.x app does not allow an OFF scene to be created. Use fade to level (opcode 0x04) commands to switch lights off.
- Only one-way communication is currently supported, which means, changes to Hue levels and scenes are not seen as messages in DyNet.
- Fade times for absolute channel level messages are supported. However, DyNet Stop Fade and Fade times are not supported for scenes in Hue.
- Changing RGB levels of the Hue lamps from DyNet is not supported.
- Hue icons are not supported on the floorplan window.
- Scenes must be edited with the Hue app.

Hue integration is not supported by the PDDEG-S.

3.1.1 Configuring Hue lamps

Create the lights, rooms and scenes in Hue app. The Hue App 2.x screenshots below, show how lights, rooms and scenes are configured.

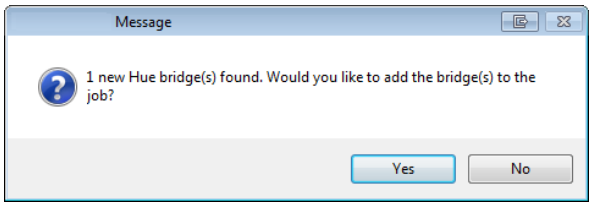
Scenes can add up quickly. By default, 11 scenes are configured for each Hue room. It is recommended to uncheck the Add default scenes checkbox so that fewer presets are created in DyNet.



3.1.2 Adding Hue bridges

Each EG supports up to four Hue bridges. Check that the System Builder PC is connected to the same network before attempting to discover the Hue bridges.

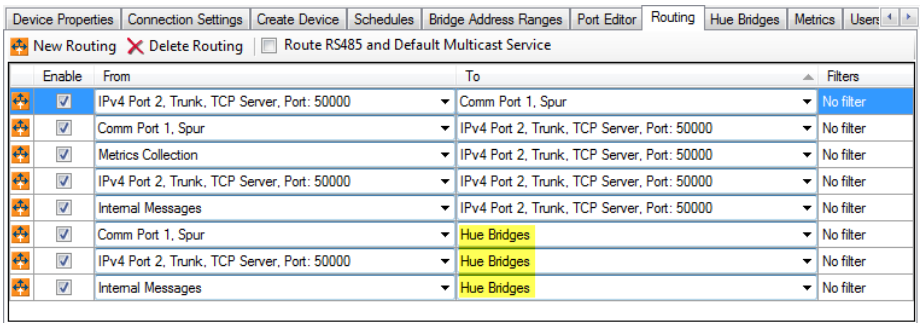
Discover Hue bridges:



1. In System View, select the EG.
2. Click the Hue Bridges tab.
3. Click Discover hue bridges. SB scans the network for the Hue bridge(s).
4. Click the Yes button to add the bridge to the job.

   Alternatively, you can click Add, to add a bridge manually if you know its IP address.

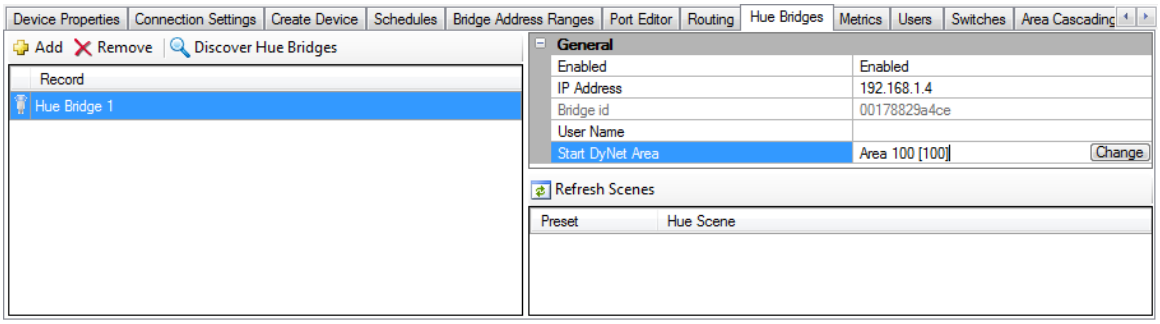
Routing is added whenever adding a new hue bridge or by running the Bridge Configuration Wizard.



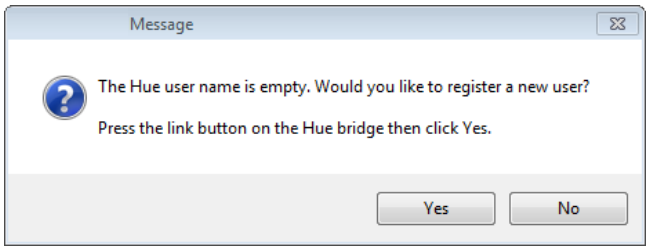
3.1.3 Mapping Hue configuration

Refresh Hue Scenes:

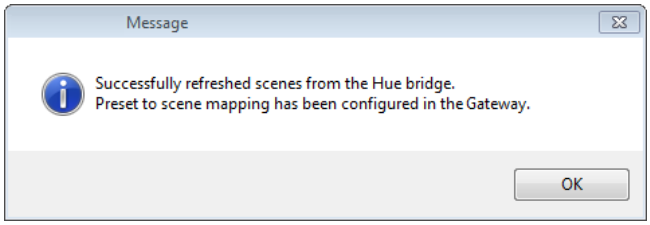
1. Enter the Start DyNet Area number. The Start DyNet Area number defines an area that contains all the Hue lamps.



2. Click Refresh Scenes to load the configuration information from the Hue bridge.
3. A new username is generated when SB refreshes scenes for the first time. If a valid username does not already exist, press the link button on the bridge and then click the Yes button in SB.



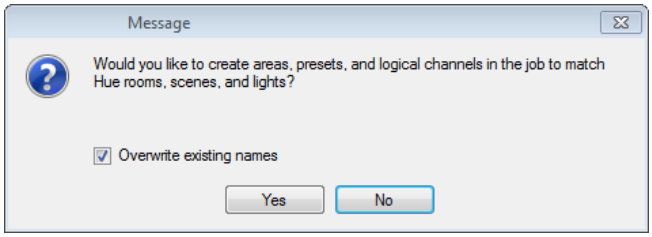
SB will then load the scene data from the Hue bridge and configure the preset to scene mapping in EG.



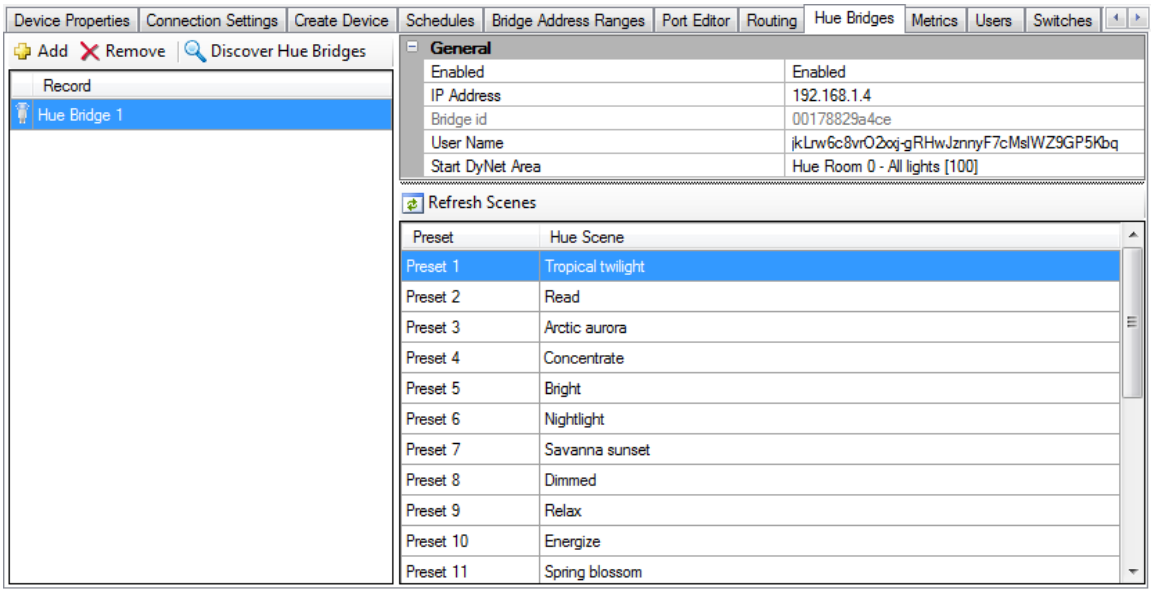
4. If you are refreshing scenes and the areas do not yet exist or do not exactly match the hue system, SB will give you the option to create them.

   Select the checkbox to overwrite existing area and preset names with the Hue names.

   Click the Yes button, to create/modify the Hue areas, logical channels and presets.



5. Click Save to device or press [F12] on the keyboard.



Scenes are grouped into rooms. However, for subsequent updates, scenes are received from the Hue bridge in the order they were entered into the Hue App. For example, if there are 10 default scenes, presets 1-10 will be scenes from the first room. Presets 11-20 from the second room etc. If a room 1 scene is created later then upon refreshing scenes it will appear at the end of the list even though it belongs to room 1

To re-sort scenes into rooms, remove then re-add the Hue bridge

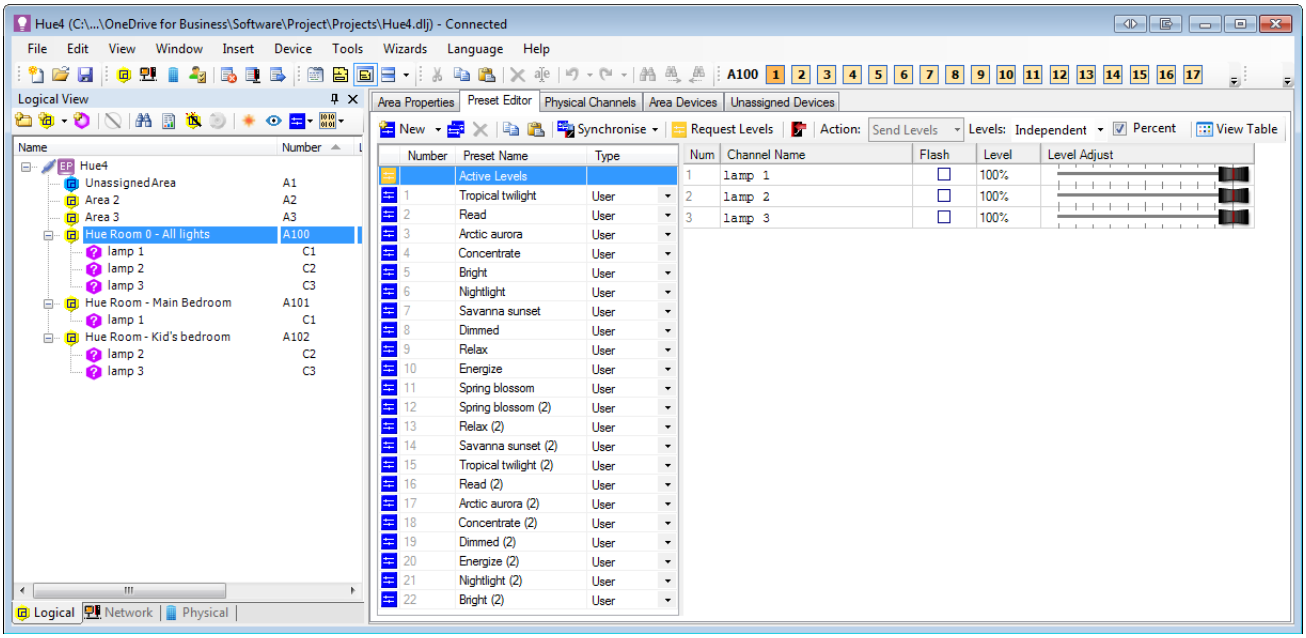
Areas are created (up to 64) for each user-configured room starting from the Start DyNet Area.

Area number = Start DyNet Area + room number.

Each area will have the presets for all scenes, but presets are hidden for scenes that do not affect the lights in that area.

The Start DyNet Area may be used to send preset or channel level messages to all Hue lamps connected to that bridge. In Hue Room 0, Logical channel X = Hue light X. All other areas contain only the logical channels for the lights in that room.

Recalling a preset for an area recalls the associated Hue scene for the corresponding Hue room. Recalling a logical channel level in DyNet recalls the individual Hue lamp intensity



3.2 Text over IP

The EG can integrate with third-party devices by sending and receiving user defined text messages in ASCII or binary protocols. Text messages can be communicated over a TCP or UDP connection. For example, sending text to an IP address to control AV equipment. There are two types of Instructions:

- A SendPF instruction is written in a task to send numbers to text ports from tilde locations.
- A SendP instruction is written in a task to define the string of ASCII or hexadecimal packets.

Setup third-party text communication port:

1. Add an EG to the System Builder Job.
2. If connecting to a third-party device using IPv4 ensure the EG is configured in the Port Editor by entering a static IPv4 address or to acquire a dynamic IP address by setting the 'Use static IP address' property to false.
3. In the Port Editor add a new port and set the port type to Text and Binary Integration. Make sure the Mode, Port and Protocol properties are correct for connecting to the third-party device.
   Refer to Port Editor port properties.
4. Open the Tasks editor and enter the SendPF or SendP task instruction.
   The instruction has the following format:

   SendP (Port Type, Port Index, Data, ...)

   Port Type: 1=Comm port (supported but cannot add), 2= IPv4 Port, 3= IPv6 Port.

   Port Index is a sequence number starting from 1 for each port type.

   (The Port Type, Index can be found in the port list)

   Data supports up to 126 characters in ASCII or Hex.

   SendPF (Port Type, Port Index, "%c %d %u %s %x", ~1,~2,~3...)

   Where %c, %d, %u, %s, %x are format specifiers.
5. Test compile the task and write to device.

For sending text using the printf format, SendPF supports the same instructions as SendP and more.
This allows values to be easily sent from tilde locations.

The SendPF command will allow for up to 8 tilde memory locations to be specified where the value of the parameters (by using the % symbol) will be output.

Supported Specifiers:

%d : Output an integer as a signed decimal number.

%u : Output for decimal unsigned int

%x : Output an integer as an unsigned hexadecimal number.

%c : Output a character (char). No null character is added.

%s : Outputs a string. No null character is added.

To send a 2-byte number append length 'l' (i.e. %ld). This allows for signed number greater than +/-127 and unsigned numbers greater than 255

To send a 4-byte number append length 'll' (i.e. %lld)

3.2.1 SendPF text commands

	Instruction examples
Direct Text	IPv4 port, Port Index = 1, Data ="sendthistext" **SendPF (2,1,"sendthistext")** If the text requires being null terminated then add '%c' after the string and use '0' as parameter **SendPF (2,1," sendthistext%c",0)** If the text requires a carriage return then add '\r' after the string **SendPF (2,1," sendthistext\r")**

From a declaration at a label	**1)**
	#const HVACLine "L1"
	Task1()
	{
	Name="Task 1"
	SendPF(2,1,"cmd %s", HVACLine)
	Null
	}
	Output will be cmd L1
	
	2)
	#const HVACLine "L1"
	#const Command "cmd %s%c%c"
	Task1()
	{
	Name="Task 1"
	SendPF(2,1, Command, HVACLine,0x0D,0x0A) //0x0D stands for carriage return & 0x0A line feed
	Null
	}
	Output will be cmd L1

From Tilde Memory	Task5()
	{
	Name="Task 5"
	Start(0x1C,x,x,x,x,x,x)
	Copy @0,~0,7
	//%u is for unsigned integer 0 to 255
	//Area value is stored at ~1
	Sendpf(1,1,"Area is %u", ~1)
	null
	}
	Output will be Area is <Area Number in the DyNet message>
	If we use %d for Area Number, then only up to Area 127 will be correctly shown.

3.2.2 SendP text commands

	Instruction examples
Direct Text	Pv4 port, Port Index = 1, Data =”sendthistext” **SendP(2,1,"sendthistext")** If the text requires being null terminated then add an additional 0 parameter **SendP(2,1,"sendthistext",0)** If the text requires a carriage return then add an additional 0x0D parameter **SendP(2,1,"sendthistext",0x0D)**
Hex Packets	**SendP(2, 1, 0x68, 0x65, 0x6c, 0x6c, 0x6f, 0x77, 0x6f, 0x72, 0x6c, 0x64)**
From Tilde Memory	Task2() { Name="Advanced Text over IP" LDA #0x41 //'A' Load 6 Bytes Into Tilde STA ~0 LDA #0x42 //'B' STA ~1 LDA #0x43 //'C' STA ~2 LDA #0x44 //'D' STA ~3 LDA #0x45 //'E' STA ~4 LDA #0x00 //Null STA ~5 LDX #0x01 // Set an offset of 1 String in memory must be null terminated. The output will be ABCDE. **SendP(2, 1, ~0)** With an offset in the index register. The output will be BCDE. **SendP(2, 1, ~0, X)** With a specified length. If L=0x03 then output will be ABC **SendP(2, 1, ~0, L)** With an offset in the X register and a specified length. If L=0x03 then output will be BCD. **SendP(2, 1, ~0, X, L)**
From a declaration at a label	**TestLabel:** **SendP(2, 1, “VWXYZ”, 0)** Send from label. String must be null terminated. The output will be VWXYZ. **SendP(2, 1, TestLabel)** With an offset in the index register. If X=1 then output will be WXYZ. **SendP(2, 1, TestLabel, X)** With a specified length. If L=0x03 then output will be VWX. **SendP(2, 1, TestLabel, L)** With an offset in the X register and a specified length. The output will be WXY. **SendP(2, 1, TestLabel, X, L)**

3.2.3 Receive text commands

Incoming text over IP messages trigger a Start task instruction. The scanf format (in the table below) is used to define the received text. The instruction allows you to specify up to 8 tilde memory locations to store the value of the parameters (by using the % symbol).

	Instruction example
Format	%[*][width][length]specifier
Specifies	%d Scan an integer as a signed decimal number. %i Scan an integer as a signed number. Similar to %d, but interprets the number as hexadecimal when preceded by 0x. %u Scan for decimal unsigned integer. %x Scan an integer as an unsigned hexadecimal number. %s Scan a character string. The scan terminates at whitespace. A null character is stored at the end of the string, which means that the buffer supplied must be at least one character longer than the specified input length. %c Scan a character (char). No null character is added. %n The number of characters read so far from stdin is stored in the pointed location. No input is consumed. %% A % followed by another % matches a single %. '*' An optional starting asterisk indicates that the data is to be read from the stream but ignored (i.e. it is not stored in the tilde memory location pointed by an argument). Width Specifies the maximum number of characters to be read in the current reading (optional) operation. Length This alters the expected type of the storage pointed to by the corresponding (optional) argument. By default in this implementation the length of numbers is 1 byte. To store a 2 byte number append length with lower case "L" (i.e. %ld). This allows for signed number greater than +/-127 and unsigned numbers greater than 255. To store a 4 byte number append length two lowercase "L"s (i.e. %lld).
Examples	Start("Hello") The command matches any incoming packet that starts with "Hello". Text is case sensitive Start("Temp A%d %d.%d",~7,~6,~5) for example: Temp A5 24.5 The command matches any incoming packet that starts with "Temp", a space, the letter "A" and a number, a space and a number with a decimal point and another number. The numbers are stored in ~7, ~6 and ~5 respectively. Start("B. %*4s F%d %d.%d",~4,~5,~6) for example: Temp F6 23.7 The command matches any incoming packet that starts with the letter "B" and a full stop, a space, a four character string that is ignored, a space, the letter "F" and a number, a space and a number with a decimal point and another number. The numbers are stored in ~4, ~5 and ~6 respectively. Start("Volume%d %ld",~20,~21) for example: Volume5 337 The command matches any incoming packet that starts with "Volume" and then a number, a space and then another number. The first number will be stored in ~20 and the second number in ~21 and ~22.

3.2.4 Receive binary commands

The Ethernet Gateway now supports receiving third party binary/hex messages over IP. System Builder 3.11.7 or newer is required to take advantage of this feature.

The "Startx" command can be used in a task to listen to third party binary/hex messages.

For example: StartX(0x01,x,0x03,x,x,x,0x07)

The command features:

- Decimal or hex (using 0x) byte values.
- Character "x" for non-matching bytes.

A dedicated, TCP IPv4 port configured as "Text and Binary Integration" is required in the Ethernet Gateway.

3.2.5 Cool Automation integration

Integration with the Cool Automation central HVAC control system enables centralized and in-room HVAC control and monitoring. Integration is performed with a CoolMasterNet bridge, dedicated HVAC Ethernet Gateways and AntumbraDisplays in each room.

Supported CoolMaster actions

Request HVAC Status (Channel 100: replies with all current settings in the HVAC unit).

On/Off Specific/All HVAC units (Channel 101: 0% = OFF, 1 - 100%= ON).

Change the HVAC mode for specific/All units (Channel 102: 0% = Cool, 1% = Heat, 2% = Fan, 3% = Dry, 4% = Auto, 5% = Aux Heat).

Change the Fan Speed for specific/All units (Channel 103: 0% = Low, 1% = Medium, 2% = High, 3% = Top, 4% = Auto). These channel levels are absolute, e.g. “Auto” is always 4% even if “High” or “Top” is disabled.

Change the Louver Position (Swing) for Specific/All units (not all Indoor Units support louver position)

(Channel 104: 0% = Horizontal, 1% = Vertical, 2% = Auto, 3% = 30°, 4% = 45°, 5% = 60°).

Report error in the HVAC unit (Channel 105: 0% = OK, 1-100% = Error)

Display the Filter status (- or #) reported by the HVAC unit (Channel 106: 0% = OK, 1% = Filter to be cleaned).

Display and Change Set point temperature for specific/All units (DyNet message sent from Antumbra).

Display the Room temperature reported by the HVAC unit (DyNet message sent from Antumbra).

Limitations and constraints

- Temperature is represented in degrees Celsius. Fahrenheit is not supported.
- Only absolute integer values are supported at this stage.

CoolMasterNet Configuration

Firstly, the CoolMasterNet Bridge must have Line and Units configured by the HVAC installer.

Ethernet Gateway Configuration

You need to add one or more Ethernet Gateways (EG) to the job in System Builder, then run the bridge configuration wizard to setup the Ethernet gateway(s) as an Access Point. One Ethernet Gateway can control up to 40 HVAC units.

The 'Text over IP' feature in the Ethernet Gateway is used for this integration via the CoolMasterNet Ethernet interface. To allow the passing of messages between the room controller and the CoolMaster system, each Ethernet Gateway in the system must have an IPv4 port preconfigured as follows:

- Port Type: Text and Binary Integration
- Mode: Client
- IP Address: <IP address of the CoolMasterNet>
- Port number: <TCP Port of the CoolMasterNet bridge>
  (Default TCP port supported by CoolMasterNet is 10102)
- Protocol: TCP

In the Ethernet Gateway Tasks Editor, select the 'CoolMaster Integration – EG.evt' task template. Edit the task template settings to match the CoolMaster configuration. Some of the settings need to come from the HVAC installer.

Simulation mode

It is recommended to first test the CoolMaster integration by placing the CoolMaster gateway into simulation mode. In the Ethernet Gateway task template, you can configure several simulated HVAC units. To enable them to start the "set simulation" task in the Ethernet Gateway. As a result, the CoolMaster gateway should be populated with the configured amount of simulation units.

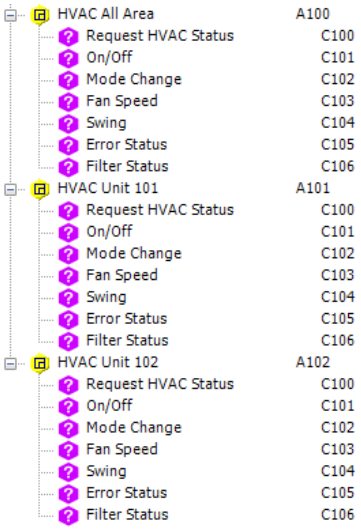
While in simulation mode the 'Swing' and 'Fan Speed = Top' functions are not supported.

Logical Configuration

Each HVAC unit is controlled by a dummy area and corresponding channels for each action (see image below). The total amount of areas should match the HVAC zones to be supported.

For example, Area 100 is for All HVAC units, Area 101 is for Room 1, Area 102 is for Room 2 etc. Each area must have seven channels numbered from channel 100 to channel 106.

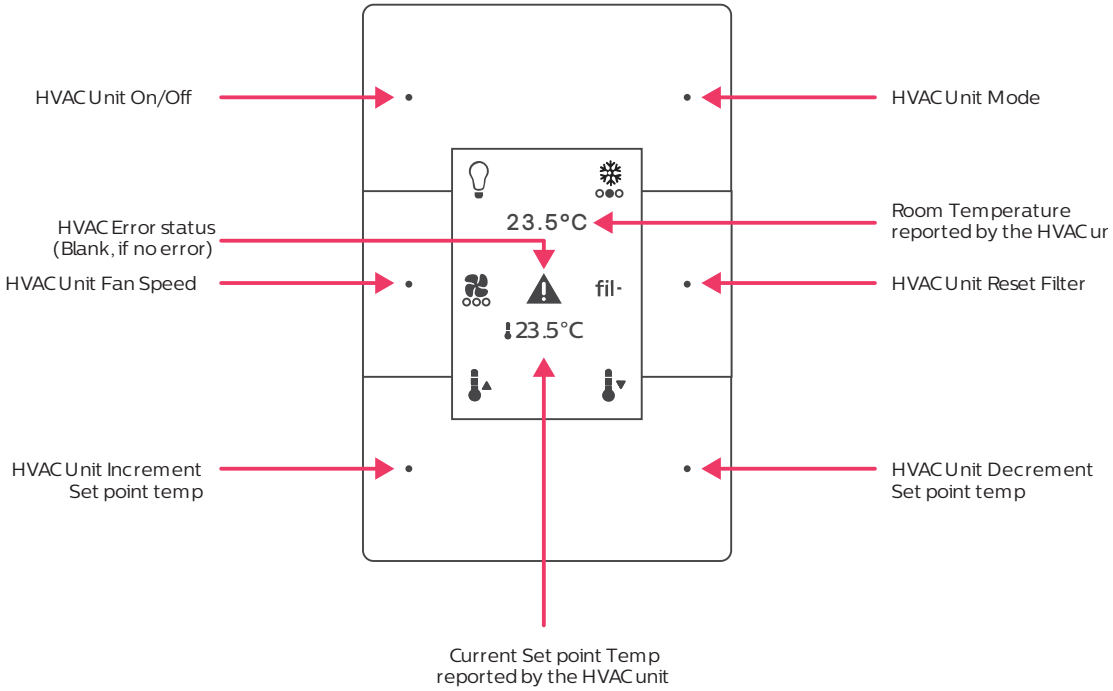
For more information refer to www.dynalite.org: FAQ #0494-CoolMaster-integration-using-EG-as-txt-gateway.



You must use these specific channel numbers. The channel numbers are hard coded in the task template and cannot be changed.

AntumbraDisplay Configuration

CoolMaster integration requires one AntumbraDisplay per HVAC unit in the room, or used by the facility manager for all HVAC units. The AntumbraDisplay polls the CoolMaster system every time the proximity sensor is triggered. This synchronizes the AntumbraDisplay with CoolMaster.



Configure AntumbraDisplay for CoolMaster:

Under the AntumbraDisplay's **Tasks** tab:

1. Click **Select Task Template**, then **Coolmaster Integration - Antumbra.evt** and click **OK**.
2. In the task template, set **Parameters > Dynet HVAC Area** to the correct logical area for the HVAC.
3. Enter 0 for any modes and fanspeeds not supported by your HVAC unit.

Open the **Device Properties** tab and make the following changes:

4. **Default Parameters > Temperature unit:** Celsius(C°)
5. **Default Parameters > Minimum/Maximum temperature setpoint:** as specified by your HVAC system.
6. **Temperature Sensor > Broadcast Temperature:** Disabled.

Now open the **Display and Buttons** tab and ensure that **Advanced** properties are enabled, then configure the display settings:

7. Configure **Top > Display type** to Current Area Temperature.
   Select the correct **Logical Area** for the HVAC.

8. (Optional) Configure the middle display to show the HVAC error status:
    a. Set **Middle > Display Type** to Multi-channel level icon.
    b. Set **Minimum channel level** to 0% and **Maximum channel level** to 1%.
    c. Click the **Icons > Change**.button.
    d. Select **Current Configuration** and set **General > Count** to 2.
    e. Change each icon to an appropriate indicator (you can use custom icons if desired):
        - **Item 1- Icon:** No Error
        - **Item 2- Icon:** Error
    f. Click **OK** to continue.
    g. Set **Middle > Logical Area** to the correct area for the HVAC.
    h. Set **Middle > Channel** to the HVAC error status channel (channel 105).
9. Set **Bottom > Display type** to Temperature setpoint.
   Select the correct **Logical Area** for the HVAC.

Configure buttons with the desired/available functions for your HVAC system:

10. This example shows the steps to configure a fan speed control button:
    a. Select **Function:** Task and **Sub function:** Task local.
    b. Select **Control type:** Start task.
    c. Select **Task:** Fan [3].
    d. Select **Display type:** Multi-channel level icon.
    e. Set **Minimum channel level** and **Maximum channel level** to the lowest and highest available fan settings.
       (See **Supported CoolMaster Actions** at the start of this topic.)
    f. Click the **Icons > Change** button to open the Antumbra Icon Library.
    g. Select **Current Configuration** and set **General > Count** to the number of fan speed options.
    h. Change each icon to an appropriate indicator (you can use custom icons if desired).
       Ensure that the icons match each fan setting.
    i. After choosing the icons, click **OK** to close the window.
    j. Set **Logical Address > Logical Area** AND **Display > Logical Area** to the correct area for the HVAC.
    k. Set the **Logical Address > Channel** AND **Display > Channel** to the fan speed channel.
       (See **Supported CoolMaster Actions** at the start of this topic.)
    l. Set **Display > Join** to FE (this is the join value for all CoolMaster task messages).
11. Repeat Step 10 for the **Indoor Unit On/Off** and **Change Mode** tasks if required.
    (See **Supported CoolMaster Actions** at the start of this topic for channel numbers and level settings.)

12. For a Filter Status button/indicator:
    a. Set the **Function** and **Sub function** to Channel level.
    b. Set **Channel Level (%)** to 0%. This allows the button to reset “Filter requires replacement” status.
    c. Set **Display Type** to Multi-channel level icon.
    d. Set **Minimum channel level** to 0% and **Maximum channel level** to 1%.
    e. Click the **Icons > Change**.button.
    f. Select **Current Configuration** and set General > Count to 2.
    g. Change each icon to an appropriate indicator (you can use custom icons if desired):
        - **Item 1- Icon:** Filter OK
        - **Item 2- Icon:** Filter requires replacement.
    h. Click **OK** to continue.
    i. Set **Logical Address > Logical Area** AND **Display > Logical Area** to the correct area for the HVAC.
    j. Set the **Logical Address > Channel** AND **Display > Channel** to the fan speed channel. (See **Supported CoolMaster Actions** at the start of this topic.)
13. For temperature setpoint control:
    a. Configure two buttons with:
        - **Function:** Temperature setpoint
        - **Sub function:** Increment temperature setpoint / Decrement temperature setpoint
        - **Step:** 1.0°C
        - Appropriate temperature up/down icons from the Antumbra Icon Library.
        - **Logical Address > Logical Area** set to the correct area for the HVAC.

Open the **Proximity Sensor** tab and configure the Antumbra to update the onscreen HVAC status information when a user approaches:

14. Select **Function > Target detected actions** and click the button.
15. Click **New > DyNet1 Logical Smart Send** and configure:
    a. **Opcode:** 83
    b. **Data1:** 0x00
    c. **Data2:** 17
    d. **Data3:** 0x00
16. Click **OK**.

Click **Save To Device** to load your changes to the AntumbraDisplay, then test and modify as required.

For more information on configuring the AntumbraDisplay, refer to the **User Interfaces Commissioning Guide**.

3.3 DyNet Text

DyNet Text is a text-based protocol that sends commands to, and receives status responses from, the control network. It is translated to DyNet 1 and DyNet 2 by the EG (dependent on port settings). DyNet Text can be sent over a serial RS-485 connection or a TCP connection made by a Telnet client.

Issues to consider:

- Presently, DyNet Text does not have an EEPROM section. This means that settings cannot be saved between sessions.
- DyNet 1 uses separate time and date messages. DyNet 2 uses a combined time and date message.
- Commands that have device codes and box numbers as arguments must either have both or neither. You cannot supply a device code without a box number.

3.3.1 Syntax

DyNet Text commands are a single keyword command that is followed by a number of arguments. Commands and arguments are not case sensitive.

Example: Preset 1 2 5000 (Area 2 fade to preset 1 over 5 seconds)

Most commands have a brief version.

Example: P 1 2 5000

DyNet Text over RS-485 requires an asterisk as a synchronization character. This character is allowed when using Telnet, however, it is not required when using Telnet.

Example: *P 1 2 5000

Arguments are separated by any number of spaces and/or a single comma.

Example: P 1, 2, 5000

Integer arguments can be written as decimal values or hexadecimal values preceded by "0x". Temperature values can be written with or without a decimal point and have two decimal values of precision.

Example: P 1, 2, 0x1388 (Area 2 fade to preset 1 over 5 seconds)

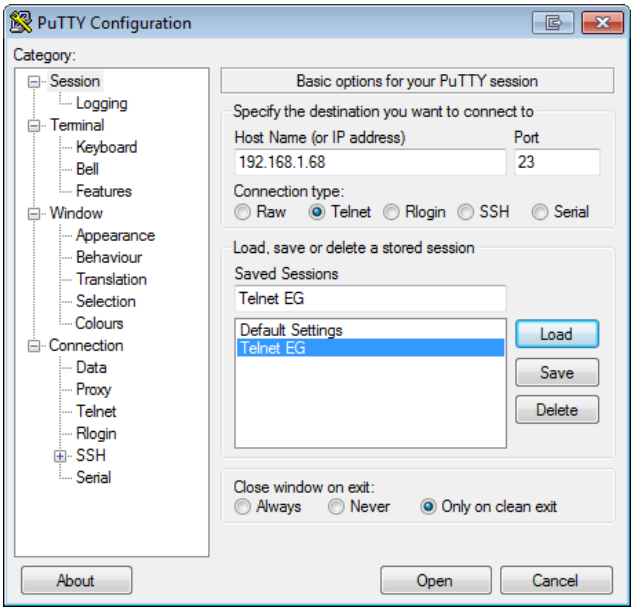
Whenever a command uses an Area, Fade time, Join or Channel Level then that value becomes the new default value for that argument type. There are two edge cases to this rule: the AreaMinMax command does not set the default value for Areas; and the JoinLevel command sets the default Join value to its third argument.

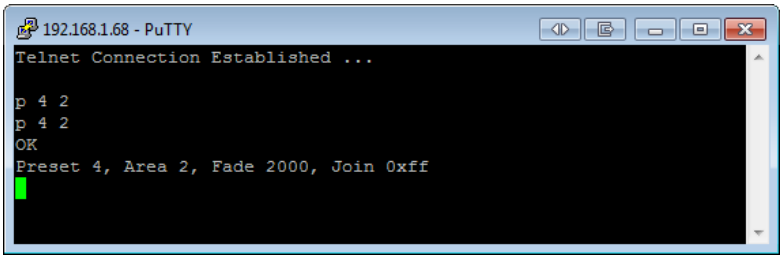
3.3.2 Telnet access

You can communicate over Telnet from your PC using a serial terminal program such as HyperTerminal or PuTTY (shown).

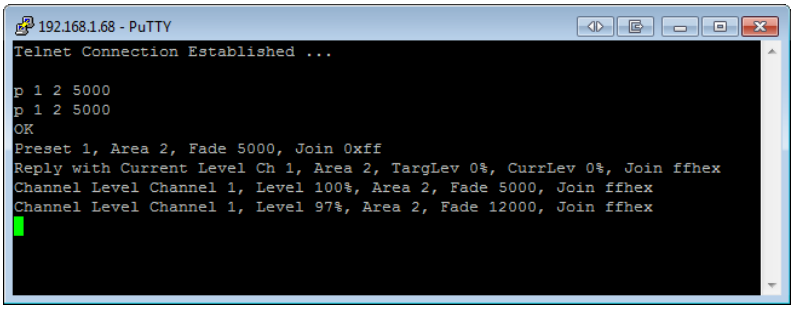
Setup DyNet Text communication from your PC:

1. Connect your PC to the lighting control network via Ethernet or Wi-Fi.
2. Open PuTTY.
3. Enter the EG IP address.
4. Select the Telnet connection type. (To save the Session settings; enter a Saved Sessions name and click the Save button).
5. Click the Open button. The command line window opens and displays; Telnet Connection Established...
6. Enter DyNet Text commands. The EG acknowledges by echoing the command and OK.
7. When the command is performed the network sends a reply confirming the action.





The command line window will also show DyNet Text messages for all network activity seen by the EG (light regulation commands shown).



3.3.3 Commands

There are three types of DyNet Text messages:

- **Logical messages**
  DyNet Text Logical messages act on logical areas. They translate to DyNet 1 and 2 logical messages.
- **Physical messages**
  DyNet Text Physical messages act on devices. They translate to DyNet 1 and 2 physical messages.
- **Configuration messages**
  DyNet Text Configuration messages act on the DyNet Text engine. They configure settings and default values for arguments. They do not translate into DyNet 1 or 2 messages.

The command tables give the long and short commands as well as the arguments they require. If an argument is bold, then it is required. The following table is the argument legend for the command tables.

Message arguments table

Argument	Explanation	Units/Format	Min	Max	Notes
P	Preset Number	16 bit Integer	0	65279	DyNet 2 allows some hard-coded presets above the maximum such as panic mode.
A	Area	16 bit Integer	0	65535	EG uses 2 byte areas. Area 0 is "All Areas".
F	Fade Time	milliseconds	0	83885.91	Fade time resolution is in milliseconds (ms) (10ms step size).
J	Join Level	8 bit Integer	0x00	0xFF	
Ch	Channel Number	16 bit Integer	0	65535	Channel 0 is "All Channels".
CL	Channel Level	Percentage	0	100	
PO	Preset Offset	16 bit Integer	0	65279	
Tmp	Temperature	°C	-127.99	127.99	EG Temperature resolution is in 0.01°C steps.
DC	Device Code	8 bit Integer	0x00	0xFF	0xAA is "Any Device"
BN	Box Number	16 bit Integer	0x0000	0xFFFF	EG uses 2 bytes box numbers. 0x5555 is "Any Box Number".
TN	Task Number	8 bit Integer	0	255	
EN	Event Number	16 bit Integer	0	65535	
H	Hours	0..23	0	23	
M	Minutes	0..59	0	59	
S	Seconds	0..59	0	59	
DoW	Day of the Week	Three letters			Either: "Sun", "Mon", "Tue", "Wed", "Thu", "Fri" or "Sat"
Day	Day of the Month	1..31	1	31	
Mon	Month	Three letters			Either: "Jan", "Feb", ... , "Dec"
Yr	Year	00-99 or 2000-2099	0	99	EG supports both 0..99 and 2000..2099
TF	True or False	0 or 1 only	0	1	

Logical messages table

Command	Brief	Description	Arguments				
Preset	P	Set Preset Message	**P**	A	F	J	
RequestCurrentPreset	RCP	Request Current Preset	A	J			
ChannelLevel	CL	Fade to Channel Level	**Ch**	**CL**	A	F	J
RampLevel	RL	Ramp to Channel Level	**Ch**	**CL**	A	F	J
RequestChannelLevel	RCL	Request Current Channel Level	Ch	A	J		
StopFade	SF	Stop Fading in Area	Ch	A	J		
Off	O	Turn Off Area	A	F	J		
Panic		Panic Area	A	F	J		
Unpanic		Un-panic Area	A	F	J		
EnablePanel	SB	Enable a Panel	A	J			
DisablePanel	DP	Disable a Panel	A	J			
PresetOffset	PO	Set Preset Offset	**PO**	A	J		
SavePreset	SP	Push Current Preset	A	J			
RestorePreset	RP	Pop Current Preset	A	F	J		
ResetPreset	RSetP	Reset Area to Last Used Preset	A	F	J		
ProgramCurrentPreset	PCP	Program Current Levels to the Current Preset	A	J			
ProgramPreset	PP	Program Current Levels to a Given Preset	**P**	A	J		
LEDBrightness	LEDBr	Set Indicator LEDs' Active Brightness	**CL**	A	F	J	
RequestLEDBrightness	RLEDBr	Request Indicator LEDs' Active Brightness	A	J			
LEDBacklightBrightness	LEDBlBr	Set Backlight LEDs' Brightness	**CL**	A	F	J	
RequestLEDBacklightBrightness	RLEDBlBr	Request Backlight LEDs' Brightness	A	J			
LCDBrightness	LCDBr	Set Display Brightness	**CL**	A	F	J	
RequestLCDBrightness	RLCDBr	Request Display Brightness	A	J			
SetTemperatureSetpoint	STmpSP	Set Temperature Setpoint	**Tmp**	A	J		
TemperatureSetpoint	TmpSP	Send a Reply Temperature Setpoint Message	**Tmp**	A	J		
RequestTemperatureSetpoint	RTmpSP	Request a Temperature Setpoint	A	J			
Temperature	Tmp	Send a Reply Actual Temperature Message	**Tmp**	A	J		
RequestTemperature	RTmp	Request Actual Temperature	A	J			

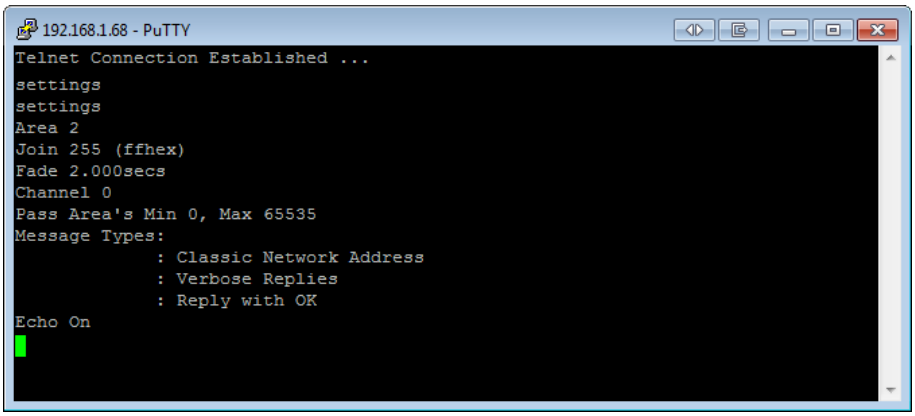
Physical messages table

Command	Brief	Description	Arguments			
Reset		Reset Device	DC	BN		
Version	V	Sign on Device	DC	BN		
StartTask	STT	Start Task Engine Task	**TN**	DC	BN	
StopTask	SPT	Stop Task Engine Task	**TN**	DC	BN	
PauseTask	PT	Pause Task Engine Task	**TN**	DC	BN	
TriggerEvent	TE	Trigger Event Scheduler Event	**EN**	DC	BN	
EnableEvent	EE	Enable Event Scheduler Event	**EN**	DC	BN	
DisableEvent	DE	Disable Event Scheduler Event	**EN**	DC	BN	
RequestTime	RT	Request Current Time	DC	BN		
RequestDate	RD	Request Date	DC	BN		
SetTime	ST	Set Current Time	**H**	**M**	**S**	
SetDate	SD	Set Date	**DoW**	**Day**	**Mon**	**Yr**
SetPhysicalTemperatureSetpoint	SPhyTmpSP	Set Temperature Setpoint	**DC**	**BN**	**Tmp**	
PhysicalTemperatureSetpoint	PhyTmpSP	Send a Reply Temperature Setpoint Message	**DC**	**BN**	**Tmp**	
RequestPhysicalTemperatureSetpoint	RPhyTmpSP	Request a Temperature Setpoint	DC	BN		
PhysicalTemperature	PhyTmp	Send a Reply Actual Temperature Message	**DC**	**BN**	**Tmp**	
RequestPhysicalTemperature	RPhyTmp	Request Actual Temperature	DC	BN		

Configuration messages table

Command	Brief	Description Arguments		
Area	A	Set Default Area	**A**	
A?		Request Default Area	-	
Fade	F	Set Default Fade Time (ms)	**F**	
F?		Request Default Fade Time	-	
Join	J	Set Default Join	**J**	
J?		Request Default Join	-	
Channel	Ch	Set Default Channel	**Ch**	
Ch?		Request Default Channel	-	
AreaMinMax	AMM	Set Maximum and Minimum Areas of Interest	**A**	**A**
AMM?		Request Maximum and Minimum Areas	-	
Brief		Set to Short Display of Reply Messages	-	
Verbose		Set to Long Display of Reply Messages	-	
ReplyOK		Set Whether or not OK is Printed after each Command	**TF**	
Settings		Display Current Settings	-	
WhoAreYou		Ask Gateway Device to Sign on	-	
Echo		Repeat the command back	**TF**	
DottedNetworkAddress	DNA	Use "Device (??hex) Box??" or "??.??" for Physical Properties	**TF**	

Example; EG Settings Message response:



3.3.4 Responses

DyNet Text responses take one of two forms:

- Network responses.
- Configuration responses.

If there is a configuration response, then "OK" is suppressed. The following table is the legend for the response arguments.

Response arguments table

Code	Explanation	Example	Notes
<24h>	24 hour time	02:23:05	
<A4>	Area as 4 char hex	000c	
<Ad>	Area as a decimal. 0 is all areas.	12	
<Bd>	Box number as a decimal.	24	
 	Baud rate as a decimal.	9600	
<C2>	Current Channel Level Percent as 2 char hex	23	
<Ch4>	Channel Number as 4 char hex	0017	
<Chd>	Channel Number as a decimal. 0 is all channels.	2	
<D2>	Device code as 2 char hex	dc	
<D2B2>	"Device (<D2>hex) Box<Bd>" or "<Dd>.<Bd>" depending on "Dotted Network Address" setting.	Device(dchex) Box24	
<Day>	Day of month as decimal	23	
<Dd>	Device code as decimal	220	
<DLS>	Either "Daylight Saving Time" or "Standard Time"	Standard Time	
<DoW>	Three letter day of week	Mon	
<Fd>	Fade time as a decimal in ms (resolution is 10ms)	2000	
<Fs>	Fade time in seconds to 3 decimal places	2.000	
<J2>	Join as 2 char hex	2f	
<Jd>	Join as a decimal	47	
<L%>	Level as percentage	75%	
<L4>	Level as 4 char hex	0044	
<Month>	Three letter month	Mar	
<P#>	Port number as a decimal number	2	Typically, Port 1 is RS-485 and Port 2 is Ethernet (inc. Telnet)
<P4>	Preset as 4 char hex	0022	
<Pd>	Preset as decimal	34	
<T2>	Target Channel Level Percent as 2 char hex	64	100% → 0x64
<Tmp4>	Temperature rounded down as 4 char hex	45	69.25°C → 0x45
<TmpF>	Temperature as a floating point number with 2 decimal places	69.25	
<V>	Version number	v3,02	Note that commas are used, not decimal points.
<Year>	Year as decimal	2015	

Network responses

In the current implementation of DyNet Text, all messages that pass through ports in EG will be checked by the DyNet Text engine. However, not all DyNet messages are understood by the DyNet Text engine. Included messages will be printed to the Telnet console or if not included in DyNet Text, they will be ignored.

Reply Type	Verbose Reply	Brief Reply
Preset	Reply with Current Preset <Pd>, Area <Ad>, Join <J2>hex	RCP <P4>,<A4>,<J2>
Channel Level	Reply with Channel Level Ch <Chd>, Area <Ad>, TargLev <L%>, CurrLev <L%>, Join <J2>hex	RCL <Ch4>,<A4>,<T2>,<C2>,<J2>
Indicator LED Active Brightness	Reply with LED Brightness <L%>, Area <Ad>, Join <J2>hex	RPLEDBR <Br4>,<A4>,<J2>
Backlight LED Brightness	Reply with LED Backlight Brightness <L%>, Area <Ad>, Join <J2>hex	RPLEDBLBR <Br4>,<A4>,<J2>
LCD Brightness	Reply with LCD Brightness <L%>, Area <Ad>, Join <J2>hex	LCDBR <Br4>,<A4>,<J2>
Temperature Setpoint (Logical)	Reply with Temperature Setpoint <TmpF>, Area <Ad>, Join <J2>hex	TMPSP <Tmp4>,<A4>,<J2>
Temperature (Logical)	Reply with Temperature <TmpF>, Area <Ad>, Join <J2>hex	TMP <Tmp4>,<A4>,<J2>
Temperature Setpoint (Physical)	Reply with Temperature Set Point <D2B2>, <TmpF>	PHYTMPSP <D2B2>,<Tmp4>
Temperature (Physical)	Reply with Temperature <D2B2>, <TmpF>	PHYTMP <D2B2>,<Tmp4>
Version	Signon (Port <P#>) <D2B2>, <V>	
Time	Time <24hr> <DLS>	
Date	Date <DoW> <Day> <Month> <Year>	
Time and Date	Time <24hr> <DLS>, Date <DoW> <Day> <Month> <Year>	DyNet 2 can send a "Time and Date" reply.

Network responses

Configuration responses are responses to queries of the DyNet Text engine itself.

Command	Reply
A?	A=<Ad>
F?	F=<Fd>
J?	J=<Jd>
Ch?	Ch=<Chd>
AMM?	AMin=<Ad>, AMax=<Ad>
WhoAreYou	I am EG (dchex) Box <Bd>, <V>
Version	Signon (Port <P#>) EG(dchex), Box <Bd>, <V>
RequestTime	Time <24hr> <DLS>
RequestDate	Date <DoW> <Day> <Month> <Year>
Settings	Refer to page 27 example: EG Settings Message response.

3.4 Integration alternatives

A selection of DyNet messages are openly available for use by third-party vendors to transfer information to and from the DyNet network. If the third party has an RS-485 port, this can be directly connected to the DyNet network, although it is recommended that direct connection is only performed on small networks. On larger networks, the recommended connection method is via a Dynalite network gateway, which provides optical isolation and message filtering between the two networks.

Where this method is commonly used:

- AV systems that have RS-485 or RS-232 capability and built in DyNet compatibility, such as AMX & Crestron.
- High level interface where a third party desires master control of parts of or the whole lighting system.
- Status feedback for the lighting system.
- Notification of alarm conditions, such as circuit breaker trips, load current monitoring.

Dynalite provides gateways for several methods of protocol converters that will translate DyNet into other protocols, in some cases this conversion can be bi-directional. Some of the available options include:

- DyNet to Somfy/Somfy to DyNet.
- DyNet to KNX/KNX to DyNet.
- DyNet to DMX512/DMX512 to DyNet.
- DyNet to ACT Protocol.
- DyNet to Custom strings over RS-232.

One technique is to use a Dynalite RS-232 Gateway, that can transmit custom packets. The basic idea is to write a script with several Tasks. Each Task contains a custom string that is transmitted out of the RS-232 port when the Task is executed. Expanding upon this concept, it is then possible to use the Start() statement at the top of the Task that will cause the Task to listen to the DyNet network for a particular message, i.e.: a Preset message in a particular Area, and then send the custom string out of the RS-232 port when the correct Preset message is heard. A basic form of this type of control is:

- Smart Panel Preset 1 Area 200 > DNG232 Task1 > VCR "Play" string
- Smart Panel Preset 2 Area 200 > DNG232 Task2 > VCR "Pause" string
- Smart Panel Preset 3 Area 200 > DNG232 Task3 > VCR "Stop" string

4 BACnet Gateway

4.1 Overview

To enable BACnet integration, the PDDEG-S can be configured as a BACnet gateway.
A BACnet gateway provides configurable data points allowing bi-directional communication to Dynalite's powerful distributed network architecture from a BACnet based building management system (BMS).
Only BACnet over Ethernet with a UDP connection is supported.

BACnet point objects

No.	Function	Object type	Data Type	Read/ Write	Point description
1	Total Offline Devices	Job, Floor	Analog	R	*Count of any offline devices for a Job or Floor.
2	Total Driver and Lamp Faults	Job, Floor, Area	Analog	R	Count of any offline drivers or lamps for a Job, Floor or Area.
3	Offline Device Alarm	Job, Floor	Binary	R	*Indicator of any offline devices for a Job or Floor.
4	Driver or Lamp Fault Alarm	Job, Floor, Area	Binary	R	Indicator of any offline drivers or lamps for a Job, Floor or Area.
5	System Manager Offline Device Alarm	SM	Binary	R	*Indicator that System Manager has identified one or more offline devices.
6	System Manager Driver or Lamp Fault Alarm	SM	Binary	R	Indicator that System Manager has identified one or more driver or lamp failures.
7	Preset	Area	Analog	R/W	Read and write the preset number for an Area.
8	Current Temperature	Area	Analog	R	Read the current Temperature (Celsius) for an Area.
9	Temperature Setpoint	Area	Analog	R/W	Read and write the temperature setpoint for an Area.
10	Channel Level	Channel	Analog	R/W	Read and write the level of a single channel within an Area.
11	Driver Status	Driver	Binary	R	Read if a single driver in a fixture is online or offline.
12	Lamp Status	Driver	Binary	R	Read if a single lamp in a fixture is working or not working.
13	Channel Runtime	Driver	Analog	R	Circuit/driver usage in minutes.
14	Device Offline Status	Device	Binary	R	*Read if a single device in the system is online or offline.
15	Light Level (Lux)	Device	Analog	R	*Read the LUX level from a single DyNet Sensor.

*Not currently available for DALI devices (Sensors and Dry Contact Interfaces).

It is not essential to have floor plans in your job to configure BACnet integration.

4.2 Integration Design

The starting point for the integration design is the scope of works. This details integration requirements for electrical, lighting, air conditioning, security, and other systems. The BMS can integrate with these systems by mapping BACnet points to each system.

To integrate the lighting control system with the BMS, you can estimate the number of BACnet points required by identifying the number of devices and areas in the job and the types of points required in each area. Use this information and your BACnet license to calculate the number of PDDEG-S gateways that need to be ordered.

- Please order your BACnet license before sending the license request for the PDDEG-S.
- It is recommended to dedicate a PDDEG-S as a BACnet gateway and configure it as a building supervisor on the trunk (at the top of your device tree in System View). Then it can map all of the applicable messages from sub-devices to BACnet.
- If two separate Ethernet connections are required, you can connect a PDEG to the trunk and the RS-485 bus to the PDDEG-S acting as a BACnet gateway.
- Preset control is sufficient for the majority of lighting control systems integrating with BACnet. Presets allow for the broadest range of control with the least number of points.
- The scope of works must include the maximum number of points. A single BACnet gateway is sufficient for installations with fewer than 10,000 points. Multiple BACnet gateways can be installed and configured when more than 10,000 points are required.

4.3 Connecting to BACnet

To setup the connection to the PDDEG-S, the BACnet client software requires some mandatory information about the PDDEG-S BACnet server. This information is entered into the PDDEG-S Device Properties editor.

Please provide the following information to the BACnet consultant:

Ports editor

IPv4 or IPv6 address
IP address of the gateway.

Device Properties editor

Port
BACnet server port number. Default = 47808.

Network ID
The BACnet network number that the gateway is connected to. Default = 1.

Device ID
The BACnet device number of the gateway.

You must first configure the PDDEG-S with the Bridge Configuration Wizard and ensure that you select the BACnet checkbox in Step 2 of the wizard.

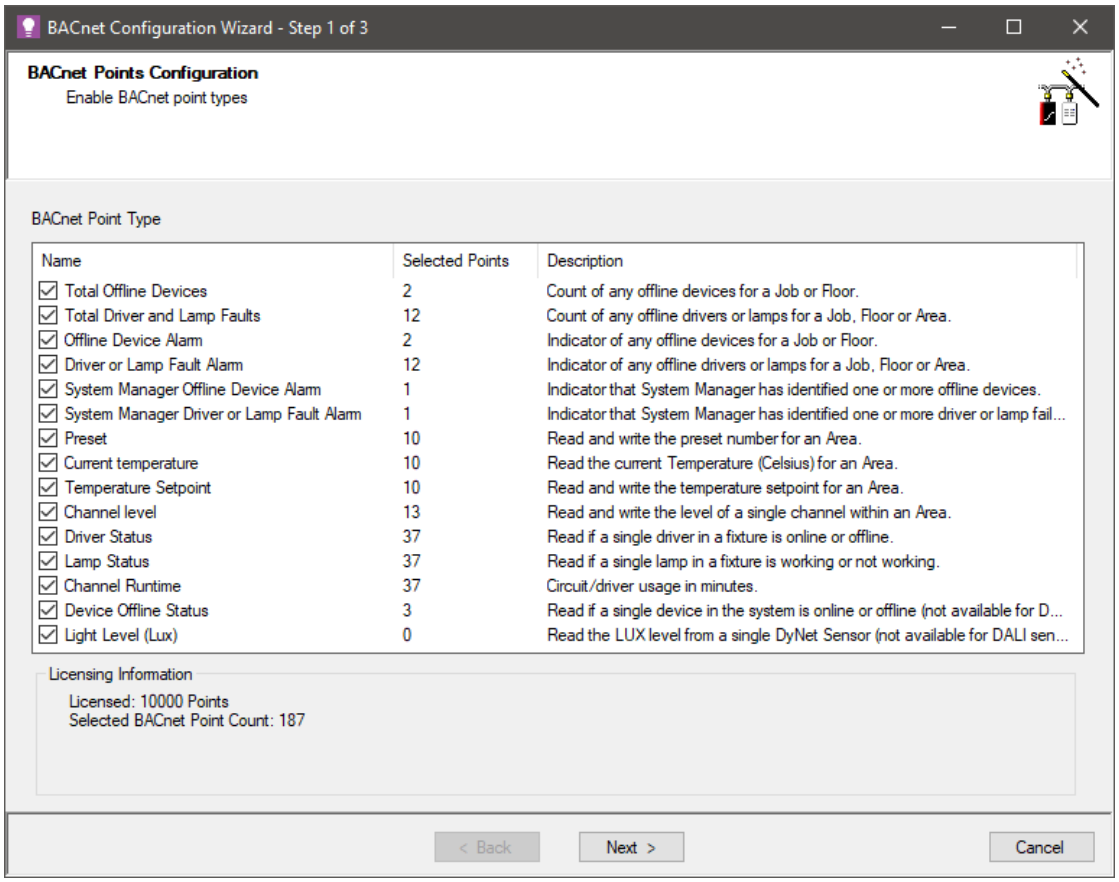
4.4 BACnet Configuration Wizard

The BACnet Configuration Wizard enables you to define and map the BACnet points required for your project. The BACnet client software can then monitor the system from any of the defined point types and can control the system with the following point types:

- Preset
- Channel Level
- Temperature Setpoint.

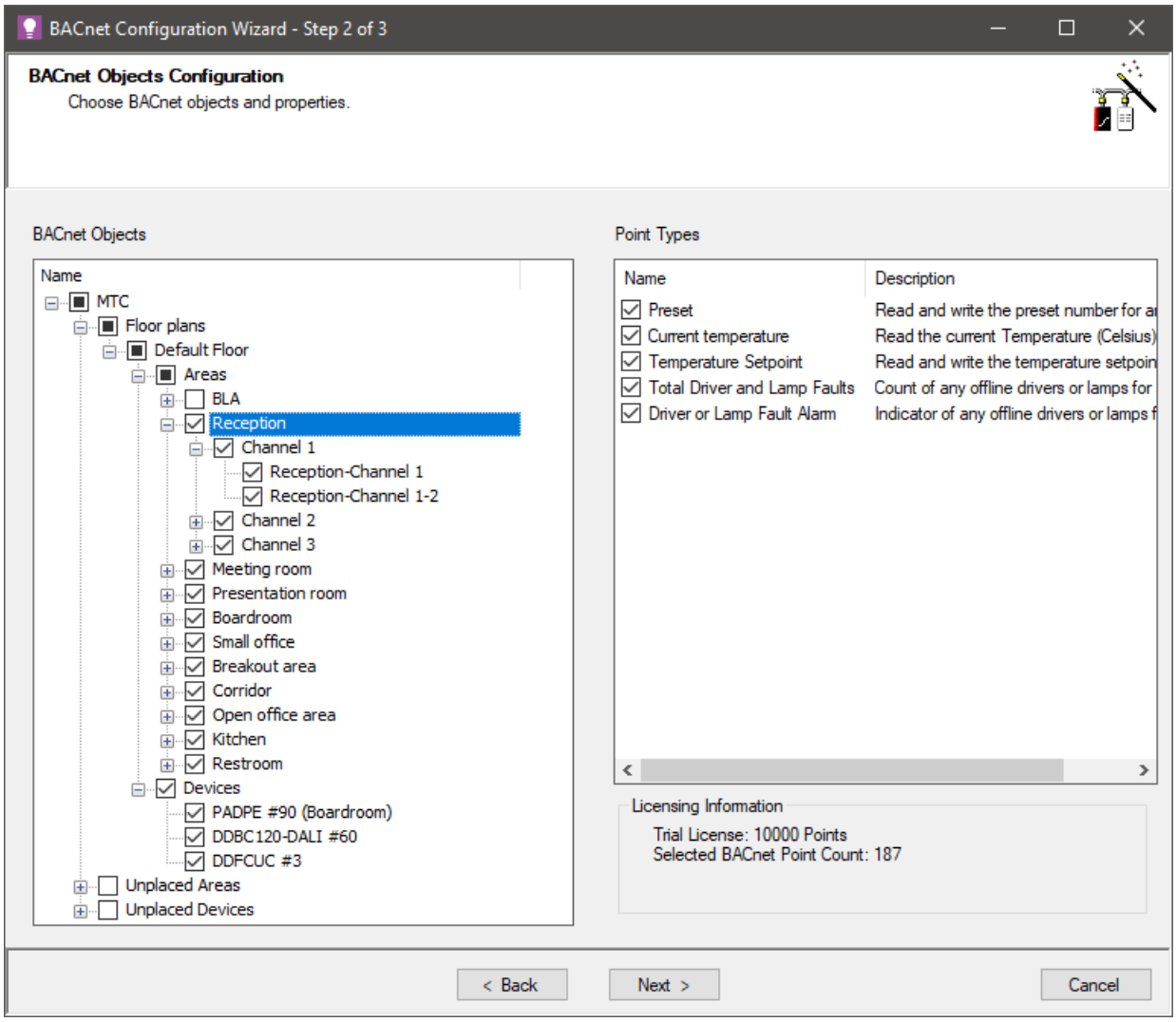
Configure BACnet Gateway:

1. After completing your system configuration, save the job file/database.
2. In System View, right-click the PDDEG-S and select BACnet Configuration to open the wizard. The wizard automatically loads the BACnet points from the areas and devices in your job.
3. Deselect the BACnet Point Types that are not required for BACnet integration and click Next.



To assist you in staying within the maximum number of points allowed for your licence, the Licenced Point Count and Selected BACnet Point Count is shown in the Licensing Information box at the bottom of the window.

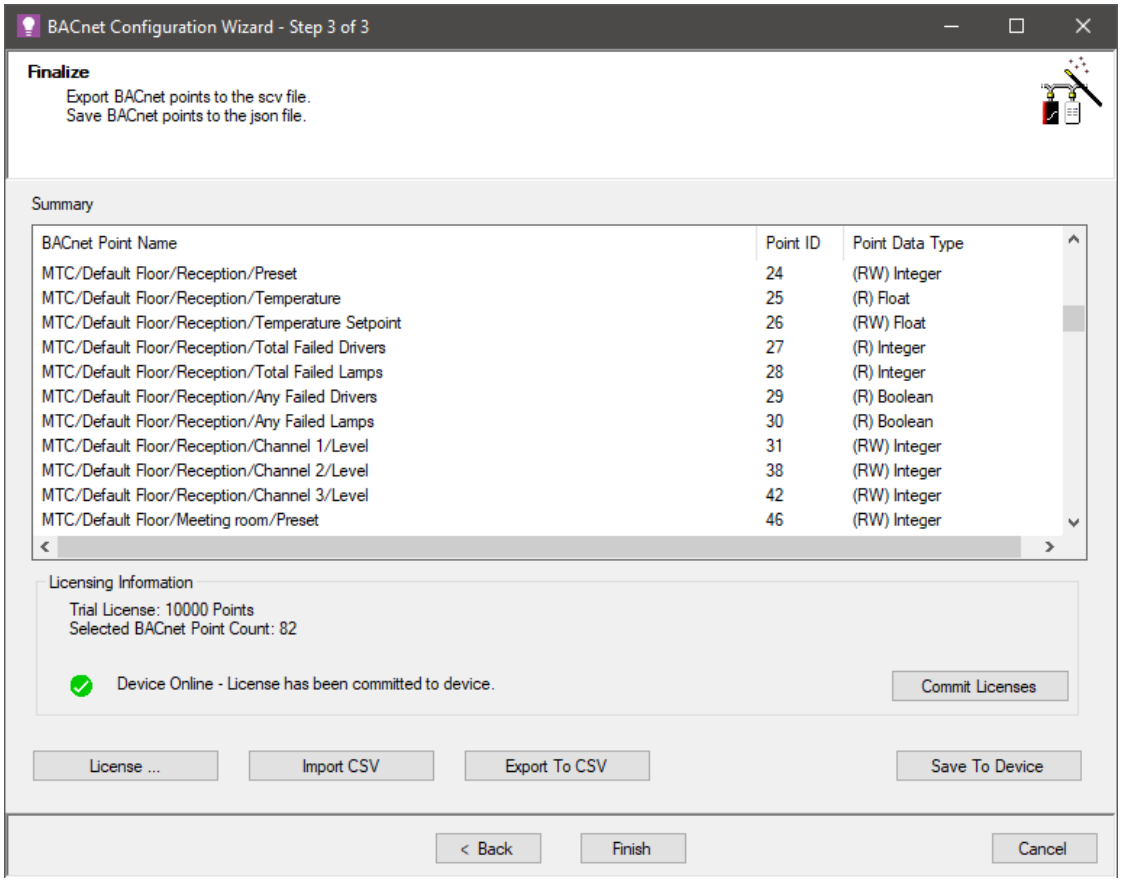
4. In the BACnet Objects window, click the + or - sign to expand and contract the tree.
5. Select or multi-select the BACnet Objects in the tree.
6. In the Point Types section, deselect the point types not required for each area or device and click Next.



The BACnet Configuration Wizard creates a BACnet point name and Point ID for each defined point. The point names are generated according to the order below and the Object Type.

Site name/Floor name/Area name or Device name/Channel name/Driver name/[point type]

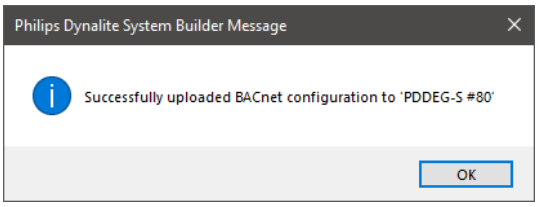
The wizard shows a list of the generated BACnet Point Names, Point IDs, and Point datatypes.



7. Click the Export To CSV button to create a spreadsheet of your BACnet points to give to the BACnet consultant. The BACnet point table must be agreed to and signed off to complete BACnet integration.

   If you want to change the autogenerated BACnet Point names and Point ID numbers, then you can edit them in the CSV file and click the Import CSV button to reload them into the wizard.

8. Click the Save To Device button to upload the json file to the PDDEG-S. SB shows a message when the configuration is successfully uploaded to the device.
9. Click the Finish button to close the wizard.
10. Reboot the gateway for changes to take effect.



To save to device, ensure gateway has an IP address and SB can establish a https connection.

Note, the Save To Device button will be disabled if you have exceeded the point count for your license.

Click the Commit Licenses button, if you already have a BACnet license file but haven't uploaded it, because you didn't have access to the gateway. Refer to the Licensing topic for more information.

Note that the BACnet configuration is saved in the job file and to the device but a "Load from device" will not include the BACnet configuration.

4.5 Licensing

Click the Enable Trial button to start a 28-day trial license. The Enable Trial button is not shown when a license exists. System Builder provides a trial license with a 10,000 point limit for each PDDEG-S. This allows the BACnet server to be fully configured whilst applying for a permanent license.

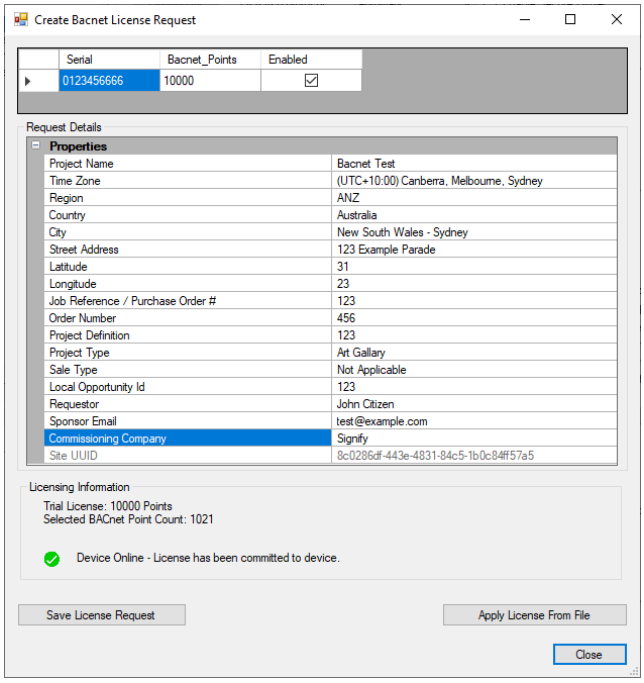
To run the PDDEG-S as a BACnet server after the free-trial period, you must purchase a BACnet license or apply the free of charge 100 point license. Licenses are available with the following number of points.

- 100 (free of charge)
- 1000
- 5000
- 10000

Request BACnet license:

1. Ensure you have the SAP order confirmation number (the order desk needs to submit the PO first).
2. In Step 3 of the wizard, click the License button to create a BACnet license request.
3. Enter the number of points required (suggested BACnet point number is calculated from your configuration) and select the Enabled checkbox for a new license.
4. Enter the property details for the request (mandatory fields are shown in red). Some fields will auto-populate from the job settings. If you have System Manager, you can copy the license request details from System Manager. Refer to https://www.dynalite.com/faq/551.
5. Click the Save License Request button and send the request file to **support.controls@signify.com** so they can match it to the BACnet license purchase order. They will then reply with the signed license file.
6. When you receive the license file, click the Apply license From File button to commit the license to the device. Click to save your job (Ctrl+S).

   If the device is offline, SB shows the following message in the Licensing Information box:
   Device Offline – License not committed to device. The license is saved in the job file, and you can try committing it again when the device is back online.

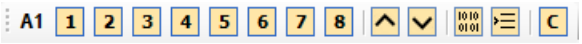


4.6 Test Functionality

The final step before hand over to the BMS contractor is to check that each point is functioning correctly. Using a BACnet client, test each point by:

- Setting a data point value from the BACnet client and monitoring the message in the SB Network Log (writing).
- Setting a data point value from SB and monitoring the corresponding data point value in the BACnet client (reading).

The System Builder Virtual Panel and DyNet Packet Sender enables you to send out the DyNet messages that (if mapped to BACnet) are read by the BACnet client (Click C or press Alt + F9 to ensure the virtual panel is configured to the area selected in the Areas View).



Refer to www.dynalite.com > Network Devices > PDDEG-S > BACnet on PDDEG-S Testing Application Note.

5 Philips Web Interface

The EG has an inbuilt web server to interface to the system. The interface provides system status monitoring, lighting control, activity scheduling, schedule editing and language selection.

The Philips Web Interface configuration relies on the PROJECT.XML file being uploaded to the EG.
Refer to Section 2.3 Ethernet Access Point.

To access the EG, ensure you have configured the EG and saved to device. Then you can enter the EG's IP address into your browser (ensure that the computer is on the same subnet as the EG).

<IP address of your EG>/Index.htm

Username and Password.

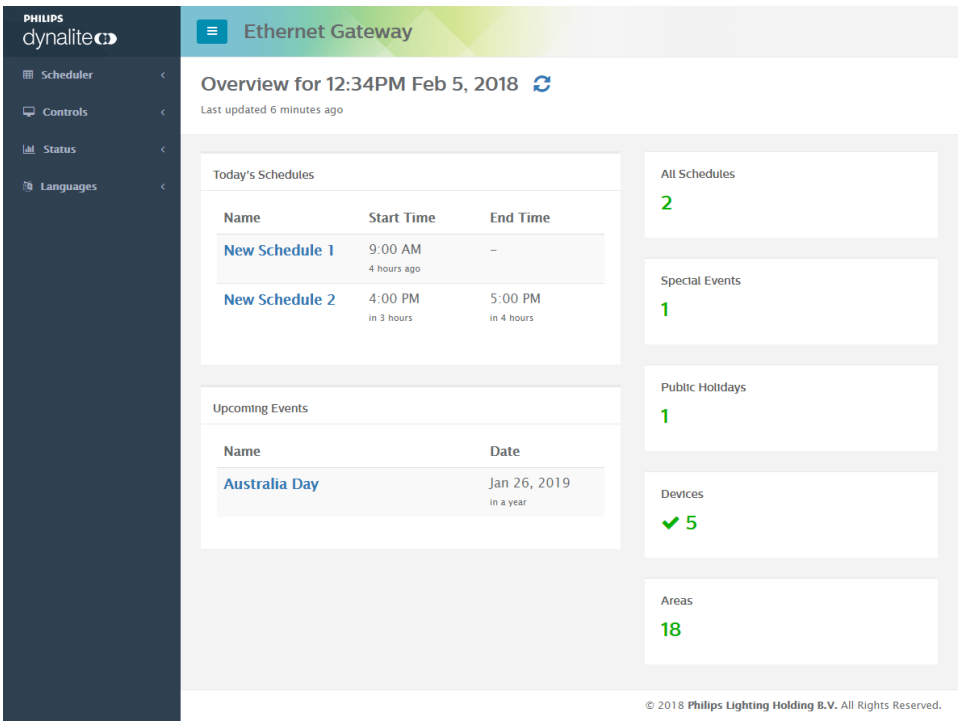
Default IP settings:

IPv4	Enabled
Fixed IP address	True
IP address	192.168.1.<box number>
Subnet mask	255.255.255.0
Default gateway	192.168.1.1
DNS server 1	192.168.1.1

- Screens are indicative only as web interface features may change between configurations and versions.
- For HTTPS connections, first upload a TLS certificate from SB to the EG. For more information, refer to topic 2.3.5 HTTPS Secure Access.
- For a self-signed certificate, you need to accept the certificate in the browser upon first connection to the EG. This effectively pins the browser on the device to the EG. All subsequent requests will then also be trusted by the browser. This is an issue for all devices that connect to a service on a field device (like the PDDEG-S or PDEG) and is caused by the fact that browsers do not trust certificates that are self-signed or from a private certificate chain.

5.1 Ethernet Gateway Overview

The home page provides a snapshot of the system showing today's schedules and upcoming events as well as the total number of schedules, special events, public holidays, devices and areas in the system.



5.2 Scheduler

The EG real time clock enables stored schedules to be run from within the gateway. Schedules can be based on time or relative to sunrise/sunset. They are defined as simple events or timed events. The gateway executes a series of actions at the start, end and (for timed events) periodically while the schedule is running.

Refer to Property Editors – Schedules, for more information on creating schedules.

If you have System Manager (SM) it is simpler to create your schedules in SM which can be pushed down to the EG. Otherwise, schedules created/modified using the web interface or in SB must first be synchronized within SM to be visible.

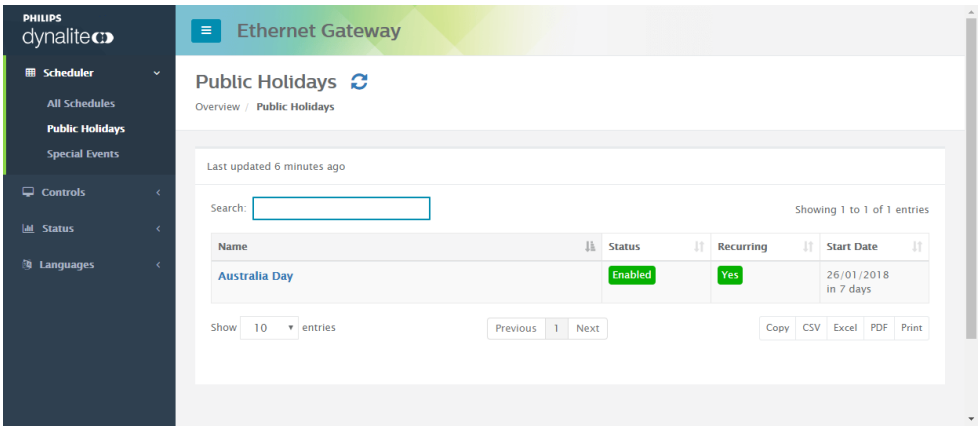
Although, you cannot create new items such as schedules, special events or public holidays from the browser window, you can modify existing items that were created in System Builder or System Manager.

5.2.1 All Schedules

The Scheduler page provides an overview of the schedules stored in the EG. Click the schedule name to edit each schedule. Refer to Schedule Editor for more information.

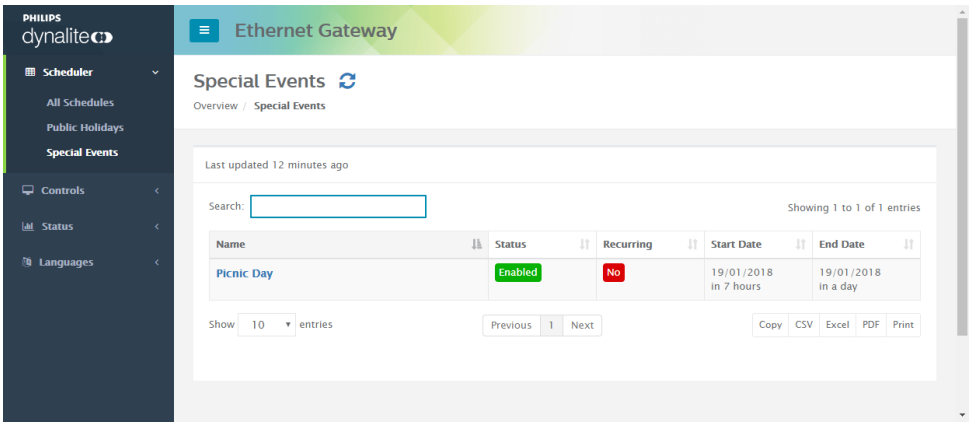
5.2.2 Public Holidays

The Public Holidays page shows a list view of saved public holidays. Click the name to edit the properties.



5.2.3 Special Events

The Special Events page shows a list view of saved Special Events days. Click the name to edit the properties.

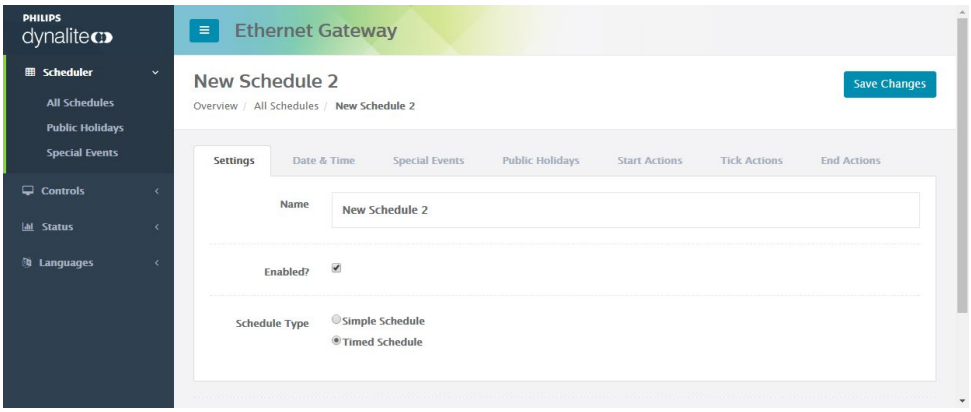


5.3 Schedule Editor

5.3.1 Edit Schedule

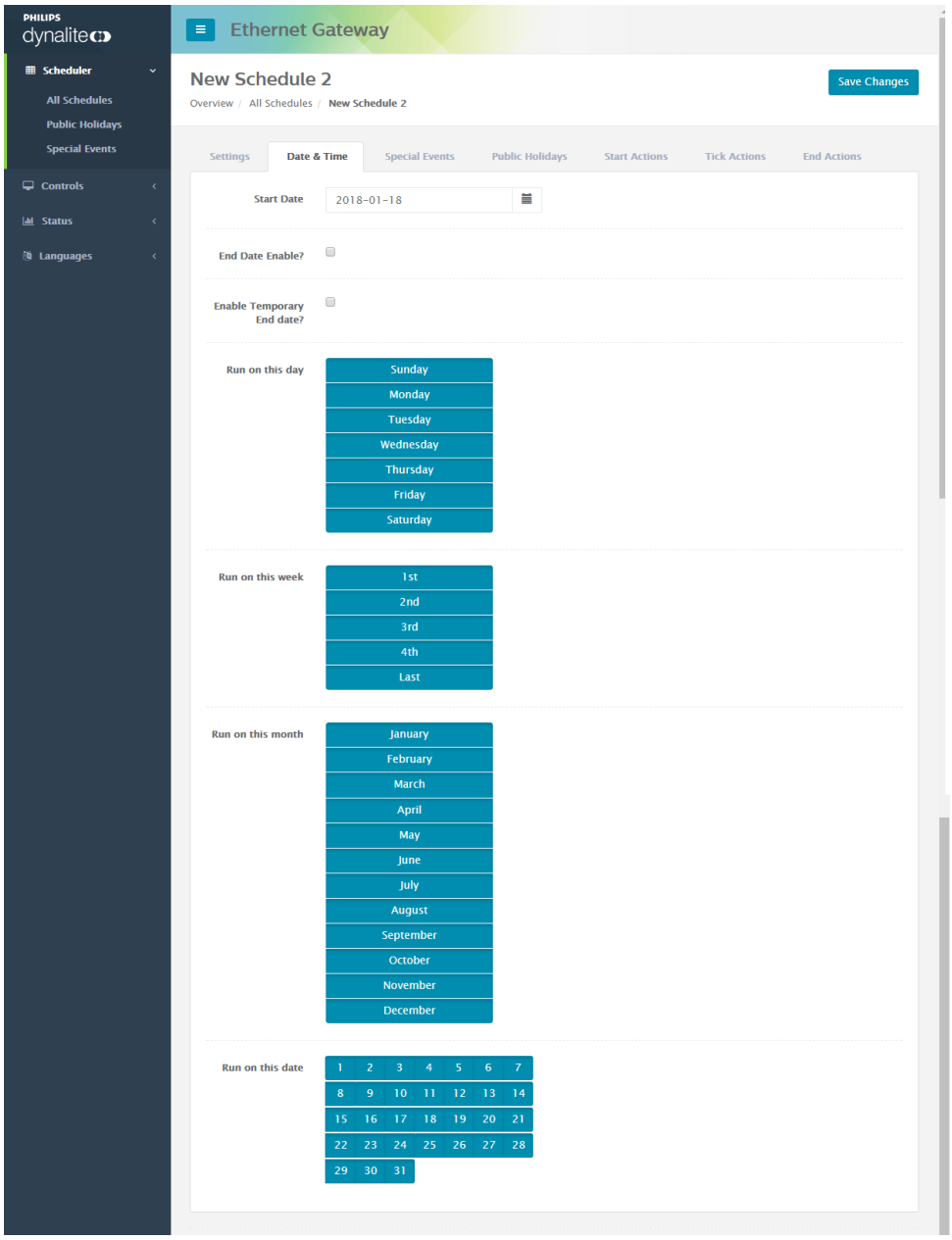
Settings

The Schedule Editor allows you to edit the properties of the schedule and add the Start, Tick and End actions.



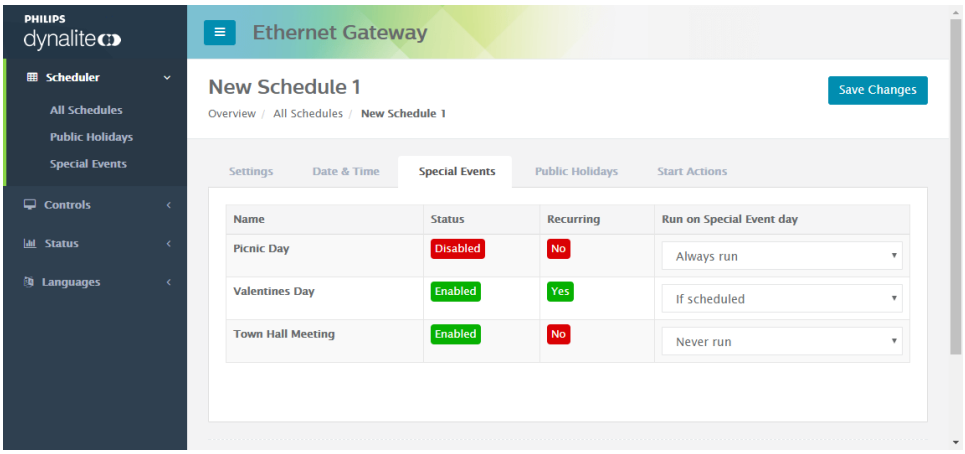
Date & Time

The Date & Time page enables you to set when the schedule will run.



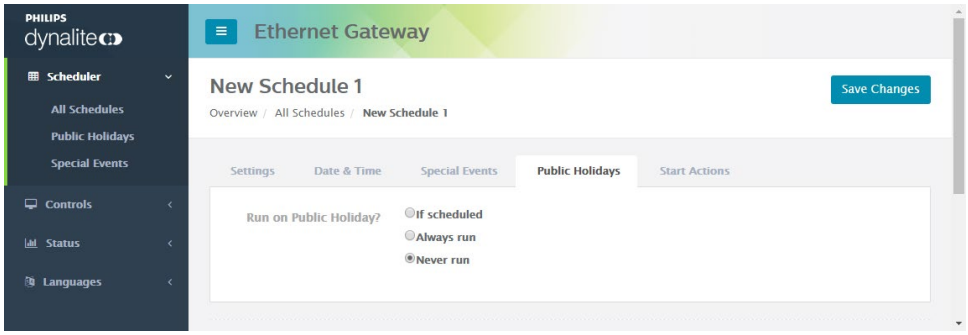
Special Events

The Special Events page enables you to set the schedule to run on special event days.



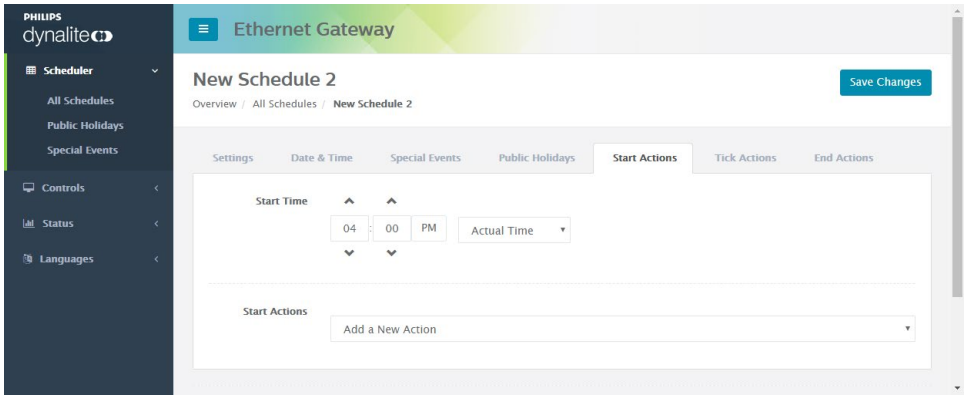
Public Holidays

The Public Holidays page enables you to set the schedule to run on public holidays.



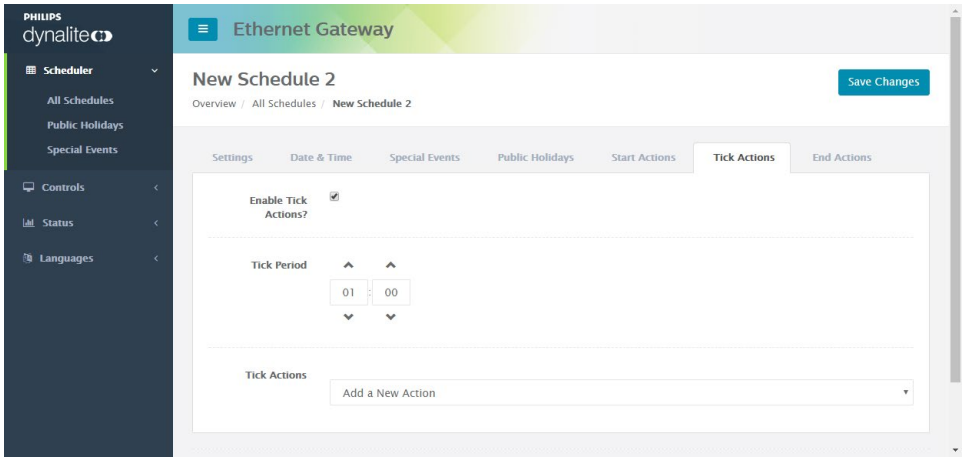
Start Actions

The Start Actions page enables you to set the actions that will occur at the schedule's start time.



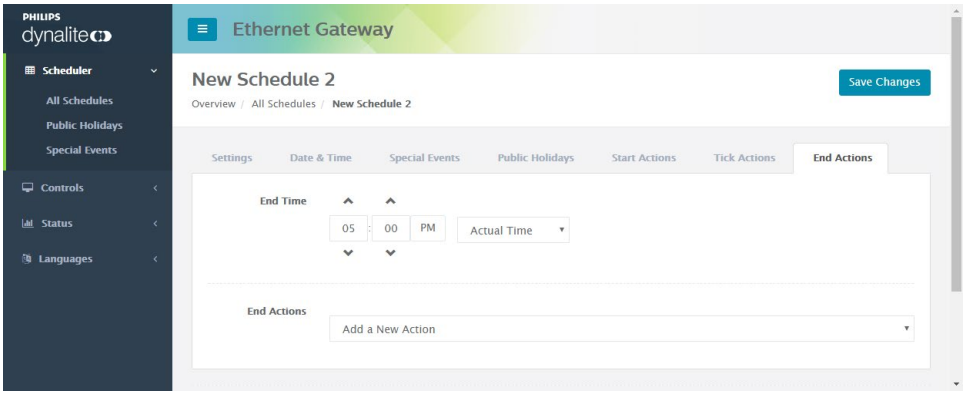
Tick Actions

The Tick Actions page enables you to set the actions that will occur periodically between the start and end of the schedule.



End Actions

The End Actions page enables you to set the actions that will occur at the schedule's End time.



5.3.2 Add Actions

You can add any combination of actions to your schedule. When selecting Start, Tick or End actions, you can select from the following actions and edit the action properties:

- Preset
- Activate Panic
- Reset Panic
- Reset Preset
- Set Preset Offset
- Channel Level
- Colour Temperature Channel Level
- Temperature Setpoint
- Disable Motion Control
- Enable Motion Control
- Disable PE Control
- Enable PE Control
- Disable Area Cascading
- Enable Area Cascading
- Set Area Link
- Clear Area Link
- Set Join Level
- Disable Panel
- Enable Panel
- Sensor Timeout Control
- Start Local Task
- Pause Local Task
- End Local Task
- Delay

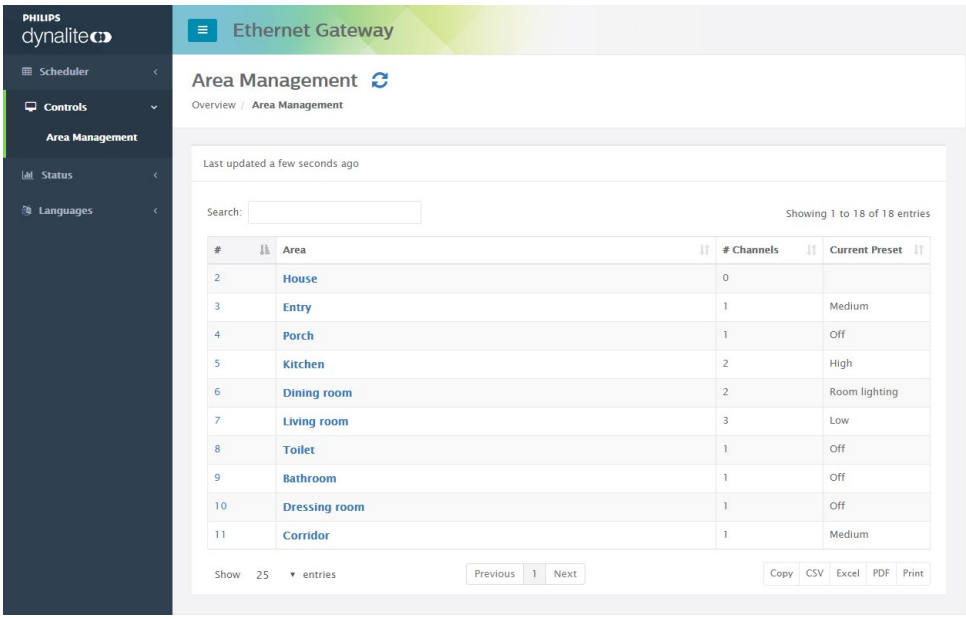
5.4 Controls

The Controls section allow the user to perform:

- Scene control
- Channel control
- Updates to channel levels for preset scenes.

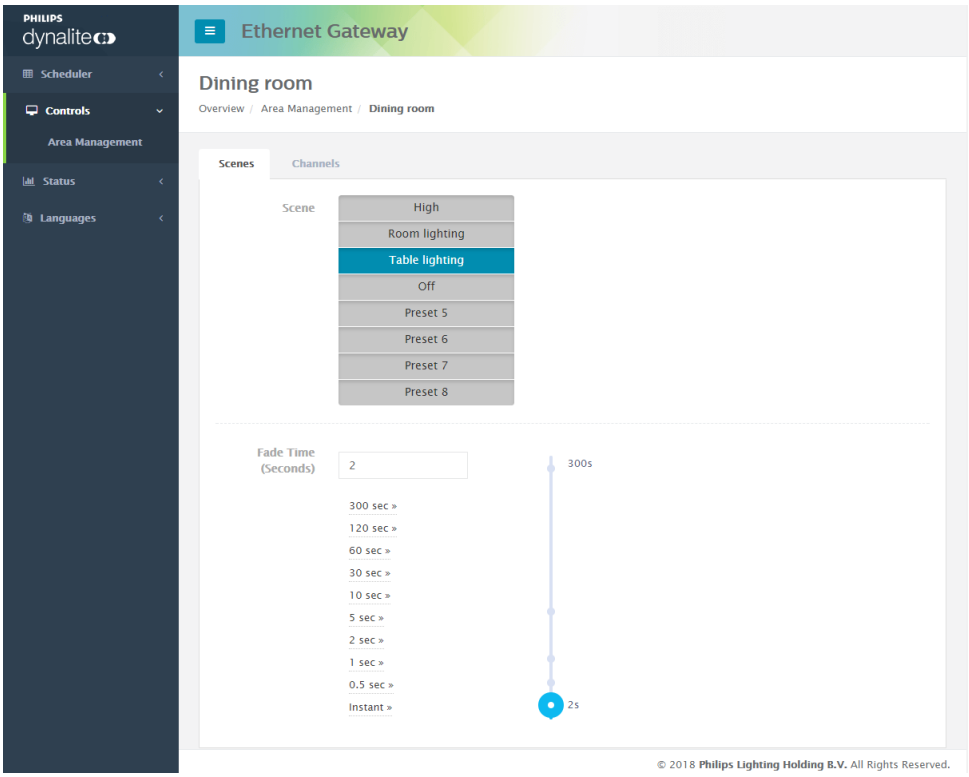
5.4.1 Area Management

This page lists the areas in the system, number of channels in each area and available preset scenes in each area. Click the area name to control the functions in the area.



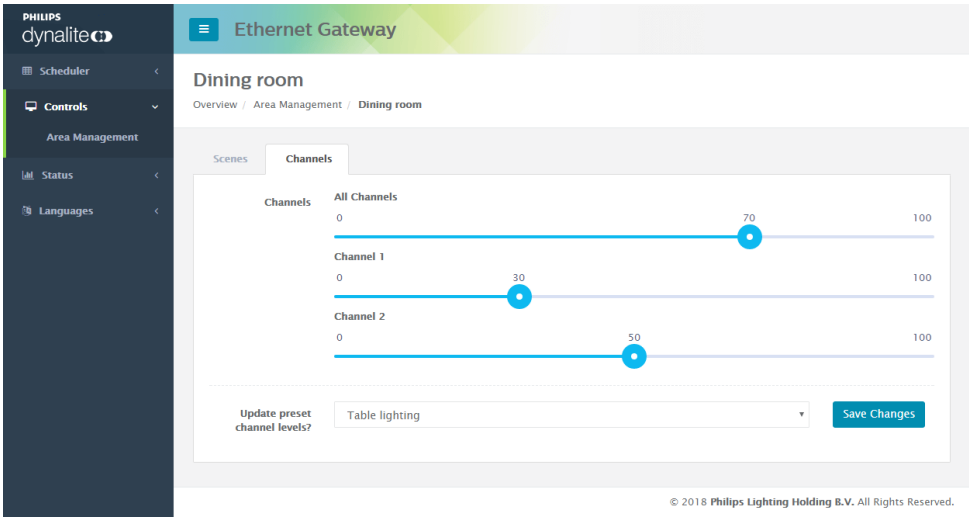
Scenes

This page enables recall of preset scenes using the specified fade time.



Channels

This page enables real-time control of channels in the selected area. You can also select a preset and save the modified channel levels to the preset.



5.5 Status

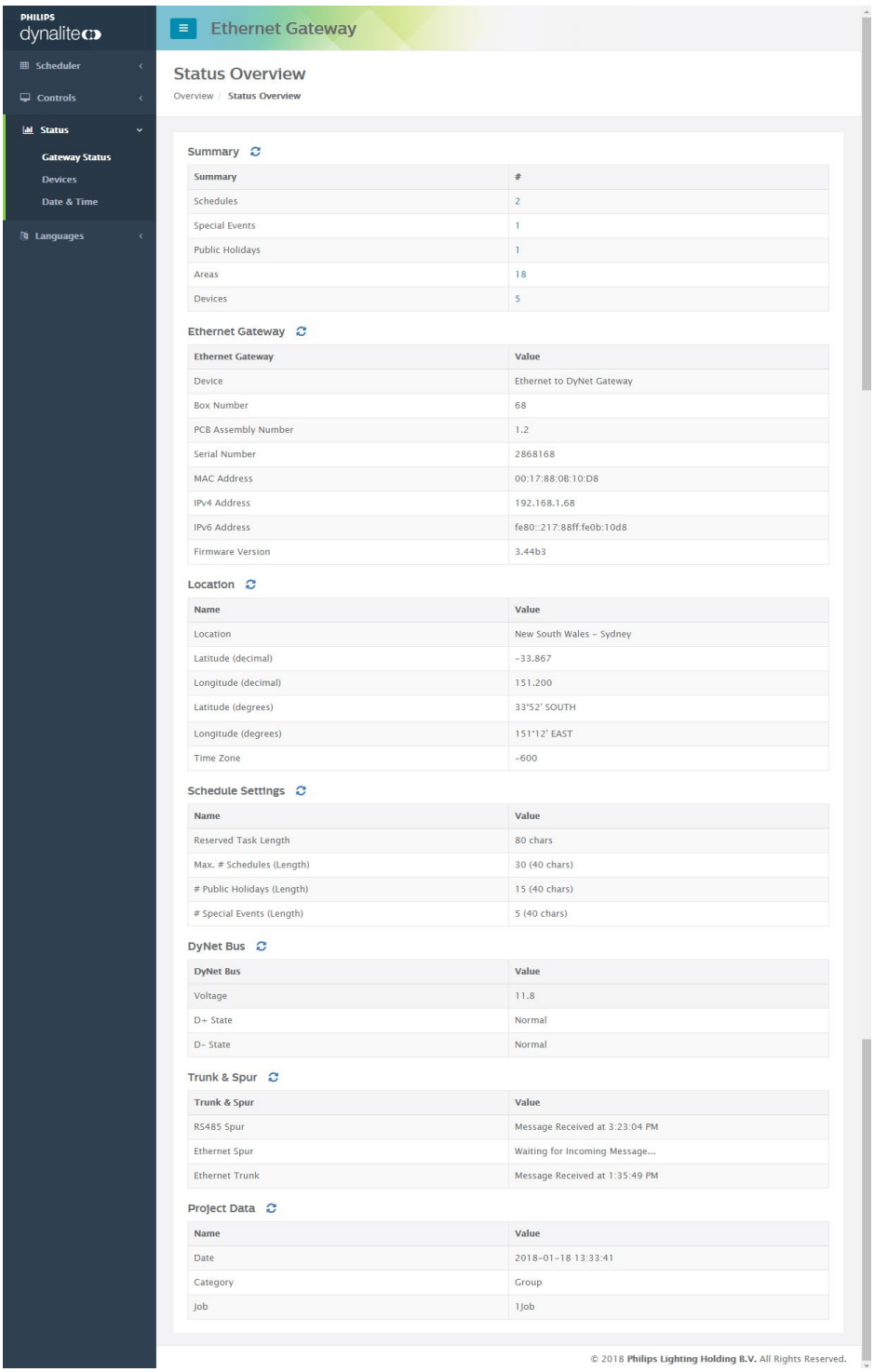
The following status pages are available:

- Gateway Status
- Devices
- Date & time

5.5.1 Status Overview

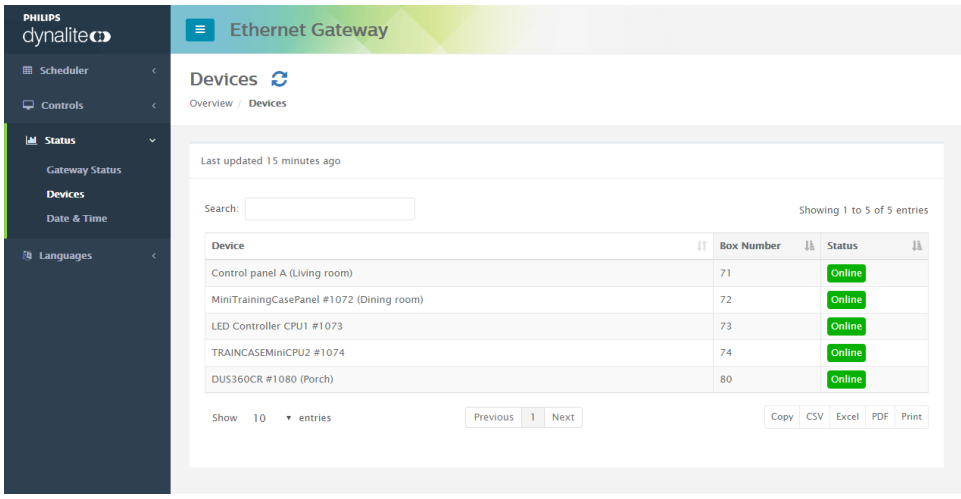
The following status information is provided:

- Summary
- Ethernet Gateway
- Location
- Schedule Settings
- DyNet Bus
- Trunk and Spur
- Project data



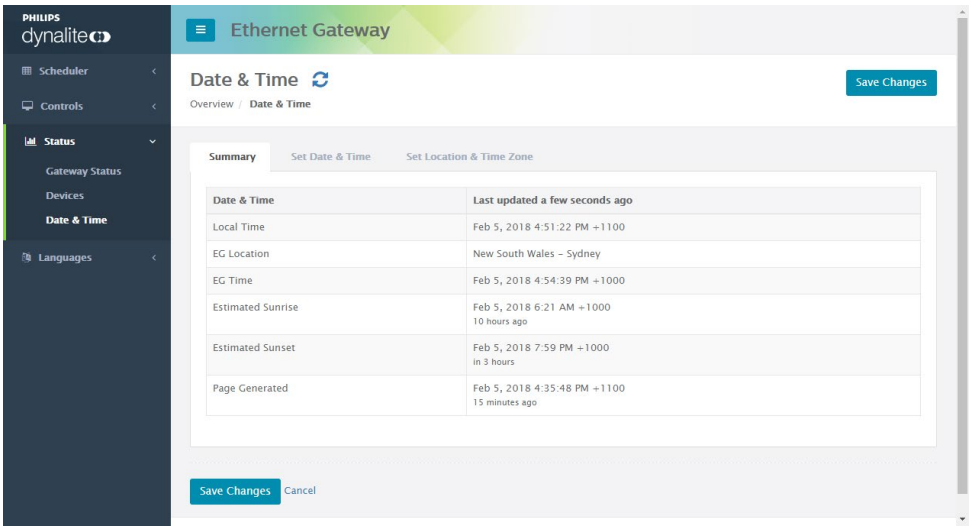
5.5.2 Devices

This page Shows the online/offline status of the devices connected on the spur.



5.5.3 Date & Time

The page shows the local time, EG location, EG time and estimated sunrise and sunset information.

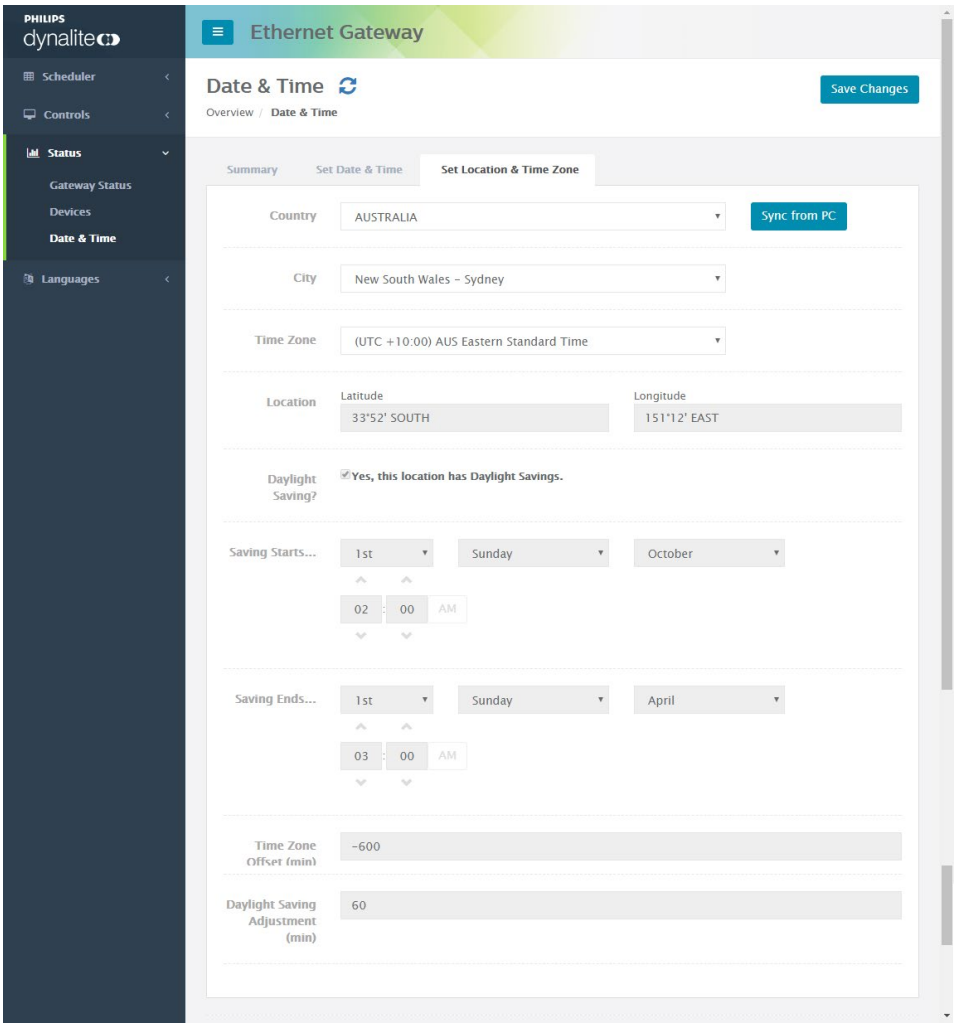


Set Date & Time

This page enables you to set the date and time or synchronize it with your PC.

Set Location & Time Zone

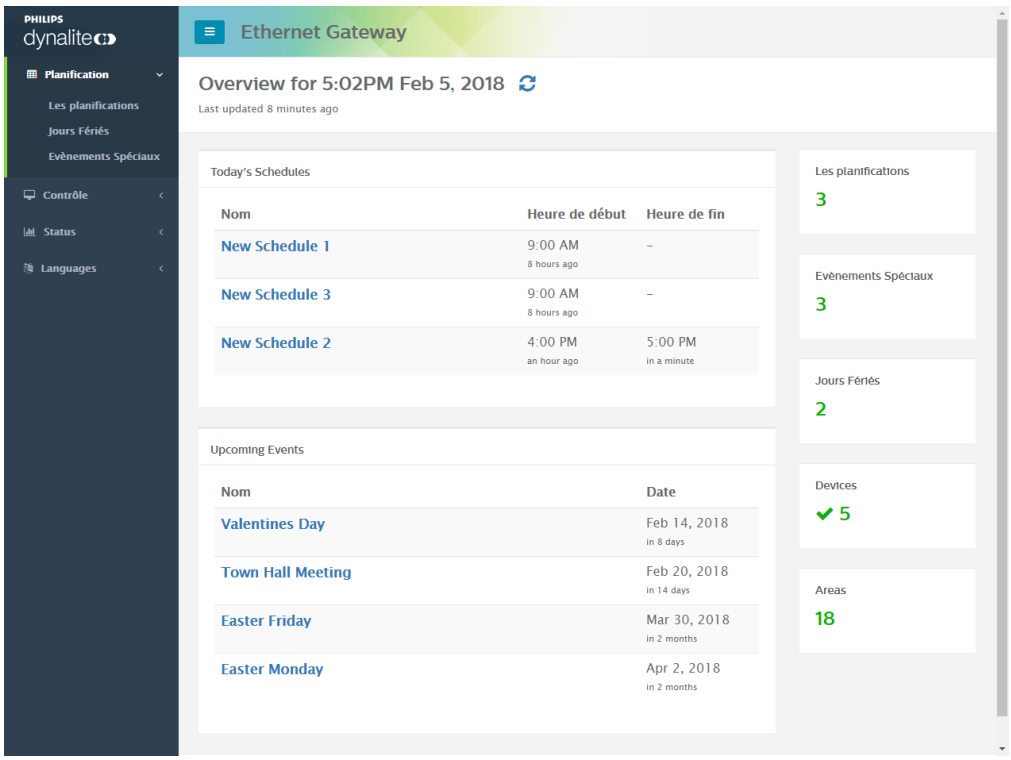
This page enables you to set the location, time zone and daylight savings information.



5.6 Languages

The language menu translates the pages into the selected language. Select one of the following languages:

- English
- Dansk
- Deutsch
- Dutch
- Français


PHILIPS
dynalite
Ethernet Gateway
Planification
Les planifications
Jours Fériés
Evènements Spéciaux
Contrôle
Status
Languages
Overview for 5:02PM Feb 5, 2018
Last updated 8 minutes ago
Today's Schedules
Nom
Heure de début
Heure de fin
New Schedule 1
9:00 AM
8 hours ago
–
New Schedule 3
9:00 AM
8 hours ago
–
New Schedule 2
4:00 PM
an hour ago
5:00 PM
in a minute
Upcoming Events
Nom
Date
Valentines Day
Feb 14, 2018
in 8 days
Town Hall Meeting
Feb 20, 2018
in 14 days
Easter Friday
Mar 30, 2018
in 2 months
Easter Monday
Apr 2, 2018
in 2 months
Les planifications
3
Evènements Spéciaux
3
Jours Fériés
2
Devices
5
Areas
18

5.7 Log files

Directory A: is used for the EG log files. EG keeps two rolling 28 day log files for maintenance and troubleshooting purposes:

- A + [Date stamp].log
  This file records all spur alarms and events.
- O + [Date stamp].log
  This file records all online/offline status and sign-on messages.
- S + [Date stamp].log
  This file records all spur traffic network messages.

The log messages are in DyNet2 format. You can download these files via the webserver or when connected to the EG via Ethernet you can right-click the EG and select Manage Log Files. You can then open and view them in the SB Monitor window.

Copy the files to a local drive and in the SB Monitor Window, click the Network Log tab. Then you can use the Network Log toolbar to open and view the downloaded log files.

Network Log Toolbar

6 System Manager Schedules

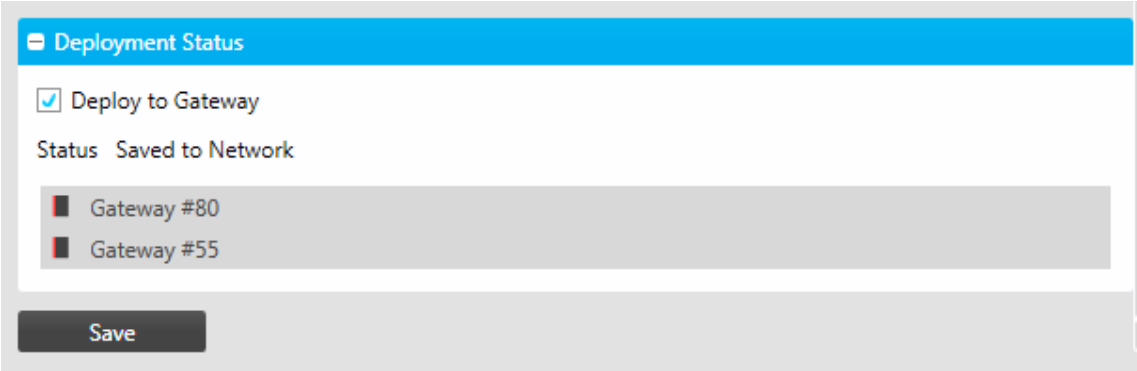
6.1 Schedule Deployment

System Manager (SM) gives you a choice to run schedules from SM Server or to delegate schedules to the EGs in the system. The benefit of running schedules in EG is that it distributes the processing and does not use any server resources. EGs will run schedules even if the server is offline.

When viewing a Schedule in SM, the ☑ Deploy to EG checkbox indicates that the schedule will run in the EGs (this is the default setting).

SM keeps a track of changes to schedules and reminds you to save the changes if you try to exit the Schedule Editor.

If a schedule runs on areas in multiple EGs, SM lists all the affected EGs in the Deployment Status list.



if you have System Manager (SM) all schedules should be created in SM.
Do not modify schedules using the web interface or in SB as SM will have no knowledge of the changes. Similarly, schedules created in SB are not visible in SM. Schedule information only flows in one direction from SM to EG or from SB to EG.

For more information on schedules refer to the Property Editors - Schedules topic.

6.2 Schedule limitations

The following table lists the schedule limitations.

Schedule parameter	SB/SM Limit
Schedules	100
Public holidays	30
Special events	30
Event scheduler names	40 characters

The following table lists the default schedule settings in each device. They can be modified in SB/SM.

Device	Number of Schedules	Schedule Reserved Bytes	Schedule Name	Number of Public Holidays	Public Holidays Name	Number of Special Events	Special Event Name
PDEG	40	200	40	5	40	15	40
PDEG-S	40	200	40	5	40	15	40
PDTS	40	200	16	5	16	15	16

System Builder/System Manager alerts the user when they reach the limit and any additional schedules required beyond the total capacity of the EG are kept as SM only schedules.

Some actions in schedules cannot be deployed because they are not supported by the EG. Schedules with non-deployable actions are run in System Manager and do not consume event memory in the EG.

Deployable actions	Non-deployable actions
Preset	Run Report
Channel Level	Schedule Control
Motion Control	Trigger Control
Sensor Timeout Control	Emergency Test
PE Control	Auto Sensor Calibration
Panel Control	Perform Backup Action
Area Cascading Control	
Set Join Level	
Panic	
Reset Preset	
Area Link	
Set Preset Offset	

These settings can be found and modified on the Device Properties editor in SB.

Scheduler	
Event schedule	Enabled
Reserved event schedule records	40
Reserved task length (bytes)	200
Grace Period (minutes)	0
Reserved event schedule name (bytes)	16
Reserved special event records	5
Reserved special event name (bytes)	16
Reserved public holiday records	15
Reserved public holiday name (bytes)	16

7 Property Editors

Standard properties are shown in ***bold italics***. Advanced properties are shown in *italics*.

Displayed fields can be sorted in one of two ways by using the following buttons:

Categorized

Alphabetical

Initially only the basic fields are shown. To reveal all fields, click the Advanced button. The list can be filtered by entering all or part of a property name in the Filter box.

7.1 Device Properties

The Device Properties editor displays information about the device and basic device configuration properties.

The available categories are:

- Device Identification
- Product Information
- Device Status
- Start-up Settings
- Real-Time Clock
- Ethernet Applications
- Scheduler
- LDAP

Device Identification

Property	Description
Device Name	Used to identify the device.
Location	The physical location of the device.
Description	Other identifying information for the device.
Box number	Physical address used for identification by the Dynalite system.
Serial number	The serial number of the device.
Device location sequence	Identifies devices sequentially on a series network, not required.
Device number	System Designer reference number.
IPv4 Address	32-bit network address expressed in decimal
IPv6 Address	128-bit network address expressed in hexadecimal (32 hexadecimal numbers)

Product Information

Property	Description
Product name	These fields are populated automatically, and identify the product type, hardware, firmware and bootloader versions.
Product category	
Product type	
Device code	
PCB assembly	
Model ID	
Firmware version	
Bootloader version	
Has RTC	Device has a built-in real-time clock. True or False.

Device Status

Property	Description
Device status list	These fields are populated automatically, and show information about device creation, modification and current status.
Date time created	
Date time modified	
Date time memory loaded	
Date time memory saved	
Date time task compiled	

Start-up Settings

Property	Description
Metric polling startup delay (sec)	If enabled, the device sends a DyNet sign-on message when turned on or reset.
Start delay (rounded to 10 ms)	Delay after start-up before sending sign-on message. Maximum value: 00:30:000 (rounded to 10 ms).

Real-Time Clock

Property	Description
Broadcast time	Enable or disable the real-time clock's time reporting. Only one timeclock should broadcast to a spur, more than one could lead to time errors.
Broadcast date	Enable or disable the real-time clock's date reporting.
Broadcast interval (seconds)	The real-time clock reporting interval 1-65534 seconds. The default is 600 seconds (10 minutes).
Network Time Protocol	Enable or disable Network Time Protocol (NTP). Enable for cloud.
NTP Polling Interval (days)	The polling interval for Network Time Protocol (NTP).
NTP Hostname	The Hostname for Network Time Protocol (NTP). Set to a valid NTP server name or IP address. Timeservers use port 123.

Ethernet Applications

Property	Description
Web server	Enable or disable web service.
Secure connection (HTTP/HTTPS)	Select supported web server protocol. HTTPS is recommended. (PDEG, PDDEG-S only)
Authentication required for	Specifies when web service authentication is required. Select: • None - no authentication. All users can access all options without needing to logon. • Web pages and CGI - web pages and CGI requests require separate authentication (Not recommended). • CGI Only – users will be requested to logon to the control app. CGI requests such as, GetDyNet.cgi, SetDyNet.cgi and WebPage.cgi need authentication.
Starting web page	The default web page. The Control app uses Index.htm. (PDEG, PDDEG-S only)
Web server caching	Enable or disable web server caching. Certain browsers such as Safari require caching to be disabled to work. (PDEG, PDDEG-S only)
CGI Timeout (milliseconds)	Changes the CGI command timeout period. Default = 1000.
File Transfer Protocol (FTP)	Enable or disable FTP. (PDEG only)
FTP timeout (seconds)	Number of seconds or no timeout. (PDEG only)
Telnet	Enable or disable Telnet. (PDEB, PDEG only)
Telnet timeout (seconds)	Number of seconds or no timeout. (PDEB, PDEG only)

Scheduler

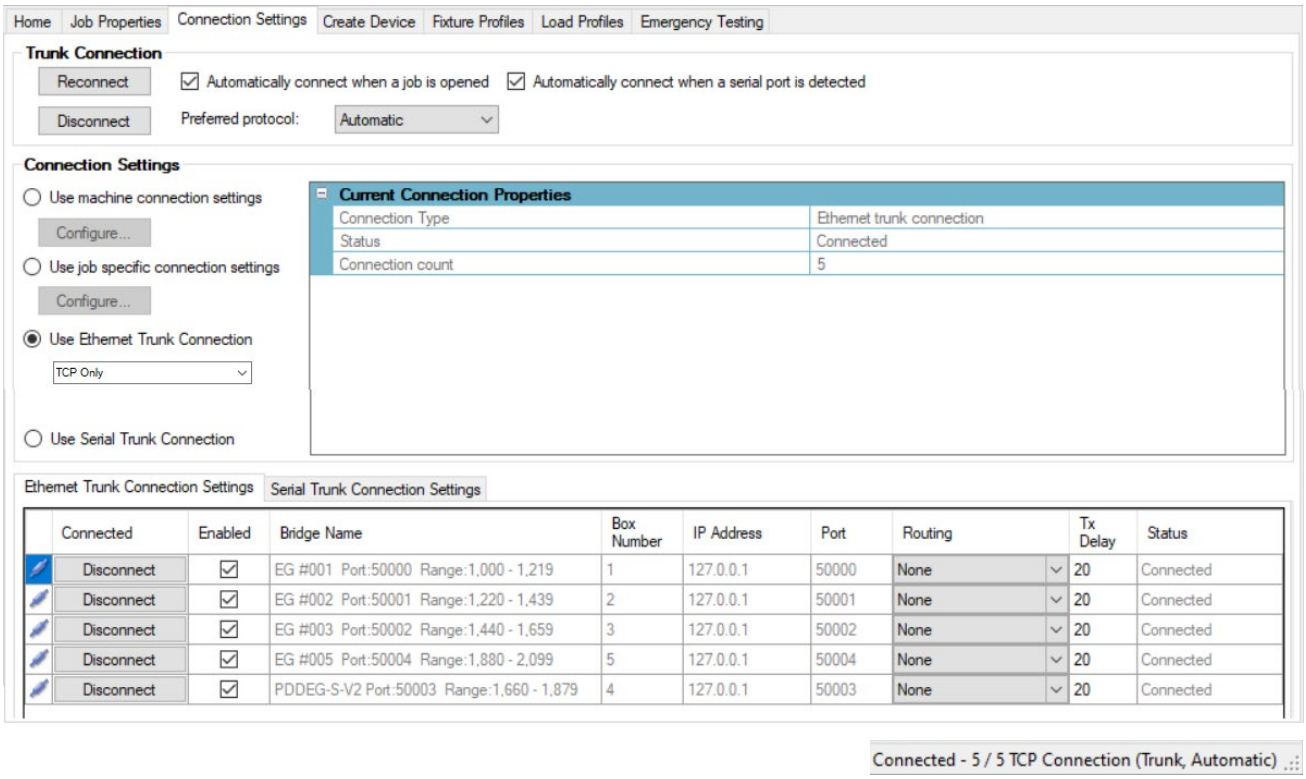
Property	Description
Event schedule	Enable or disable all the event schedules.
Reserved event schedule records	The number of reserved event schedule records. Default = 100.
Reserved task length (bytes)	Default minimum reserved length of task list. Default = 200.
Grace Period (minutes)	Task grace period.
Reserved event schedule name (bytes)	Reserved bytes for UTF-8 text of event schedule. Default = 40.
Reserved special event records	The number of reserved special event records. Default = 5.
Reserved special event name (bytes)	Reserved bytes for UTF-8 text of special event Default = 40.
Reserved public holiday records	The number of reserved public holiday records Default = 15.
Reserved public holiday name (bytes)	Reserved bytes for UTF-8 text of public holiday Default = 40.

LDAP

Property	Description
Enabled	Enable or disable LDAP. if set, Lightweight Directory Protocol (LDAP) configuration is applied to the device.
Port	Standard LDAP port numbers are automatically selected for the user when they change the Encryption type. Port 636 is used for LDAP running over secure sockets layer transport (SSL). LDAP over SSL is sometimes called LDAPS. Port 389 is a default port used for both secure and unsecure methods. The secure method requires Encryption Type property set to LDAP + StartTLS
Timeout (seconds)	Timeout value used for requests to the LDAP server. May be further restricted by the [LDAP] server's configured maximum time.
Authentication Type	None - No Authentication Simple – Username and Password
Encryption Type	Both LDAPS and LDAP + StartTLS are encrypted. Selection depends on what the site uses. None - no encryption is used. LDAPS – LDAP over Secure Sockets Layer (SSL). LDAP + StartTLS.
Host name	LDAP server's hostname or an IP address. Example: ldap.example.com, 172.217.18.196
Base DN	This is the LDAP subtree for users that will be allowed to use the service. Example: OU=Users, DC=example, DC=com
Admin group	The name of the LDAP group of which the user must be a member of to allow access.

7.2 Connection Settings

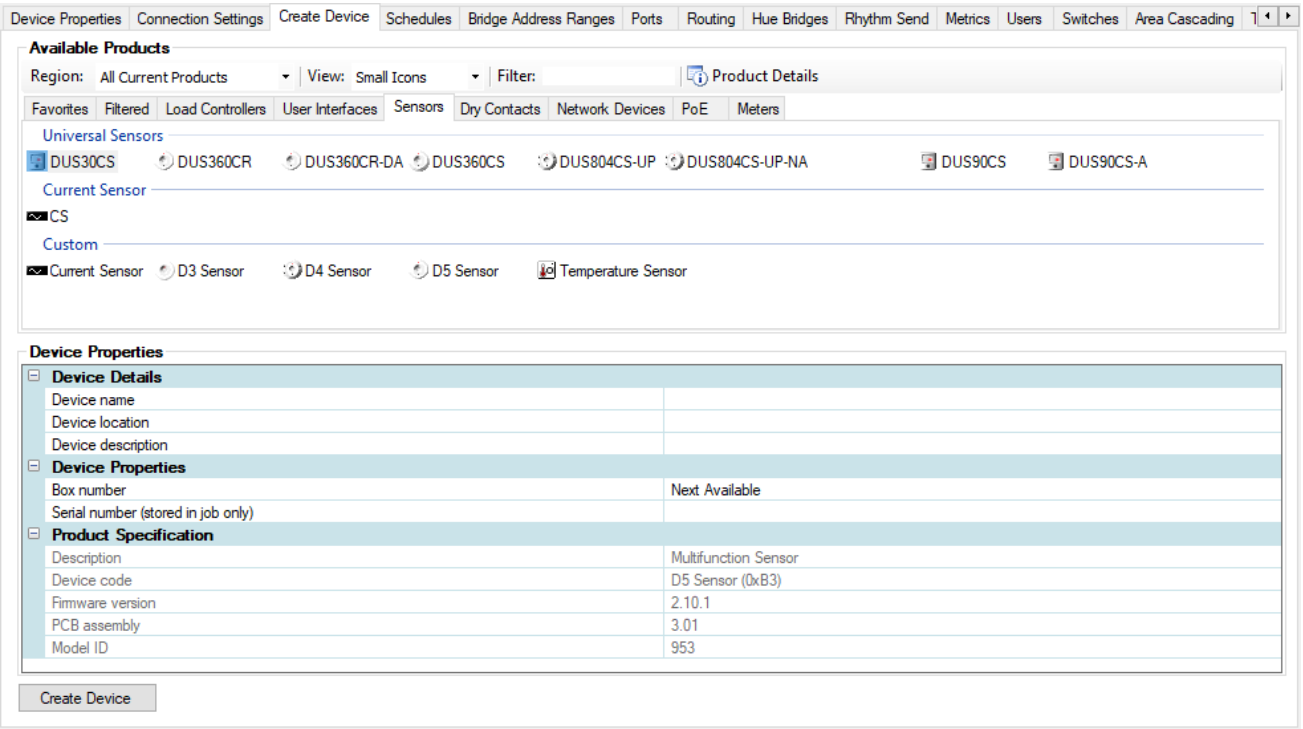
For configuration purposes, you can connect System Builder to the device via Ethernet using TCP/IP or via an RS-485 Serial Connection.



7.3 Create Device

The Create Device page is only required if pre-commissioning devices. It enables offline creation of devices on the spur connected to the EG, such as:

- Load Controllers
- User Interfaces
- Sensors
- Dry Contacts
- Network Devices
- PoE
- Meters



7.4 Schedules

The Schedules Editor enables SB to create and deploy different schedules to the device that are triggered by the internal realtime clock. A series of actions can be defined to run when the schedule is active. The user can also edit, enable or disable schedules in the device.

If you think there are existing schedules in the device, then you should click Load from Device, otherwise they may be overwritten when saving new SB schedules.

To allow the user to create schedules from the device, you need to firstly create them in SB and save them to the device. They must be enabled but do not have to be configured. Ten schedules are preloaded by default.

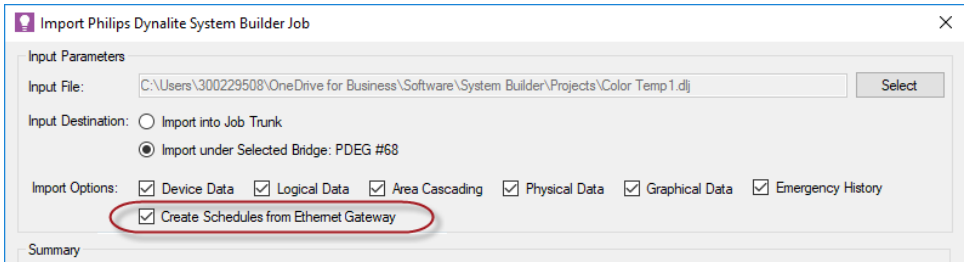
There are two types of schedules:

System Schedules – are created in SM and run on multiple EGs or on the SM Server. System schedules are only visible in SM.

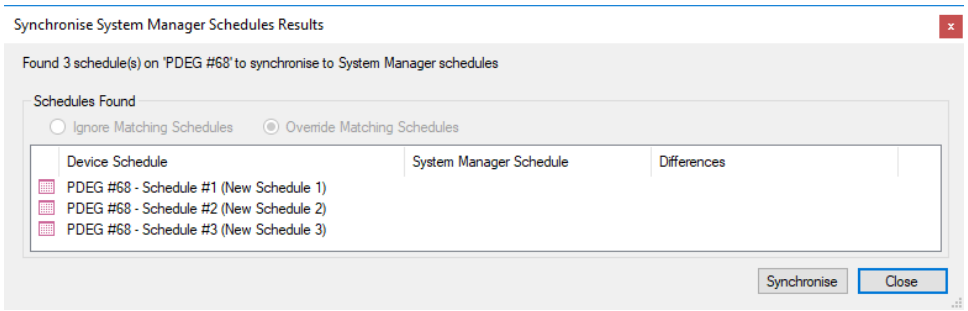
Gateway Schedules – are created in SB or from the EG Web pages and run on a single EG. Gateway schedules are only visible in SM when synchronized.

Gateway schedules can be made into system schedules:

1. During job import



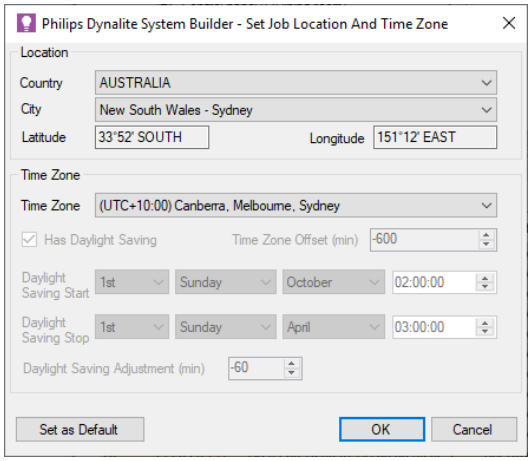
2. Or by clicking Synchronise to System Manager in the SB Schedule Editor and clicking the Synchronize button in the dialogue box.



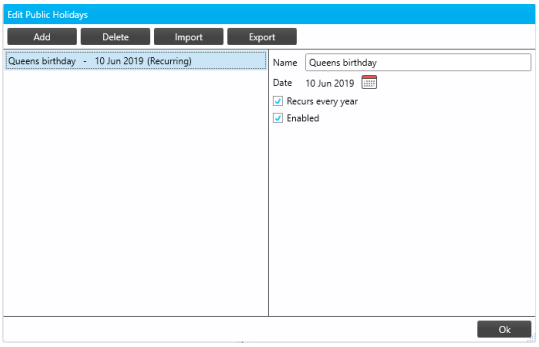
EG schedules modified in the web pages can be made into system schedules by selecting the EG and clicking Load from Device, then clicking Synchronize to System Manager.

The following settings apply to all schedules in the Schedules Editor:

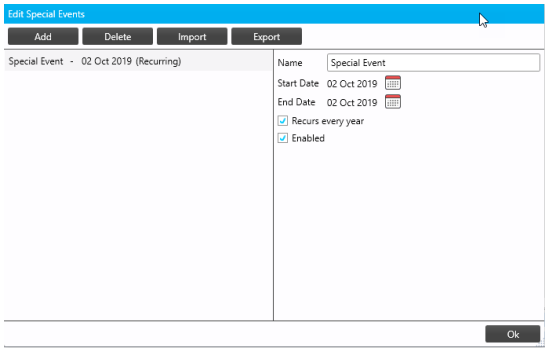
Set Location And Time Zone Opens the Set Device Location and Time Zone dialog box. Click to change the location and time zone for the device, if different from your current location.



Set Public Holidays Opens the Edit Public Holidays dialog box. Click to add, delete, edit, import (.xml or .ics files) and export public holidays for your region. You can include all or exclude all public holidays in a schedule.



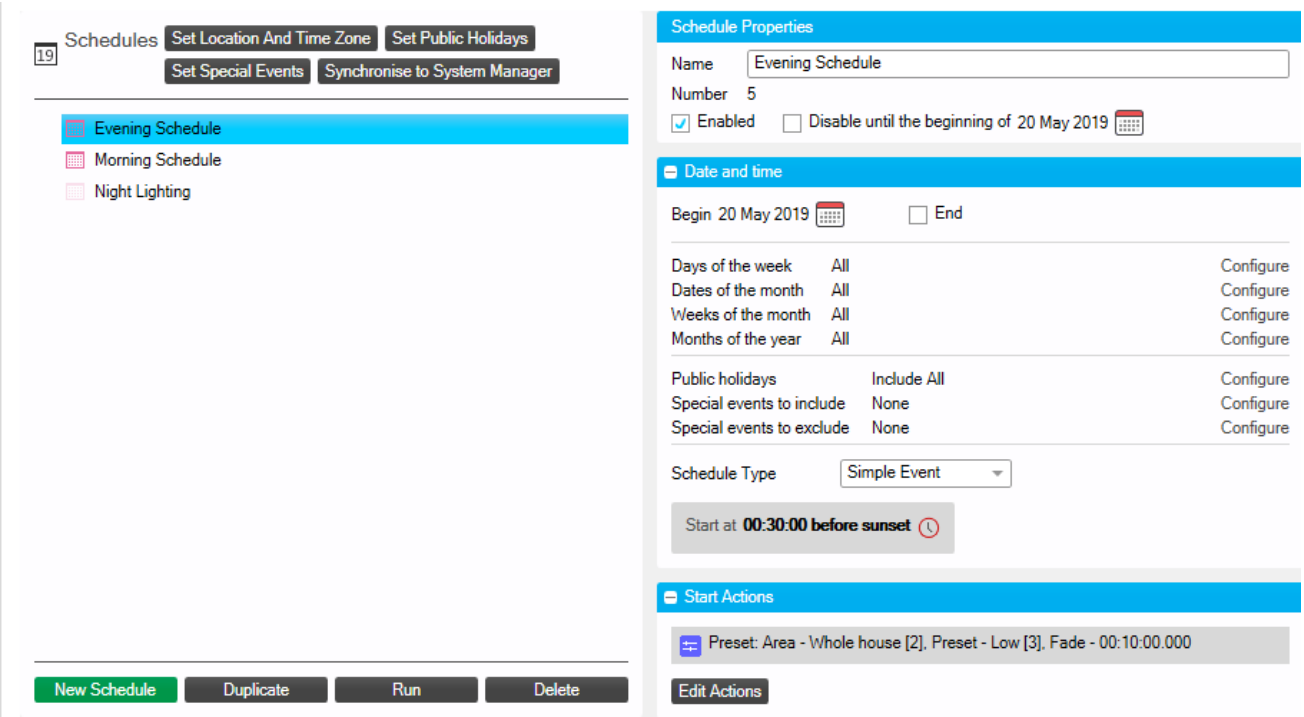
Set Special Events Opens the Edit Special Events dialog box. Click to add, delete, edit, import (.xml files) and export special events for your region. Special events temporarily override normal operational schedules.



Create a Schedule:

1. Select the device in System View.
2. Select the Schedules tab.
3. Click the New Schedule button to add a new schedule to the Schedules list.
4. Select a schedule in the list to edit the Schedule Properties.

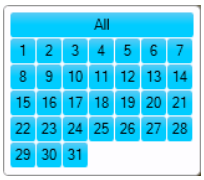
You can click the Duplicate button to add a new schedule with the same properties or click the Delete button to remove a schedule from the list. If you are connected to the device, you can click the Run button to test a schedule.



Edit a Schedule:

1. Under Schedule Properties, enter a name for your schedule.
   (the schedule number is displayed below the name).
2. Tick Enabled, to enable the schedule after it is configured. You set an active period for a schedule by enabling it and checking Disable until the beginning of [Date].
3. Select the Begin and End date to set the date range for the schedule. Untick the End date if you want the schedule to run indefinitely.
4. Select the Days of the week by clicking Configure and selecting the days you want your schedule to run.

5. Select the Dates of the month by clicking Configure and selecting the dates in the month you want your schedule to run.



6. Select the Weeks of the month by clicking Configure and selecting the weeks of the month you want your schedule to run.

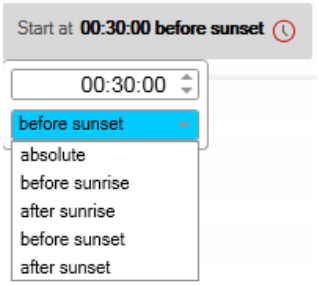
7. Select the Months of the year by clicking Configure and selecting the months in a year you want your schedule to run.

8. Select Include All or Exclude All to run or not run your schedule on Public holidays. When included, select none for Days of the week, Dates of the month, Weeks of the month and Months of the year to only run the schedule on public holidays. Click Edit to add, delete, import or export Public Holidays.
9. Select Special events to include or exclude by clicking Configure and selecting specific special event days. When included, select none for Days of the week, Dates of the month, Weeks of the month and Months of the year to only run the schedule on the Special Event days. Click Edit to add, delete, import or export Special Events.

Selecting Special events to include, runs the schedule on the special event day, even if it would not usually run on that day. Selecting Special events to exclude, will not run the schedule on the special event day, even if it would usually run on that day.

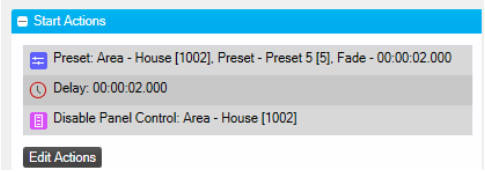
10. Select the Schedule Type. Schedule type can be a simple one-off event or a timed event. For a timed event you can check the Tick every checkbox to add actions at specific time intervals.

11. Specify the Start time, Tick time (for timed events) and Stop time for your schedule. Start and Stop times can be absolute or relative to Sunrise/Sunset.

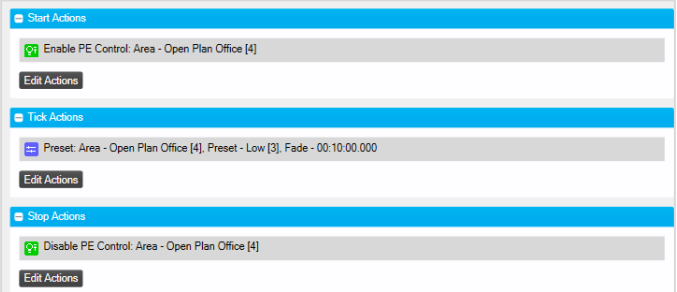


The logic for running a schedule is: Day and Week and Month and Date and included Public holidays and not excluded public holidays and included Special Events and not excluded Special Events.

A Simple Event allows you to add Start Actions to your schedule. Starting a schedule triggers the start actions.



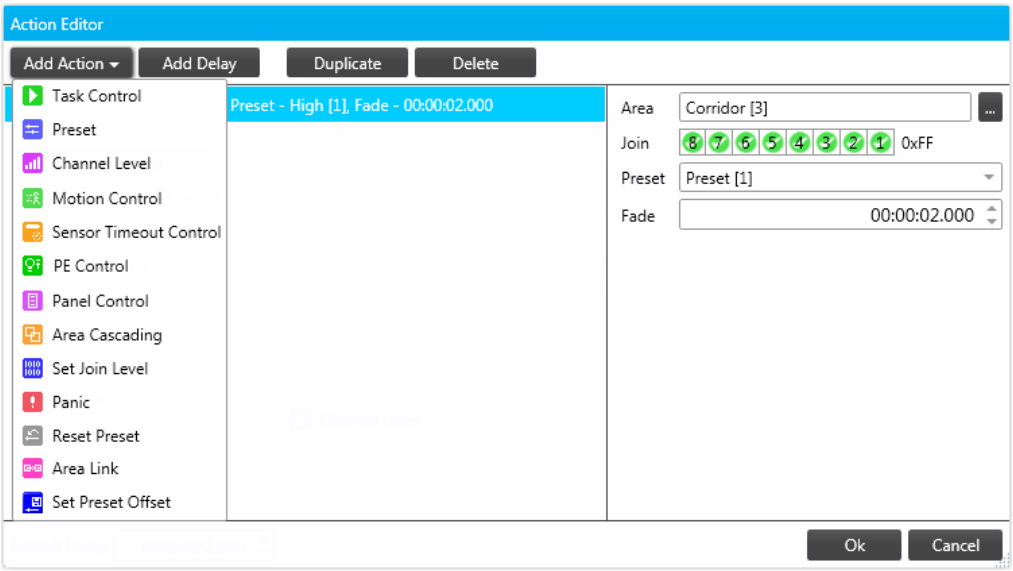
A Timed event allows you to add Stop Actions and Tick Actions. Ending the schedule triggers the Stop Actions and the Tick actions are triggered at specified intervals (Ticks) during the schedule.



Set Actions:

1. Specify the time at which you want the Actions to be triggered.
   When you select the time for Start and Stop Actions, the time can be set as:
   - Absolute
   - Before sunrise
   - After sunrise
   - Before sunset
   - After sunset

2. Click the Edit Actions button. This opens the Action Editor.



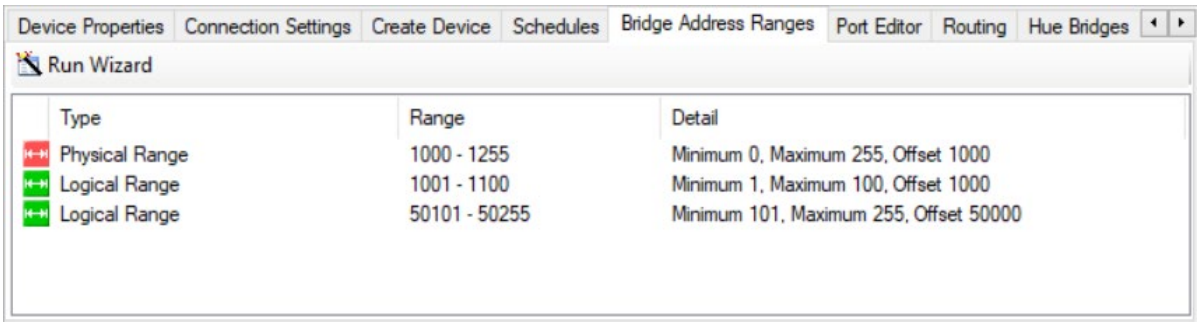
3. Click the Add Action button. A list of actions is displayed.
4. Select an Action from the list.
5. Enter the Action properties on the right-hand side.
6. Click the Add Delay button to add a delay between actions, if required.
7. Click the Add Action button again to add further actions, if applicable.
8. Click the OK button to add the Action sequence to the schedule.

You can repeat any action in the Action Sequence by selecting the action and clicking the Duplicate button.

7.5 Bridge Address Ranges

The Bridge Address Ranges page displays the address offsets for the EG created by the Bridge Configuration Wizard.

The Min value for the primary logical offset range must start at one (or zero, see tip below). Other logical ranges can have any Min value.



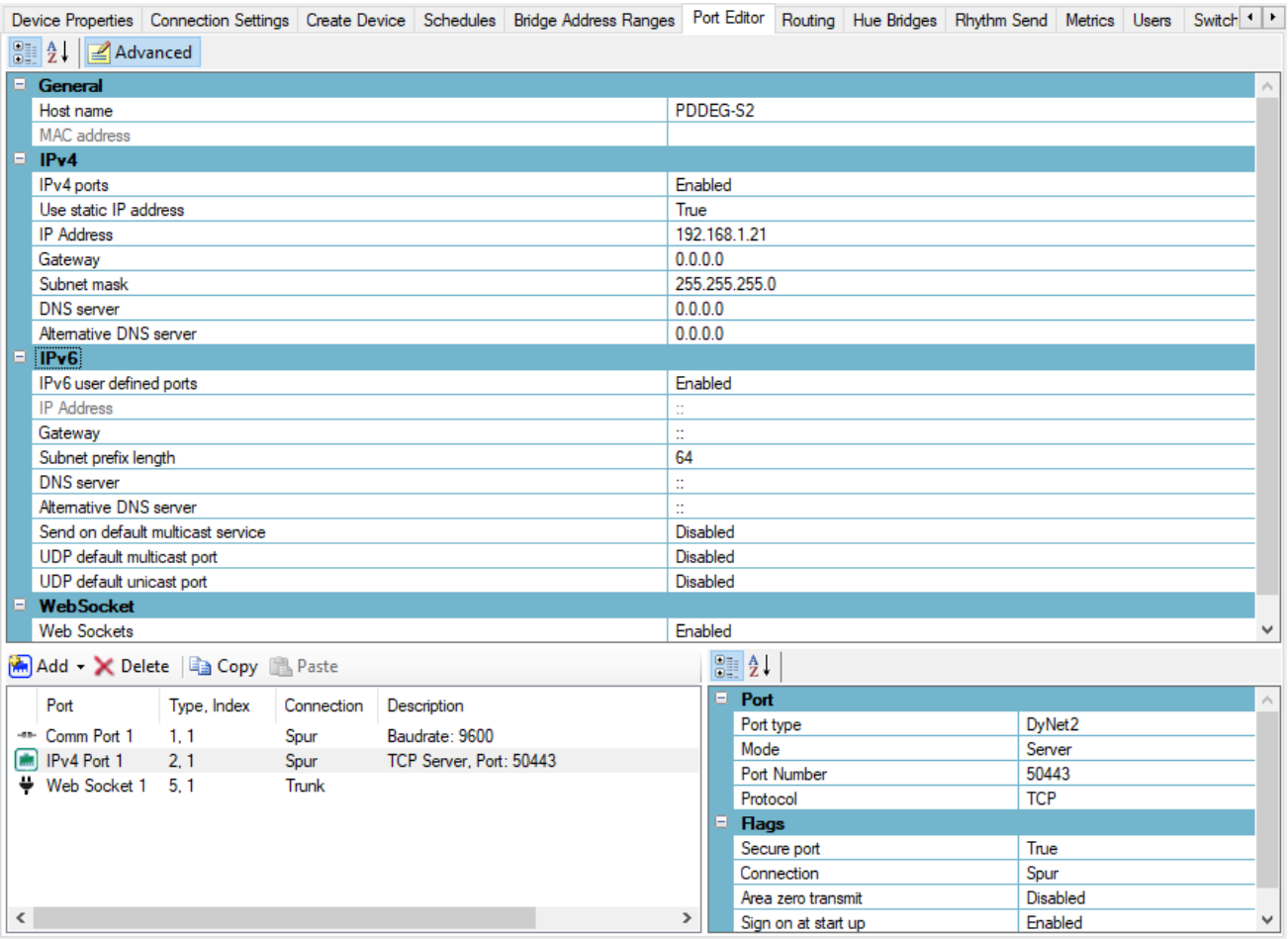
The primary logical range can also start from zero if you want to allow for Area 0 (All Areas) messages to be sent from the trunk. You also need to enable the Area Zero Transmit property on the port record. See Port Editor on next page.

7.6 Port Editor

The EG supports Serial and Ethernet ports. The Port Editor allows you to configure the serial port and the IPv4/IPv6 addresses and ports for connection to the system and to the commissioning PC.

The Port Type can be set to DyNet 1, DyNet2, Fidelio or Text and Binary Integration to define the trunk and spur topology of the system or to connect to a third-party device/system.

To configure the correct routing, it is recommended to add Ports with the Bridge Configuration Wizard.



General

Property	Description
Host Name	Name displayed on the router's connected devices page.
MAC Address	A hardware identification number that uniquely identifies each device on a network.

IPv4

Property	Description
IPv4 ports	Enabled or disabled
Use static IP address	True or False
IP address	The IP address of this device
Gateway	LAN's NAT gateway IPv4 address
Subnet Mask	A 32-bit number that divides an IPv4 address into network address and host address. A Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s.
DNS server	Domain Name Server address
Alternative DNS server	Alternative Domain Name Server address

IPv6

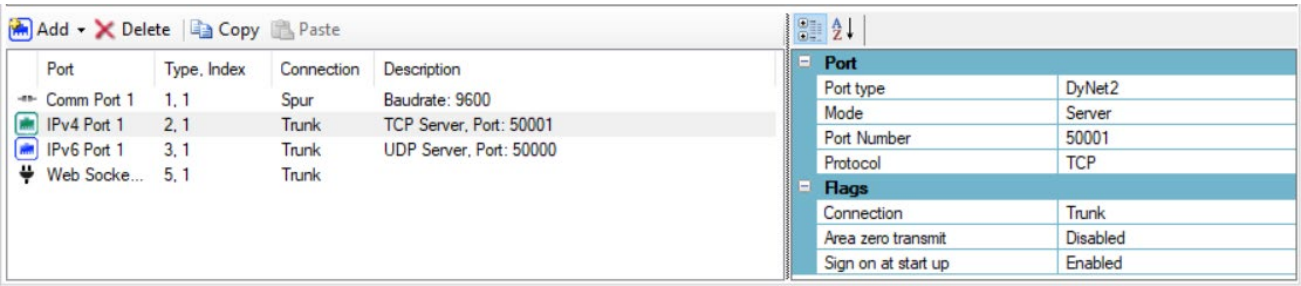
Property	Description
IPv6 user defined ports	Enabled or disabled
IP Address	IPv6 address
Gateway	LAN's NAT gateway IPv6 address
Subnet prefix length	The prefix-length in IPv6 is the equivalent of the subnet mask in IPv4. Default value is 64.
DNS server	Domain Name Server address
Alternative DNS server	Alternative Domain Name Server address
Send on default multicast service	Enabled or disabled (disable for system security purposes)
UDP default multicast port	Enabled or disabled (disable for system security purposes)
UDP default unicast port	Enabled or disabled (disable for system security purposes)

Web Socket

Property	Description
Web Sockets	Enabled or disabled. Allows the device to listen to system messages via the API (not available in the PDEB/PDEG)

Add Port

Click Add to add an IPv4 port or IPv6 port to the device.



Port

Property	Description
Port type	Port type can be set to DyNet1, DyNet 2, Fidelio or Text & Binary Integration. The ports are grouped by Port type; Serial Comm Port = 1, IPv4 Port = 2, IPv6 Port = 3, WebSocket Port = 5. The Port Index is a sequence number within each Port group.
Mode	Defines if the controller is acting as the client or server.
IP Address	The IPv4 or IPv6 address of the remote port
Port Number	Port number
Protocol	TCP or UDP

Flags

Property	Description
Connection	Specifies a Trunk or a Spur connection for address translation purposes.
Area Zero Transmit	Enable all areas messages for diagnostic use. Leave this option disabled unless advised by Philips Dynalite.
Sign on at start up	Sending a sign on message at startup may be enabled or disabled.
Reply using a unicast message	True or False. If set to true, then when a message is received on a UDP broadcast or multicast port the device will respond directly using a unicast message and not broadcast the response.

Comm Port properties not shown. Please leave at default settings.

7.7 Routing

The device includes the default Routing Editor and routing-related properties.

To configure the correct routing, it is recommended to run the Bridge Configuration Wizard.

7.8 Hue Bridges

The device includes a Hue Bridges Editor and Hue-related properties.

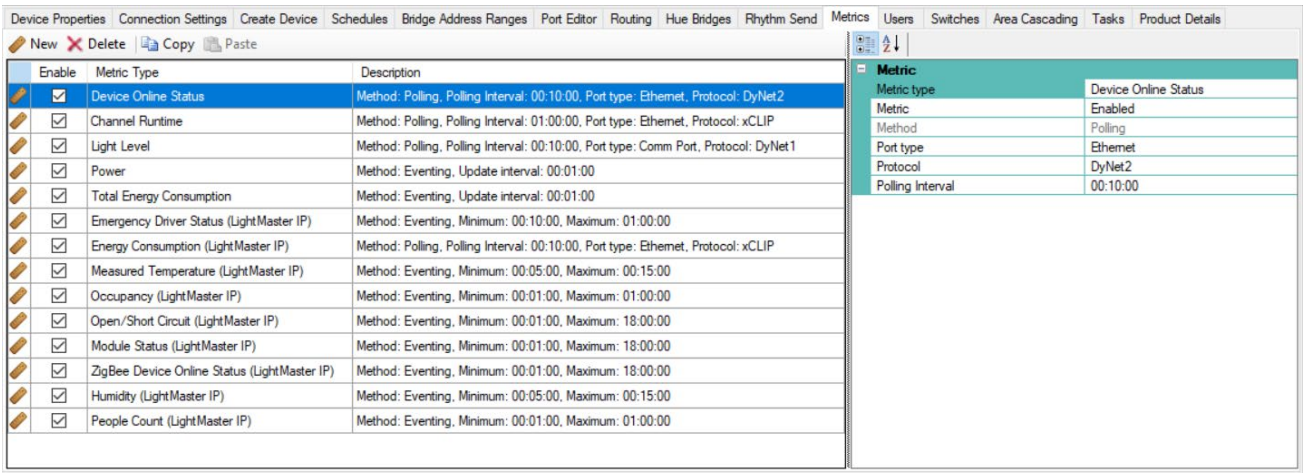
To configure the Hue bridges, please ref to topic 3.1 Hue Integration.

7.9 Metrics

The Metrics Editor enables the EG to collect system/device/fixture status and runtime information.
Metrics– defines the data provided by the connected devices to System Manager.

It is recommended to add Metrics with the Bridge Configuration Wizard.

Only enable the metrics that are necessary for your system. as they have a significant CPU and network overhead.



7.10 Users

The Users Editor allows you to create users by setting up a username, password and permissions for each user.

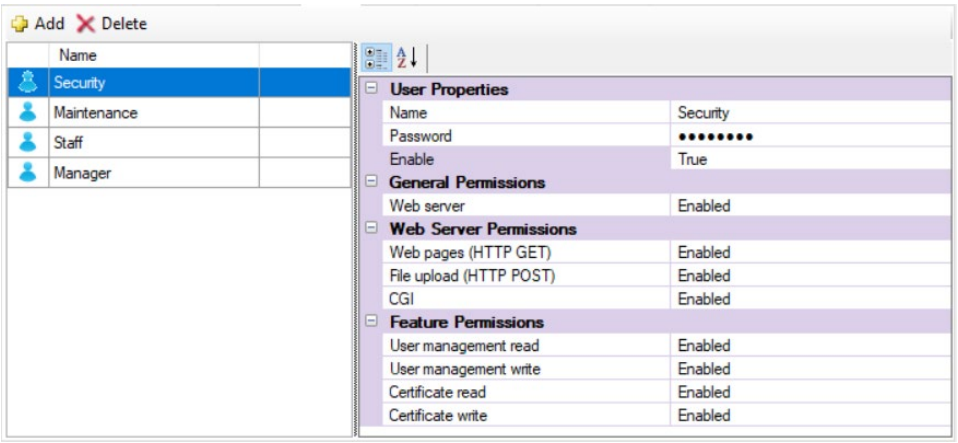
A user must be added to perform some operations such as file transfers and enabling the security features.

You can implement User Authentication to restrict access to the user interface and to restrict access to the device over Ethernet.

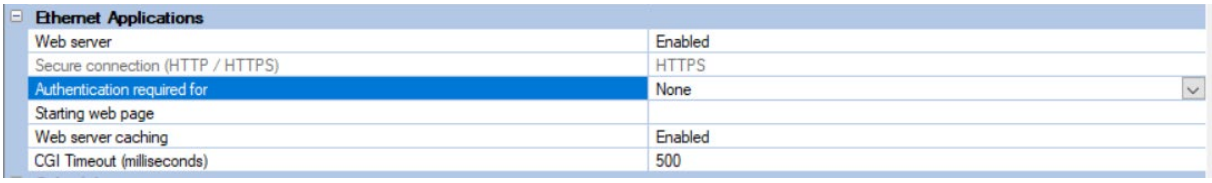
You must change the default user password to complete commissioning of the device.

Add Users:

1. Click the Users tab.
2. Click Add (maximum of five users).
3. Enter the Name and Password (Usernames and passwords have a 40-character limit and are case sensitive).
4. Confirm password.
5. In the Enable property, select True.
6. For General, Web Server and Feature permissions, select Enabled or Disabled.



7. Click the Device Properties tab.
8. In Device Properties > Ethernet Applications > Authentication required for, select None or CGI only. Select other properties, if applicable. For more information refer to topic 6.1 Device Properties.



9. Press F12 or click Save to Device.

User Properties

Property	Description
Name	Username
Password	User password
Confirm Password	Confirm User password
Enable	True or False.

General Permissions

Property	Description
FTP	Enabled or disabled.
Telnet	Enabled or disabled.
Web server	Enabled or disabled.
Web Socket	Enabled or disabled.

Web Server Permissions

Property	Description
Web pages (HTTP GET)	Enabled or disabled.
File upload (HTTP POST)	Enabled or disabled.
CGI	Enabled or disabled.

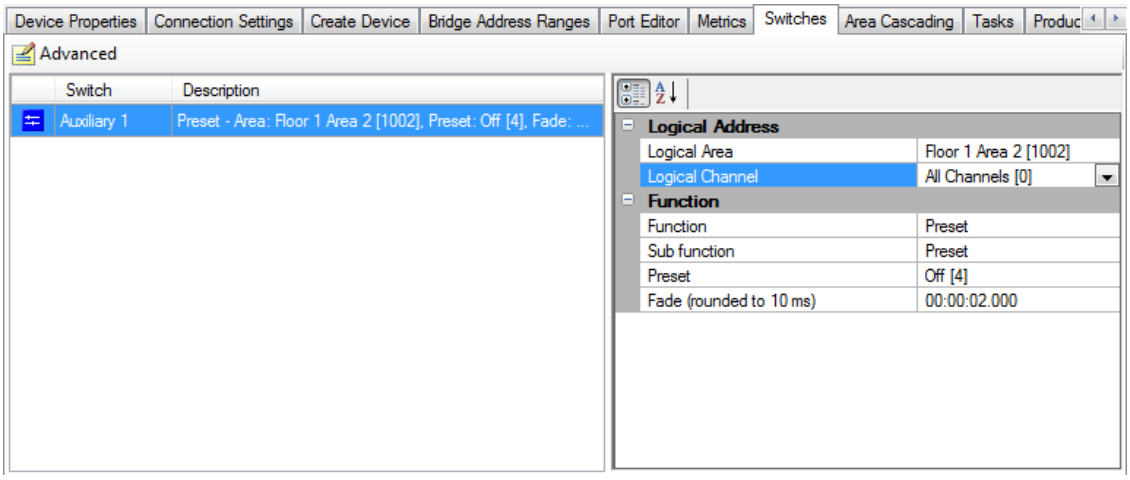
Feature permissions

Property	Description
User management read	Enabled or disabled.
User management read	Enabled or disabled.
Certificate read	Enabled or disabled.
Certificate write	Enabled or disabled.

- To modify log files the user must be given both **FTP** and **File upload** permissions.
- If usernames or passwords are forgotten and you do not have the job file, they can be retrieved by loading from the device.

7.11 Switches

The Switches Editor allows you to define actions for the EG Auxiliary input.



The following functions are available for the Auxiliary Switch. Each function may have one or more sub functions and associated settings:

Advanced	Sign On Panic
Channel level	Channel Level
Custom	Custom
One touch	One touch ramp only One touch ramp with program
Preset	Preset Off preset Reset Preset Preset offset Toggle Preset
Ramp	Ramp up Ramp down
Task	Task Local
No function	No function

Advanced > Sign On

This diagnostic function checks the device by sending a DyNet message to the network.

Advanced > Panic

Property	Description
Panic	True/False – If True, sets the selected area to panic mode when the button is pressed, raising all dimming levels to 100% and locking UI controls for that area. If setting this option to False (disable panic mode), set General > Enable when panel disabled to True.
Fade time	The time taken for dimming levels to fade from their current setting to 100%.

Channel Level

Property	Description
Level (%)	Sets the percentage level of light on the channel
Fade	The time taken to fade to the requested channel level
Off preset	Defines the off preset number for the area. If this preset is recalled, the button's indicator LED will deactivate.
DyNet mute	Stop DyNet messages being created by this function.

Custom

This function enables advanced custom actions built using the Action Chain Editor. Refer to the System Builder Training Guide for more information.

Property	Description
Standard function name	Internal system function, not user-editable.
Press actions	Opens the Action Chain Editor.
Release actions	Opens the Action Chain Editor.
Extended press actions	Opens the Action Chain Editor.
Extended release actions	Opens the Action Chain Editor.

One Touch > One touch ramp only

Property	Description
On Preset	Defines the preset for the button's On state.
Off Preset	Defines the preset for the button's Off state.
Fade (rounded to 10 ms)	Time taken to reach the preset level if the button is tapped.
Ramp rate	Time taken to ramp up to the required level if the button is held.
Min Level	Minimum light level when ramping down.
DyNet Mute	Stops DyNet messages being created by this function.
Double send stop fade	If True, the 'stop fade' command is sent twice to ensure correct operation on busy networks.

One Touch > One touch ramp with program

This function allows the user to change the levels for a particular preset. For a long press, the current levels will ramp up or down. If the press is released while ramping up, the new lighting levels will be saved to the On preset.

Pressing briefly will toggle between the currently saved On preset and the Off preset.

Property	Description
On Preset	Defines the preset for the button's On state.
Off Preset	Defines the preset for the button's Off state.
Fade (rounded to 10 ms)	Time taken to reach the preset level if the button is tapped.
Ramp rate	Time taken to ramp up to 100% if the button is held. When the button is released, the current level will be saved to On preset.
Min Level	Minimum light level when ramping down.
DyNet Mute	Stops DyNet messages being created by this function.

Preset > Preset

Property	Description
Preset	Defines the preset for the button's ON state.
Fade (rounded to 10 ms)	Time taken to reach the On state.
DyNet Mute	Stops DyNet messages being created by this function.

Preset > Off preset

Instantly drops all channels in the specified area to 0%.

Property	Description
Off Preset	Defines the area's Off preset for the button's indicator LED.
DyNet Mute	Stops DyNet messages being created by this function.

Preset > Reset Preset

Resets all channels in an area to the currently selected preset.

Property	Description
Fade	Time taken to reset the current preset.
DyNet Mute	Stops DyNet messages being created by this function.

Preset > Preset offset

Property	Description
Preset offset	When button is pressed, all other preset commands are incremented by this number.
DyNet Mute	Stops DyNet messages being created by this function.

Preset > Toggle Preset

This function toggles between the selected On preset and the Off preset.

Property	Description
On Preset	Defines the preset for the button's On state.
Off Preset	Defines the preset for the button's Off state.
Fade (rounded to 10 ms)	Time taken to transition between presets.
DyNet Mute	Stops DyNet messages being created by this function.

Ramp > Ramp up

Property	Description
Fade (rounded to 10 ms)	Time taken to fade from the current level to 100%.
On channels only	If True, only channels with a level 1% or higher will ramp up.
DyNet Mute	Stops DyNet messages being created by this function.
Double send stop fade	If True, the 'stop fade' command is sent twice to ensure correct operation.

Ramp > Ramp down

Property	Description
Min Level	Minimum light level when ramping down.
Fade (rounded to 10 ms)	Time taken to reach the preset level if the button is tapped.
Ramp rate	Time taken to ramp up to the required level if the button is held.
DyNet Mute	Stops DyNet messages being created by this function.
Double send stop fade	If True, the 'stop fade' command is sent twice to ensure correct operation on busy networks.

Task > Task Local

This function controls a custom task that is stored and executed on the device. For more information on basic and advanced tasking, refer to the System Builder Training Guide.

Property	Description
Control type	Start, Pause or Stop the selected task.
Task	Defines the task number.

No Function

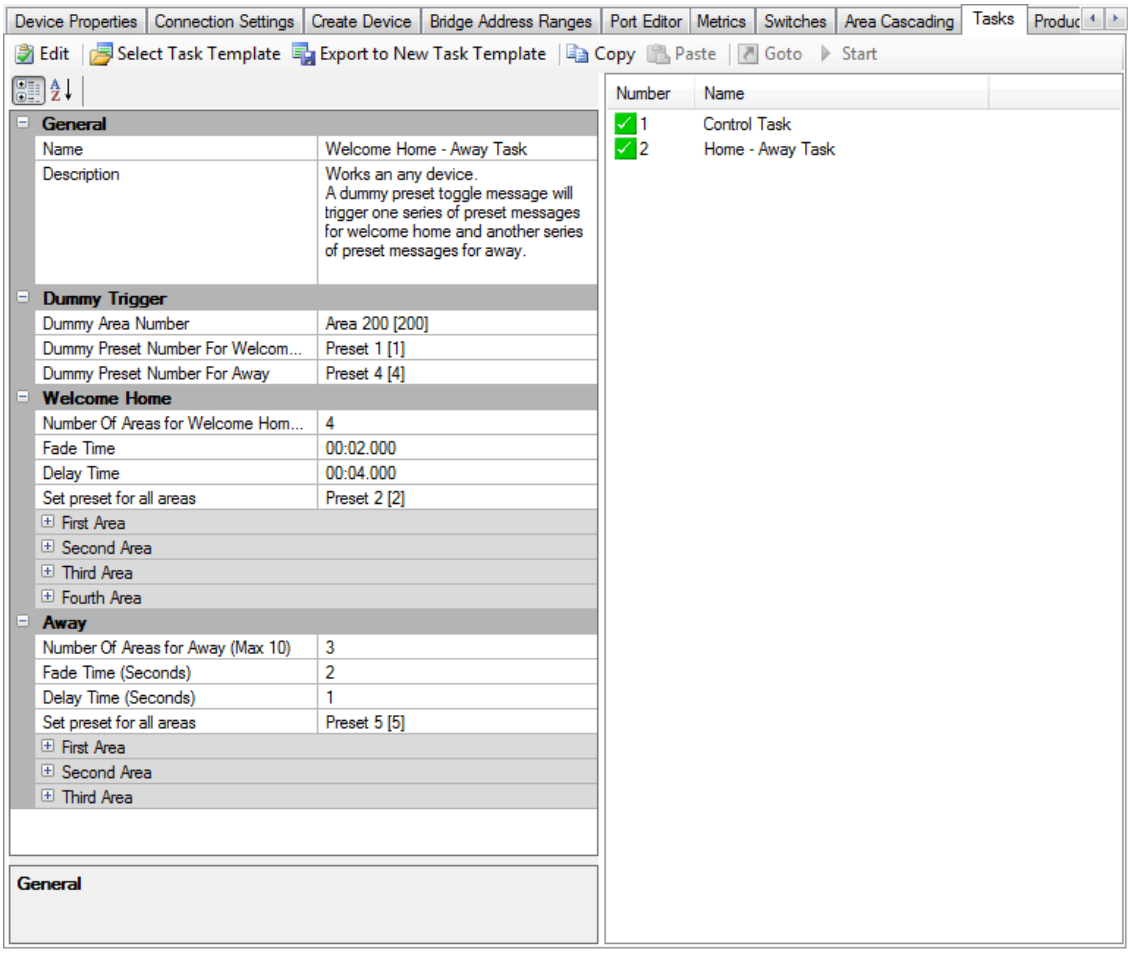
Select this option for buttons that are not in use.

7.12 Tasks

The Task Editor enables you to select a Task Template for fast creation of complex tasks and allows code editing for custom tasks

The device includes the default Task Editor and task-related properties.

For information on custom task scripting, refer to the System Builder Training Guide or contact Dynalite support at support.controls@signify.com.



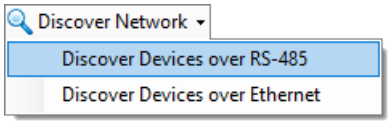
7.13 Device Discovery

Upon installation, the Ethernet Gateway (EG) uses background polling to automatically discover DyNet devices on its spur (DALI multi-master devices are discovered when data from a DALI-2 controller is loaded).

When SB is connected to the spur, the Discover Devices over RS-485 feature, speeds up commissioning by allowing the engineer to load the device list directly from the EG instead of searching the entire spur with SB.

When SB is connected to the trunk, the Discover Devices over Ethernet feature enables SB to discover Ethernet devices using mDNS and attempt to connect to them securely using the default factory certificate. (if a secure connection is not available SB will try to connect over an unsecure connection).

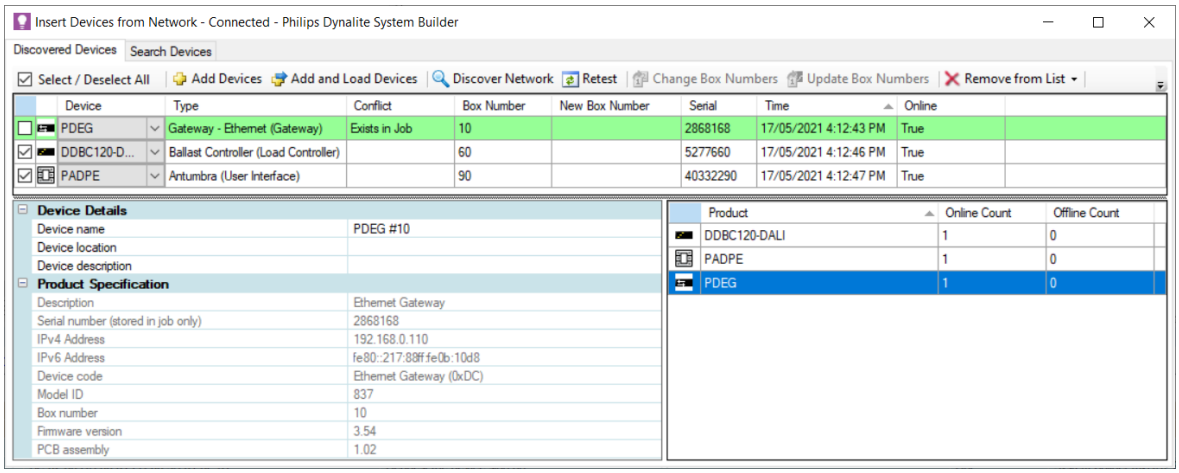
The default factory certificate is not intended for permanent operation. If a secure connection to an Ethernet device is required for operation, you must set a Site CA Certificate, then create and upload the site certificate to each Ethernet device. For more information, refer to the following topics:
2.1.3 Creating a Site CA Certificate
2.4.4 Secure Ethernet to RS-485
2.4.5 Secure Ethernet to Ethernet.



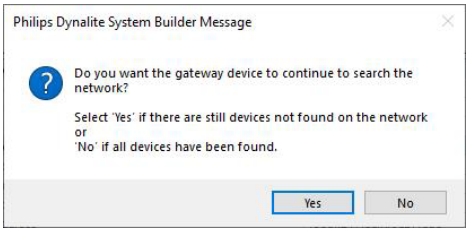
Discover Devices over RS-485:

1. Click **Insert Devices from Network.**
2. Click **Discover Network > Discover Devices over RS-485** to list all discovered devices on the EG's spur. This automatically disables background polling. You can click the Retest button to list the discovered devices again.

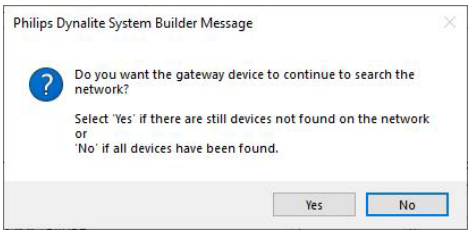
   All devices discovered during background polling are listed under the Discovered Devices tab, including currently offline devices that were previously discovered by the EG. The Online Count and Offline Count for each discovered device type are displayed in the bottom right pane.

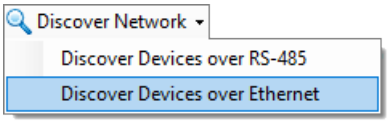


3. The following dialog box appears:
   a. If the device list is incomplete, click Yes to reenable polling and wait for the EG to complete device discovery before repeating this procedure. This may take up to two hours on larger spurs.



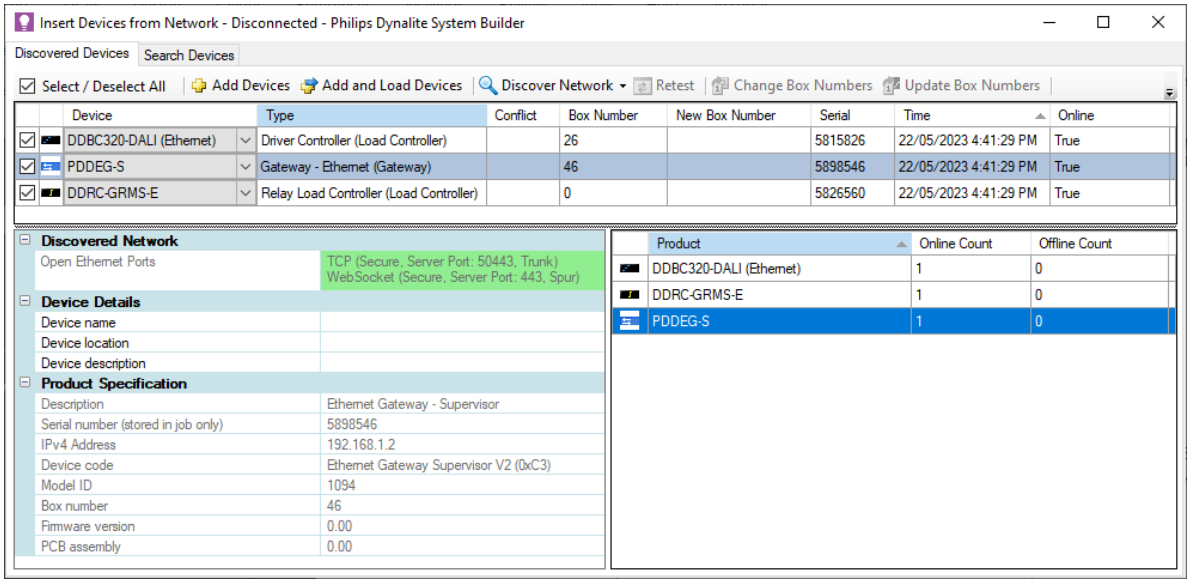
b. If the device list is complete, click No to disable polling and continue with the commissioning process. Polling for device discovery must be disabled in the Device Discovery editor before completing commissioning.



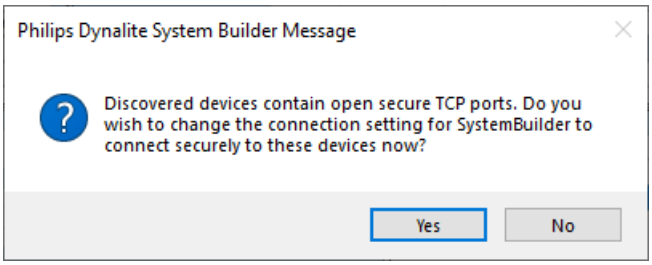


Discover Devices over Ethernet:

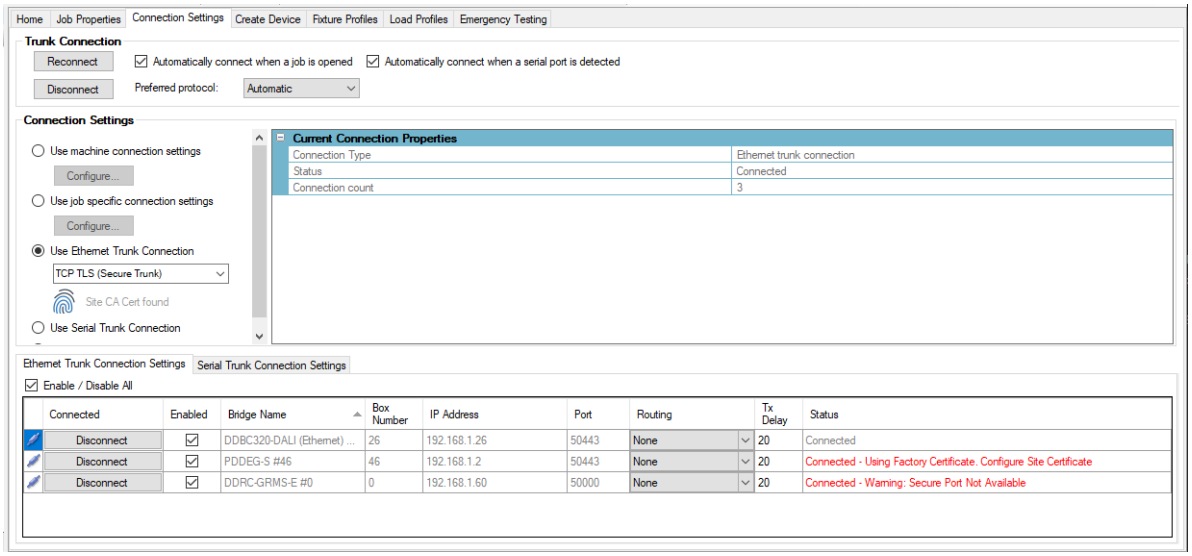
1. Click **Insert Devices from Network.**
2. Click **Discover Network > Discover Devices over Ethernet** to list all discovered devices on the trunk. Note: SB can be disconnected as it uses mDNS to discover devices over Ethernet.



3. Click Add Devices to add them to the job.
4. Click the Yes button. SB will change the connection Settings to TCP TLS (Secure Trunk) and attempt to reconnect to the Ethernet devices.



5. Click the top of the device tree and check the **Ethernet Trunk Connection Settings**. Depending on each device's configuration SB will:
    a. Connect using the Job's Site Certificate if it has been created and uploaded to the device.
    b. Connect using the Default Factory Certificate when the Site Certificate has not yet been uploaded to the device.
    c. Connect unsecurely to the device when a secure port has not been added to the device.
    d. Not connect when there is no IP Port configured on the device.



7.14 Product Details

The Product Details page displays the name, short description and an image of the physical product.

8 Appendix A: Firmware Upgrade

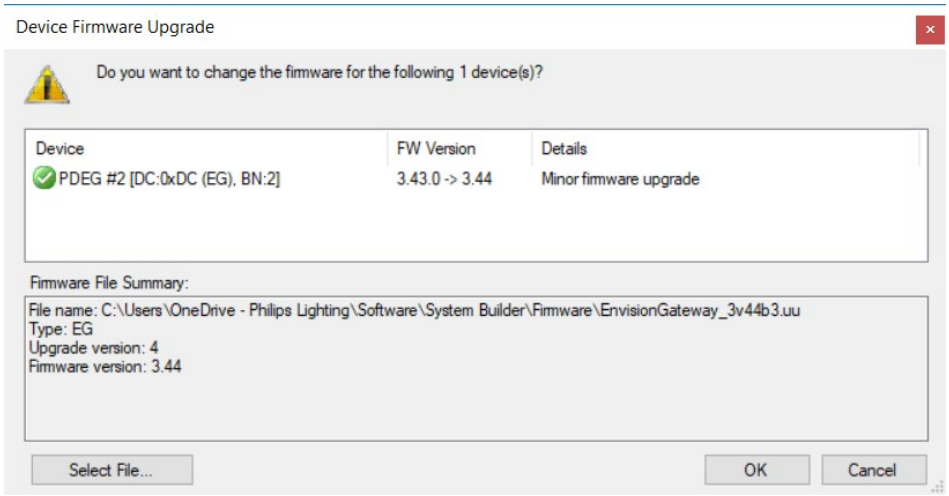
PDEG firmware can be upgraded with System Builder (SB). SB allows you user to cancel any queued firmware upgrades at any time.

If using SB to upgrade the firmware, SB supports firmware upgrades over:

- DyNet – the download is performed over RS-485 using standard upgrade messages.
- Ethernet – A download is performed using an IPv6 UDP connection (or an IPv4 TCP connection for EGs with minimum firmware 3v32 and bootloader 64v5).

Upgrade Firmware with SB (recommended):

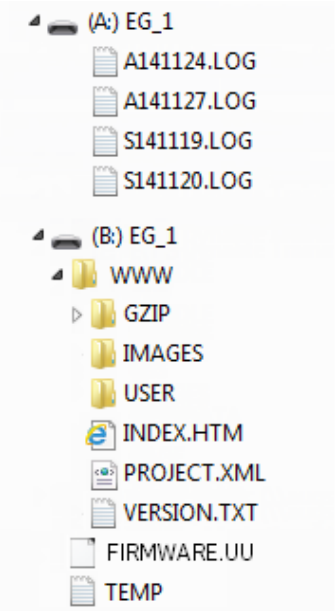
1. Multi-select the EG devices (must be the same type) that require a firmware upgrade.
2. Right-click on the devices and select Firmware Upgrade.
3. Browse to the EG*.uu file (or dfw file for older firmware) and click the OK button.
   To confirm the upgrade, SB displays the Device Firmware Upgrade window. The window displays the current and new firmware version for the device being upgraded.
4. Click the OK button. The progress and status of each firmware upgrade is displayed.
   When complete, SB verifies that the firmware upgrade has been successful.



SB configuration changes should be complete, saved to device and tested before hand otherwise you may lose access to the EG.

If the device does not come back online, use a serial connection to the device to discover it again.

Upgrade Firmware with an FTP Client (not supported for current devices):



1. Connect your PC to the EG over Ethernet or Wi-Fi.
2. Run your FTP client.
3. Add FTP connection settings.
   a. Enter the EG IP address.
   b. Enter default FTP port 21.
   c. Enter the Username as 'guest' and Password as 'guest' or a configured Username and password.
   d. Set default remote directory to B:
4. Connect and view the directory on the EG. Only one FTP client at a time can connect to the EG.

   Ensure all other sessions are disconnected before opening a new session. There is a two-minute timeout period.
5. Transfer the uu file (or dfw file for older firmware) to the root of the B directory. The EG will perform the upgrade and reset (~10 seconds). Once the EG resets the new firmware will be activated.

- FTP cannot be used to update files on PDDEG-S, PDTS and PDEG (firmware 3.58 or later)
- EGs from Q2 2016 support all upgrade options.
  EGs newer than Q3 2014 support FTP upgrades.
  EGs older than Q3 2014 must use the standard IPv4/DyNet upgrade methods.
- When upgrading firmware with an FTP client you must use bootloader version 64v04 or newer with a uu file.

9 Appendix B: Replacing a 100BT

Where existing installations have a legacy DDNG100BT or a DMNG100BT (100BT), you can replace these devices with EGs. However, because the devices have different properties you must copy the individual property values between the devices.

The 100BT communicates over Ethernet using one of the following five modes:

1. Passive TCP – In this mode the local 100BT awaits a TCP connection made by a remote 100BT or PC application. DyNet Packets are transported using TCP Packets. This option is good for point-to-point networks over the internet.
2. Active TCP – In this mode the local 100BT initiates and maintains a TCP connection to a remote 100BT. DyNet Packets are transported using TCP Packets.
3. UDP – In this mode the local 100BT relays DyNet messages to multiple other 100BTs. DyNet Packets are transported using Broadcast UDP Packets. This option is good for multi-device networks within intranets.
4. HTML – In this mode the 100BT hosts basic web pages that can be used to send commands to and show status of the Dynalite network. A CGI interface provides the dynamic content for those pages. This option is good for providing a customized user interface to the Dynalite network.
5. Telnet - In this mode the local 100BT awaits a TCP connection made by a remote Ethernet enabled device or PC application. The DyNet Text protocol can be used to send commands to and retrieve status from the Dynalite network. This option is good for integration to third party devices that are Ethernet enabled.

The table below details functionality on each of the IP transport layers:

<table>
<tr><th>Mode</th><th>TCP</th><th>UDP</th><th>HTML</th><th>Telnet</th></tr>
<tr><td>Application</td><td colspan="2"></td><td>HTML, JavaScript, Flash</td><td>Telnet</td></tr>
<tr><td>Presentation</td><td colspan="2"></td><td>CGI</td><td>DyNet Text Protocol</td></tr>
<tr><td>Session</td><td>DyNet</td><td>DyNet</td><td>HTTP</td><td rowspan="2">TCP</td></tr>
<tr><td>Transport</td><td rowspan="2">TCP</td><td rowspan="2">UDP</td><td rowspan="2">TCP</td></tr>
<tr><td>Network</td></tr>
<tr><td>Data Link</td><td colspan="4">IP, ARP, DHCP, AutoIP</td></tr>
<tr><td>Physical</td><td colspan="4">Ethernet</td></tr>
</table>

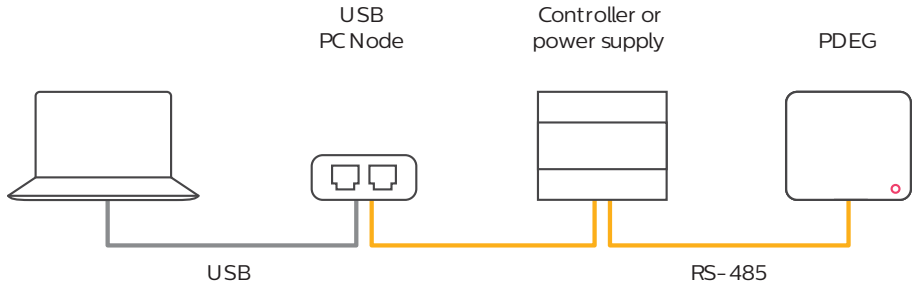
In operational systems, the 100BT was used primarily for the following applications:

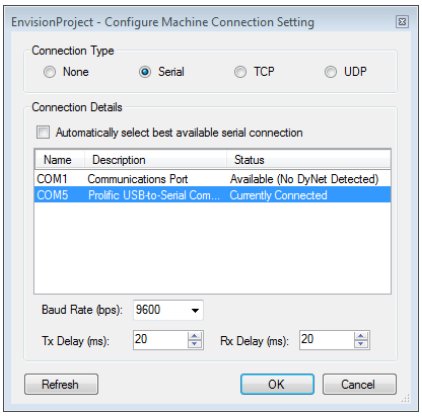
- Ethernet access point – the 100BT provides an intranet web interface to DyNet using common gateway interface (CGI) commands. With a port exposed to the internet it can be used for remote monitoring of sites.
- Ethernet bridge – the 100BT provides and Ethernet connection between DyNet RS-485 segments, to establish a trunk connection or where it is not practical to run DyNet cabling.

With an EG you have the option of connecting over Ethernet using the IPv6 default service address or over DyNet. The initial connection to the 100BT must be over DyNet until TCP properties are entered and saved to the device.

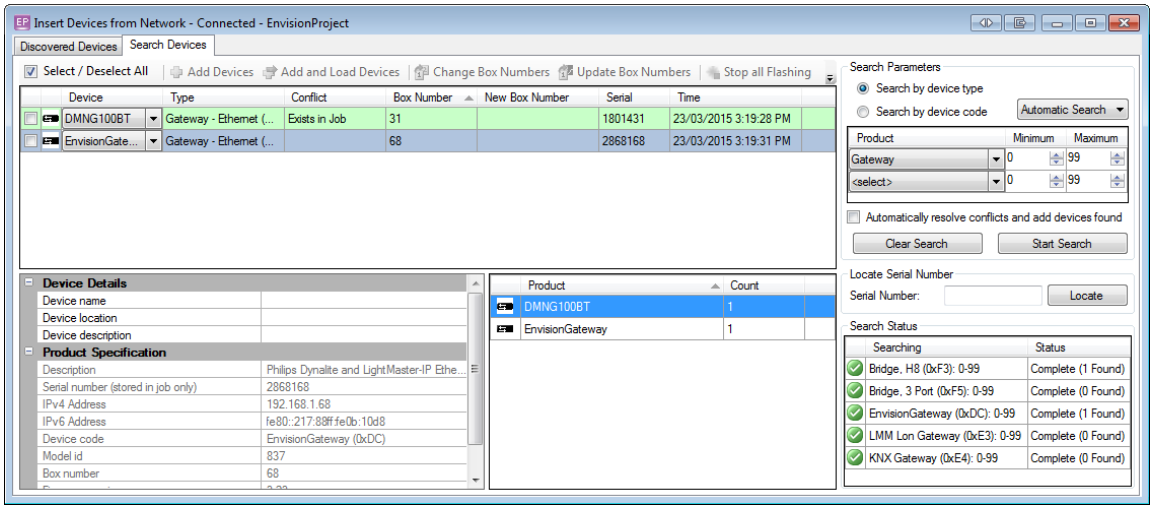
Configure EG to replace a 100BT Ethernet access point:

1. Plug the EG into a DyNet port on a spur to provide power and communications via the RS-485 network.
2. Plug the commissioning PC into a USB PC node, then plug the USB PC node into a DyNet port on the same spur.



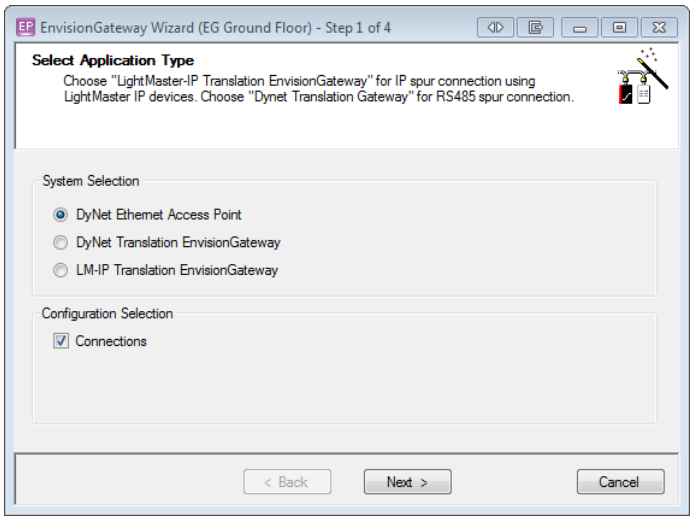


3. Launch SB and open the job file.
4. Select the job name.
5. In the Connections Settings page, click the Configure... button and connect using a serial connection.
6. Click Insert Devices from Network.
7. Press the Service switch on top of the EG (to sign-on the device) or search by device type for Gateway. The EG now appears in the Discovered Devices list.

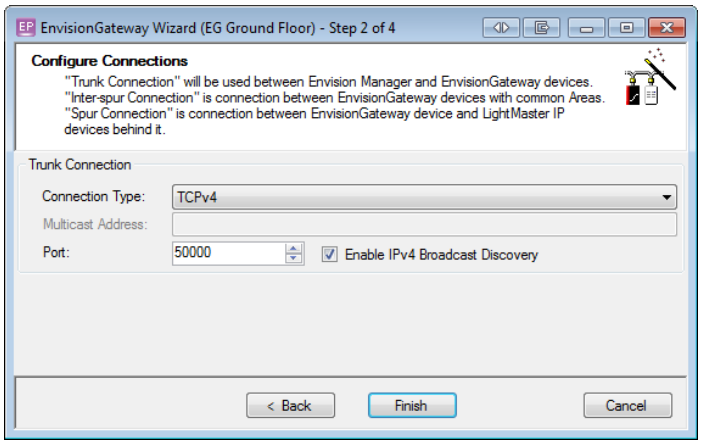


8. Select Add and Load Devices and close the dialogue box. The EG appears in the job.
9. Select the 100BT and copy the relevant properties to the EG (ensure you copy the 100BT Local IP address to the EG IP address).

10. Click Save to Device.
11. Right-click the EG in the Device tree and select Bridge Configuration Wizard... or press Alt+W.
12. Select DyNet Ethernet Access Point and click the Next button.



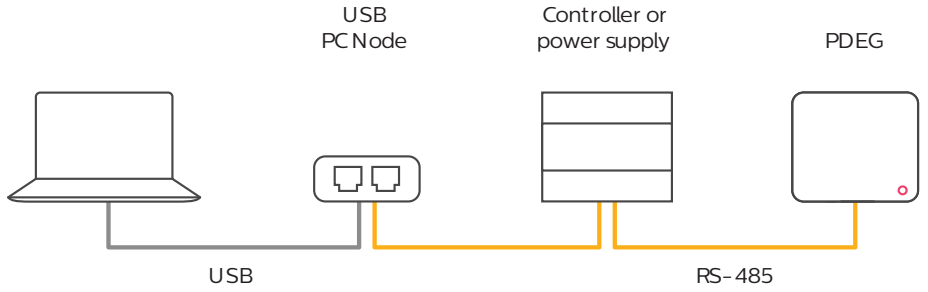
13. In Connection Type, select TCPv4 and in Port, select 50000. Click the Finish button.

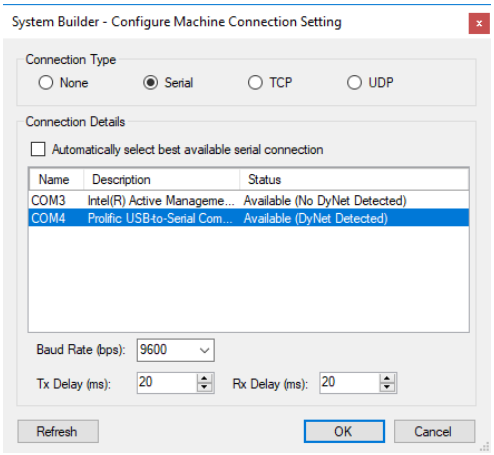


14. Select the EG and click Save to Device.
15. Right-click and select Upload logical configuration (Project.xml).
    Refer to 2.3.3 Wi-Fi access.
16. Delete the 100BT from the job.
17. Click File Save to save the job to your PC.

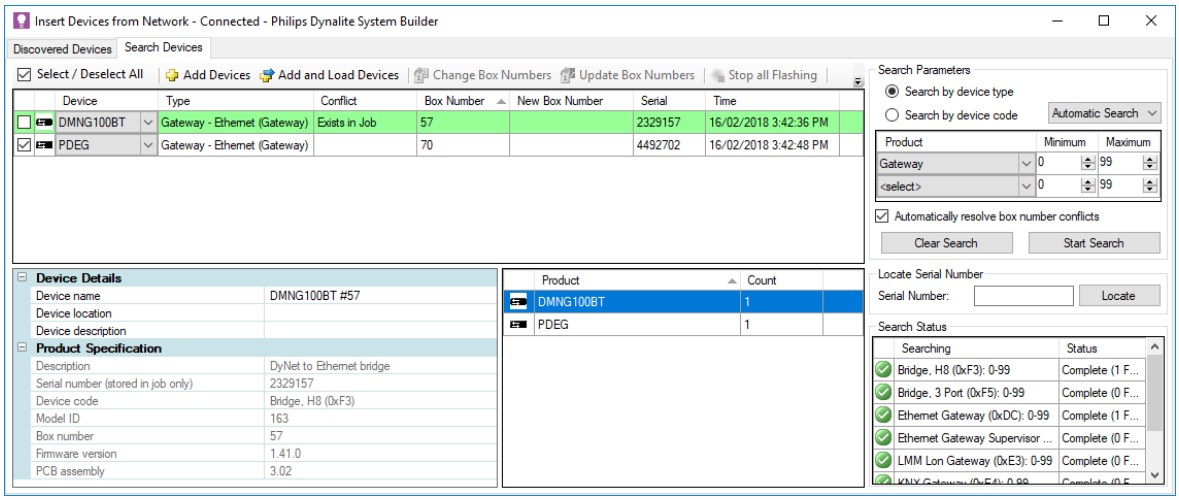
Configure EG to replace a 100BT Ethernet bridge:

1. Plug the EG into a DyNet port on a spur to provide power and communications via the RS-485 network.
2. Plug the commissioning PC into a USB PC node, then plug the USB PC node into a DyNet port on the same spur.



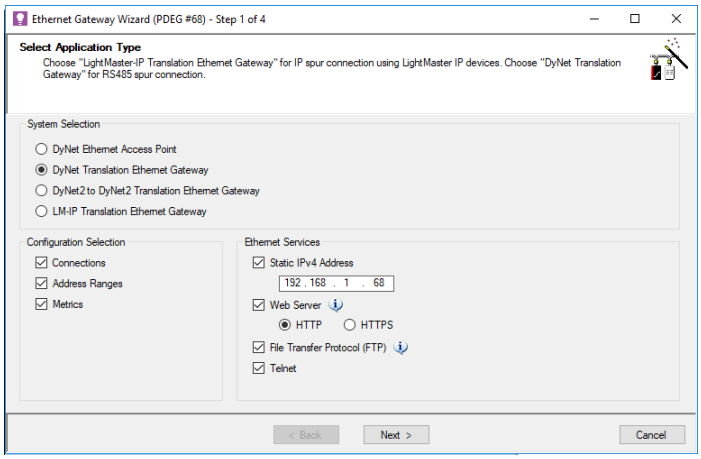


3. Launch SB and open the job file.
4. Select the job name.
5. In the Connections Settings page, click the Configure... button and connect using a serial connection.
6. Click Insert Devices from Network.
7. Press the Service switch on top of the EG (to sign-on the device) or search by device type for Gateway. The EG now appears in the Discovered Devices list.

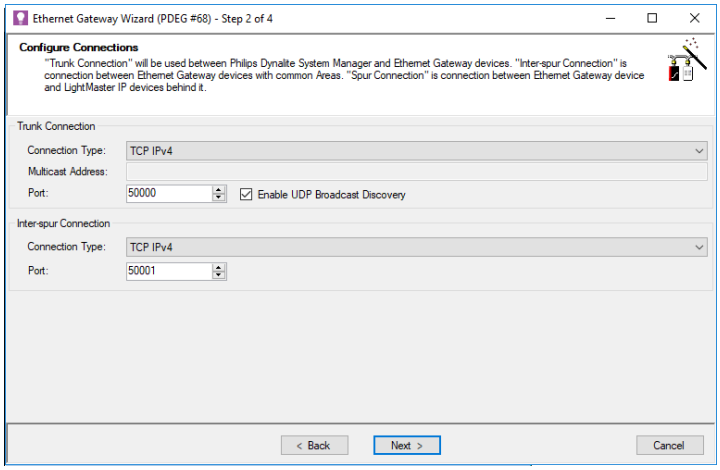


8. Select Add and Load Devices and close the dialogue box. The EG appears in the job.
9. Select the 100BT and copy the relevant properties to the EG (ensure you copy the 100BT Local IP address to the EG IP address).
10. Click Save to Device.

11. Right-click the EG in the Device tree and select
    Bridge Configuration Wizard... or press Alt+W.
12. Select DyNet Translation EG and click the Next button.



13. Under Trunk Connection, set the Connection Type to TCPv4, port 50000.
14. Under Inter-spur Connection, set the Connection Type as TCPv4, port 50001 and click the Next button. Ensure Enable UDP Broadcast Discovery is ticked.



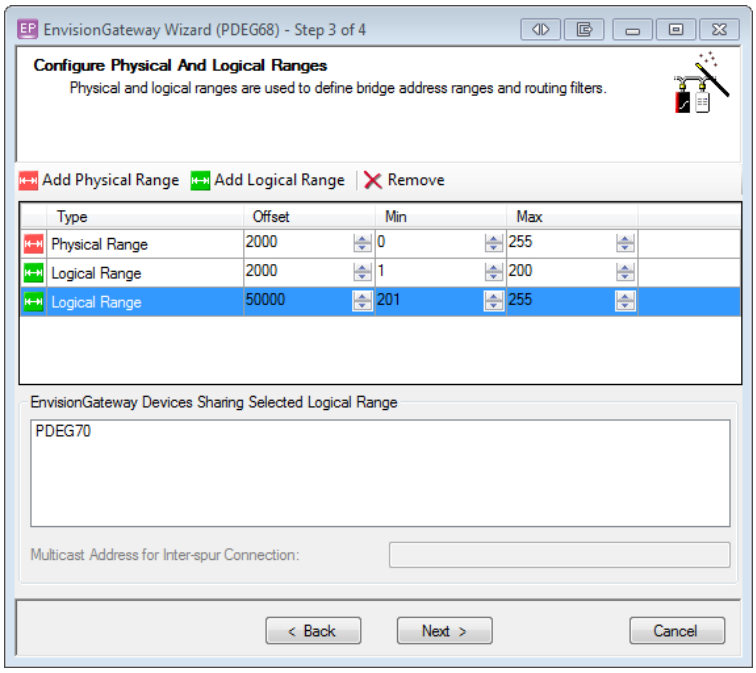
The Enable UDP Broadcast Discovery checkbox enables the UDP discovery port (Port 9998) used by SB to find the bridges in the system (listed in the Connection Settings page under Ethernet Trunk Connection Settings). It also enables DynamicTouch access.

15. Click the Add Physical Range icon and enter Offset, Min and Max values.
16. Click the Add Logical Range icon and enter Offset, Min and Max values.
    Primary address Min value must be 1 or 0 (see Note).
17. Click the Add Logical Range icon again to enter address ranges that are common to multiple EGs. The range defined by the Min and Max values must not overlap with the other logical ranges.

    SB lists the EG devices that it finds in the job that share common address ranges. The address ranges must match exactly.

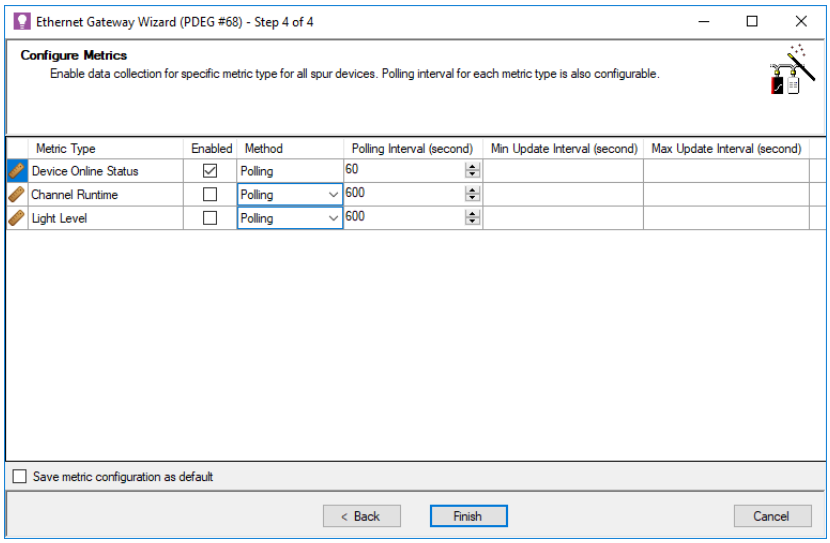
    Click the Next button.

The primary logical range for the spur can also be changed to start from 0 if you want to allow for Area 0 (All Areas) messages to be sent from the trunk. You must enable the Area Zero Transmit property on the port record for the EG and for all the devices on the spur.

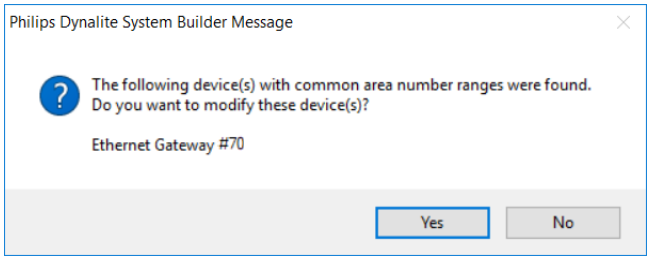


A common logical range enables the system to address areas that span multiple spurs. A common physical range enables devices to appear on a single spur when attached to different EGs.

18. Click the next button to accept the default metrics for devices and channels on the spur. You can tick/untick the checkbox or enter different polling periods, if applicable.



19. Click the Finish button.
20. A popup message indicates the other EGs that must have their settings saved.
21. Click Yes.



22. Click Save to Device.
23. Move all devices under the 100BT to under the EG.
24. Delete the 100BT from the job.
25. Click File Save to save the job to your PC.

10 Appendix C: Signify Certificate Installation

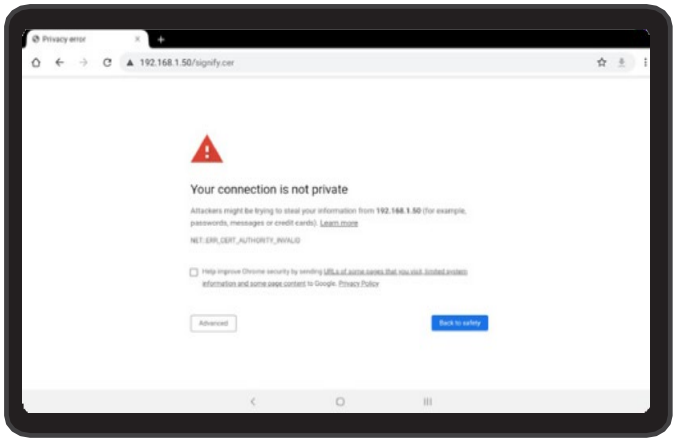
You can find the procedure how to install the certificate for every operating system in the following sections.

A certificate is required to enable a secure connection between the operating device (for example a tablet) and the gateway. When you use a device for the first time, while accessing the user interface the warning message “Your connection is not private”, or similar, shows up.

This instruction is written using a Chromium-based browser. Other browsers require similar steps, but for clarity it is recommended to also use a Chromium-based browser.

Download certificate:

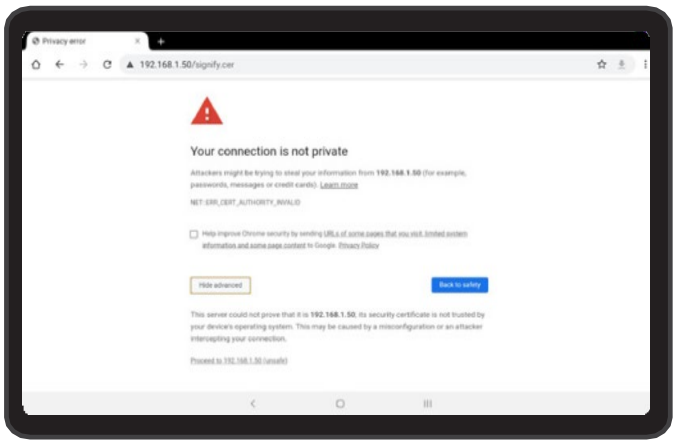
1. In the web-browser, go to https://[localhost]/Signify.cer or you can make your own SB certificate.
2. If the message **Your connection is not private** appears, click **Advanced**.



To establish a HTTPS connection with Dynalite Network devices using a System Builder certificate, it is required to install SB root CA certificate file in client systems.

You can use the SB Manage Certificate feature from a previous job file to download the root CA certificate file from a connected network device, such as a PDEG, and reuse this job file in future when you need to download the certificate.

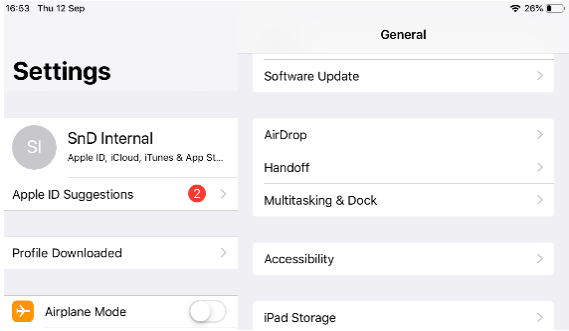
3. Click/Tap **Proceed to [localhost]/(unsafe).** The certificate is downloaded to the device.



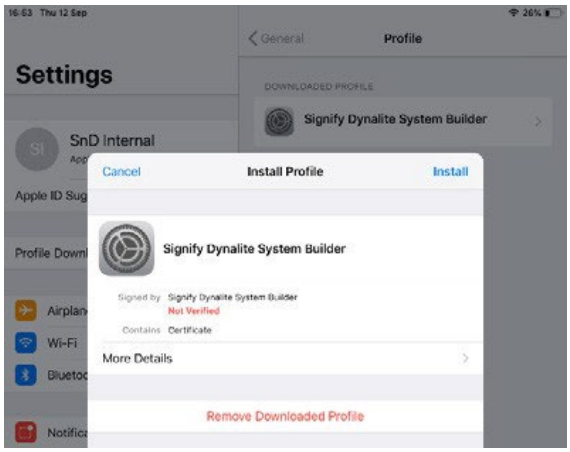
When given the option to open the file, ignore and click × to close the message.

Install the certificate on a tablet running iOS:

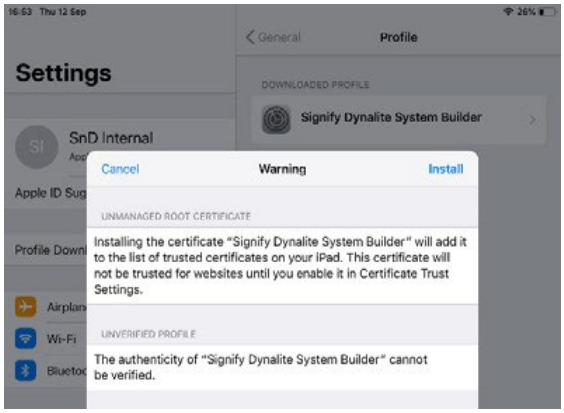
1. In Settings, select **Profile Downloaded.**



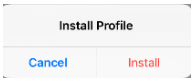
2. Select **Signify Dynalite System Builder**. Tap **Install.**



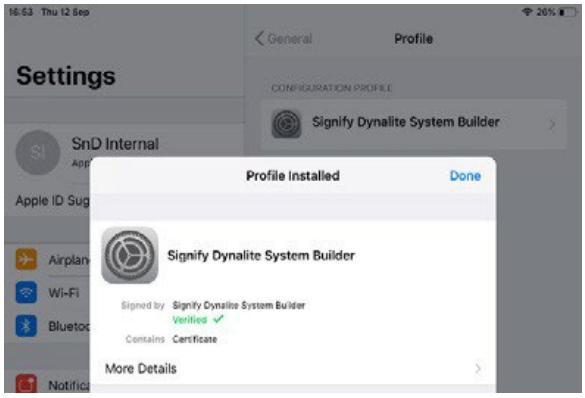
3. A warning appears, tap **Install**.



4. A popup appears to confirm, tap **Install**.



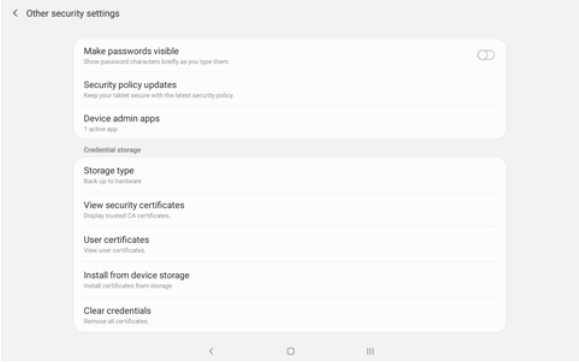
5. Tap **Done**



6. Clear the browser cache and close the web browser.

Install certificate on a tablet running Android:

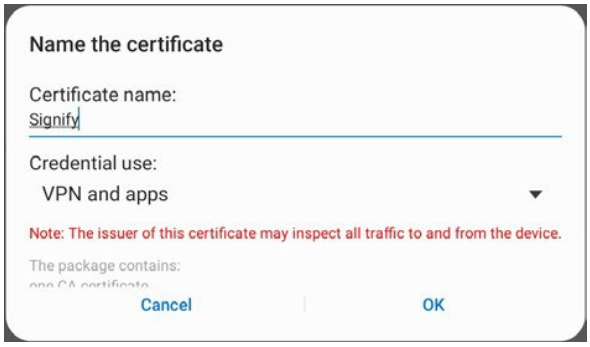
1. In Settings, tap **Security > Other security settings**.
2. Find Credential storage and tap **Install from device storage**.



3. Select the file **signify.cer** and tap **Done**.
4. Enter your Screen Lock (for example a pattern or PIN-code). Tap **OK**.

When you haven't defined a Screen Lock, you are asked to set one up. Without a Screen Lock, you can't install the certificate.

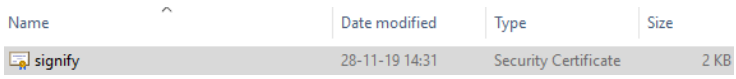
5. Give the certificate the name Signify.
6. Under Used for, select **VPN and apps**. Tap **OK**.



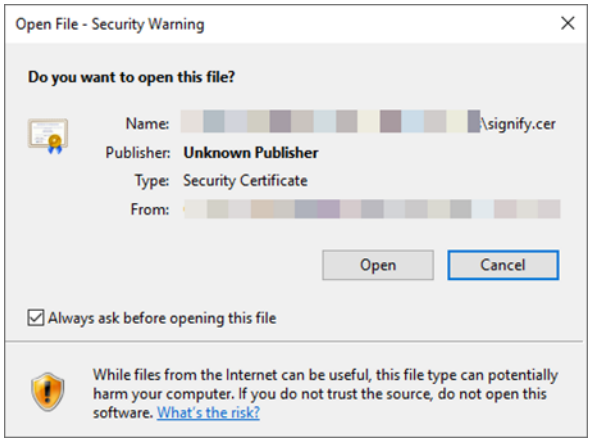
7. A message that the installation was successful appears.
8. Clear the browser cache and close the web browser.

Install certificate on a PC:

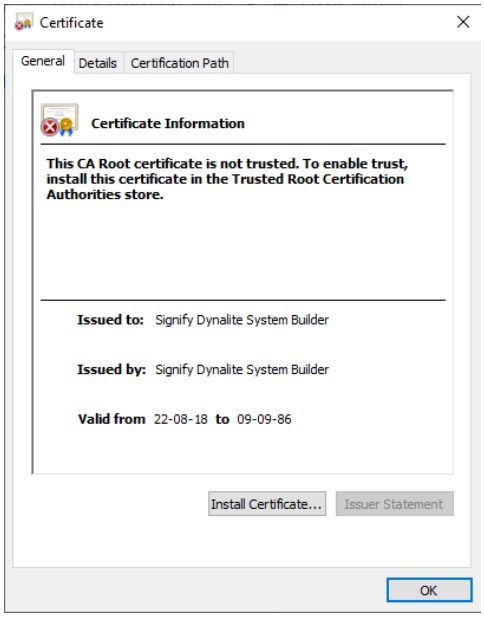
1. Find the certificate in the file system



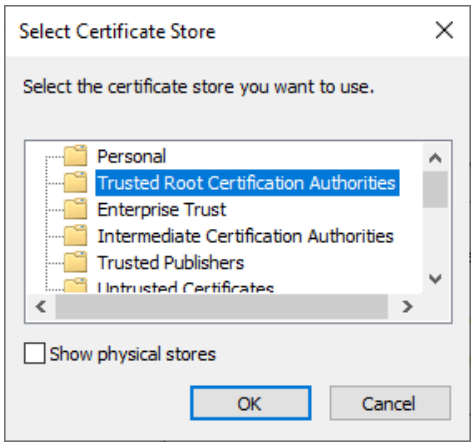
2. Double-click the certificate to start installation. Click **Open**.



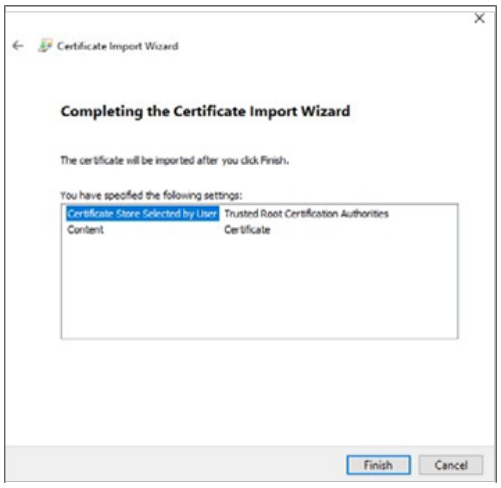
3. Click **Install Certificate...**



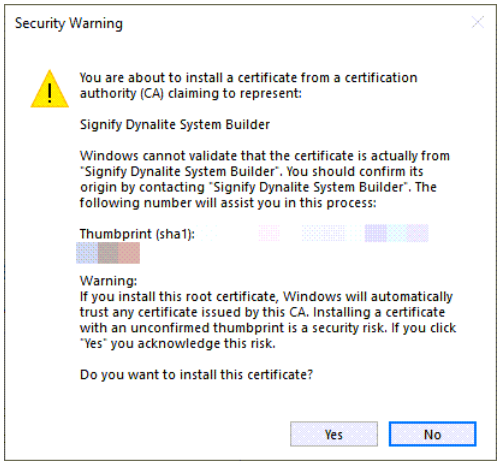
4. In the Certificate Import Wizard:
   - Select **Current User**. Click **Next**.
   - Select **Place all certificates in the following store**. Click **Browse**.
   - Select **Trusted Root Certification Authorities**. Click **OK**.



- Click Next, then click **Finish**



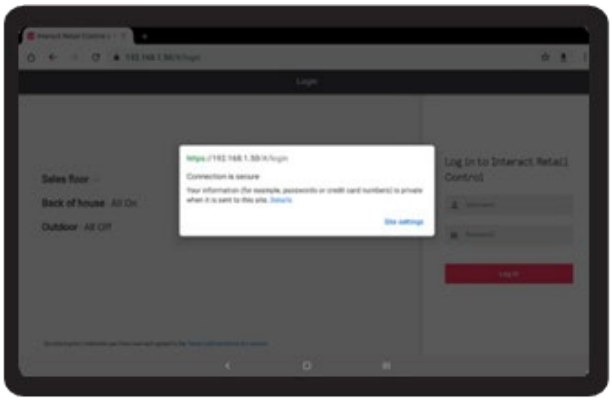
5. A Security Warning appears. Click **Yes**.



6. A message that the import was successful appears. Click **OK**.
7. Click **OK** to close the Certificate popup.
8. Clear the browser cache and close the web browser.

Check secure connection of the user interface:

1. Open the web-browser and go to https://[localhost]/. Login to the system.
2. Check the address bar if a closed padlock is displayed. You can click the padlock to see the details of the connection and certificate.



Philips Dynalite

www.lighting.philips.com/dynalite